3GPP TS 22.071 V5.1.1 (2002-03)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Location Services (LCS);
Service description, Stage 1
(Release 5)

Keywords
GSM, UMTS, location, stage 1

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 Specification (TS) has been produced by the 3GPP.

The contents of this document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of this TS, 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 specification;

1 Scope

This document provides the Stage One description of Location Services (LCS). A Stage One description provides an overall service description, primarily from the service subscriber's and user's points of view, but not dealing with the details of the Man Machine Interface (MMI). This TS includes information applicable to network operators, service providers and terminal, base station system, switch, and data base manufacturers.

NOTE: Location Services may be considered as a network provided enabling technology consisting of standardized service capabilities which enable the provision of location based applications. These applications may be service provider specific. The description of the numerous and varied possible location applications which are enabled by this technology are outside the scope of this specification. However, clarifying examples of how the functionality being specified may be used to provide specific location services is included in various sections of the specification.

This document provides core requirements to an extent sufficient to derive a complete definition of location services at the service level. However, the present document also provides additional requirements which may suggest in a non-normative manner certain ways the system may be implemented to support location services.

LCS can be offered without subscription to basic telecommunication services. LCS is available to the following categories of LCS clients:

- Value Added Services LCS Clients – use LCS to support various value added services. These clients can include UE subscribers as well as non-subscribers to other services.
- PLMN Operator LCS Clients – use LCS to enhance or support certain O&M related tasks, supplementary services, IN related services and bearer services and teleservices.
- Emergency Services LCS Clients – use LCS to enhance support for emergency calls from subscribers.
- Lawful Intercept LCS Clients – use LCS to support various legally required or sanctioned services.

LCS is applicable to any target UE whether or not the UE supports LCS, but with restrictions on choice of positioning method or notification of a location request to the UE user when LCS or individual positioning methods, respectively, are not supported by the UE.

LCS is being developed in phases with enhancements added in yearly releases:

1 GSM Release 98: This is the initial default phase of LCS. It provides a generic flexible architecture capable of supporting all positioning methods. Specific support is provided for Time Of Arrival (TOA), Enhanced Observed Time Difference (E-OTD) and Global Positioning System (GPS) based positioning methods. Support is provided for emergency services, value added services and PLMN operator services.

2 GSM Release 99: This provides the same capabilities as GSM Release 98, since GSM Release 98 specifications were copied as "mirror" specifications in GSM Release 99.

3 3GPP Release 99: LCS is supported in the circuit switched domain of the 3GPP core network (GMLC connected to MSC). UTRAN R99 specifications support cell coverage (ie cell identity) based LCS. (The radio interface RRC specification also support IPDL-OTDOA and network assisted GPS (assistance data broadcasting), but the UTRAN internal interfaces do not yet support these two methods in R99.)

4 3GPP Release 4 (including both UTRAN and GERAN): LCS shall be supported in the circuit switched domain and in the packet switched domain including GPRS. LCS shall be supported in GERAN and in UTRAN FDD and UTRAN TDD. The positioning methods in UTRAN will be at least the 3 methods identified earlier: cell coverage based, IPDL-OTDOA and assisted GPS. LCS support is to be included in the Open Service Architecture (OSA) including enhancements for the support of value added services, and support for the velocity parameter in the position request /response. The objective is to have common service descriptions for all Access Networks in this stage 1 specification. Possible deviations shall be noted in the text.

5 Future releases: For further study.

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*.

2.1 Normative references

[1] 3GPP TR 21.905: “Vocabulary for 3GPP Specifications”.

[2] 3GPP TS 23.032: "Universal Geographical Area Description"

[3] 3GPP TS 22.101: "Service principles"

[4] 3GPP TS 22.105: "Services and Service Capabilities"

[5] 3GPP TS 22.115: "Charging and Billing"

[6] 3GPP TS 22.121: "Virtual Home Environment"

[7] 3GPP TS 23.110: " UMTS Access Stratum; Services and Functions"

2.2 Informative references

[8] 3GPP TR 25.923: "Report on Location Services (LCS)"

[9] PD 30.lcs: "Project Plan for location services in UMTS"

[10] Third generation (3G) mobile communication system; Technical study report on the location services and technologies, ARIB ST9 December 1998.

[11] The North American Interest Group of the GSM MoU ASSOCIATION: Location Based Services, Service Requirements Document of the Services Working Group

3 Definitions and abbreviations

3.1 Abbreviations

For the purposes of the present document, in addition to 3GPP TR.21.905, the following abbreviations apply:

LCS	Location Service
NA-ESRD	North American Emergency Services Routing Digits
NA-ESRK	North American Emergency Services Routing Key
NANP	North American Numbering Plan

NOTE: In the present document, acronyms are used in the text as if they are read either in their fully expanded form or in their alphabet names with no consistent principle.

3.2 Definitions

For the purposes of the present document the following definitions apply:

Change of Area: is one event supported for deferred Location Requests. Change of Area means that the network is required to report the location or the occurrence of the event of the requested subscriber in triggered fashion immediately after the network (MSC/SGSN) processes the mobility event for the the new location of the subscriber. Usually new location is noticed after the Location Update, Handover, RAU, Registration or RANAP Location Report, e.g. when the SAI changes.

Codeword: access code, which is used by a Requestor or LCS Client in order to gain acceptance of a location request for a Target UE. The codeword is part of the privacy information that may be registered by a Target UE user.

Current Location: after a location attempt has successfully delivered a location estimate and its associated time stamp, the location estimate and time stamp are referred to as the 'current location' at that point in time.

Deferred location request: a location request where the location response (responses) is (are) required after specific event has occurred. Event may or may not occur immediately. In addition event may occur many times.

Immediate location request: a location request where a single location response only is required immediately.

Initial Location: in the context of an originating emergency call the location estimate and the associated time stamp at the commencement of the call set-up is referred to as 'initial location'.

Last Known Location: The current location estimate and its associated time stamp for Target UE stored in the LCS Server is referred to as the 'last known location' and until replaced by a later location estimate and a new time stamp is referred to as the 'last known location'.

LCS Client: a software and/or hardware entity that interacts with a LCS Server for the purpose of obtaining location information for one or more Mobile Stations. LCS Clients subscribe to LCS in order to obtain location information. LCS Clients may or may not interact with human users. The LCS Client is responsible for formatting and presenting data and managing the user interface (dialogue). The LCS Client is identified by a unique international identification, e.g. E.164, number or Access Point Name (APN).

NOTE: The LCS Client may reside inside or outside the PLMN.

LCS Client Access barring list: an optional list of MSISDNs per LCS Client where the LCS Client is not allowed to locate any MSISDN therein.

LCS Client Subscription Profile: a collection of subscription attributes of LCS related parameters that have been agreed for a contractual period of time between the LCS client and the service provider.

LCS Feature: the capability of a PLMN to support LCS Client/server interactions for locating Target UEs.

LCS Server: a software and/or hardware entity offering LCS capabilities. The LCS Server accepts requests, services requests, and sends back responses to the received requests. The LCS server consists of LCS components which are distributed to one or more PLMN and/or service provider.

Location Estimate: the geographic location of a UE and/or a valid Mobile Equipment (ME), expressed in latitude and longitude data. The Location Estimate shall be represented in a well-defined universal format. Translation from this universal format to another geographic location system may be supported, although the details are considered outside the scope of the primitive services.

North American Emergency Services Routing Digits (NA-ESRD): a telephone number in the North American Numbering Plan (NANP) that can be used to identify a North American emergency services provider and its associated LCS client. The ESRD also identifies the base station, cell site or sector from which a North American emergency call originates.

North American Emergency Services Routing Key (NA-ESRK): a telephone number in the North American Numbering Plan (NANP) assigned to an emergency services call by a North American VPLMN for the duration of the call. The NA-ESRK is used to identify (e.g. route to) both the emergency services provider and the switch in the VPLMN currently serving the emergency caller. During the lifetime of an emergency services call, the NA-ESRK also identifies the calling mobile subscriber.

PLMN Access barring list: an optional list of MSISDN per PLMN where any LCS Client is not allowed to locate any MSISDN therein except for certain exceptional cases.

Privacy Class: list of LCS Clients defined within a privacy exception class to which permission may be granted to locate the target UE. The permission shall be granted either on activation by the target UE or permanently for a contractual period of time agreed between the target UE and the service provider.

Privacy Exception List: a list consisting of various types of privacy classes (i.e. operator related, personal etc.). Certain types of classes may require agreement between the service provider and the target MS.**Target MS:** The UE being positioned.

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

Target UE: The UE being positioned.

Target UE Subscription Profile: the profile detailing the subscription to various types of privacy classes.

UE available: deferred Location Request event in which the MSC/SGSN has established a contact with the UE. Note, this event is considered to be applicable when the UE is temporarily unavailable due to inaction by the UE user, temporarily loss of radio connectivity or IMSI detach and so on. Note that IMSI detach is only applicable in the case UE has previously been registered and information is still kept in the node.

4 Functional Requirements

3GPP standards shall support location service features, to allow new and innovative location based services to be developed. It shall be possible to identify and report in a standard format (e.g. geographical co-ordinates) the current location of the user's terminal and to make the information available to the user, ME, network operator, service provider, value added service providers and for PLMN internal operations.

The location is provided to identify the likely location of specific MEs. This is meant to be used for charging, location-based services, lawful interception, emergency calls, etc., as well as the positioning services.

The standard shall support both GERAN and UTRAN to facilitate determination of the location of a mobile station.

The following subsections provide general descriptions of attributes that can be used to describe or characterize various location services.

The relative importance of these attributes varies from service to service. However, accuracy, coverage, privacy and transaction rate may be considered the primary distinguishing attributes that define a value-added service. Briefly:

- accuracy is the difference between actual location and estimated location,
- coverage is an expression of the geographic area in which the UE user will receive an adequate perceived quality of service,
- privacy describes the user's perception of confidentiality of the location information, and
- transaction rate indicates how frequently network messaging is required to support the service.

A general comparison of the specific attributes of various location-based services is provided in Annex C of this document.

4.1 High Level Requirements

The following high level requirements are applicable:

1 The supporting mechanisms should incorporate flexible modular components with open interfaces that facilitate equipment interoperability and the evolution of service providing capabilities.

2 The network should be sufficiently flexible to accommodate evolving enabling mechanisms and service requirements to provide new and improved services.

3 It shall be possible to provide multiple layers of permissions to comply with local, national, and regional privacy requirements.

4 Multiple positioning methods should be supported in the different Access Networks, including (but not limited to) UL-TOA, E-OTD, IPDL-OTDOA, Network Assisted GPS and methods using cell site or sector information and Timing Advance or RoundTrip Time measurements.

5 The location determining process should be able to combine diverse positioning techniques and local knowledge when considering quality of service parameters to provide an optimal positioning request response.

6 It should be possible to provide position information to location services applications existing within the PLMN, external to the PLMN, or in Mobile Equipment;

7 Support should be provided for networks based on an Intelligent Network architecture (i.e. with specific support for CAMEL based Location Services).

4.2 Location Information

Location Information consists of Geographic Location, Velocity, and Quality of Service information, as described in the subsequent sections.

4.2.1 Geographic Location

Provision of the geographic location of a target UE is applicable to all LCS services.

Note: For services other than LCS the network may also determine within which Cell or Service Area the Target UE is located ("Service Area" is a UTRAN concept and it may consist of one (in R99) or more than one cell). The Service Area information or Cell ID may be used for routing of calls or for CAMEL applications.

It should be noted that the Service Area concept is different from the Localized Service Area concept used for SoLSA.

4.2.2 Velocity

Velocity is the combination of Speed and Heading (direction) of a Target UE. The LCS Server may provide the Velocity of an UE.

For Value Added Services and PLMN Operator Services, the following is applicable:

Provision of the velocity of a target UE is application driven. Location Services may allow an LCS Client to request or negotiate the provision of velocity.

For Emergency Services there is no requirement to provide velocity.

4.3 Quality of Service

4.3.1 Horizontal Accuracy

The accuracy that can be provided with various positioning technologies depends on a number of factors, many of which are dynamic in nature. As such the accuracy that will be realistically achievable in an operational system will vary due to such factors as the dynamically varying radio environments (considering signal attenuation and multipath propagation), network topography in terms of base station density and geography, and positioning equipment available.

The accuracy for location services can be expressed in terms of a range of values that reflect the general accuracy level needed for the application. Different services require different levels of positioning accuracy. The range may vary from tens of meters (navigation services) to perhaps kilometers (fleet management).

The majority of attractive value added location services are enabled when location accuracies of between 25m and 200m can be provided.

Based on decreasing accuracy requirement some examples of location services are provided in table 4.1.

Table 4.1; Example of location services with decreasing accuracy requirement

· Location-independent	Most existing cellular services, Stock prices, sports reports
· PLMN or country	Services that are restricted to one country or one PLMN
· Regional (up to 200km)	Weather reports, localized weather warnings, traffic information (pre-trip)
· District (up to 20km)	Local news, traffic reports
· Up to 1 km	Vehicle asset management, targeted congestion avoidance advice
· 500m to 1km	Rural and suburban emergency services, manpower planning, information services (where are?)
· 100m (67%) · 300m (95%)	U.S. FCC mandate (99-245) for wireless emergency calls using network based positioning methods
· 75m-125m	Urban SOS, localized advertising, home zone pricing, network maintenance, network demand monitoring, asset tracking, information services (where is the nearest?)
· 50m (67%) · 150m (95%)	U.S. FCC mandate (99-245) for wireless emergency calls using handset based positioning methods
· 10m-50m	Asset Location, route guidance, navigation

Accuracy may be independently considered with respect to horizontal and vertical positioning estimates. Some location services may not require both, others may require both, but with different degrees of accuracy.

Given that the location estimate is the best possible within the bounds of required response time, the location estimates of a fixed position UE (assuming several estimates are made) will reveal a 'spread' of estimates around the actual UE position. The distribution of locations can be described by normal statistical parameters and suggests that a small proportion of location estimates may lie outside of the acceptable Quality of Service (QoS) parameters for specific services (as determined by the network operator).

It may be possible to provide information on the confidence that can be associated with a location estimate. This may be used by location services to decide if a position update should be requested, for example, if the reported accuracy falls below a threshold determined by the LCS Client or Network Operator for a specific service.

It may also be possible to determine velocity (speed and heading) information from a single location request. (i.e. the response to a single request may provide the results of multiple positionings).

When delivered with a location estimate, the confidence region parameters, speed and heading may allow an application to improve the service delivered to the UE user. Some examples are given below:

a) Confidence Region: Simple measure of uncertainty that specifies the size and orientation of the ellipse in which an UE is likely to lie with a predetermined confidence (e.g. 67%). The size of the confidence region may be used by the network operator or the LCS Client to request an updated location estimate.

b) Speed: enables e.g. congestion monitoring, and average travel time estimates between locations.

c) Heading: the location estimate of a vehicle may be improved to identify the appropriate side of the highway. This may enable the provision of traffic information that relates only to the user's direction of travel.

For Value Added Services and PLMN Operator Services, the following is applicable:

Accuracy is application driven and is one of the negotiable Quality of Service (QoS) parameters.

The precision of the location shall be network design dependent, i.e., should be an operator's choice. This precision requirement may vary from one part of a network to another.

The LCS shall allow an LCS Client to specify or negotiate the required horizontal accuracy. The LCS shall normally attempt to satisfy or approach as closely as possible the requested or negotiated accuracy when other quality of service

parameters are not in conflict. The achieved accuracy level of location information shall be indicated using the shapes and uncertainty areas defined in 3GPP TS 23.032 [2].

For Emergency Services (where required by local regulatory requirements) the following requirements shall be met:

- The LCS Server shall attempt to obtain the horizontal location of the calling UE, in terms of universal latitude and longitude coordinates, and shall provide this to an Emergency Service Provider. The accuracy shall be defined by local regulatory requirements. Annex A shows such requirements as exist in the United States.

NOTE: The LCS Server provides the location service capabilities but the mechanism by which location is reported to an emergency service provider is outside the scope of this service.

4.3.2 Vertical Accuracy

For Value Added Services, and PLMN Operator Services, the following is applicable:

The LCS Server may provide the vertical location of an UE in terms of either absolute height/depth or relative height/depth to local ground level. The LCS Server shall allow a LCS Client to specify or negotiate the required vertical accuracy. The LCS Server shall normally attempt to satisfy or approach as closely as possible the requested or negotiated accuracy when other quality of service parameters are not in conflict.

The vertical accuracy may range from about ten metres (e.g. to resolve within 1 floor of a building) to hundreds of metres.

For Emergency Services (where required by local regulatory requirements) there is no requirement for the support of vertical positioning.

4.3.3 Response Time

Different location based services, or different LCS Clients, may have different requirements (depending on the urgency of the positioning request) for obtaining a response. The location server may need to make trade-offs between requirements for positioning accuracy and response time.

For Value Added Services, and PLMN Operator Services, the following is applicable:

Response Time is one of the negotiable QoS parameters. Support of response time by a Public Land Mobile Network (PLMN) is optional. The LCS Server may allow a LCS Client to specify or negotiate the required response time (in the context of immediate location request, see table 1) either at provisioning or when the request is made. The LCS Server may optionally ignore any response time specified by the LCS Client that was not negotiated. If response time is not ignored, the LCS Server shall attempt to satisfy or approach it as closely as possible when other quality of service parameters are not in conflict.

For immediate location request response time options are as follows::

a) “no delay”: the server should immediately return any location estimate that it currently has. The LCS Server shall return either the Initial or Last Known Location of the Target UE. If no estimate is available, the LCS Server shall return the failure indication and may optionally initiate procedures to obtain a location estimate (e.g. to be available for a later request).

b) “low delay”: fulfillment of the response time requirement takes precedence over fulfillment of the accuracy requirement. The LCS Server shall return the Current Location with minimum delay. The LCS shall attempt to fulfill any accuracy requirement, but in doing so shall not add any additional delay (i.e. a quick response with lower accuracy is more desirable than waiting for a more accurate response).

c) “delay tolerant”: fulfillment of the accuracy requirement takes precedence over fulfillment of the response time requirement. If necessary, the server should delay providing a response until the accuracy requirement of the requesting application is met. The LCS Server shall obtain a Current Location with regard to fulfilling the accuracy requirement.

For Emergency Services (where required by local regulatory requirements) there may be no requirement to support negotiation of response time. The network shall then provide a response as quickly as possible with minimum delay. Response time supervision is implementation dependent.

4.4 Reliability

Reliability provides a measure of how often positioning requests that satisfy QoS requirements are successful. For some applications, such as cross-country vehicle tracking, this may not be especially critical. If a positioning attempt fails, due to lack of coverage or transient radio conditions, etc, another positioning attempt may be made. This attempt should be specified in Location Service Request. (see the section 5.3.1.1). However for other services, perhaps such as child tracking, reliability may be more important.

The network shall provide statistical reporting of reliability (QoS parameters) data.

4.5 Priority

Location requests for different services may be processed with different levels of priority.

For Value Added Services, and PLMN Operator Services, the following is applicable:

The LCS Server may allow different location requests to be assigned different levels of priority. A location request with a higher priority may be accorded faster access to resources than one with a lower priority and may receive a faster, more reliable and/or more accurate location estimate.

For Emergency Services (where required by local regulatory requirements) the location request shall be processed with the highest priority level.

4.6 Timestamp

For Value Added Services, and PLMN Operator Services, and Emergency Services (where required by local regulatory requirements), the LCS Server shall timestamp all location estimates provided to a LCS Client indicating the time at which the estimate was obtained.

4.7 Security

Specific local, national, and regional security regulations must be complied with.

Position information should be safeguarded against unapproved disclosure or usage. Position information should also be provided in a secure and reliable manner that ensures the information is neither lost nor corrupted. Audit records should be maintained of positioning requests and responses to facilitate resolution of security violations.

The LCS Client may be authorized by the LCS Server. Existing security mechanisms as well as security mechanisms of the LCS Server shall be used for authorizing the LCS Client and its request for location information.

For Value Added Services, the following is applicable:

Only authorized LCS Clients shall be able to access the LCS Server. Before providing the location of a Target UE to any authorized LCS Client, the LCS Server shall verify both the identity and authorization privileges of the LCS Client .

Once the LCS Server has verified that a particular LCS Client is authorized to locate a particular Target UE, any location estimate requested shall be provided to the LCS Client in a secure and reliable manner, such that the location information is neither lost, corrupted nor made available to any unauthorized third party.

For PLMN operator services, location information shall be provided in a secure and reliable manner. The ability to obtain location information shall depend on local regulatory laws and requirements in conjunction with requirements for UE privacy.

For Emergency Services (where required by local regulatory requirements) the following requirements shall be met:

Position information shall be provided to the Emergency Services Network as an authorized LCS client. Target UE authorization checks normally performed for value added services are not applicable (privacy is over-ridden). The position information shall be provided to the Emergency Services Network in a secure and reliable manner, such that the location information is neither lost, corrupted, nor made available to any unauthorized third party.

4.8 Privacy

Specific local, national, and regional privacy regulations must be complied with, and multiple layers of permissions may be required.

Location information must always be available to the network service provider.

Means shall be provided for the UE subscriber to control privacy for value added services.

The user shall be able to change the setting of the Privacy exception list at any time.

Unless required by local regulatory requirements, or overridden by the target UE User, the target UE may be positioned only if allowed in the UE subscription profile. In general, for valued added location services, the target UE being positioned should be afforded the maximum possible privacy, and should not be positioned unless the positioning attempt is explicitly authorized. In the absence of specific permission to position the target UE, the target UE should not be positioned.

It may also be possible for a target UE to authorize positioning attempts after the target UE is notified of a positioning request and the target UE grants permission for positioning This notification condition (notification with privacy verification) shall be specified in the Target UE Subscription Profile. (See the subsequent "target subscriber notification" section of this document for charging and billing aspects.)

The privacy of an inanimate asset for an embedded target UE may be completely defined by the UE subscriber.

Additionally, specific privacy exceptions may exist for compliance with mandated location based services (such as for emergency services or lawful intercept) which are required by national or local regulatory requirements.

For Value Added Services, the following is applicable:

The Target UE Subscriber shall be able to restrict access to the Location Information (permanently or on a per attempt basis). The LCS Client access shall be restricted unless otherwise stated in the Target UE Subscription Profile. The home network shall have the capability of defining the default circumstances in which the Target UE's Location Information is allowed to be provided - as required by various administrations and/or network requirements.

It shall be possible for location services to support conditional positioning. Under these conditions, an application that is granted conditional positioning authorization must notify and obtain positioning authorization from the user of the target UE prior to performing the positioning process. Thus the user of the target UE shall be able to accept or reject the positioning attempt.

The default treatment, which is applicable in the absence of a response from the Target UE, shall be specified in the Target UE Subscription Profile. Thus for some location services the default treatment may be to accept the positioning request, whereas for other location services the default treatment may be to reject the positioning attempt.

However, considering that in general, users shall be afforded the maximum possible privacy, and shall not be positioned unless the target subscriber authorizes the requesting location application to perform positioning, the default condition shall normally be to deny the positioning attempt.

For PLMN operator services, the target UE subscriber may be able to restrict access to location information used to enhance or support particular types of service. The LCS client access shall be restricted unless stated otherwise in the Target UE subscription profile. The target UE user shall not be notified of any authorized location attempt.

For Emergency Services (where required by local regulatory requirements) Target UEs making an emergency call may be positioned regardless of the privacy attribute value of the subscriber associated with the Target UE (or ME) making the call.

For Lawful Interception Services (where required by local regulatory requirements), target UEs may be positioned under all circumstances required by local regulatory requirements. The target UE user shall not be notified of any location attempt.

4.8.1 Service Type Privacy

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

The users shall be able to allow or deny their location information to be given to LCS clients providing an indicated type of service. The user could e.g. allow all dating type services to get location information but decline other types of services to get the user's location. The location request message issued by the LCS client may include a service identity,

and the LCS Server may interpret that the indicated service belong to a certain Service Type. The subscriber shall be able to define and set privacy rules based on service type, so that services belonging to that service type shall be handled according to the corresponding service type privacy setting.

It shall be possible to verify that the service type indicated by the LCS client is correct. The service type privacy check may be done by the LCS server or by the user of the target mobile.

The LCS Server shall be aware of what service types a certain LCS Client supports. The LCS Server shall map the service identity given by the LCS client to a service type, as described below. The PLMN operator defines to what service type the given service identity belongs to.

4.8.1.1 Standardized Service Types

Annex C 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 4.2 and are based on the services listed in Annex C. It is noted that not all services listed in Annex C need belong to a standardized service type.

It should be noted that only the names and identities (number) of the Service Types are standardized.

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

Table 4.2, Standardized Service Types

Location based services categories	Standardized Service Types
Public Safety Services	Emergency Services
	Emergency Alert Services
Location Sensitive Charging	
Tracking Services	Person Tracking
	Fleet Management.
	Asset Management
Traffic Monitoring	Traffic Congestion Reporting
Enhanced Call Routing	Roadside Assistance
	Routing to Nearest Commercial Enterprise
Location Based Information Services	Navigation
	City Sightseeing
	Localized Advertising
	Mobile Yellow Pages
Service Provider Specific Services	

Note: 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.

4.9 Service Authorization

Requests for positioning information should be processed only if the requesting application is authorized. The identity and authorization privileges of the requesting application should be verified prior to processing positioning requests.

4.10 Service Activation and De-Activation

To maximize the adoption of location services, the service activation process must be simple. Three types of service package, may be distinguished, each of which may require a different service activation process:

1 On Demand: the user accesses services only when required.

2 Period Subscription: the subscriber requires periodic availability of the service

3 Mixed: some services provided on subscription and the remainder on-demand.

The process of activation + service delivery + deactivation may be provided in a single transaction. It may be possible for a subscriber to activate a location service on one occasion before deactivating an existing invocation.

Furthermore, a location service may be 'enabled' at the point of sale as part of the service package purchased by the UE subscriber. The use of Over-The-Air (OTA) provisioning may allow the location feature to be enabled for UE-based positioning methods.

4.11 Coverage

In general an UE user should be able to access a location service anywhere within the operator's coverage area, or within the roaming area. Three levels of coverage may be considered:

1 Home Network - Complete

2 Home Network - Partial

3 Roaming Networks

Considering network topography and dynamically varying environmental factors, a network operator may not be able to guarantee homogeneous service quality across the entire home network geographic area, or roaming partners' networks. Even within those areas where service is offered, the provided quality of service may vary due to dynamic environmental (i.e. radio) conditions. Additionally, the location method may have an accuracy that depends on the UE location, for example due to varying radio conditions, cell configuration and cell density in different areas, and geometric dilution of precision.

Furthermore the roaming partner's network may not accept a similar location method to that experienced by the user in the home network.

Finally, the service may not be available in a roaming partner's network despite technical interoperability between the location method supported by the UE and the network.

Therefore coverage may be considered not only to be a technical attribute, but may also be related to roaming contracts between network operators. In general, provided that a roaming agreement exists, any properly authorized location-based service may position a Target UE in either the Home PLMN (HPLMN) or a Visited PLMN (VPLMN). It may also be noteworthy that some location based services (such as location based information services) may be especially attractive to subscribers roaming outside their home networks.

4.12 Roaming Target UE

With respect to roaming, specific local, national, and regional privacy regulations must be complied with, and multiple layers of permissions may be required.

Many location-based services may be especially attractive to subscribers roaming outside their home PLMN. As such, support should be provided for the transparent and consistent provision of location based services to the fullest extent possible. Consideration for roaming support should be provided with the following priorities:

1. Roaming between 3GPP networks.

2. Roaming between 3GPP systems and IMT 2000 family networks.

3. Roaming between 3GPP and ANSI-41 or other systems.

If the location capability in the VPLMN is compatible with that provided in the HPLMN, the same parameters must be provided to the location server in the VPLMN that would be provided to the server in the HPLMN to enable provision of the same services.

For Value Added Services, the following is applicable:

Provided that a roaming agreement exists, the LCS feature shall allow any properly authorized LCS client to request and receive the location of a particular Target UE when the Target UE is either located in its Home PLMN (HPLMN) or Visited PLMN (VPLMN). The LCS client shall be authorised by the HPLMN of the subscriber whose UE is the target of the location attempt. Any PLMN not supporting the LCS feature shall return a suitable error response to any other PLMN from which an LCS request is received. The requesting PLMN shall then infer that the LCS feature is not supported and provide a suitable error response in turn to the requesting LCS Client.

For PLMN Operator Services, location of any roaming target UE shall be supported in the VPLMN as allowed by both local regulatory requirements and considerations, where applicable, of UE privacy.

For Emergency Services (where required by local regulatory requirements) the Serving PLMN shall support the positioning of all Target UEs including roaming Target UEs currently serviced by that serving PLMN. There is no requirement for a HPLMN to position Target UEs that have roamed outside the HPLMN.

4.13 Support for all UEs

For value added services, and PLMN operator services, the LCS feature may be supported for all UEs.

For Emergency Services (where required by local regulatory requirements), positioning shall be supported for all UEs (i.e. including legacy UEs) where coverage is provided, and also UEs without a SIM/USIM.

Both “active” and “idle” UEs shall be capable of being positioned.

4.14 Support for Unauthorized UEs

For value added services, support of unauthorized UEs may be provided by the PLMN.

For PLMN operator services, positioning of unauthorized UEs may be provided by the PLMN as required by local regulatory requirements.

For Emergency Services (where required by local regulatory requirements), the PLMN shall support positioning for unauthorized UEs (i.e. including stolen UEs and UEs without a SIM/USIM).

NOTE: A subscriber is in general identified as an UE containing in it the SIM/USIM associated with the subscriber. In some exceptional cases (e.g., an Emergency call), an UE without a valid subscription recognized in the PLMN can become a Target UE. In such a case, the subscriber may be identified by the identity associated with the Mobile Equipment (ME) involved in the call.

4.15 Periodic Location Reporting

Periodic location reporting is the act of the LCS Server initiating multiple position locations spread over a period of time.

The periodic reporting function is generally applicable for asset management services and exists as several variants, each applicable to different value added services:

· Location reporting only within predetermined period	e.g. commercial asset tracking and, subject to provision of privacy, manpower planning.
· Periodic location reporting within specified period and reporting triggered by a specific event	e.g. high value asset security, stolen vehicle monitoring, home zone charging.
· Periodic location reporting triggered by a specific event	e.g. 24hr depot management, transit passenger information systems

Periodic location determination and reporting increases network traffic. However, scheduling the periods of location monitoring and reporting will reduce this. Finally, event-based logic provided by the network operator that monitors the asset (location and status) and only reports events that meet conditions agreed with the application may reduce network traffic further without reducing the QoS.

If this event-based or time-based decision process is the responsibility of the application and not the network operator then all of the above services can be regarded as periodic location reporting.

For value added services, and PLMN operator services, support of periodic location reporting may be provided by the PLMN.

When an LCS client activates Periodic Location Reporting, the LCS server shall be able to inform the target Ms of this activation according to the Privacy Exception List.

It should be possible for the target UE at any time to query the LCS server about any valid requests activated for that target UE, and/or cancel the request.

When a request is cancelled by the target UE, the LCS server shall inform the LCS client of this cancellation.

It should be possible for more than one LCS client to activate requests for the same target UE.

For Emergency Services (where required by local regulatory requirements), there is no requirement for the PLMN to support periodic location reporting.

4.16 UE-Based Location Calculation

UE-Based Location Calculation may be supported on either a per-request basis or autonomously whereby a single request from an UE subscriber enables UE based location calculation over an extended period without further interaction with the PLMN.

For Commercial Services, the following may be applicable for autonomous location:

The network may broadcast location assistance information to mobiles, which enables mobiles to calculate their own location. The network may encrypt the location assistance information. If the location assistance information is encrypted, a single common standardized encryption algorithm shall be used.

The location assistance information may be available to the UE at all times, continuously in idle mode and during a call, without additional point to point signalling. The network may request location information from the UE for operator or for service provider applications. For this purpose a point to point signalling connection must be established.

4.17 UE_Assisted LCS Location Calculation

The UE-Assisted Location Calculation is accomplished by network resources based upon radio ranging measurements provided by the UE.

For Commercial Services, the following may be applicable for UE-Assisted location services:

The network may broadcast assistance information to mobiles, which enables mobiles to obtain the appropriate radio ranging measurements. The network may encrypt the assistance information. If the assistance information is encrypted, a single common standardized encryption algorithm shall be used.

The assistance information may be available to the UE at all times, continuously in idle mode and during a call, without additional point to point signalling. The network may request radio ranging measurement data from the UE for operator or for service provider applications. For this purpose a point to point signalling connection must be established. Optionally, this point to point connection can be used to deliver the resulting location to the UE.

4.18 Mobile Originating Location

Mobile Originating Location is the capability of the mobile station to obtain its own geographical location or have its own geographic location transferred to another LCS client.

For Value Added Services, the following may be applicable:

There are three classes of mobile originating location:

Basic Self Location - The mobile station needs to interact with the network for each separate location request

Autonomous Self Location - The mobile station does not need to interact with the network for each separate location request. One interaction with the network enables the mobile station to obtain multiple location positionings over a predetermined period of time.

Transfer to Third Party – The location of the mobile station is transferred by request of the mobile station to another specified LCS client.

4.19 Network support for LCS

The provision of location services shall be possible without significantly adversely impacting the radio transmission or the signalling capabilities of the network.

5 Logical Description

5.1 Logical Reference Model

Figure 1 shows the logical reference model for LCS whereby an LCS Client is enabled to request location information for one or more certain target UEs from the LCS Server supported by a PLMN. The LCS Server employs a positioning function to obtain the location information and furnish the information to the LCS Client. The particular requirements and characteristics of an LCS Client are made known to the LCS Server by its LCS Client Subscription Profile. The particular LCS-related restrictions associated with each Target UE are detailed in the Target UE Subscription Profile. The LCS feature shall allow a Target UE to be positioned within a specified Quality of Service. The LCS feature shall allow the location of a Target UE to be determined at any time whilst the UE is attached.

The LCS feature shall support conveyance of both the location Quality of Service (QoS) requirements of the LCS Client and the location information returned to the LCS Client in a universal standard format.

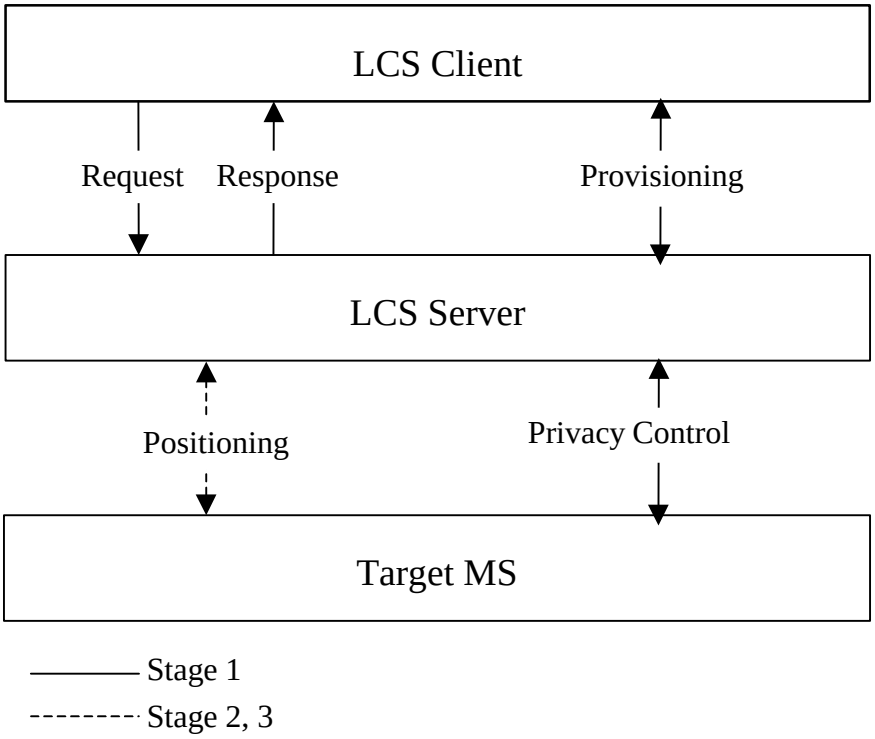


Figure 1. LCS Logical Reference Model

5.2 Functional Entities

5.2.1 LCS Client

An LCS Client is a logical functional entity that makes a request to the PLMN LCS server for the location information of one or more than one target UEs within a specified set of parameters such as QoS. The LCS Client may reside in an entity (including an UE) within the PLMN or in an entity external to the PLMN. When the LCS client resides in an entity external to the PLMN, the LCS client may be connected to several Requestors who originate the location requests. The specification of the LCS Client's internal logic and its relationship to any external user (e.g. Requestor) is outside the scope of this document.

5.2.2 LCS Server

An LCS server consists of a number of location service components and bearers needed to serve the LCS clients. The LCS server shall provide a platform which will enable the support of location based services in parallel to other telecommunication services such as speech, data, messaging, other teleservices, user applications and supplementary services and therefore enable the market for services to be determined by users and service providers. The LCS server may respond to a location request from a properly authorized LCS client with location information for the target UEs specified by the LCS client if considerations of target UE privacy are satisfied. The LCS server may enable an LCS client to determine the services provided to it by the LCS server through a process of provisioning.

5.2.3 Positioning Function

Positioning is the basic function that performs the actual positioning of a specific target UE. The input to this function is a positioning request from a LCS Client with a set of parameters such as QoS requirements. The end results of this function are the location information for the positioned target UE.

5.2.4 Target UE

The Target UE is the object to be positioned by the LCS Server. For network based positioning methods, no support for LCS is required by the target UE. For mobile assisted and mobile based positioning methods, the target UE actively supports LCS. For all positioning methods, the ability to control privacy may be required to be given to the UE user for each location request and/or to the UE subscriber through the Target UE subscription profile to satisfy local regulatory requirements (see the previous section on Privacy).

5.3 Functional Interfaces

5.3.1 LCS Client / LCS Server Interface

The LCS client/server use LCS messages to exchange information. Each LCS message contains a set of parameters.

In the case of UE Based positioning methods, if the LCS Client is located in the UE, then an internal LCS Client /LCS Server interface may be supported.

NOTE: Further regional/national specific interfaces between LCS clients and servers may need to be supported in addition to the interfaces described here.

5.3.1.1 Location Service Request

Using the Location Service Request, an LCS client communicates with the LCS server to request the location information for one or more target UEs within a specified set of quality of service parameters.

As shown in Table 1, a location service may be specified as immediate or deferred.

Table 1: Location Service Requests

Request Type	Response Time	Number of Responses
Immediate	Immediate	Single
Deferred	Delayed (event driven)	One or More

If a positioning attempt fails, the LCS server may make another positioning attempt. This attempt should be made when the target UE can be detected by the network. It may be possible for the LCS client to set this action as an option. This optional action should be applied for both request types.

Note: This functionality may be provided using one or more of the existing toolkits, including but not limited to CAMEL and OSA.

When using the Deferred type (event driven), the LCS client shall be able to set the following items:

- Time interval of positioning
- Number of responses (if needed)
- Valid period of the request (if needed)
- Type of event

  Currently following events are introduced:

  - UE available
  - Change of Area

It shall be possible for the LCS client to cancel the pre-arranged request.

It shall be possible for the LCS server to set the minimum time interval of positioning allowed.

It shall be possible to limit the area where the Change of Area event will be reported e.g use the OSA messages defined in 3GPP TS 29.198.

For Emergency Services, LCS shall support requests for the initial, the current (updated), or the last known position of an ME while a voice connection is established.

5.3.1.2 Location Service Response

The Location Service Response provides the result of a Location Service Request from the LCS Server to the LCS Client.

A LCS response is either '*immediate*' or '*deferred*'. The LCS Request indicates the type of response the LCS Client wishes to receive. The two types of location response are described in table 2.

Table 2: Types of LCS Response

Response	Description
Immediate	A Location Response is referred to as 'immediate ', when a response to a request for location information is answered immediately (within a set time). The response shall be single and not dependent to any event.
Deferred	A Location Response is referred to as 'deferred', when a response to a request for location information is returned after the occurrence of an event specified by the LCS client. The response can be single or periodic.

When the location positioning for the target UE has failed, the LCS server may be able to report the reason for failure and Last Known Location with the relevant timestamp.

5.3.1.3 Location Service Request Report

The Location Service Request Report provides the result of a deferred Location Service Request from the LCS Server to the LCS Client. The report is provided using a dialog between the LCS Client and the LCS Server that is initiated by the LCS Server.

5.4 Location information

5.4.1 Sources of location information

It shall be possible for the location determining process to make use of several sources of information in determining the location. Propagation and deployment conditions may limit the number or quality of measurements or additional measurements may be possible. Some ME may also have additional (independent) sources of position information. The LCS shall be capable of making use of the restricted or the extra information as appropriate for the service being requested.

6 Service Provision

6.1 Identification of a Target UE

For value added services, the following is applicable:

The LCS client shall identify a target UE using the UEISDN.

The LCS Client shall be able to identify the target UE using IP addressing.

For PLMN operator services, the LCS client may identify a target UE using any of the following:

MISISDN

IMSI

An identifier internal to the PLMN

For emergency services (where required by local regulatory requirements), the LCS client may identify a target UE using any one of the following:

MSISDN

IMSI

NA-ESRK + (optionally) IMEI

6.2 Location Information Provided to the LCS Client

For value added services, the following is applicable:

The LCS Server shall provide, on request, the current or most recent Location Information (if available) of the Target UE or, if positioning fails, an error indication plus optional reason for the failure.

For PLMN operator services (where allowed by local regulatory requirements and restrictions on UE privacy), Location Information for a particular target UE may be provided to a PLMN operator LCS client either on request or on the occurrence of an event in the LCS server that has been defined to equate to such a request.

For emergency services (where required by local regulatory requirements), the geographic location may be provided to an emergency services LCS Client either without any request from the client at certain points in an emergency services call (e.g. following receipt of the emergency call request, when the call is answered, when the call is released) or following an explicit request from the client. The former type of provision is referred to as a "push" while the latter is known as a "pull". In the case of a "pull", the emergency service LCS Client shall identify the Target UE as defined in section 6.1. Table 3 shows the information that may be provided to the client for either a "push" or a "pull".

Table 3: Location related information provided to an emergency services LCS Client

Type of Access	Information Items
Push	Current Geographic Location (if available) MSISDN IMSI IMEI NA-ESRK NA-ESRD State of emergency call – unanswered, answered, released (note 1)
Pull	Geographic location (note 2), either: Current location initial location at start of emergency call

NOTE 1: indication of call release means that any NA-ESRK will no longer identify the calling UE subscriber

NOTE 2: which type of location is required will be indicated by the LCS Client

6.3 LCS Client Subscription

It shall be possible for an LCS Client to subscribe to the LCS feature for third-party location with or without subscription to other services. A LCS Client may subscribe to one or more service providers' LCS feature in one or more PLMNs. The LCS Client Subscription Profile of a client may contain the range of QoS and subscriptions that the LCS Client is allowed to request.

For certain authorized LCS Clients internal to the PLMN, a subscription profile may be unnecessary. For these LCS Clients subscription to LCS feature is given implicitly as a result of subscription to an authorized PLMN service (e.g. supplementary services). These LCS Clients are empowered to access the LCS Server and request location information for a Target UE.

For emergency services, the subscription requirements to the LCS feature may not be needed.

6.4 Target UE Subscription

6.4.1 Privacy Subscription Options

It shall be possible for a Target UE Subscriber to subscribe to various types of privacy classes. The default treatment in the absence of the information to the contrary in the Target UE Subscription Profile shall be to assume that access is restricted to all LCS Clients (unless using privacy overriding, or otherwise overridden by local regulatory requirements).

Privacy Attributes consist of:

Codeword: an additional level of security that may be set by a Target UE user to determine which Requestors are allowed to request location information;

Privacy Exception List: determines which LCS Clients and classes of LCS Clients may position a Target UE;

Service Type Privacy: determines whether the service type allows the LCS Clients to get the position of a Target UE;

Privacy Override Indicator: determines applicability of the Privacy Exception List.

6.4.2 Codeword

It shall be possible for a Requestor to request location information by indicating a Codeword associated with the Target UE user. The codeword may be either checked by the Target UE/user or by any entity in the network. In the former case, the codword supplied by the requestor and forwarded by the LCS client with the request shall be forwarded to the TargetUE/user for verification and acceptance. In the latter case, the codeword shall be registered by the Target UE subscriber in advance. A comparision of the codeward sent by the requestor and the registered codeword shall be performed. A location request shall only be accepted if this comparision is successful. In the case where the Target UE/user does not check the codeword, the codeword need not be sent to the Target UE/user. In the case where the codeword is checked by the Target UE/user, the Target UE subscriber need not register the codeword in advance.

The other privacy settings should also be checked even when the codeword has been checked.

The Target UE Subscriber may register multiple codewords for multiple requestors. Once the codeword has been set and properly distributed, the Target UE user would be protected against location requests from third parties, which do not know the appropriate codeword.

It should be possible for a Target UE subscriber to enable and disable codeword checking.

The codeword is applicable to the value added services only.

6.4.3 Privacy Exception List

To support privacy, the LCS Server shall enable each Target UE Subscriber to subscribe to a “privacy exception list” containing the LCS Client identifiers, classes of LCS Clients, the target subscriber notification setting (with/without notification) and the default treatment, which is applicable in the absence of a response from the Target UE for each LCS Client identifiers.

The privacy exception list shall support a minimum of 20 clients. The maximum number of clients shall be determined by implementation constraints.

If the target subscriber notification is set as “notification with verification”, each positioning request from the LCS Client shall be notified to the target UE before positioning. The treatment for location request from the LCS Client, which is not registered in the privacy exception list, shall also be specified in the privacy exception list. An empty privacy exception list shall signify an intent to withhold location from all LCS Clients.

The classes that can be included are as follows.

- Universal Class: location services may be provided to all LCS Clients;

- Call/session-related Class: location services may be provided to any value added LCS clients or a particular value added LCS client or particular group of value added LCS Clients – where each LCS Client or group of LCS Clients is identified by a unique international identification, e.g. E.164 or Access Point Name (APN) that currently has a temporary association with the Target UE in the form of an established voice, data call or PS session originated by the Target UE. For each identified LCS Client or group of LCS Clients, one of the following geographical restrictions shall apply:

    a) Location request allowed from an LCS Client served by identified PLMN only;

    b) Location request allowed from an LCS Client served in the home country only;

    c) Location request allowed from any LCS Client;

- Call/session-unrelated Class; location services may be provided to a particular value added LCS Client or particular group of value added LCS Clients – where each LCS Client or group of LCS Clients is identified by a unique international identification, e.g. E.164, number or Access Point Name (APN). For each identified LCS Client or group of LCS Clients, one of the following geographical restrictions shall apply:

    a) Location request allowed from an LCS Client served by identified PLMN only;

    b) Location request allowed from an LCS Client served in the home country only;

    c) Location request allowed from any LCS Client;

PLMN Operator Class – location services may be provided by particular types of LCS clients supported within the HPLMN or VPLMN. The following types of clients are distinguished (see note):

a) Clients broadcasting location related information to the UEs in a particular geographic area – e.g. on weather, traffic, hotels, restaurants;

b) O&M client (e.g. an Operations System) in the HPLMN

c) O&M client (e.g. an Operations System) in the VPLMN

d) Clients recording anonymous location information (i.e. without any UE identifiers) – e.g. for traffic engineering and statistical purposes

e) Clients enhancing or supporting any supplementary service, IN service, bearer service or teleservice subscribed to by the target UE subscriber.

NOTE: The definitions of the various PLMN operator categories may be supplemented by more precise language in contractual agreements both between UE subscribers and their home service providers and between individual network operators with inter-PLMN roaming agreements. Such classification of the PLMN operator categories is outside the scope of this specification.

6.4.4 Privacy Override Indicator

The privacy override indicator is applicable to lawful intercept and emergency services as allowed by local regulatory requirements. It is not applicable to value added and PLMN operator services. The Privacy Override Indicator shall be used to determine whether Subscriber Privacy of the Target UE subscriber should be overridden or not. This indicator will be set for certain special LCS Clients when it is justified. Each LCS Client shall be associated with a particular value of a position privacy override indicator during the LCS Client provisioning. The privacy override indicator is normally only valid when the LCS Server for the LCS client is located in the same country of the Target UE. If agreed by bi-lateral agreements between operators, the privacy override indicator shall also be valid when the LCS client is not located in the same country as the Target UE.

6.4.5 Subscription to Mobile Originating Location

The UE subscriber may subscribe to the following types of Mobile Originating Location (as defined in section 4):

A) Basic Self Location

B) Autonomous Self Location

C) Transfer to Third Party

6.4.6 Requestor

The Location Request issued by the LCS client to GMLC shall 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 requestor shall be authenticated by the LCS client and/or the network.

The identity of the Requestor shall be included in the privacy interrogation request. It may be either checked by an entity in the network, the Target UE or the user.

6.5 Security

The LCS Server may authorize the LCS Client. There may be security mechanisms to authorize the LCS Client's request for locating a Target UE based on:

LCS Client access barring list(s),

PLMN/SP access barring list,

Point of origin of a location request.

6.6 Charging

The LCS Server shall enable a PLMN to charge LCS Clients for the LCS features that the PLMN provides. . The information that the operator uses to generate a bill to an LCS Client is operator or service provider specific. The charging information may be collected both for the LCS Client and for inter-network revenue sharing.

To support charging and billing for location services, additional information will need to be provided in call detail records.

Charging for value added location services may be provided on a transaction basis, periodically, or a mixture of both.

To support transaction based charging where applicable, service associated call detail records may need to include (as a minimum) the following additional information (depending on the specific service):

- Type and Identity of the LCS Client;
- Identity of the target UE;
- Results (e.g. success/failure, method used, position, response time, accuracy)
- Time Stamp;
- Type of coordinate system used.

6.7 LCS Open Service Architecture and Application Programming Interface

LCS shall support the Open Service Architecture (OSA) standardized Application Programming Interface (API). The OSA and Virtual Home Environment (VHE) service aspects of LCS are described in 22.121.

7 Provisioning and Administration

7.1 Procedures for an LCS Client

These procedures are concerned with the LCS client's provisioning and administration to the LCS feature.

7.1.1 Provisioning

Provisioning is an action to make the LCS feature available to a subscriber.

Provisioning may be:

- General: where the service may be made available to all subscribers without prior arrangements being made with the service provider (i.e. emergency calls).
- Pre-arranged: where the service is made available to an individual LCS Client only after the necessary arrangements have been made with the service provider.

7.1.2 Withdrawal

Withdrawal is an action taken by the service provider to remove an available LCS feature from a LCS Client's subscription profile.

Withdrawal may be:

- General: where the LCS feature is removed from all LCS Clients.
- Specific: where the LCS feature is removed on an individual basis per LCS Client.

7.1.3 Invocation

Invocation is an action to invoke the LCS feature, taken by the LCS Client (e.g. issuing a location request) or automatically by the LCS server as a result of a particular condition (e.g. periodic location request, mobile originating emergency call, etc.).

7.2 Procedures for a Target UE

These procedures are concerned with a Target UE's privacy exception list.. For emergency services, provisioning and withdrawal for Target UEs may not apply.

7.2.1 Provisioning

Provisioning is an an action to make the privacy exception list with its privacy classes available to a Target UE. The provision may be:

- General: where the list is made available to all Target UE's without prior arrangements being made with the service provider. The list shall contain the default privacy class.
- Pre-arranged: where any extra privacy permission class (--granting permission to locate an UE Client) shall be capable of being independently provisioned for a target UE as agreed with the service provider for a certain contractual period.

7.2.2 Withdrawal

Withdrawal is an action taken by the service provider to remove an available privacy class from a target UE's PEL. Withdrawal may be:

- General: where a privacy class is removed from all target UEs provided with this privacy class.
- Specific: where each of the privacy classes in the privacy exception list shall be independently withdrawn at the subscriber's request or for administrative reasons.

7.2.3 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 codeword
- the requestor
- the service types
- the target subscriber 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.

8 Interactions with Bearer and Teleservices and Other Services

LCS shall support location of any Target UE that is idle or has established any CS teleservice, bearer service or PS session.

Location of a GPRS terminal or an UE using SMS may be supported.

Provision of location services to assist supplementary services and CAMEL is outside the scope of this specification. The operation of location services shall be independent of other services - including Number Portability, private numbering, CAMEL, supplementary services, teleservices, and bearer services.

9 Cross Phase Compatibility between releases

This section details the cross phase compatibility requirements relating to the service requirements in this document.

Note: when a change is introduced which affects the 3GPP specifications, it is said to be 'backward compatible' if existing equipment can continue to operate and perform correctly with equipment that conforms to the new implementation.

9.1 Compatibility With Existing Standards

Where the service and operational requirements in this document relate to a core network functionality, compatibility is required.

UTRAN LCS mechanisms shall be developed to maximise synergies with earlier LCS phases.

9.2 Compatibility With Future Releases

It is envisaged that 3GPP standards will evolve in future releases, for example with the addition of new service requirements. The standards which define the technical implementation of LCS should be developed in such a way that it is practical to add the requirements in this section in a backward compatible manner.

Following chapters include requirements that are foreseen for future release.

9.2.1 Void

9.2.2 Location determination in call or PDP context activation and release

A possible future enhancement in LCS is that location information of a specific target UE may be obtained at the activation of a Call or PDP Context. A corresponding mechanism to obtain the location information of a specific target UE at the release of a Call or PDP Context may also be feasible.

9.2.3 Void

9.2.4 Defined geographical areas

It shall be possible to specify a geographical area as ellipse to a resolution that will be limited by the accuracy capability of the part of the serving network where the user is registered.

It may be possible to identify and report when the user's terminal enters or leaves a specified geographic area.

In order to enable ME to determine itself if it enters or leaves a defined geographical area information about the defined geographical area shall be made available to client. The method is FFS, one alternative is that cells covering parts of the geographical area broadcasts information about the geographical area.

9.2.5 Continuous check of location

The client may continuously check its current location with or without requesting signalling support from the network using the Self Location feature. In this way the client may become aware of entering or leaving a predefined geographical area, as defined above, and/ or it can supply the user or an application with real-time tracking information.

9.2.6 Identification of a Target UE

In future releases usage of IP addresses for UE identification shall be supported by the standard.

9.2.7 Void

9.2.8 VHE

LCS shall support VHE 22.121 [6].

Annex A (informative): USA FCC Wireless E911 Rules

Action was taken by the FCC on September 15, 1999, with respect to E911 location technology by the Third Report and Order (FCC 99-245).The FCC has adopted the following revisions to its wireless E911 rules:

- Wireless carriers who employ a Phase II location technology that requires new, modified or upgraded handsets (such as GPS-based technologies) may phase-in deployment of Phase II subject to the following requirements:

  - Without respect to any PSAP request for Phase II deployment, the carrier shall:

    1. Begin selling and activating ALI-capable handsets no later than March 1, 2001;
    2. Ensure that at least 50 percent of all new handsets activated are ALI-capable no later than October 1, 2001; and
    3. Ensure that at least 95 percent of all new digital handsets activated are ALI- capable no later than October 1, 2002.

  - Once a PSAP request is received, the carrier shall, in the area served by the PSAP:

  Within six months or by October 1, 2001, whichever is later:

    1. Ensure that 100 percent of all new handsets activated are ALI-capable;
    2. Implement any network upgrades or other steps necessary to locate handsets; and
    3. Begin delivering to the PSAP location information that satisfies Phase II requirements.

  Within two years or by December 31, 2004, whichever is later, undertake reasonable efforts to achieve 100 percent penetration of ALI-capable handsets in its total subscriber base.

- For roamers and other callers without ALI-capable handsets, carriers shall support Phase I ALI and other available best practice methods of providing the location of the handset to the PSAP.

- To be allowable under the FCC rules, an ALI technology that requires new, modified, or upgraded handsets shall conform to general standards and be interoperable, allowing roaming among different carriers employing handset-based location technologies.

- For carriers employing network-based location technologies, the FCC replaces its current plan, which requires that implementation be fully accomplished within 6 months of a PSAP request, with a revised rule requiring the carrier to deploy Phase II to 50 percent of callers within 6 months of a PSAP request and to 100 percent of callers within 18 months of such a request.

- The FCC adopts the following revised standards for Phase II location accuracy and reliability:

- For network-based solutions: 100 meters for 67 percent of calls, 300 meters for 95 percent of calls;

- For handset-based solutions: 50 meters for 67 percent of calls, 150 meters for 95 percent of calls.

- The FCC directs wireless carriers to report their plans for implementing E911 Phase II, including the technology they plan to use to provide caller location, by October 1, 2000. This report shall provide information to permit planning for Phase II implementation by public safety organizations, equipment manufacturers, local exchange carriers, and the FCC, in order to support Phase II deployment by October 1, 2001.

Annex B (informative): Descriptions of possible location based services

B1 Public Safety Services

Service providers offer these location-based services for the good of the public. They are made available without requiring pre-subscription.

B1.1 Emergency Services

Specific consideration of mandated Emergency Services is outside the scope of this specification. Such requirements may be regionally or nationally specific.

B1.1.1 Attributes

Specific consideration of the attributes for mandated Emergency Services is outside the scope of this specification. However, the current requirements specified by the U.S. FCC Phase II Mandate may be useful as an example.

> The FCC's Third Report and Order (FCC 99-245) in the matter of revision of the commission's rules to ensure compatibility with Enhanced 911 Emergency Calling Systems (CC Docket No. 94-102 RM-8143), adopted September 15, 1999, states:
>
> *We adopt the following revised standards for Phase II location accuracy and reliability:*
>
> - *For network-based solutions: 100 meters for 67% of calls, 300 meters for 95 percent of calls;*
> - *For handset-based solutions: 50 meters for 67% of calls, 150 meters for 95 percent of calls.*

The network should be sufficiently flexible to accommodate evolving enabling mechanisms and service requirements to provide new and improved services.

B1.1.2 Emergency Alert Services

Emergency Alert Services may be enabled to notify wireless subscribers within a specific geographic location of emergency alerts. This may include such alerts as tornado warnings, pending volcano eruptions, etc.

No requirements currently exist for Emergency Alert Services, and they may be considered for further study.

B2 Location Based Charging

Location Based Charging allows a subscriber to be charged different rates depending on the subscriber's location or geographic zone, or changes in location or zone. The rates charged may be applicable to the entire duration of the call, or to only a part of call's duration. This service may be provided on an individual subscriber basis, or on a group basis.

For example, when provided on an individual basis this service could apply reduced rates to those areas most often frequented by the subscriber by taking into consideration the subscriber's daily route and life style. Different rates may be applied at country clubs, golf courses, or shopping malls. For example, a "home" zone may be defined which is centered around a user's home, an agreed larger area, work or travel corridor or some unrelated zone. The zone may vary in size and shape from a cell (or sector) coverage area to a precisely defined polygon completely independent of cell coverage.

Additionally, different rates may be applied in different zones based on the time of day or week.

In addition to being applicable on an individual basis, this service may be applicable on a group basis, which may be desirable for example, for business groups. Locations may be defined for business groups to include corporate campuses, work zones or business zones with different tiers of charging rates.

Individual and group subscribers should be notified of the zone or billing rate currently applicable, and be notified when the rate changes. Location Based Charging may be invoked upon initial registration. A charging zone would then be associated with the subscriber's location. When the subscriber moves to a different zone, the subscriber would be notified.

This service should be transparently provided to the subscriber (i.e. independent of existing voice calls, data, or other services being provided).

B2.1 Attributes

Normal service operation includes invocation upon initial registration, autonomous registration, call origination, and call termination. Location-Based Charging should analyze location information to compare against service zones established for the subscriber. The service would notify the subscriber of their relative location to the established service zone, indicating either "in" or "out" of zone. As the subscriber changes location or predefined location service area they should be notified of their location-based charging service opportunity, being "in" or "out" of a subscribed zone. Except for subscriber notification, the user should experience transparency in interaction with other services (Voice, Data, SMS, etc).

This service may, as an option, be activated/de-activated using special feature codes on a subscriber or business customer basis.

B2.1.1 Target Subscriber Notification

The user needs to be informed on an ongoing basis which zone and billing rate is currently applicable.

Users should be enabled to make an informed decision on expected call charges and therefore need to be provided charging zone information accurately, and in a timely manner, being notified which zone they are in when a call is set up. Notification to the subscriber/user could be provided in several forms including tone, announcement, or short message.

The billing system will need to consider the following possible scenarios:

1. For the duration of the call, the subscriber remains in a single charging zone

2. During the call, the charging zones may change

2.1. The user may initiate a call in one zone, then move to a different zone where the call is terminated.

2.2. The user may cross back and forth between zones multiple times during the duration of a call, and the call may terminate in the zone it was originated from, or in a different zone.

Notification to the user may be via the UE MMI prior to initiation of the call and, during the call.

B2.1.2 Charging

To support appropriate charging, call detail records may need to include the following additional information:

1 Location Service (Location Based Charging) Identification

2 Location Information

3 Zone Information

4 Type of Event

5 Duration of Event

B2.1.3 Roaming

If a subscriber with active location based charging roams into a system that does not support the service, the subscriber may be notified of an "out of coverage zone" notification using the best possible method (UE display, SMS, etc.).

B3 Tracking Services

Although Fleet and Asset Management services may be offered as separate services, within this document they are described as a single service category. In a similar manner, Person Tracking may be viewed as a form of personal asset tracking.

B3.1 Fleet and Asset Management Services

Fleet and Asset Management services allow the tracking of location and status of specific service group users. Examples may include a supervisor of a delivery service who needs to know the location and status of employees, parents who need to know where their children are, animal tracking, and tracking of assets.

The service may be invoked by the managing entity, or the entity being managed, depending on the service being provided.

Fleet Management may enable an enterprise or a public organization to track the location of vehicles (cars, trucks, etc.) and use location information to optimize services.

Asset management services, for example, may range from asset visualization (general reporting of position) to stolen vehicle location and geofencing (reporting of location when an asset leaves or enters a defined zone). The range of attributes for these services is wide.

For Fleet and Asset Management services, a distinction may be made between the manager of the fleet/assets in charge of tracking, and the entities being tracked (service group users, etc). The tracking service may make use of mobile station handsets with possible specialized functions (Web browsers, etc) to allow for tracking and specific methods for communicating with the managing entity. A managing entity would be able to access one or several managed entities' location and status information through a specified communication interface (Internet, Interactive Voice Response, Data service, etc). The managing entity would be able to access both real-time and recent location and status results of managed entities.

The network shall provide the capability to provide the last known location and timestamp. In cases where the service group user's mobile station is not registered (i.e. Inactive, out of coverage) the last known location information and timestamp may optionally be provided. If this information is unavailable in real-time, a reason for why the information is unattainable may be provided. The managing entity may also be able to relay messages to service group users through the appropriate interface, as well as receive messages originated by the service group users.

Activation of Fleet and Asset Management services could be performed via subscriber provisioning by the service provider, as well as by offering subscriber-based service activation codes to the service group user/subscriber. The managing entity could also initiate service via requests to a provisioning system through Interactive Voice Response or Internet request. A feature code may optionally also be provided to allow for specific mobile user group subscriber activation by the managing entity (*FC + Mobile ID). A specific user group mobile could also be able to self-activate through the use of a feature code.

B3.2 Traffic Monitoring

Mobiles in automobiles on freeways anonymously sampled to determine average velocity of vehicles. Congestion detected and reported.

Congestion, average flow rates, vehicle occupancy and related traffic information can be gathered from a variety of sources including roadside telematic sensors, roadside assistance organizations and ad-hoc reports from individual drivers. In addition average link speeds can be computed through anonymous random sampling of UE locations.

B3.2.1 Attributes

B3.2.1.1 Privacy

Anonymous sampling of target UE requires all unique information relating to the UE location to be retained by the network operator. Depending on the capabilities of the location method (ref. section 3.4) traffic behavior described above can only be determined if an UE is sampled at least twice within a finite predetermined period.

The UE identification must be sufficiently unique to allow time separated measurements to be paired before discarding the source UE identification.

The level of uniqueness can be a highly truncated form of the UE-IMSI (or equivalent). For example maintaining 1000 unattached location estimates for subsequent pairing with future estimates will only require 3 least significant digits of the IMSI. Ambiguity in matching will occur but at a low (detectable) rate. Finally, all unattached estimates can be set to expire after a preset time.

B4 Enhanced Call Routing

Enhanced Call Routing (ECR) allows subscriber or user calls to be routed to the closest service client based on the location of the originating and terminating calls of the user. The user may optionally dial a feature or service code to invoke the service (*GAS for closest gas station, etc).

In addition to routing the call based on location, ECR should be capable of delivering the location information to the associated service client. For example, this capability may be needed for services such as Emergency Roadside Service. This could be used for the purpose of dispatching service agents for ECR service clients that can make use of this information.

ECR services may be offered, for example, through menu driven access allowing users to interactively select from a variety of services.

B5 Location Based Information Services

Location-Based Information services allow subscribers to access information for which the information is filtered and tailored based on the location of the requesting user. Service requests may be initiated on demand by subscribers, or automatically when triggering conditions are met, and may be a singular request or result in periodic responses.

The following subsections provide some examples of possible location based information services.

B5.1 Navigation

The purpose of the navigation application is to guide the handset user to his/her destination. The destination can be input to the terminal, which gives guidance how to reach the destination. The guidance information can be e.g. plain text, symbols with text information (e.g. turn + distance) or symbols on the map display. The instructions may also be given verbally to the users by using a voice call.

Note: this may involve a service provider giving verbal directions to a lost motorist, or providing periodic short text messages (possibly using SMS), in addition to, or as an alternative to the provision of a graphic map.

This can be accomplished through carrying a mobile phone that has location technology capabilities down to a few feet. Less granularity impedes the applicability of this functionality.

This service can either be menu driven from a handset using SIM Application Toolkit or a WAP based terminal with a map application running – similar to a GPS system. A central server may handle all mapping of locations, and may save specific locations (i.e., favorite fishing holes).

B5.2 City Sightseeing

City Sightseeing would enable the delivery of location specific information to a sightseer. Such information might consist of combinations of the services described throughout this document to describe historical sites, providing navigation directions between sites, facilitate finding the nearest restaurant, bank, airport, bus terminal, restroom facility, etc.

B5.3 Location Dependent Content Broadcast

The main characteristic of this service category is that the network automatically broadcasts information to terminals in a certain geographical area. The information may be broadcast to all terminals in a given area, or only to members of specific group (perhaps only to members of a specific organization). The user may disable the functionality totally from the terminal or select only the information categories that the user is interested in.

An example of such a service may be localized advertising. For example, merchants could broadcast advertisements to passersby based on location / demographic / psychographic information (for example "today only, 30% off on blue jeans").

B5.4 Mobile Yellow Pages

The internet has also changed how people find phone numbers. Instead of thumbing through the yellow pages or calling Directory assistance you simply go online and search the number. The need for paper copy phonebooks is gone. Wireless takes this one step further by adding the location of the subscriber to the search. Now the phone number of the nearest location can be ascertained as opposed to all locations within a 50-mile area.

Mobile Yellow Pages services provide the user with the location of the nearest service point, e.g. Italian restaurant. The result of the query may be a list of service points fulfilling the criteria (e.g. Italian restaurants within three kilometers). The information can be provided to the users in text format (e.g. name of the restaurant, address and telephone number) or in graphical format (map showing the location of the user and the restaurants).

B5.5 Location Sensitive Internet

Location Sensitive Internet is for further study.

B6 Network Enhancing Services

The Network Enhancing Services described in this section are for further study and privacy issues will require further consideration.

B6.1 Applications for Network Planning

The network operator may be able to use location information to aid network planning. The operator may be able to locate calls in certain areas to estimate the distribution of calls and user mobility for network planning purposes. These applications may be used for hot spot detection and user behavior modeling

B6.2 Applications for Network QoS Improvements

The network operator may be able to use location services to improve the Quality of Service of the network. The location system may be used to track dropped calls to identify problematic areas. The system may also be used to identify poor quality areas.

B6.3 Improved Radio Resource Management

The location of the handset may be used for more intelligent handovers and more efficient channel allocation techniques.

Appendix C (Informative): Attributes of Specific Services

The following table (provided by the GSM Alliance Services Working Group) depicts ranges of values that may be expected for various attributes of location based services.

Requirement -> Service Category	Service Authorization	Privacy	Target Subscriber Notification	Horizontal Accuracy	Vertical Accuracy	Response Time	Reliability	Security	Periodic Location Reporting	Service Registration	Service Activation	Service De-Activation	Service Invocation	Roaming	Service Specific Considerations	Interactions With Other Wireless Services
Public Safety Services																
Emergency Services	None req'd	Implied when dialing 911 info provided to safety organizations	Not required	Network based: 100m (67%) 300m (95%) Handset based: 50m (67%) 150m (95%)	n/a now (5-15m future?)	5 sec.	Same as GSM	Same as GSM	Required Period TBD suggest 1-10 minutes	None req'd	None required	Not Allowed	Keystroke or Dialed string (911)	Required if emergency call can be made		Lat and Long. To PSAP

Requirement -> Service Category	Service Authorization	Privacy	Target Subscriber Notification	Horizontal Accuracy	Vertical Accuracy	Response Time	Reliability	Security	Periodic Location Reporting	Service Registration	Service Activation	Service De-Activation	Service Invocation	Roaming	Service Specific Considerations	Interactions With Other Wireless Services
Emergency Alert Services	Req'd	Info only passed to subscribed to service provider	Not required	125 m (10 m future?)	n/a now (5-15m future?	5 sec.	Same as GSM	Same as GSM	Required Period TBD suggest 1-10 minutes	Req'd	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	Automatic	Preferred where roaming is allowed		Lat & Long to Service Provider Live, SMS or other data service (WAP,GPRS) return msg.
Location Sensitive Charging																
Home-Zone Billing	Req'd	Info only passed to subscribed to carrier	Not required	Depends on billing zone (5m-300m)	n/a	Depends on increments of billing.	Same as GSM	Same as GSM	Required depends on billing increment and coverage zone	Req'd	Interactive with Carrier	Interactive with Carrier	Automatic	n/a		Lat & Long to Carrier

Requirement -> Service Category	Service Authorization	Privacy	Target Subscriber Notification	Horizontal Accuracy	Vertical Accuracy	Response Time	Reliability	Security	Periodic Location Reporting	Service Registration	Service Activation	Service De-Activation	Service Invocation	Roaming	Service Specific Considerations	Interactions With Other Wireless Services
Tracking Services																
Fleet Mgment.	Req'd	Info only passed to subscribed to service provider	Not required	125m-Cell ID	n/a	5 sec.	Same as GSM	Same as GSM	Required (1-10 minutes)	Req'd	Interactive or live operator	Interactive or live operator	Interactive or live operator	Preferred where roaming is allowed		Lat & Long to Service Provider To requesting customer's interface (e-mail, Web or live operator

Requirement -> Service Category	Service Authorization	Privacy	Target Subscriber Notification	Horizontal Accuracy	Vertical Accuracy	Response Time	Reliability	Security	Periodic Location Reporting	Service Registration	Service Activation	Service De-Activation	Service Invocation	Roaming	Service Specific Considerations	Interactions With Other Wireless Services
Asset Mgment	Req'd	Info only passed to subscribed to service provider	Not required	10m-125m	n/a (5-15m future?	5 sec.	Same as GSM	Same as GSM	Required (1-10 minutes)	Req'd	Interactive or live operator	Interactive or live operator	Interactive or live operator	Preferred where roaming is allowed	Specail Terminal	Lat & Long to Service Provider To requesting customer's interface (e-mail, Web or live operator
Person Tracking	Req'd	Info only passed to subscribed to service provider	May be required (Child versus Employee?)	10m-125m	n/a (5-15m future?	5 sec.	Same as GSM	Same as GSM	Required (1-10 minutes)	Req'd	Interactive or live operator	Interactive or live operator	Interactive or live operator	Preferred where roaming is allowed		Lat & Long to Service Provider To requesting customer's interface (e-mail, Web or live operator

Requirement -> Service Category	Service Authorization	Privacy	Target Subscriber Notification	Horizontal Accuracy	Vertical Accuracy	Response Time	Reliability	Security	Periodic Location Reporting	Service Registration	Service Activation	Service De-Activation	Service Invocation	Roaming	Service Specific Considerations	Interactions With Other Wireless Services
Pet Tracking	Req'd	Info only passed to subscribed to service provider	Not required	10m-125m	n/a (5-15m future?	5 sec.	Same as GSM	Same as GSM	Required (1-10 minutes)	Req'd	Interactive or live operator	Interactive or live operator	Interactive or live operator	Preferred where roaming is allowed	Specia l Termi nal	Lat & Long to Service Provider To requesting customer's interface (e-mail, Web or live operator
Traffic Monitoring																
Traffic Congestion Reporting	Req'd	No specific Target UE info allowed	Not required	10-40m Hi- res. req'd muti- near proximity lanes (opposing and adjacent)	May be req'd for over-passes	5 sec.	Same as GSM	Same as GSM	Required (1-2 minutes)	Req'd	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	Preferred where roaming is allowed	High bandwidth req on network.	Lat & Long to Service Provider Live or SMS return msg.
Enhanced Call Routing																

Requirement -> Service Category	Service Authorization	Privacy	Target Subscriber Notification	Horizontal Accuracy	Vertical Accuracy	Response Time	Reliability	Security	Periodic Location Reporting	Service Registration	Service Activation	Service De-Activation	Service Invocation	Roaming	Service Specific Considerations	Interactions With Other Wireless Services
Routing to Nearest Commercial Enterprise	Req'd	Info only passed to subscribed to service provider	Not required	10m-125m	n/a	5 sec.	Same as GSM	Same as GSM	Not required	Req'd	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	Preferred where roaming is allowed		Lat & Long to Service Provider
Roadside Assistance	Req'd	Info only passed to subscribed to service provider	Not required	10m-125m	n/a	5 sec.	Same as GSM	Same as GSM	Not required	Req'd	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	Preferred where roaming is allowed		Lat & Long to Service Provider Live or SMS return msg.
Location Based Information Services																

Requirement -> Service Category	Service Authorization	Privacy	Target Subscriber Notification	Horizontal Accuracy	Vertical Accuracy	Response Time	Reliability	Security	Periodic Location Reporting	Service Registration	Service Activation	Service De-Activation	Service Invocation	Roaming	Service Specific Considerations	Interactions With Other Wireless Services
Navigation	Req'd	Info only passed to subscribed to service provider	Required	10m-125m	n/a	5 sec.	Same as GSM	Same as GSM	Required (1-10 minutes)	Req'd	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	Preferred where roaming is allowed		Lat & Long to Service Provider Live, SMS or other data service (WAP,GPRS) return msg.
City Sightseeing	Req'd	Info only passed to subscribed to service provider	Not required	10m-125m	n/a	5 sec.	Same as GSM	Same as GSM	Not required	Req'd	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	Preferred where roaming is allowed		Lat & Long to Service Provider Live, SMS or other data service (WAP,GPRS) return msg.

Requirement -> Service Category	Service Authorization	Privacy	Target Subscriber Notification	Horizontal Accuracy	Vertical Accuracy	Response Time	Reliability	Security	Periodic Location Reporting	Service Registration	Service Activation	Service De-Activation	Service Invocation	Roaming	Service Specific Considerations	Interactions With Other Wireless Services
Localized Advertising	Req'd	Info only passed to subscribed to service provider	Not required	125m-Cell ID	n/a	Not sensitive (default to 5 sec.)	Same as GSM	Same as GSM	Not required	Req'd	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	Preferred where roaming is allowed		Lat & Long to Service Provider SMS return msg.
Mobile Yellow Pages	Req'd	Info only passed to subscribed to service provider	Not required	125m-Cell ID	n/a	5 sec.	Same as GSM	Same as GSM	Not required	Req'd	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	By menu, keystroke, interactive or live operator	Preferred where roaming is allowed		Lat & Long to Service Provider Live, SMS or other data service (WAP,GPRS) return msg.
Service Provider Specific Services																
Network Planning	Not Req'd	Specific Target UE info allowed	Not Required	10m-Cell ID	n/a	5 sec.	Same as GSM	Same as GSM	Required (1 minute)	Not Req'd	N/a	n/a	n/a	n/a		n/a

Requirement -> Service Category	Service Authorization	Privacy	Target Subscriber Notification	Horizontal Accuracy	Vertical Accuracy	Response Time	Reliability	Security	Periodic Location Reporting	Service Registration	Service Activation	Service De-Activation	Service Invocation	Roaming	Service Specific Considerations	Interactions With Other Wireless Services
Dynamic Network Control	Not Req'd	Specific Target UE info allowed	Not Required	10m-Cell ID	n/a	5 sec.	Same as GSM	Same as GSM	Required (1 minute)	Not Req'd	N/a	n/a	n/a	n/a		n/a

Annex D (informative): Change history

Change history											
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	WI
Jun 1999			GSM 02.71					Transferred to 3GPP SA1	7.0.0		
SP-04			22.071						3.0.0		
SP-05	SP-99486	S1-99831	22.071	001	1	R99	C	UMTS LCS service requirements support for mobile originated positioning requests, and velocity as a service parameter	3.0.0	3.1.0	
SP-05	SP-99438	S1-99832	22.071	002		R99	B	UMTS LCS service requirements	3.0.0	3.1.0	
SP-05	SP-99438	S1-99833	22.071	003		R99	C	LCS accuracy requirements	3.0.0	3.1.0	
SP-05	SP-99479	S1-99625	22.071	004		R99	D	Editorial changes for alignment	3.0.0	3.1.0	
SP-06	SP-99522	S1-99955	22.071	005		R99	D	U.S. specific Emergency Services requirements included as an informative annex.	3.1.0	3.2.0	
SP-08	SP-000212	S1-000338	22.071	006		R00	C	Incorporation of TSG SA1#8 LCS Contributions and email contributions	3.2.0	4.0.0	
SP-09	SP-000378	S1-000484	22.071	008		R4	F	Correction to LCS Service Description Stage 1 Document (R'00)	4.0.0	4.1.0	
SP-09	SP-000392	S1-000667	22.071	009		R4	C	Provision of Velocity for Location Services	4.0.0	4.1.0	
SP-09	SP-000392	S1-000670	22.071	010		R4	B	External LCS client identity	4.0.0	4.1.0	
SP-09	SP-000392	S1-000671	22.071	011		R4	B	Privacy Control for LCS	4.0.0	4.1.0	
SP-09	SP-000392	S1-000672	22.071	012		R4	F	Privacy Control for LCS	4.0.0	4.1.0	
SP-09	SP-000392	S1-000673	22.071	013		R4	D	Clarifications to LCS on privacy and Service response	4.0.0	4.1.0	
SP-09	SP-000392	S1-000674	22.071	014		R4	F	LCS: Geographic Location	4.0.0	4.1.0	
SP-09	SP-000392	S1-000675	22.071	015		R4	D	Adding statement on "active" and "idle" UE in chapter 4.13	4.0.0	4.1.0	
SP-09	SP-000392	S1-000676	22.071	016		R4	D	Radio Access Network support for LCS	4.0.0	4.1.0	
SP-09	SP-000392	S1-000677	22.071	017		R4	D	LCS, Identification of a Target UE using IP addresses	4.0.0	4.1.0	
SP-09	SP-000392	S1-000678	22.071	018		R4	D	LCS: LCS Open Service Architecture (OSA) and Application Programming Interface.	4.0.0	4.1.0	
SP-10	SP-000544	S1-000787	22.071	019		Rel-4	B	Privacy Exception List	4.1.0	4.2.0	LCS
SP-10	SP-000544	S1-000788	22.071	020		Rel-4	B	Periodic Location Reporting	4.1.0	4.2.0	LCS
SP-10	SP-000544	S1-000791	22.071	021		Rel-4	B	Location Service Request	4.1.0	4.2.0	LCS
SP-10	SP-000544	S1-000851	22.071	022		Rel-4	C	Periodic Location Reporting amendment	4.1.0	4.2.0	LCS1
SP-10	SP-000544	S1-000803	22.071	023		Rel-4	C	Addition of achieved location information accuracy with reference to TS 23.032	4.1.0	4.2.0	LCS1
SP-11	SP-010044	S1-010235	22.071	024		Rel-4	C	Quality level negation	4.2.0	4.3.0	LCS1
SP-11	SP-010044	S1-010239	22.071	025		Rel-4	C	Location determination in call or PDP context activation and release	4.2.0	4.3.0	LCS1-PS
SP-11	SP-010044	S1-010237	22.071	026		Rel-4	C	OSA support for LCS	4.2.0	4.3.0	LCS1
SP-11	SP-010044	S1-010218	22.071	027		Rel-4	D	Editorial Cleanup	4.2.0	4.3.0	LCS1
SP-11	SP-010044	S1-010269	22.071	028		Rel-4	C	Number of LCS Clients	4.2.0	4.3.0	LCS1

SP-14	SP-010673	S1-011285	22.071	029		Rel-5	C	Privacy Override Indicator	4.3.0	5.0.0	LCS1
SP-15	SP-020047	S1-020467	22.071	030		Rel-5	B	CR 22.071 Rel.5 B Requestor	5.0.0	5.1.0	LCS1
SP-15	SP-020047	S1-020478	22.071	031		Rel-5	B	CR 22.071 Rel.5 B Introducing service type privacy for location services	5.0.0	5.1.0	LCS1
SP-15	SP-020047	S1-020479	22.071	032		Rel-5	C	Introduction of a Codeword Setting	5.0.0	5.1.0	LCS1
SP-15	SP-020047	S1-020632	22.071	033		Rel-5	B	CR to 22.071 on Clarifying checking of requester ID	5.0.0	5.1.0	LCS1
SP-15	SP-020043	S1-020455	22.071	036		Rel-5	A	CR 22.071 Rel-5 A Closure of a loophole in the privacy settings	5.0.0	5.1.0	TEI
SP-15	SP-020047	S1-020466	22.071	037		Rel-5	B	CR 22.071 Rel.5 B Deferred Location Request with Change of Area Event	5.0.0	5.1.0	LCS1
SP-15	SP-020045	S1-020457	22.071	039	-	Rel-5	A	Editorial CR to correct terms and references	5.0.0	5.1.0	CORRECT
			22.071	-	-	Rel-5		Editorial to change page layout for Annex C	5.1.0	5.1.1	

3GPP TSG SA WG3 Security — S3#23
14 - 17 May 2002
Victoria, Canada

S3-020303_2

3GPP TS 23.271 V5.2.0 (2002-03)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional stage 2 description of LCS (Release 5)

Keywords
UMTS, location, stage 2

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 Specification (TS) 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.

1 Scope

The present document specifies the stage 2 of the LoCation Services (LCS) feature in UMTS and GSM, which provides the mechanisms to support mobile location services for operators, subscribers and third party service providers.

The present document replaces the specifications TS 23.171 (Release 1999) and the system and core network parts of GSM 03.71 (Release 1999). TS 43.059[16] replaces the radio access network parts of GSM 03.71 (Release 1999).

Location Services may be considered as a network provided enabling technology consisting of standardised service capabilities, which enable the provision of location applications. The application(s) may be service provider specific. The description of the numerous and varied possible location applications which are enabled by this technology are outside the scope of the present document. However, clarifying examples of how the functionality being described may be used to provide specific location services may be included.

This stage 2 service description covers the LCS system functional model for the whole system, the LCS system architecture, state descriptions, message flows, etc.

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*.

2.1 Normative references

[1] 3G TS 25.305: "Stage 2 functional specification of UE positioning in UTRAN".

[2] GSM 01.04 (ETR 350): "Abbreviations and acronyms".

[3] 3G TS 21.905: "UMTS Abbreviations and acronyms".

[4] 3G TS 22.071: "Technical Specification Group Systems Aspects; Location Services (LCS); Stage 1".

[5] (void)

[6] 3G TS 48.008: "Mobile-services Switching Centre - Base Station System (MSC - BSS) interface; Layer 3 specification".

[7] 3G TS 22.100: "UMTS phase 1 (Release 1999)".

[8] 3G TS 22.101: "Service principles".

[9] 3G TS 22.105: "Services and Service Capabilities".

[10] 3G TS 22.115: "Charging and Billing".

[11] 3G TS 23.032 (GSM 03.32): "Universal Geographical Area Description (GAD)".

[12] 3G TS 22.121: "The Virtual Home Environment".

[13] 3G TS 23.110: "UMTS Access Stratum Services and Functions".

[14] 3G TS 25.413: "UTRAN Iu Interface RANAP signaling".

[15] 3G TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[16] 3G TS 43.059: "Functional Stage 2 description of Location Services in GERAN".

[17] 3G TS 23.003: "Numbering, addressing and identification".

[18] 3G TS 29.002: "Mobile Application Part (MAP) Specification".

[19] GSM 04.02: "GSM Public Land Mobile Network (PLMN) access reference configuration".

[20] 3G TS 23.002: "Network architecture".

[21] 3G TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL) - stage 2".

[22] 3G TS 23.011: "Technical realization of Supplementary Services".

[23] 3G TS 23.007: "Restoration procedures".

[24] 3G TS 24.008: "Mobile Radio Interface - Layer 3 MM/CC Specification".

[25] 3G TS 25.331 "RRC protocol specification".

[26] 3G TS 23.127 "Virtual Home Environment/Open Service Access".

[27] 3G TS 29.198-1: “Open Service Access (OSA); Application Programming Interface (API); Part 1; Overview”.

[28] 3G TS 29.198-2: “Open Service Access (OSA); Application Programming Interface (API); Part 2; Common Data”.

[29] 3G TS 29.198-3: “Open Service Access (OSA); Application Programming Interface (API); Part 3; Framework”.

[30] 3G TS 29.198-6: "Open Service Access (OSA); Application Programming Interface (API); Part 6: Mobility".

[31] LIF TS 101 V2.0.0 "Mobile Location Protocol Specification" (Location Interoperability Forum 2001) [Available at http://www.locationforum.org/public_document_area.htm]

2.2 Informative references

[32] Third generation (3G) mobile communication system; Technical study report on the location services and technologies, ARIB ST9 December 1998.

[33] The North American Interest Group of the GSM MoU ASSOCIATION: Location Based Services, Service Requirements Document of the Services Working Group.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

CAMEL: CAMEL is a network functionality, which provides the mechanisms of Intelligent Network to a mobile user

Call Related: any LCS related operation which is associated with an established call in CS domain and a session via an active PDP context in PS domain.

Current Location: after a location attempt has successfully delivered a location estimate and its associated time stamp, the location estimate and time stamp is referred to as the "current location" at that point in time

Deferred location request: location request where the location response (responses) is (are) not required immediately

Global Positioning System: Global Positioning System (GPS) consists of three functional elements: Space Segment (satellites), User Segment (receivers), and Control Segment (maintenance etc.). The GPS receiver calculates its own position based on the received time differences for several satellites

Immediate location request: location request where a single location response only is required immediately

Initial Location: in the context of an originating emergency call the location estimate and the associated time stamp at the commencement of the call set-up is referred to as "initial location"

Last Known Location: current location estimate and its associated time stamp for Target UE stored in the LCS Server is referred to as the "last known location" and until replaced by a later location estimate and a new time stamp is referred to as the "last known location"

LCS (LoCation Services): LCS is a service concept in system (e.g. GSM or UMTS) standardization. LCS specifies all the necessary network elements and entities, their functionalities, interfaces, as well as communication messages, due to implement the positioning functionality in a cellular network. Note that LCS does not specify any location based (value added) services except locating of emergency calls

LCS Client: software and/or hardware entity that interacts with a LCS Server for the purpose of obtaining location information for one or more Mobile Stations. LCS Clients subscribe to LCS in order to obtain location information. LCS Clients may or may not interact with human users. The LCS Client is responsible for formatting and presenting data and managing the user interface (dialogue). The LCS Client may reside in the Mobile Station (UE)

LCS Client Access barring list: optional list of MSISDNs per LCS Client where the LCS Client is not allowed to locate any MSISDN therein

LCS Client Subscription Profile: collection of subscription attributes of LCS related parameters that have been agreed for a contractual period of time between the LCS client and the service provider

LCS Feature: capability of a PLMN to support LCS Client/server interactions for locating Target UEs

LCS Server: software and/or hardware entity offering LCS capabilities. The LCS Server accepts requests, services requests, and sends back responses to the received requests. The LCS server consists of LCS components, which are distributed to one or more PLMN and/or service provider

Local Service: service, which can be exclusively provided in the current serving network by a Value added Service Provider

Local Information: information related to a given location, or general information, which is made available in a given location

Location (Based) Application: location application is an application software processing location information or utilizing it in some way. The location information can be input by a user or detected by network or UE. Navigation is one location application example

Location Based Service (LBS): service provided either by teleoperator or a 3rd party service provider that utilizes the available location information of the terminal. Location Application offers the User Interface for the service. LBS is either a pull or a push type of service (see Location Dependent Services and Location Independent Services). In ETSI/GSM documentation of SoLSA, LBS is called "Location Related Service". ETSI and/or 3GPP -wide terminology harmonization is expected here

Location Dependent Service: service provided either by teleoperator or a 3rd party service provider that is available (pull type) or is activated (push type) when the user arrives to a certain area. It doesn't require any subscription in advance, but the push type activation shall be confirmed by the user. The offered service itself can be any kind of service (e.g. a public Xerox machine or the discount list in a store)

Location Estimate: geographic location of an UE and/or a valid Mobile Equipment (ME), expressed in latitude and longitude data. The Location Estimate shall be represented in a well-defined universal format. Translation from this universal format to another geographic location system may be supported, although the details are considered outside the scope of the primitive services

Location Independent Service: service provided either by teleoperator or a 3rd party service provider that is available and therefore can be activated anywhere in the network coverage. It is activated by the user's request or by other user's activated service, and therefore it requires a subscription in advance (pull type). The offered service itself can be any kind of service (e.g. MMS, SWDL, or LBS!)

Mobile Assisted positioning: any mobile centric positioning method (e.g. IPDL-OTDOA, E-OTD, GPS) in which the UE provides position measurements to the network for computation of a location estimate by the network. The network may provide assistance data to the UE to enable position measurements and/or improve measurement performance

Mobile Based positioning: any mobile centric positioning method (e.g. IPDL-OTDOA, E-OTD, GPS) in which the UE performs both position measurements and computation of a location estimate and where assistance data useful or essential to one or both of these functions is provided to the UE by the network. Position methods where an UE performs measurements and location computation without network assistance data are not considered within this category

Mobile Station: mobile station (MS) consists of Mobile or User Equipment (ME or UE) with a valid SIM or USIM attached. The abbreviation "UE" in this specification refers both to MS and User Equipment, see below.

PLMN Access barring list: optional list of MSISDN per PLMN where any LCS Client is not allowed to locate any MSISDN therein except for certain exceptional cases

Positioning (/location detecting): positioning is a functionality, which detects a geographical location (of e.g. a mobile terminal)

Positioning method (/locating method): principle and/or algorithm which the estimation of geographical location is based on, e.g. AOA, TOA, TDOA. For example, GPS is based on TOA, whilst OTDOA and E-OTD (on GSM) are based on TDOA

Positioning technology (/locating technology): technology or system concept including the specifications of RF interfaces, data types, etc. to process the estimation of a geographical location, e.g. GPS, E-OTD (GSM), and OTDOA (WCDMA)

Predefined area: geographical area, which is not related to cell or radio coverage. The mobile may take special action when it recognises it has entered or left a predefined area

Privacy Class: list of LCS Clients defined within a privacy exception class to which permission may be granted to locate the target UE. The permission shall be granted either on activation by the target UE or permanently for a contractual period of time agreed between the target UE and the service provider

Privacy Exception List: list consisting of various types of privacy classes (i.e. operator related, personal etc.). Certain types of classes may require agreement between the service provider and the target UE

Prohibited area: area where the mobile must not activate its transmitter. The Prohibited area may be a Predefined area described above or related to radio cell(s)

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.

Subscription Profile: profile detailing the subscription to various types of privacy classes

Target UE: UE being positioned

User Equipment: term 'User Equipment', or 'UE', should for GSM be interpreted as 'MS', as defined in GSM TS 04.02 [19]. UE in this specification may also refer to a Mobile Equipment or User Equipment used for emergency calls, that do not have valid SIM or USIM

Further UMTS related definitions are given in 3G TS 22.101.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Gb	Interface between 2G-SGSN and BSS
Gs	Interface between MSC and SGSN
Lc	Interface between gateway MLC and gsmSCF (CAMEL interface)
Le	Interface between External User and MLC (external interface)
Lg	Interface between Gateway MLC - VMSC, GMLC - MSC Server, GMLC - SGSN (gateway MLC interface)
Lh	Interface between Gateway MLC and HLR (HLR interface)
Um	GERAN Air Interface
Uu	UTRAN Air Interface

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

2G-	Second Generation
3G-	Third Generation
AC	Admission Control
AI	Application Interface (prefix to interface class method)
ANM	Answer Message (ISUP)
APN	Access Point Name
APN-NI	APN Network Identifier
ARIB	Association of Radio Industries and Business
ATD	Absolute Time Difference
BCCH	Broadcast Control Channel
BER	Bit Error Rate
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CAMEL	Customised Application For Mobile Network Enhanced Logic
CAP	CAMEL Application Part
CM	Connection Management
CN	Core Network
CSE	Camel Service Environment
DL	Downlink
DRNC	Drift RNC
E-OTD	Enhanced Observed Time Difference
FER	Frame Error Rate
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMLC	Gateway MLC
GPRS	General Packet Radio Service
GPS	Global Positioning System
HE	Home Environment
HSS	Home Subscriber Server
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPDL	Idle Period Downlink
LA	Location Application
LAF	Location Application Function
LBS	Location Based Services
LCAF	Location Client Authorization Function
LCCF	Location Client Control Function
LCCTF	Location Client Co-ordinate Transformation Function
LCF	Location Client Function
LCS	LoCation Services

LDR	Location Deferred Request
LIR	Location Immediate Request,
LMU	Location Measurement Unit
LSAF	Location Subscriber Authorization Function
LSBcF	Location System Broadcast Function
LSBF	Location System Billing Function
LSCF	Location System Control Function
LSOF	Location System Operation Function
LSPF	Location Subscriber Privacy Function
MAP	Mobile Application Part
ME	Mobile Equipment
MExE	Mobile Execution Environment
MLC	Mobile Location Center
MLP	Mobile Location Protocol
MM	Mobility Management
MO-LR	Mobile Originated Location Request
MS	Mobile Station
MSC	Mobile Services switching Center
MSC	Mobile services Switching Centre
MSISDN	Mobile Station Integrated Services Data Network
MT-LR	Mobile Terminated Location Request
NA-ESRD	North American Emergency Service Routing Digits
NA-ESRK	North American Emergency Service Routing Key
NI-LR	Network Induced Location Request
OSA	Open Service Architecture
OTDOA	Observed Time Difference Of Arrival
PC	Power Control
PCF	Power Calculation Function
PLMN	Public Land Mobile Network
POI	Privacy Override Indicator
PRCF	Positioning Radio Co-ordination Function
PRRM	Positioning Radio Resource Management
PSE	Personal Service Environment
PSMF	Positioning Signal Measurement Function
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RA	Routing Area
RACH	Random Access Channel
RAN	Radio Access Network
RANAP	Radio Access Network Application Part
RIS	Radio Interface Synchronization
RNC	Radio Network Controller
RRM	Radio Resource Management
RTD	Real Time Difference
SAT	SIM Application Tool-Kit
SCCP	Signalling Connection Control Part
SCS	Service Capability Server
SGSN	Serving GPRS Support Node
SI	Service Interface (prefix to interface class method)
SIM	Subscriber Identity Module
SIR	Signal Interference Ratio
SLPP	Subscriber LCS Privacy Profile
SMLC	Serving Mobile Location Center
SMS	Short Message Service
SP	Service Point
SRNC	Serving RNC
SS7	Signaling System No 7
TA	Timing Advance
TMSI	Temporary Mobile Subscriber Identity
TOA	Time Of Arrival
UDT	SCCP Unitdata message
UE	User Equipment

UL	Uplink
UMTS	Universal Mobile Telecommunication System
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VASP	Value Added Service Provider
VHE	Virtual Home Environment
WCDMA	Wideband Code Division Multiple Access

Further GSM related abbreviations are given in GSM 01.04. Further UMTS related abbreviations are given in 3G TS 21.905 [3].

4 Main concepts

A general description of location services and service requirements are given in the specification TS 22.071 [4]. The positioning of the UE is a service provided by the Access Network. In particular, all Access Networks (e.g. UTRAN, GERAN), that facilitate determination of the locations of User Equipments, shall be able to exchange location information with the core network as defined in the present document (when connected to a Core Network).

By making use of the radio signals the capability to determine the (geographic) location of the user equipment (UE) or mobile station (UE) shall be provided. The location information may be requested by and reported to a client (application) associated with the UE, or by a client within or attached to the Core Network. The location information may also be utilised internally in the system; for example, for location assisted handover or to support other features such as home location billing. The position information shall be reported in standard, i.e. geographical co-ordinates, together with the time-of-day and the estimated errors (uncertainty) of the location of the UE according to specification TS 23.032 [11].

It shall be possible for the majority of the UE (active or idle) within a network to use the feature without compromising the radio transmission or signaling capabilities of the GSM/UMTS networks.

The UE and the network may support a number of different positioning methods and the UE may support or not support privacy invocation request and response. The UE informs the core network and radio access network about its LCS capabilities in this respect as defined in TS 24.008 [24] and TS 25.331 [25].

The uncertainty of the location measurement shall be network design (implementation) dependent at the choice of the network operator, this is further described in TS 25.305 [1] and TS 43.059 [16].

There are many different possible uses for the location information. The positioning feature may be used internally by the GSM/UMTS network (or attached networks), by value-added network services, by the UE itself or through the network, and by "third party" services. The positioning feature may also be used by an emergency service (which may be mandated or "value-added"), but the position service is not exclusively for emergencies.

4.1 Assumptions

As a basis for the further development work on LCS in GSM and UMTS the following assumptions apply:

- positioning methods are Access Network specific, although commonalties should be encouraged between Access Networks;
- commercial location services are only applicable for an UE with a valid SIM or USIM;
- the provision of the location services in the Access Network is optional through support of the specified method(s);
- the provision of location services is optional in MSC and SGSN;
- LCS is applicable to any target UE whether or not the UE supports LCS, but with restrictions on choice of positioning method or notification of a location request to the UE user when LCS or individual positioning methods, respectively, are not supported by theUE;
- LCS shall be applicable for both circuit switched and packet switched services;
- the location information may be used for internal system operations to improve system performance;
- it shall be possible to accommodate future techniques of measurement and processing to take advantage of advancing technology so as to meet new service requirements;
- it may be necessary to support LCS signaling between separate access networks via the core network. The Iur interface should be used if available.
- Provide positioning procedures through the circuit-switched domain are also applicable to GPRS UEs which are GPRS and IMSI attached.

4.2 Location Services Categories

Generally there are four categories of usage of the location service. These are the Commercial LCS, the Internal LCS, the Emergency LCS and the Lawful Intercept LCS. The definition of these services and their categories is outside the scope of the present document.

- The Commercial LCS (or Value Added Services) will typically be associated with an application that provides a value-added service through knowledge of the UE location to the subscriber of the service. This may be, for example, a directory of restaurants in the local area of the UE, together with directions for reaching them from the current UE location.

- The Internal LCS will typically be developed to make use of the location information of the UE for Access Network internal operations. This may include; for example, location assisted handover and traffic and coverage measurement. This may also include support certain O&M related tasks, supplementary services, IN related services and GSM bearer services and teleservices.

- The Emergency LCS will typically be part of a service provided to assist subscribers who place emergency calls. In this service, the location of the UE caller is provided to the emergency service provider to assist them in their response. This service may be mandatory in some jurisdictions. In the United States, for example, this service is mandated for all mobile voice subscribers.

- The Lawful Intercept LCS will use the location information to support various legally required or sanctioned services.

4.3 Positioning methods

The LCS feature utilises one or more positioning methods in order to determine the location of user equipment (UE). Determining the position of a UE involves two main steps:

- Radio signal measurements; and

- Position estimate computation based on the measurements.

The positioning methods for UTRAN are further described in TS 25.305 [1].

4.3.1 Standard LCS Methods in UTRAN

The specification TS 25.305 UTRAN Stage 2 specifies the locating methods to be supported:

- cell coverage based positioning method;

- OTDOA positioning method;

- GPS based positioning methods.

For more details on these positioning methods, refer to TS 25.305 [1].

4.3.2 Standard LCS Methods in GERAN

The specification TS 43.059 GERAN LCS Stage 2 specificies the locating methods to be supported in GERAN:

- cell coverage based positioning method;

- Enhanced Observed Time Difference (E-OTD) positioning method;

- GPS based positioning methods.

4.4 Types of Location Request

4.4.1 Immediate Location Request

Request for location where the LCS Server replies immediately to the LCS Client with the current location estimate if this could be obtained.

4.4.2 Deferred Location Request

Request for location contingent on some current or future events where the response from the LCS Server to the LCS Client may occur some time after the request was sent.

4.4.2.1 Types of event

a) UE available: Any event in which the MSC/SGSN has established a contact with the UE. Note, this event is considered to be applicable when the UE is temporarily unavailable due to inaction by the UE user, temporarily loss of radio connectivity or IMSI detach and so on. Note that IMSI detach is only applicable in the case UE has previously been registered and information is still kept in the node.

b) Other events are FFS (Release 5)

5 General LCS architecture

5.1 LCS access interfaces and reference points

There is one reference point between the LCS server and LCS client called Le, see figure 5.1. The general aspects of the Le reference point are described in TS 22.071 [4]. Protocol specifics that may be implemented for the Le interface have been specified by LIF (Location Inter-operability Forum) [31]. There may be more than a single LCS network interface to several different LCS clients or other networks. These networks may both differ in ownership as well as in communications protocol. The network operator should define and negotiate interconnect with each external LCS client or other network.

An interface differs from a reference point in that an interface is defined where specific LCS information is exchanges and needs to be fully recognized.

There is an interface called Lg that connects two independent LCS networks (different PLMNs) for message exchange.

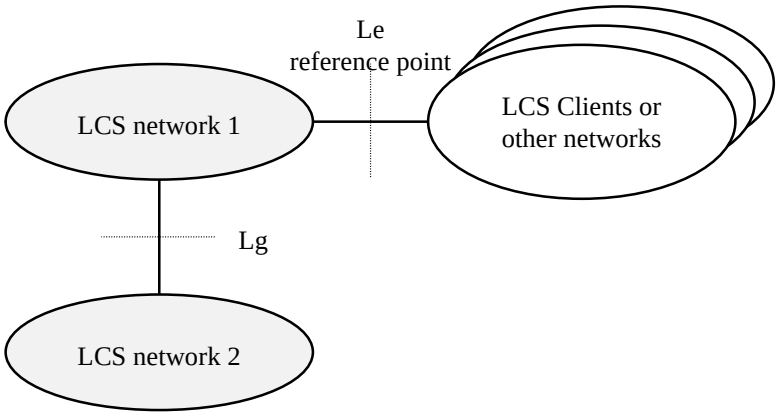


Figure 5.1: LCS Access Interfaces and Reference Points

5.2 LCS Functional diagram, high level functions

TS 22.071 [4] describes LCS services from the LCS client point of view. In the present document, a more detailed description of LCS is given. The LCS functional diagram shown in figure 5.2 depicts the interaction of the LCS client and the LCS server within the PLMN. The PLMN uses the various LCS components within the LCS server to provide the target UE Location Information to the LCS client.

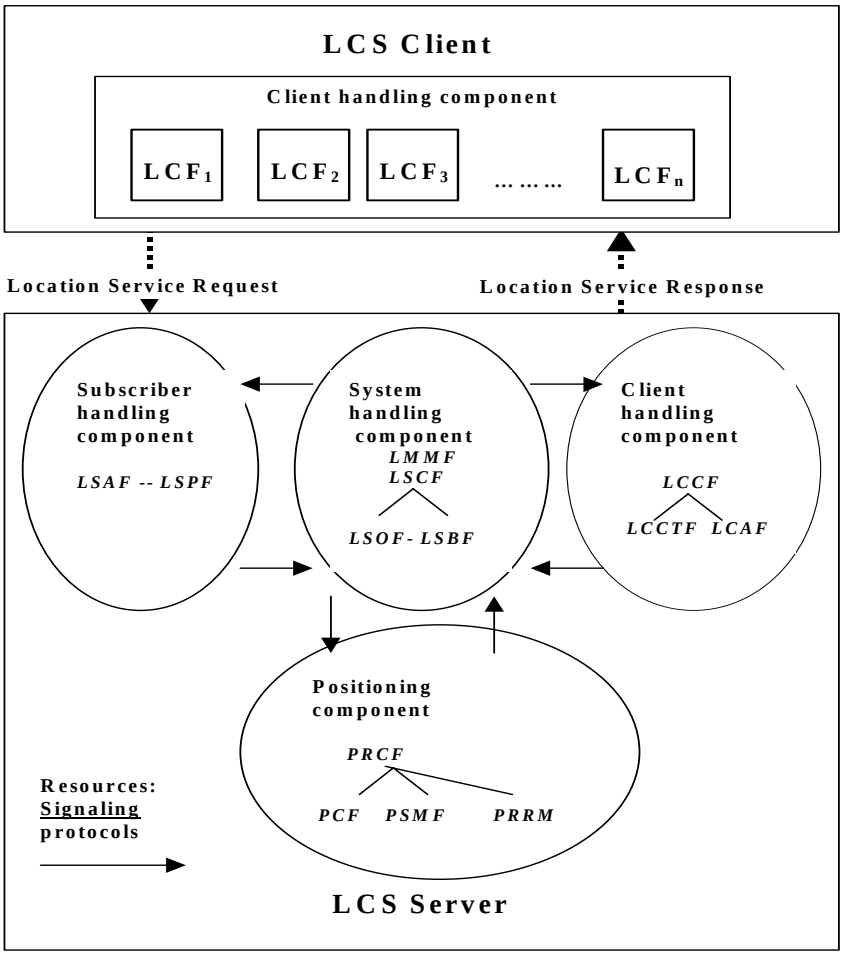


Figure 5.2: LCS capability server Functional Diagram

The following list gives the logical functional entities for the LCS. Two main functional groupings are defined which encompass a number of smaller functions.

The LCS Functional entities are grouped as follows:

- the LCS Client functional group;
- the LCS Server functional group consists of functions in the UMTS PLMN supporting LCS:
  - client handling component;
  - system handling component;
  - subscriber handling component;
  - positioning component.

The functions of the LCS Client and the LCS Server in the PLMN are described in more detail in this clause.

The allocation of LCS functions to network elements is specified in clause 6.

5.3 LCS Client functional group

An LCS client contains an LCS component with one or more client(s), which by using location information can provide location, based services.

An LCS client is a logical functional entity that requests from the LCS server in the PLMN location information for one or more than one target UE within a specified set of parameters such as Quality of Service (QoS). The LCS Client may reside in an entity (including the UE) within the PLMN or in an entity external to the PLMN.

The specification of the LCS Client's internal logic and its relation to the external use is outside the scope of the present document.

5.3.1 External Location Client Function (LCF)

The Location Client Function (LCF) provides a logical interface between the LCS client and the LCS server.

This function is responsible for requesting location information for one or more UEs, with a specified "QoS" and receiving a response, which contains either location information or a failure indicator.

[Editor's note: this is only possible if the location request originates in the core network].

5.4 LCS Server functional group

The LCS server functional group consists of the functions that are needed for GSM and UMTS to support Location Services.

5.4.1 Client handling component

5.4.1.1 Location Client Control Function (LCCF)

The Location Client Control Function (LCCF) manages the external interface towards LCF. The LCCF identifies the LCS client by requesting client verification and authorization (i.e. verifies that the LCS client is allowed to position the subscriber) through interaction with the Location Client Authorization Function (LCAF). The LCCF handles mobility management for location services (LCS) e.g., forwarding of positioning requests to VMSC or SGSN. The LCCF determines if the final positioning estimate satisfies the QoS for the purpose of retry/reject. The LCCF provides flow control of positioning requests between simultaneous positioning requests. It may order the Location Client Co-ordinate Transformation Function (LCCTF) to perform a transformation to local co-ordinates. It also generates charging and billing related data for LCS via the Location System Billing Function (LSBF).

5.4.1.2 Location Client Authorization Function (LCAF)

The Location Client Authorization Function (LCAF) is responsible for providing access and subscription authorization to a client. Specifically, it provides authorization to a LCS client requesting access to the network and authorizes the subscription of a client. LCAF provides authorization to a LCS client requesting Location Information of a specific UE.

5.4.1.2.1 Access Subfunction

An *Access Subfunction* enables LCS clients to access LCS services. This subfunction provides verification and authorization of the requesting client.

When a LCS is requested, the Access Subfunction uses the information stored in the LCS client *subscription profile* to verify that:

- the LCS client is registered; and
- the LCS client is authorized to use the specified LCS request type;
- the LCS client is allowed to request location information for the subscriber(s) specified in the LCS request.

5.4.1.2.2 Subscription Subfunction

The LCS client Subscription profile shall contain a minimum set of parameters assigned on per LCS client basis for an agreed contractual period. The LCS client profile shall contain the following set of access parameters:

- LCS client identity;
- allowed LCS request types (i.e. LIR, LDR or both) (see note);
- maximum number of subscribers allowed in a single LCS request;
- priority;
- position override indicator;
- state(s);
- event(s) (applicable to LDR requests only);
- local coordinate system;
- LCS client access barring list (optional);
- PLMN access barring list applicability.

NOTE: LIR = Location Immediate Request; and
LDR = Location Deferred Request.

For certain authorized LCS client internal to the PLMN, a subscription profile is unnecessary. These clients are empowered to access any defined service that is not barred for an UE subscriber. This permits positioning of emergency calls without the need for pre-subscription.

5.4.1.3 Location Client Co-ordinate Transformation Function (LCCTF)

The Location Client Co-ordinate Transformation Function (LCCTF) provides conversion of a location estimate expressed according to a universal latitude and longitude system into an estimate expressed according to a local geographic system understood by the LCF and known as location information. The local system required for a particular LCF will be either known from subscription information or explicitly indicated by the LCF.

5.4.2 System handling component

5.4.2.1 Location System Control Function(LSCF)

The Location System Control Function (LSCF) is responsible for co-ordinating location requests. This function manages call-related and non-call-related positioning requests of LCS and allocates network resources for handling them. The LSCF retrieves UE classmark information for the purpose of determining the LCS capabilities of UE.

The LSCF performs call setup if required as part of a LCS e.g., putting the UE on dedicated radio resources. It also caters for co-ordinating resources and activities with regard to requests related to providing assistance data needed for positioning. This function interfaces with the LCCF, LSPF, LSBF and PRCF. Using these interfaces, it conveys positioning requests to the PRCF, relays positioning data to the LCCF and passes charging related data to the LSBF.

The U-LSCF for UTRAN is further described in TS 25.305 [1], LSCF for GERAN is described in TS 43.059 [16].

5.4.2.2 Location System Billing Function (LSBF)

The Location System Billing Function (LSBF) is responsible for charging and billing activity within the network related to location services (LCS). This includes charging and billing of both clients and subscribers. Specifically, it collects charging related data and data for accounting between PLMNs.

5.4.2.3 Location System Operations Function (LSOF)

The Location System Operations Function (LSOF) is responsible for provisioning of data, positioning capabilities, data related to clients and subscription (LCS client data and UE data), validation, fault management and performance management of LCS.

An LSOF may be associated with each entity.

5.4.2.4 Location System Broadcast Function (LSBcF)

The Location System Broadcast Function (LSBcF) provides broadcast capability. The LSBcF capability is only used when broadcast data is required for E-OTD, OTDOA or assisted GPS positioning methods.

5.4.3 Subscriber handling Component

5.4.3.1 Location Subscriber Authorization Function (LSAF)

The Location Subscriber Authorization Function (LSAF) is responsible for authorizing the provision of a location service (LCS) for a particular mobile station (UE with SIM/USIM). Specifically, this function validates that a LCS can be applied to a given subscriber. In case LCF is in the UE then LSAF verifies that the UE subscriber has subscribed to the requested LCS service.

5.4.3.2 Location Subscriber Privacy Function (LSPF)

The Location Subscriber Privacy function is responsible performs all privacy related authorizations. For a target UE it shall authorize the positioning request versus the privacy options of the target UE, if any.

5.4.4 Positioning components

The positioning components Positioning Radio Co-ordination Function (PRCF), Positioning Calculation Function (PCF), Positioning Signal Measurement Function (PSMF) and Positioning Radio Resource Management (PRRM) are described in documents specific to each Access Network type.

For location services the Access Network shall send the result of the positioning to the core network in geographical co-ordinates as defined in TS 23.032. The Access Network shall map the cell(s) the Target UE is associated with into geographical co-ordinates, but this mapping is not standardized.

These entities are defined in TS 25.305 [1] for UTRAN and in TS 43.059 [16] for GERAN.

5.5 Information Flows between Client and Server

Other types of national specific information flows may be supported in addition to the information flow specified here.

Any of the information flows here indicated may not be externally realized if the information does not flow over an open interface. On the other hand, if a flow goes over an open interface, it shall abide to a well-defined protocol, e.g. LIF TS 101 [31], Location Inter-Operability Forum 2001.

5.5.1 Location Service Request

Via the Location Service Request, the LCS client communicates with the LCS server to request for the location information of one or more than one UE within a specified quality of service. There exist two types of location service requests:

- Location Immediate Request (LIR); and
- Location Deferred Request (LDR).

The attributes for the information exchange between the LCS Client and the LCS Server have been standardized by LIF based on requirements set by TS 22.071 and TS 23.271.

The following attributes are identified for Location Service Request information flow:

- Target UE identity;
- LCS Client identity;
- Service identity, if needed;
- Codeword, if needed;
- Requestor identity, if needed;
- Number dialled by the target mobile user or APN-NI, if the request is call or session related ;
- Event, applicable to deferred location requests only;
- Start time, stop time and interval, applicable to periodical and deferred requests only;
- Requested Quality of Service information, if needed;
- Type of location, i.e. current location or last known location;
- Priority, if needed;
- Local coordinate reference system, if needed;
- Geographical area, if needed.

Some of the information may be stored in GMLC and the LCS client does not need to include such information in the location service request.

5.5.2 Location Service Response

The LCS server (GMLC) sends the Location Service Response to the LCS client either as an:

- Immediate Response; or a
- Deferred Response, these deferred responses can be either single or periodic.

The following attributes are identified for the Location Service Response information flow:

- Location indication of UE in geographical coordinates expressed as a shape as defined in TS 23.032 or local coordinate system;
- Indication when UE enters or leaves the Geographical area, if needed;
- Acknowledgement for a deferred location request, if needed.

In addition the information attributes of the location service request may be used also in the location service response.

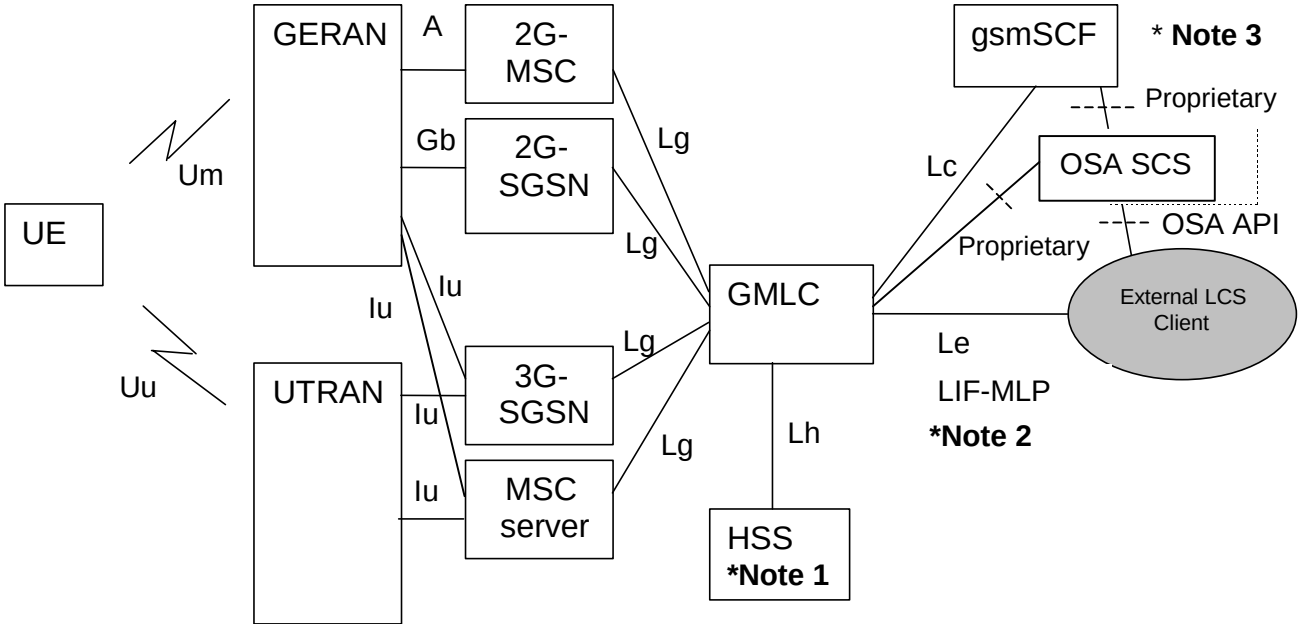
6 LCS Architecture

Figure 6.1 shows the general arrangement of the Location Service feature in GSM and UMTS. This illustrates, generally, the relation of LCS Clients and servers in the core network with the GERAN and UTRAN Access Networks. The LCS entities within the Access Network communicate with the Core Network (CN) across the A, Gb and Iu interfaces. Communication among the Access Network LCS entities makes use of the messaging and signaling capabilities of the Access Network.

As part of their service or operation, the LCS Clients may request the location information of UE. There may be more than one LCS client. These may be associated with the GSM/UMTS networks or the Access Networks operated as part of a UE application or accessed by the UE through its access to an application (e.g. through the Internet).

The clients make their requests to a LCS Server. There may be more than one LCS Server. The client must be authenticated and the resources of the network must be co-ordinated including the UE and the calculation functions, to

estimate the location of the UE and result returned to the client. As part of this process, information from other systems (other Access Networks) can be used. As part of the location information returned to the client, an estimate of the accuracy of the estimate and the time-of-day the measurement was made may be provided.



NOTE 1: HSS includes both 2G-HLR and 3G-HLR functionality. LCS is included in the overall network architecture in TS 23.002 [20].
NOTE 2: LIF-MLP may be used on the Le interface
NOTE 3: As one alternative the LCS client may get location information directly from GMLC, which may contain OSA Mobility SCS with support for the OSA user location interfaces. See TS 23.127 [26] and TS 29.198 [27, 28, 29 and 30].

Figure 6.1: General arrangement of LCS

6.1 Schematic functional description of LCS operations

The allocation of LCS functional blocks to the Client, LCS server, Core Network, Access Network and UE is based on the schematic functional description below. The detailed functions and interactions are specified later in the present document and in TS 25.305 [1] for UTRAN, in TS 43.059 [16] for GERAN and in corresponding Stage 3 specifications.

The operation begins with a LCS Client requesting location information for a UE from the LCS server. The LCS server will pass the request to the LCS functional entities in the core network. The LCS functional entities in the core network shall then:

- verify that the LCS Client is authorized to request the location of the UE or subscriber;
- verify that LCS is supported by the UE;
- establish whether it is allowed to locate the UE or subscriber, for privacy or other reasons;
- establish which network element in the Access Network should receive the Location request;
- request the Access Network (via the A, Gb or Iu interface) to provide location information for an identified UE, with indicated QoS;
- receive information about the location of the UE from the Access Network and forward it to the Client;

- send appropriate accounting information to an accounting function.

The Access Network LCS functional entities shall determine the position of the target UE according to TS 25.305 [1] for UTRAN and TS 43.059 [16] for GERAN.

6.2 Allocation of LCS functions to network elements

Table 6.1 shows a summary of the Functional Groups and Functional Blocks for Location services. Table 6.2 and figure 6.2 show the generic configuration for LCS and the distribution of LCS functional blocks to network elements. Different positioning methods, including network-based, mobile-based, mobile-assisted and network-assisted positioning methods may be used. With this configuration both the network and the mobiles are able to measure the timing of signals and compute the mobile's location estimate. Depending on the applied positioning method it is possible to utilise the corresponding configuration containing all needed entities. For instance, if network-based positioning is applied, the entities that are involved in measuring the mobile's signal and calculating its location estimate are allocated to the network elements of the access stratum. On the other hand, in case mobile-based or network-assisted methods are used these entities should be allocated to the UE.

LCS is logically implemented on the network structure through the addition of one network node, the Mobile Location Center (MLC). It is necessary to name a number of new interfaces. The LCS generic architecture can be combined to produce LCS architecture variants.

Table 6.1: Summary of Functional Groups and Functional Blocks for Location services

Funct. Group	Functional component	Full name of Functional Block	Abbrev.
Loc. Client	Location Client Component	(External) Location Client Function	LCF
		Internal Location Client Function	LCF -internal
LCS Server in PLMN	Client handling component	Location Client Control Function	LCCF
		Location Client Authorization Function	LCAF
	System handling component	Location System Control Function	LSCF
		Location System Billing Function	LSBF
		Location System Operations Function	LSOF
	Subscr. handling component	Location Subscriber Authorization Function	LSAF
		Location Subscriber Privacy function	LSPF
	Positioning component	Positioning Radio Control Function	PRCF
		Positioning Calculation Function	PCF
		Positioning Signal Measurement Function	PSMF
		Positioning Radio Resource Management	PRRM

Table 6.2 and figure 6.2 illustrate the allocation of functional entities in the reference configuration of LCS. It is assumed that the CS and PS have either their own independent mobility management or use the joint mobility management through the optional Gs interface.

It is also seen that LCS may take benefit of the Iur interface between RNCs, when uplink radio information and measurement results are collected.

The functional model presented in the figure includes functional entities for both CS and PS related LCS. In addition, it consists of all the entities needed for different positioning methods, i.e. network based, mobile based, mobile assisted, and network assisted positioning, exploiting either uplink or downlink measurements. It is noted that the UE may use e.g. the GPS positioning mechanism, but still demand e.g. auxiliary measurements from the serving network. RAN specific functional entities are specified in TS 25.305 [1] for UTRAN and in TS 43.059 [16] for GERAN.

Table 6.2: Allocation of LCS functional entities to network elements

	UE	RAN	GMLC	SGSN	MSC/MSC Server	HLR/HSS	Client
Location client functions							
LCF	X			X	X		X
LCF Internal	Ffs	X					
Client handling functions							
LCCTF			X				
LCCF			X				
LCAF			X				
System handling functions							
LSCF		X		X	X		
LSBF			X	X	X		
LSOF	X	X	X	X	X		
Subscriber handling functions							
LSAF				X	X		
LSPF				X	X	X	
Positioning functions							
PRCF		X					
PCF	X	X					
PSMF	X	X					
PRRM		X					
	UE	**RAN**	**GMLC**	**SGSN**	**MSC/MSC Server**		**Client**

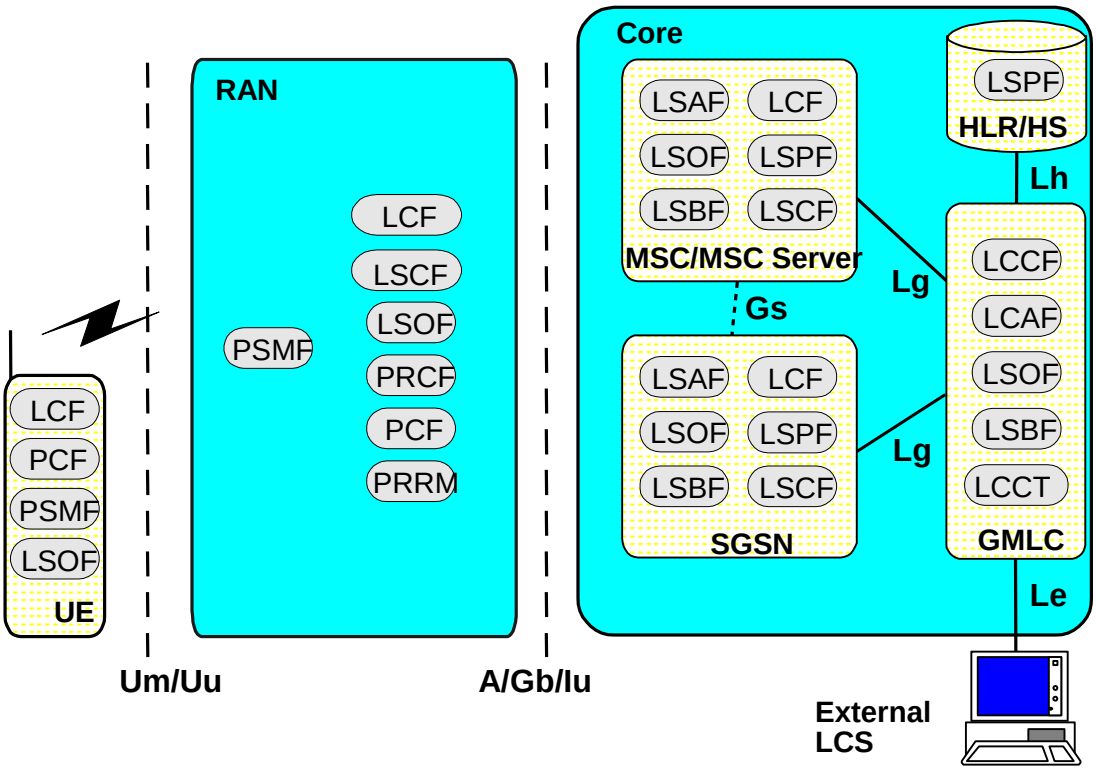


Figure 6.2: Generic LCS Logical Architecture

6.3 Functional description of LCS per network element

6.3.1 Access Network

The Access Network is involved in the handling of various positioning procedures.

The LCS specific functionalities of the radio access network elements are specified in TS 25.305 [1] for UTRAN and TS 43.059 [16] for GERAN.

6.3.2 LCS Clients, LCS applications and Requestors

There are two classes of LCS Application - Internal applications and External applications. Internal applications represent entities internal to the GSM/UMTS that make use of location information for the (improved) operation of the network. Internal LCS client can be identified by LCS client internal ID. LCS client Internal ID distinguishes the following classes: (LCS client broadcasting location related information, O&M LCS client in the HPLMN, O&M LCS client in the VPLMN, LCS client recording anonymous location information, LCS Client supporting a bearer service, teleservice or supplementary service to the target UE). External applications represent entities (such as Commercial or Emergency services) that make use of location information for operations external to the mobile communications network. External LCS client can be identified by LCS client external ID. The LCS Applications interface to the LCS entities through their Location Client functions (LCF). Location requests from the external LCS clients may be originated by external entities (i.e. Requestor). LCS client should authenticate the Requestor Identity but this is outside the scope of this specification.

The LCS Client, LCS applications and Requestors are outside the scope of the present document. However, an external LCS Client may communicate with the LCS Server as specified in [31].

6.3.3 Gateway Mobile Location Center, GMLC

The Gateway Mobile Location Center (GMLC) contains functionality required to support LCS. In one PLMN, there may be more than one GMLC.

The GMLC is the first node an external LCS client accesses in a GSM PLMN (i.e. the Le reference point is supported by the GMLC). The GMLC may request routing information from the HLR or HSS via the Lh interface. After performing registration authorization, it sends positioning requests to either VMSC, SGSN or MSC Server and receives final location estimates from the corresponding entity via Lg interface.

6.3.4 LCS support in the UE

The UE may be involved in the various positioning procedures. Specific UE involvement is specified in each of the positioning procedures specified in TS 25.305 [1] for UTRAN and TS 43.059 [16] for GERAN.

The UE interacts with the measurement co-ordination functions to transmit the needed signals for uplink based LCS measurements and to make measurements of downlink signals. The measurements to be made will be determined by the chosen location method.

The UE may also contain LCS applications, or access a LCS application through communication with a network accessed by the UE or an application residing in the UE. This application may include the needed measurement and calculation functions to determine the UE's location with or without assistance of the GSM/UMTS LCS entities.

In GSM the positioning methods supported by the UE are signalled by the UE to the core network and radio access network using Classmark3 in CS mode, as specified in TS 24.008 [24].

In UMTS the UE capability to support different positioning methods is only communicated within UTRAN, as specified in TS 25.331 [25].

The UE informs the core network about its capability to support privacy invocation request and response using Classmark2 in CS mode and MS Network Capability in PS mode, as specified in TS 24.008 [24].

The UE may also, for example, contain an independent location function (e.g. Global Satellite Positioning Service GPS) and thus be able to report its location, independent of the RAN transmissions. The UE with an independent location function may also make use of information broadcast by the RAN that assists the function.

6.3.5 MSC/VLR

The MSC/VLR contains functionality responsible for UE subscription authorization and managing call-related and non-call related positioning requests of LCS. The MSC is accessible to the GMLC via the Lg interface. The LCS functions of MSC are related to charging and billing, LCS co-ordination, location request, authorization and operation of the LCS services. If connected to SGSN through the Gs interface, it checks whether the UE is GPRS attached to decide whether to page the UE on the A/Iu or Gs interface.

The MSC/VLR may inform HLR/HSS about the UE's LCS Capabilities in the MAP UPDATE LOCATION message, during Registration and Inter MSC Update Location procedures.

6.3.6 MSC Server

The MSC Server handles the same functionality as the MSC/VLR including charging and billing, LCS co-ordination, location request, authorization and operation of the LCS services. The MSC Server is accessible to the GMLC via the Lg interface.

6.3.7 SGSN

The SGSN contains functionality responsible for UE subscription authorization and managing positioning requests of LCS. The SGSN is accessible to the GMLC via the Lg interface. The LCS functions of SGSN are related to charging and billing, LCS co-ordination, location request, authorization and operation of the LCS services.

The SGSN may inform HLR/HSS about the UE's LCS Capabilities for GPRS in the MAP UPDATE GPRS LOCATION message, during Attach and Inter SGSN Routing Area Update procedures.

The SGSN forwards the circuit-swiched paging request received from the Gs interface to the BSS/RNC.

6.3.8 Home Location Register, HLR

The HLR contains LCS subscription data and routing information. The HLR is accessible from the GMLC via the Lh interface. For a roaming UE, HLR may be in a different PLMN.

6.3.9 HSS

The HSS contains LCS subscription data and routing information. The HSS is accessible from the GMLC via the Lh interface. For roaming UEs, HSS may be in a different PLMN.

6.3.10 gsmSCF

The Lc interface supports CAMEL access to LCS and is applicable only in CAMEL [phase 3?]. The procedures and signaling associated with it are defined in TS 23.078 [21] and TS 29.002 [18], respectively.

6.4 Addressing the target UE for LCS purposes

It shall be possible to address and indicate the target UE using MSISDN. It may be possible in certain cases to address the target UE using IP address when a static or dynamic IP address (IPv4 or IPv6) has been allocated for the UE.

In the mobile terminated location request procedures in the PS domain (as well as in the CS domain), the target UE is always identified using MSISDN.

NOTE: It is recognized that IP-addressing of the target UE is only possible when there is an active PDP context established between the target UE and the external LCS client. Using the established PDP context, the LCS client can request the target UE, as identified with the IP address it currently uses, to initiate a Mobile originated location request. The actual signaling exchange between the LCS Client/server and the target UE or the user of the target UE is outside the scope of this specification. The resulting MO-LR is performed as specified in this document.

7 Signaling and Interfaces

7.1 LCS signaling between Access and Core Networks

The core network sends location requests to the access network, which then sends the corresponding responses back to the core network.

Communication between access and core networks is accomplished through Iu interface in UMTS whereas the A, Gb and Iu interfaces are used for the purpose in GSM (see TS 25.305 [1] and TS 43.059 [16]).

7.1.1 Core network Location Request

The core network request for a location estimate of a target UE shall contain sufficient information to enable location of the Target UE according to the required QoS using any positioning method supported by the PLMN and, where necessary, UE. For location services the core network may request the geographical co-ordinates of the Target UE.

In UMTS the core network may also request in which Service Area the Target UE is located. The Service Area information may be used for routing of corresponding Emergency calls, or for CAMEL services. (The MSC Server or SGSN shall not send the Service Area Identity to GMLC).

In GSM this corresponds to the usage of Cell ID in the core network.

It should be noted that the Service Area concept is different from the Localized Service Area concept used for SoLSA services.

When the location of a Target UE in Idle Mode is requested, the core network shall determine which RAN entity is associated with the Target UE.

7.1.2 Location Report

The access network reports the location of the Target UE to the core network entities. The location report may contain the following information as defined in the corresponding location request:

- the geographical co-ordinates of the Target UE;
- the service area in which the Target UE is located;
- achieved quality level of the location estimate.

7.2 Um and Uu Interfaces

NOTE: This chapter may change depending on whether air interface LMU will exists in the logical architecture or not.

The Um and Uu interfaces are used to communicate among the LCS entities associated with the BSC and RNC, the UE and the stand-alone Location Measurement Units (LMU). The Um and Uuinterfaces are also used to communicate between the LCS entities in the core network and the UE.

The Um/Uu interfaces may pass measurement requests and results to and from UE or the stand-alone LMU.

The Um/Uu interfaces may also pass location requests from internal or external LCS Clients (Applications) at the UE. Note that these requests may require the services of the LCS entities associated with the core network to authenticate clients and subscriber subscriptions to aspects of the LCS.

The Um/Uu interfaces may also be used for broadcast of information that may be used by the UE or stand-alone LMU for their LCS operations. This may, for example, include timing information about nearby Node-B/BTS transmissions that may assist the UE or LMU in making their measurements. In UTRAN code information may be included.

The Um and Uu interfaces may also pass messages relating to changes or reporting of the data associated with the Location System Operations Function (LSOF) in the UE or the remote LMU.

UTRAN Stage 2 specification TS 25.305 [1] specifies LCS signaling over the Uu interface and GERAN Stage 2 specification TS 43.059 [16] over the Um interface correspondingly.

Message segmentation is specified in GERAN LCS Stage 2, TS 43.059 [16].

7.3 MAP Interfaces

The following interfaces are based on MAP in LCS.

- Lh interface: interface between GMLC and HLR. This interface is used by the GMLC to request the address of the visited MSC or SGSN for a particular target UE whose location has been requested.
- Lg interface:interface between GMLC MSC and GMLC - SGSN. This interface is used by the GMLC to convey a location request to the MSC or SGSN currently serving a particular target UE whose location was requested. The interface is used by the MSC or SGSN to return location results to the GMLC.
- Lc: interface between GMLC and gsmSCF, CAMEL. This interface is used to get location information for CAMEL based services.

The following MAP services are defined for LCS.

- MAP-SEND-ROUTING-INFO-FOR-LCS Service.

This service is used between the GMLC and the HLR/HSS to retrieve the routing information needed for routing a location service request to the serving VMSC , SGSN. The service may be used in GMLC - HSS interface to retrieve routing information in order to route the location service request to the correct VMSC, SGSN and MSC Server.

- MAP-PROVIDE-SUBSCRIBER-LOCATION Service.

This service is used by a GMLC to request the location of a target UE from the visited MSC, SGSN or MSC Server at any time.

- MAP-SUBSCRIBER-LOCATION-REPORT Service.

This service is used by a VMSC, SGSN or MSC Server to provide the location of a target UE to a GMLC when a request for location is either implicitly administered or made at some earlier time.

The MAP Subscriber Location Report could also be used to send information about location of the Target UE (for MO-LR) to an external client.

8 General network location procedures

8.1 State description for GMLC

8.1.1 GMLC states

8.1.1.1 NULL State

In the NULL state, a particular location request from some LCS client either has not been received yet or has already been completed. After a location request is received from a LCS client, the GMLC remains in the NULL state while the identity of the client and nature of its location request are verified. While the NULL state exists conceptually, it need not be represented explicitly in the GMLC.

8.1.1.2 INTERROGATION State

In this state, the GMLC has sent an interrogation to the home HLR/HSS of the UE to be located and is awaiting a response giving one or several of the following addresses:the VMSC, MSC Server, SGSN address and IMSI for this UE.

8.1.1.3 LOCATION State

In this state, the GMLC has sent a location request to the VMSC, MSC Server, SGSN or serving the UE to be located and is awaiting a response containing a location estimate.

8.1.2 State functionality

8.1.2.1 State Transitions

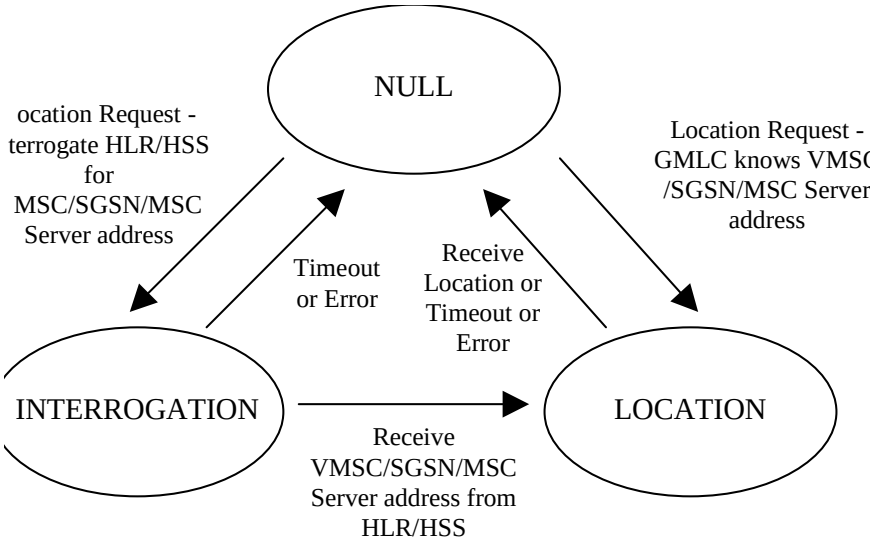


Figure 8.1: State Transitions in the GMLC

Moving from NULL to INTERROGATION state:

If the GMLC does not know any of the following addresses:VMSC, MSC Server, SGSN address or IMSI when it receives a location service request from some LCS client, it moves from the NULL state to the INTERROGATION state and sends a request to the UE's home HLR/HSS for the VMSC/ MSC Server/ SGSN address and IMSI.

Moving from NULL to LOCATION state:

If the GMLC already knows one of the following addresses: VMSC, MSC Server, SGSN or UE IMSI, when it receives a location service request from some LCS client (e.g. from information retained for an earlier location request for the same UE), it moves from the NULL state to the LOCATION state and sends a location request to either the VMSC, MSC Server or SGSN.

NOTE: It is for further study how GMLC selects if it shall send the location request to VMSC, MSC server and/or SGSN in different cases. This should be specified in the signaling procedures.

Moving from INTERROGATION to LOCATION state:

After the GMLC, in the INTERROGATION state, receives one or several of the addresses VMSC, MSC Server, SGSN, and IMSI from the home HLR/HSS, it enters the LOCATION state and sends a location request to either the VMSC, MSC Server or SGSN of the UE being located.

Moving from LOCATION to NULL state:

After the GMLC receives a location estimate response from the VMSC, MSC Server or SGSN, it forwards the location estimate to the requesting LCS client and re-enters the NULL state.

8.1.2.2 INTERROGATION Timer Function

The GMLC runs a timer while in the INTERROGATION state to limit the amount of time waiting for an interrogation response from the HLR/HSS. If the timer expires before an interrogation response is received, the GMLC indicates a location failure to the LCS client and re-enters the NULL state.

8.1.2.3 LOCATION Timer Function

The GMLC runs a timer while in the LOCATION state to limit the amount of time waiting for a location estimate response from the VMSC/ MSC Server /SGSN. If the timer expires before a response is received, the GMLC indicates a location failure to the LCS client and re-enters the NULL state.

8.2 State description for VMSC and MSC Server

8.2.1 VMSC and MSC Server States

NOTE: Periodic location service may need to be covered in the state descriptions.

8.2.1.1 LCS IDLE State

In this state, the VMSC/MSC Server location service is inactive for a particular UE. The UE may be known in the VMSC/MSC Server (except for a USIM less or SIM less Emergency call or where the UE information has been cancelled or lost in the VMSC/MSC Server), but there may not be an active Mobility Management to the UE.

8.2.1.2 LOCATION State

In this state, the VMSC/MSC Server is awaiting a response from RAN after requesting the location for a particular UE.

8.2.2 State Functionality

8.2.2.1 State Transitions

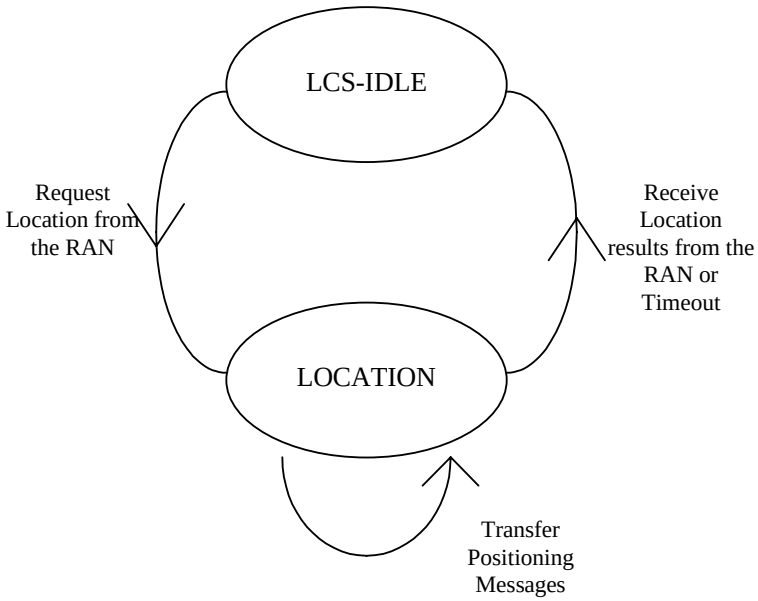


Figure 8.2: State Transitions in the VMSC/MSC Server

Moving from LCS IDLE to LOCATION state:

After a request has been received to locate a particular UE and the UE subscription options have been verified, a location request is sent to the RAN of the UE to be located: the VMSC/MSC Server then enters the LOCATION state. Before entering this state, the VMSC/MSC Server must have setup a Mobility Management connection to the UE if none was previously active. The mobile is paged and authenticated before positioning.

Moving from LOCATION to LCS IDLE state:

After the return of a location estimate result from RAN, the VMSC/MSC Server shall re-enter IDLE state.

8.2.2.2 LOCATION Timer Function

TheVMSC/MSC Server runs a timer while in the LOCATION state to limit the amount of time waiting for a location response from the RAN. If the timer expires before such information is received, the VMSC/MSC Server indicates a location failure to the original requesting entity and re-enters IDLE state.

8.3 LCS State description for SGSN

8.3.1 SGSN States

8.3.1.1 LCS IDLE State

In this state, the SGSN location service is inactive for a particular UE. The UE is known in the SGSN except in case where the UE data has been cancelled or lost in the SGSN. There is not an active Mobility Management to the UE.

8.3.1.2 LOCATION State

In this state, the SGSN is awaiting a response from the RAN after requesting the location for a particular UE. In this state, a Mobility Management connection to the target UE will be active.

8.3.2 State Functionality

8.3.2.1 State Transitions

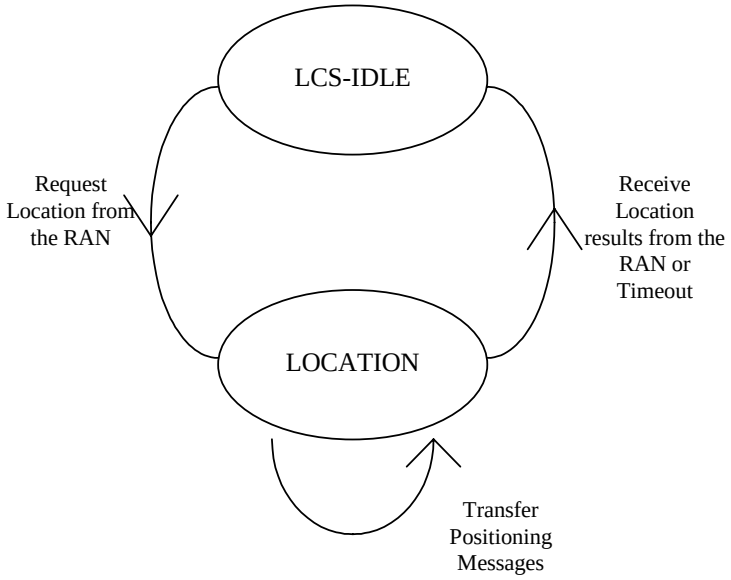


Figure 8.3: State Transitions in the SGSN

Moving from LCS-IDLE to LOCATION state:

After a request has been received to locate a particular UE and the UE subscription options have been verified to allow this, the SGSN sends a location request to the RAN. The SGSN then enters the LOCATION state. Before entering this state, the SGSN must have setup a Mobility Management connection to the UE if none was previously active. The mobile is paged and authenticated before positioning.

Moving from LOCATION to LCS IDLE state:

After the return of a location estimate result from RAN, or if the Location Timer described below expires, the SGSN shall re-enter IDLE state.

8.3.2.2 LOCATION Timer Function

The SGSN runs a timer while in the LOCATION state to limit the amount of time waiting for a location response from the RAN. If the timer expires before such information is received, the SGSN indicates a location failure to the original requesting entity and re-enters IDLE state.

8.4 Signaling connection for the Iu interface

When using the Iu interface, before SGSN/MSC server can request location information of a target UE from RAN, an Iu signaling connection must have been established between SGSN/MSC server and RAN. The SGSN/MSC server sends a location request message to RAN, which determines the location of the target UE related to this Iu signaling connection and sends a location report to SGSN/MSC server over the same Iu signaling connection.

8.5 Signaling connection for the A-interface

When using the A interface, before MSC can request location information of a target UE from RAN, an A interface signaling connection must have been established between MSC and RAN. The MSC sends a location request message to RAN, which determines the location of the target UE related to this A interface signaling connection and sends a location report to MSC over the same A interface signaling connection.

8.6 Gb interface mapping of target UE

The pre-requisite for LCS procedures on the Gb interface is that UE is in "ready state".

9 General Network Positioning Procedures

The generic network positioning procedure of providing the location information of an UE subscriber can be partitioned into the following procedures.

Location Preparation Procedure

This generic procedure is concerned with verifying the privacy restrictions of the UE subscriber, reserving network resources, communicating with the UE to be located and determining the positioning method to be used for locating the UE subscriber based on the requested QoS and the UE and network capabilities.

Positioning Measurement Establishment Procedure

This procedure is concerned with performing measurements by involving the necessary network and/or UE resources. Depending on the positioning method to be used for locating the UE the internals of this procedure can be positioning method dependent. The procedure is completed with the end of the positioning measurements.

Location Calculation and Release Procedure

This generic procedure is initiated after the measurements are completed and is concerned with calculating the location of the UE and releasing all network and/or UE resources involved in the positioning.

9.1 Mobile Terminating Location Request

9.1.1 MT-LR routing procedure in PS and CS domain

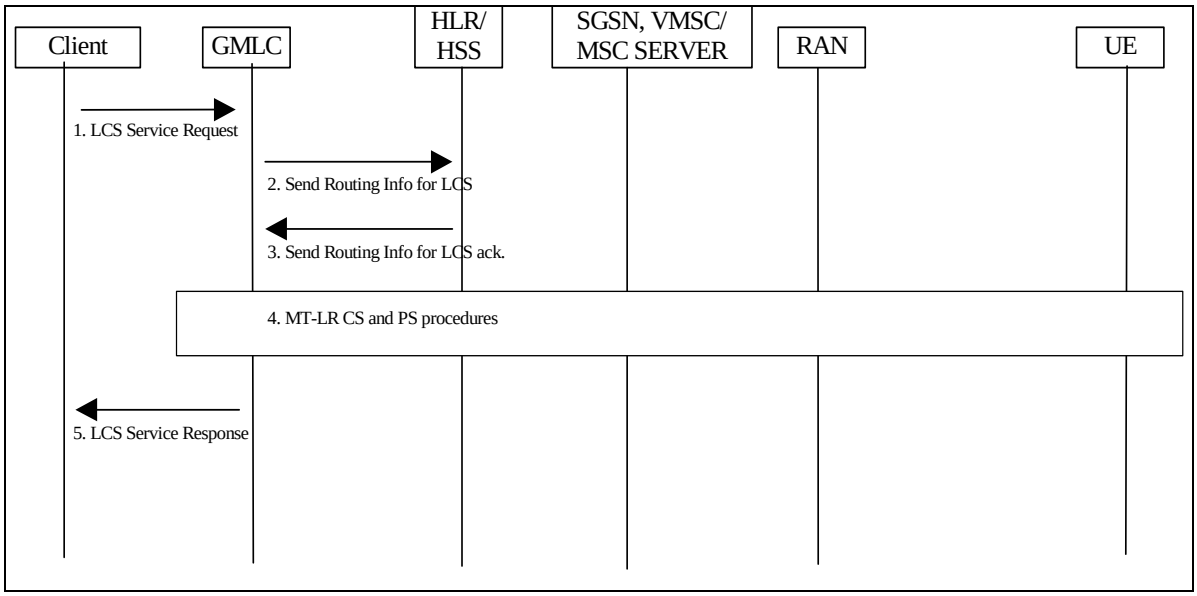


Figure 9.1: General Network Positioning for a MT-LR

1) An external LCS client requests the current location of a target UE from a GMLC. The LCS Client may also request a deferred location request, i.e. based on event. The GMLC verifies the identity of the LCS client and its subscription to the LCS service requested and derives the MSISDN or IMSI or PDP address, (NOTE: IP addressing in this context is FFS, one reason is the dynamic IP addressing used in IPv4.) of the target UE to be located and the LCS QoS from either subscription data or data supplied by the LCS client. For a call related location request, the GMLC obtains and authenticates the called party number of the LCS client.

   The LCS request may carry also the Service Identity and the Codeword. The GMLC may verify that the Service Identity received in the LCS request matches one of the service identities allowed for the LCS client. If the service identity does not match one of the service identities for the LCS client, the GMLC shall reject the LCS request. Otherwise, the GMLC can map the received service identity in a corresponding service type.
   If the codeword functionality is supported, the GMLC shall reject the LCS service request in case the LCS client type is “value added” and the codeword was not received.
   If the location request is originated by a Requestor, the Requestor Identity may be added to the LCS service request. LCS client should authenticate the Requestor Identity but this is outside the scope of this specification.

   For a session related location request, the GMLC obtains and authenticates the APN-NI of the LCS client.
   If location is required for more than one UE, or if periodic location is requested, the steps following below may be repeated.
   Note: This means that GMLC handles the periodicity of location requests as requested by the LCS client both in CS and PS domain.

2) If the GMLC already knows both the VMSC/MSC server or SGSN location and IMSI for the particular MSISDN or PDP address, (e.g. from a previous location request), and the codeword functionality is not supported, this step and step 3 may be skipped. Otherwise, the GMLC sends a SEND_ROUTING_INFO_FOR_LCS message to the home HLR/HSS of the target UE to be located with the IMSI, PDP address or MSISDN of this UE. When the GMLC supports the codeword functionality, steps 2 and 3 shall not be skipped. The SEND_ROUTING_INFO_FOR_LCS message may carry also the Codeword received by the LCS client in the LCS Service request. For a LCS client type different from “value added” an indication may be sent to the HLR, in order to inform the HLR that the codeword is not applicable.

Editor´s note: The use of the PDP address for identifying the subscriber is ffs.

3) The HLR/HSS verifies that the calling party SCCP address of the GMLC corresponds to a known GSM/UMTS network element that is authorized to request UE location information. The HLR/HSS then returns one or several

of the addresses, the current SGSN and/or VMSC/MSC server and whichever of the IMSI and MSISDN was not provided in step (2) for the particular UE.
Note: HLR may prioritize between the MSC/VLR or SGSN address sent to GMLC. The prioritisation might be based on information received from SGSN and/or MSC/VLR concerning the MS's capabilities for LCS. Other priority criteria are for further study.

The HLR may check if the codeword received in SEND_ROUTING_INFO_FOR_LCS message matches one of the codewords stored for the target subscriber. If it doesn't match, then the HLR shall return an error message to the GMLC. If no codeword is stored in the HLR for the target subscriber, the request shall not be rejected by the HLR and shall send to the GMLC the related indication in SEND_ROUTING_INFO_FOR_LCS_ack message. If the HLR receives the indication from the GMLC that the codeword is not applicable, the codeword check is not performed in the HLR.

Moreover, if the HLR supports the Enhanced User Privacy, the HLR shall check if the VMSC and/or the SGSN under which the target subscriber is located supports the enhanced user privacy mechanisms (Service type and Requestor), by checking the supported LCS capabilities set. Only the address of a serving node that supports the enhanced user privacy mechanism will be returned to GMLC. If none of the VMSC or SGSN supports the Enhanced User Privacy, then the HLR shall send an error indication to the GMLC.

NOTE: This handling allows the HPLMN to have the control about the fact that the VPLMN supports the EUP mechanisms, in order to fully protect the user privacy.

4) In case GMLC receives only the MSC/VLR address, the MT LR proceeds as the CS-MT-LR procedure described in 9.1.2. In case GMLC receives only the SGSN address, the MT LR proceeds as the PS-MT-LR procedure described in 9.1.6. In case the GMLC receives several of the following addresses, SGSN, VMSC and/or MSC Server, it has to decide where to send the location request. If the requested MT-LR is known to be associated with a CS call, the CS-MT-LR procedure shall be invoked. If the requested MT-LR is associated with a PS session, the PS-MT-LR procedure only shall be invoked. Otherwise, both CS-MT-LR and PS-MT-LR are applicable. If LCS Client indicated deferred location request, GMLC shall indicate this together with applicable event type (ex. MS available) in requested PS/CS-MT-LR, see 9.1.8.

NOTE: The order in which these procedures are invoked and whether one or both procedures are used may depend on subscription information for the LCS client, possible priority information returned by the HSS or information already stored in the GMLC (e.g. obtained from previous location requests).

5) GMLC sends the location service response to the LCS client. If the LCS client requires it, the GMLC may first transform the universal location co-ordinates provided by the SGSN or MSC/MSC server into some local geographic system. The GMLC may record billing for both the LCS client and inter-network revenue charges from the SGSN or MSC/MSC server's network.

The detailed CS-MT-LR and PS-MT-LR procedures in step 4 of figure 9.1 are described in 9.1.2 and 9.1.6.

The detailed procedure for deferred PS/CS-MT-LR is described in 9.1.8.

9.1.2 Circuit Switched Mobile Terminating Location Request (CS-MT-LR)

Figure 9.2 illustrates general network positioning for LCS clients external to the PLMN. In this scenario, it is assumed that the target UE is identified using either an MSISDN or IMSI.

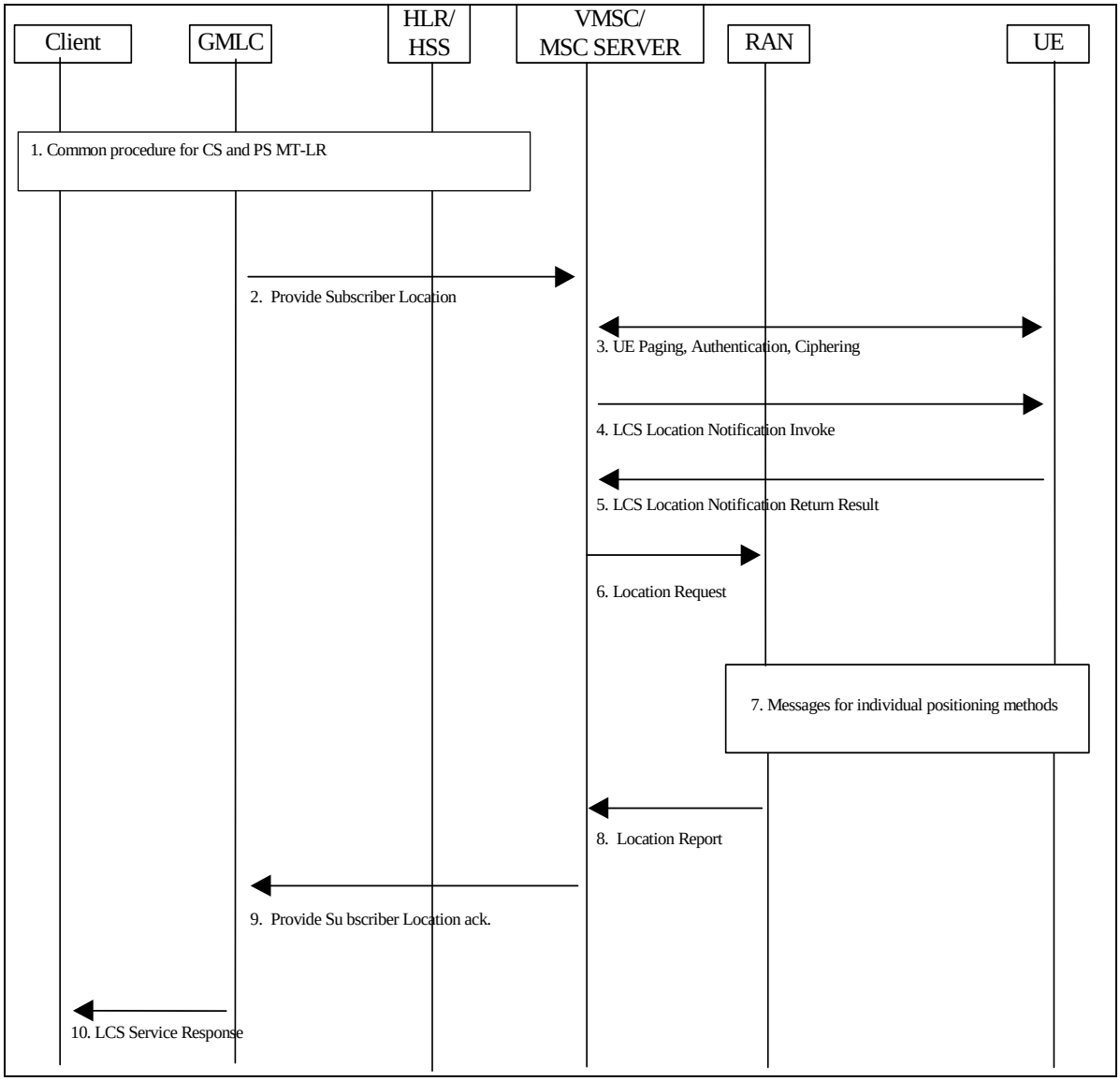


Figure 9.2: Network Positioning for a CS-MT-LR

9.1.2.1 Location Preparation Procedure

1) Common PS and CS MT-LR procedure as described in 9.1.1.

2) The GMLC sends a PROVIDE_ SUBSCRIBER _LOCATION message to the MSC/MSC server indicated by the HLR/HSS. This message carries the type of location information requested (e.g. current location), the UE subscriber's IMSI, LCS QoS information (e.g. accuracy, response time) and an indication of whether the LCS client has the override capability. For a call related location request, the message also carries the LCS client's called party number. For a value added LCS client, the message shall carry the client name, the external identity of the LCS client and the Requestor Identity (if that is both supported and available). For a PLMN operator LCS client, the message shall carry the internal identity of the LCS client. Moreover the message may also carry the Service Type**.** If the HLR indicated that no codeword was stored for the UE user, the message may carry also the codeword received from the LCS client, to be displayed to the UE. For a PLMN operator LCS client, the message shall carry the internal identity of the LCS client.

3) If the GMLC is located in another PLMN or another country, the VMSC/MSC server first authenticates that a location request is allowed from this PLMN or from this country. If not, an error response is returned. The VMSC/MSC server then verifies LCS barring restrictions in the UE user's subscription profile in the MSC server. In verifying the barring restrictions, barring of the whole location request is assumed if any part of it is barred or any requisite condition is not satisfied. If LCS is to be barred without notifying the target UE and a LCS client accessing a GMLC in the same country does not have the override capability, an error response is returned to the GMLC. Otherwise, if the UE is in idle mode, the Core Network performs paging, authentication and ciphering. The MSC will page a GPRS attached UE either through A/Iu or Gs interface, depending on the presence of the Gs interface (see Note).The UE will inform the network about its LCS capabilities, as described in chapter 6.3.4.. If the UE is instead in dedicated mode, the VMSC/MSC server will already have UE classmark information. In GSM this is supported by controlled early classmark sending.

[Note 1: In GSM, if the target UE has an established circuit call other than speech, the location request may be denied and an error response is then returned to the GMLC. If the location request is allowed for a non-speech circuit call, it shall be up to RAN to decide, on the basis of the applicable position methods and requested QoS, whether positioning is possible. This is FFS]

Note: In some network mode of operation, a GPRS capable UE may not receive the CS paging. In addition, upon receipt of a CS paging, a GPRS capable UE may immediately answer to the Paging Request or delay the answer, as defined in 3GPP TS 22.060 and 23.060. A GPRS UE in class B mode may also suspend its GPRS traffic, sending a GPRS Suspension Request to the network.

4) 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, the Requestor Identity (if that is both supported and available) and whether privacy verification is required. Moreover, the message may carry also the service type and the codeword.

   [FFS: For a call related location request, the LCS client identity shall be set to the LCS client's called party number if no separate LCS client identity was received from the GMLC.] Optionally, the VMSC/MSC server may after sending the LCS Location Notification Invoke message continue in parallel the location process, i.e. continue to step 6 without waiting for a LCS Location Notification Return Result message in step 5.

NOTE 2: This step is for further study, it should be investigated e.g. which client identities to include in the Privacy Notification message to be shown to the end-user.

5) The target UE notifies the UE user of the location request. If privacy verification was requested, the target UE indicates to the UE user whether the location request will be allowed or not allowed in the absence of a response and waits for the user to grant or withhold permission. The UE then returns an LCS Location Notification Return Result to the VMSC/MSC server indicating, if privacy verification was requested, whether permission is granted or denied. Optionally, the LCS Location Notification Return Result message can be returned some time after step 4, but before step 9. If the UE user does not respond after a predetermined time period, the VMSC/MSC server shall infer a "no response" condition. The VMSC/MSC server shall return an error response to the GMLC if privacy verification was requested and either the UE user denies permission or there is no response with the UE subscription profile indicating barring of the location request in the absence of a response.

6) The MSC/MSC server sends a Location Request message to RAN. This message includes the type of location information requested and requested QoS and, in GSM, the UE's location capabilities.

9.1.2.2 Positioning Measurement Establishment Procedure

7) RAN determines the positioning method and instigates the particular message sequence for this method, as specified in UTRAN Stage 2, TS 25.305 [1] and GERAN Stage 2, TS 43.059 [16].

9.1.2.3 Location Calculation and Release Procedure

8) When a location estimate best satisfying the requested QoS has been obtained, RAN returns it to the MSC/MSC server in a Location Report message. If a location estimate could not be obtained, RAN returns a Location Report message containing a failure cause and no location estimate.

9) The MSC/MSC server returns the location information and its age to the GMLC, if the VMSC/MSC server has not initiated the Privacy Verification process in step 4. If step 4 has been performed for privacy verification, the VMSC/MSC server returns the location information only, if it has received a LCS Location Notification Return Result indicating that permission is granted. If a LCS Location Notification Return Result message indicating that permission is not granted is received, or there is no response, with the UE subscription profile indicating barring of location in the absence of a response, the VMSC/MSC server shall return an error response to the GMLC. If RAN did not return a successful location estimate, but the privacy checks in steps 4 - 5 were successfully executed, the VMSC/MSC server may return the last known location of the target UE if this is known and the LCS client is requesting the current or last known location. The MSC server may then release the Mobility Management connection to the UE, if the UE was previously idle, and the MSC/MSC server may record billing information.

10) The GMLC returns the UE location estimate to the requesting LCS client as described in chapter 9.1.1.

9.1.3 CS-MT-LR without HLR Query - applicable to North America Emergency Calls only

Figure 9.3 illustrates location for a North American Emergency Services call, where an emergency services client identifies the target UE using an IMSI, MSISDN or NA-ESRK plus, possibly IMEI, that were previously provided to it by the VMSC. The emergency services client also identifies the VMSC to the GMLC by providing an NA-ESRD or NA-ESRK or by referring to information for the target UE already stored in the GMLC. This allows the GMLC to request location from the VMSC without first querying the home HLR of the target UE. This is necessary when the home HLR either cannot be identified (e.g. client provides an NA-ESRK but not IMSI or MSISDN) or does not support the LCS query procedure.

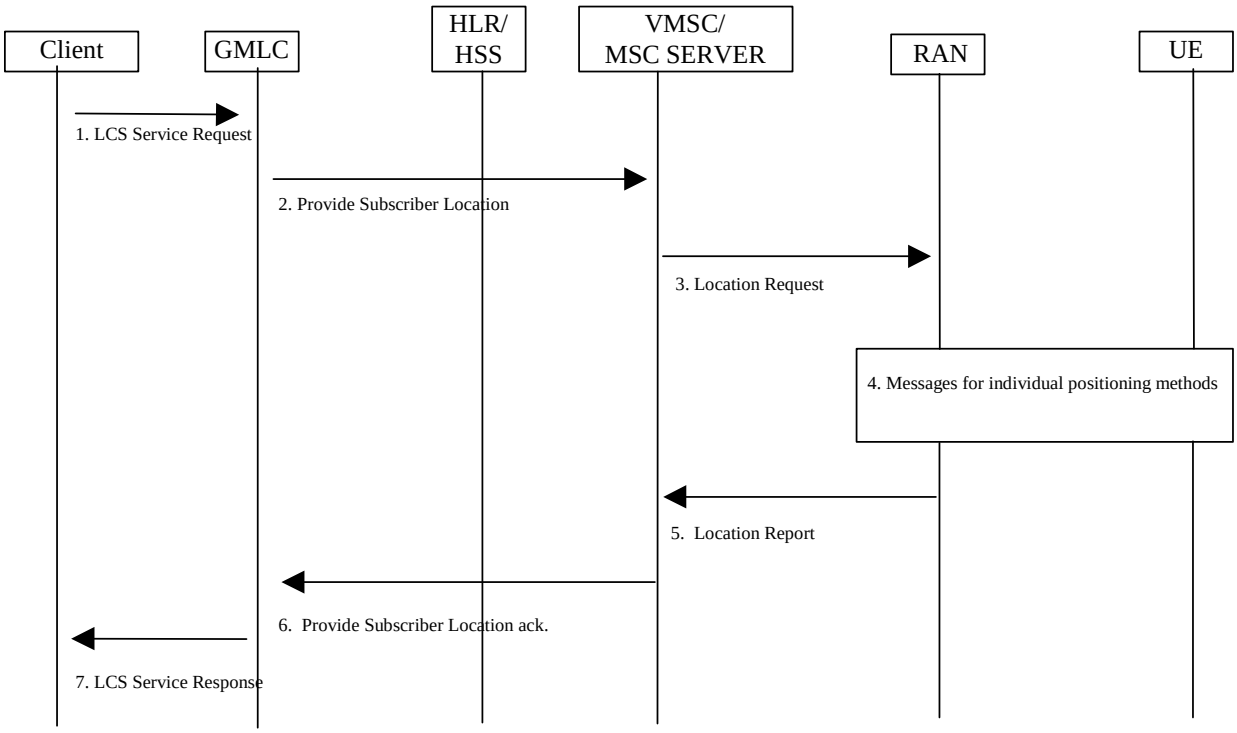


Figure 9.3: Positioning for a Emergency Services MT-LR without HLR Query

1) Same as step 1 in figure 9.1 but with the LCS client identifying first the target UE by an IMSI, MSISDN or NA-ESRK and possibly IMEI and, second, the VMSC by an NA-ESRK or NA-ESRD.

2) If the GMLC already has stored information for the target UE (e.g. from a prior location estimate delivery to the LCS client), the GMLC may determine the VMSC from this information. Otherwise, the GMLC determines the VMSC using the NA-ESRK or NA-ESRD - with use of the NA-ESRK taking priority over that of the NA-ESRD. The MAP_PROVIDE_SUBSCRIBER_LOCATION message sent to the VMSC carries the IMSI, if available or MSISDN and, if provided, the IMEI for the target UE, as well as the required QoS and an indication of a location request from an emergency services client. The VMSC identifies the target UE using the IMSI or MSISDN and, if provided, the IMEI.

3) The MSC verifies that UE privacy is overridden by the emergency services provider and that positioning is not prevented for other reasons (e.g. unreachable UE, inapplicable call type to the UE). The VMSC then sends a Location Request to the RAN, as for a normal MT-LR.

4) RAN performs positioning as for a normal CS-MT-LR.

5) RAN returns a location estimate to the VMSC as for a normal CS-MT-LR.

6) Same as steps 9 for a normal CS-MT-LR.

7) Same as steps 10 for a normal CS-MT-LR.

9.1.4 CS-MT-LR and PS-MT-LR for a previously obtained location estimate

Every time the location estimate of a target UE subscriber is returned by the RAN to the VMSC, MSC Server or SGSN, the corresponding entity may store the location estimate together with a time stamp. The MSC/MSC server may store this information in the subscriber's MSC server record.

The time stamp is the time at which the location estimate is stored at the corresponding entity i.e. after the RAN returns the location estimate to the VMSC, MSC Server or SGSN. The time stamp indicates the "age" of the location estimate.

9.1.4.1 Initial Location

In the context of an originating emergency call the location estimate and the associated time stamp at the commencement of the call set-up is referred to as *"initial location"*.

9.1.4.2 Current Location

After a location attempt has successfully delivered a location estimate and its associated time stamp, the location estimate and time stamp is referred to as the *"current location"* at that point in time.

9.1.4.3 Last known Location

The current location estimate and its associated time stamp are stored in MSC/VLR, MSC Server or SGSN and until replaced by a later location estimate and a new time stamp is referred to as the *"last known location"*. The last known location may be distinct from the initial location - i.e. more recent.

9.1.4.4 Security and Privacy

The handling of security and privacy of the target UE with regard to returning the last known or initial location estimate of the target UE shall be the same as when the target UE is reachable for positioning. (i.e. the requesting LCS client is authorized and the privacy of the target UE is secured before the VMSC/MSC server check the MSC server status of the target UE (i.e. whether the UE is marked as attached or detached in the MSC server). A similar status check apply for SGSN and MSC Server.

9.1.4.5 Failing to locate the target UE

In case of a "Detached" or "Not Reachable" target UE, the last known location and a time stamp stored at the VLR, MSC Server or SGSN, may be returned to a LCS client requesting location information if the LCS client specifically requested the current or last known location. This does not apply to a value added LCS client where the target UE subscribes to notification of the location request: if the notification cannot be performed, the VMSC, MSC Server or SGSN shall reject the location request.

NOTE: Due to CAMEL, the MSC/MSC server/VLR may already be storing other location information parameters like location number, service area identity and MSC server number in the subscriber's MSC server record.

When a request for location information is received at the VMSC, MSC Server or SGSN, the request shall indicate whether the "last known location of the target UE" should be returned in case of a "detached" or "not reachable" target UE.

If the VLR, MSC Server or SGSN has a valid copy of the subscriber's permanent data and the target UE's privacy settings are such that positioning is allowed, then the following two cases can occur.

9.1.4.5.1 Target UE is "Not Reachable"

If the target UE is marked as "attached" in the VLR, MSC Server or SGSN, the corresponding entity orders paging of the target UE. If paging fails, due to target UE being "not reachable" then the corresponding VMSC, MSC Server or SGSN shall check whether the LCS client has requested "last known location" in case of "not reachable" target UE.

If such a request exists and notification to the target UE does not apply for a value added LCS client, the VMSC, MSC Server or SGSN shall include the last known location together with the time stamp available in its response to the request for location information.

An indicator of "last known location" returned shall be marked at the CDR at VMSC, MSC Server or SGSN correspondingly.

9.1.4.5.2 Target UE is "Detached"

If the target UE is marked as "detached" in the VLR, MSC Server or SGSN, the corresponding entity shall check whether the LCS client has requested "last known location" in case of "detached" target UE.

If such a request exists and notification to the target UE does not apply for a value added LCS client, the VMSC, MSC Server or SGSN includes the "last known location" together with the time stamp available in its response to the request for location information.

An indicator of "last known location" returned shall be marked at the CDR at VMSC, MSC Server or SGSN.

9.1.4.5.3 Target UE is Reachable but Positioning Fails

If the target UE is reachable (e.g. paging succeeds), but the VMSC, MSC Server or SGSN is unable to obtain a current location estimate, then the corresponding entity shall check whether the LCS client has requested "last known location".

If such a request exists and notification to the target UE either does not apply or was successfully executed for a value added LCS client, the VMSC, MSC Server or SGSN includes the "last known location" together with the time stamp available in its response to the request for location information. An indicator of "last known location" returned shall be marked at the CDR at VMSC.

9.1.4.5.4 MSC Server or SGSN.Target UE is "Purged"

If the target UE is marked as "Purged" in HLR/HSS, then an indication "Absent Subscriber" is returned to the GMLC.

9.1.5 Network Induced Location Request (NI-LR)

Figure 9.4 illustrates positioning for an emergency service call.

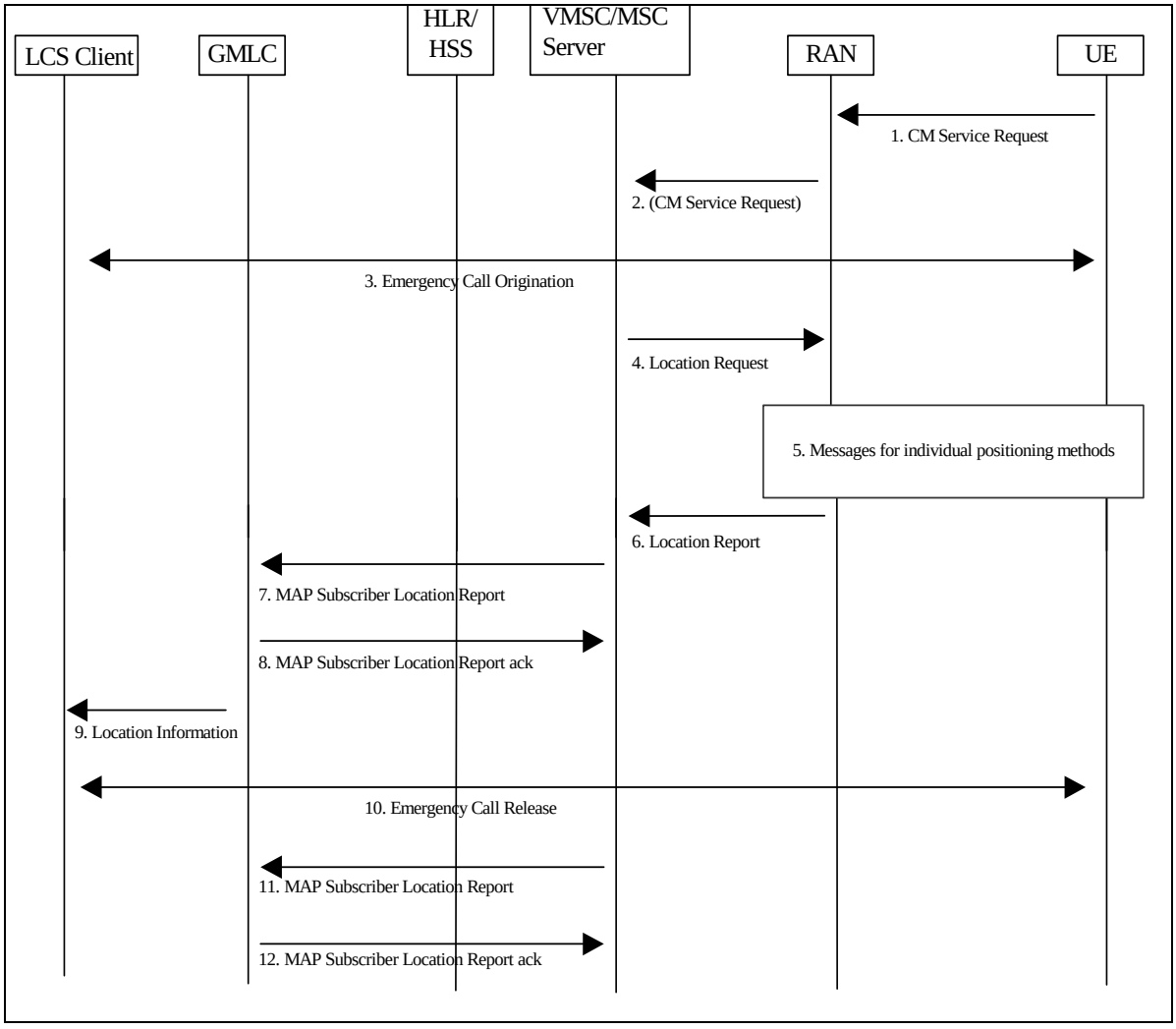


Figure 9.4: Positioning for a NI-LR Emergency Service Call

9.1.5.1 Location Preparation Procedure

1) An initially idle UE requests radio connection setup indicating a request for an Emergency Service call to the VMSC/MSC server via RAN.

2) RAN shall convey the CM service request to the core network. (Before having a CM connection there must be a radio connection.) The UE may identify itself using a TMSI, IMSI or IMEI.

3) The emergency call procedure is applied. The VMSC/MSC server, RAN and UE continue the normal procedure for emergency call origination towards the appropriate emergency services client. Depending on local regulatory requirements, the sending of call setup information into the PSTN may be delayed until either the UE's location has been obtained or the location attempt has failed or a PLMN defined timer has expired before location was obtained. Call setup information sent into the PSTN may include the UE location (if already obtained) plus information that will enable the emergency service provider to request UE location at a later time (e.g. NA-ESRD and NA-ESRK in North America).

4) At any time after step 1, the VMSC/MSC server may initiate procedures to obtain the UE's location. These procedures may run either in parallel with the emergency call origination or while emergency call origination is suspended to delay sending of call setup information into the PSTN according to step 3. The VMSC/MSC server sends a Location Request message to RAN associated with the UE's current location area (see step 6 for a MT-LR). This message includes the QoS required for an emergency call.

9.1.5.2 Positioning Measurement Establishment Procedure

5) When a location estimate best satisfying the requested QoS has been obtained, the RAN returns it to the MSC server in a location response. If a location estimate could not be obtained, the RAN returns a location response containing a failure cause and no location estimate.

9.1.5.3 Location Calculation and Release Procedure

6) When a location estimate best satisfying the requested QoS has been obtained, RAN returns it to the VMSC/MSC server.

7) Depending on local regulatory requirements, the VMSC/MSC server may send a MAP Subscriber Location report to a GMLC associated with the emergency services provider to which the emergency call has been or will be sent. This message shall carry any location estimate returned in step 6, the age of this estimate and may carry the MSISDN, IMSI and IMEI of the calling UE. In North America, any NA-ESRD and any NA-ESRK that may have been assigned by the VMSC/MSC server shall be included. The message shall also indicate the event that triggered the location report. If location failed (i.e. an error result was returned by RAN in step 6), an indication of failure rather than a location estimate may be sent to the GMLC: the indication of failure is conveyed by not including a location estimate in the MAP Subscriber Location Report.

8) The GMLC acknowledges receipt of the location information. For a North American Emergency Services call, the GMLC shall store the location information for later retrieval by the emergency services LCS client.

9) The GMLC may optionally forward the information received in step 8 to the emergency services LCS client. For a North American emergency services call the client is expected to obtain the location information by requesting it from the GMLC.

10) At some later time, the emergency services call is released.

11) For a North American Emergency Services call, the MSC/MSC server sends another MAP Subscriber Location Report to the GMLC. This message may include the same parameters as before except that there is no position estimate and an indication of emergency call termination is included.

12) The GMLC acknowledges the MSC/MSC server notification and may then release all information previously stored for the emergency call.

Editorial Note: The procedure for Network Induced Location Request (NI-LR and PS-NI-LR) for a Target UE in dedicated mode should be defined in UTRAN system stage 2 [1] and GERAN Stage 2 specifications [16].

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

Figure 9.5 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 UE is identified using an MSISDN, PDP address or IMSI.

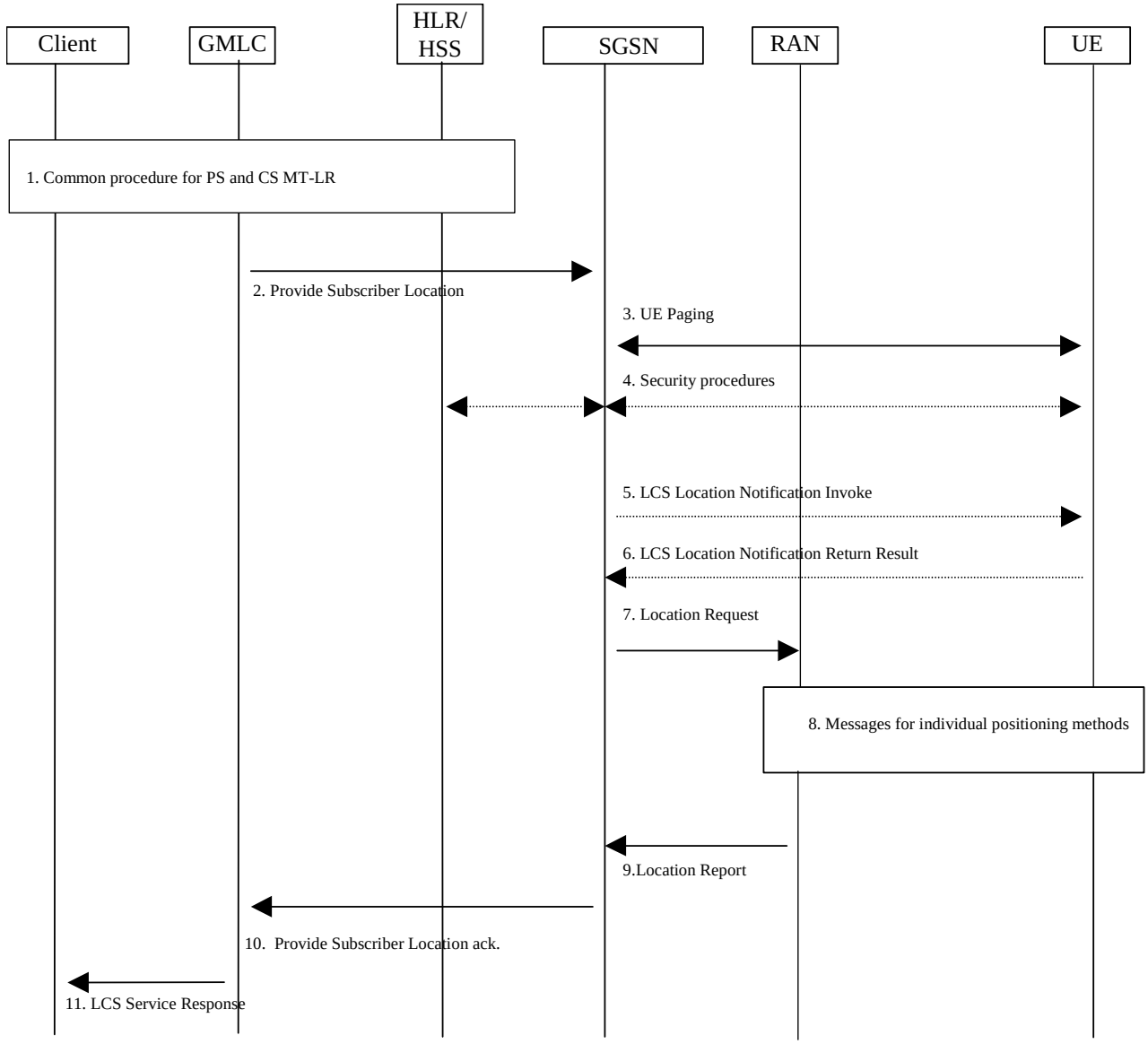


Figure 9.5: General Network Positioning for Packet Switched MT-LR

9.1.6.1 Location Preparation Procedure

1) Common PS and CS MT-LR procedure as described in 9.1.1.

2) GMLC sends a Provide Subscriber Location message to the SGSN indicated by the HLR/HSS. This message carries the type of location information requested (e.g. current location), the UE subscriber's IMSI, LCS QoS information (e.g. accuracy, response time) and an indication of whether the LCS client has the override capability. For a session related location request, the message also carries the APN-NI to which the user has established the session. For a value added LCS client, the message shall carry the client name, the external identity of the LCS client and the Requestor Identity (if that is both supported and available), optionally the message may also carry the Service Type. If the HLR indicated that no codeword was stored for the UE user, the message may carry also the codeword received from the LCS client, to be displayed to the UE. For a PLMN operator LCS client, the message shall carry the internal identity of the LCS client.

3) If the GMLC is located in another PLMN or another country, the SGSN first authenticates that a location request is allowed from this PLMN or from this country. If not, an error response is returned. The SGSN then verifies LCS barring restrictions in the UE user's subscription profile in the SGSN. In verifying the barring restrictions, barring of the whole location request is assumed if any part of it is barred or any requisite condition is not satisfied. If LCS is to be barred without notifying the target UE and a LCS client accessing a GMLC in the same country does not have the override capability, an error response is returned to the GMLC.
Otherwise, if the UE is in idle mode, the SGSN performs paging. The paging procedure is defined in TS 23.060[15].

   FFS: The UE may be paged for location services even when in UMTS a signaling connection between mobile station and the network is established and in GSM when in Ready Mode. This makes it possible for the UE to start preparing an anticipated location service coming later by e.g. starting to measure GPS signals.

4) Security functions may be executed. These procedures are defined in TS 23.060 [15].

5) 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, a 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 and the Requestor Identity (if that is both supported and available), whether privacy verification is required. Moreover, the message may carry also the service type and the codeword. Optionally, the SGSN may after sending the LCS Location Notification Invoke message continue in parallel the location process, i.e. continue to step 7 without waiting for a LCS Location Notification Return Result message in step 6.

6) The target UE notifies the UE user of the location request and, if privacy verification was requested, waits for the user to grant or withhold permission. The UE then returns a notification result to the SGSN indicating, if privacy verification was requested, whether permission is granted or denied. Optionally, this message can be returned some time after step 5, but before step 10. If the UE user does not respond after a predetermined time period, the SGSN shall infer a "no response" condition. The SGSN shall return an error response to the GMLC if privacy verification was requested and either the UE user denies permission or there is no response with the UE subscription profile indicating barring of the location request.

7) The SGSN sends a Location Request message to the RAN. This message includes the type of location information requested, the requested QoS and any other location information received in paging response.

9.1.6.2 Positioning Measurement Establishment Procedure

8) If the requested location information and the location accuracy within the QoS can be satisfied based on parameters received from the SGSN and the parameters obtained by the RAN e.g. cell coverage and timing information (i.e. RTT or TA), the RAN may send a Location Report immediately. Otherwise, the RAN determines the positioning method and instigates the particular message sequence for this method in UTRAN Stage 2 TS 25.305 and in GERAN Stage 2 TS 43.059. If the position method returns position measurements, the RAN uses them to compute a location estimate. If there has been a failure to obtain position measurements, the RAN may use the current cell information and, if available, RTT or TA value to derive an approximate location estimate. If an already computed location estimate is returned for an UE based position method, the RAN may verify consistency with the current cell and, if available, RTT or TA. If the location estimate so obtained does not satisfy the requested accuracy and sufficient response time still remains, the RAN may instigate a further location attempt using the same or a different position method. If a vertical location co-ordinate is requested but the RAN can only obtain horizontal co-ordinates, these may be returned.

9.1.6.3 Location Calculation and Release Procedure

9) When location information best satisfying the requested location type and QoS has been obtained, the RAN returns it to the SGSN in a Location Report message. If a location estimate could not be obtained, the RAN returns a Location Report message containing a failure cause and no location estimate.

10) The SGSN returns the location information and its age to the GMLC, if the SGSN has not initiated the Privacy Verification process in step 5. If step 5 has been performed for privacy verification, the SGSN returns the location information only, if it has received a LCS Location Notification Return Result indicating that permission is granted. If a LCS Location Notification Return Result message indicating that permission is not granted is received, or there is no response, with the UE subscription profile indicating barring of location, the SGSN shall return an error response to the GMLC. If the SGSN did not return a successful location estimate, but the privacy checks were successfully executed, the SGSN may return the last known location of the target UE if this is known and the LCS client is requesting the current or last known location. The SGSN may record billing information.

11) The GMLC returns the UE location information to the requesting LCS client. If the LCS client requires it, the GMLC may first transform the universal location co-ordinates provided by the SGSN into some local geographic system. The GMLC may record billing for both the LCS client and inter-network revenue charges from the SGSN's network.

9.1.7 Packet Switched Network Induced Location Request (PS-NI-LR)

Figure 9.6 illustrates a network induced location request from the SGSN. This procedure may be used e.g. for positioning of an emergency call.

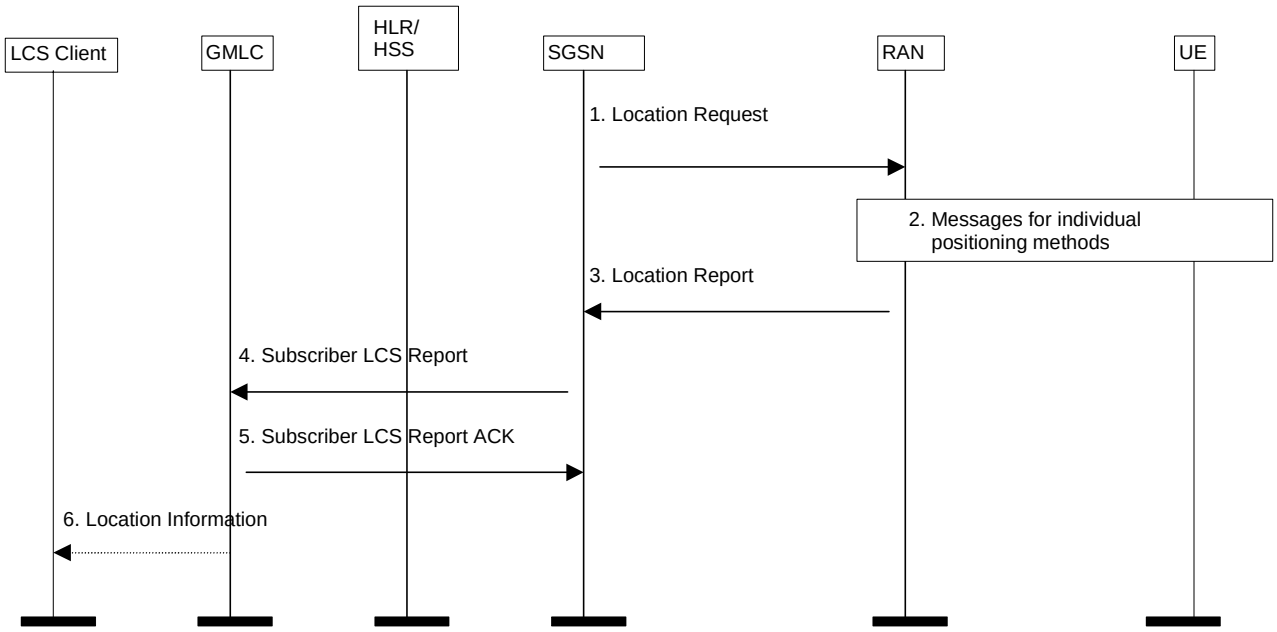


Figure 9.6: Network Induced Location Request

1) The SGSN sends a Location Request message to the RAN. This message indicates the type of location information requested and requested QoS.

9.1.7.1 Positioning Measurement Establishment Procedure

2) If the requested location information and the location accuracy within the QoS can be satisfied based on parameters received from the SGSN and the parameters obtained by the RAN e.g. cell coverage and timing information (i.e. RTT or TA), the RAN may send a Location Report immediately. Otherwise, the RAN determines the positioning method and instigates the particular message sequence for this method. If the position method returns position measurements, the RAN uses them to compute a location estimate. If there has been a failure to obtain position measurements, the RAN may use the current cell information and, if available, RTT or TA value to derive an approximate location estimate. If an already computed location estimate is returned for an UE based position method, the RAN may verify consistency with the current cell and, if available, RTT or TA value. If the location estimate so obtained does not satisfy the requested accuracy and sufficient response time still remains, the RAN may instigate a further location attempt using the same or a different position method. If a vertical location co-ordinate is requested but the RAN can only obtain horizontal co-ordinates, these may be returned.

9.1.7.2 Location Calculation and Release Procedure

3) When a location estimate best satisfying the requested QoS has been obtained , the RAN returns a Location Report to the SGSN. This message carries the location estimate that was obtained. If a location estimate was not succesfully obtained , a failure cause is included in the Location Report.

4) The SGSN shall send a MAP Subscriber Location Report to the GMLC obtained in step 1 carrying the MSISDN or PDP address of the UE, the identity of the LCS client, the event causing the location estimate (NI-LR-PS) and the location estimate and its age.

5) The GMLC shall acknowledge receipt of the location estimate provided that it serves the identified LCS client and the client is accessible.

6) The GMLC may transfer the location information to the LCS client either immediately or upon request from the client.

9.1.8 Mobile Terminating Deferred Location Request

Figure 9.6a illustrates the procedures for a Deferred Location Request, where the Location Report is returned based on a event.

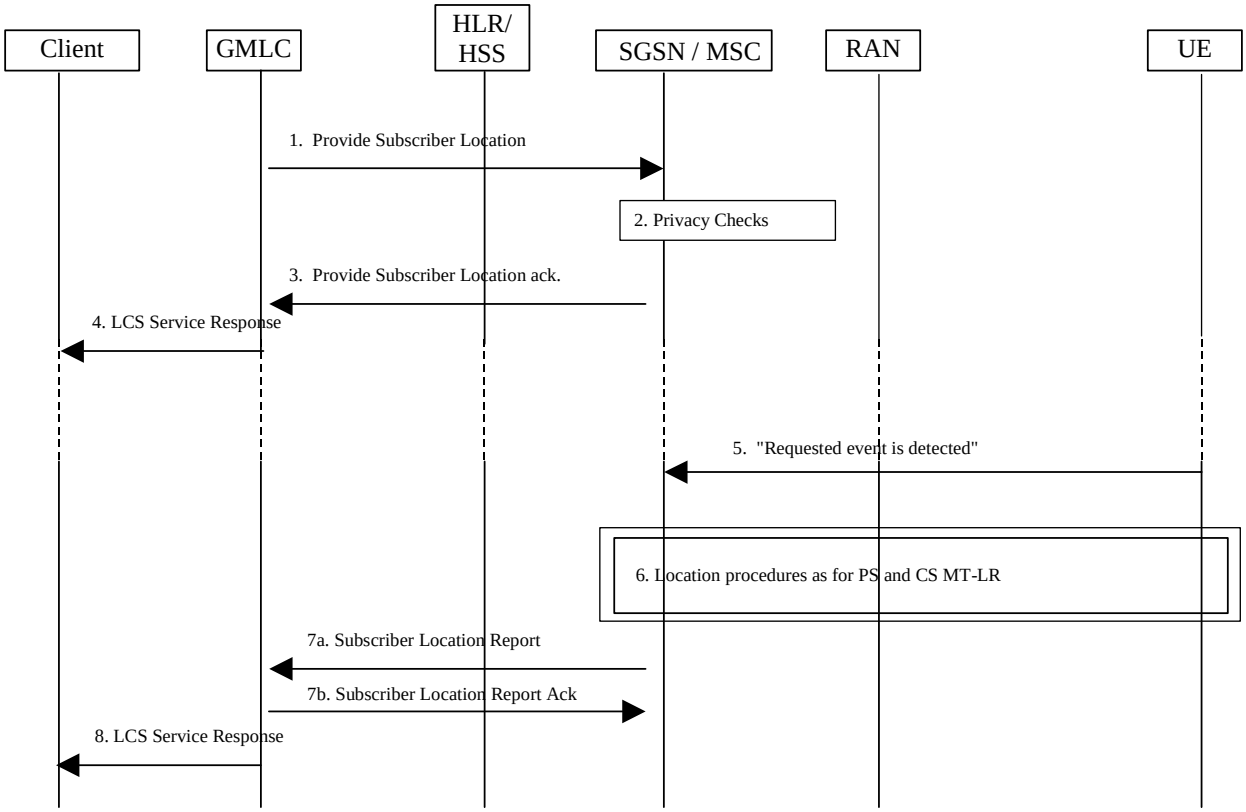


Figure 9.6a: General Network Positioning for a Deferred MT-LR

9.1.8.1 Deferred Location Request Procedure

1) Provide Subscriber Location is received in SGSN/MSC as described in 9.1.2/9.1.6. In addition, the Deferred Location Request includes the event that shall trigger the sending of Location Report.

2) If the SGSN/MSC cannot support the deferred location request for the specified event (for temporary or permanent reasons), a Provide Subscriber Location return error shall be returned in step 3 with a suitable cause. The SGSN/MSC verifies that the LCS client is allowed to position the requested UE according to subscription information (no interaction at this stage with the UE). If not, a Provide Subscriber Location return error is returned in step 3.

3) If the SGSN/MSC can support the deferred location request for the specified event and the privacy checks in step 2 are satisfied, a Provide Subscriber Location ack. shall be returned to the GMLC without a location estimate.

4) The GMLC then returns the LCS Service Response to the LCS Client to notify whether the request was successfully accepted or not.

9.1.8.2 Location Report Procedure

5) Immediately following step 3, the SGSN/MSC shall verify if the requested event is already satisfied (e.g. UE available inferred from a current transaction) or can be invoked immediately (e.g. by paging the UE and receiving a page response). If requested event is not existing the SGSN/MSC waits until it has occurred or until some maximum time has expired.

=> In case the SGSN/MSC receives an indication that the UE has moved to another SGSN/MSC while it is waiting for the requested event to happen, a Subscriber Location Report is directly sent to the GMLC with the information that MT-LR must be re-initiated against the new SGSN/MSC. The adress of the new SGSN/MSC is included in Subscriber Location Report if available. (If new SGSN/MSC adress was included, the GMLC continues at step 1 above, otherwise it continues with an interrogation against HLR as described in 9.1.1.)

6) When the requested event is detected, the SGSN/MSC will proceed with the location request as described in 9.1.2/9.1.6.

If either security or privacy checks fails, a Subscriber Location Report is returned with appropriate error cause indicating termination of the deferred location request.

7) When location information has been obtained from the RAN, the SGSN/MSC returns the Subscriber Location Report. Included in the report is an indication that this is a response to a previously sent deferred location request.

If the location information could not be obtained, or the SGSN/MSC for some other reason decides to not wait any longer for the requested event to occur (ex. timer expires), the Subscriber Location Report will be returned with an appropriate error cause indicating termination of the deferred location request.

8) GMLC then returns the LCS Service Response to the LCS Client as in 9.1.2/9.1.6.

9.1.8.3 Combined Periodical/Deferred Mobile Terminating Location Request

Figure 9.6b illustrates the procedures for a Combined Periodical/Deferred Mobile Terminating Location Request, where the response to the LCS client is returned periodically and based on the event.

Note: In the current specification, it is assumed the LCS client issues the Periodical/Deferred MT-LR with only the location estimate type of "current location".

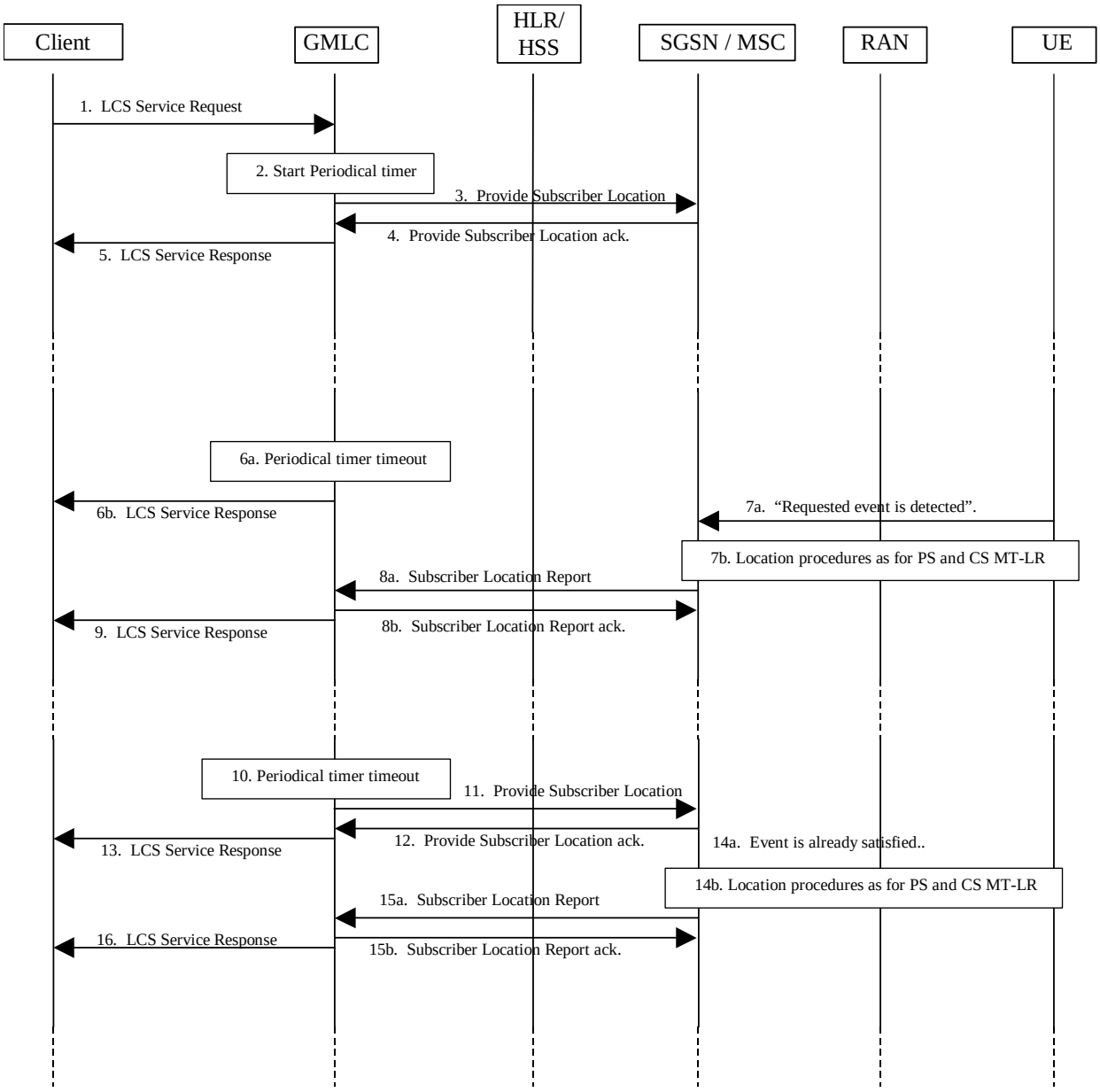


Figure 9.6b: General Network Positioning for a Combined Periodical/Deferred MT-LR

1) When a GMLC receives a LCS Service Request from a LCS client, the GMLC verifies the identity of the LCS client as described in 9.1.1.

2) The GMLC starts the periodical timer, sends a Send Routing Info for LCS to the home HLR/HSS of the target UE and gets SGSN/MSC addresses from the HLR/HSS as described in 9.1.1. If the GMLC already knows both the VMSC/MSC server or SGSN location and IMSI for the particular MSISDN or PDP address, (e.g. from a previous location request), the Send Routing Info is not sent to the HLR/HSS.

3) The GMLC sends a Deferred Location Request to the SGSN/MSC by means of Provide Subscriber Location as described in 9.1.2/9.1.6. In addition, the Deferred Location Request includes the event that shall trigger the sending of Subscriber Location Report.

4) If the SGSN/MSC cannot support the deferred location request for the specified event or the LCS client is not allowed to position the requested UE according to subscription information, a Provide Subscriber Location error is returned to the GMLC. If the SGSN/MSC can support the deferred location request for the specified event and the privacy checks are satisfied, a Provide Subscriber Location ack shall be returned to the GMLC without a location estimate.

5) The GMLC then returns the LCS Service Response to the LCS Client to notify whether the request was successfully accepted or not.

6) When the periodical timer expires, if the GMLC is still waiting for the event, the GMLC shall send a LCS Service Response to the LCS client, indicating that the location is not available at that moment.

7) When the requested event is detected, the SGSN/MSC will proceed with the location request as described in 9.1.2/9.1.6.

8) When location information has been obtained from the RAN, the SGSN/MSC returns the Subscriber Location Report. The report includes an indication that this is a response to a previously sent deferred location request.

If the location information could not be obtained, or the SGSN/MSC for some other reason decides to not wait any longer for the requested event to occur (ex. timer expires), the Subscriber Location Report will be returned with an appropriate error cause indicating termination of the deferred location request.

9) GMLC then returns the LCS Service Response to the LCS Client as in 9.1.2/9.1.6.

10) When the timer expires, if the GMLC is not waiting for the event, the GMLC sends a Send Routing Info for LCS to the home HLR/HSS of the target UE and receives SGSN/MSC addresses from the HLR/HSS as described in 9.1.1. If the GMLC already knows both the VMSC/MSC server or SGSN location and IMSI for the particular MSISDN or PDP address, (e.g. from a previous location request), the Send Routing Info is not sent to the HLR/HSS.

11) Same as step 3.

12) Same as step 4.

13) Same as step 5.

14) If the requested event is already satisfied, the SGSN/MSC will proceed with the location request as described in 9.1.2/9.1.6.

15) Same as step 8.

16) Same as step 9.

9.1.8.4 Cancellation of a Deferred Location Request

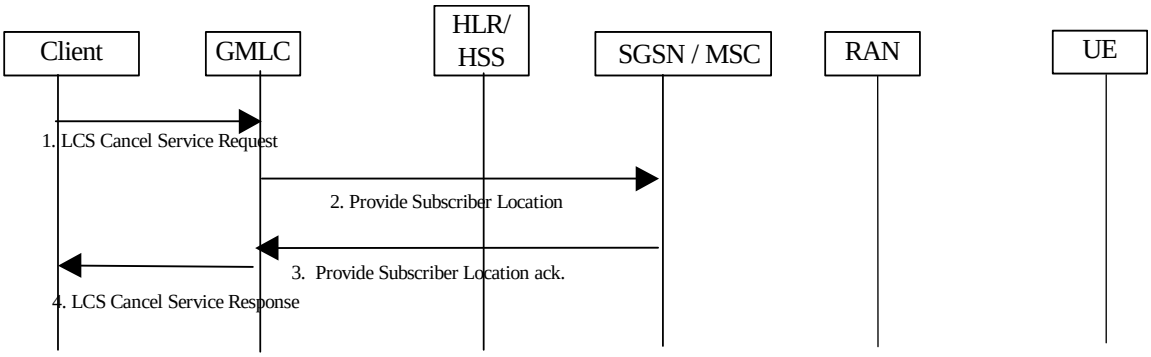


Figure 9.6c: Cancellation of a Deferred MT-LR procedure

1) The LCS Client requests the cancellation of a previously requested Deferred Location Request. The cancellation could be initiated by the GMLC itself for some reasons (e.g. implementation dependent timer in the GMLC expired). The event type to cancel must be indicated in the Cancellation procedure.

2) The GMLC will indicate this cancellation request in the Provide Subscriber Location toward the SGSN/MSC.

3) When the SGSN/MSC completes the cancellation procedure, it notifies it to the GMLC in the Provide Subscriber Location Ack (with no location estimate included).

4) The GMLC informs the LCS Client that the cancellation procedure has been successfully completed.

9.2 Mobile Originating Location Request

9.2.1 Mobile Originating Location Request, Circuit Switched (CS-MO-LR)

The following procedure shown in figure 9.7 allows an UE to request either its own location, location assistance data or broadcast assistance data message ciphering keys from the network. Location assistance data may be used subsequently by the UE to compute its own location throughout an extended interval using a mobile based position method. The ciphering key enables the UE to decipher other location assistance data broadcast periodically by the network. The MO-LR after location update request may be used to request ciphering keys or GPS assistance data using the follow-on procedure described in TS 24.008 [24]. The procedure may also be used to enable an UE to request that its own location be sent to another LCS client.

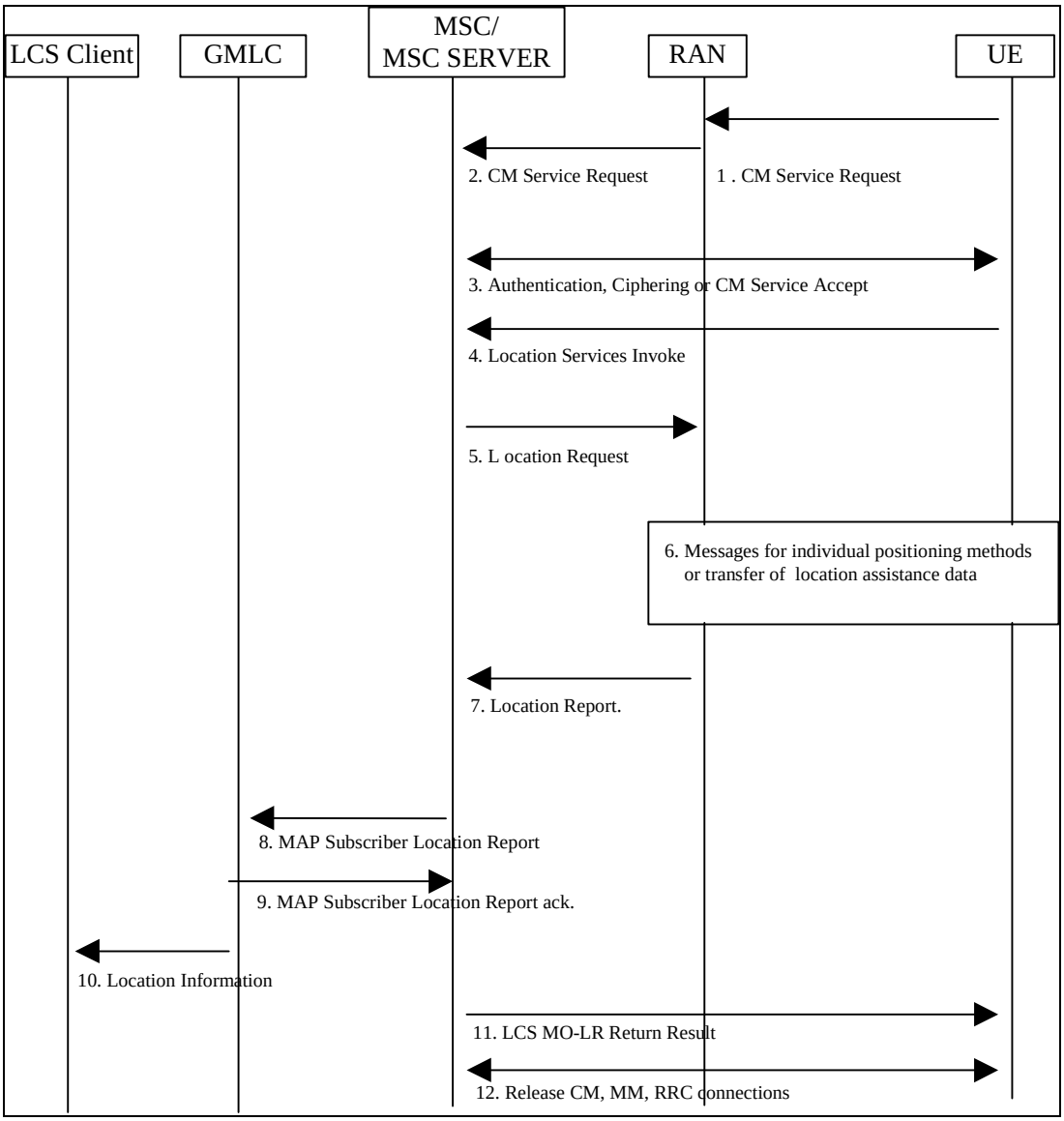


Figure 9.7: General Network Positioning for CS-MO-LR

9.2.1.1 Location Preparation Procedure

1) If the UE is in idle mode, the UE requests a radio connection setup and sends a CM service request indicating a request for a call independent supplementary services to the VMSC/MSC server via RAN.

2) RAN shall convey the CM service request to the core network. If the UE is in dedicated mode, the UE sends a CM Service Request on the already established radio connection.

3) The VMSC/MSC server instigates authentication and ciphering if the UE was in idle mode or returns a Direct Transfer CM Service Accept if the UE was in dedicated mode. The UE will inform the network about its LCS capabilities, as described in chapter 6.3.4.

4) The UE sends a LCS CS-MO-LR Location Services invoke to the VMSC/MSC server. If the UE is requesting its own location or that its own location be sent to another LCS client, this message carries LCS requested QoS information (e.g. accuracy, response time). If the UE is requesting that its location be sent to another LCS client, the message shall include the identity of the LCS client and may include the address of the GMLC through which the LCS client should be accessed. If a GMLC address is not included, the VMSC/MSC server may assign its own GMLC address and may verify that the identified LCS client is supported by this GMLC. If a GMLC address is not available for this case, the VMSC/MSC server shall reject the location request. If the UE is instead requesting location assistance data or ciphering keys, the message specifies the type of assistance data or deciphering keys and the positioning method for which the assistance data or ciphering applies. The VMSC/MSC server verifies in the UE's subscription profile that the UE has permission to request its own location, request that its location be sent to another LCS client or request location assistance data or deciphering keys (whichever applies). If the UE is requesting positioning and has an established call, the VMSC/MSC server may reject the request for certain non-speech call types.

5) The VMSC/MSC server sends a Location Request message to RAN associated with the Target UE. The message indicates whether a location estimate or location assistance data is requested and, in GSM, includes the UE's location capabilities. If the UE's location is requested, the message also includes the requested QoS. If location assistance data is requested, the message carries the requested types of location assistance data.

9.2.1.2 Positioning Measurement Establishment Procedure

6) If the UE is requesting its own location, RAN determines the positioning method and instigates the particular message sequence for this method, as specified in UTRAN Stage 2, TS 25.305 [1] and GERAN Stage 2, TS 43.059 [16]. If the UE is instead requesting location assistance data, RAN transfers this data to the UE as described in subsequent clauses in TS 25.305 [1] and TS 43.059 [16] UE.

9.2.1.3 Location Calculation and Release Procedure

7) When a location estimate best satisfying the requested QoS has been obtained or when the requested location assistance data has been transferred to the UE, RAN returns a Location Report to the VMSC/MSC server. This message carries the location estimate or ciphering keys if this was obtained. If a location estimate or deciphering keys were not successfully obtained or if the requested location assistance data could not be transferred successfully to the UE, a failure cause is included in the Location Report.

8) If the UE requested transfer of its location to another LCS client and a location estimate was successfully obtained, the VMSC/MSC server shall send a MAP Subscriber Location Report to the GMLC obtained in step 4 carrying the MSISDN of the UE, the identity of the LCS client, the event causing the location estimate (CS-MO-LR) and the location estimate and its age.

9) The GMLC shall acknowledge receipt of the location estimate provided that is serves the identified LCS client and the client is accessible.

10) The GMLC transfers the location information to the LCS client either immediately or upon request from the client.

11) The VMSC/MSC server returns an CS-MO-LR Return Result to the UE carrying any location estimate requested by the UE, ciphering keys or a confirmation that a location estimate was successfully transferred to the GMLC serving an LCS client.

12) The VMSC/MSC server may release the CM, MM and radio connections to the UE, if the UE was previously idle, and the VMSC/MSC server may record billing information.

NOTE: In case of positioning of emergency call stage 3 of the pervious sequence is naturally omitted.

9.2.2 Mobile Originating Location Request, Packet Switched (PS-MO-LR)

The following procedure shown in figure 9.8 allows an UE to request either its own location; location assistance data or broadcast assistance data message ciphering keys from the network. Location assistance data may be used subsequently by the UE to compute its own location throughout an extended interval using a mobile based position method. A ciphering key enables the UE to decipher other location assistance data broadcast periodically by the network. The PS-MO-LR may be used to request ciphering keys or GPS assistance data. The procedure may also be used to enable an UE to request that its own location be sent to another LCS client.

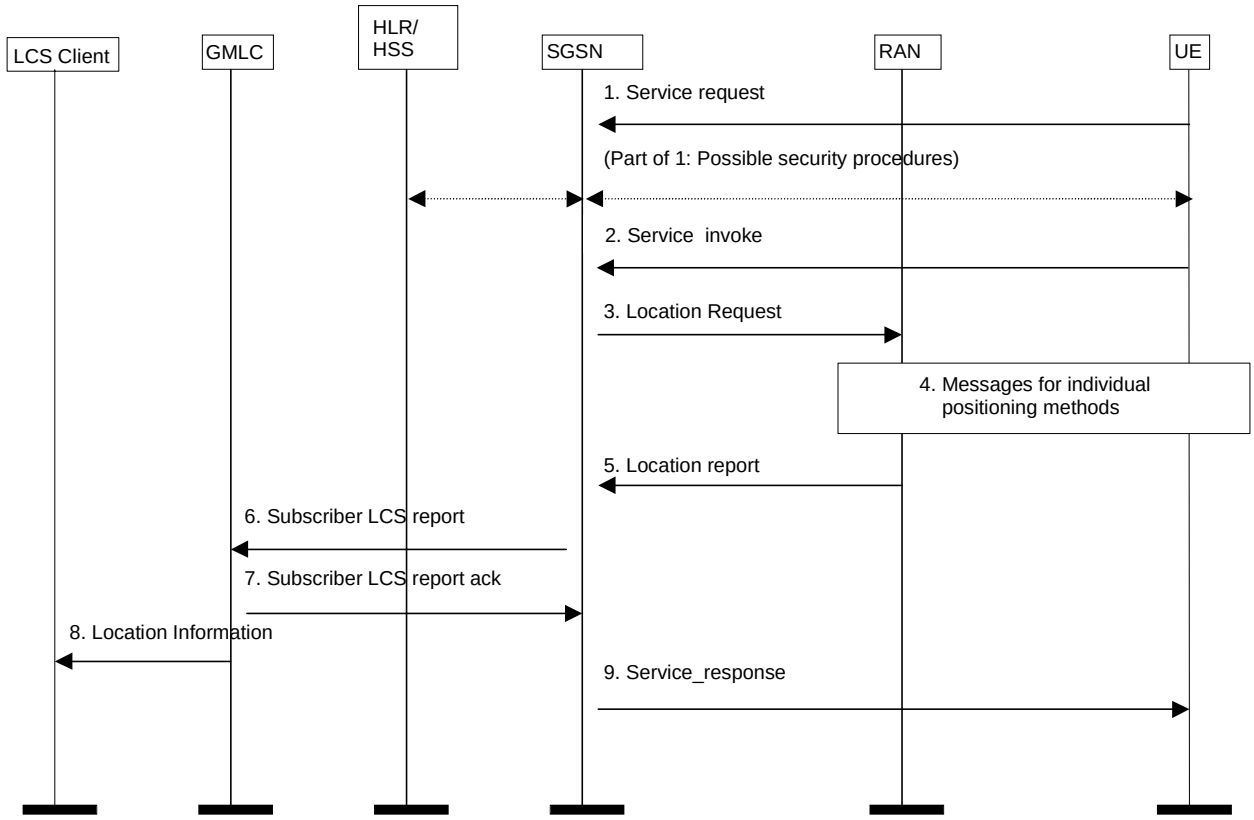


Figure 9.8: General Network Positioning for packet switched MO-LR

9.2.2.1 Location Preparation Procedure

1) In UMTS, if the UE is in idle mode, the UE requests a PS signaling connection and sends a Service request indicating signaling to the SGSN via the RAN. If the UE already has PS signaling connection, the UE does not need to send Service request. Security functions may be executed. These procedures are described in TS 23.060 [15]. In GSM this signaling step is not needed.

2) The mobile station sends a service invoke message to the SGSN. Different types of location services can be requested: location of the UE, location of the UE to be sent to another LCS client, location assistance data or ciphering keys. If the UE is requesting its own location or that its own location be sent to another LCS client, this message carries LCS requested QoS information (e.g. accuracy, response time). If the UE is requesting that its location be sent to another LCS client, the message shall include the identity of the LCS client and may include the address of the GMLC through which the LCS client should be accessed. If a GMLC address is not included, the SGSN may assign its own GMLC address and may verify that the identified LCS client is supported by this GMLC. If a GMLC address is not available for this case, the SGSN shall reject the location request. If the UE is instead requesting location assistance data or ciphering keys, the message specifies the type of assistance data or deciphering keys and the positioning method for which the assistance data or ciphering applies. The SGSN verifies the subscription profile of the UE and decides if the requested service is allowed or not.

3) The SGSN sends a Location Request message to the RAN associated with the Target UE's location. The message indicates whether a location estimate or location assistance data is requested. If the UE's location is requested, the message also includes the requested QoS. If location assistance data is requested, the message carries the requested types of location assistance data. The message carries also location parameters received in the Service Invoke message.

9.2.2.2 Positioning Measurement Establishment Procedure

4) If the UE is requesting its own location, the actions described in UTRAN Stage 2, TS 25.305 [1] or GERAN stage 2 TS 43.059 [16] are performed. If the UE is instead requesting location assistance data, the RAN transfers this data to the UE as described in subsequent clauses. The RAN determines the exact location assistance data to transfer according to the type of data specified by the UE, the UE location capabilities and the current cell.

9.2.2.3 Location Calculation and Release Procedure

5) When a location estimate best satisfying the requested QoS has been obtained or when the requested location assistance data has been transferred to the UE, the RAN returns a Location Report to the SGSN. This message carries the location estimate or ciphering keys if this was obtained. If a location estimate or deciphering keys were not successfully obtained or if the requested location assistance data could not be transferred successfully to the UE, a failure cause is included in the Location Report.

6) If the UE requested transfer of its location to another LCS client and a location estimate was successfully obtained, the SGSN shall send a Subscriber Location Report to the GMLC obtained in step 1 carrying the MSISDN or PDP address of the UE, the identity of the LCS client, the event causing the location estimate (MO-LR-PS) and the location estimate and its age.

7) The GMLC shall acknowledge receipt of the location estimate provided that it serves the identified LCS client and the client is accessible.

8) The GMLC transfers the location information to the LCS client either immediately or upon request from the client.

9) The SGSN returns a Service Response message to the UE carrying any location estimate requested by the UE, ciphering keys or a confirmation that a location estimate was successfully transferred to the GMLC serving an LCS client.

NOTE: Steps 3 - 9 may be repeated a number of times in case of periodic location request.

9.3 LCS signaling procedures specified in UTRAN and GERAN Stage 2

The signaling procedures in UTRAN and GERAN are defined in TS 25.305 [1] and TS 43.059 [16] respectively.

9.4 Exception Procedures

The procedures in this clause apply to all variants of an MT-LR, NI-LR and MO-LR where a Location Request message has been sent to RAN requesting some location service (e.g. provision of a location estimate for a target UE or transfer of assistance data to a target UE).

9.4.1 Procedures in the VMSC

After the VMSC has requested a location service for a particular UE from RAN, certain events may occur that may temporarily or permanently interfere with the location service attempt. For each such event notified to the VMSC, the VMSC shall employ one of the following error recovery actions.

Restart the Location Service

This action shall be employed for any event that temporarily impedes a location service attempt and cannot be delayed until the location service attempt is complete. When such an event is notified to the VMSC, it shall immediately cancel the location service attempt and the associated signaling dialogue with RAN, if this still exists by sending a "stop reporting" message to RAN. The "stop reporting" message shall contain the reason for the location procedure cancellation in case of GERAN in A/Gb mode or the indication about the type of location request to cancel (e.g. direct) in case of GERAN and UTRAN in Iu mode.

After aborting the location request dialogue with RAN, the VMSC may queue the location service request until the event causing the restart has terminated (if not already terminated). The VMSC may optionally wait for an additional time period (e.g. if the queuing delay is minimal) to ensure that any resources allocated in and by RAN have time to be released. The VMSC may then send another location service request to RAN associated with the target UE.

Abort the Location Service

This action shall be employed for any event that permanently impedes a location service attempt, such as loss of the dedicated signaling channel to the target UE. When such an event is notified to the VMSC, it shall cancel the current location service attempt and the associated signaling dialogue with RAN, if still existing, by sending a "stop reporting" message to RAN. The "stop reporting" message shall contain the reason for the location procedure cancellation in case of GERAN in A/Gb mode or the indication about the type of location request to cancel (e.g. direct) in case of GERAN and UTRAN in Iu mode. The VMSC shall then return an error response to the client or network entity from which the location request was originally received. The VMSC shall also release all resources specifically allocated for the location attempt.

The following table indicates the appropriate error recovery procedure for certain events. For events not listed in the table, the VMSC need take no action.

Table 9.1: LCS Error Recovery Procedures in the VMSC for certain Events

Event	VMSC Error Recovery
Release of radio channel to the UE	Abort
Any error response from RAN except for SRNC relocation or inter-MSC handover	Abort
In UMTS SRNC relocation	[Note: This is being discussed in RAN WG2 and RAN WG3.]
In GSM inter-MSC Handover and inter-BSC handover	Restart after handover completed

If the RNC is in an overload condition, it may reject a location request by indicating congestion. The MSC may reduce the frequency of future location service requests until rejection due to overload has ceased.

9.4.2 Procedures in the MSC Server

9.4.3 Procedures in the SGSN

After the SGSN has requested a location service for a particular UE from RAN, certain events may occur that may temporarily or permanently interfere with the location service attempt. For each such event notified to the SGSN, the SGSN shall employ one of the following error recovery actions.

Restart the Location Service

This action shall be employed for any event that temporarily impedes a location service attempt and cannot be delayed until the location service attempt is complete. When such an event is notified to the SGSN, it shall immediately cancel the location service attempt and the associated signaling dialogue with RAN, if this still exists by sending a "stop reporting" (Iu mode) or "location abort" (A/Gb mode) message to RAN. The "stop reporting"/"location abort" message shall contain the reason for the location procedure cancellation.

After aborting the location request dialogue with RAN, the SGSN may queue the location service request until the event causing the restart has terminated (if not already terminated). The SGSN may optionally wait for an additional time period (e.g. if the queuing delay is minimal) to ensure that any resources allocated in and by RAN have time to be released. The SGSN may then send another location service request to RAN associated with the target UE.

Abort the Location Service

This action shall be employed for any event that permanently impedes a location service attempt, such as loss of the radio channel to the target UE. When such an event is notified to the SGSN, it shall cancel the current location service attempt and the associated signaling dialogue with RAN, if still existing, by sending a "stop reporting"/"location abort" message to RAN. The "stop reporting"/"location abort" message shall contain the reason for the location procedure cancellation. The SGSN shall then return an error response to the client or network entity from which the location request was originally received. The SGSN shall also release all resources specifically allocated for the location attempt.

The following table indicates the appropriate error recovery procedure for certain events. For events not listed in the table, the SGSN need take no action.

Table 9.2: LCS Error Recovery Procedures in the SGSN for certain Events

Event	SGSN Error Recovery
Release of radio channel to the UE	Abort
Any error response from RAN causing unavailable signalling connections	Abort
SRNC relocation (Iu mode only)	[Note: This is being discussed in RAN WG2 and RAN WG3.]
Suspend of GPRS services (A/Gb mode only)(During CS connection for class B UE)	Abort
Intra SGSN Routing Area Update (A/Gb mode only)	Restart
Inter SGSN Routing Area Update	Abort (Note: GMLC may restart)
Standalone P-TMSI Reallocation (A/Gb mode only)	Restart

9.4.4 Procedures in the UE

9.4.5 Further Procedures for Handover

[Editor's note: During soft and softer handovers in WCDMA (inter Node-B, inter RNC) the existing RRC connection can be used with no need for aborting the on-going positioning process. In case of hard handovers, e.g. inter RNC hard handover (or SRNC relocation) and inter CN (MSC, SGSN) handovers the same approach can be followed as for any service connection (e.g. call handover). Therefore, aborting the service requests, including LCS request, because of handovers is not needed.
The exception procedures and error cases in UMTS need to be further studied.
It is currently being discussed between RAN WG2 and WG3 how to handle the LCS request during SRNC relocation.]

9.4.5.1 MSC procedure for Inter-MSC Handover

[When a location estimate is required for a target UE with an established call in a state of inter-MSC handover, the serving location area ID shall be used by the visited MSC to identify the correct RAN to perform the location. All Location request related messages that are transferred over the Iu-interface shall now be sent via MAP/E interface piggy-backed in MAP_FORWARD_ACCESS_SIGNALLING and MAP PROCESS_ACCESS_SIGNALLING between the visited and serving MSCs. The handling of LCS request during Inter-MSC handover in UMTS is FFS.]

9.4.5.2 Handling of an ongoing handover while a request for positioning arrives at MSC/VLR

[If during an ongoing radio handover procedure a request for location information arrives at RAN, the request shall be suspended until the handover is completed. On completion of the handover, RAN shall continue with location preparation procedure.]

9.5 Privacy

9.5.1 Privacy Override Indicator (POI)

The POI is used to determine whether the privacy settings of the subscriber to be positioned shall be overridden by the request for location services. The POI is applicable only to Emergency service and Lawful intercept service. The assignment of a POI value with an "override" or "not override" value in the LCS client profile is done during the LCS client provisioning. The type of LCS client requesting location information (i.e. emergency, law-enforcement etc.) shall determine the value of the POI assigned to the LCS client profile.

There are two distinct cases regarding the handling of the privacy override indicator.

Procedure A: If the subscriber to be positioned is in the same country as the GMLC or if the subscriber to be positioned is in a different country than the GMLC and an appropriate bilateral agreement exists between operators, then the POI shall override the subscriber's privacy options, as allowed by regulatory requirements.

Procedure B: Otherwise the POI shall not override the subscriber's privacy options.

9.5.2 Privacy Procedures

The SLPP shall contain the privacy options defined in the HLR of the UE subscriber.

The SLPP shall be downloaded to the VMSC, MSC Server and SGSN together with the rest of his subscription information in the existing operation INSERT_SUBSCRIBER_DATA. It will be deleted with the existing operation DELETE_SUBSCRIBER_DATA.

The POI is transferred from the GMLC to the VMSC/MSC Server/SGSN in the location request. Based on the location of the GMLC the VMSC/MSC Server/SGSN evaluates whether to accept or ignore the received POI according to the definition in clause.

If the POI is accepted the location requested is unconditionally performed. Otherwise if the POI is ignored the VMSC/MSC Server/SGSN evaluates the privacy options in the UE subscriber's subscription profile (assuming this is held in the VLR/MSC Server/SGSN). If the corresponding register does not contain the UE subscription profile, LCS will rely on the existing GSM recovery mechanisms to obtain the profile.

If more than one privacy class are subscribed, privacy class for an MT-LR is selected according to the rule described in the ANNEX A.

If the location request is allowed by the privacy options the location request is performed. Otherwise, if the location request is barred by the privacy options, the location request is refused an error response is returned to the GMLC with a cause code indicating that the request was rejected by the subscriber.

9.5.3 UE Privacy Options

The UE privacy options in the SLPP apply to an CS-MT-LR/PS-MT-LR or NI-LR/PS-NI-LR and either indicate that no CS-MT-LR/PS-MT-LR or NI-LR/PS-NI-LR is allowed for the UE (except as may be overridden by the POI or local regulatory requirements) or define the particular classes of LCS client for which an CS-MT-LR/PS-MT-LR or NI-LR/PS-NI-LR for location are allowed, with the following classes being possible:

[Editor's note: An e-mail comment pointed out that there are different cases still to be covered in the description of the classes: 1. the LCS Client identity is included in SLPP or 2. the LCS Client identity is NOT included in SLPP. Also some GMLC restriction conditions need to be mentioned.]

a) Universal Class - allow positioning by all LCS clients;

b) Call/Session related Class

c) Call/Session-unrelated Class

d) PLMN operator Class

Moreover the SLPP may contain the service types allowed by the subscriber.
All UE privacy options of above four classes are commonly used for both CS and PS domain.
Note: If a privacy option setting in a domain is updated, the same modification will be applied to the other domain.

9.5.3.1 The classes and corresponding subscription options are described below.Universal class

When the user of the UE subscribes to the "Universal Class" the CS-MT-LR/PS-MT-LR or NI-LR/PS-NI-LR positioning is allowed by all LCS clients.

If the UE subscribes to the universal class, any CS-MT-LR or NI-LR shall be allowed by the VMSC/MSC Server and any PS-MT-LR or PS-NI-LR shall be allowed by the SGSN. If local regulatory requirements mandate it, any MT-LR for an emergency services LCS client and any NI-LR for an emergency services call origination shall be allowed by the VMSC/MSC Server.

9.5.3.2 Call/Session related class

When the user of the UE subscribes to the "Call/Session related Class" the CS-MT-LR/PS-MT-LR or NI-LR/PS-NI-LR positioning is allowed in the following cases:

Allow positioning by specific identified value added LCS client or groups of value added LCS Client to which the UE originated a call in CS domain or a value added LCS client with which the UE has a session via an active PDP context in PS domain indicated by a specific APN-NI. For all clients in the call related class, OR For each identified LCS client or group of LCS Clients, one of the following subscription options shall apply:

* location request allowed only from GMLCs identified in the SLPP;
* location request allowed only from a GMLC in the home country;
* location request allowed from any GMLC (default case).

For each identified value added LCS client or group of LCS Clients in the privacy exception list, one of the following subscription options shall apply:

* 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.

For all value added LCS clients sending a call related CS-MT-LR/PS-MT-LR that are not identified in the privacy exception list, one of the following subscription option shall apply:

* 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.

NOTE 2: The usage of Call/Session related Class in the IM subsystem is FFS.

9.5.3.2.1 Call/session-related class in the CS-domain

If the UE subscribes to the call/session-related class, an CS-MT-LR may be allowed if both of following conditions are met:

- The UE previously originated a call in CS domain that is still established and the called party number dialled by the UE matches the called party number received from the GMLC.
- The identity of the LCS client or LCS client group supplied by the GMLC matches the identity of any LCS Client or LCS Client group contained in the UE's SLPP and any other GMLC restrictions associated with this LCS Client identity in the SLPP are also met

If these conditions are satisfied, the CS-MT-LR shall be allowed if the UE user subscribes to either location without notification or location with notification. If the UE user subscribes to location with notification and privacy verification, the CS-MT-LR shall be allowed following notification to the UE if the UE user either returns a response indicating that location is allowed or returns no response but subscribes to allowing location in the absence of a response. In all other cases, the CS-MT-LR shall be restricted.

9.5.3.2.2 Call/session-related class in the PS-domain

If the UE subscribes to the call/session-related class, a PS-MT-LR may be allowed if all of the following conditions are met:

- The UE previously originated a PDP-context towards the network where the external client is located and that this context is still established
- The APN-NI negotiated between the UE and SGSN matches the APN-NI received from the GMLC.
- The identity of the LCS client or LCS client group supplied by the GMLC matches the identity of any LCS Client or LCS Client group contained in the UE's SLPP and any other GMLC restrictions associated with this LCS Client identity in the SLPP are also met

If these conditions are satisfied, the PS-MT-LR shall be allowed if the UE user subscribes to either location without notification or location with notification. If the UE user subscribes to location with notification and privacy verification, the PS-MT-LR shall be allowed following notification to the UE if the UE user either returns a response indicating that location is allowed or returns no response but subscribes to allowing location in the absence of a response. In all other cases, the PS-MT-LR shall be restricted.

9.5.3.2.3 Call/session-related class when LCS client not in SLPP

If the UE subscribes to the call/session related class, a CS-MT-LR or PS-MT-LR from an LCS client that is NOT contained in the SLPP of the target UE shall be allowed or restricted according to the following conditions:

- For any non-matched LCS client, the CS-MT-LR or PS-MT-LR shall be allowed, if the UE user subscribes to either location without notification or location with notification.

If the UE user subscribes to location with notification and privacy verification, the CS-MT-LR or PS-MT-LR shall be allowed following notification to the UE if the UE user either returns a response indicating that location is allowed or returns no response but subscribes to location in the absence of a response. In all other cases, the CS-MT-LR or PS-MT-LR shall be restricted.

9.5.3.3 Call/Session-unrelated class

When the user of the UE subscribes to the "Call/Session unrelated Class" the CS-MT-LR/PS-MT-LR or NI-LR/PS-NI-LR positioning is allowed in the following cases:

Allow positioning by specific identified value added LCS Clients or groups of value added LCS Client with the following restrictions allowed for each identified value added LCS Client or group of value added LCS Clients:

* location request allowed only from GMLCs identified in the SLPP;
* location request allowed only from a GMLC in the home country;
* location request allowed from any GMLC (default case).

For each identified value added LCS client in the privacy exception list, one of the following subscription options shall apply:

* 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.

For all value added LCS clients sending a non-call related CS-MT-LR/PS-MT-LR that are not identified in the privacy exception list, one of the following subscription option shall apply:

* positioning not allowed (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.

9.5.3.3.1 Call/session-unrelated class when LCS client identities match

If the UE subscribes to the call/session-unrelated class, an CS-MT-LR/PS-MT-LR may be allowed by the MSC/MSC server or SGSN if the identity of the LCS client or LCS client group supplied by the GMLC matches the identity of any LCS Client or LCS Client group contained in the UE's SLPP and any other GMLC restrictions associated with this LCS Client identity in the SLPP are also met.

If the LCS client is correctly matched in this way and any GMLC restrictions are satisfied, the CS-MT-LR/PS-MT-LR shall be allowed if the UE user subscribes to either location without notification or location with notification. If the UE user subscribes to location with notification and privacy verification, the CS-MT-LR/PS-MT-LR shall be allowed following notification to the UE if the UE user either returns a response indicating that location is allowed or returns no response but subscribes to location in the absence of a response. In all other cases, the CS-MT-LR/PS-MT-LR shall be restricted.

9.5.3.3.2 Call/session-unrelated class when LCS client identities do not match

If the UE subscribes to the call/session-unrelated class, an CS-MT-LR/PS-MT-LR from an LCS client that is not contained in the UE's SLPP shall be allowed or restricted according to the following conditions. For any non-matched LCS client, the CS-MT-LR/PS-MT-LR shall be allowed if the UE user subscribes to location with notification. If the UE user subscribes to location with notification and privacy verification, the CS-MT-LR/PS-MT-LR shall be allowed following notification to the UE if the UE user either returns a response indicating that location is allowed or returns no response but subscribes to location in the absence of a response. In all other cases, the CS-MT-LR/PS-MT-LR shall be restricted.

9.5.3.4 PLMN operator class

When the user of the UE subscribes to the " PLMN operator Class" the CS-MT-LR/PS-MT-LR or NI-LR/PS-NI-LR positioning is allowed in the following cases:

Allow positioning by specific types of client within or associated with the VPLMN, with the following types of client identified:

* clients providing a location related broadcast service;
* O&M client in the HPLMN (when the UE is currently being served by the HPLMN);
* O&M client in the VPLMN;
* clients recording anonymous location information without any UE identifier;
* clients enhancing or supporting any supplementary service, IN service, bearer service or teleservice subscribed to by the target UE subscriber.

If the UE subscribes to the PLMN class, an NI-LR/PS-NI-LR or CS-MT-LR/PS-MT-LR shall be allowed if the client within the VPLMN, for an NI-LR/PS-NI-LR, or the client identified by the GMLC, for an CS-MT-LR/PS-MT-LR, either matches a generic type of client contained in the UE's SLPP or is otherwise authorized by local regulatory requirements to locate the UE.

9.5.3.5 Service type checking

If the SLPP contains service types, an CS-MT-LR/PS-MT-LR may be allowed by the MSC/MSC server or SGSN if the service type supplied by the GMLC matches the identity of any service type contained in the UE's SLPP and any other GMLC restrictions associated with this service type in the SLPP are also met.

If the service type is correctly matched in this way and any GMLC restrictions are satisfied, the CS-MT-LR/PS-MT-LR shall be allowed if the UE user subscribes to either location without notification or location with notification. If the UE user subscribes to location with notification and privacy verification, the CS-MT-LR/PS-MT-LR shall be allowed following notification to the UE if the UE user either returns a response indicating that location is allowed or returns no response but subscribes to location in the absence of a response. In all other cases, the CS-MT-LR/PS-MT-LR shall be restricted.

9.5.3.6 Matching of LCS client identities

In evaluating privacy where any address "A" associated with the LCS client (e.g. LCS client ID or GMLC address) needs to be compared with a corresponding address "B" in the target UE's SLPP, a match shall be determined if a match is found for each of the following components of each address:

a) numbering plan;

b) nature of address indicator;

c) corresponding address digits for all digits in "B" (the digits or initial digits in "A" must match all the digits in "B", but "A" may contain additional digits beyond those in "B").

All addresses shall be transferred to the MSC/VLR, MSC server or SGSN in international format, except for the called party number received from the GMLC during a Call-Related CS MT-LR when the LCS client was reached via IN or abbreviated number routing (e.g. toll-free number or emergency call routing). In these cases it is up to the GMLC to use the valid national specific number of the visited country.

In evaluating privacy where an APN-NI associated with the LCS client notified by the GMLC needs to be compared with a corresponding APN-NI that is used to set up the associated PDP context, a match shall be determined if a match is found for each component of APN-NI.

9.6 Mobile Originating Location

An UE may subscribe to any of the following classes of mobile originating location:

a) Basic Self Location;

b) Autonomous Self Location;

c) Transfer to Third Party.

An MO-LR shall be allowed by the VMSC if the type of request is supported by the appropriate subscription according to the following table.

Table 9.3: Required UE Subscription Options for MO-LR Requests

Type of MO-LR Request	Required UE Subscription
UE requests own location	Basic Self Location
UE requests location assistance data	Autonomous Self Location
UE requests transfer of own location to another LCS Client	Transfer to Third Party

9.7 CM Procedures

9.7.1 Location request for a mobile in idle-mode

When a request for location information is received at the VMSC the LCS-layer shall order paging of the UE subscriber. In case of first unsuccessful paging, normal paging procedures should apply. After successful paging the LCS-layer shall invoke the location preparation procedure.

9.7.2 Location request for a mobile in dedicated-mode

When a request for location information is received at the VMSC, if the UE is already busy on CM level, the LCS-layer shall attempt to establish a parallel transaction to the existing one. If successful, the LCS-layer shall invoke the location preparation procedure.

10 Information storage

This clause describes information storage structures that are mandatory (M), conditional (C) or optional (O) for LCS, and the recovery and restoration procedures needed to maintain service if inconsistencies in databases occur and for lost or invalid database information. Information storage in RAN network elements is specified in UTRAN Stage 2 (TS 25.305 [1]) and GERAN Stage 2 (TS 43.059 [16]) specifications.

10.1 HLR and HSS

The HLR/HSS holds LCS data for both UE subscribers and LMUs.

10.1.1 LCS Data in the HLR/HSS for an UE Subscriber

The IMSI is the primary key for LCS UE subscription data in the HLR/HSS. This subscription data may be stored in a Multiple Subscriber Profile (MSP), with the HLR/HSS able to hold a number of MSPs per IMSI.

The HLR may store a list of codewords given by the UE subscriber, to be provided by the LCS client in order not to get the location request rejected.
LCS UE subscription data includes a privacy exception list containing the privacy classes for which location of the target UE is permitted. Each privacy class is treated as a distinct supplementary service with its own supplementary service code. The following logical states are applicable to each privacy class (refer to TS 23.011 [22] for an explanation of the notation).

Table 10.1: Logical States for each LCS Privacy Class

Provisioning State	Registration State	Activation State	HLR Induction State
(Not Provisioned,	Not Applicable,	Not Active,	Not Induced)
(Provisioned,	Not Applicable,	Active and Operative,	Not Induced)

For each LCS privacy class, the HLR/HSS shall store the logical state of the class on a per-subscriber (or per subscriber MSP) basis. In addition, the permanent data indicated below shall be stored on a per subscriber (or per subscriber MSP) basis when the logical provisioning state of the associated LCS privacy class is "provisioned". For the meaning of each LCS privacy class, refer to clause 9 and to TS 22.071 [4].
Moreover a list of allowed service types may be stored. The meaning of service types is defined in TS 22.071 [4].

Table 10.2: LCS data stored in the HLR privacy exception list for an UE Subscriber (or UE Subscriber MSP)

LCS Privacy Class	Status	Additional HLR Data when Class is provisioned
Universal Class	-	No additional data
Call/session Related Class	M	Indication of one of the following mutually exclusive options for any LCS client not in the external LCS client list: • Location not allowed • Location allowed without notification (default case) • Location allowed with notification • Location with notification and privacy verification; location allowed if no response • Location with notification and privacy verification; location restricted if no response
	O C O C	External LCS client list: a list of zero or more LCS clients, with the following data stored for each LCS client in the list: • International E.164 address identifying a single LCS client or a single group of LCS clients that are permitted to locate this target UE • Restriction on the GMLC. Possible values are: - Identified GMLCs only - Any GMLC in the home country • Indication of one of the following mutually exclusive options: - Location allowed without notification (default case) - Location allowed with notification - Location with notification and privacy verification; location allowed if no response - Location with notification and privacy verification; location restricted if no response
Call/session Unrelated Class	M	Indication of one of the following mutually exclusive options for any LCS client not in the external LCS client list: • Location not allowed (default case) • Location allowed with notification • Location with notification and privacy verification; location allowed if no response • Location with notification and privacy verification; location restricted if no response
	O C O C	External LCS client list: a list of zero or more LCS clients, with the following data stored for each LCS client in the list: • International E.164 address identifying a single LCS client or a single group of LCS clients that are permitted to locate this target UE • Restriction on the GMLC. Possible values are: - Identified GMLCs only - Any GMLC in the home country • Indication of one of the following mutually exclusive options: - Location allowed without notification (default case) - Location allowed with notification - Location with notification and privacy verification; location allowed if no response - Location with notification and privacy verification; location restricted if no response
PLMN Operator Class	O	LCS client list: a list of one or more generic classes of LCS client that are allowed to locate the particular UE. The following classes are distinguished: • LCS client broadcasting location related information • O&M LCS client in the HPLMN • O&M LCS client in the VPLMN • LCS client recording anonymous location information • LCS Client supporting a bearer service, teleservice or supplementary service to the target UE

Table 10.3: LCS Service types stored in the HLR/HSS per UE subscriber

Service type indication	Status	Additional HLR data when the indication is stored
Service Types	O	Indication of one of the following mutually exclusive options for any service type not in the service type list: • Location not allowed (default case) • Location allowed with notification • Location with notification and privacy verification; location allowed if no response • Location with notification and privacy verification; location restricted if no response Service types list: a list of one or more service types for which the LCS client is allowed to locate the particular UE. The possible service types are defined in 22.071. • Restriction on the GMLC. Possible values are: - Identified GMLCs only - Any GMLC in the home country • Indication of one of the following mutually exclusive options: - Location allowed without notification (default case) - Location allowed with notification - Location with notification and privacy verification; location allowed if no response Location with notification and privacy verification; location restricted if no response

LCS UE subscription data may include a mobile originating list containing the LCS mobile originating classes that an UE is permitted to request. Each LCS mobile originating class is treated as a distinct supplementary service with its own supplementary service code. The following logical states are applicable to each mobile originating class (refer to TS 23.011 [22] for an explanation of the notation).

Table 10.4: Logical States for each Mobile Originating LCS Class

Provisioning State	Registration State	Activation State	HLR Induction State
(Not Provisioned,	Not Applicable,	Not Active,	Not Induced)
(Provisioned,	Not Applicable,	Active and Operative,	Not Induced)

For each LCS Mobile Originating class, the HLR/HSS shall store the logical state of the class on a per-subscriber (or per subscriber MSP) basis. In this version of LCS, there is no additional permanent data in the HLR. The table below shows the defined mobile originating classes. For the meaning of each LCS mobile originating class, refer to clause 8 and to TS 22.071 [4].

Table 10.5: Data stored in the HLR for the LCS Mobile Originating List for an UE (or UE Subscriber MSP)

LCS Mobile Originating Class	Status	Additional HLR Data when Class is provisioned
Basic Self Location	-	No additional data
Autonomous Self Location	-	No additional data
Transfer to Third Party	-	No additional data

In addition to the privacy exception list, the following other data itemsmay be stored in the UE subscription profile in the HLR to support LCS.

Table 10.6: Temporary LCS data in the HLR

Other Data in the HLR	Status	Description
GMLC List	O	List of one or more E.164 addresses of the GMLCs from which a location request for an MT-LR is allowed, The addresses are only relevant to an LCS client that is restricted (in the UE privacy exception list) to making call/session related or call/session unrelated location requests.

10.2 VLR

The VLR contains the same LCS permanent data for each registered UE subscriber, as does the HLR/HSS. This data is downloaded to the VLR as part of the location update procedure between the VLR and HLR/HSS for an UE subscriber.

10.3 GMLC

The GMLC holds data for a set of external LCS clients that may make call related or non-call related CS-MT-LR/PS-MT-LR requests to this GMLC. The permanent data administered for each LCS client is as follows.

Table10.7: GMLC Permanent Data for a LCS Client

LCS Client data in GMLC	Status	Description
LCS Client Type	M	Identifies the type LCS client from among the following: - Emergency Services - Value Added Services - PLMN Operator Services - Lawful Intercept Services
External identity	O	A list of one or more identifiers used to identify an external LCS client. The identity may be used when making an MT-LR and/or MO-LR. The format of the identity is international E.164 addresses. Each external identity shall be associated with a logical client name.
Authentication data	M	Data employed to authenticate the identity of an LCS client – details are outside the scope of the present document
Call/session related identity	O	A list of one or more international E.164 addresses, which are used to make calls by mobile subscribers, or APN-NIs (see NOTE) to identify the client for a call related MT-LR In case the LCS client was reached via IN or abbreviated number routing (e.g. toll free number or emergency call routing), the E.164 number(s) stored in the GMLC shall be the number(s) that the UE has to dial to reach the LCS Client. In these cases the E.164 number is not to be in international format. The country in which the national specific number(s) is (are) applicable is (are) also stored (or implied) in this case. Each call related identity may be associated with a specific external identity. Each call/session-related identity shall be associated with a logical client name.
Internal identity	O	Identifies the type PLMN operator services and the following classes are distinguished: - LCS client broadcasting location related information - O&M LCS client in the HPLMN - O&M LCS client in the VPLMN - LCS client recording anonymous location information - LCS Client supporting a bearer service, teleservice or supplementary service to the target UE This identity is applicable only to PLMN Operator Services.
Client name	O	An address string which is a logical name associated with LCS client's external identity (i.e., E.164 address).
Override capability	O	Indication of whether the LCS client possesses the override capability (not applicable to a value added and PLMN operator service)
Authorized UE List	O	A list of MSISDNs or groups of MSISDN for which the LCS client may issue a non-call related MT-LR. Separate lists of MSISDNs and groups of MSISDN may be associated with each distinct external or non-call related client identity.
Priority	M	The priority of the LCS client – to be treated as either the default priority when priority is not negotiated between the LCS server and client or the highest allowed priority when priority is negotiated
QoS parameters	M	The default QoS requirements for the LCS client, comprising: - Accuracy - Response time Separate default QoS parameters may be maintained for each distinct LCS client identity (external, non-call related, call related)
Allowed LCS Request Types	M	Indicates which of the following are allowed: - Non-call related CS-MT-LR/PS-MT-LR - Call/session related CS-MT-LR/PS-MT-LR - Specification or negotiation of priority - Specification or negotiation of QoS parameters - Request of current location - Request of current or last known location
Local Co-ordinate System	O	Definition of the co-ordinate system(s) in which a location estimate shall be provided – details are outside the scope of the present document
Access Barring List(s)	O	List(s) of MSISDNs or groups of MSISDN for which a location request is barred
Service Identities	O	List of service identities allowed for the LCS client.

NOTE: The LCS Client is identified with E.164 number or APN-NI. APN-NI is specified in TS 23.003.

10.4 Recovery and Restoration Procedures

The LCS recovery and restoration procedures allow temporary data to be recovered or reinitialized following loss or corruption of data, such that normal LCS service is rapidly restored and inconsistency between the data held by different LCS network elements is removed. For a full description, refer to TS 23.007 [23].

10.5 Interworking with pre-Rel'4 LCS

This clause describes possible scenarios for interworking with a node which support only pre-Rel'4 LCS features and functions.

10.5.1 Interworking with the VLR supporting only pre-Rel'4 LCS

The VLR that supports only pre-Rel'4 LCS cannot handle the extended privacy control for call-related/call-unrelated class of the Rel'4 LCS. That is, the VLR cannot provide the extended call-related/call-unrelated class service to the user who subscribes to the Rel'4 LCS. Therefore HLR/HSS does not send the subscriber data on call-related/call-unrelated class for users who subscribe to the call-related class of Rel'4 LCS to the VLR that supports only pre-Rel'4 LCS. The HLR/HSS is notified whether the VLR supports Rel'4 LCS or not by an indication , which indicates all the LCS core network signalling capabilities the VLR supports, from the VLR during location update procedure. The following LCS core network signalling capabilities are identified in the current version of this specification.

- LCS core network signalling capability set 1: R98 and R99 LCS (pre-Rel'4 LCS)
- LCS core network signalling capability set 2: Rel'4 or later LCS (no Enhanced User Privacy support)
- LCS core network signalling capability set 3: Rel'5 or later LCS (with Enhanced User Privacy support)

The serving node, which notified the HLR/HSS that it supports LCS core network signalling capability set 2, shall be able to handle the extended LCS Client list and LCS Client List for call-related class from the HLR. A Rel'5 serving node without support for Enhanced User Privacy shall also indicate LCS core network signalling capability set 2.

The serving node, which notified the HLR/HSS that it supports LCS core network signalling capability set 3 shall be able to handle the Enhanced User Privacy mechanisms, as foreseen for rel-5. If the HLR/HSS is notified that the LCS capability set 3 is not supported, it may decide to not send the LCS subscriber data to the VLR, in order to protect user privacy.

[Note: this interworking scenario can be also applied for PS domain. Generalization of the description in this sub clause to cover both CS and PS domain should be done.][Note2: the concept of LCS capability set is newly introduced in Rel4 so that it doesn't appear in the specifications for R98 and R99 LCS]

11 Operational Aspects

11.1 Charging

Charging Information collected by the PLMN serving the LCS Client.

The following charging information shall be collected by the PLMN serving the LCS Client:

- type and identity of the LCS Client;
- identity of the target UE;
- results (e.g. success/failure, method used if known, response time, accuracy) - to be repeated for each instance of positioning for a deferred location request;
- identity of the visited PLMN;
- LCS request type (i.e. LDR or LIR);

- state;
- event (applicable to LDR requests only);
- time stamp;
- type of co-ordinate system used.

11.2 Charging Information Collected by the Visited PLMN

The following charging information shall be collected by the visited PLMN:

- tate and time;
- type and identity of the LCS Client (if known);
- identity of the target UE;
- location of the target UE (e.g., MSC, MSC Server, SGSN, location area ID, cell ID, location co-ordinates);
- which location services were requested;
- results (e.g. success/failure, positioning method used, response time, accuracy) - to be repeated for each instance of positioning for a batch location request;
- identity of the GMLC or PLMN serving the LCS Client;
- state;
- event (applicable to LDR requests only).

Annex A (normative): Privacy Class selection rule

If more than one privacy class are subscribed, privacy class for an MT-LR is selected according to the following flow diagram.

An MT-LR may be applied to more than one privacy class. In this case, looser privacy setting shall be selected. All possible privacy setting values are listed in the table below. The privacy settings to be compared are the results of the privacy checks for each applicable class. The interrelation among each privacy setting in terms of privacy strictness is shown as follows:

loose	Positioning allowed without notifying the UE user
↑	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
strict	Positioning not allowed

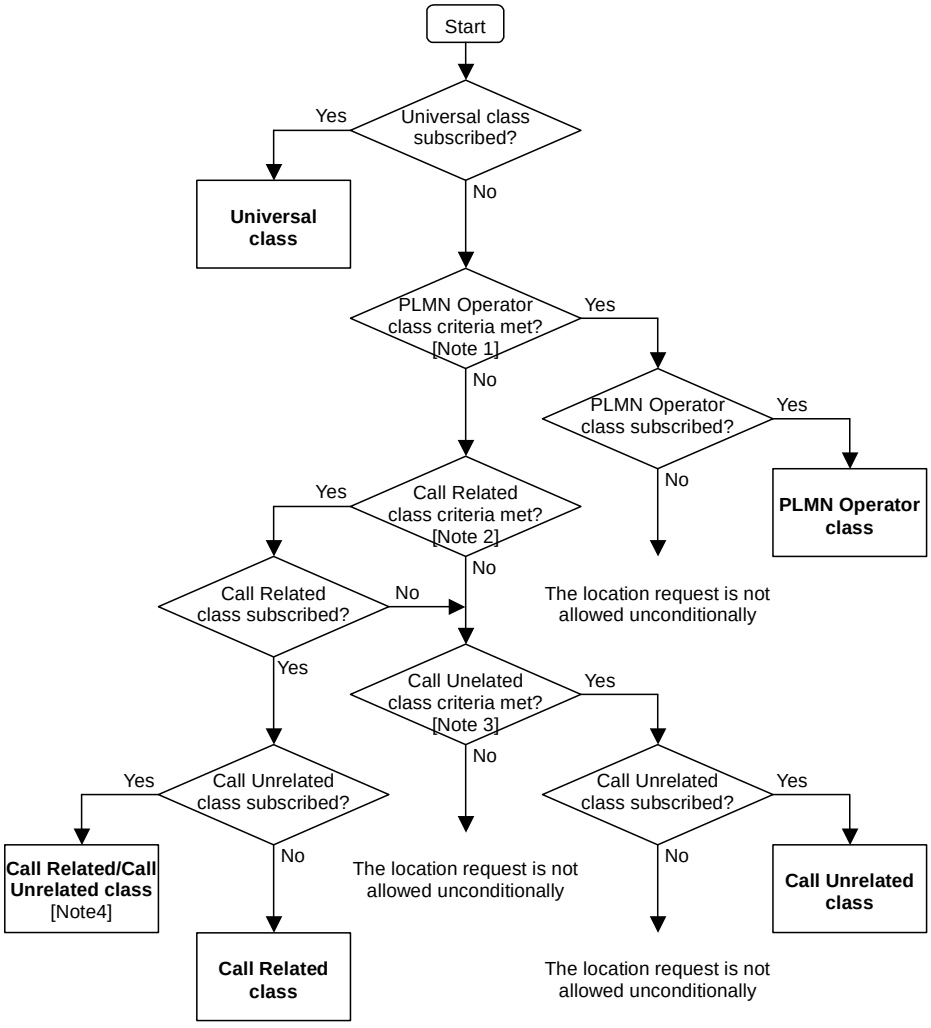


Figure A.1: Privacy Class selection flow diagram

Note 1: The client type indicates PLMN Operator service, and the client is within or associated with the VPLMN.
Note 2: The client type indicates value added service, and the Dialled by UE is available and matched with a call/session established.
Note 3: The client type indicates value added service.
Note 4: The looser privacy setting shall be selected.

Annex B (normative): Presence of LCS client ID Components in MT-LR

The LCS client identity is composed of one or more than one of the following components: LCS client type, external identity, internal identity, call/session related identity, APN-NI, client name and Requestor Identity. The LCS client type shall always be present and for each LCS client type the presence of the other components are defined as follows:

Component LCS Client type	External identity	Internal identity	Call/session related identity	Client name	Requestor Identity
Emergency	O	N.A.	N.A.	N.A.	N.A.
Value added	M	N.A.	O [Note]	M	O
PLMN operator	N.A.	M	N.A.	N.A.	N.A.
Lawful Intercept	N.A.	N.A.	N.A.	N.A.	N.A.

Note: This component shall be present if the MT-LR is associated to either CS call or PS session. If the MT-LR is associated with the CS call, the number dialled by UE is used. Otherwise if the MT-LR is associated with the PS session, the APN-NI is used.

Annex C:
(void)

(void)

Annex D (informative): Change history

Date	Version	Comment
September 2000	1.0.0	Presented for information to SA#9.
21.11.00	1.1.0	Changes and additions from LCS drafting group 16.11.00, sent out for S2 e-mail approval
4.12.00	1.2.0	S2 e-mail comments received before 4.12.00 included
10.12.00	2.0.0	For approval at SA#10. Same content as v.1.2.0
31.01.01	4.0.0	Cleaning up of v.2.0.0. Same technical content as in 2.0.0.
05.04.01	4.1.0	CRs approved at TSG SA Plenary #11 in March 2001 included
30.06.01	4.2.0	CRs approved at TSG SA Plenary #12 in June 2001 included (SP-010371)

Document history		
5.0.0	October 2001	Created from v.4.3.0 + CR approved at TSG SA#13: 035rev1 Release 5 alignment of 23.271 with GERAN LCS stage 2, TS 43.059
5.1.0	December 2001	CRs approved at TSG SA Plenary #14 in December 2001 included: 038r1 LCS Capability Handling for GPRS MS's 042r1 Removal of PDP address from HLR/HSS in the MT-LR procedure 044 Response to LCS client in case of deferred MT-LR 049r1 SGSN Exception procedures 051r1 Correction of referred signaling step in MO-Location Request 055 Editorial correction to front page
5.2.0	March 2002	CRs approved at TSG SA Plenary #15 in March 2002: 057 Supported LCS capabilities sets 059r3 Clarification of OSA support for LCS in TS23.271 061r1 Requestor and Requestor Identity 062r1 Combined Periodical/Deferred Mobile Terminating Location Request 064 Essential correction for session related class 065r2 Adding references to the LIF MLP specification for the Le interface 069r1 Handling of service type and codeword 071r1 Handling of privacy override indicator 072r2 Correction of information flows LCS client – GMLC 077r1 Removal of NA-ESRK from MT-LR request for North American Emergency call

3GPP TR 23.871

V2~~1~~.0.0 (2002-

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 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' 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".~~

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 that~~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
- Functional~~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~~n~~ functional entity containing a ~~that performs privacy check based on policies specified in a~~ database with~~containing~~ subscriber privacy information for location services and functionality to perform the related privacy checks. Note: the PPR is used in the architectural alternatives described in sect. 7.1 and 7.2.

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 LCS Server maps the services indicated by an LCS Client into a Service Type as specified in TS 22.071. ~~[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

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 MSC. The visited MSC~~/VLR~~ or SGSN maps the received LCS client ID to subscriber's Privacy parameters (e.g. list of allowed LCS clients) to screen out the 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' 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".~~

5. Functional Description and Functional Requirements ~~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 the user requests from this LCS client or which service the LCS client offers to the user.

~~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 requirements for service type privacy and the standardized service types are specified in TS 22.071 [1].

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

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 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-standardized 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 Information Services	Navigation	
	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.

TS 22.071 [1] specifies a~~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. 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 identity 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 identity could be the identity 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 [1] 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 is handled according to the national regulatory guidelines option~~ for LCS location services to protect UE against third party monitoring his/her location.

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 by the subscriber. 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 subscriber of the UE is responsible to distribute his/her codeword to such requestors, whom the subscriber has allowed to request his/her location. Once the codeword has been set and properly distributed, the subscriber 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 of the codeword to the requestors and registration of the codeword by the UE subscriber with the operator is outside the scope of 3GPP. The mechanisms to generate the codeword are not yet described in this Technical Report and it is for further study whether the mechanisms need to be standardized.

The codeword is applicable to the value added services only.

The codeword may be checked by the user of the UE or by the network.

TS 22.071 [1] specifies the service requirements for the codeword function.

5.7 ~~—~~Anonymity

For enhanced privacy the subscriber's true identity (MSISDN) can be hidden and replaced with an alias that is used as a permanent or temporary reference of the subscriber. As one solution the alias can be passed on from terminal to the LCS Client application when the subscriber invokes a request e.g. to a specific service type. As another solution some secured network proxy may allocate the anonymous ID (alias) to replace MSISDN. The LCS client will use alias as an identifier for the target subscriber instead of the true MSISDN identity. GMLC will in response use the same alias.
It should be possible to define both permanent and temporary alias.

The service requirements for anonymity are to be discussed and agreed in SA1 and specified in TS 22.071 [1].

5.8 Related privacy issues in Presence and Location services

Location information is an important part of the Presence information used in the Presence service. The subscriber should be able to set privacy requirements also for the location information used in the Presence service. Preferably the privacy settings and control mechanisms that the subscriber has defined for location services should be applicable as such also for the location information in Presence services.

Privacy settings for presence could possibly be shared with LCS, but it need further discussion is needed between presence and LCS people.

The relations between privacy issues in presence and in LCS should be discussed in SA1 and SA3.

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 (privacy profile register) 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 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.

6.1 Privacy profile register (PPR)

The PPR as used in the architectural alternatives of clause 7.1 and 7.2. contains a database with the subcribers privacy information and performs the related privacy checks and reports the result to the requesting entity.

It is FFS and dependent on the architectural alternative, if the PPR should also be used for mapping of the service identities exchanged between LCS client and GMLC to service types used for roaming scenarios.

It is FFS, if the PPR should be used for interoperations between LCS and other services, e.g. presence service.

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

In order to keep the compatibility with Rel-4 privacy functionality (notification/verification), the concept of “pseudo-external identity” is introduced. In the current stage 2 specification, the external identity is defined as the identity of external LCS client. The pseudo-external identity is not the identity of real external LCS client but the identity which is used for notifying SGSN/MSC of the location request class (call/session related or non-related) and the required type of indication for the target UE user. The pseudo-external identity shall be defined by each operator. Eight pseudo-external identities shall be defined according to the type of indication and the location request class (call/session related class or not). The eight pseudo-external identities are summarized in the table 1. Operator allocates E.164 addresses for the pseudo-external identities.

Table 1: Pseudo-external identities

Pseudo-external identity	location request class	type of indication
Pseudo-external identity 1	Call/Session related class	Location allowed without notification
Pseudo-external identity 2		Location allowed with notification
Pseudo-external identity 3		Location with notification and privacy verification; location allowed if no response
Pseudo-external identity 4		Location with notification and privacy verification; location restricted if no response
Pseudo-external identity 5	Call/Session non-related class	Location allowed without notification
Pseudo-external identity 6		Location allowed with notification
Pseudo-external identity 7		Location with notification and privacy verification; location allowed if no response
Pseudo-external identity 8		Location with notification and privacy verification; location restricted if no response

Note: More pseudo identities may be required.

The pseudo-external identities are registered in HLR/HSS as SLPP of each UE in advance.

When a GMLC receives a location request, the GMLC performs the privacy check, may be with PPR. In case negative result of the privacy check, the GMLC immediately returns the response back. In case positive result, in order to indicate SGSN/MSC which type of indication (notification/verification) is required for the location request, the GMLC selects a proper pseudo-external identity according to the privacy check result. Then the GMLC replaces the external identity to the selected pseudo-external identity. The original external identity may be included in the LCS client name field if the operator want to notify the UE of not only original LCS client name but also the original identity. Then the GMLC sends Provide Subscriber Location message to MSC/SGSN as specified in 23.271. The SGSN/MSC selects the type of behavior according to the SLPP of the target UE and the pseudo external identity.

With the pseudo-external identity, it is possible to enable the Rel-4 MSC/SGSN to behave according to the result of the enhanced privacy check mechanism without any modification of the Rel-4 SGSN/MSC. The pseudo-external identity also enables to handle the call/session related class.

Even in the case when the target UE wants to be protected by the enhanced privacy check mechanism and the original external identity is replaced by the pseudo-external identity, the target UE can receive the client name of the LCS client to identify the LCS client. In the case when the target UE does not want to be protected by the enhanced privacy check mechanism and the HSS stores the SLPP including the original external identity list, the original external identity is sent to the target UE as previous release.

Even with the pseudo-external identities shown above, the enhanced privacy parameters (i.e. Requestor ID, Codeword and Service Type) cannot be notified to the target UE, when the SGSN/MSC is Rel-4.

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 database, 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.

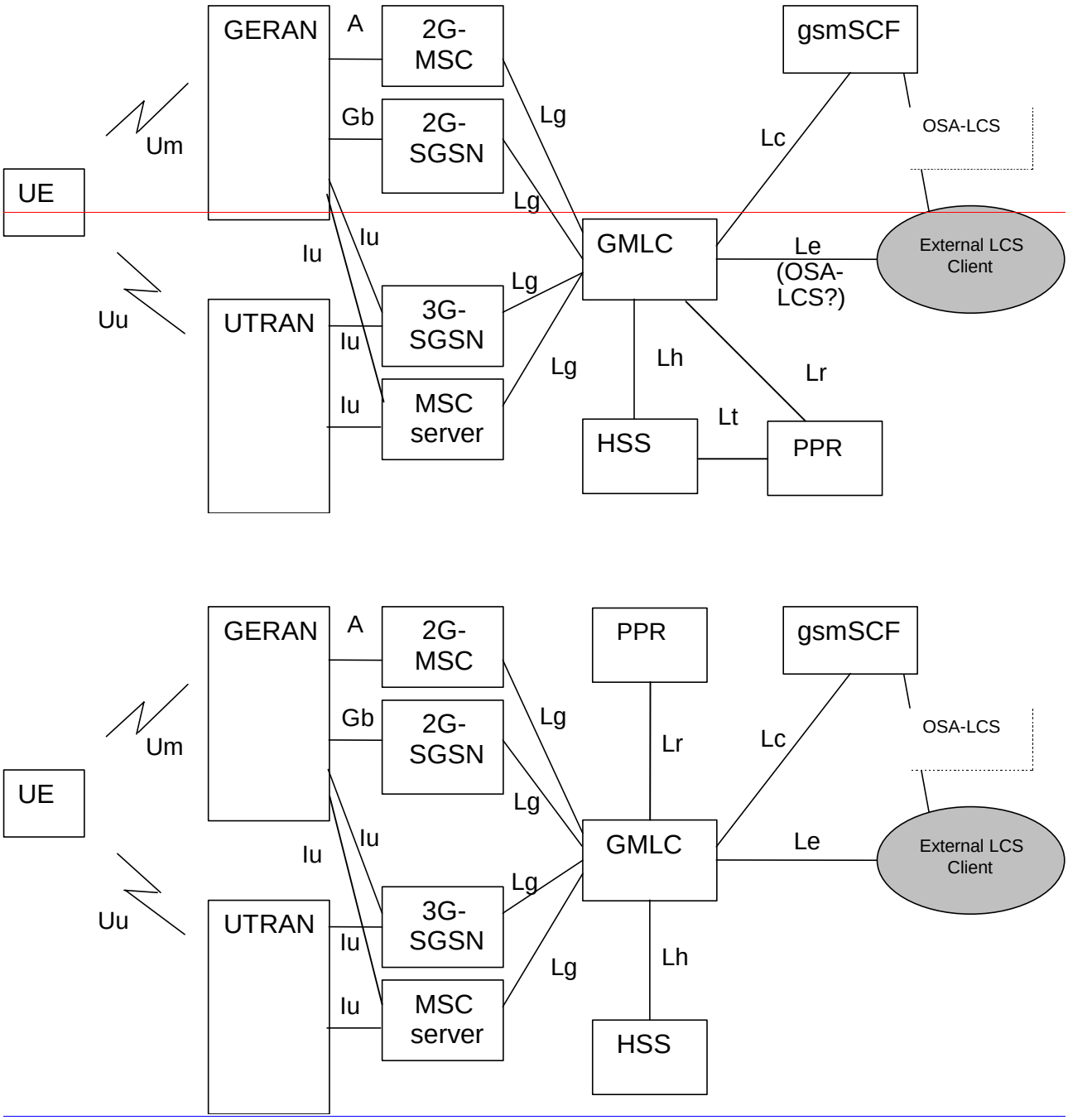


Figure 7.1.1; *LCS architecture alternative with PPR attached to GMLC*

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, (e.g. ~~i.e.~~ the 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 described ~~proposed~~ in this TR) may lead to different results

GMLC sends the privacy check request to 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 whether~~is~~ the request is 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 TS 23.271, 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 checked~~done~~ in a single point that holds the ~~subscriber~~ subscriber's 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. This ~~at would~~ means that there is no need to send the location request further to MSC/SGSN This functionality hence~~would~~ reduces the MSC/SGSN and the Lg interface capacity load.

The~~To insure that there is no inconsistency between~~ privacy settings in HLR and PPR shall be consistent with the privacy settings in PPR, but this is seen as a network management issue outside the scope of this TR.~~, 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 the Lr interface it should inform~~send that information to~~ HLR about this in the SRI procedure. If HLR does not receive such~~that~~ information ~~is not received~~ it can anticipate ~~the home operator can then know~~ that the enhanced privacy check could not be handled. ~~and the~~ HLR can in this case select to reject the location request if necessary or send routing information to GMLC.~~could be rejected already by the HLR.~~

Note 1: SA3 will be asked to verify whether the preferred solution alternative is acceptable from security point of view.

Note 2: It should be defined in MSC/SGSN what is the level of trust that MSC/SGSN can apply for 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: GMLC includes in the privacy request to ~~The~~ PPR an indication~~could not identify~~ whether the Location request is call/session related or not. ~~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

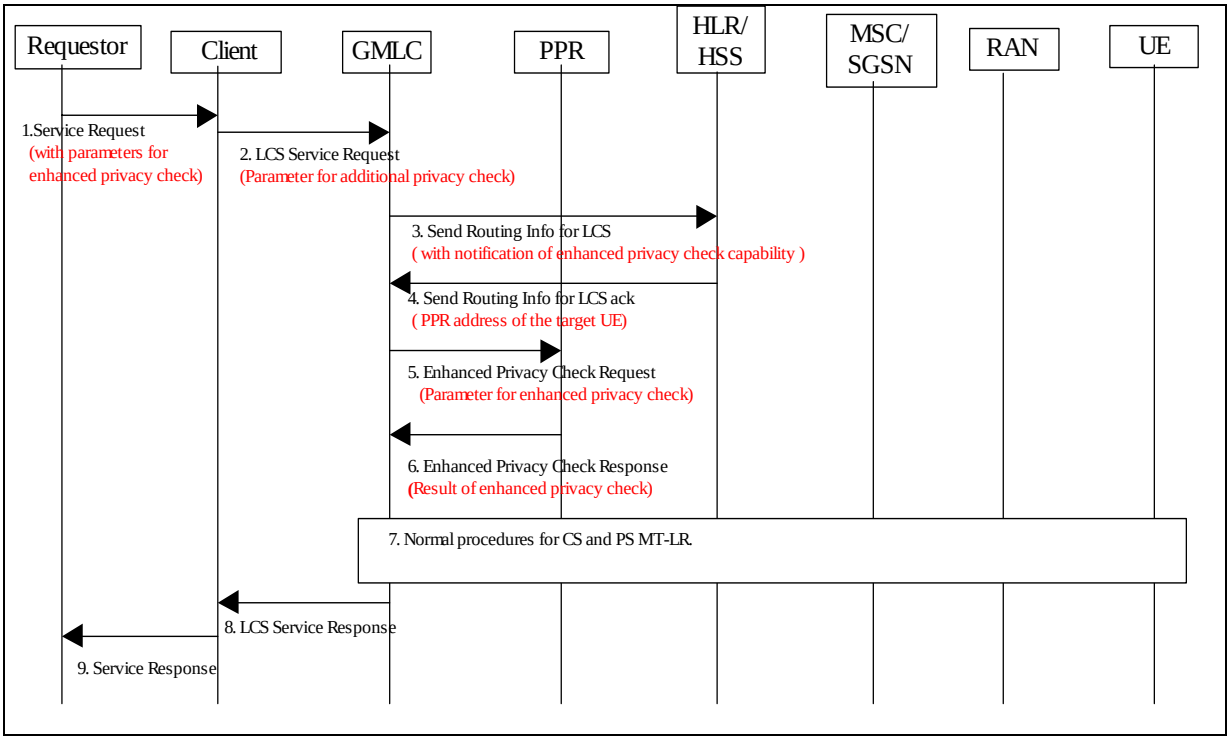


Figure 7.1.2~~1~~; *General information flow for the architectural alternative with the PPR attached to GMLC*

*Note 1. The Enhanced Privacy Check Request may contain the codeword and the service type.

*Note 2. The Requestor ID and the codeword shall be sent to the MSC/SGSN if they are wanted to be shown to the UE user in the LCS notification invoke procedure. Also the privacy check result shall be carried to the MSC/SGSN.

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 - call related/unrelated, PLMN operator - as well as the overall control of privacy checks - notification, verification, (emergency), privacy override - 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.

Determintation of a call or a session to a LCS client to which the UE has an active connection is done in the MSC or SGSN respectively. This information will be applied for the call/session related privacy checks in the SLPP of Rel-4 and the Rel-5 enhancements in PPR accordingly.

The notification and verification settings for the enhanced privacy check in the PPR are reported as result to MSC/SGSN, where the according procedures towards the UE are initialized.

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.

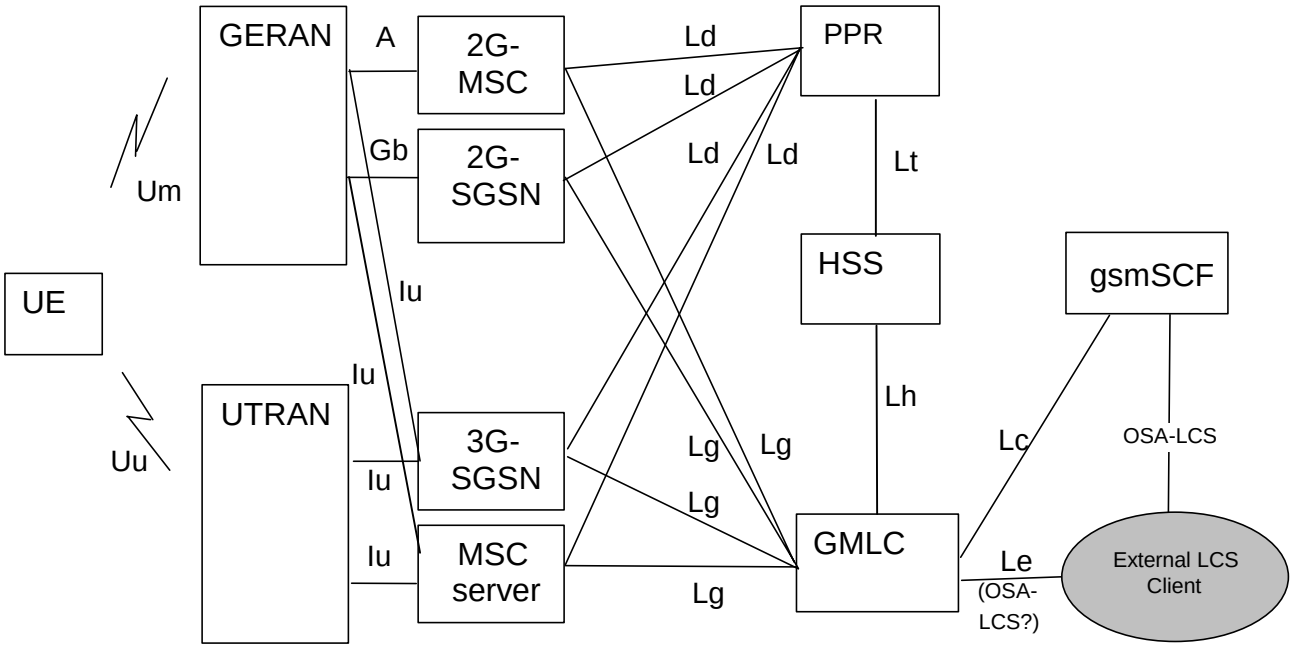


Figure 7.2.1; *LCS architecture alternative with PPR attached to MSC/SGSN*

7.2.2 Information Flow

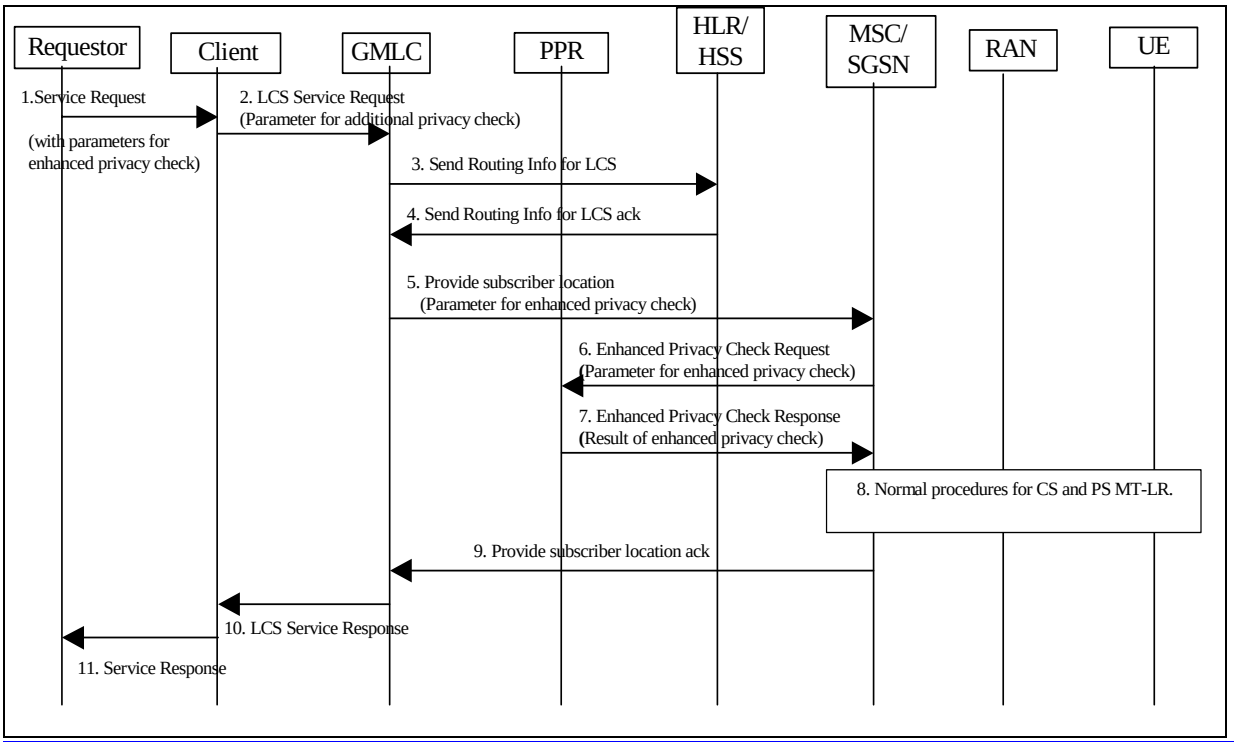


Figure 7.2.2; *General information flow for the architectural alternative with the PPR attached to MSC/SGSN*

7.2.3 Exceptional handling

The privacy settings for an active deferred MT-LR may have been changed while waiting for the event: For this, the MSC/SGSN shall access the PPR again, when the event is detected.

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, (originated~~l~~ 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 originated~~l~~ 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 selects a proper pseudo-external identity, according to the required type of indication and the LCS privacy class (call/session related class or non-related class) of the location request, and replaces the external identity to the appropriate pseudo-external identity. Then the Home GMLC sends Provide Subscriber Location message to MSC/SGSN as specified in 23.271. If the target UE user's privacy setting does not require the enhanced privacy check and the HSS stores the SLPP including the original external identity list, the Home GMLC does not replace the external identity and sends Provide Subscriber Location message with the original external identity. ~~and~~ The Home GMLC forwards the location report received from the SGSN/MSC to the originated~~l~~ GMLC. In case negative result of the

enhanced privacy check, the Home GMLC immediately returns the response back to the originated~~l~~ 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, which is held in Home GMLC of the UE, is changed, the 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 may hold~~s only~~ both of the enhanced privacy settings and Rel-4 privacy setting.. ~~The legacy~~Rel-4 privacy check in SGSN/MSC is performed as in the previous releases in order to decide the type of indication for the target UE.

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.

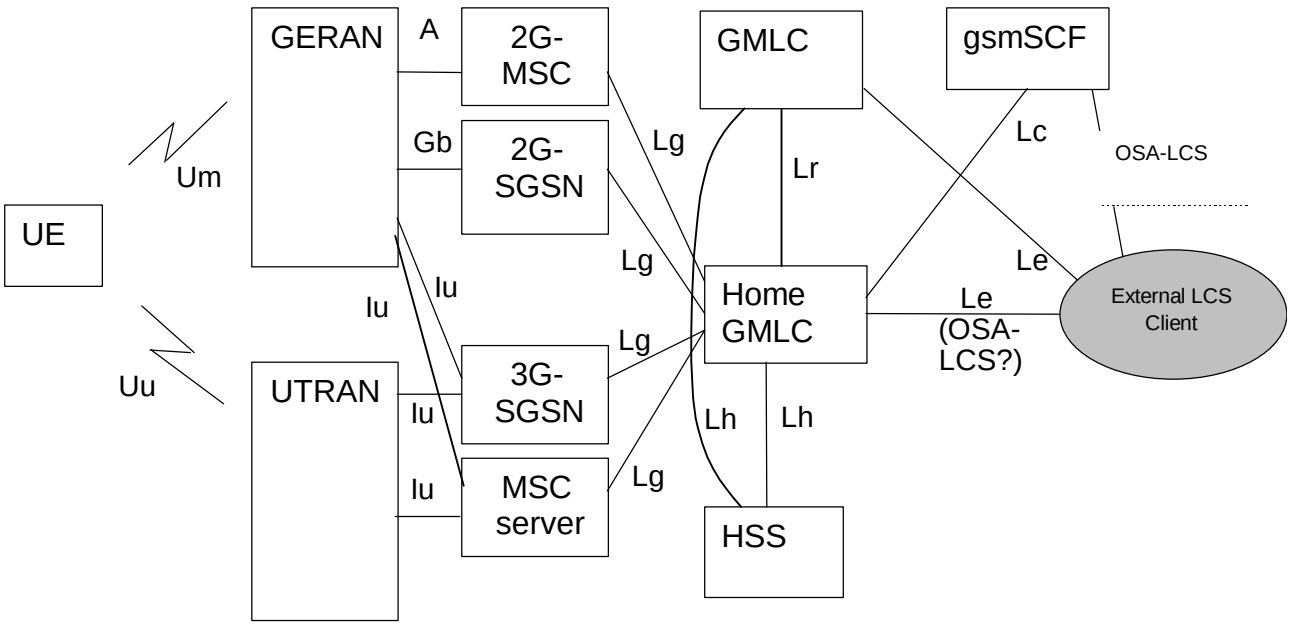


***Figure 7.3.1**; LCS architecture alternative with Home GMLC*

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

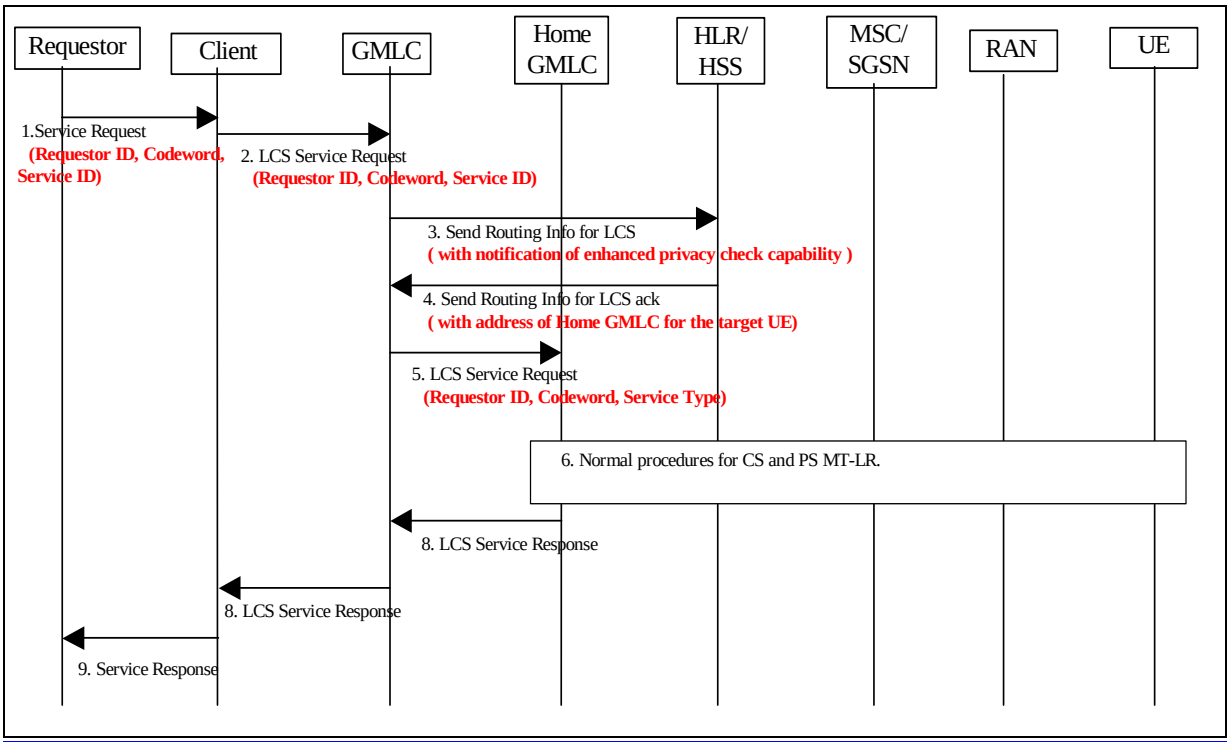


Figure 7.3.2~~1~~*; General information flow for the architectural alternative with the Home GMLC*

Note : In step 6, the Requestor ID and the codeword shall be sent to the MSC/SGSN (Rel-5) if they are wanted to be shown to the UE user in the LCS notification invoke procedure. Also the result shall be carried to the SGSN/MSC (Rel-5).

The Home GMLC may in step 6 send also a pseudo-LCS client identity to MSC/SGSN of Rel-4 or earlier. This signaling step should be further detailed.

7.4 Architecture alternative with PPR associated with the HSS only

Section 7.4 ~~in version 1.1.0~~ was removed as other architectural alternatives consider similar mechanisms to what it introduced. This was~~is~~ done with the aim to simplifying the consideration and decision of the alternative methods.

~~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:

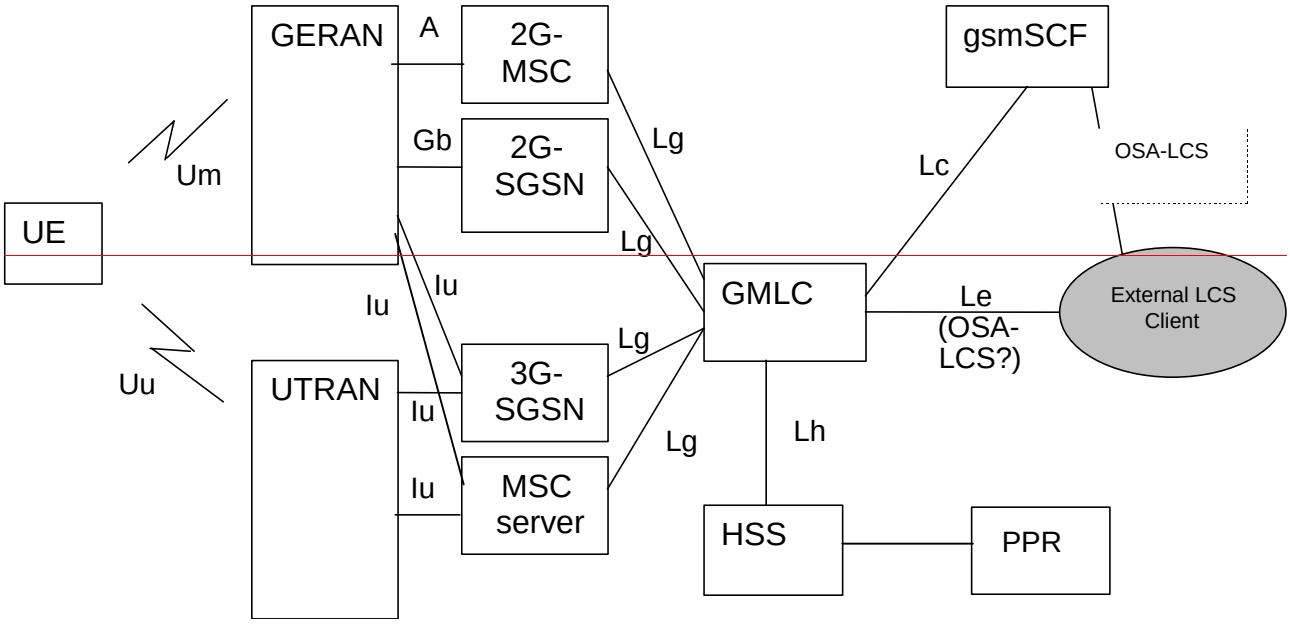


***Figure 7.4**; LCS architecture alternative with PPR attached to HLR*

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 Enhanced User Privacy using existing LCS architecture.

7.5.1 Architecture

In order to support the service requirements for enhanced privacy checks, the LCS architecture as specified in LCS stage 2 3GPP TS 23.271 rel-4 can be used, without the addition of new nodes/network entities.

7.5.2 Information flow

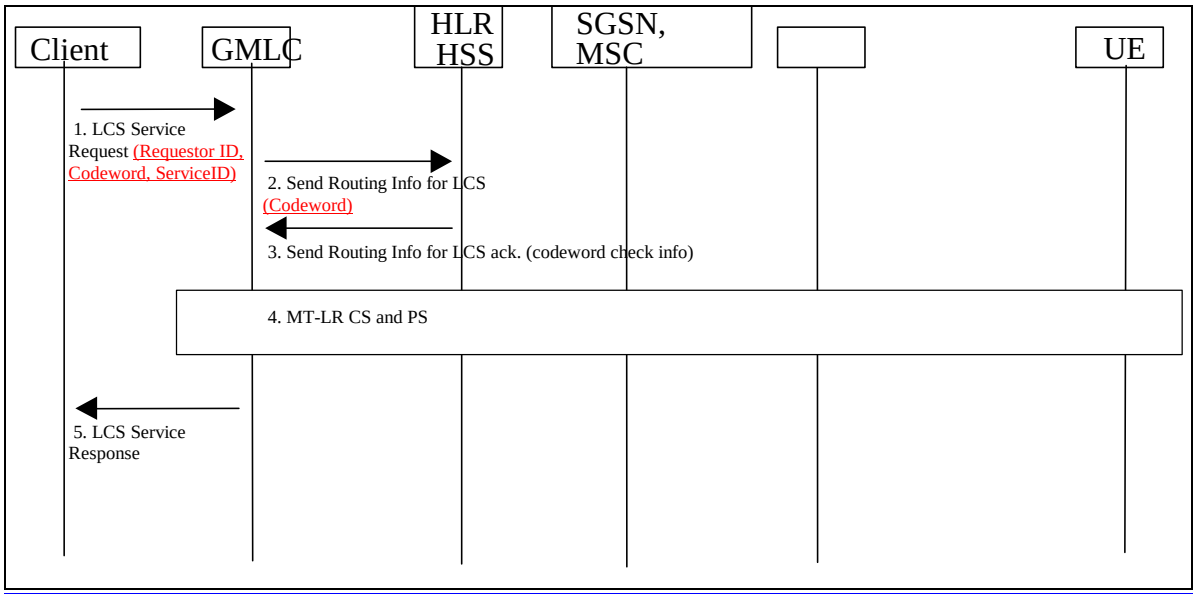


***Figure 7.5.1**; General information flow when using existing architecture*

1. The LCS service request sent from the LCS Client to the GMLC carries the parameters for enhanced privacy checks (Requestor Id, Codeword and Service ID).

2. The GMLC verifies in the LCS client profile that the service ID received by the LCS client matches one of the allowed Service identities for that LCS client.

3. The GMLC sends a Send_Routing_Info_for_LCS message to the HLR/HSS, carrying the codeword received from the LCS client.

4. The HLR/HSS verifies that the Codeword received from the GMLC matches one of the codewords stored for the target subscriber. If the check is unsuccessful, the HLR/HSS sends an error indication to the GMLC and the LCS procedure is ended. If the check is successful, the HLR/HSS may verify that the VMSC supports the EUP mechanisms (this information is received in the HLR/HSS at location update in the "LCS supported capabilities set"). In order to protect the privacy of a roaming subscriber, the HLR/HSS may reject the

Send_Routing Info_for _LCS if the VMSC/SGSN does not supported enhanced privacy checks. If the codeword check is successful and the VMSC/SGSN supports the needed LCS capabilities, the HLR/HSS sends the VMSC/SGSN address in Send_Routing_Info_for_LCS_ack message.

5. If no codeword is registered in the HLR for the subscriber, the HLR shall not reject the request and inform the GMLC by setting the codeword check info in the Send_Routing_Info_for_LCS_ack message

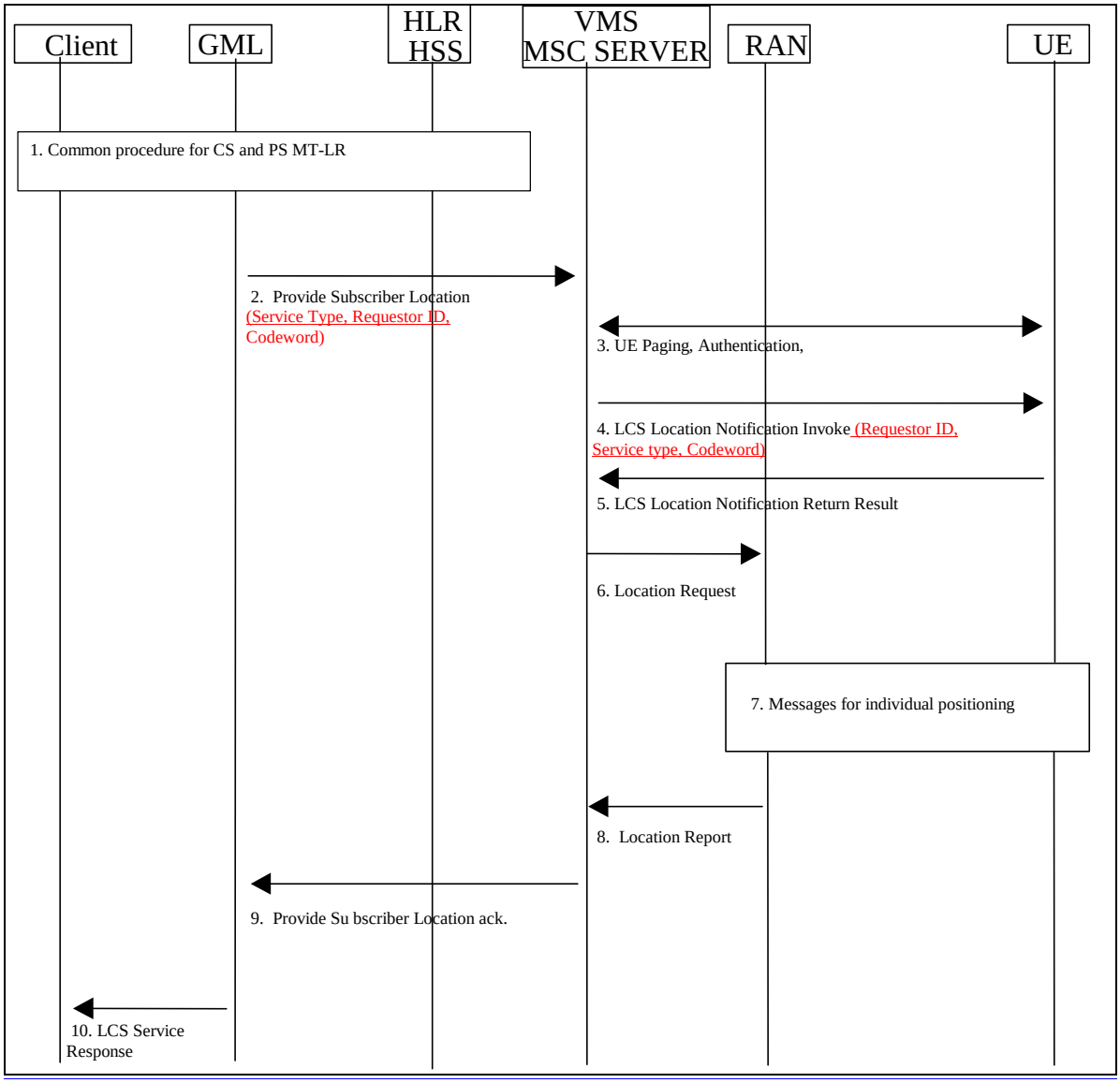


***Figure 7.5.2**; Continued general information flow when using existing architecture*

6. The GMLC converts the service identity received by the LCS client in the proper service type and sends the service type and the Requestor identity in the MAP Provide Subscriber Location message. If the GMLC received the information that no codeword for the subscriber was stored in the HLR, the codeword shall be include in the Provide Subscriber Location message, in order to have the codeword check in the UE (note that the PSL message has to carry the codeword for notification, not depending of the chosen architecture).

7. If the SLPP contains service types/requestor ids, an CS-MT-LR/PS-MT-LR will be allowed by the MSC/MSC server or SGSN if the service type/requestor id supplied by the GMLC matches the identity of any service type/requestor id contained in the UE's SLPP. If the SLPP does not contain service types/requestor ids, the already existing privacy checks will be performed.

8. If notification has to be performed, the LCS Notification Invoke message will carry also the requestor ID, the service type and the codeword, if received.

7.65 Comparison between each architectural alternatives

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

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

Note: The criteria is whether an operator can protect the operator's subscribers against location requests, which needs enhanced privacy check. The operator may reject a Rel-4 location request in a Rel-5 network.
The Rel-5 GMLC includes a notification to HLR that it supports enhanced user privacy.

SGSN/MSC	Rel-5	Rel-4 or earlier	Rel-5
HLR	Rel-5	Rel-5	Rel-5
GMLC which received the location request from LCS client	Rel-4 or earlier	Rel-5	Rel-5
7.1 PPR attached to GMLC	Yes If the operator wants to protect operator's subscriber against unwelcome location request, HLR needs to reject SRI from the GMLC because the enhanced privacy cannot be checked. HLR may reject SRI from the GMLC depending on the setting in HLR The GMLC cannot access the PPR	Yes Enhanced privacy check is performed in the PPR and the PPR rejects the unwelcome location request. GMLC will use in PSL request to MSC a Pseudo LCS Client ID that it receives from the PPR to provide backward compatibility	Yes Enhanced privacy check is performed in the PPR and the PPR rejects the unwelcome location request.
7.2 PPR attached to MSC/SGSN	Yes Rel-4 privacy checks remain in MSC/SGSN and are possible If the operator wants to protect operator's subscriber against unwelcome location request, HLR needs to reject SRI from the GMLC because the GMLC cannot send some parameters for enhanced privacy to the MSC/SGSN and the MSC/SGSN cannot check the enhanced privacy by using new parameters (i.e. codeword, requestor id, service type, etc) 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.	Yes, the HLR may reject the SRI if the MSC/ SGSN does not support the proper LCS capability set. The Pseudo Id cannot be used. The MSC/SGSN cannot access the PPR and rejects the request due to Rel-4 incompatibility reasons.	Yes Enhanced privacy check is performed in the PPR and the PPR rejects the unwelcome location request.

7.3 Home GMLC	Yes If the operator wants to protect operator's subscriber against unwelcome location request, HLR needs to reject SRI from the GMLC because the enhanced privacy cannot be checked. The GMLC cannot access the Home GMLC and SGSN/MSC.	Yes Pseudo Id are used towards Rel-4 MSC/SGSN. 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 PPR- HSS	NA	NA	NA
7.5 Rel-4 architecture	Yes If the operator wants to protect operator's subscriber against unwelcome location request, HLR needs to reject SRI from the GMLC because the enhanced privacy cannot be checked. HLR may reject SRI from the GMLC depending on the setting in HLR, so the GMLC could not access the SGSN/MSC	Yes HLR may reject SRI if the MSC/SGSN does not support the proper LCS capability set.	Yes Codeword is checked in the HLR and the HLR rejects the requests if the codeword check is not successful or the MSC/SGSN does not support proper capabilities

***Table 7.5.2**; Other criteria*

Note: The Network Scenario for this table is that GMLC, HLR, MSC/SGSN are all Release 5 (except column 2).

	Enhanced support for location information privacy in other services e.g. Presence and Generic User Profile	The operator can provide the enhanced Rel-5 privacy mechanisms to the Target UE subscriber or not in the Rel-4 MSC/SGSN.	Call/Session related Class (Note 2)	Deferred MT-LR (Note 3) Handling of event-based LCS (Note 4)
7.1 PPR attached to GMLC	FFS	Yes for enhanced privacy check in network. The operator can provide the en-hanced privacy mechanism even if the MSC/ SGSN is Rel-4 using pseudo id. No in the sense that codeword, service type, requestor are not shown to target UE.	Yes PPR can send two results: - call/session unrelated and - call/session relatedMSC/SGSN shall confirm if the request is call/session related	Yes VMSC/SGSN might have to contact PPR in the HPLMN (depending on the event), carrying the information needed to perform privacy checks.
7.2 PPR attached to MSC/SGSN	FFS	Yes for codeword check in HLR No for other enhanced privacy checks. No in the sense that codeword, service type,	Yes MSC/SGSN recognize the call/session related connections and can support it for the enhanced services	Yes VMSC/SGSN might have to contact PPR in the HPLMN (depending on the event), carrying the information needed to perform privacy

MSC/SGSN		requestor are not shown to target UE.		checks.
7.3 Home GMLC	FFS	Yes for enhanced privacy check in network. The operator can provide the enhanced privacy mechanism even if the MSC/ SGSN is Rel-4 using pseudo ids No in the sense that codeword, service type, requestor are not shown to target UE.	Yes Call/Session related class is handled in SGSN/MSC. Home GMLC may replace the external client identity to the pseudo-external client identity.	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 PPR- HSS	NA	NA	NA	NA
7.5 Rel-4 architecture	FFS	Yes for codeword check in HLR No for other enhanced privacy checks. No in the sense that codeword, service type, requestor are not shown to target UE.	Yes (no impact)	Yes (no impact for deferred LR) For event based LR the VMSC/SGSN can perform privacy checks when the event occurs, basing on the event related information and SLPP. The SLPP would need to be updated.

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 and to be enhanced for the Rel-5 privacy settings. 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.

Note 4: In deferred location request the privacy check has to be performed when the event occurs. The criteria is the possibility to handle event-based LCS: for some events, the result of the privacy checks may depend on information owned by the VPLMN. When such new events are defined, the information has to be transferred to the node performing privacy checks. If privacy checks are performed in the HPLMN, the interfaces between the VPLMN and HPLMN have to be updated for each new privacy check. This shows that if the privacy checks are performed in the HPLMN, there will be anyway the need to update interfaces when new privacy checks are introduced.

The description of the architecture alternatives might need to be changed to show how the privacy of deferred location requests is handled.

Editor's note: Table 7.5.3 below is the same as in version 1.1.0 of this TR. The discussion is still to be continued regarding this table.

***Table 7.5.3**; Other differences between architecture alternatives*

	Interface that is new or affected.	Enhanced privacy check.	SLPP check in MSC/SGSN	Other features?
7.1	New	PPR contains and	MSC/SGSN may	

PPR attached to GMLC	Lr: FFS Affected Lh, Lg	checks both the enhanced privacy settings and the legacy privacy settings.	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*~~

7.76 Conclusion on architecture for the enhanced privacy checking

Editor's note: The content of this chapter is not yet agreed.

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 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.

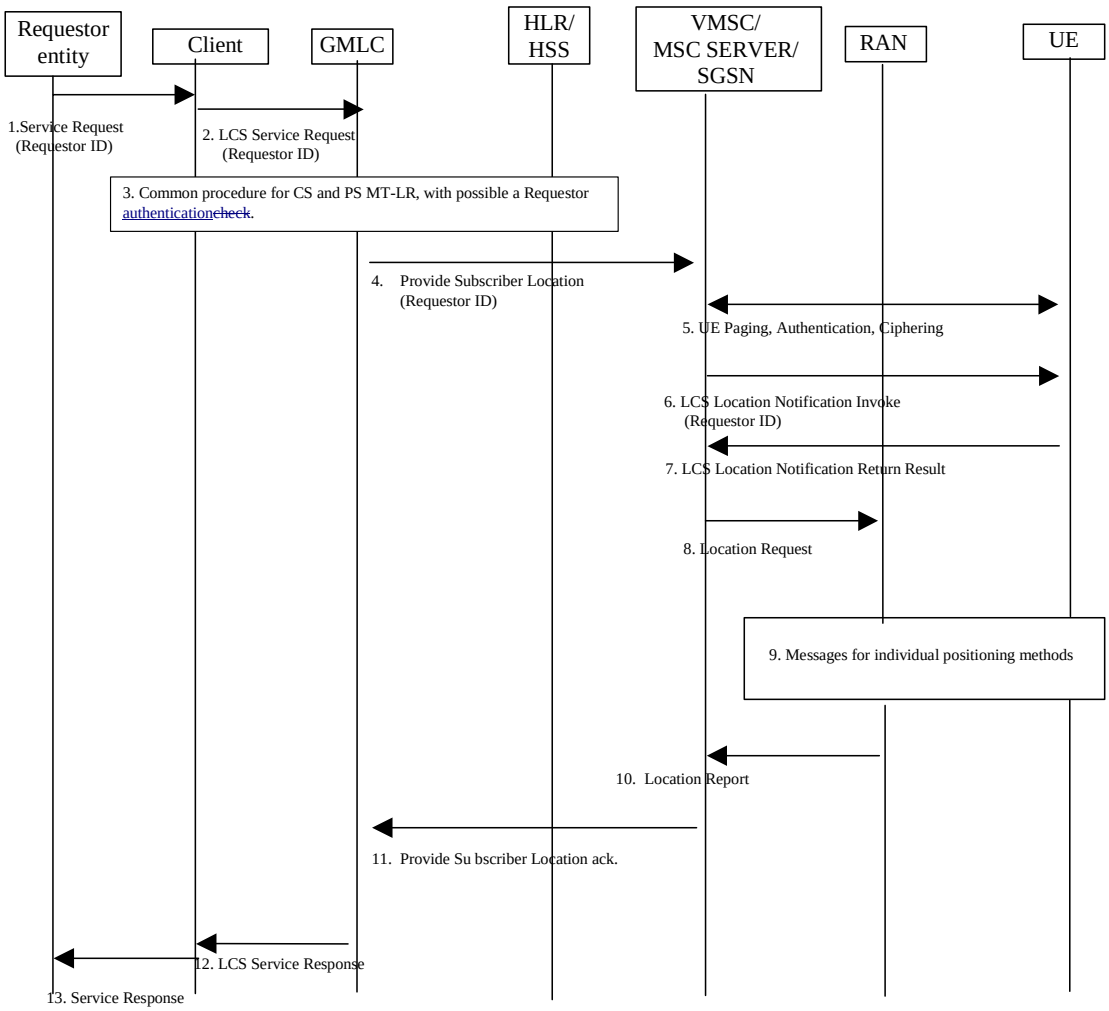


***Figure 8.1**; MT-LR signaling procedure when the requestor identity is authenticated in GMLC*

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 a 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.

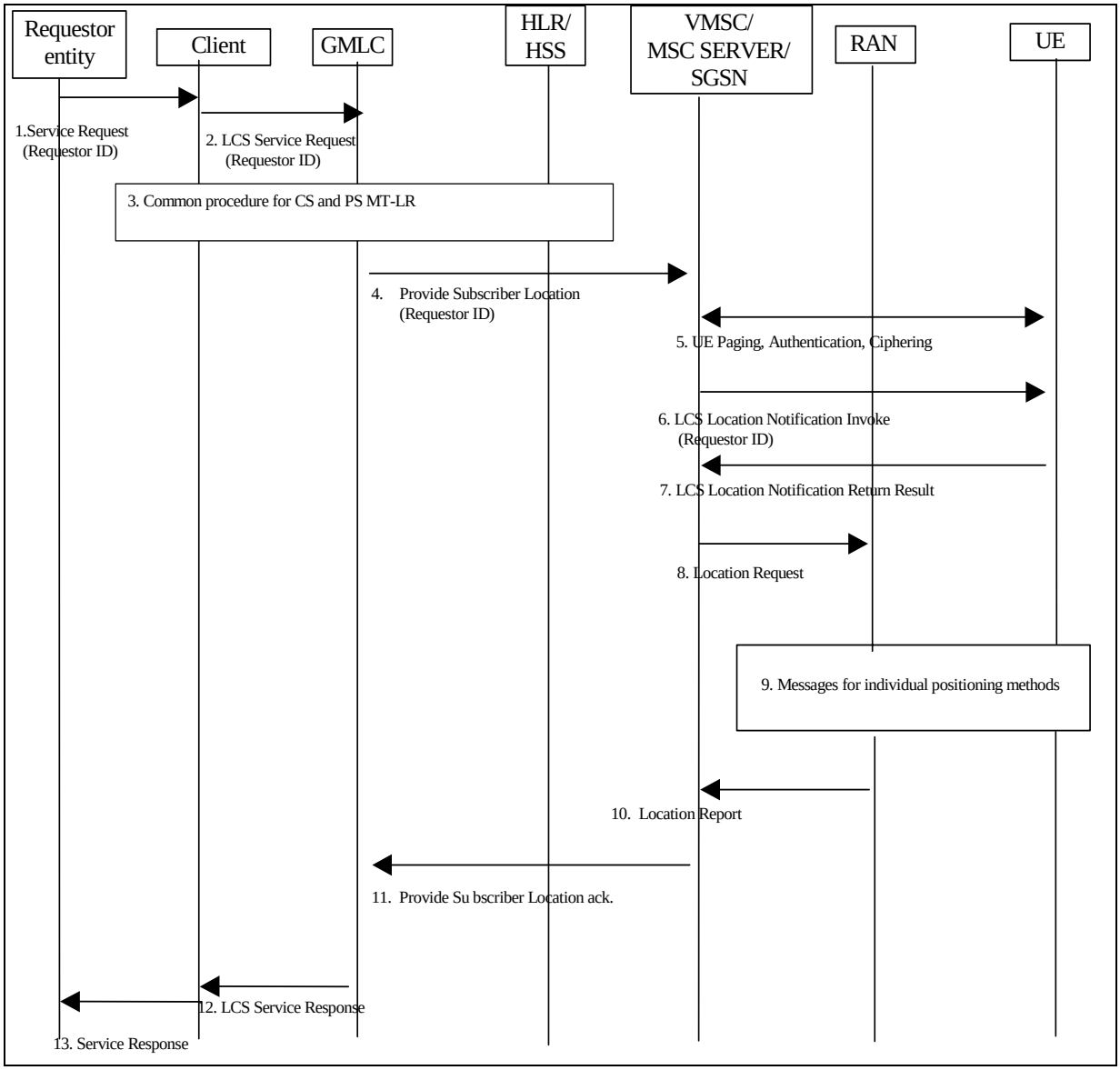


***Figure 8.2**; MT-LR signaling procedure when the requestor identity is authenticated in the LCS client*

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.

2) The LCS Client issues a 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 UE is able to judge that the requestor identity was dropped due to the lack of network capability.

As an alternative, the requestor identity could be carried as part of the LCS client name. 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~~three 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. A further solution is that the codeword is stored and compared in the HLR. These alternatives are described and compared in chapter 7.

10. Stage 2 description of the anonymity concept

The stage 2 description is FFS.

11. Common stage 2 privacy issues in Presence and Location services

The Presence service may act as a LCS client and request location information from GMLC. The location request and privacy are handled as specified in 23.271 for this LCS client.

The Presence service itself may request from the location server what are the privacy settings that shall be applied for the location information of the target mobile before forwarding location information or other presence attributes to other parties.

Possible differences between privacy settings in presence and in LCS should be resolved.

120. Charging Aspects

131. Security aspects

142. 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.
Ver. 1.2.0	February 25, 2002	Changes and addition as agreed in SA2#23 LCS session, Sophia-Antipolis, France

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
					V.2.0.0 created for submission at TSG SA#15. Same technical content as v.1.2.0	1.2.0	2.0.0