PRD SE.23

Title	**Location Based Services**
Version	**3.1.0**
Date	**January 2003**

GSM Association Classifications

Non-Binding

Non-Core

Security Classification Category:	
Unrestricted - Public	**X**

Information Category	General

Document History

Version	Date	Brief Description
0.1	17.9.2001 (w38)	Structure of document. Scenarios by Jean-Christophe Beclier, Cegetel. Editor Katarina Engblom (Radiolinja) katarina.engblom@radiolinja.fi
0.2	1.10.2001 (w40)	Text on scenarios by Jean-Christophe Beclier Cegetel and on inter-operator charging issues by BT Cellnet added
0.3	17.10.01 (w42)	Text on scenarios and additional scenarios based on phone conference added.
0.4	29.10.01 (w43)	Text and pictures by Telia added. A new chapter no. 17 added.
0.5	30.10.01	Additions made on day one in the Helsinki interim meeting.
0.6	31.10.01	Additions made on day two in the Helsinki interim meeting.
0.7	6.11.01	Comments and additions by Graham Trickey.
1.0	9.11.01	Ready for SerG #46 (Madrid)
1.1	14.12.01	Final scenarios discussion and agreement by Jean-Christophe Beclier, Cegetel
1.2	19.12.01	Chapter numbering changed.
1.3	21.12.01	Ready for approval as 2.0
3.0.0	15.2.02	Published version
3.1.0	15.01.03	Modified based on the agreed changes in LBS#4 – LBS#10. Ready for SerG#49 (Melbourne).

Table of Contents

Referenced Documents

GSM 03.71 version 8.0.0 Release 1999 - LCS Functional description - Stage 2
3GPP TS 23.271 version 400 Release 4 - LCS Stage 2

Glossary

A-GPS	Assisted Global Positioning System
AOA	Angle Of Arrival
API	Applications Programming Interface
BSC	Base Station Controller
BTS	Base Transceiver Station
CAMEL	Customised Applications for Mobile network Enhanced Logic
CBC	Cell Broadcast Centre
CGI	Cell Global Identity
CI	Cell Identity
CLI	Calling Line Identity
CLIP	Calling Line Identity Presentation
CLIR	Calling Line Identity Restriction
CP	Content Provider
DCS	Digital Cellular System
DGPS	Differential Global Positioning System
DTAP	Direct Transfer Application Part
EC	European Commission
EGMLC	Enhanced Gateway Mobile Location Centre
E-OTD	Enhanced Observed Time Difference
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GCR	Group Call Register
GMLC	Gateway Mobile Location Centre
GPRS	General Packet Radio Services
GPS	Global Positioning System
GSM	Global System for Mobile communication
GsmSCF	Global System for Mobile communications Service Control Function
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
IMSI	International Mobile Subscriber Identity
ISDN	Integrated Services Digital Network
LCAF	Location Client Authorisation Function
LCCF	Location Client Control Function
LCCTF	Location Client Coordinate Transformation Function
LCS	Location Services
LDR	Location Deferred Request
LIF	Location Interoperability Forum
LIR	Location Immediate Request
LMU	Location Measurement Unit
LOS	Line-Of-Sight
LSBF	Location System Billing Function
LSOF	Location System Operations Function
MD	Mediation Device
MLC	Mobile Location Centre
MO-LR	Mobile Originating Location Request
MS	Mobile Station
MSC	Mobile-services Switching Centre
MS-ISDN	Mobile Station Integrated Services Digital Network number
MSRN	Mobile Station Roaming Number
MT-LR	Mobile Terminating Location Request
NILR	Network Induced Location Request
NMD	Network Measurement Data
NMR	Network Measurement Report
OTD	Observed Time Difference
OTDOA-IPDL	Observed Time Difference Of Arrival - Idle Period Down Link
PCF	Position Calculation Function
PCS	Personal Communication Services
PDN	Public Data Networks
PLI	Provide Local Information
PLMN	Public Land Mobile Network
PMN	Public Mobile Network
PRD	Permanent Reference Document

PSTN	Public Switched Telephone Network
RMSE	Root Mean of Squared Errors
RPLMN	Requesting Public Land Mobile Network
RTD	Real Time Difference
RX	Received Signal Strength
SMLC	Serving Mobile Location Centre
SP	Service Provider
TA	Timing Advance
TOA	Time Of Arrival
UMTS	Universal Mobile Telecommunications System
VLR	Visitor Location Register
VMSC	Visited Mobile services Switching Centre
VPLMN	Visited Public Land Mobile Network
WAP	Wireless Application Protocol
Times of Day	Defined periods of times on defined days which define time windows throughout a week.

1. Objective

The objective of this PRD is to

- Brief the operator community at large on Location Based Services (LBS) and examples thereof.
- Develop guidelines and requirements for roaming and interoperability between operators.
- Help GSMA develop strategies to build pro-active co-operation with other significant industry fora.
- To provide operational guidelines to operators in advance of the availability of technical standards (e.g. inter-GMLC interface).

2. Introduction

2.1 Background

When talking about Location Based Services (LBS) the question about how customers' position will add value of service is often raised. Technically there are several proposals on how mobile phones can be positioned. However, there are also other issues that must be solved before LBS can be launched to mass markets. The most important issue is perhaps privacy and especially who owns positioning data and how to handle permissions. Other issues that must be addressed are international roaming, charging capabilities and interoperability between operators within the same market.

Implementation of LBS is in an early stage. Operators will need to consider the International Roaming Scenario and interoperability with operators within the same market when they implement LBS. From both the cost and the revenue opportunity point of view, it would be preferable that operators make plans to implement LBS roaming in parallel to the implementation of LBS in the home market. The cost of roaming post implementation is likely to be significantly higher than if it is done as part of the main implementation.

Operators should seriously consider the question of provision of services that can be accessed and used by customers of other networks in the same market. By doing this, operators can increase the chances of LBS becoming mass-market services rather than remaining niche products. A similar example of how this approach has been successful in the recent past is SMS where the usage increased dramatically in markets where operators allowed inter-working with other networks in their market.

Location information itself does not provide a good service, but if location information can be combined with content to form LBS there are possibilities to create useful services. Location information can be used for example following ways:

- As a filter
  When a customer is searching for a particular service, he can typically restrict results of search with parameters like service type, opening times etc. Automatic positioning can be an effective tool for intelligent search because it makes it possible to offer only results that are close enough to the customer's location.
- As a pointer
  Location information can be used as a pointer in tracking services. The simplest example is showing the location of the customer as a dot on a map.
- As a definer/launcher
  In services like tracking it would be possible to create buffers that would initiate different kinds of notices/alarms when the target is out of defined area. If for example a transport vehicle has gone out of a pre-defined route there would be an automatic notice/alarm for the transportation control centre.
  There are a lot of interesting business cases that deal with "area alarms". The idea for this kind of feature is to launch activity X when customer arrives to area Y. E.g. when a customer comes to a harbour area he automatically gets information about declaration desks etc.

This document will provide an overview of where we are today, of what options are available for the operators and a possible way forward to a future development of the standards. There are several ways to implement LBS; it is not the objective of this PRD to recommend one solution over another solution. That is a choice that every individual operator needs to make based on local market conditions. However, where the choice of solution has implications on international roaming and/or interoperability, then these will be identified and highlighted.

The technical solutions we have highlighted in this PRD are not, as a matter of fact, binding to any operator, but a way to make the Mobile world identify its needs and put them into practice.

It is also intended that this document will guide operators how to inter-work in the absence of the technical standards. The principal technical standard that is required is the Lr interface (inter-GMLC interface). This is an approved 3GPP work item and is scheduled for completion in Release 6 (mid 2003).

In the absence of the technical standard, it is recommended that operators implement the Lr interface as shown in the scenarios. The functional requirements have been defined for 3GPP and it is recommended that operators implement this based on those requirements. The high level functional requirements of the Lr interface are shown in Appendix 5.

2.2 Outline of the Document

Chapter 3 defines the overall picture of LBS. In chapter 4 general issues are presented. Single network use cases and scenarios of LBS are presented in chapter 5. In chapter 6 inter-network operation use cases and scenarios of LBS are considered. Roaming use cases and scenarios are considered in chapter 7. The conclusions of the PRD SE.23 are presented in chapter 8.

2.3 Terminology of the Document

Target: Target is the entity being positioned. It can be a person, an animal or a vehicle, for example. The Target may have a contract with his home operator enabling the positioning of the customer. The customer is responsible for authorising who is allowed to access the location information either directly to the Operator or via a Service Provider. The Target may be a person or a telematic device such as vehicle or ATM. In the 3GPP specifications the Target is referred as Target UE.

Requestor: The entity requesting the location information. The Requestor may be the same as the Target in the case when a subscriber requests for service based on his/her location. The Requestor may be a person, a company or a telematic device. The term Requestor is used as well in the 3GPP specifications.

Service Provider: The Service Provider provides the Location Based Service for end-users. The service can be an internal service of an operator but may also be provided by an external party. The Service Provider may use external content providers to provide content to the service. The Service Provider may have a contract with the operator providing location information as well as with content providers. The Service Provider is responsible for charging the Requestor for the service. The Requestor must either have a direct contract with the Service Provider which allows for direct billing to the Requestor, or alternatively the Service Provider must have a method of implementing an m-commerce or micro payment to the Requestor HPLMN so that a billable item can be added to the Requestor bill. The charging issues are discussed more detailed in the chapter 4.8.

Target Home PLMN: The Target Home PLMN (HPLMN) has a contract with the Target. It is responsible for keeping register on who is allowed to access the location data of its customers and in which situations. All the location requests are always made via the Target HPLMN to ensure privacy.

Target Visited PLMN: The Visited PLMN (VPLMN) is a network operator who is providing the mobile access when the Target is abroad. This operator is the only operator who has the direct access to the location information. Only the Target HPLMN may request the position of the Target.

Requesting PLMN: The Requesting PLMN (RPLMN) is the first PLMN receiving the location request from the Service Provider. The Service Provider typically cannot make a contract with all the operators in the world but only with domestic operators. Therefore the operator having a contract with the Service Provider may be different from Target HPLMN as well as Requestor HPLMN. The RPLMN offers the Service Provider the access to the location information. In addition the RPLMN may provide a micro payment service to the Service Provider for charging the Requestor. In this case the Requestor is either billed or the pre-paid account of the customer is charged in real time by the Requestor HPLMN.

Requestor HPLMN/VPLMN: The Requestor may be a subscriber of a different operator than the Target. A typical example of this is a find-a-friend service when the Requestor has friends who are subscribers of different domestic operators. If the RPLMN has a micro payment contract with the Requestor HPLMN and Service Provider has a micro payment contract with the RPLMN, it may be possible for the Requestor HPLMN to bill the Requestor either in real-time or post-paid on behalf of the Service Provider. To prevent fraud the Requestor HPLMN may be willing to authenticate its customer.

Clearing House: The clearing houses are responsible for inter-operator billing in roaming of Location Based Services. The clearing of the payments are post-processed after the actual location requests. The clearing house will not be responsible for end-user billing.

Location Based Services: Location Based Services (LBSs) are services that use the location of the Target for adding value to the service. In this PRD the term LBS covers wider range of services than in the 3GPP specifications (e.g. Location Based Service and Location Dependent Service mentioned in the 3GPP TS 23.271). As the term LBS covers the service aspects it should not be mixed up with the term LoCation Services (LCS), which is used in the 3GPP specifications and which covers all the hardware e.g. network elements and entities necessary to provide LBS thus the LCS does not specify any location based (value added) services except locating of emergency calls.

3. Location Based Services

3.1 Purpose of the Chapter

Aim of this chapter is to describe on a general level which features make LBS special. What services will be killer applications and be implemented by operators is out of the scope of this document. However, in this chapter there are described as an examples three basic type of LBS.

3.2 Nature of LBS

Locaton Based Services are business and consumer services that give users a set of services starting from the geographic location of the client. These services offer the possibility to users or machines to find/locate other persons, machines, vehicles, resources and also location-sensitive services, as well as the possibility for users to track their own location. The request for location can be originated from the client himself and from another entity such as an application provider or the network. Anyway, whenever location is requested, the customer has to give permission for the location request. Location Based Services cut across many mobile classes of services since they add the feature of placement to these.

Most Location Based Services will include two major actions:
1. Obtaining the location of a user
2. Utilising this information to provide a Service

Location Based Services can automatically be triggered when the client is at a specific location, e.g. geographical areas subjected to different billing systems. Alternatively it can originate from the client himself in order to satisfy location based requests such as information needs; finding point of interest, persons or checking the traffic conditions, finding other people, vehicles, resources, services or machines and emergency requests.

3.3 Examples of LBS

There are three basic types of Location Based Services: **pull**, **push** and **tracking**. In the case of a **pull** service, a customer makes by himself a request for LBS. When making this request he/she gives permission for his/her position to be given because without that location information the request for service cannot be completed.

<u>An example for pull-type-of service:</u> the customer sends a request for local weather forecast by SMS to the service number 1234. To offer local weather forecast, a Service Provider has to know from where the request was made. By the basis of the customer’s location information the Service Provider will send as a reply a forecast for the area from where the request was made.

The **push** services differ from the pull services on the point that the request for service is not technically made by the customer but by the Service Provider. In these cases the customer must give permission for the Service Provider to send information to his mobile phone.
<u>An example for push-type-of service:</u> The customer has registered himself to a weather service and set up a profile on which he requests local weather forecast every morning at 08.00 am. To send the forecast of the right area to the customer, the Service Provider has to know where the customer is at 08.00. Because the customer has allowed positioning every morning 08.00 for weather service, the operator will tell the Service Provider where this customer is at the time of service request. After getting the position of the customer the Service Provider can send the right forecast to the customer.

Tracking services are the third basic type of LBS. The idea for that type of service is that someone (person or service) asks for a location of the mobile terminal (person, vehicle, fleet etc.). As in the pull and push cases the assumption is the customer has given the permissions which allow particular persons or services to track him.
An example of a tracking service: the buddy finder. A cycling team has signed up on the service to keep better in touch with each other. Every member of the team has given permission to be tracked by the other members. When the team is on the training round, individual team members might choose optional routes to get to the meeting place. Those who are first on the meeting point would like to know where the others are at the moment. They may set up a connection to the tracking service (for ex. WAP, WEB, etc.) and make the request of the positions of those members who aren't yet at the meeting place.

Many of the services, like those mentioned above, are quite easy to implement when the operator is also Service Provider and is offering these services only to its own customers. However, nature of the LBS requires interoperability between operators both at national and international level. To reach mass markets with LBS, we could compare it to the SMS business case: after inter-operator SMS functionality was provided, the market grew very fast. When considering e.g. tracking example above, it is obvious all the members of the cycling team are not necessarily customers of the same operator. However the team could be interested in the service if it was possible to add all the members to the service irrespective of who is their operator. Similarly the roaming customer who is on vacation in the foreign country would like to use local LBS such as "find the nearest ATM". Without solving the roaming problems a huge market potential will not be realised.

4. General Issues

4.1 Purpose of the Chapter

In this chapter is given an overall view of the factors which have to be considered when LBS are implemented. There is described a simplified chain from LBS producers to LBS users as well as requirements for those who are implementing LBS.

4.2 Players in LBS

It is likely that many Location Based Services will require the involvement of many different parties in order to provide the complete service. In the following chapters there will be more detailed classification of the players but the following diagram Figure 4-1 shows on a general level the players who are involved in LBS.

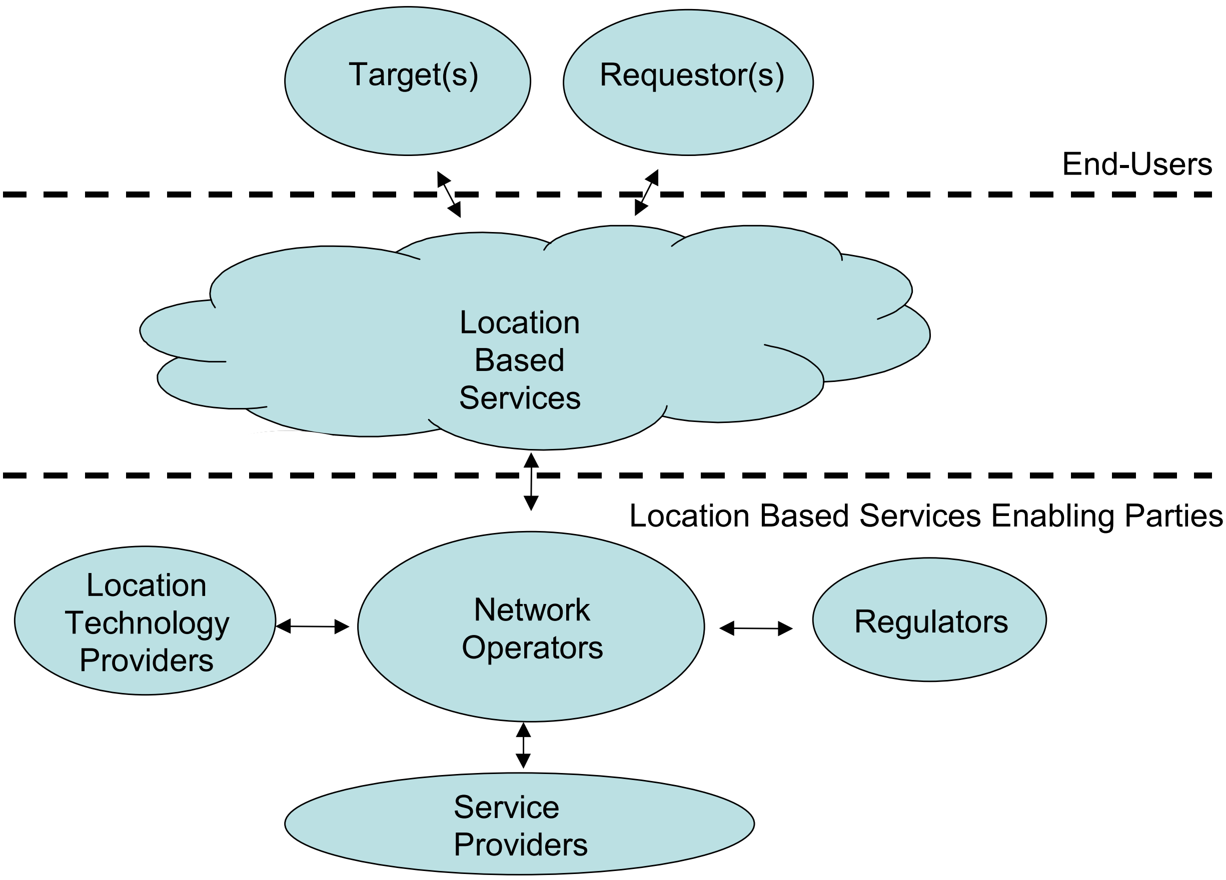


Figure 4-1 Players in LBS

In the middle of Figure 4-1 is a “cloud” describing LBS, from which there are two connections: to the end users and to those players who make it possible to create LBS.
End-Users are divided in two categories: Mobile Users to Be Located, Targets, and Location Requesting Users, Requestors. The Targets are End-Users whose position is asked by someone else or by some service. The Requestors are those who are asking the position of some service or some person. Obviously the End-User can simultaneously have both roles.
Location Based Services Enabling Parties are described at the bottom of the picture. These players are divided roughly into four categories: Location Technology Providers (LTP),

Network Operators (NO), Regulators (REG) and Service Providers (SP).
Location Technology Providers (LTP) are manufacturers of different hardware and software, which enables positioning of mobile terminals. These are vendors manufacturing network based and handset based positioning solutions. Some of the positioning systems require specific capabilities both within the network and within the mobile terminal. This leads to significant interoperability problems, which need to be addressed.
Network Operators (NO) are companies that have infrastructure for GSM telecommunications. They are the only agent which is able to effectively position the by GSM-network based methods. Their primary interest and responsibility is to protect their subscriber from unsolicited use of the positioning data. The most effective solution would be to handle the data in a secure way inside the network but this is not going to be possible in an early stage one. They make it possible to transfer data such as positioning results. Network operator types are RPLMN, HPLMN and VPLMN.
Regulators (REG) set up laws, regulations etc., which give guidelines how LBS can be legally implemented. The major issue is likely to be privacy, with both the European Union and individual countries having their own regulations, which will need to be followed.
Service Providers (SP) create and sometimes provide LBS, which are used via NO. SPs are the companies that implement service logic and user interfaces, interfaces between LBS and NO systems etc. However, SPs don't necessarily have either data or infrastructure to offer LBS to the customers.

4.3 LBS Components

When looking at Services, it is often useful to relate the Service to the technical Enablers that will be required to implement such a service. In the next table there is a division into three categories; Services, Features and Enablers.

SERVICES	End-to-End specific products/applications	*Example: Current Position, Point of Interest, Location Tracking*
FEATURES	A set of capabilities that is required to implement a service.	*Example: Position Server, Gateway, Mediation Device, Map Server*
ENABLERS	Set of generic network and terminal functionalities, including standardised toolkits, protocols and application interfaces, providing basic transport and control mechanisms.	*Example: Positioning system, SMLC, GMLC, SMS, Circuit switched Channel, Packet switched channel, WEB protocol, WAP protocol, WAP Push Protocol*

Table 4-1 Relationship between services, features and enablers

An example: Service is the product, which is sold to the customer. It is created using Features such as user interface, privacy checking, personalisation, charging etc. Enablers, such as the GSM network, are needed to implement features and to deliver service to the customer.

The following general assumptions are made throughout this document.

- Operators are prepared to sign a contract on reasonable commercial terms with any Service Provider or Network Operator to provide location information on mobiles actually using their network.
- Operators will be able to extend their existing commercial agreements for roaming to include the ability to provide Location Information on request to other Operators.
- That the regulatory and privacy concerns can currently be met by requiring an Operator to

maintain a database containing information on which Service Providers, which Services and what "time of day" their Customer has authorised the Operator to provide Location Information to.

4.4 General LBS Architecture

As a basis for the scenarios described in chapters 5, 6 and 7, a general LBS architecture is defined in this chapter. The architecture is shown in Figure 4-2, which is followed by descriptions of the related elements and functions.

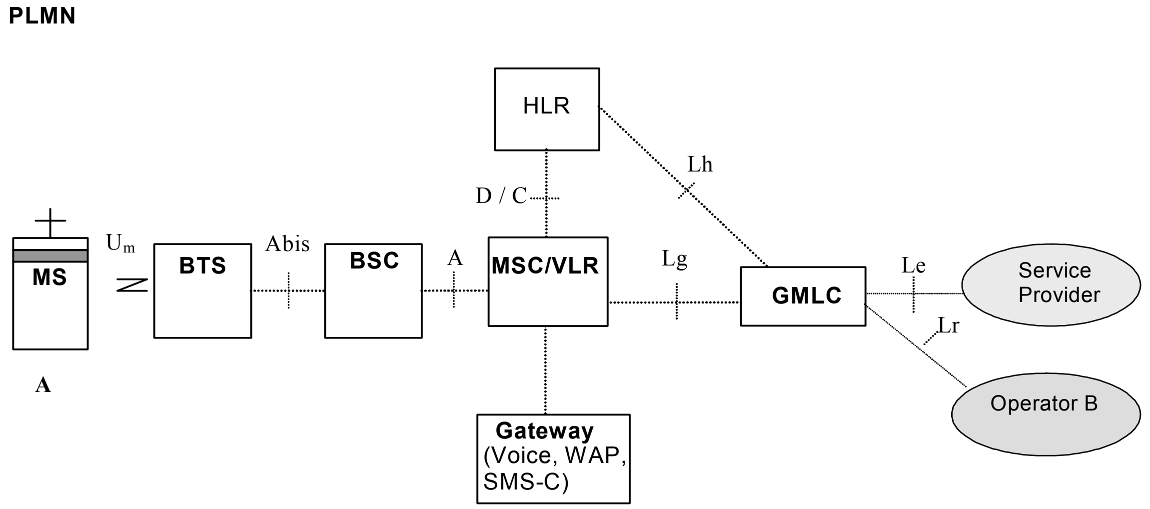


Figure 4-2 General architecture for LBS provisioning

The functions can be described in the following manner:

Gateway provides the interface between a mobile user and an external Content Provider. The interface may support one or more transport technologies such as voice, SMS or WAP. The Gateway also provides firewall, authentication and authorisation features to control access to the Gateway from 3rd parties.

The **Gateway Mobile Location Centre (GMLC)** is as defined in 3GPP specification for LCS, 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 via the Lh interface. After performing registration and authorisation, it sends positioning requests to and receives final location estimates from the VMSC via the Lg interface or where the PLMNs involved have implemented Lr interface this could be used instead. The GMLC can include the following functions.

Location Client Control Function (LCCF)
The LCCF manages the external interface towards the LCS client. The LCCF identifies the LCS client within the GSM PLMN by requesting client verification and authorisation (i.e. verifies that the LCS client is allowed to position the subscriber) through interaction with the Location Client Authorisation Function (LCAF). The LCCF handles mobility management for location services e.g., forwarding of positioning requests to VMSC. 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 Coordinate Transformation Function (LCCTF) to perform a transformation to local coordinates. It also generates charging and billing related data for LCS via the Location System Billing Function (LSBF).

Location Client Authorisation Function (LCAF)
The LCAF is responsible for providing access and subscription authorisation to a client. Specifically, it provides authorisation to a LCS client requesting access to the network and authorises the subscription of a client. LCAF provides authorisation to a LCS client requesting Location Information of a specific MS.

Access Subfunction enables LCS clients to access LCS services. This subfunction provides verification and authorisation 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
- the LCS client is authorised 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

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)
- 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

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

Location System Billing Function (LSBF)
The 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.

Location Client Coordinate Transformation Function (LCCTF)
The 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 LCS Client and known as location information. The local system required for a particular LCS Client will be either known from subscription information or explicitly indicated by the LCS Client.

Location System Operations Function (LSOF)
The LSOF is responsible for provisioning of data, positioning capabilities, data related to clients and subscription (LCS client data and MS data), validation, fault management and performance management of GSM LCS. This function can also reside in LMU, BSC, SMLC or MSC.

Positioning Function
Positioning function is a combination of network entities that accepts an MS-ISDN, and returns the latitude and longitude of that MS-ISDN. The implementation of this function

may vary by Operator. The Positioning Function can be either integrated to the GMLC or be a separate network element e.g. Serving Mobile Location Centre (SMLC) (the SMLC is as defined by the 3GPP). The Positioning Function of the requesting PLMN must be able identify the Target HPLMN, and must be able to communicate with all the necessary network elements (depending on the positioning method) within the HPLMN to provide location of the Target. The Positioning Function is also responsible for creating appropriate Charging Data Records (CDR) to provide for inter-operator charges against the provision of location information and the routing of location information requests and location information to other Operators.

In summary, the GMLC is responsible for handling location requests and answers. The GMLC also provides authorisation features to control access to the GMLC from 3rd parties.

Service Providers (SP) create LBS services, which are used via Operators. SPs are the companies that implement logic and user interfaces for services, interfaces between LBS and Network Operator systems. However, SPs have neither data nor infrastructure to offer LBS to the customers. A Network Operator may also act in the role of SP.

MSC is as defined by 3GPP, as well as the **HLR**.

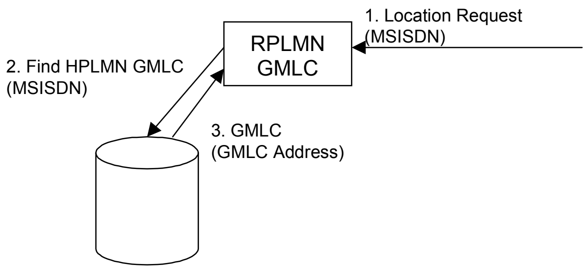
4.5 Determining Target HPLMN

When a Service Provider requests the location of a subscriber, it will send a request to the GMLC of the network of its choice (RPLMN). This choice may be based on a number of factors, including which network(s) it has agreements with or which subscriber it is locating.

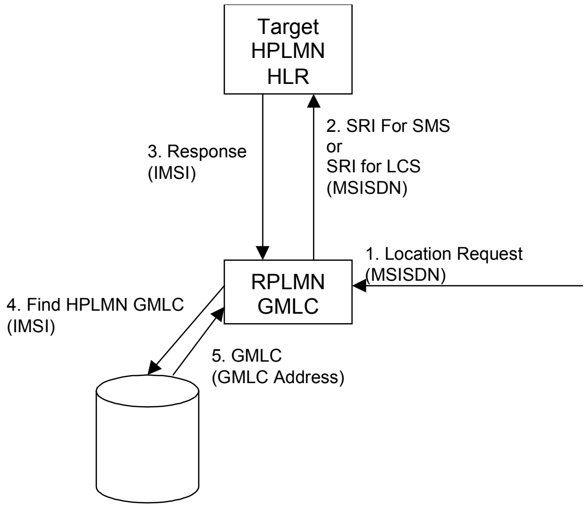
If the RPLMN is not the Target HPLMN, it will need to pass the request on to the GMLC in that network. The RPLMN may use any method to determine which is the Target HPLMN, depending on factors possibly including:

- National situation
- Agreements with other networks
- Available data

Basically there are two approaches which can be taken. One is for the RPLMN to hold a database to map MSISDNs to Target HPLMN GMLC. The other is for it to query the subscriber’s HLR (using either SRI for SMS or SRI for LCS) to obtain the IMSI. From this it can use the country code and network code to access a database to obtain the Target HPLMN GMLC.



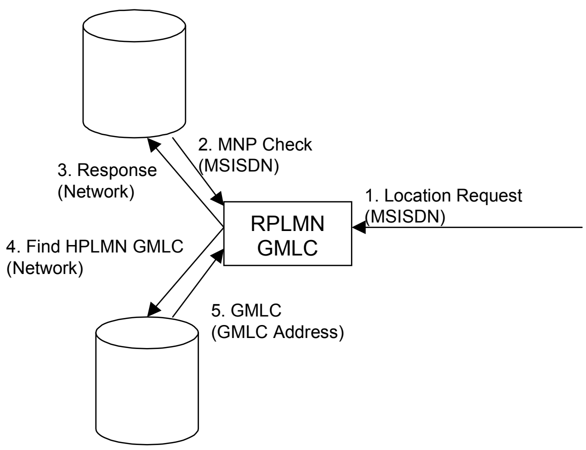
Method A: MSISDN Database



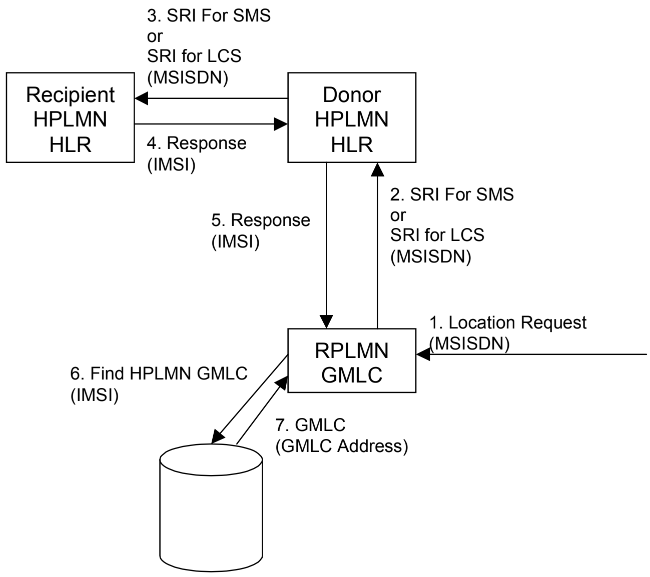
Method B: HLR Query

This is then further complicated when Mobile Number Portability (MNP) is introduced. MNP (in force in some countries) allows a subscriber to change networks, keeping the same MSISDN. This results in fragmented number blocks, where some numbers within a block “belonging” to one network, are actually for subscribers on one or more other networks. The method used to implement MNP varies between countries, requiring different solutions.

Where MNP is handled by means of a database of ported numbers (either just for it's own ported out numbers or a national database for all ported numbers), the RPLMN GMLC can query this first, then use the network provided to determine the address of the Target HPLMN GMLC. Where there is no database (or the database does not cover the number range concerned), the Target GMLC must use method B. In this case the Target HLR will need to pass on the request to the recipient network, which will return the result.



Method A: National Database



Method B: HLR Query

Note that even if the RPLMN can use a database for nationally ported numbers, it would be very unlikely to hold details of ported numbers within another country. It would therefore not be able to use method A for that situation and would need to support method B.

4.6 Privacy Principles

4.6.1 General on Privacy Principles

Location privacy is a complex matter, especially when the Target is roaming. Traditionally operators have kept subscriber location information within their own networks. With the take off of roaming LBS the subscriber's location will be transferred over network boundaries and outside networks. There are laws to protect subscriber data, such as location that regulate operators. However, laws differ from country to country. Therefore, it is of high importance that operators align their general requirements with each other and give this as input to ongoing standardisation in order to make roaming LBS feasible in the future.

4.6.2 Basic Requirements

The identified basic requirements are applicable for all positioning cases. These basic requirements are presented below.

The identity of the Target (for example MSISDN) shall be made anonymous to the Service Provider if desired. The user identity shall be authenticated as well. The authentication method depends on bearer service used, (e.g. CLI, username/password, Certificates, PIN).

The user shall have control over whom or which application(s) may locate them. Different levels of control may be offered

- Control statically by user for each application
- Control dynamically on per application basis
- Control dynamically on per location request basis (asked every time)

The User shall be informed when they are being located. Different levels of notification may be offered

- no notification
- per request notification
- historical logging (i.e. log of who has asked for location)

The user can control the level of accuracy of positioning to protect privacy. For example one application can pinpoint, another may get just the name of the town.

In tracking services the locations of the user are logged to give trace of movement. The logging should be done for short time to provide a local cache, and then discarded.

4.6.3 Requirements for Inter-operator Location Requests

As a basic principle the privacy check should always be performed by the home operator, HPLMN of the user whose location is being requested, i.e. the Target, in order to make sure the Target privacy settings are applied. Furthermore, any possibility that location information can be obtained without the explicit approval of the Target HPLMN for any location request should be prevented. By using the Lr (inter-GMLC) interface it will be ensured that the above principle can be applied. The GSMA SerG has sent a liaison statement to the 3GPP requesting that 3GPP SA WG 1 and 3GPP SA WG 2 ensure that the above principle can be applied.

4.7 Positioning Accuracy Issues

The concept of "accuracy classes" has been suggested as a metric for determining the degree to which positioning solutions meet the requirements of services. A liaison statement was received by the GSMA SerG from the 3GPP SA WG 1 requesting the SerG to provide operator's view on accuracy classes and their requirements (positioning range and probability). The 3GPP SA WG 1 is of the opinion that the establishment of accuracy classes would be helpful to the industry as a metric for determining the degree to which positioning solutions meet the requirements of services (rather than merely as a metric for distinguishing between technologies). The 3GPP SA WG 1's opinion is that accuracy classes should be directly related to the requirements of Location Based Services and that it may be desirable to define multiple classes, perhaps aligned with the accuracy requirements of services as indicated in section 4.3.1 of the LoCation Services (LCS) stage 1 specification TS 22.071.

The GSMA has replied to the liaison statement that on the basis of the below mentioned issues the GSMA opposes the establishment of location accuracy classes.

The services can not as such be tied to certain accuracy classes since the density of services usually varies depending on the area or country. For example in urban areas searching for the nearest fast food restaurant may require positioning accuracy of a few metres whereas in rural areas positioning accuracy of even tens of kilometres may be sufficient. Applying even coarse user location information adds value to many services even regardless of the area or environment (rural, suburban or urban). Thus, the requirements of Location Based Services can not in many cases be related to or expressed with certain accuracy classes.

The LBS accuracy is a function of both the terminal and of the network. Accuracy is not mainly dependent on the terminal. Marking a terminal with the positioning method(s) supported is already covered.

As well, for example E-OTD accuracy varies depending on
- terminal timing measurement resolution
- cell geometry
- network stability
- topographic features (ie multipath)

For AGPS the accuracy will vary mainly depending on
- whether positioning is made indoors or outdoors
- satellite geometry.
- assistance data provided by network

For all the above mentioned factors only terminal timing measurement resolution is terminal dependent. Therefore there is no need for terminal marking of accuracy classes. Such a marking would be misleading for the end-users because all the other factors are independent of the terminal.

However, when the application requests a location measurement there should be an option to specify the actual accuracy required and to receive from the location server the accuracy delivered. The individual operator can then choose how to use this information and how it should be presented to the end user.

It is recommended that the marketplace, not standards or regulations, should decide which technologies serve the needs of customers' best. However, the need for consistency of operation of handsets from different manufacturers is recognised. For this reason, the GSMA has asked the 3GPP to ensure that it would be possible for the accuracy information to be interpreted and presented correctly by the terminal device if the operator chooses to send this information to the end user.

4.8 Charging Principles

4.8.1 Purpose of the Chapter

The charging principles need to be defined for Location Based Services where multiple operators, Service Provider and customers are involved. In this chapter the charging related requirements are described, principally for roaming scenarios.

4.8.2 Introduction to Charging Requirements

It is important to distinguish between the charging for location information and the charging for Location Based Services.

Operators will charge each other for the location information provided across the inter-GMLC interface and will charge 3rd parties for location information provided across the Le interface. The location information will be required to support a specific Location Based Service

Location Based Services are used by end users. Operators will charge each other for specific Location Based Services provided to roaming users. This charge would normally be sent from the Visited PLMN to the Home PLMN using the TAP procedure. The Home PLMN then bills the end user at the appropriate retail rate. Retail charging is outside the scope of this document.

4.8.3 Charging for Location Information

The actual charge for the information should be based on the following parameters.
As a principle, in such a transaction, the party providing the information is entitled to charge for the resource. These principles apply for the charging of another operator or for a 3rd party. This charge will depend on the following attributes of the transaction:

- QOS
  - Requested
    - Accuracy in metres
    - Response time
  - Delivered
    - Transaction status (Success, Last Known Location, Total Failure, Denied)
    - Accuracy in metres (provided for Success & Last Known Location status)
    - Response time
    - Age of last known location (provided for Last Known Location status)
- Tracking or single request
  - Overall tracking period
  - Tracking frequency

It is required that a field is added in the Le interface to identify the type of service request (e.g. emergency, advertising, …)

The basic principles required for inter-operator and operator-3rd party charging for location information are:

- The standard must allow all operators involved in the location process to receive revenue share;
- The charging of the requesting entity must be possible to be made in real-time;
- The charging mechanism must allow roll-back of payments in the case where the service cannot be provided for the end-user for some reason

4.8.4 Charging for Location Based Services

Location Based Services can be considered as a subgroup of m-commerce services. As described above, network operators will charge each other for the use of location resource to support the service. In addition, the serving network operator is entitled to charge the home operator for the use of the service by the visiting user. The charging principles for Location Based Services are up to the serving network operator. The charge for the service will be transferred using the TAP inter-operator charging procedure. The home network operator can then apply the retail charge to the end user.

Examples of Location Based Services are defined below.

- roaming customer requesting location of local facilities (e.g. cash machine)
- roaming customer requesting local navigation
- roaming customer making an emergency call. EU's directive on universal services indicates that emergency calls should be free of charge. If positioning of emergency calls will be mandatory, no charge can be associated with it, at least not for the subscriber.
- home based customer requesting location of a user in another network
- third party requesting location of roaming user (e.g. for tracking service).

In some of the above cases, the Location Based Service is the provision of location information. However, it is important to maintain the logical distinction between the provision of location information and a Location Based Service. Nevertheless, the charge for the provision of location information could be included in the call charge levied by the visited network for the service provided. In some cases, however, it might be more appropriate for the location information to be separately charged.

The basic principles required for the charging of Location Based Services are:

- Charging must be possible regardless of the access channel of requesting user (WAP, WWW, SMS, voice call);
- All scenarios must be supported by the charging mechanisms;
- Charging must be possible regardless of the bearer of the service (IP, GPRS, data-call, voice-call, SMS);
- Charging must be possible for services that require both continuous tracking and single event requests;
- The charging mechanism must allow reservation of money from end-user's account to be used for Location Based Service charges.

4.8.5 Overall View of the Charging Process and Flows

A view of the revenue flow involving all the entities is shown in Figure 4-1, below.

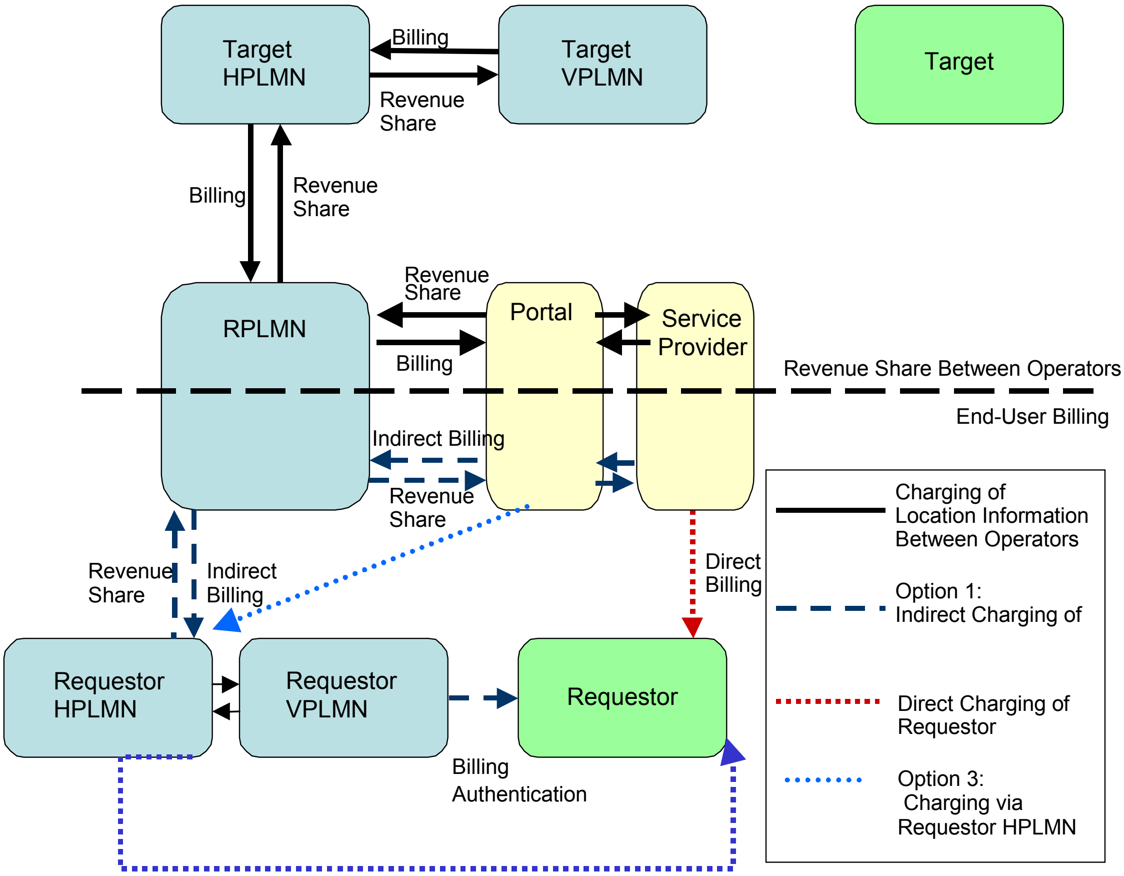


Figure 4-3 A schematic diagram of the two-step charging process. In the upper-half of the picture the revenue share is taken care of between Service Provider and the operators involved in the location request chain. In the lower half of the picture the Requestor is billed for the service either directly by the Service Provider or indirectly via operator chain.

The upper half of Figure 4-3 describes a process in which a Service Provider requests location information. The Service Provider is responsible for paying for this information. This responsibility arises from the contract it has with the RPLMN. The way the RPLMN bills the Service Provider will not be defined in this document and is up to the operator itself.

The way the operators charge one another must be defined. The billing can happen as batch processed billing after the actual transaction. This won't limit the real-time requirements of the actual location request process and requesting end-user billing.

The Target VPLMN bills the Target HPLMN. The Target HPLMN bills the RPLMN. The RPLMN bills the Service Provider. Charging between involved operators is based on the charging elements as defined above. The actual format of the records that should be used for these inter-operator billings is to be defined.

4.8.6 Charging of an End User by a 3rd Party

The 3rd party Service Provider may provide a Location Based Service for the Requestor. In this case, the 3rd party Service Provider is responsible for billing the end-user for the service it's providing.

The 3rd party Service Provider has alternatives it must choose from. It may have a direct contract with the Requestor and bill this Requestor directly. This can be the case for example with corporate customers tracking their property. This method is out of the scope of this document. It’s up to the Service Provider which way it chooses to bill the customer.

A second possibility is the 3rd party Service Provider to bill the requesting home operator and the home operator to bill the requesting party. This is similar to the ‘classic’ post-paid billing scenario.

Another possibility for the 3rd party Service Provider is to route the payment to the requesting customer via the customer home operator. This request must be made in real-time to allow charging with pre-paid accounts. The method must also allow reserving credits for continuous tracking and roll-back of payments when something fails.

4.8.7 Service Price and Accuracy

The Service Provider has no way of knowing if the Target is roaming on another network or not. As the charge for providing location information will be set by each operator individually, and will also depend on the method actually utilised to track the mobile, the price for the request in general is different for the case when the Target is roaming. Regulators in many countries require that the user knows the price of the service before he makes the final decision on using the service.

Some services require accuracy information for location information. Operators may be able to give accuracy information for the location requests. Accuracy information should be incorporated in the location information sent to the Service Provider if available.

The Service Provider sets a price and accuracy limit for the location request. If the request fails because these limits are not met, the price and accuracy of the request sent as reply message to the Service Provider. The failed requests might not be charged either from the Service Provider or from any operator involved.

4.8.8 Event-Based Location Request Including End-User Charging

One time location request including Requestor charging could consist of separate phases.

Table 4-2 Phases of one time location request

1.	The Service Provider requests a money reservation.
2.	The Service Provider request the location information with limit set to the amount reserved.
3.	The Service Provider delivers the service
4.	The Service Provider closes the payment.

4.8.9 Continuous Tracking Request Including End-User Charging

Table 4-3 Phases of continuous tracking request

1.	The Service Provider requests a money reservation.
2.	The Service Provider requests continuous tracking.
3.	The Service Provider continuously retrieves tracking information and delivers the service to the Requestor.
4.	When the reserved amount is used the SP closes the first payment and further reserves more money (back to step 1.)
5.	When the Requestor closes the service the final money reservation is closed.

4.9 Anonymity

4.9.1 General Issues on Anonymity

Generally the identity of a subscriber is given to a Service Provider when accessing a service. However, in some cases this may not be appropriate. In these cases the network would encrypt (or make anonymous) the subscriber's identity into an Opaque ID. The form of encryption used is the responsibility of the network concerned.

Applications can then use this to refer to the subscriber, without the application knowing the subscriber's identity. By doing this, the network is able to provide access to location information without the need to ensure that full data protection is in place.

Note that the issue of anonymity is wider than LBS. The same principles may apply to other service supported by an external Service Provider. For the purposes of this section the scope is limited to LBS.

4.9.2 Mediation Device

Within the LBS architecture, a Mediation Device (MD) is introduced within the requesting PLMN. This is responsible for the encryption and decryption of the MSISDN. The requesting PLMN determines whether to encrypt the MSISDN based on the specific agreement between the network and the Service Provider concerned.

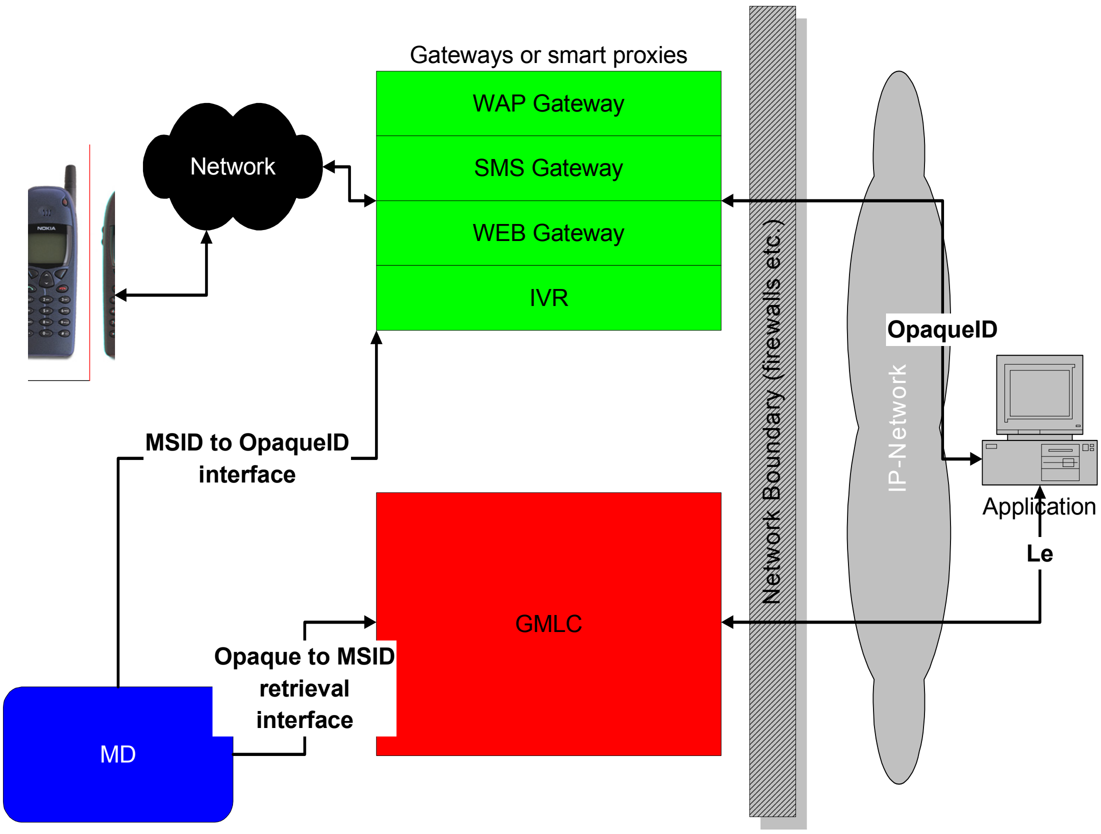
It must be possible to identify from the Opaque ID the network that generated it, so that it can be routed to the correct network for decryption (as encryption methods can vary between networks). This routing may be done by the Service Provider, but must be done by the networks. The Opaque ID should, therefore, contain the mobile country and network codes in plain view of the network in which it was generated.

4.9.3 Use of Opaque ID

The Opaque ID can be used in a number of different situations:
- When the subscriber accesses the LBS
- When the Service Provider requests the subscriber's location
- When the Service Provider takes other actions requiring the subscriber's identity

The MD must, therefore, be accessible from:
- The Requesting PLMN GMLC
- Any gateway used to access LBS

The following diagram shows an example of how the Unique Id is encrypted when the LBS request is made and decrypted when the Service Provider requests the subscriber's location.



4.9.4 Opaque ID Persistence

An opaque ID may be for a single session, be static, or extend beyond a single session.
- A Session Opaque ID is allocated when the subscriber first accesses the LBS and only lasts until that access is completed. Typically, this may be allocated at the start of a WAP session and be deleted at the end of the session. In this case it would be used for any LBS accessed during that WAP session.

- A static Opaque ID is allocated when the subscriber first accesses the LBS, and is retained for all future accesses to that LBS. This may be used, for example, with an LBS which needs to locate subscribers on an ongoing basis (such as polling). These may be used by the Service Provider, without active involvement by the subscriber.

An extended Opaque ID is allocated when the subscriber first accesses the LBS and is retained on completion of the session, for example for a specific time or until a specific number of uses have occurred. Typically this may be allocated at the start of a WAP session with a LBS but where the delivery of information, or subscriber location accesses, occur after the end of the WAP session. An example would be where the subscriber accesses a LBS to obtain a route but has the routing instructions delivered by text message whilst travelling to the destination.

4.10 Terminal Issues

4.10.1 Positioning Method Terminal Interoperability with Visited Network

The terminals and the visited network must support the same positioning method in order for location services to work effectively outside the home network. For services based on cell ID or enhanced cell ID levels of accuracy, this will not be an issue. However, for services based on the accuracy provided by E-OTD, OTDOA or A-GPS, it cannot be assured that the service will be available whilst roaming.

Furthermore, there are numerous options for the implementation of these accurate positioning methods, especially A-GPS. This could lead to difficulties when roaming. The consequences could be either that the service will not work (e.g. an A-GPS handset-based terminal in a network that only supports handset-assisted modes), or wide performance variations (e.g. differing amounts of GPS assistance leading to differing time-to-first-fix). A further issue might be the optional use of either broadcast or dedicated signalling for assistance data.

Whilst such issues may be resolved over time, operators will need to exercise caution when considering roaming for services which are based on these handset dependent technologies.

4.10.2 Handset-Based and Handset Assisted Positioning Modes

The GSM and UMTS specifications for E-OTD/OTDOA and for A-GPS specify two modes of operation. Firstly are the handset-based modes, where the position calculation function is carried out in the handset, then sent back to the network. Second is the handset-assisted mode, where the terminal makes only measurements, and reports these back to the network SMLC node, which calculates the handset position. These modes are shown below in

Figure 4-4 and in Figure 4-5.

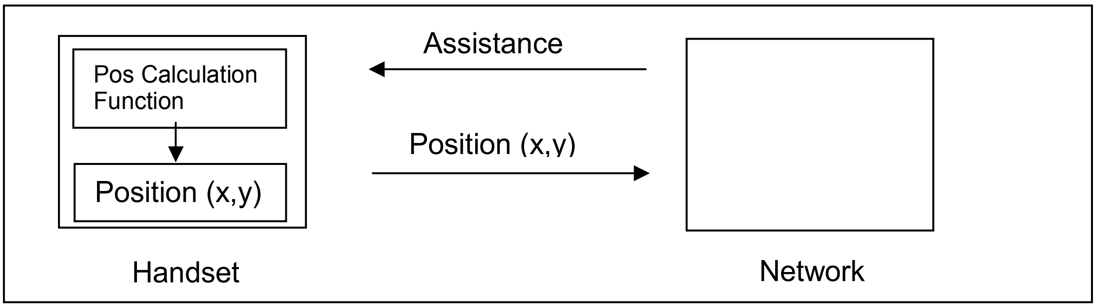


Figure 4-4 Handset-Based Mode

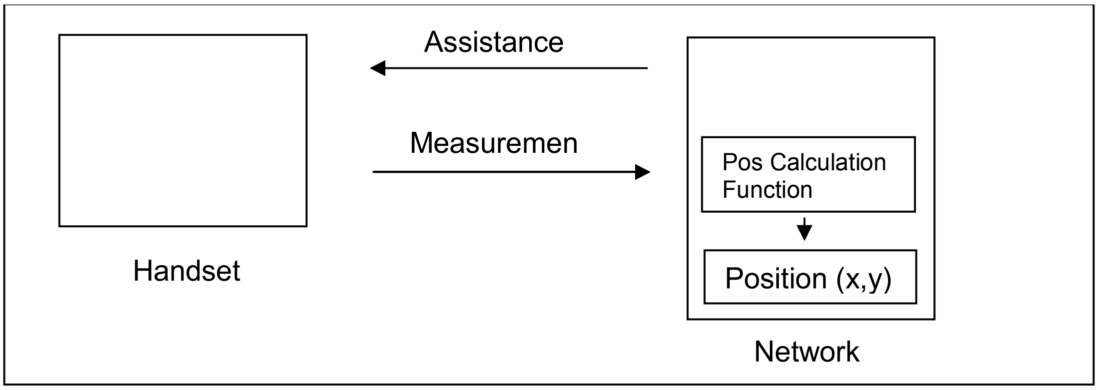


Figure 4-5 Handset-Assisted Mode

Whilst both modes are available in the standards, many GSM operators have expressed a clear desire to support only handset-assisted modes. The reason for this is clear – with handset-assisted modes the location is not stored in the terminal, and so remains secure in the network. With handset-based modes, storing the location in the terminal, there exists a significant security risk as third-parties could access the subscribers location from the handset. This presents a privacy threat to the subscriber.

For E-OTD and OTDOA, most practical implementations will be handset-assisted, but for A - GPS many terminal implementations may be capable of operating in either mode. Furthermore GSM infrastructure providers and terminal suppliers have been prioritising handset-based modes, over handset-assisted modes.

SerG recommends that GSM operators support only handset-assisted modes of A-GPS.

4.10.3 Risks of Java to Location Security/Privacy

There are two possible LBS related issues relating to the use of Java code running on mobile handsets.

The first is that a Java Location API might enable a Java Applet to access location information from the handset without any interaction with the location infrastructure that the operator has deployed. This raises serious concerns about privacy and security. GSM A SerG has taken action to request that the JCP specify that the Java Location API will make use of the mechanisms defined by 3GPP.

The second risk is that a “rogue” application exploits the stored location on the terminal that was stored there as a result of legitimate (and 3GPP compliant) application usage. This risk again could severely impact on the customers' privacy and security. The terminal manufacturers should ensure that any location data stored on the terminal as a result of legitimate location service is not accessible by any application that has not been properly authenticated. Of course, such risks are not present if the terminal does not alone have access to the location, i.e. if the terminal is used in Handset-Assisted Mode.

4.10.4 Handset Functional Variations

Operators should also note that consistent behaviour of terminals is not always guaranteed when using some LCS methods. Of particular importance are;

- Variable performance of GPRS terminals in receiving circuit-switching paging messages for LCS when active in a GPRS data session.
- Not all handsets responding correctly on reception of SMS Type 0 paging for the ATI method.
- Variable support of SMS SIM Toolkit functions which might be used for LCS.

5. Single Network Operation

5.1 General

These scenarios cover the cases where only one network is involved. The network is the home network of both the Requestor and the Target. Where the Requestor and Target are shown as separate users, clearly these may be the same.

5.2 Requestor is Target, Pull

For this scenario the Requestor accesses an LBS which needs to find the location of the same subscriber (Requestor) at the time of access. This includes cases such as “find my nearest …”.

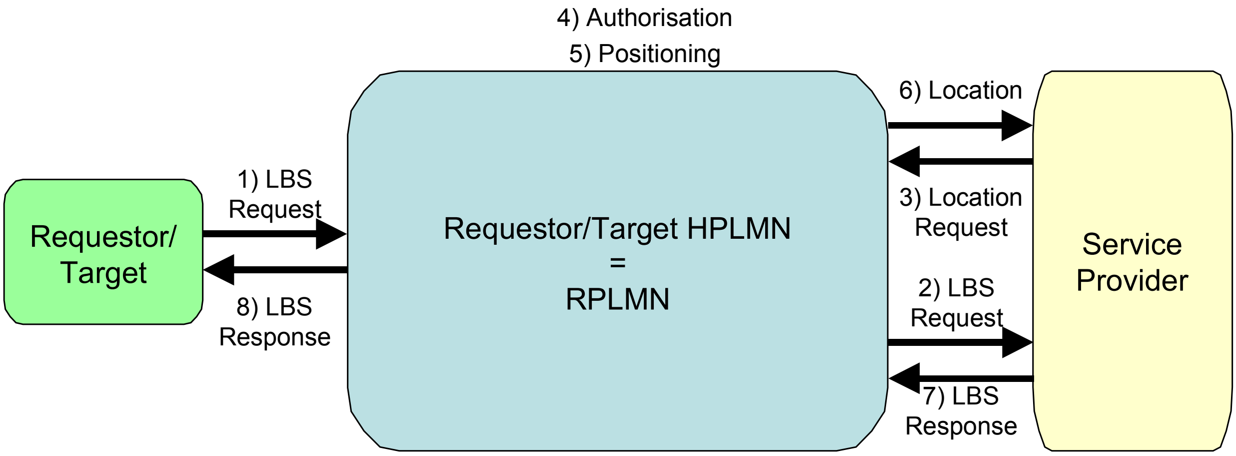


Figure 5-1 Requestor is Target, Pull

Table 5-1 Message flow in Figure 5-1

	Step	Description
1, 2.	LBS Request	Requestor requests service
3.	Location Request	Service Provider requests location of Target
4.	Authorisation	Target HPLMN authorises positioning for this service
5.	Positioning	Target VPLMN positions subscriber
6.	Location	Location reply to Service Provider
7, 8.	LBS Response	Service Provider returns result

5.3 Requestor is Not Target, Pull

For this scenario the Requestor accesses an LBS which needs to find the location a different subscriber (Target) at the time of access. This includes cases such as “buddy finder”.

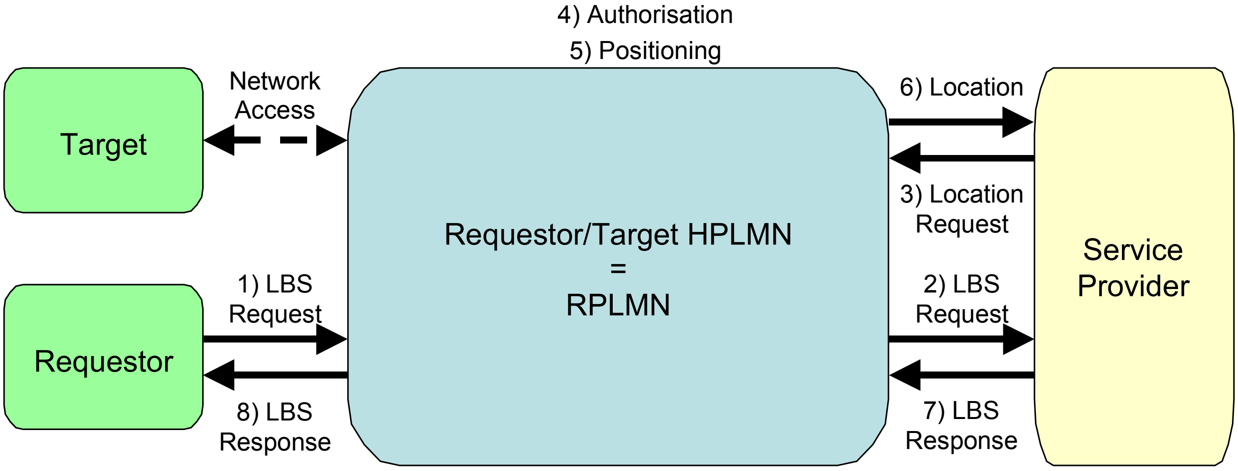


Figure 5-2 Requestor is Not Target, Pull

Table 5-2 Message flow in Figure 5-2

	Step	Description
1, 2.	LBS Request	Requestor requests service
3.	Location Request	Service Provider requests location of Target
4.	Authorisation	Target HPLMN authorises positioning for this service
5.	Positioning	Target VPLMN positions subscriber
6.	Location	Location reply to Service Provider
7, 8.	LBS Response	Service Provider returns result

5.4 Push

For this scenario the LBS provides the Requestor with information based on the location of the Target. This includes cases such as “local weather every morning” or “tell me when he gets to…”.

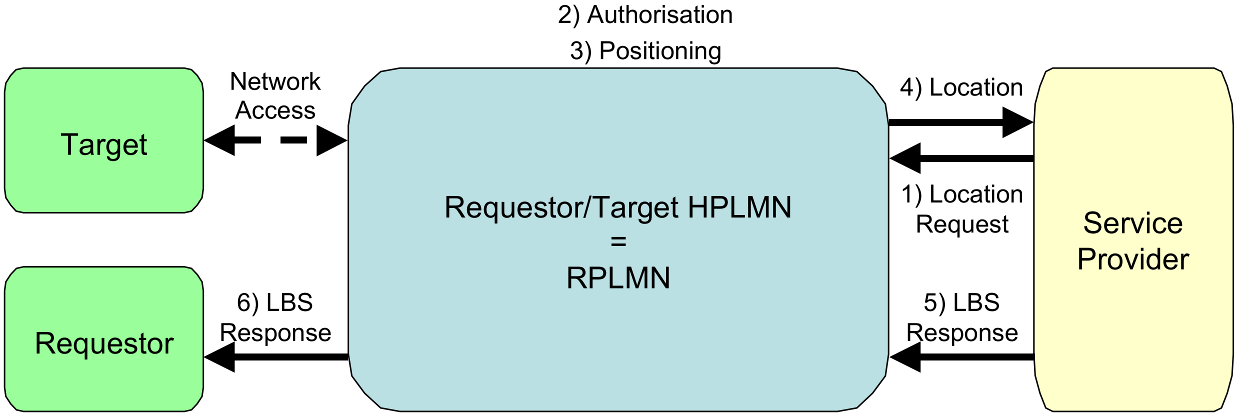


Figure 5-3 Push

Table 5-3 Message flow in Figure 5-3

	Step	Description
1.	Location Request	Service Provider requests location of Target
2.	Authorisation	Target HPLMN authorises positioning for this service
3.	Positioning	Target VPLMN positions subscriber
4.	Location	Location reply to Service Provider
5, 6.	LBS Response	Service Provider returns result

5.5 Tracking

For this scenario the Requestor accesses an LBS which provides ongoing reports on the location of the Target. This includes cases such as “asset tracking”.

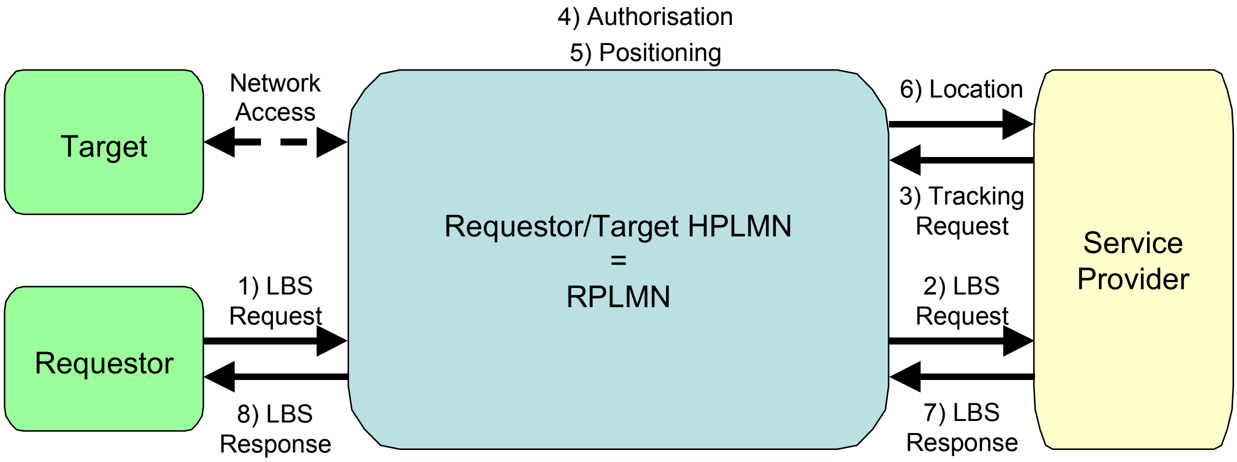


Figure 5-4 Tracking

Table 5-4 Message flow in Figure 5-4

	Step	Description
1, 2	LBS Request	Requestor requests service
3.	Tracking Request	Service Provider requests tracking of Target
4.	Authorisation	Target HPLMN authorises tracking for this service
5.	Positioning	Target VPLMN positions subscriber
6.	Location	Location reply to Service Provider
7, 8.	LBS Response	Service Provider returns result

Note: While tracking is active part of this sequence will be repeated, based on tracking criteria. If the Target HPLMN supports tracking, this would normally be steps 4-7. If the Target HPLMN does not support tracking, step 3 will need to be a standard Location Request and steps 3-7 will need to be repeated.

5.6 Mobile Originated Request

For this scenario the Target mobile needs to find its own location. This may be for its own use (e.g. a SIM based application) or to provide it to an LBS (e.g. to report when an event occurs). Note that security of the location information in this case must be considered, as discussed in chapter 4. A further point here is charging. Presumably the VPLMN charges the Target for the location.

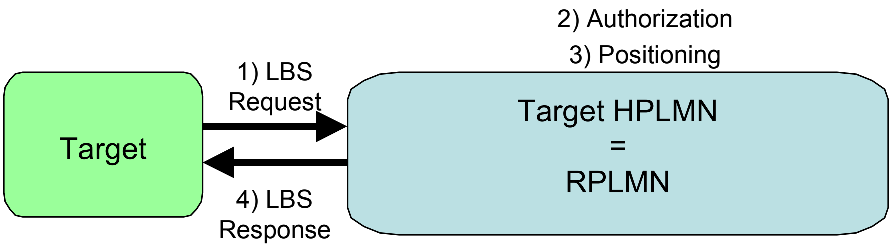


Figure 5-5 Mobile Originated Request

Table 5-5 Message flow in Figure 5-5

	Step	Description
1.	LBS Request	Target requests own location
2.	Authorisation	Target HPLMN authorises positioning for this service
3.	Positioning	Target VPLMN positions subscriber
4.	LBS Response	Location reply to Target

6. Inter-network Operation

6.1 General

These scenarios build on the scenarios of section 5, covering the cases where more than one network is involved, where the Requestor and the Target are on different HPLMNs.

6.2 Service Hosted On Requestor's HPLMN

For this scenario the Requestor accesses an LBS based on its HPLMN, which needs to find the location of the Target (on a different network) at the time of access. This includes cases such as "buddy finder".

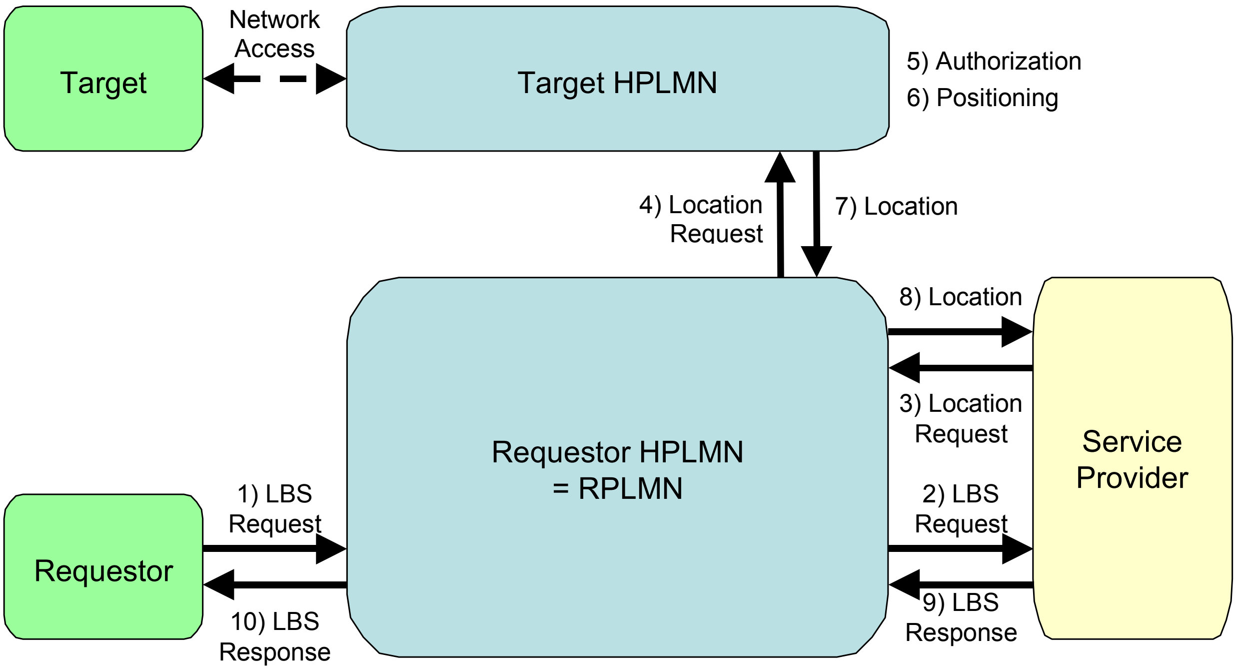


Figure 6-1 Service Hosted On Requestor's HPLMN

Table 6-1 Message flow in Figure 6-1

	Step	Description
1, 2.	LBS Request	Requestor requests service
3, 4.	Location Request	Service Provider requests location of Target
5.	Authorisation	Target HPLMN authorises positioning for this service
6	Positioning	Target VPLMN positions subscriber
7, 8.	Location	Location reply to Service Provider
9, 10.	LBS Response	Service Provider returns result

6.3 Service Hosted On Target's HPLMN

For this scenario the Requestor accesses an LBS based on the Targets HPLMN, which needs to find the location of the Target (on a different network) at the time of access.

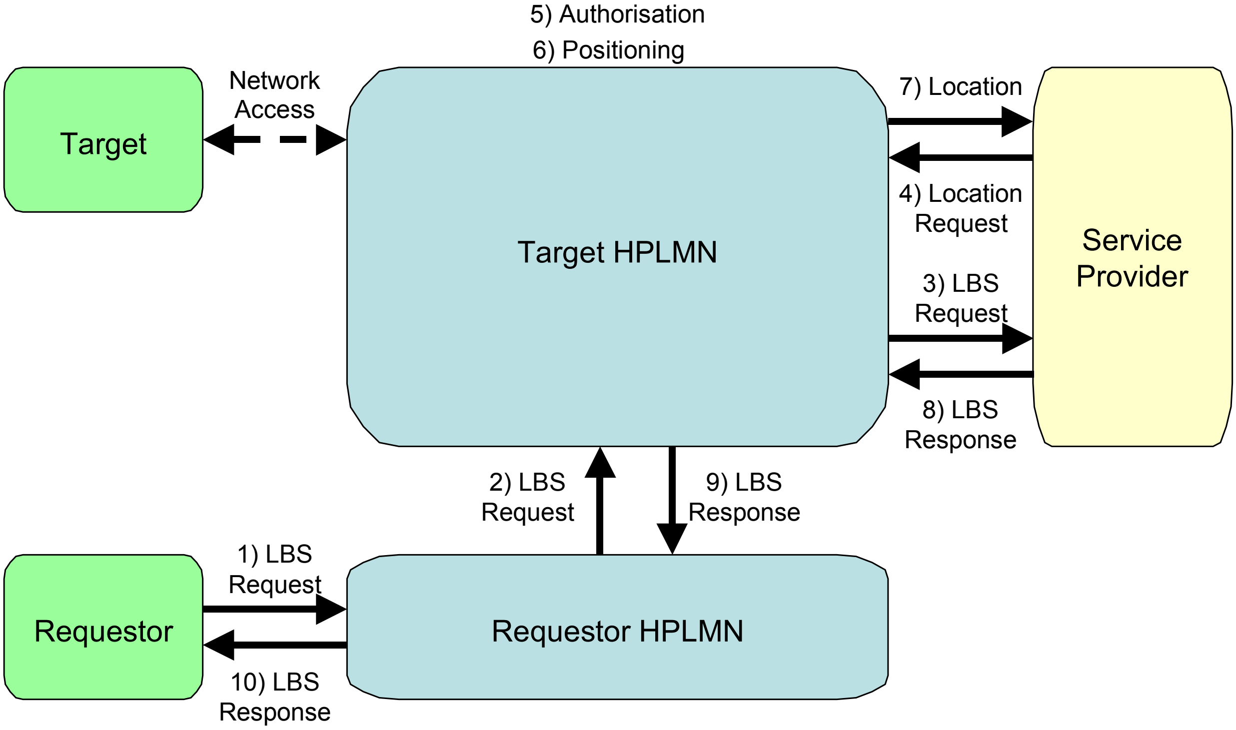


Figure 6-2 Service Hosted On Target's HPLMN

Table 6-2 Message flow in Figure 6-2

	Step	Description
1-3.	LBS Request	Requestor requests service
4.	Location Request	Service Provider requests location of Target
5.	Authorisation	Target HPLMN authorises positioning for this service
6.	Positioning	Target VPLMN positions subscriber
7.	Location	Location reply to Service Provider
8-10.	LBS Response	Service Provider returns result

6.4 Service Hosted On Third Party Network

For this scenario the Requestor accesses an LBS based on an independent network, which needs to find the location of the target on a different network. While this may not be normal, it could be the case when accessing an independent Service Provider which makes use of a third party network for network access. This is equivalent to an internet Service Providers offering SMS to all networks via a single network.

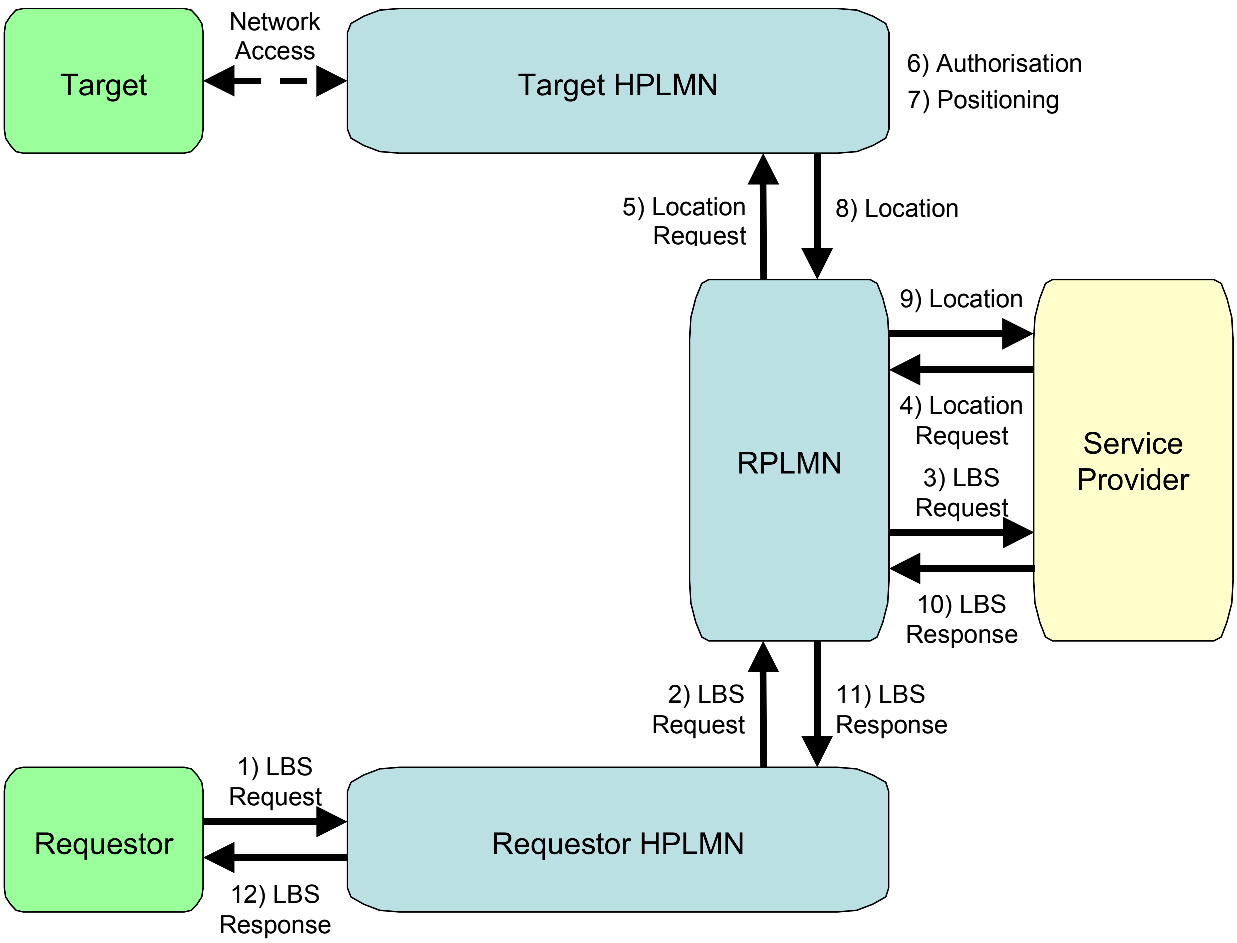


Figure 6-3 Service Hosted On Third Party Network

Table 6-3 Message flow in Figure 6-3

	Step	Description
1-3.	LBS Request	Requestor requests service
4, 5.	Location Request	Service Provider requests location of Target
6.	Authorisation	Target HPLMN authorises positioning for this service
7.	Positioning	Target VPLMN positions subscriber
8, 9.	Location	Location sent to Service Provider

10-12	LBS Response	Service Provider returns result

7. Roaming

7.1 Roaming and Interoperability Issues

It is important that any location-based service can be shown to operate across boundaries of network operators in the roaming case. This means that Interoperability test cases will need to be defined for each service. The Enablers will normally be defined by standards, so interoperability at this level is easier. It is at the Feature level that the interoperability problems will occur. It is the intent of this document to define features in such a way that they can be implemented by a vendor in their own preferred way, whilst still retaining the required functionality. It will therefore be necessary for test cases to be written which check the functionality of the features used.

A good example is the Mediation Device. The MD can be considered as an optional network element with the scope of protecting the client's sensitive data. The vision of the MD in this PRD is of an internal node that will handle the security issue. How this will be implemented is outside the scope of this document, but any implementation must support the abilities to perform the features of creating and decoding Opaque ID's, and authorising the release of Location information on a specific user to a specific 3rd party.

The overall aim is that a document can be written in such a way as to define the required functionality, and that vendors can test their implementations and indicate conformance to that document.

These scenarios build on the scenarios of sections 5 and 6, covering the cases where the Requestor and/or the Target is roaming. In all cases the Requestor and Target are shown as separate. Clearly these may be the same.

7.2 Purpose of the Chapter

Location based services where one or both of the subscribers concerned are roaming. The roaming of location based services is more complicated than the roaming of voice calls and SMS. The complexity arises from the fact that there may be very many parties involved in each location based service process. The roles of different parties as well as the general roaming process are described in this chapter.

7.3 Service Hosted on Requestor's HPLMN

For this scenario the Requestor accesses an LBS based on its HPLMN, which needs to find the location of the Target (on a different network) at the time of access.

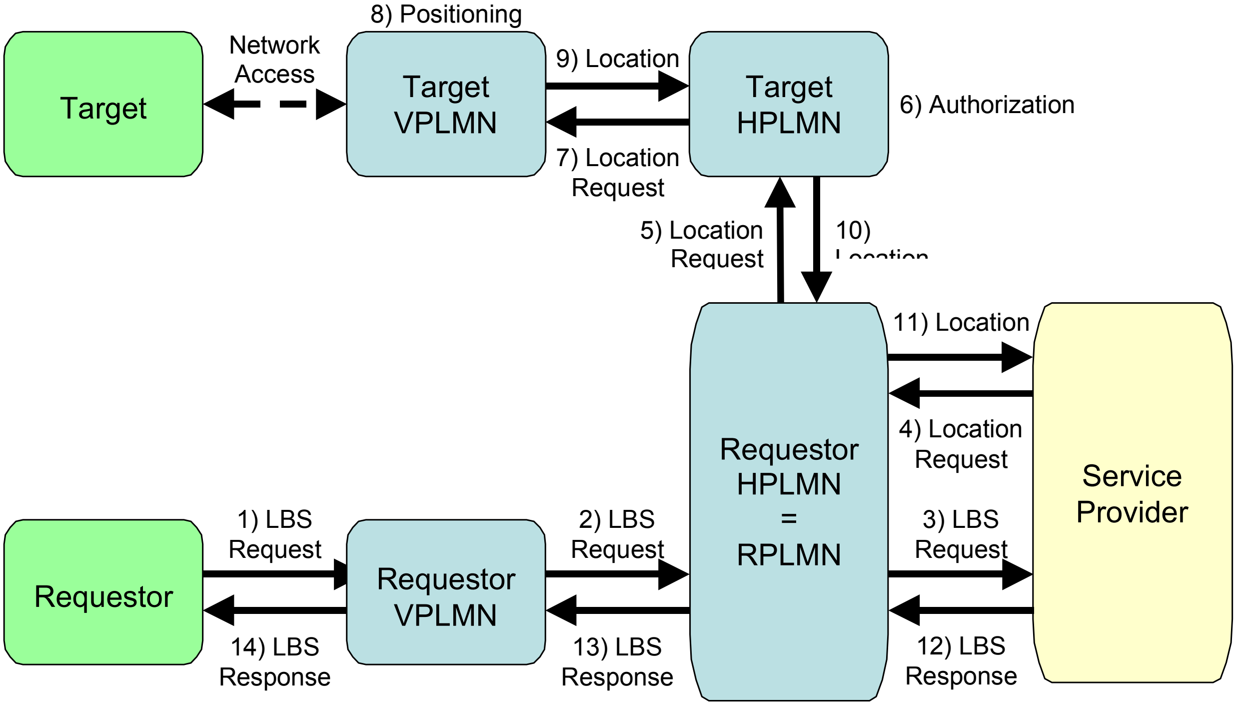


Figure 7-1 Service Hosted on Requestor's HPLMN

Table 7-1 Message flow in Figure 7-1

	Step	Description
1-3.	LBS Request	Requestor requests service
4, 5.	Location Request	Service Provider requests location of Target
6.	Authorisation	Target HPLMN authorises positioning for this service
7.	Location Request	Location Request to Target's VPLMN
8	Positioning	Target VPLMN positions subscriber
9-11.	Location	Location reply to Service Provider
12-14.	LBS Response	Service Provider returns result

7.4 Service Hosted on Requestor's VPLMN

For this scenario the Requestor accesses an LBS based on its VPLMN, which needs to find the location of the Target (on a different network) at the time of access.

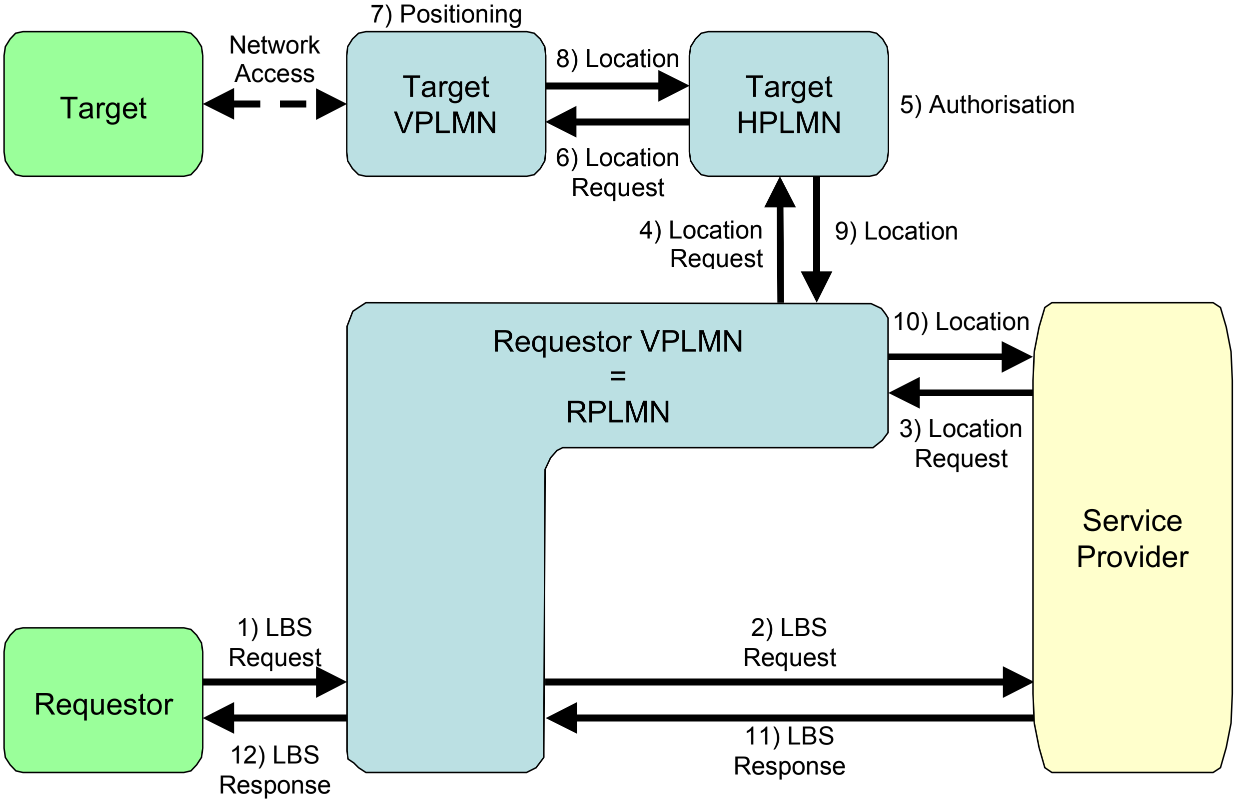


Figure 7-2 Service Hosted on Requestor's VPLMN

Table 7-2 Message flow in Figure 7-2

	Step	Description
1, 2.	LBS Request	Requestor requests service
3, 4.	Location Request	Service Provider requests location of Target
5.	Authorisation	Target HPLMN authorises positioning for this service
6.	Location Request	Location Request to Target's VPLMN
7.	Positioning	Target VPLMN positions subscriber
8-10.	Location	Location reply to Service Provider
11, 12.	LBS Response	Service Provider returns result

7.5 Service Hosted on Target's HPLMN

For this scenario the Requestor accesses a service that can directly access the Target's HPLMN.

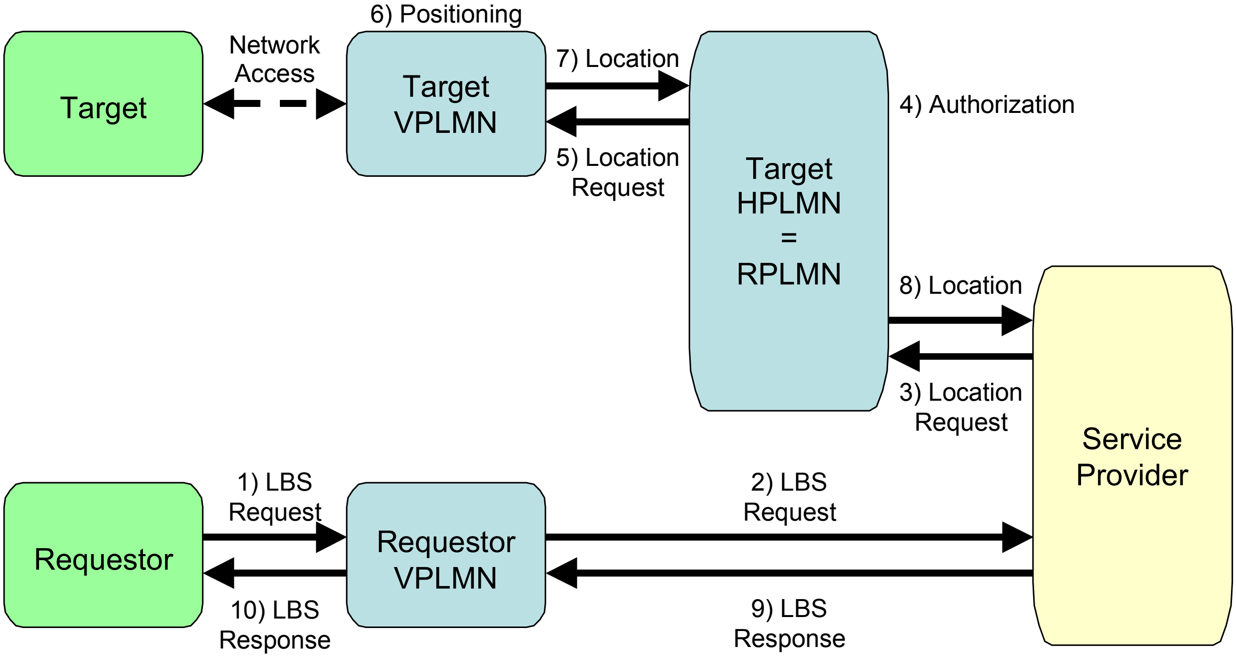


Figure 7-3 Service Hosted on Target's HPLMN

Table 7-3 Message flow in Figure 7-3

	Step	Description
1, 2.	LBS Request	Requestor requests service
3.	Location Request	Service Provider requests location of Target
4.	Authorisation	Target HPLMN authorises positioning for this service
5.	Location Request	Location Request to Target's VPLMN
6.	Positioning	Target VPLMN positions subscriber
7, 8.	Location	Location reply to Service Provider
9, 10.	LBS Response	Service Provider returns result

7.6 Service Hosted on Target's VPLMN

For this scenario the Requestor accesses a service which uses the Target's VPLMN to request the location.

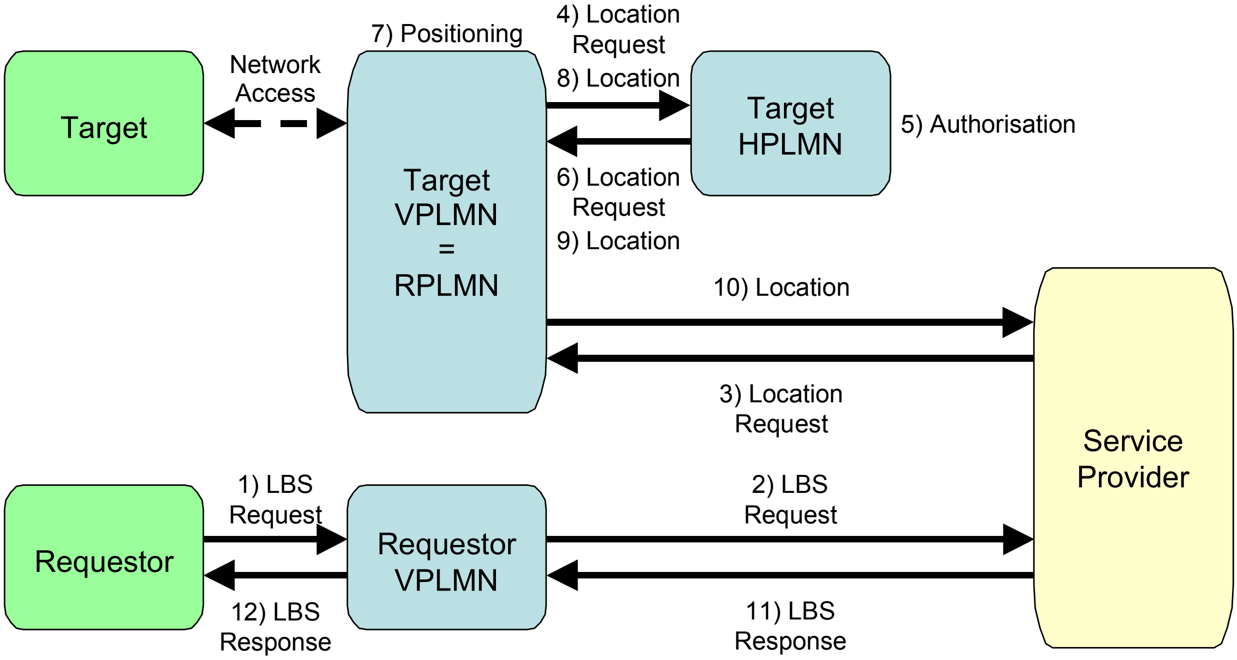


Figure 7-4 Service Hosted on Target's VPLMN

Table 7-4 Message flow in Figure 7-4

	Step	Description
1, 2.	LBS Request	Requestor requests service
3, 4.	Location Request	Service Provider requests location of Target
5.	Authorisation	Target HPLMN authorises positioning for this service
6.	Location Request	Location Request to Target's VPLMN
7.	Positioning	Target VPLMN positions subscriber
8-10.	Location	Location reply to Service Provider
11, 12.	LBS Response	Service Provider returns result

In this case it would be possible for the VPLMN/RPLMN to simply request authorisation from the Target HPLMN, rather than pass the location request and the location via the HPLMN. However, by passing these through the HPLMN, it allows the HPLMN to authorise the location as well as the request (not currently shown) and reduces the complexity of needing to be aware of which method to use. This is at the cost of the additional signalling.

7.7 Tracking, Service Hosted on Requestor's HPLMN

For this scenario the Requestor accesses an LBS which provides ongoing reports on the location of the Target which the target is roaming.

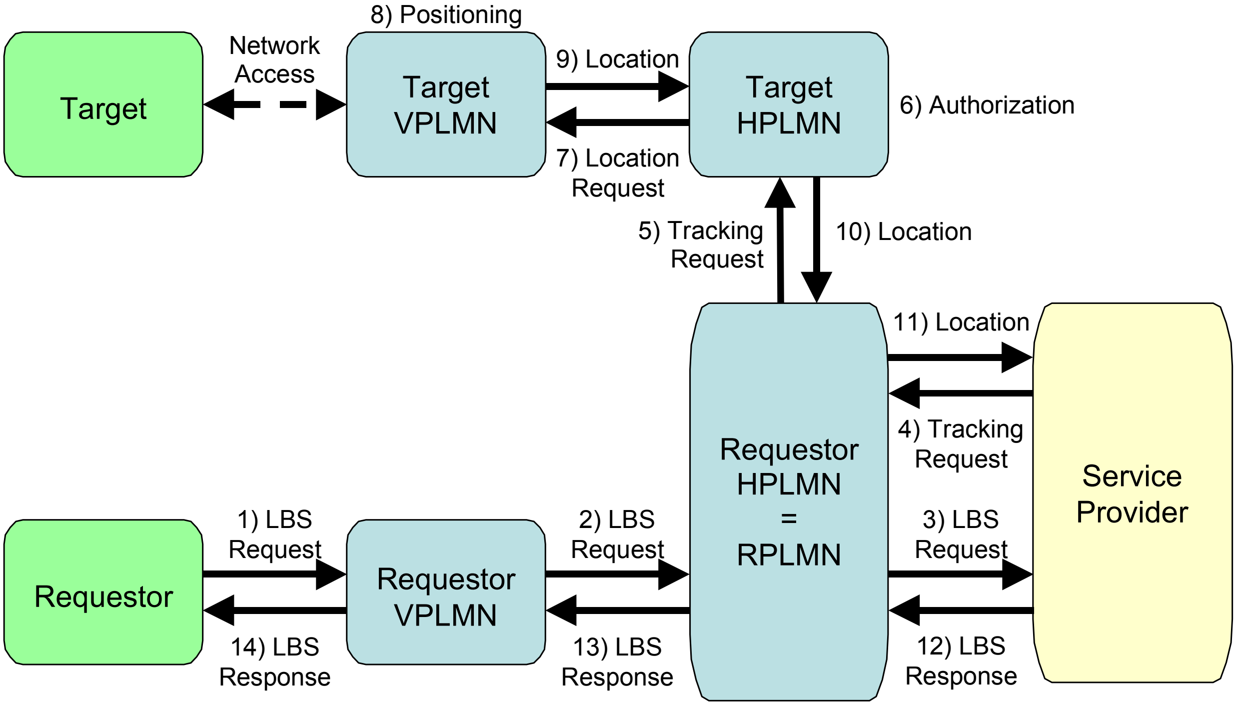


Figure 7-5 Tracking, Service Hosted on Requestor's HPLMN

Table 7-5 Message flow in Figure 7-5

	Step	Description
1-3.	LBS Request	Requestor requests service
4, 5.	Tracking Request	Service Provider requests tracking of Target
6.	Authorisation	Target HPLMN authorises positioning for this service
7.	Location Request	Location Request to Target's VPLMN
8.	Positioning	Target VPLMN positions subscriber
9-11.	Location	Location reply to Service Provider
12-14.	LBS Response	Service Provider returns result (If required)

Tracking is centred on the Target HPLMN. The HPLMN authorises the tracking each time it polls the Target (repeating steps 6-13 each time), sending a standard location request to the VPLMN (marked as a tracking request for charging purposes). This automatically manages roaming, as it sends the request to the current VPLMN, rather than the one at the time of the request. It also supports any authorisation changes, as they are checked each time.

7.8 Mobile Originated Request

For this scenario the Target requests its own location. There is no separate Requestor involved.

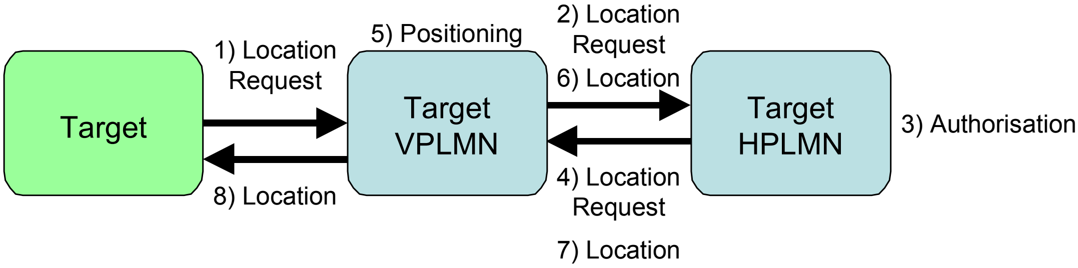


Figure 7-6 Mobile Originated Request

Table 7-6 Message flow in Figure 7-6

	Step	Description
1, 2.	Location Request	Target requests own location
3.	Authorisation	Target HPLMN authorises positioning for this service
4.	Location Request	Location Request to Target's VPLMN
5.	Positioning	Target VPLMN positions subscriber
6-8.	Location	Location reply to Target

As can be seen, the signalling follows the same route as when the service is hosted on the Target's VPLMN, be passing the request and response via the HPLMN. This could be done by simply sending an authorisation request, but the same arguments apply.

8. Conclusions

The objectives of this document were, firstly to provide an overview of where we are today, of what options are available for the operators and a possible way forward to a future development of the standards and secondly to guide the operators on how to inter-work in the absence of the technical standards.

Additions to the previous version of the document were Mobile Number Portability (MNP), charging consideration, privacy and anonymity aspects and terminal issues. The scenarios were redrawn in more general level in order to avoid technical details in the document.

The conclusion of this PRD is that the existing LCS standards (GSM 02.71 and GSM 03.71) do not provide enough features and functions to fulfil operators' demands for a secure interface and the needs of broad variety of possible services. The reasons for this are that privacy, roaming and charging related issues are not covered thoroughly.

Charging issues need to be studied furthermore in relevant groups within the GSMA.

Roaming cases would benefit from GMLC-GMLC interface since allowing other network operators to access the MSC could be risky.

Privacy issues can not be fully resolved in the HLR because it does not support sufficient number of user privacy profiles needed for different applications, which naturally limits the user's possibility to use a wide range of LBSs. There are also some implications that the privacy issue in a roaming scenario is complicated.

In these are the operator requirements for Location Based Services. Henceforward, further communication between the GSMA (SerG) and the standardising foras is advisable.

APPENDIX 1

Positioning Methods

Positioning technologies can be divided to three categories: basic, enhanced and advanced. Basic positioning methods are based on the use of cell identification (cell id). Cell id can be used alone, or together with timing advance (TA) and network measurement reports (NMR). Enhanced Observed Time Difference (E-OTD) is usually referred to as an enhanced positioning method. Assisted GPS (A-GPS) is an advanced positioning method.
The division of position technologies above is based on accuracy of the positioning method. Other factors, which are very important, are for example complexity of the system and the investment needed on the network side and possibly in handsets.

Table A1-1 Positioning methods

Level	***Method***	***Handset dependence***
Basic	CI, CI+TA, CI+TA+RX	No
Enhanced	E-OTD, TOA	Yes/No
Advanced	A-GPS	Yes

Cell ID

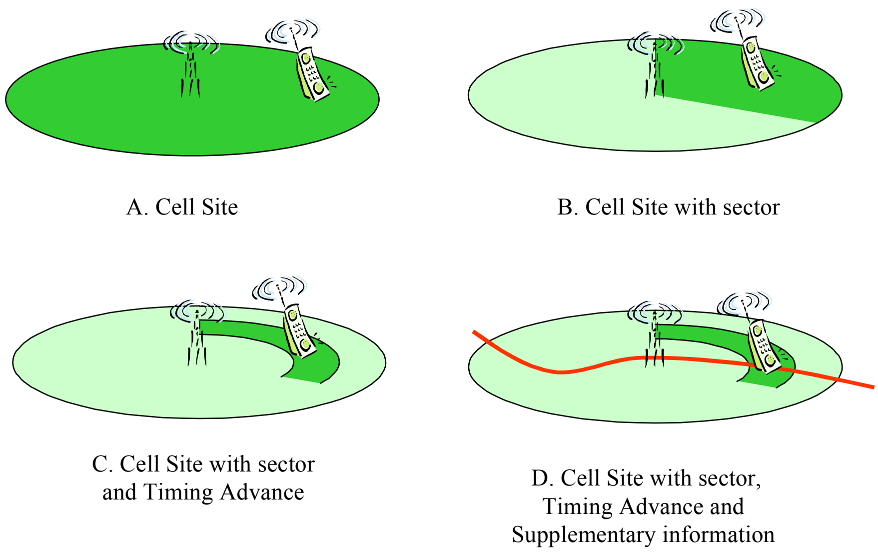


Figure A1-1 Cell ID positioning method.

In the Cell ID positioning method, the cell that the handset is connected to is the location 'measurement' of the handset's position. This information is available in the network and at the handset. The Cell ID is then converted to a geographic position using knowledge of the operator's network, e.g. coverage database at the SMLC.

Cell ID positioning can support all legacy handsets and roaming subscribers. Accuracy is of course dependent on cell size.

If available, Timing Advance (TA) can be used to improve performance. TA is a measure of the MS range from BTS (to a resolution of 50m resolution) and improves accuracy in some cases. Its main benefit is in identifying when an MS is not connected to nearest cell (e.g. congestion, umbrella cells).

It is expected that Cell ID + Round Trip Time (the analogy of TA) will give better performance in UMTS.

Table A1-2 Accuracy of Cell ID

Technology	Rural	Suburban	Urban	Indoor
Cell ID	Range 1km-35km Typically 15km Extreme ~100km	Range 1km-10km Typically 5km	Macrocells: Range 500m-5km Typically 2km Microcells: Range 50m-500m Typically 200m	If Pico cells are deployed typically 10m-50m
Cell ID + TA	TA gives no major improvements in accuracy. However, it is a good parameter to check whether a handset has connected to the nearest cell			

Enhanced CGI

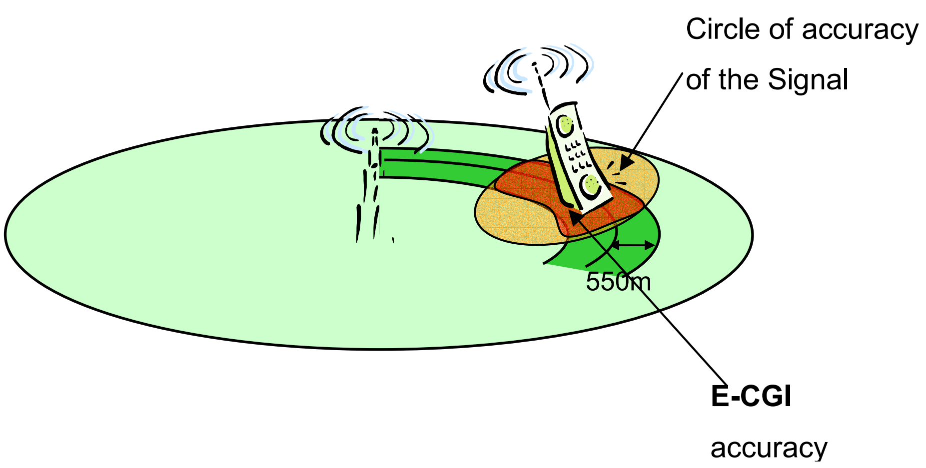


Figure A1-2 Enhanced CGI vs Cell ID.

In all cellular systems the handset will make measurements on the air interface, and send them to the network for hand-over decisions. In GSM these 'measurement reports' contain the estimated power level at the handset from the serving cell and the cells on the neighbour list. The power level measured at the handset can be used to estimate the BTS -MS distance, based upon simple propagation models and/or network planning tools.

Power measurements from adjacent sectors of the same cell site can provide an estimate of the angle of the MS from the site. Pattern recognition algorithms can be used with multiple measurement reports to give improvements in accuracy

Some points to note are that the accuracy is only as good as the prediction tool used and the radio environment is highly variable. Accuracy is also dependent on cell density, network configuration and environment. Field measurements will improve prediction tool accuracy and there may be methods of collecting such measurements when more accurate methods (e.g. A-GPS) are available – i.e. by requesting a position estimate and measurement report from an A-GPS handset. E-CGI performs poorly indoors and in rural areas with low BTS density.

A study is required to assess the performance of E-CGI in UMTS. There will be improvements due to soft handover mechanism but degradations due to the near-far problem.

Table A1-3 Accuracy of Enhanced CGI

Technology	Rural	Suburban	Urban	Indoor
E-CGI	250m-35km	250m-2.5km	50-550m	Highly variable
	More accurate than Cell ID + TA			

E-OTD

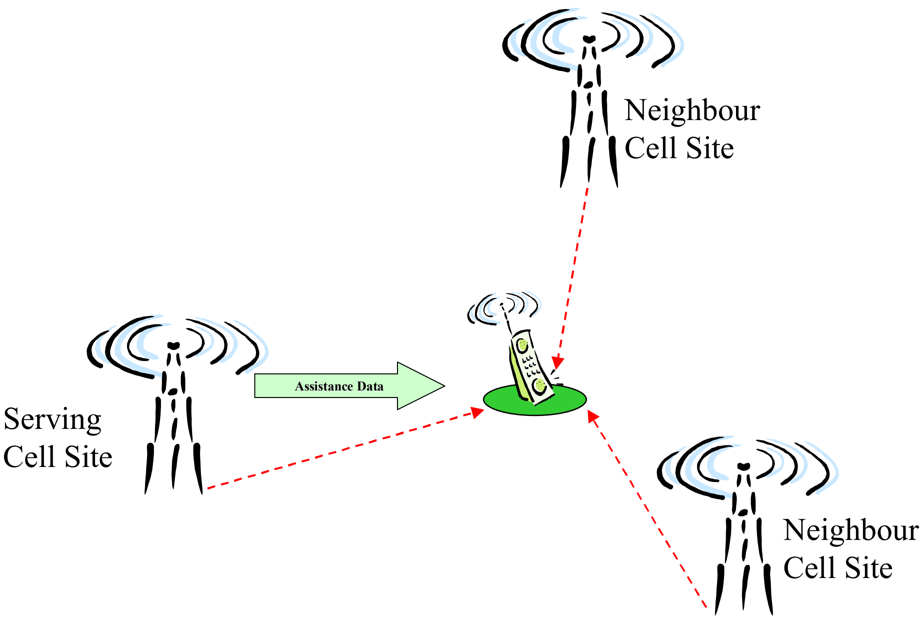


Figure A1-3 E-OTD.

E-OTD is a time based method, whereby the handset measures the arrival time of signals transmitted from 3+ BTSs. This time measurement capability of E-OTD is a new function in the handset. In MS assisted E-OTD the timing measurements made by the handset are then transferred to the SMLC using standardised LCS signalling. The measurements returned are related to the distance from each BTS to the MS and the position of the MS is estimated using triangulation. In MS based E-OTD, the position calculation function is in the handset and the position is returned to the SMLC.

The position of each BTS must be accurately known (<10m recommended) to perform triangulation and estimate the position of the handset. The transmission times of each BTS must also be accurately known to perform E-OTD. If the network is not synchronised, then BTS transmission time must be measured using a network of Location Measurement Units

(LMUs). LMUs are essentially modified mobiles, optionally with a GPS receiver, placed in a fixed position with the capability to perform E-OTD measurements and return them to the SMLC.

E-OTD accuracy is dependent on cell density, cell plan, multipath, interference, noise, LMU performance, cell site position accuracy. Accuracy does not degrade much indoors and E-OTD performs well in high BTS density areas. Conversely, E-OTD has poor performance in low BTS density areas

The E-OTD method in UMTS (Observed Time Difference Of Arrival - Idle Period Down Link – OTDOA-IPDL) still has technical issues to be solved before performance can be considered as good as E-OTD in GSM.

Table A1-4 Accuracy of E-OTD

Technology	Rural	Suburban	Urban	Indoor
E-OTD	50m-150m	50m-150m	50m-150m	Good
	Severe multipath and blocking may sharply degrade performance in difficult urban conditions. Poor performance in low BTS density areas such as rural environments. Will fall back to cell ID if method fails			

A-GPS

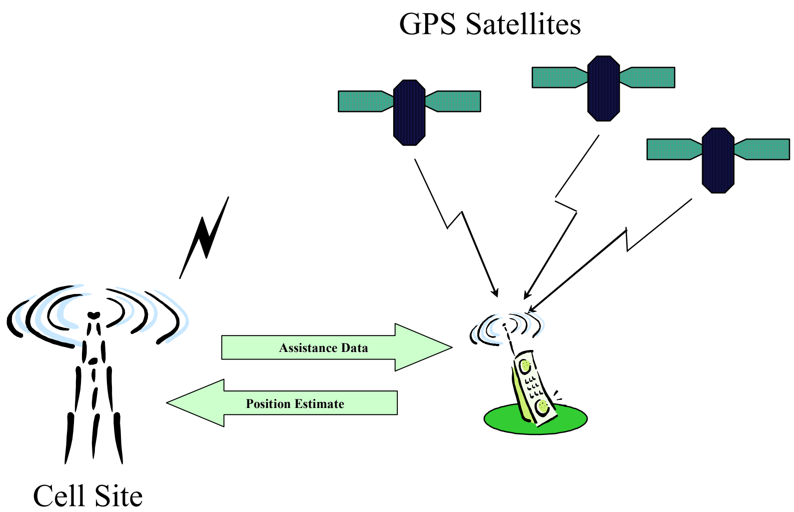


Figure A1-4 Assisted GPS.

A-GPS is a time based method, whereby the handset measures the arrival time of signals transmitted from 3+ GPS satellites. Adding GPS functionality has a high impact on the handset with new hardware and software required. Most implementations of A-GPS have a low impact on the network, requiring only support at the SMLC

In general, the information normally decoded by the GPS receiver from the satellites is transmitted to the MS via the radio network bringing improvements in Time to First Fix and

Battery Life – as the handset no longer needs to search for and decode the signals from each available satellite. Removing the need to decode the satellite signals also enables detection and time of arrival estimation over multiple bits bringing improvements in sensitivity i.e. A-GPS can provide position estimates

- Under Foliage
- In Car
- Most if not all outside environments
- Many indoor environments

A-GPS also provides good vertical accuracy and velocity estimates. Signalling of GPS assistance data to the MS may take 10s of seconds but once received by the handset, assistance data is useful for up to 4 hours.

There are toe implementations of A-GPS. MS assisted, whereby the measurements are passed back to the network for position calculation and MS based, whereby the position is calculated in the handset.

A-GPS is Radio Access Network independent so there is consistent performance in UMTS. Additionally, performance of A-GPS in UMTS is expected to improve.

Table A1-5 Accuracy of Assisted GPS

Technology	Rural	Suburban	Urban	Indoor
A-GPS	10m	10-20m	10-100m	Variable
	Still not proven in many indoor environments – will fall back to Cell ID if method fails.			

APPENDIX 2 - Detailed Scenarios

General Case

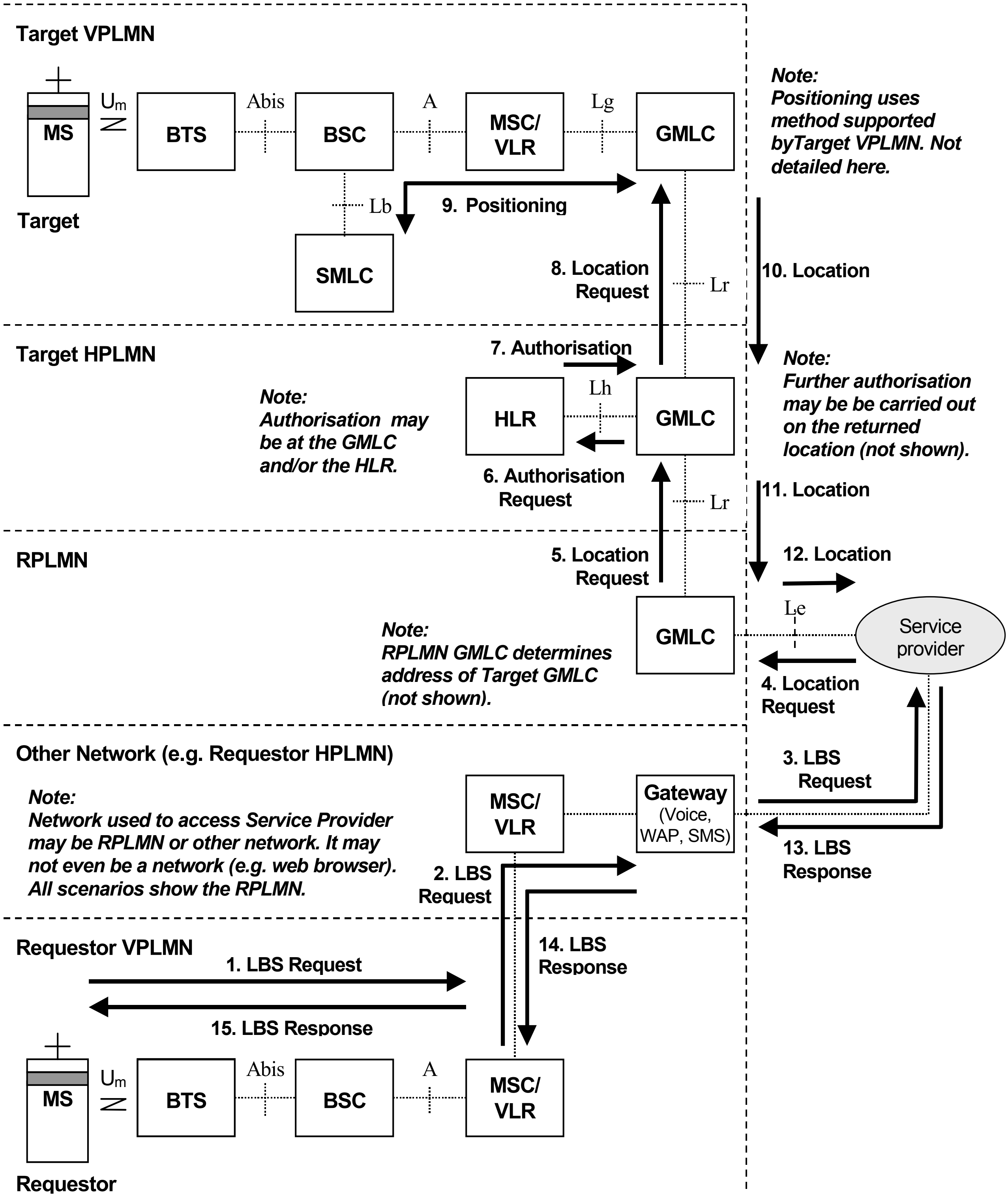


Figure A2- 1 General Case

Scenario 1: Single Network: Requestor is Target, Pull

Customer A on his own network asking for a location service.
Use case: Customer asking for localised weather service using home operator service.

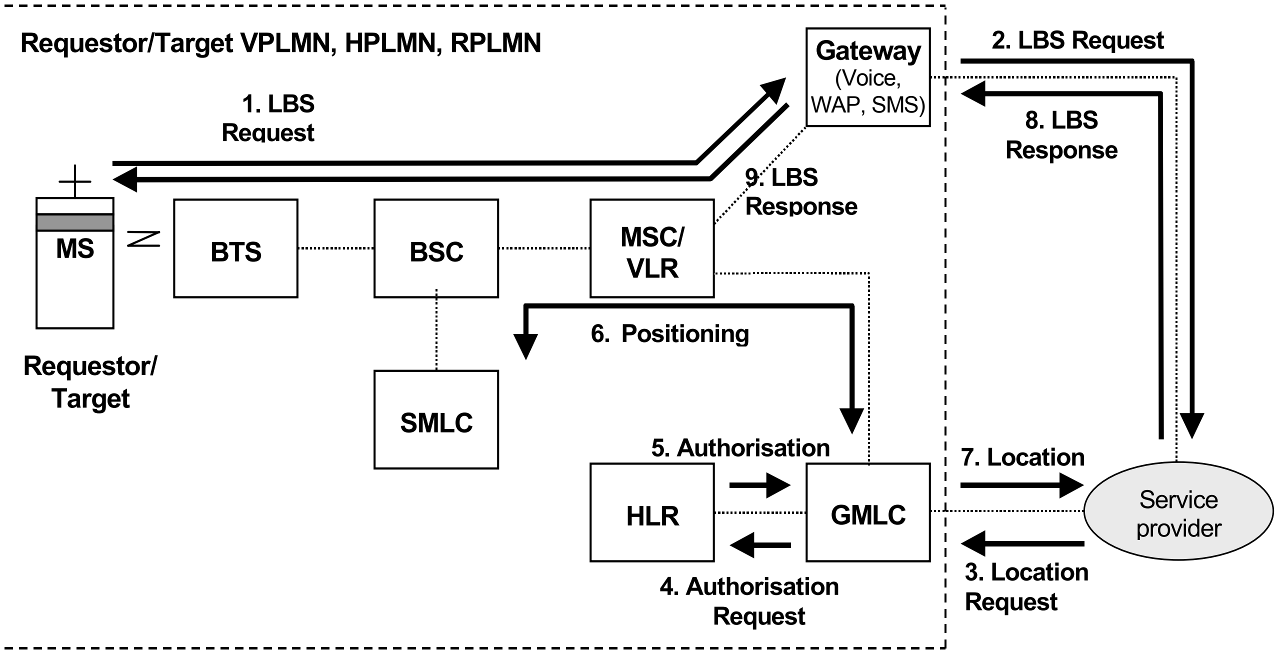


Figure A2- 2 Scenario 1: Single Network: Requestor is Target, Pull

Scenario 2: Single Network: Requestor is not Target, Pull

Customer A on his own network asking for a location service using the location of another subscriber.
Use case: Customer using buddy finder to locate friend.

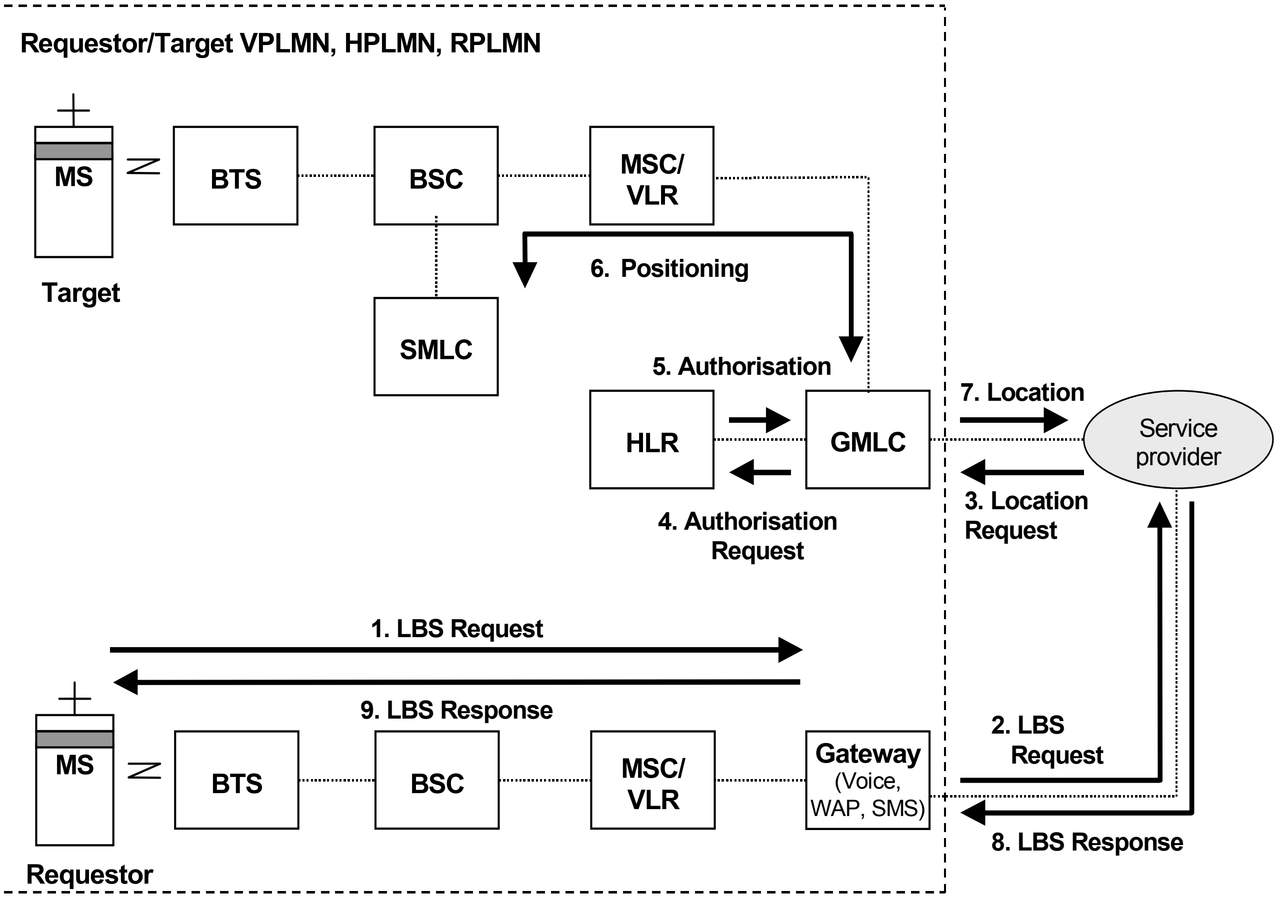


Figure A2- 3 Scenario 2: Single Network: Requestor is not Target, Pull

Scenario 3: Single Network: Push

Location services provides information to Customer A on his own network.
Use case: Customer asking for localised weather service using home operator service every morning.

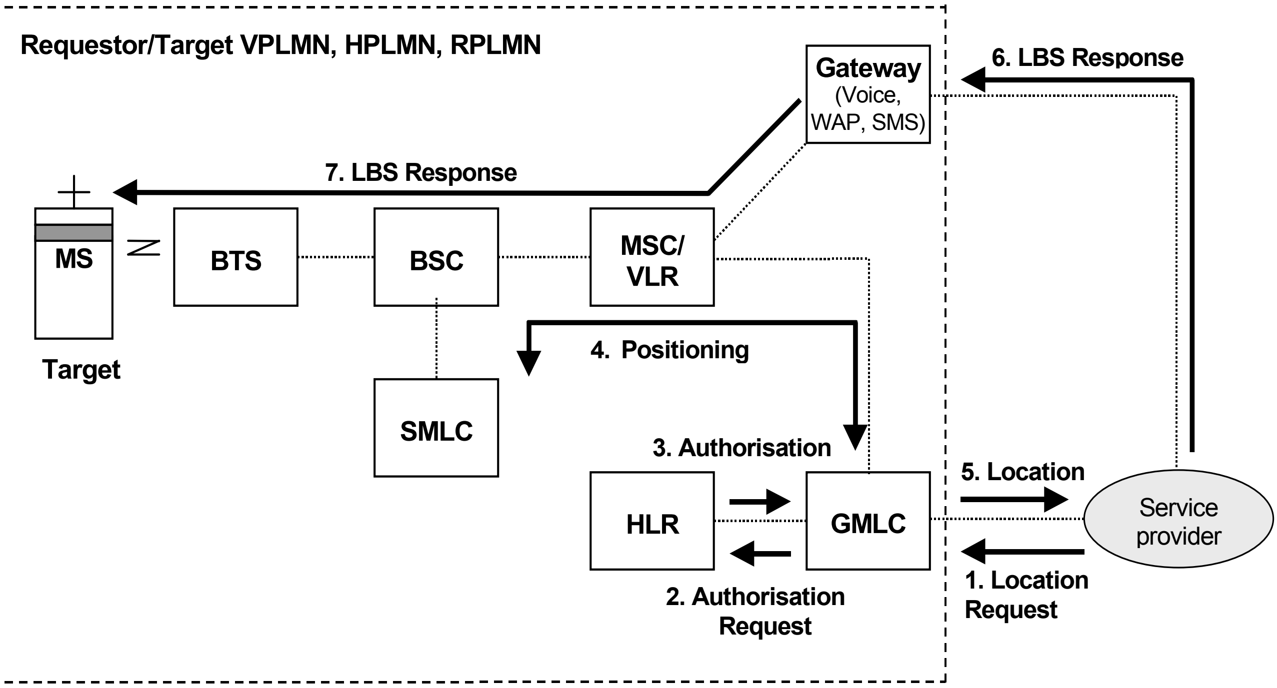


Figure A2- 4 Scenario 3: Single Network: Push

Scenario 4: Single Network: Tracking

Customer A on his own network asking for regular updates of location of subscriber B.
Use case: Asset tracking.

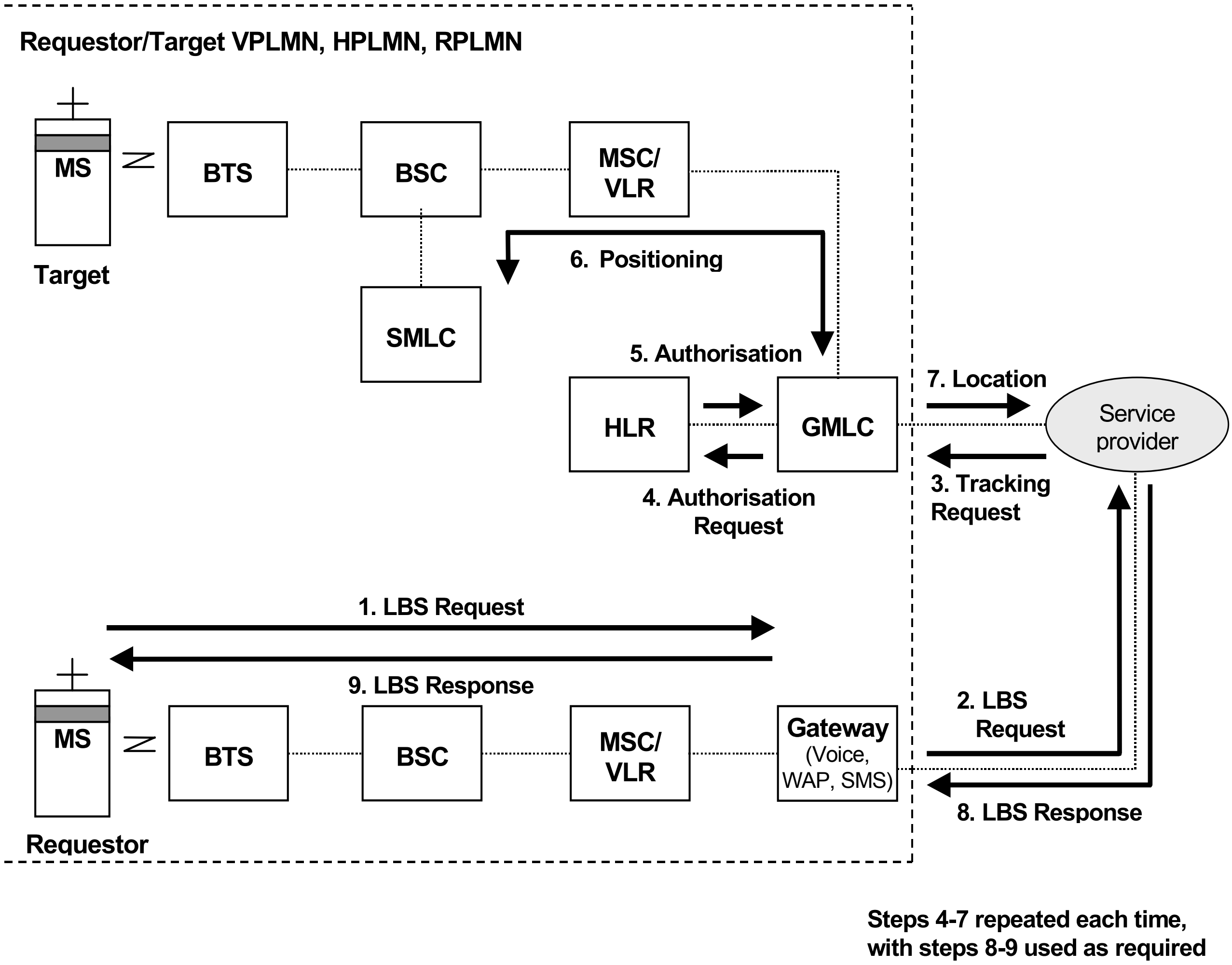


Figure A2- 5 Scenario 4: Single Network: Tracking

Scenario 5: Single Network: Mobile Originated Request

Customer (or handset/SIM application) asks for own location.
Use case: Local mapping.

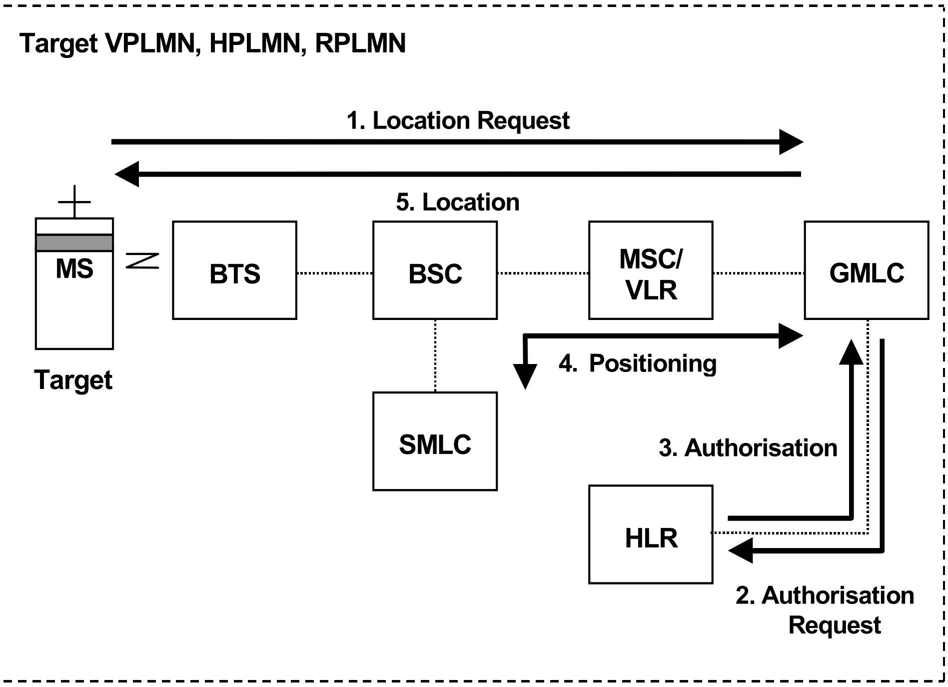


Figure A2- 6 Scenario 5: Single Network: Mobile Originated Request

Scenario 6: Inter-Operator: Service Hosted on Requestor's HPLMN

Customer A on network A asking a service hosted on network A for the location of customer B on network B.
Use case: Chris on SFR asks an SFR service for the location of Bob on Orange.

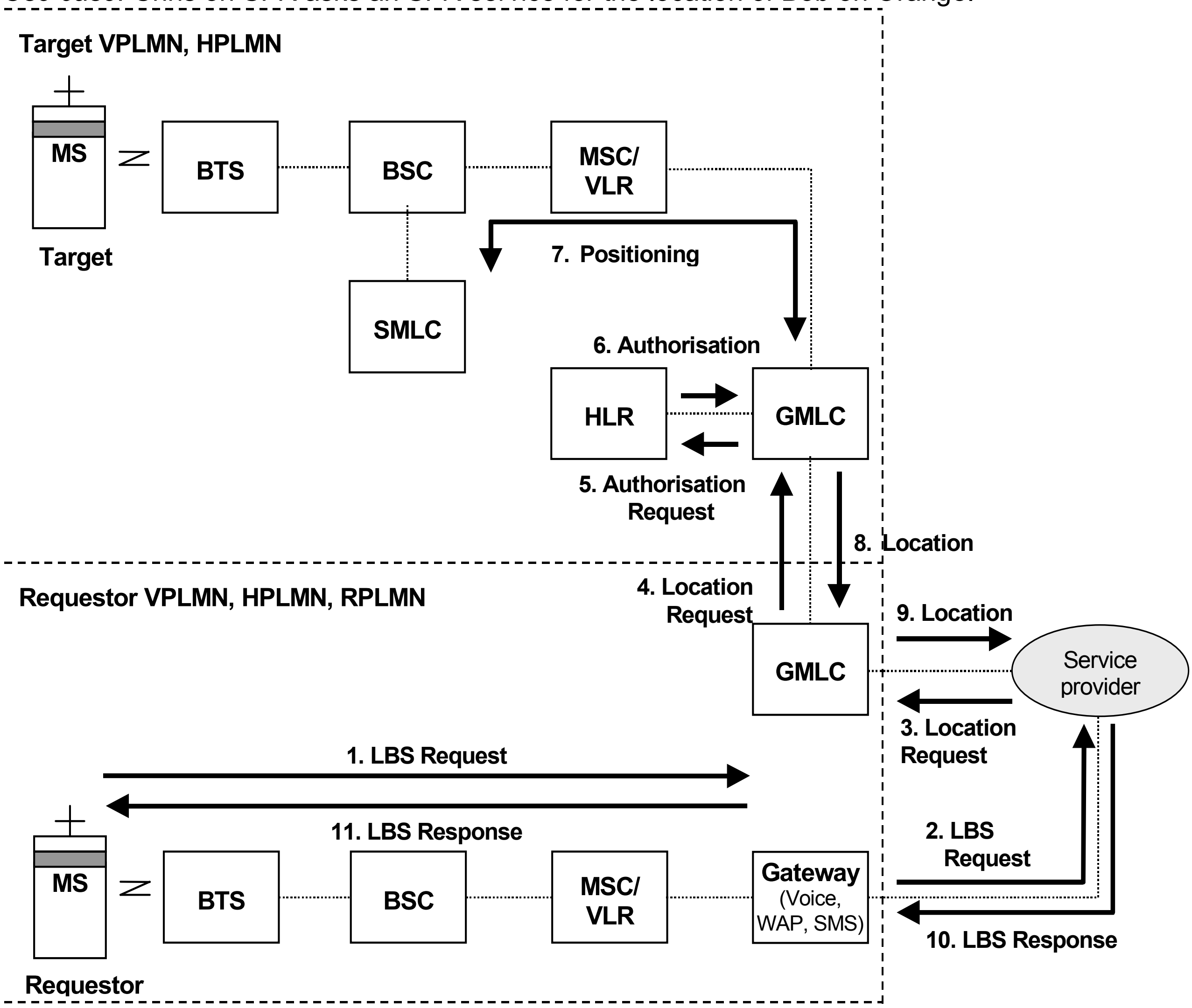


Figure A2- 7 Scenario 6: Inter-Operator: Service Hosted on Requestor's HPLMN

Scenario 7: Inter-Operator: Service Hosted on Target's HPLMN

Customer A on network A asking a service hosted on network B for the location of customer B on network B.
Use case: Chris on SFR asks an Orange service for the location of Bob on Orange.

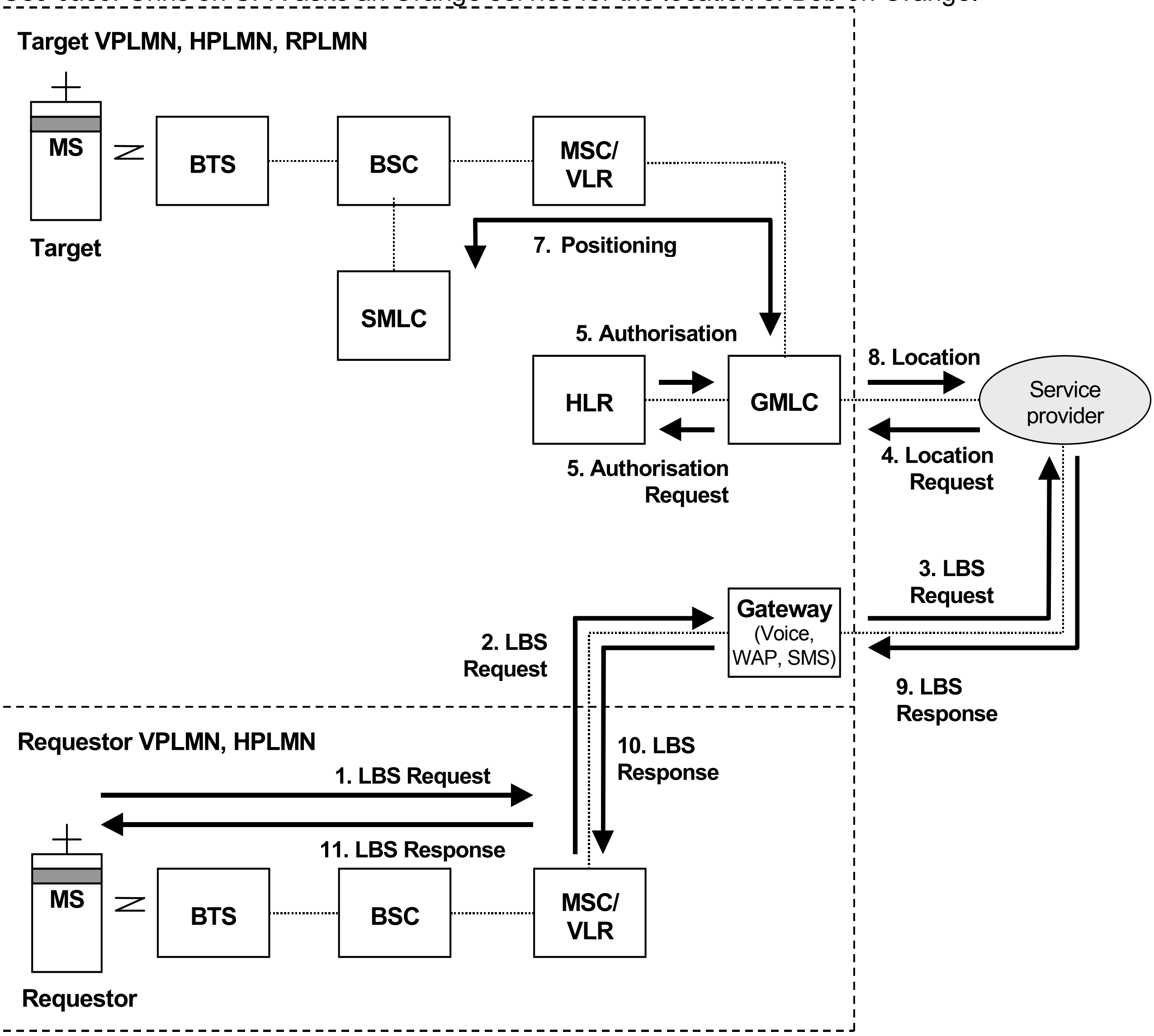


Figure A2- 8 Scenario 7: Inter-Operator: Service Hosted on Target's HPLMN

Scenario 8: Inter-Operator: Service Hosted on Third Party Network

Customer A on network A asking a service hosted on network C for the location of customer B on network B.
Use case: Chris on SFR asks a Bouygues service for the location of Bob on Orange.

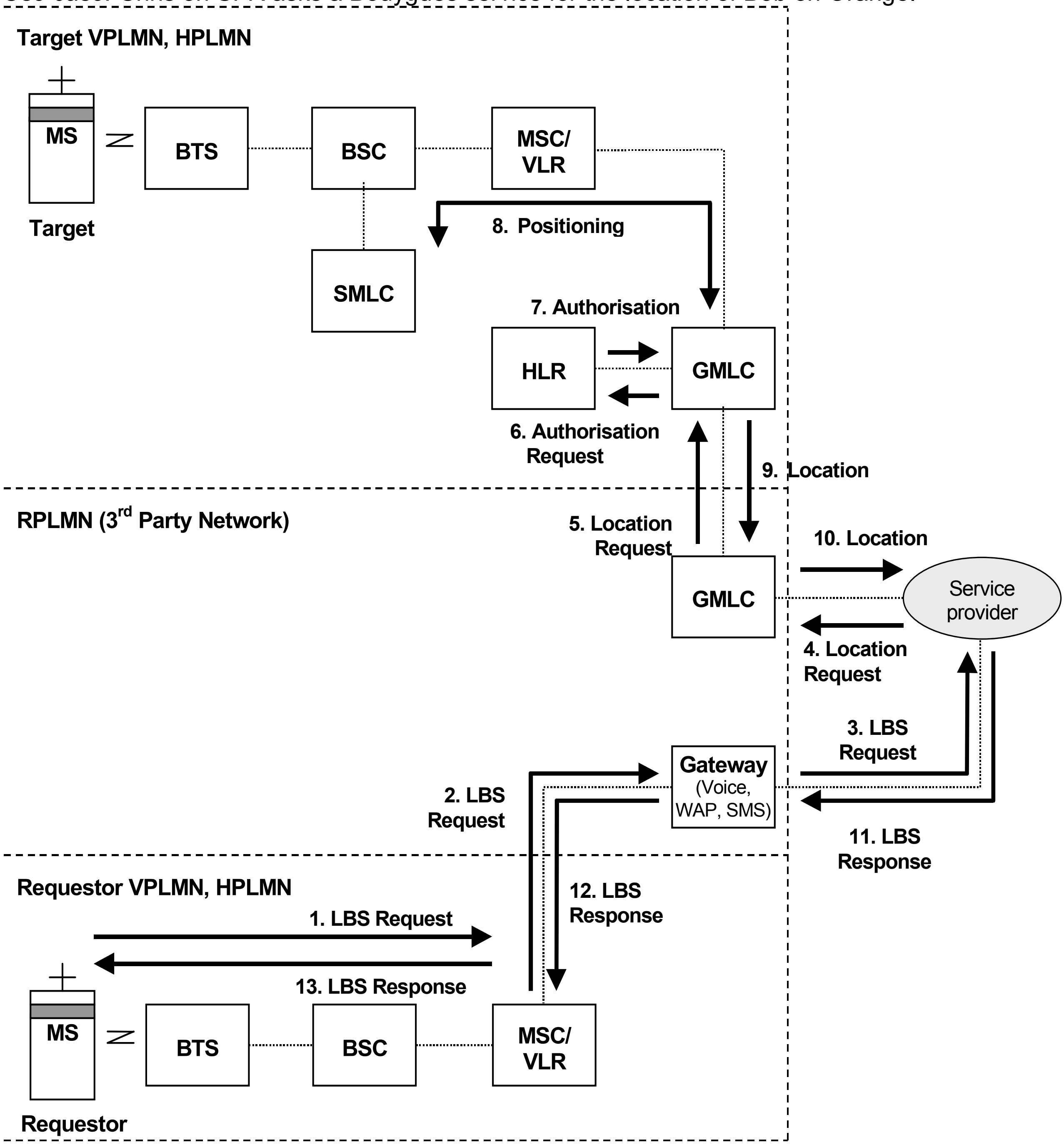


Figure A2- 9 Scenario 8: Inter-Operator: Service Hosted on Third Party Network

Scenario 9: Roaming: Service Hosted on Requestor's HPLMN

Customer A roaming on network C asking for a location service needing the location of customer B roaming on network D. The service is hosted on network A.
Use case: Chris, an SFR (France) customer, roaming on E-Plus (Germany), asks an SFR service for the location of Bob, a Wind (Italy) customer, roaming on Optimus (Portugal).

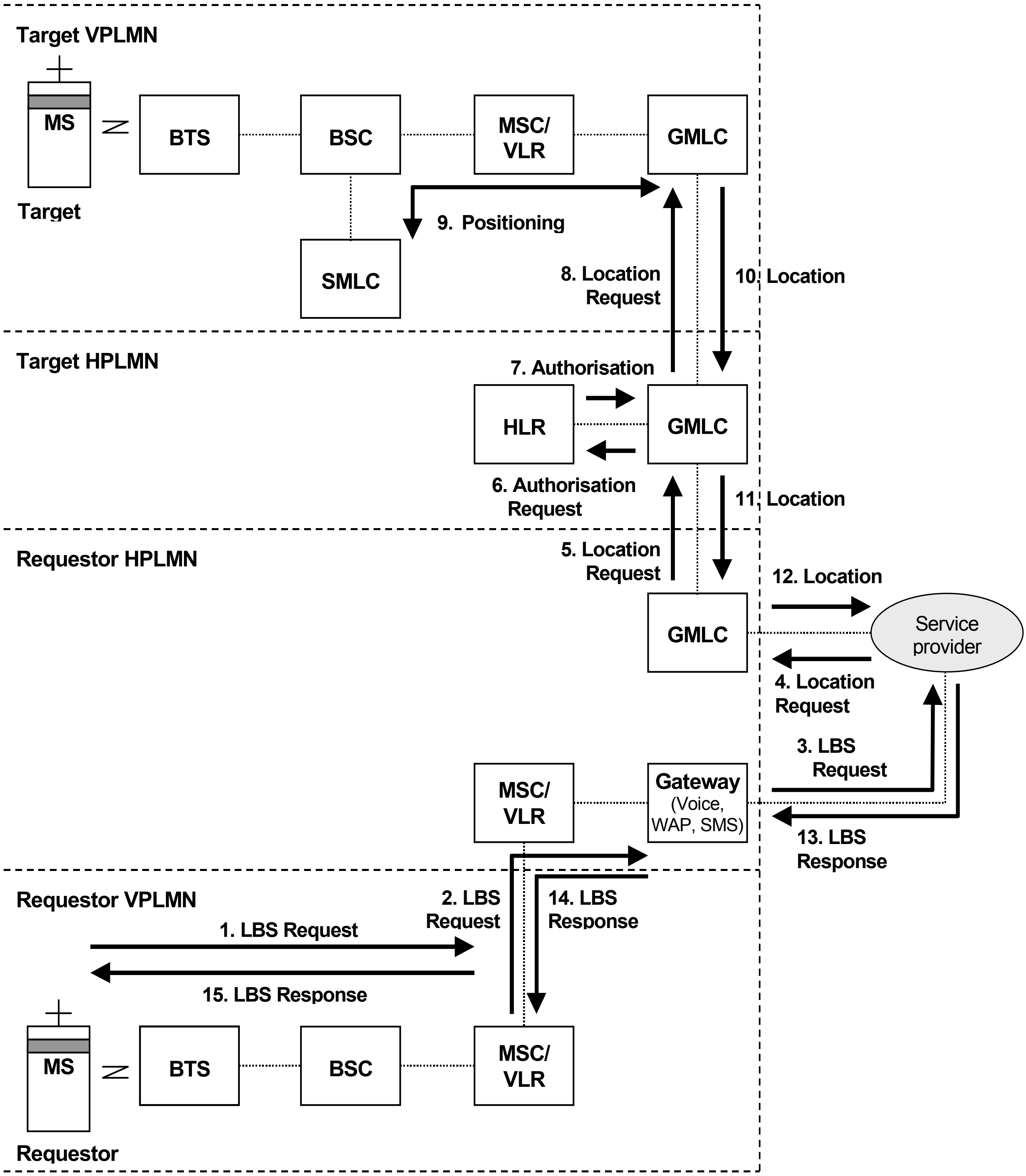


Figure A2 10 Scenario 9: Roaming: Service Hosted on Requestor's HPLMN

Scenario 10: Roaming: Service Hosted on Requestor's VPLMN
Customer A roaming on network C asking for a location service needing the location of customer B roaming on network D. The service is hosted on network C.
Use case: Chris, an SFR (France) customer, roaming on E-Plus (Germany), asks an E-Plus service for the location of Bob, a Wind (Italy) customer, roaming on Optimus (Portugal).

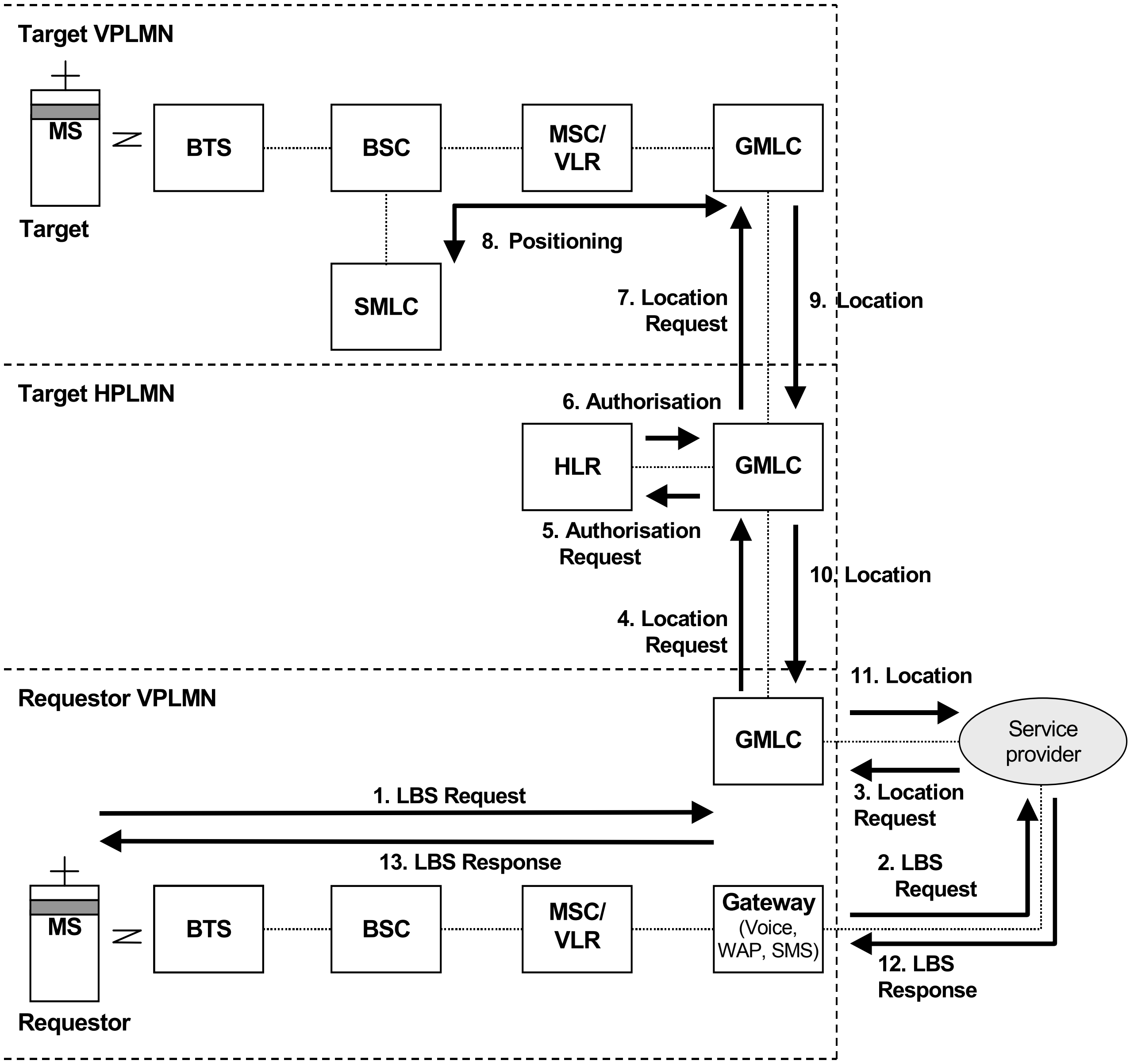


Figure A2- 11 Scenario 10: Roaming: Service Hosted on Requestor's VPLMN

Scenario 11: Roaming: Service Hosted on Target's HPLMN

Customer A roaming on network C asking for a location service needing the location of customer B roaming on network D. The service is hosted on network A.
Use case: Chris, an SFR (France) customer, roaming on E-Plus (Germany), asks a Wind service for the location of Bob, a Wind (Italy) customer, roaming on Optimus (Portugal).

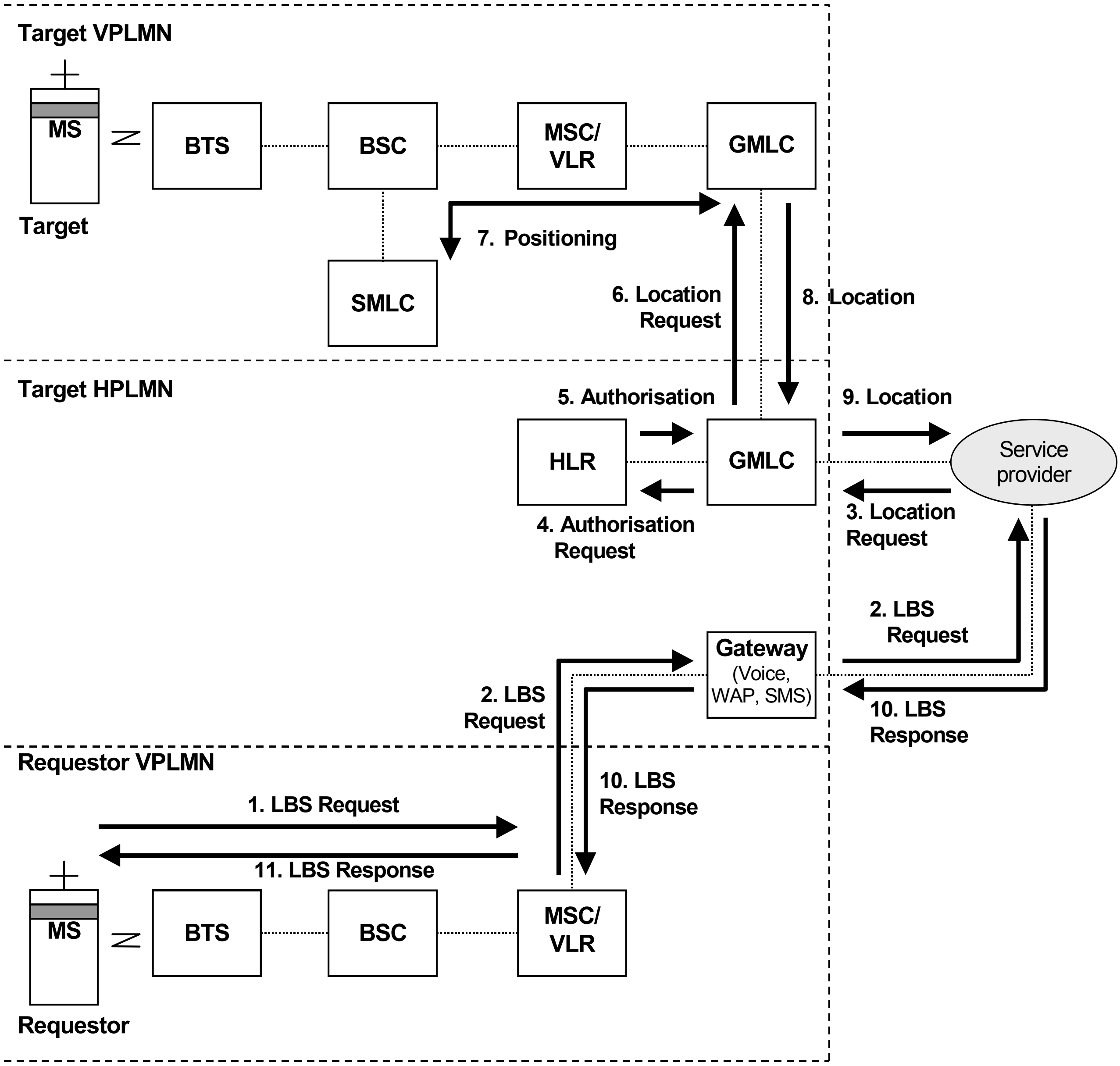


Figure A2- 12 Scenario 11: Roaming: Service Hosted on Target's HPLMN

Scenario 12: Roaming: Service Hosted on Target's VPLMN

Customer A roaming on network C asking for a location service needing the location of customer B roaming on network D. The service is hosted on network A.
Use case: Chris, an SFR (France) customer, roaming on E-Plus (Germany), asks an Optimus service for the location of Bob, a Wind (Italy) customer, roaming on Optimus (Portugal).

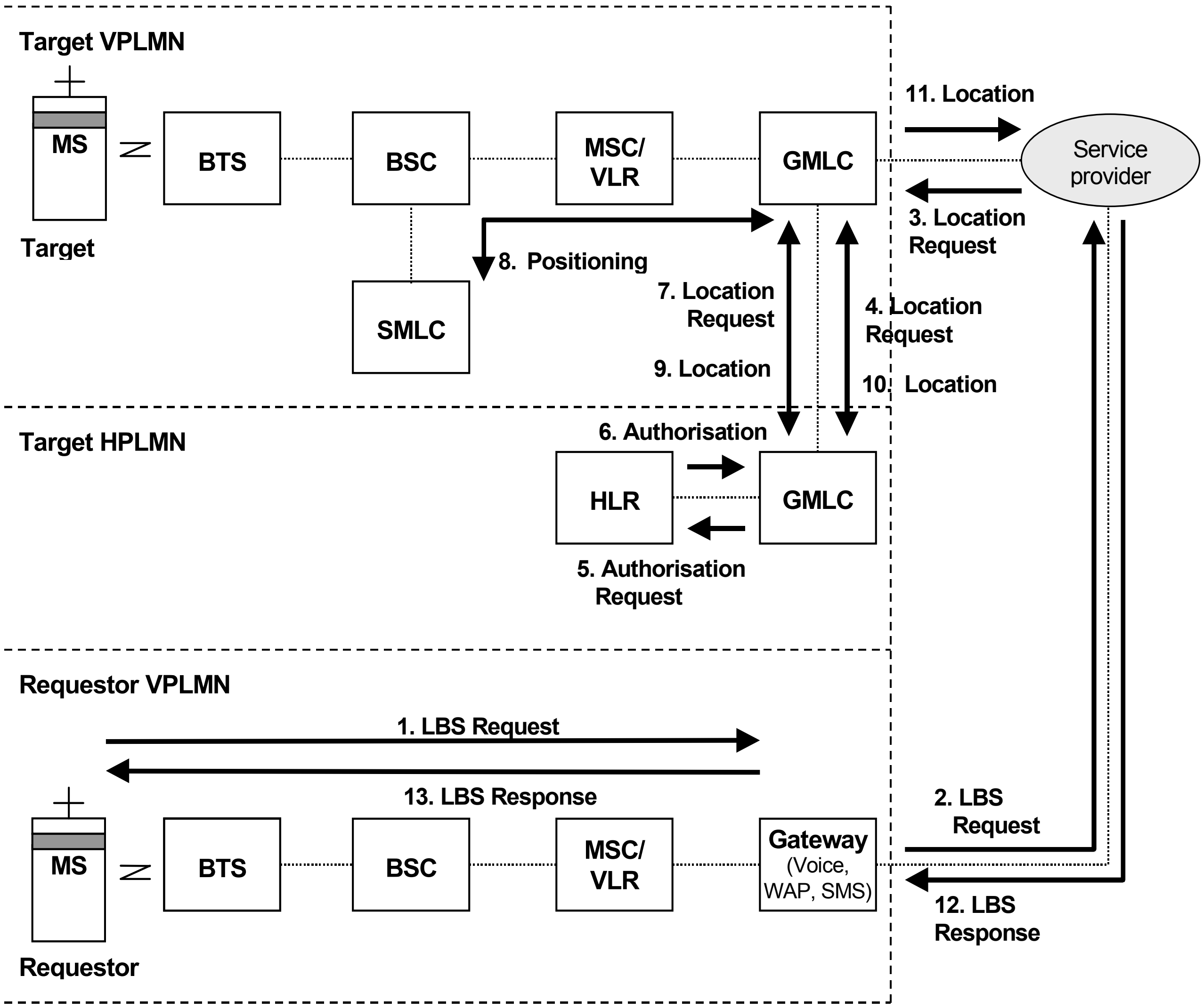


Figure A2- 13 Scenario 12: Roaming: Service Hosted on Target's VPLMN

Scenario 13: Roaming: Tracking, Service Hosted on Requestor's HPLMN

Customer A roaming on network C tracking customer B roaming on network D. The service is hosted on network A.

Use case: Chris, an SFR (France) customer, roaming on E-Plus (Germany), asks an SFR service for the location of Bob, a Wind (Italy) customer, roaming on Optimus (Portugal).

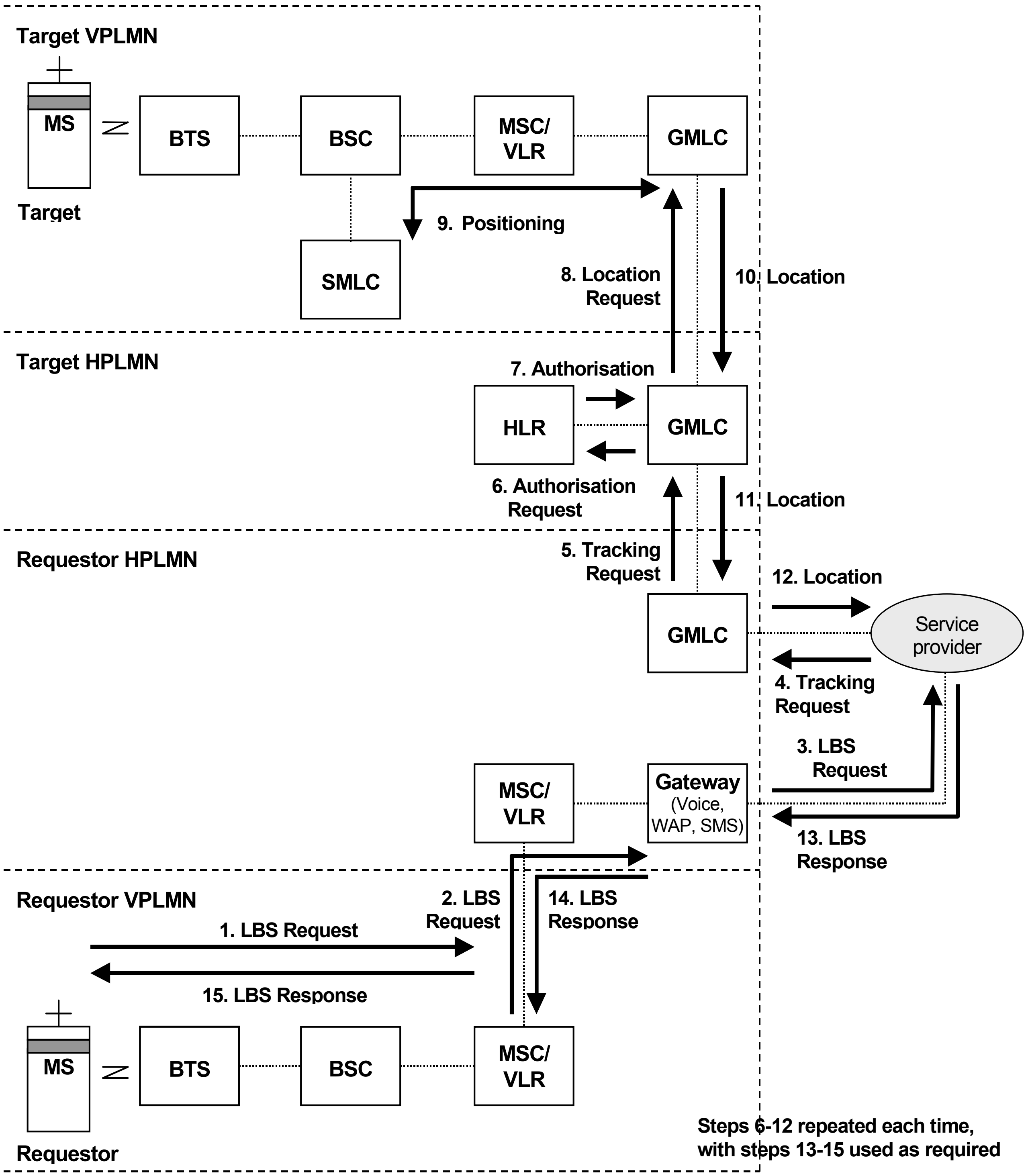


Figure A2- 14 Scenario 13: Roaming: Tracking, Service Hosted on Requestor's HPLMN

Scenario 14: Roaming: Mobile Originated Request

Customer (or handset/SIM application) asks for own location while roaming.
Use case: Local mapping.

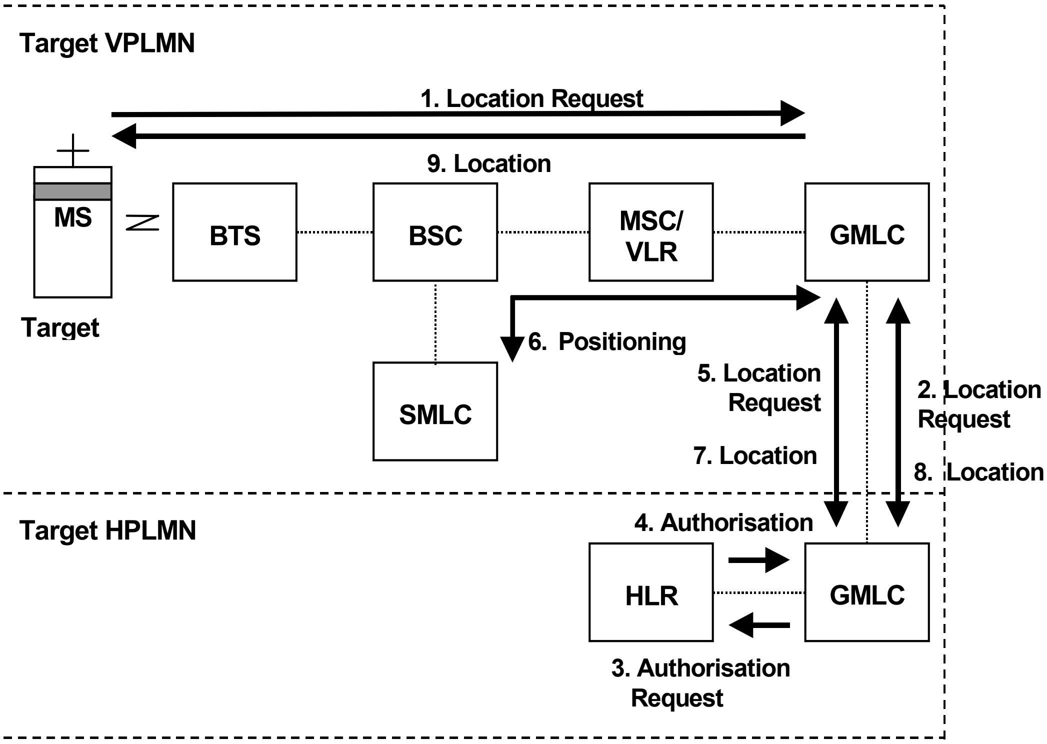


Figure A2- 15 Scenario 14: Roaming: Mobile Originated Request

APPENDIX 3

Interim GPRS location enabling

GPRS Problem:
The problem today, is that the HLR is not able to retrieve the location information directly from the SGSN (it cannot ask the question to SGSN as it is not standardized, so we need an interim solution.

Interim solution 1

This following scenario is designed as a potential interim SMS solution for Class A / B phones as they got information to update the cell in the HLR with class 0 SMS, and a Sim Toolkit application for class C handsets.
Use case: Customer A on his own network asking for a location service.

Table A3- 1 Message flow in Figure A3- 1

	Message	Description
1/2.	Service Request	Subscriber requests service
3.	Service Request	Service request to the Service Provider
4.	Location Request	Service Provider requests location
5.	Location Request	GMLC can not retrieve location information as not available from HLR, asks SMS-C to issue SMS to MS in order to retrieve location
6/7/8.	SMS location update	SMS-C is initiating an SMS in order to update location information and pass it to GMLC
9.	Location Reply	Location reply to the Service Provider
10/11/12.	Service Reply	Service Provider delivers service via Gateway

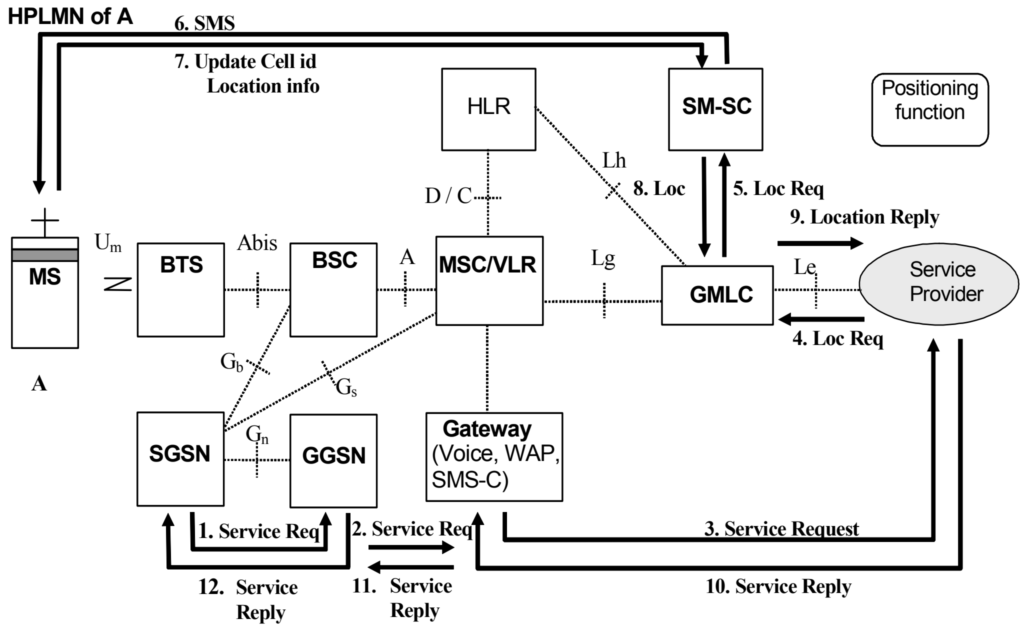


Figure A3- 1 GPRS location enabling, interim solution 1

Interim solution 2

Customer A on his own network asking for a location service. Possible solution 2.
Use case: A SFR customer on his own network is asking for the localised weather forecast.
His MS-ISDN is sent to the Gateway (WAP, SMS…)

Table A3- 2 Message flow in Figure A3- 2

	Message	Description
1/2.	Service Request	Subscriber requests service
3.	Service Request	Service request to the Service Provider
4.	Location Request	Service Provider requests location
5/6/7.	Location Request	GMLC can not retrieve location information as not available from HLR, asks VLR to retrieve location from SGSN
8/9/10.	Location update	SGSN gives back location information to GMLC through VLR
11.	Location Reply	Location reply to the Service Provider
12/13/14.	Service Reply	Service Provider delivers service via Gateway

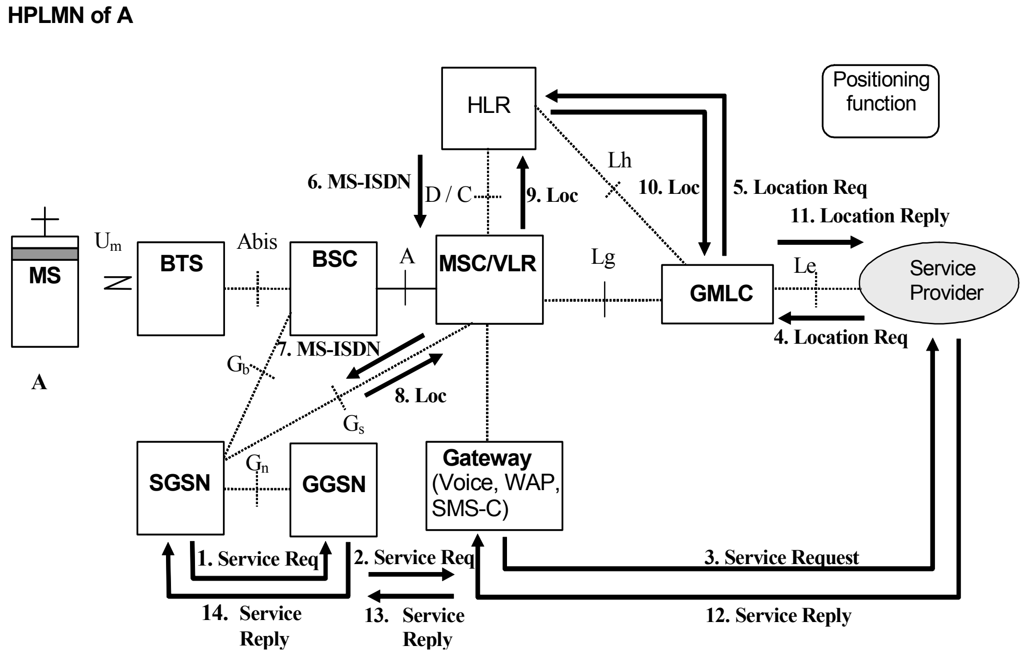


Figure A3- 2 GPRS location enabling, interim solution 2

Targeted solution

Customer A on his own network asking for a located service. Targeted solution.
Use case: A SFR customer on his own network is asking for the localised weather forecast.

Table A3- 3 Message flow in Figure A3- 3

	Message	Description
1/2.	Service Request	Requestor requests service
3.	Service Request	Service request to the Service Provider
4.	Location Request	Service Provider requests location
5/6.	Location Request	GMLC asks HLR to retrieve information from SGSN
7/8.	Location update	Location is updated and passed to GMLC
9.	Location Reply	Location reply to the Service Provider
10/11/12.	Service Reply	Service Provider delivers service via Gateway

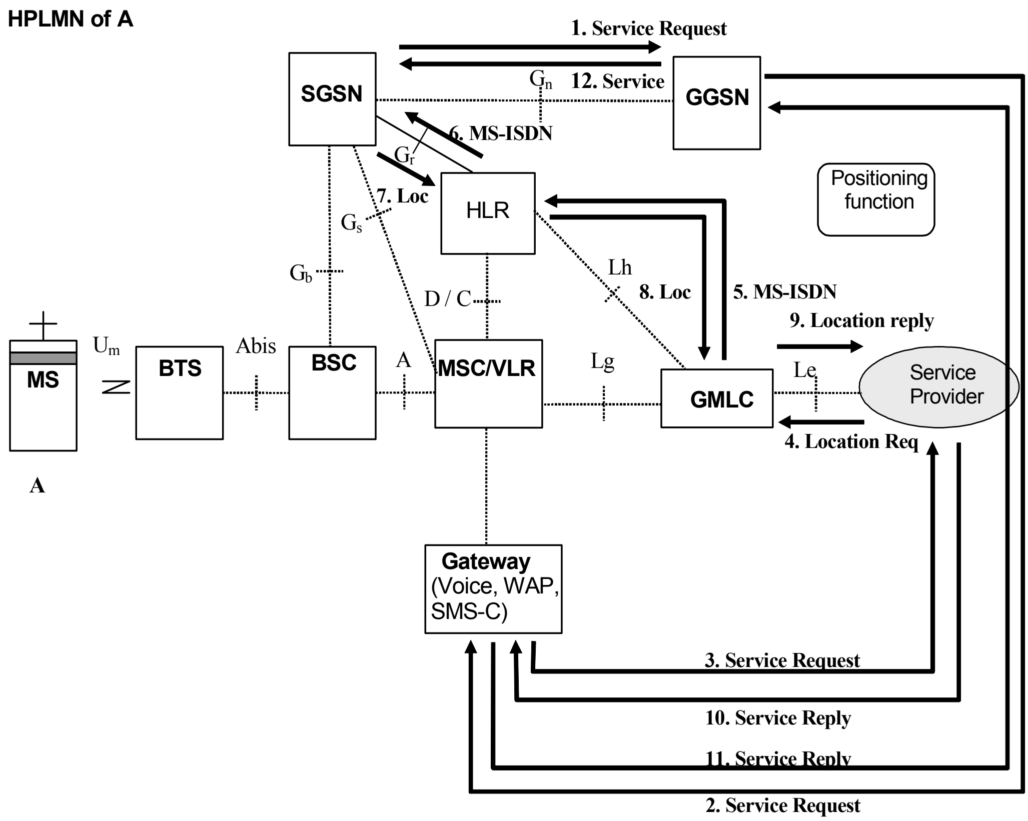


Figure A3- 3 GPRS location enabling, targeted solution

APPENDIX 4

Liaison statement from SerG to GSME, GSMNA and LRG:

"SERG166_01 LS on LBS to GSMNA-GSME

Response to LS from GSME:

"SERG184_01 LS SERG lbs from GSME

Response to LS from LRG:

"SERG183_01 LS SERG lbs.doc"

Liaison statement from SerG to 3GPP SA WG 2 on inter-GMLC interface:

serg017_02.doc

Responses to LS from 3GPP:

serg058_02.doc serg067_02.doc serg068_02.doc

Liaison statement from SerG to 3GPP CN WG 4, 3GPP SA WG 2 and GSMA IREG (Cc: 3GPPSA WG 1) on inter -GMLC interface utilising IP as transport:

serg107_02.doc

Response to LS from 3GPP:

lbs028_02 s2-021919.doc

Liaison statement from SerG to 3GPP SA WG 1 and 3GPP SA WG 2 on privacy control for LBS:

lbs005_02.doc

Liaison statement reply from SerG to 3GPP SA WG 1 (Cc: 3GPP RAN WG 2, 3GPP RAN WG 4 and 3GPP SA WG 2) on Accuracy Classes:

serg115_02 ls reply on accuracy classes_

APPENDIX 5 – The Inter-GMLC Interface

Functional Description

GSM Association SerG has defined a new interface to support Location Based Services (LBS) Roaming. This is the Inter-GMLC interface and is based on the LIF Le interface (GMLC to 3rd party interface). 3GPP have agreed to standardise this interface as part of Release 6. It will be known as the Lr interface and, although mandated for Release 6 GMLCs, its use will be optional.

The principal reasons for the definition of a new interface are:

- To support enhanced user privacy checking in the Home-PLMN, prior to the authorised release of subscriber location information to any 3rd party;
- To facilitate the ability for the VPLMN to apply charging for location requests from the HPLMN;
- To allow inter-operability for LBS roaming with a mix of pre-standards and standards based roaming partners.

SerG believes that the above requirements can be met if all location requests, for inbound and outbound roamers, are made using the Lr interface.

The Lr interface has the advantages that:

- Both pre-standards (MAP ATI) and standards based location mechanisms "behind" the GMLC can be supported and no further integration/testing is required when a roaming partner migrates from a pre-standards to a standards based implementation;
- The HPLMN GMLC is always involved with a location request, to satisfy that a user has authorised such a request;
- Charging a roaming partner for satisfying their location requests becomes like charging any other location application that queries the GMLC for location information;
- Throttling mechanisms that exist within the MLC can be reused to regulate the location requests coming from a roaming partner, and SLAs can be established.

The Lr interface makes the request for location information from one operator to another very similar to the request from a 3rd party Application to an operator (that uses the Le interface). SerG has requested 3GPP to base the Lr interface on the LIF Le interface with the following additional requirements:

- ability to identify the requesting party as another operator or a VNO [Note: this may not be required as it will be evident from the use of the Lr interface that the requesting party is an operator]
- an indicator to show that the privacy requirements for the location request have already been applied [Note: this may also not be required as it should be explicit that authorisation will have been checked]
- a field to identify the MSC/VLR that is serving the roaming mobile whose location has been requested (ie Target VLMPN). This will facilitate the identification of the Target location by the VPLMN's GMLC.

Note that 3GPP has yet to analyse the requirements for the Lr interface and so it is not possible at this stage to give exact details of its architecture. As the development of the Lr interface proceeds, this guidance will be updated.

The Lr interface has the advantage that there is no requirement for a roaming partner or the home network to support LCS MAP messages to allow roaming between them. Also, no further action is required when either party does migrate to support the standards.

Another option for the Lr interface would be MAP based, such that the HPLMN GMLC uses a MAP Provide_Subscriber_Location query towards the VPLMN GMLC, with the Destination-Point Code and/or Global Title of the VLR/VMSC encoded in the MAP SS7 message.

In both cases, the response from the VPLMN GMLC to HPLMN GMLC should pass back WGS84 co-ordinates, in accordance with GSM 03.32.

Transport

The transport of the Lr interface needs to ensure the following:

- Security
- Performance
- Time to implement
- Implementation cost
- Ease of future evolution

In order to minimise the number of options a single method of transport should be implemented.
Following discussions in SerG and with IREG, it has been concluded that an IP based transport would fulfil the above requirements and this is recommended for the Lr interface.

Anonymity

Extending the Opaque with an Country Code and Network Code extension allows routing of the request to the applicable (requesting) network which on it's turn then issues the applicable location request to the HPLMN (i.e. privacy validation). As the Lr is MLP based, the Opaque ID is supported by the ASID element.

Other Changes – HLR Upgrade

To support the extra Routing Information needed for Release 6 GMLCs, (e.g. the address of the H-GMLC and/or the V-GMLC), it will be necessary to upgrade the HLR to store this data. The requesting GMLC (R-GMLC) obtains this information from the HLR via the existing Lh interface, for which additional MAP messages are being specified. Note that where the Lr interface is used, the Lh interface is required only internally to the HPLMN.