Openwave Location Studio

Location Enabling Server

About Openwave

Openwave Systems Inc. (Nasdaq: OPWV) is the worldwide leader of open IP-based communication infrastructure software and applications. Openwave is a global company headquartered in Redwood City, California. For more information, please visit www.openwave.com.

Executive Summary

The success of consumer mobile Internet requires the delivery of many applications and services. There is no one killer application that will ensure a profitable business and timely return on investment. A cross-section of information, entertainment, and utilitarian offerings are necessary in order to appeal to the broadest possible market segment. But with each new service introduced the costs of integration, support, and maintenance goes up. Without an effective strategy to manage these services the cost of this support effort can escalate exponentially significantly reducing the profitability of these services.

Privacy and Access controls are essential components of LBS. The wired Internet evolved at a pace that left consumer privacy and security in the back seat. However, privacy advocates have caught up with the technology and are increasing consumer awareness of the issues, and forcing change to legislation and governance. The wireless Internet does not have the same grace period with respect to subscriber privacy and access. Effective solutions are available today, and will be necessary to build and maintain consumer confidence in new services.

Successfully deploying LBS services does not have to be a complex and protracted effort. Obtaining the raw location of the mobile subscriber is a critical first step, but the location gateway is just one of several operator network elements involved in end-to-end service fulfillment. Each additional element represents another touch-point of integration, with associated costs and complexities. While this integration is a daunting task to network operators, it is doubly so to application developers who face the prospect of different legacy systems in each operator network, and do not have the resources to customize their products to these changing interfaces. Indeed, their time is better spent on the services themselves and not the network integration

Choosing the right Location Middleware can pave the way to successful LBS deployment. This document presents an overview of Openwave's *Location Studio*. *Location Studio* is a location middleware product designed to enhance privacy and security, and simplify integration of location applications with a network operator's value-added services infrastructure. *Location Studio* enables subscribers to control access to sensitive location information by third-party applications, and integrates to the operator's SMSC, WAP Gateway, billing system and provisioning gateway in support of location-based services

Openwave Location Studio

Location Enabling Server

Table of Contents

Openwave Location Studio

Location Enabling Server

1. Introduction

Location Studio is a location-enabling server, which is either deployed within the wireless operator's network or hosted by an ASP. Location Studio simplifies the integration of multiple location-based applications, and maintains access, security, and privacy rules for each transaction.

Location Studio delivers a lower-cost of LBS deployment through integration with internal operator infrastructure, including: location server, SMSC, WAP gateway, subscriber portal, customer care/activation system, billing systems, and operational support systems. Location Studio integrates with these elements **once**, so that individual LBS applications don't have to do so.

Location Studio's subscriber privacy features allow mobile subscribers to control which location-based services have access to their location. Advanced privacy controls allow subscribers to control how, when and under which circumstances specific location-based services can receive their location.

Location Studio facilitates subscriber access to personal profiles and privacy preferences using the web, WAP or SMS - making it easy for subscribers to opt in and out of location-based enhanced services. This means subscribers will use location-based services more frequently, thus increasing overall mobile phone usage.

Location Studio compliments Openwave Location Manager™ GMLC and MPC offerings, as well as third-party location servers, with enhanced subscriber privacy and client management capabilities.

This document describes Location Studio 2.0, the second major release of this product. Location Studio is deployed commercially in both GSM and CDMA networks in Europe and North America.

2. Product Description

2.1 Location Studio in the Operator's Network

The primary purpose of Location Studio (LSt) is to broker the location of subscriber mobile terminals to location-based services/applications in a controlled manner. Location Studio utilizes HTTP connections with external entities to exchange data over primary interfaces using XML. Location Studio is a companion product to Location Manager (LM), or other location servers (Ericsson MPS or Nokia mCatch for example), providing advanced **privacy** and **access** features.

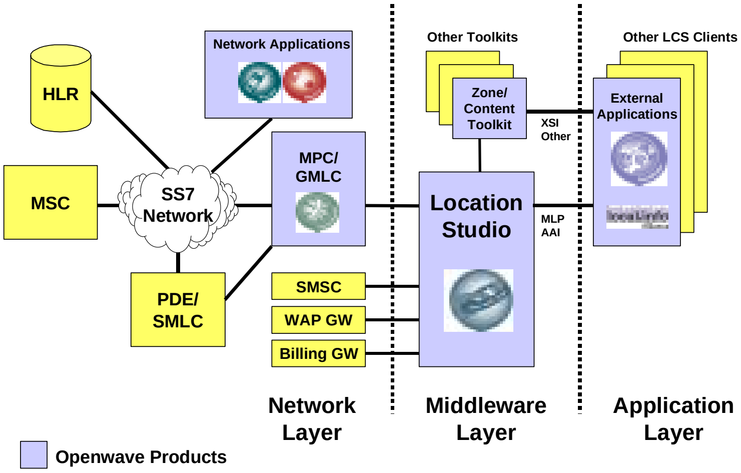
To Clients (ie. Location-Based-Services), Location Studio offers open or encrypted (SSL/HTTPS) connections over which location of a subscriber mobile station may be obtained. In this way, all data transferred between Location Studio and external, non-trusted entities can be secured if desired.

To Subscribers, Location Studio offers the ability to control which location based services, and individual applications, may obtain their location. The subscriber may be presented with basic or advanced features to control how and when their location is provided to external applications.

To Operators, Location Studio offers the ability to define which services a Subscriber can use, and which applications are able to request services from the network. Additionally, Location Studio provides a single, unified point for securing external access, providing logging for billing.

2.2 Commercial Services Architecture

The following figure illustrates the reference architecture for deployment of commercial location based services.



2.2.1 Deployment Layers

Network The internal network elements typically interconnected via the SS7 network.

Access Transition layer between the internal SS7-connected network elements and the external Internet. This layer provides control and mediation of access by non-trusted internet-based clients and network-provided resources. Managing subscriber privacy at this layer allows for a consistent user experience across all offered services.

2.2.2 HLR, MSC, PDE/SMLC

These internal network elements are within the operator’s network and may be involved in the call flow for retrieval of a subscriber terminal location. The definition and description of these elements is beyond the scope of this document.

2.2.3 SMSC, WAP GW, Billing GW

These internal elements are part of the value-added services infrastructure of the network. The Short Message Service Center, and the Wireless Application Protocol Gateway are often part of the LBS call flow – providing the bearer for interaction with the subscriber terminal. The Billing Gateway is a point of integration to the operator's billing system, which is required to bill for value-added services. These three elements will vary widely from network to network and will often require custom integration services.

2.2.4 SS7 Network

This is the Signaling System 7 telecommunications network used to interconnect network elements to pass call processing data.

2.2.5 Network Applications

These are trusted applications typically deployed within the operator's network and often have special privileges with respect to location (e.g. privacy override, high priority). These applications may interface to the GMLC or MPC using a trusted interface, therefore bypassing Location Studio in the call flow. Examples of network applications include Openwave Intelligent Network Routing and Openwave Safety First emergency services (911/112) application.

2.2.6 Location Manager (LM)

The core GMLC/MPC network element for location based services; LM provides multiple methods of extracting location of a Subscriber mobile terminal from the wireless network, including cell sector based positioning and higher accuracy handset or network-based Position Determining Equipment (PDE) or SMLC.

The GSM and 3GPP standards define a Gateway Mobile Location Center (GMLC) as a network element providing delivering subscriber terminal location data from the network. The ANSI standards define a Mobile Positioning Center (MPC) as a network element that provides locations for emergency (911) and commercial services.

2.2.7 Location Studio (LSt)

Location Studio provides controlled access to Subscriber terminal location data from non-trusted LCS Clients (applications). LSt provides secure connections for access to data, robust authentication of all users accessing the platform, and both Client and Subscriber authorization functions. LSt contains optional advanced subscriber privacy controls based on flexible permission sets.

2.2.8 Zone/Content Toolkit

The Openwave Zone/Content toolkit is a content management and zone determination utility which is deployed as an optional accessory to Location Studio. Using the XML Service Invoke (XSI) toolkit interface, external LCS Clients can find content near a subscriber, or convert a subscriber's location into a zone-based location description (zip code, city, state). The zone/content toolkit is a spatial-processing engine, and GIS data is provisioned using the Openwave MAPS provisioning tool.

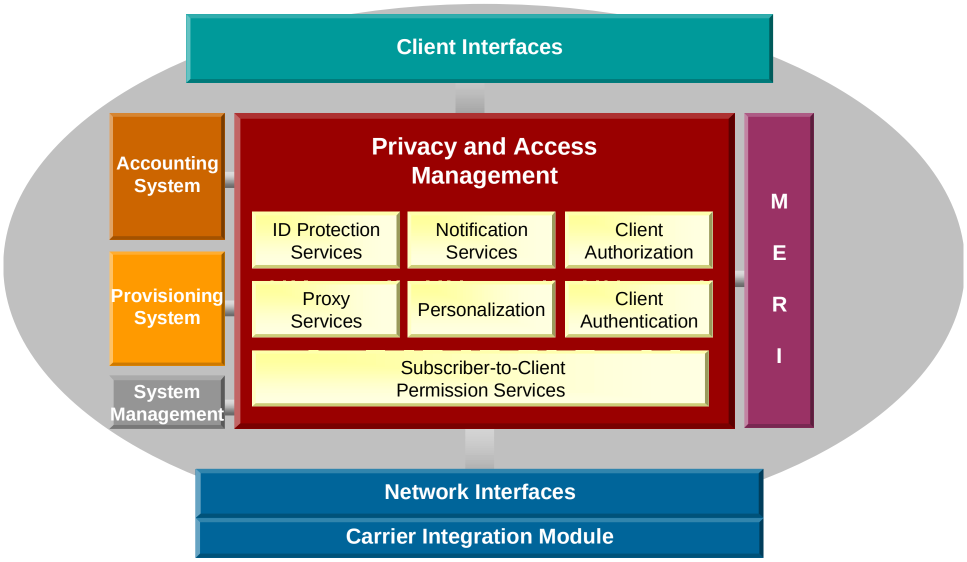
Additional third-party toolkits may be used in place of, or to enhance, the content and zone functions provided by this toolkit. All toolkits interface to Location Studio through the Middleware Extension Request Interface (MERI), which is described later in this document.

2.2.9 External Applications

External LCS Clients are non-trusted applications that may be hosted either within the Operator's network or by the application service providers themselves (interconnected via the Internet or other TCP/IP facilities). LCS Clients use Client interfaces of Location Studio to request location of a Subscriber terminal from the network, send or receive short messages with the terminal, request content or spatial services, verify a service subscription, or submit billing information to the operator. Openwave's FriendFinder application is an example of an external client.

3. Component Architecture

The diagram below shows a more detailed view of the functional components that make up the Location Studio product.



Client Interfaces: XML and Web-Services based interfaces providing access to core functionality required to implement location-based services. LCS client (application) interfaces are provided for the following services: Location Request, Messaging (e.g. SMS), Subscription Validation and Service Billing.

Network Interfaces: Consists of 2 parts: Upper layer and Carrier Integration Module (CIM). The CIM interfaces to value-added services infrastructure within the operator's network, including: SMSC, WAP-GW and Location Server. One instance of Location Studio will support several Carrier Integration Modules in the event that separate infrastructure elements must be addressed for different subscribers (i.e. common middleware for multiple networks).

Privacy & Access Management: The core value-added functionality provided by Location Studio. Privacy management at the middleware layer provides a consistent mechanism to control access to location on an application-by-application basis. The Subscriber can personalize their privacy profile to allow different privacy and notification setting depending on the application. For the operator, the Location Studio provides a single point of access to the network by LCS Clients using privileges stored in a client-profile.

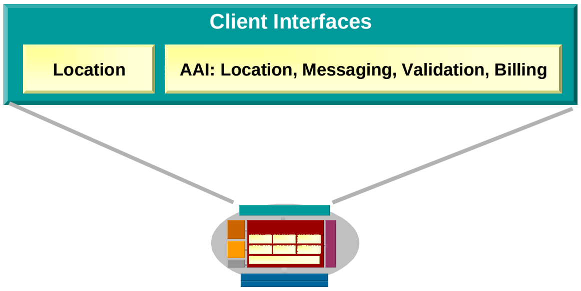
Accounting System: Location Studio provides detailed accounting of all micro-transactions executed against the platform by LCS Clients. Micro-transactions are defined as basic service requests - location, messaging and spatial/content toolkit services. Each Client transaction is stored in a log file, formatted as a Transaction Detail record (TDR) which uniquely identifies the originating Client, the date/time, the type of transaction, and the result. Log files are rolled off the system at periodic intervals and transferred to an external mediation system for statistical analysis and/or billing and reconciliation.

Micro-transactions can also be correlated against service level billing events submitted by Clients to identify a macro-transaction – one that is billable directly to the end-user/subscriber (such as "delivered premium content", "located three friends", …).

Provisioning System: The provisioning system of Location Studio provides interconnection to the operator's customer activation and support systems. A combination of web-based graphical user interfaces, and an XML provisioning API allow both manual and electronic modifications to Subscriber and Client profiles. Additional features support more advanced self-provisioning functions allowing the subscriber more direct control, and lessening the requirements for human interaction with operator support personnel.

MERI: A key differentiating feature of Location Studio is the Middleware Extension Request Interface (MERI). The MERI is used to extend the privacy and access capabilities of Location Studio to third-party providers of spatial and content toolkits. The operator may integrate one or more such platforms with Location Studio to provide additional services to LCS Clients to promote more rapid and consistent introduction of services. Location Studio applies consistent authorization, accounting and monitoring functions to all requests – whether direct to Location Studio interfaces or to interfaces belonging to toolkits connected via the MERI.

3.1 Client Interfaces



3.1.1 Location

Location Studio has adopted the Location Interoperability Forum (LIF) recommendation, Mobile Location Protocol (MLP), as the standard location interface for third-party Client applications. The MLP specification is very extensive, and includes many parameters in anticipation of future needs. As such, the complete specification is not implemented within Location Studio – only the basic set of features required for today's LBS applications (Standard Location Immediate Service). A detailed Statement of Compliance is available upon request. Location Studio will maintain compliance with the relevant portions of the LIF MLP specification as it is updated and ratified (currently MLP 3.0). Openwave is an active member of the LIF and one of the first commercial location gateway suppliers to offer a LIF MLP compatible location request interface for third-party applications.

- The core privacy and access features of Location Studio are applied to all requests against this interface. The advantages of adopting the LIF MLP protocol are:
- LIF membership is open to all vendors and is well represented by all major vendors of LCS infrastructure
- The MLP protocol is feature-rich and well-defined – the specification team is comprised of leading engineers from different vendors
- The LIF Forum is liasing with other industry forums to promote broader common standards across these groups – specifically the WAP Forum and Open GIS Consortium.
- LIF MLP is supported by a growing number of GMLC and MPC products, and in turn LCS applications. This results in a growing selection of compatible applications.

3.1.2 Advanced Application Interface

The Advanced Application Interface provides additional key services to enable location-based applications, combined with location requests in a single web-services defined API. These services provide access to the underlying location, messaging, billing and customer information systems within the operator's network. The AAI is a WebServices interface, within which there are four separate services as follows:

Location: The Wireless Location Service (WLS) in Location Studio provides location request functionality for third-party client applications, which is similar in form to the LIF MLP 3.0 protocol but is implemented as a web-service for convenience of use along with the other AAI Services. As such, the WLS is a proprietary Openwave protocol implemented using Web Services to enable easy integration with a wide range of integrated development environments.

All of the parameters and return values are compliant with the LIF specification. For detailed description on each of these values please refer back to the LIF specification version 3.0.0. For detailed information on what LIF functionality are supported by LSt, please refer to the Openwave LSt Interface Statement of Compliance for LIF MLP.

Advantages of using the WLS include:

- The location request is compatible with the LIF MLP 3.0 definitions
- Web-services implementation allows for convenient generation of request services in the native development environment of the developers using WSDL converters

Messaging: The Wireless Messaging Service (WMS) in Location Studio provides messaging functionality for third-party client applications. Wireless messages in this case are either SMS or WAP-push. WMP is a proprietary Openwave protocol implemented using Web Services to enable easy integration with a wide range of integrated development environments.

The WMP supports both upstream and downstream messaging between Clients (applications) and subscribers. Down-stream messages are defined as those initiated by the Client and sent to one or more mobile stations through Location Studio. Upstream messages are originated by mobile subscribers and 'tunneled' through Location Studio to client applications.

Advantages of using the WMS include:

- The Client application is sheltered from having to support every underlying SMSC protocol (LSt supports SMPP, UCP and CIMD2),
- LSt ID protection services (subscriber alias) can be used for anonymity and privacy
- Message Transaction Detail Records provide auditing and accounting functions
- LSt can select best available messaging transport based on defined handset capabilities and call-state
- Web-services implementation allows for convenient generation of request services in the native development environment of the developers using WSDL converters

Subscriber Validation: The Wireless Validation Service (WVS) in Location Studio provides a mechanism for Client applications to validate subscribers, subscriptions, and client application credentials. WVS is a proprietary Openwave protocol implemented using Web Services to enable easy integration with a wide range of integrated development environments.

The Client Applications will make use of this interface to:

- Check that an end-user is still a customer of the operator
- That the end-user is authorized by the operator to access their service
- That the end-user has adequate credit remaining in his/her pre-paid account
- That an end-user registering for a service using an internet browser is in possession of the Mobile Station he/she registers (identity verification loop using SMS pin code)
- Receive a persistent alias that may be used to identify the mobile station in subsequent transactions (location, messaging, billing, toolkit services) with Location Studio while maintaining privacy and anonymity.
- The advantages of using the WVS are:
- Service only requests from valid subscribers with established billing relationship

- Support anonymity and privacy for internet-based community and gaming services
- No network resources are consumed (e.g. location attempt) if the subscriber validation turned out negative.

Web-services implementation allows for convenient generation of request services in the native development environment of the developers using WSDL converters

Event Billing: The Wireless Billing Service (WBS) in Location Studio provides Client applications functionality to submit application/event-level billing records. WBS is a proprietary Openwave protocol implemented using Web Services to enable easy integration with a wide range of integrated development environments.

Billing events submitted through this interface convey *consolidated* macro-transactions that result from an action that is billable to the end subscriber using the service. For example, a billing event may be submitted by a yellow-pages application provider for a “premium content search” resulting in a single billing entry on the subscriber’s account. However, in order to complete that single billable event there may have been multiple underlying micro-transactions required to complete the request – one or more location requests, one or more geo-coding events, a map rendered, turn-by-turn directions delivered, …

Advantages of using the WBS include:

- Service-level billing events allow integration with the operator billing system so that transactions are charged directly on the subscriber’s monthly bill, or debited from pre-pay accounts.
- Facilitates revenue sharing and Bill-On-Behalf-Of relationships between operators and application providers.
- Supports correlation of micro-transactions with the service billable macro-transaction for better understanding of cost-of-delivery.
- Web-services implementation allows for convenient generation of request services in the native development environment of the developers using WSDL converters

3.2 Privacy and Access

The Privacy and Access features of Location Studio are the primary value-added feature provided by location middleware. These features provide the controls and safeguards necessary to ensure anonymity and privacy of the subscriber – a function critical to the adoption of location-based services. The subscriber must be provided with a consistent set of access control mechanisms that may be applied to all applications with access to the operators LCS infrastructure. The subscriber must be able to control their experience and have confidence with the integrity of the network.

The basic steps in a successful transaction against Location Studio are:

Location Request: Location is requested on any of the supported interfaces.

Password check, Active account check: The client application is checked for a valid Password based on the authentication values in the client profile. The client application user ID and password must be present for each request. Active account check checks the value of the account status field in the client profile. The status must be enabled for this check to pass.

Client authorized for interface: Check if the client is authorized to make requests on this request interface.

Apply the client profile restrictions to the request: Some clients have defaulted or restricted parameters on the request interface, these clients will have the defaults or restrictions applied at this point.

Client Privacy Bypass: Some clients such as the emergency services, lawful intercept, or internal applications have the right to override the subscriber privacy settings. If this is enabled in the client profile, the location request is made.

Subscriber profiles deployed: Some deployments of Location Studio may be without a subscriber profile database. If no profile exists, the location request is made without further checks

Is the client Operator Enabled: Provides the ability to restrict the clients that the subscriber may be located by. The client - subscriber permission set should have the client enabled for the requested subscriber for this check to pass.

Is the client Subscriber Enabled: This checks to see if the subscriber has added this client to the client-subscriber permission set. The client - subscriber permission set should have the client enabled for the requested subscriber for this check to pass.

Master Subscriber Privacy: The operator or subscriber may at some time desire to be location invisible (deny all requests at this point) or visible (allow all requests at this point). If this parameter is set to “OFF”, the explicit and default permissions are active.

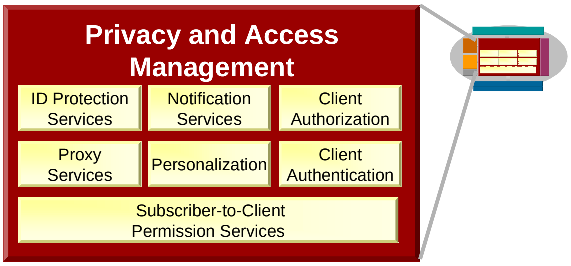
Explicit permission: This can be any number of filters that have been set up for the client by the subscriber. All of the filters must pass before this check passes.

Apply Permission constraints to location request: This allows the subscriber to specify the best accuracy in which they may be located as well as any notification (or Ask) options.

Get Location: The location is requested from the location server

Subscriber default privacy: This is the privacy behavior that is applied if no explicit permissions exist for the client.

The following features of Location Studio provide these critical features:



Privacy and Access Management

ID Protection Services

Notification Services

Client Authorization

Proxy Services

Personalization

Client Authentication

Subscriber-to-Client Permission Services

3.2.1 Client Authentication

All transactions against Location Studio require positive authentication of the requestor's credentials. Basic authentication is provided as a ClientID and password embedded with each request. More advanced authentication may be incorporated using external third-party products – for example bi-directional SSL using certificates. These advanced capabilities are not part of Location Studio – they are accessories to enhance the implementation.

3.2.2 Client Authorization

Once a Client has successfully authenticated to Location Studio their request is authorized based on privileges established within a Client profile. The Client profile is a set of parameters used for identification and authorization of access by LCS Clients (applications). The Client profile contains parameters that define what services a Client may access from the network, the allowed quality of service, as well as physical identification data used for authentication and billing. The Client Profile is stored within Location Studio. Each Client may have different settings established, depending on their business relationship or application type.

The basic Client profile includes the following parameters:

Name	**Description**
Client ID	Unique identifier. Used to identify for each Client. This is the finest granularity of identification of the client Generated by LSt
Friendly Name	Short string used for notification messages and service provisioning/selection. This is the display name of the client
Login ID	Unique. Login ID for the client. This is the ID used in the external request interfaces.
Password	Specified by operator/client.
Enabled	Enabled or Disabled (default Disabled). Only active Clients will be allowed to make requests to LSt This field allows for the suspension of Client privileges. This allows the carrier to temporarily revoke the privileges of the client without having to delete them from the system.
Privacy Override	If set to yes, all requests from this client will be set to override privacy. Allows the carrier to specify clients that can override the privacy settings of the user. Client authentication/authorization checks must still pass.
Best Allowed request accuracy	Uncertainty [Radius in meters] This is the best accuracy that the client may request. If a better accuracy is requested, the request is changed to be equal to this value. In the implementation this is kept in the operator-client relation table, since different operators may have different values.
Priority request Allowed	A permission for the client to make a location request with a priority specified.
Default Notification	This option sets the default notification and transport option if no

Option	sub profile exists or if no notification option is set by the subscriber. The default is no notification.
WLI Allowed	A permission for the client to make a location request on any available interface.
WMP Allowed	A permission for the client to make use of the WMP.
WBP Allowed	A permission for the client to make use of the WBP.
WVP Allowed	A permission for the client to make a use of the WVP.
MERI Allowed	A permission for the client to make a use of the MERI.
SMS Post URL	URL used to post requests received from the SMS interface. If required this URL also contains authentication information.
SMS Bnumber	The shortnumber the SMS was sent to. In the implementation this is kept in the operator-client relation table, since different operators may have different values.
MSID Allowed	Allow the use of the subscriber phone number on location requests.
PSID Allowed	Allow the use of PSID
TSID Allowed	Allow the use of TSID
OSID Allowed	Allow the use of OSID (External ID or WAP ID etc.)
OSID Type	The type of OSID, e.g. WAPID, XID etc. String

3.2.3 Personalization

The key to effective privacy management is the presentation of the privacy options in a way that allows the subscriber to personalize the services according to their wishes. Location Studio provides reference user interfaces to allow the subscriber to personalize their services using SMS, WAP and WEB interfaces. However, the user experience is a critical service differentiation for operators and the final implementation of these interfaces must be customized to the specific requirements of the operator. This is completed as professional services during deployment.

The Subscriber profile is a set of parameters used for identification, authorization, and privacy preferences of subscribers within the serving operator’s network. The Subscriber profile contains parameters that define what services the subscriber is allowed to access, and what applications the subscriber authorizes to receive location. Permissions within this database are unique to specific subscriber-client relationships. The Subscriber profile is stored in a database managed by Location Studio.

The basic Subscriber profile contains the following parameters:

Name	**Description**
Operator ID	FK used to identify operator the subscriber is associated with. This will allow for future support of operator separation on a single deployment of LSt
Subscriber ID	Unique field for the subscriber. Unique key generated by LSt.
MS ID	Phone number assigned to the mobile or SIM card

MS ID Type	MIN/MSISDN (future IP)
Master Subscriber Privacy	If set to **DENY ALL (TRUE)**, then all location requests (except for privacy override) are blocked. If **OFF (FALSE)** then existing permission sets define privacy.

Extensions from the basic Subscriber profile include:

- A set of parameters for use when the Location Studio deployment contains "portal" functionality, like password management, direct serving of personalization web/wap pages, etc.
- The subscriber-to-client permission set, which contains the privacy preferences on a client-by-client basis.

3.2.4 Subscriber-To-Client Permission Services

Subscriber-to-Client Permissions provide the ability to grant specific Client Applications unique authority to locate oneself. Newly provisioned services are assigned a set of default privacy conditions, which then may be personalized by the subscriber according to their wishes for that specific service. Permissions can be uniquely assigned to each client application enabled in the subscriber's profile.

For each Client-to-Subscriber relation several attributes are use to protect the subscribers privacy and control access by subscribers to applications, including:

Subscriber authorized to access the Client application (granted by operator)

Client allowed to locate subscriber (granted by subscriber)

Best allowed return accuracy for a specific client (set by subscriber), e.g. a dating service

Irrespective of the established permissions in effect the Subscriber may override all permissions with a *Global OFF* privacy setting, which allows the ability to go invisible until the original permission sets are restored (*Global ON* privacy).

The basic Subscriber-to-Client permission set contains the following parameters:

Name	**Description**
Operator service enabled	This specifies if the subscriber is authorized by the operator to add the client.
Subscriber service enabled	This specifies if the subscriber has enabled the client.
Best Allowed Returned accuracy	This specifies the best accuracy that maybe returned to the client. This values is applied to the request at the "apply permissions constraints to location request" in the permissions hierarchy and at the post filtering stage. This value overrides the value in the client profile.
Notification Option	This lists how the user may wish to be notified of the location request. This is applied to the request flow at the "apply permissions constraints to location request" in the permissions hierarchy. The default value is no notification.

PSID	This is the PSID, i.e. a persistent alias that is tied directly to the specific client. The default value is null.
PIN	Temporary ID used for First-Time-Through (FTT) provisioning used in the SMS loop
First Request	This information allows LSt to know if this is the first time through for the user, potentially triggering other provisioning events to occur.

The permissions established in this table can be a blanket allow/deny, or include a set of filters to control time of day, and day of week.

During active sessions, a subscriber must be assured that these applications will only be able to position the MS when the subscriber is directly engaged with the application (ie. active session). Appropriate privacy options for subscribers to control access by these types of services are:

- Always Allow
- Allow with time/day filter
- Allow with notification (only notification, not "ask")
- Never Allow

Passive requests may come at any time and rarely will occur when the user is engaged with the actual application. Their engagement with the application itself is not always correlated to the positioning event. In these cases the subscriber is much more likely to select a notification feature, with additional controls related to the *release* of information.

For non-call-related sessions, it is reasonable that the subscriber will want:

- Notification that a positioning request has been received
- Knowledge of which application is requesting their position
- Yes/No option to release position information to the application

3.2.5 ID Protection Services

Location Studio supports advanced features to support anonymous and private exchange of location data with Client applications. The primary method of protecting subscriber identity is through the use of aliases, from which the MIN/MSISDN is not easily derived. Location Studio supports a very flexible alias function, including:

- Internally generated temporary (one use only) and persistent identifiers
- Synchronization with external identifier managers (such as those generated within a WAP gateway, or messaging gateway)

- Distribution of identifiers (exchange with client applications) during subscriber-initiated service invocation and for community services originated from fixed-network (Internet) access

The use of subscriber aliases is mandatory by regulations or law in some jurisdictions.

The type of identifier used depends upon operator preference (the use of an external identifier vs one generated by Location Studio), the Client profile settings (specifies the valid identifier type for that Client) or the type of positioning scenario (active vs passive positioning).

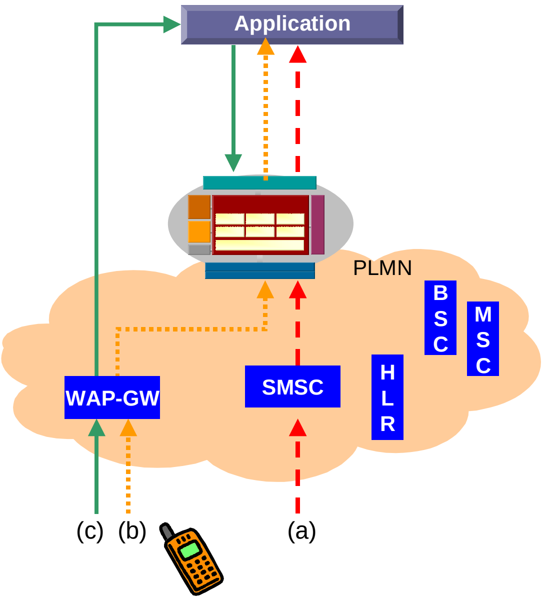
A Temporary Subscriber Identifier (TSID) is generally used when the mobile station is engaged in an **active** session with an LBS application, and the subscriber has initiated a service requiring its location be provided to the Client. Active sessions will use the Invocation Proxy feature of Location Studio to originate the LBS service using either WAP or SMS data services. Active sessions are commonly associated with information-type services (eg. find-the-nearest services) and some games/entertainment services where no persistent association between the subscriber and the end service is required.

A Persistent Subscriber Identifier (PSID) is generally used for **passive** positioning requests – when the request is made by the Client application independent of any current action of the target mobile station. The mobile station may be in any state: off, idle, active with voice session, active with data session. Passive sessions are commonly associated with tracking or community (ie. friend-finder) types of services where a persistent association between the subscriber and the end service is required.

3.2.6 Proxy Services

Location Studio provides both WAP and SMS proxy functions for user invocation of WAP and SMS-based services. The WAP and SMS invocation proxies support both information and community types of services, and provide key features necessary to support identification of subscriber-originated (active sessions) and applicable client access privileges.

The proxy functions are illustrated in the following diagram:



The Location Studio WAP proxy enables the following features:

- Replacement of MSISDN or WAP gateway generated identifier with Location Studio-generated subscriber identifiers (TSID/PSID). The TSID/PSID may be used by the application to position the MS, and send or receive SMS messages.
- TSID/PSID identifiers enable anonymity (application does not know subscriber identity or MIN/MSISDN). The PSID is persistent from connection to connection and can provide Personalization and Instant Sign-on capabilities.

The WAP proxy feature requires that Location Studio proxy all traffic to and from the specified Client for the duration over which positioning requests are to be authorized. Location Studio will proxy requests to the client, translating all URLs to and from the client. Location Studio will track state on requests to the client in order to translate the URL to the appropriate client URL on the response.

A key feature of Location Studio is the support of Mobile Originated SMS for LBS service invocation. This feature allows for creation of easy to use messages that will perform a function within an application and return a SMS message with the result. An example would be to send a command word of “FIND” followed by a word describing what you are looking for “Pizza” and the application could then return information about the 3 closest pizza restaurants. This interface can be utilized to SMS enable applications that currently are only Web and WAP enabled.

The Location Studio SMS proxy enables the following features:

- Delivery of temporary and persistent subscriber identifiers (TSID/PSID), which are used by the application to position the MS, and send or receive SMS messages (content or commands).
- TSID/PSID identifiers enable anonymity (application does not know subscriber identity or MIN/MSISDN). The PSID is persistent from connection to connection and can provide Personalization and Instant Sign-on capabilities. The TSID is generated uniquely for each user-invocation and when used for a location request is used to correlate with the call-related session status.

The SMS proxy feature requires that Location Studio proxy all traffic to and from the specified Client. Location Studio will proxy requests to the client, translating MIN/MSISDN to TSID/PSID for each transaction. Location Studio will track state on requests to the client in order to tracks call-related (active) status.

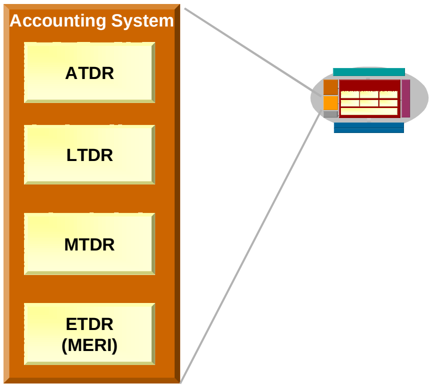
3.2.7 Notification Services

Location Studio supports notification options for each Subscriber-to-Client association (permission) based on either SMS or WAP-push messaging. There are subscriber-specific default permissions that apply to all Clients newly provisioned into the Subscriber’s profile (authorized for access by the operator). The subscriber can further modify all permission options (including notification) on a Client-by-Client basis. The notification options provided are as follows:

- Notify only
- Notify with response required
- Do not notify

Notify only will always use MT-SMS as the standard delivery as it is sent after the positioning event is completed and it is assumed a low priority.

3.3 Accounting System



Accounting functions in Location Studio are accomplished by the generation of log files containing Transaction Detail Records (TDRs) applicable to the specific transaction. Location Studio provides 4 different types of Transactions Detail records:

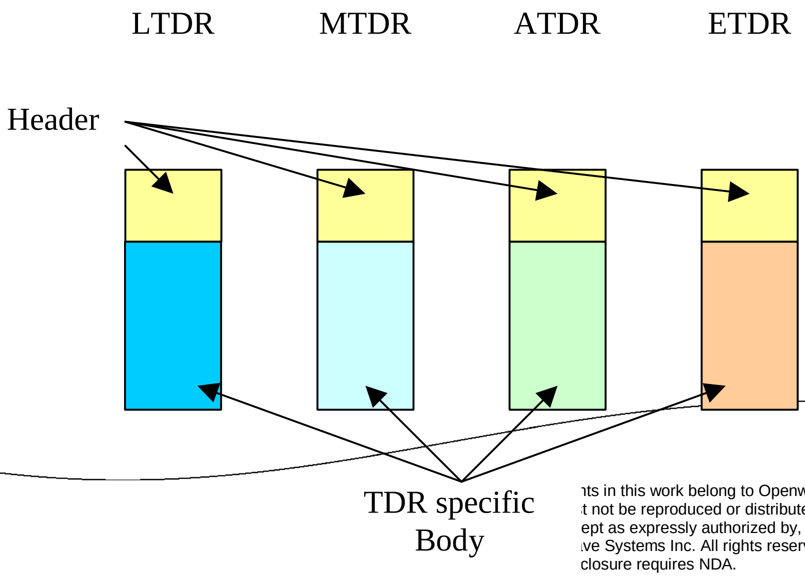
a) ATDR- Application Transaction Detail Record

b) LTDR - Location transaction Detail Record

c) MTDR- Messaging Transaction Detail Record

d) ETDR- External Transaction Detail Record

The following subsections describe the parameters that comprise the log records that are generated by Location Studio for each TDR. A configurable character delimits each field within the TDR, with the default delimiter being the pipe. (i.e. |) The following picture illustrates the composition of the different



TDR entries:

For example, the LTDR is comprised of two distinct segments. The first segment contains parameters that are common to all Transaction Detail Records. The second segment contains parameters that specific to location transactions.

The contents of the header are as follows:

ID	TDR Parameter	Comments
1	Record Type	This parameter is used to record the “type” of log record that has been generated.
2	Log Transaction ID	This parameter is used to record a sequentially generated ID for auditing of log records.
3	Timestamp of Request Initiation	YYYY/MM/DD HH:mm:ss:zzz
4	Recording Entity	This parameter is used to record the entity (and instance) that generated the log file.
5	Transaction Status Code	This parameter is used to record the status of a transaction, such as, whether the transaction was successful or not and if there are any additional explanations on that status.
6	Time to Complete Transaction	Complete Time minus Request Time

3.3.1 ATDR- Application Level Billing

Application Transaction Detail Records (ATDR) submitted by Clients provides the operator with billing information on service (application) level and allows correlating micro transactions like LTDR and MTDR.

ID	Parameter	Comments
1	Client Name	This is the originator of the WBI request
2	Mobile ID	The international number associated with the Mobile Station which the message is sent to. If an alias is used, the actual international MIN or MSISDN will be recorded here.
3	Requesting ID Type	PSID|TSID|MSID|OSID
4	Requesting ID	Actual OSID, TSID, PSID used in the transaction.

ID	Parameter	Comments
		If MSID is used this will be left empty
5	Event ID	The ID of the event that has occurred. This meaning of this value is known by the client and the operator.
6	Start Time	Start time of the event
7	End Time	End time of the event
8	Tracking ID	ID provided by Client in order to track the billing record.

3.3.2 LTDR

Every location request going through Location Studio generates a Location Transaction Detail Record (LTDR) with information about the located subscriber and the client identifier.

The following is a partial list of parameters available in the LTDR:

ID	Parameter	Comments
1	Mobile ID	This parameter is used to record the international number associated with the Mobile Station being positioned. If an alias is used, the actual international MIN or MSISDN will be recorded here.
2	Request Type	Immediate, Periodic, Update, Deferred
3	Location Information – Latitude	[-]DDMMSS.sss (default MLP format, as used by LSt 2.0)
4	Location Information – Longitude	[-]DDDMMSS.sss (default MLP format, as used by LSt 2.0)
5	Location Information – Altitude	In meters If not available, this field should be left empty.
6	Uncertainty Returned – Horizontal	Radius of a circle around the requested position within which the position of the MS will be 90% of the time. Measured in meters
7	Uncertainty Returned – Vertical	Radius of a circle around the requested position within which the position of the MS will be 90% of the time.
8	Client Name	This value is a cross reference from the Client Profile (FRIENDLY_NAME)

ID	Parameter	Comments
9	Requesting ID Type	PSID|TSID|MSID|OSID
10	Location Server Transaction ID	The unique transaction ID between the LM and either the LSt or a Openwave WLA. If another Location server is used, that transaction ID is recorded.
11	Requesting ID	Actual OSID, TSID, PSID used in the transaction. If MSID is used this will be left empty
12	Originator	This is a direct record of the contents of the originator field from the MLP interface.

3.3.3 MTDR

Messaging transactions between Clients and Subscribers are recorded in a Messaging Transaction Detail Record (MTDR) with information about message bearer (e.g. SMS, WAP), clients and subscriber identifier.

ID	Parameter	Comments
1	Client Name	From FRIENDLY_NAME in the client profile
2	Mobile ID	The international number associated with the Mobile Station which the message is sent to. If an alias is used, the actual international MIN or MSISDN will be recorded here.
3	Requesting ID Type	PSID|TSID|MSID|OSID
4	Requesting ID	Actual OSID, TSID, PSID used in the transaction. If MSID is used this will be left empty
5	Delivery Method	SMS or WAP
6	Originator	

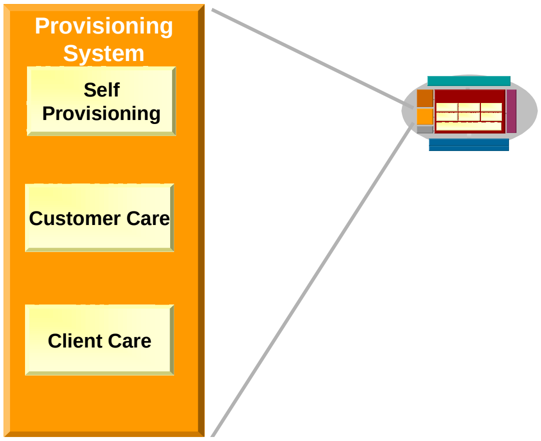
3.3.4 ETDR (MERI)

3rd party middleware extensions connected through the MERI interface may submit specialised External Transaction Detail Record (ETDR), which will then be forwarded to the operator as any other TDR.

ID	Parameter	Comments
1	MERI name	This is the MERI component name
2	Client Name	This is the originating client

ID	Parameter	Comments
3	Mobile ID	The international number associated with the Mobile Station has utilized the MERI component If an alias is used, the actual international MIN or MSISDN will be recorded here.
4	Requesting ID Type	PSID|TSID|MSID|OSID
5	Requesting ID	Actual OSID, TSID, PSID used in the transaction. If MSID is used this will be left empty
	Event ID	The ID of the event that has occurred. This meaning of this value is known by the client and the operator.
6	Start Time	Start time of the event
7	End Time	End time of the event
8	Tracking ID	ID provided by Client in order to track the billing record.

3.4 Provisioning System



Location Studio includes a full-featured HTML-based graphical user interface to allow Operator personnel to:

- Add/delete/modify Client Application profiles
- Add/dele/modify Subscriber profiles
- Create and modify subscriber privacy permissions

3.4.1 Client Care

The Client Care component of the provisioning user interface allows selected operator personnel to add/modify/delete Client profiles. This interface is used to establish the access privileges and default handling behavior for requests of Location Studio services from external Clients. This User Interface is provided as the primary access point for Client Profile management and may be used with little or no customization.

Operator personnel that access this interface are part of a unique user role, so that access to Client Management can be restricted.

3.4.2 Customer Care

Customer Care functions are provided for basic provisioning of Subscribers, and Subscriber preferences (including privacy settings), into Location Studio. The Customer Care component of the provisioning user interface allows selected operator personnel to add/modify/delete Subscriber profiles.

However, this Customer Care user interface is **not** intended for deployment to the entire population of customer care representatives in an operator’s network – that interface can be greatly simplified by integrating common features with the pre-existing Customer Care and Activations system. Rather, this user interface is provided as out-of-the-box functionality for modifying Subscriber Profiles before IT integration is complete and as a secondary access point.

Operator personnel that access this interface are part of a unique user role, so that access to Subscriber Management can be restricted.

To support integration of Location Studio to the operator’s customer care and activations systems an extensive XML provisioning API provides access to all data elements of Location Studio that define:

- Client Profiles
- Subscriber Profiles
- Privacy Permission Sets
- Real-time updates can be submitted through this interface.

It is not necessary to provision all subscribers in order to give them access to location-based services. The Self-provisioning functionality allows Location Studio to automatically provision a subscriber “on-the-fly” when he/she is accessing a service the first time.

3.4.3 Self-Provisioning

Subscriber self-provisioning is desirable whenever possible to reduce the impact of new services on the operator’s support organization. Self-provisioning is provided in Location Studio in two basic forms:

WEB/WAP and SMS interfaces for subscriber personalization of services and their privacy profile

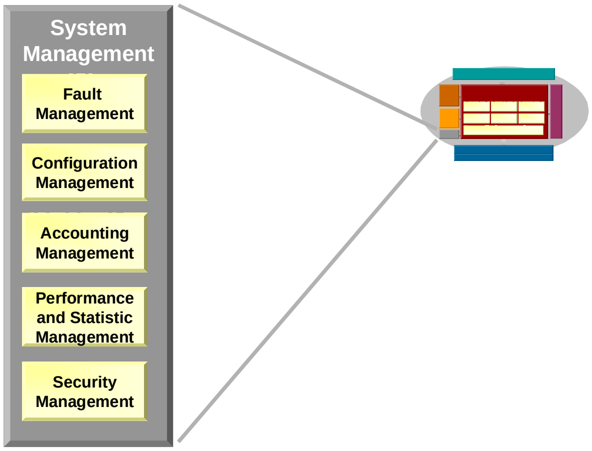
First-time-through service handling to direct subscribers to personalization tools

If a subscriber accesses a service, and the subscriber has not yet authorized the service to make position requests, there are two ways to support automated first-time-through activation of the service:

If the subscriber accesses a WAP service directly the application can redirect the WAP session to the subscriber WAP provisioning interface to set the authorization. If access is via SMS a subscription command can be sent as a text message to the subscriber who then must send that command to Location Studio to enable the service (complicated procedure – may be best to send text message prompting them to call customer care).

If access to the application is through the SMS or WAP proxy function of Location Studio then the redirection to the subscription utility can be more direct (preferred approach)

3.5 System Management



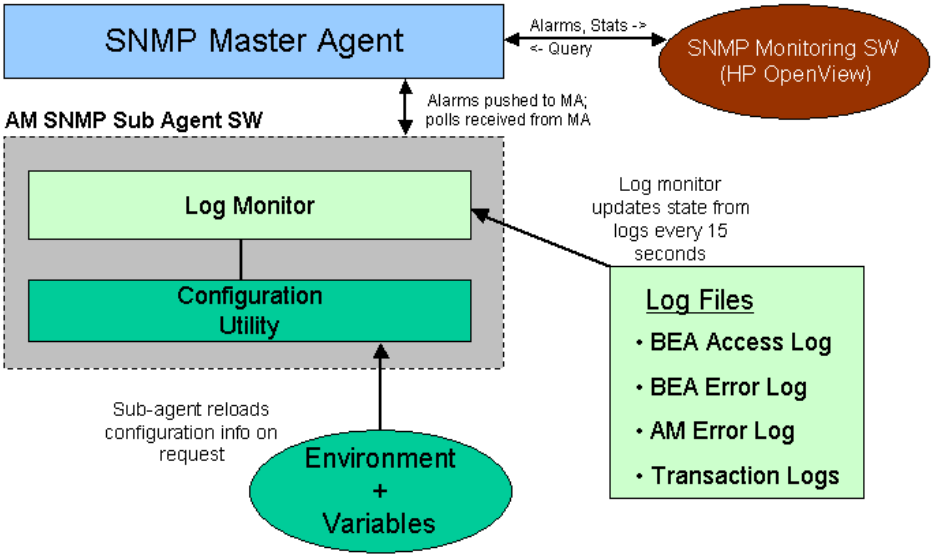
3.5.1 Fault Management

SNMP (Simple Network Management Protocol) is an open industry standard that may be used to manage Location Studio processes. SNMP management will be compatible with many wireless network elements by multiple manufacturers. SNMP consists of a:

Management System - monitors and controls network elements and processes. The Management System may also be referred to as an SNMP Manager. SNMP Managers are typically GUI applications from Hewlett Packard, Sun, Microsoft and others. Any standard SNMP package may be used to interact with Location Studio (the managed system).

Managed System - collection of applications and network elements. The managed system is Location Studio, which consists of various application modules and processes. An SNMP Agent is developed to manage Location Studio. Location Studio status, log files, statistics, and external connections and security will be managed and monitored by the SNMP manager. The specific processes and functions are defined through a management information base (MIB).

In a wireless network there may be many SNMP agents. Location Studio will be one of many agents. Multiple SNMP agents may be managed under a master agent.



- The Location Studio application SNMP process is a sub-agent
- The master-agent is provided as part of the operating system (Solaris, Tru64). For example, Solstice Enterprise Agent is provided by Solaris
- Each master-agent's capabilities may vary, but in general they provide monitoring of HW and system resources (memory, disk, etc.)
- Location Studio MIBs are SNMP v2 compliant

3.5.2 Configuration Management

- The persistent configuration for a domain of WebLogic Servers and clusters is stored in an XML configuration file. You can modify the configuration file in three ways:
- Through the Administration Console, BEA WebLogic Server's Graphical User Interface (GUI) for managing and monitoring a domain configuration. This is intended as the main way to modify or monitor the domain configuration;
- By writing a program to modify the configuration attributes, based on the configuration Application Programmatic Interface (API) provided with WebLogic Server; or

- By running the WebLogic Server command-line utility for accessing configuration attributes of domain resources. This is provided for those who want to create scripts to automate domain management.

Several configuration files control the behaviour of Location Studio software. The configuration files are XML based and each module has its own unique file. There is also one file that contains global parameters that all modules access through the environment.

There is a validation tool, which verifies the files and makes backups of old versions. This tool makes the configuration controllable, reversible and recoverable. The same verification is used when the modules read their corresponding configuration files, thus guaranteeing consistency.

3.5.3 Accounting Management

All collected billing information, such as LTDRs or MTDRs is provided as plain delimited ASCII file for easy post-processing with operator's billing engines. For each operator a post-processing tool may be developed as a professional service to fit the TDRs to the operators billings system. Additional tools may also be required to help integration to a real-time billing system, as well as file downloads to/from the billing system.

3.5.4 Performance and Statistics Management

In Location Studio, performance management is provided through NMS monitoring of a number of key-performance indicators such as Average response time, average TPS during the last X requests etc.

In addition, reporting and analysis tools can be provided to monitor these indicators and calculate other statistics: such as grade of service, response times, failed requests, interface usage etc. These tools use the extensive TDR and log files as a base.

Additionally, the BEA WebLogic Server Administrative interface may be utilized to monitor a number of important application server metrics.

3.5.5 Security Management

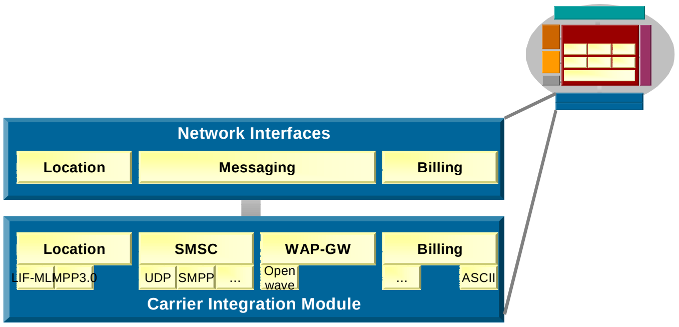
Security management in Location Studio utilizes wherever possible the security features of the core operating system and platform. Security features of the UNIX operating system can meet operator requirements though there is a need to "harden" the system configuration by removing known security gaps.

Implementing security in a WebLogic Server deployment consists of configuring the fields that define security policy for a particular deployment. WebLogic Server provides an Administration Console to help define the security policy for a particular deployment. Using the Administration Console, indicate security-specific values for the following elements of your deployment:

- Realms
- Users and Groups
- Access Control Lists (ACLs) and permissions for WebLogic Server resources
- SSL protocol
- Mutual authentication

- Audit providers
- Custom filters
- Security context propagation

3.6 Network Integration



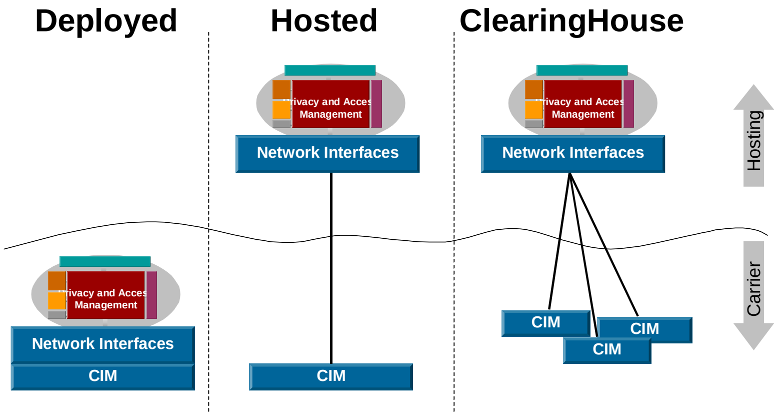
3.6.1 Carrier Integration Module

The Carrier Integration Module (CIM) of Location Studio provides the points of physical interface to the operator’s network. One instance of Location Studio supports multiple CIMs in order to interface to:

Multiple operator networks, when Location Studio is deployed in a hosted environment for clearinghouse or portal applications

A single operator network with a subscriber population divided amongst multiple network nodes (ie. multiple location servers)

The following diagram illustrates the various deployments of the Carrier Integration Module:



In the *deployed* scenario, Location Studio is installed within an operator's network and there is typically only one CIM. In the *hosted* scenario, only a single CIM is deployed in the Operator's network and the remaining functionality of Location Studio is hosted at a separate location. In the *ClearingHouse* scenario Location Studio is used as a cross-carrier gateway – to interconnect multiple networks and share applications. In this case multiple CIMs tie back to a single Location Studio core element.

When multiple CIM are deployed, the selection of CIM is controlled within the Operator profile, and the association of Subscribers to CIMs is set by the Operator attribute of the Subscriber profile.

3.6.2 Location Server Interface

Location Studio supports connectivity to industry-leading GMLC and MPC location servers compatible with the following interfaces:

- SGSF Location Manager (TWLI)
- Generic GMLC (LIF-MLP 2.0 or higher)
- Ericsson MPS 3.0 (MPP 3.0)
- Others as required

3.6.3 SMSC Interface

Location Studio supports inbound (service invocation) and outbound (e.g. notification) messaging via SMS, with standard support for the following industry leading SMSCs and protocols:

UCP	- CMG,
SMPP	- Logica, Sema, CMG
CIMD2	- Nokia
Others as required	

A Key feature of the SMSC interface is the ability to give the Operator a method to SMS -enable existing applications. The SMSC interface does this with its ability to act upon commands such as "search" to translate and route this request to a specific application using HTTP. An example would be a subscriber sending the SMS of "find pizza" to a short code and the SMSC interface would handle this request by routing the request as an HTTP request to an existing Yellow Pages application and then return information about the closest pizza places to the subscriber.

3.6.4 WAP Gateway

Location Studio supports inbound (service invocation) and outbound (e.g. notification) messaging via WAP and SMS, including the following industry leading gateways and protocols:

- Openwave
- Nokia

- CMG

Location Studio will also integrate with the WAP GW to exchange the gateway-generated WAP-ID and convert it to a MIN/MSISDN. The gateway-generated WAP ID is an example of an Operator-generated Subscriber ID (OSID), which is used as an alias for wap-based services. By integrating with the WAP Gateway to convert WAP-IDs, it is possible for applications to use the WAP-ID for requests top Location Studio.

3.6.5 Billing Mediation Interface

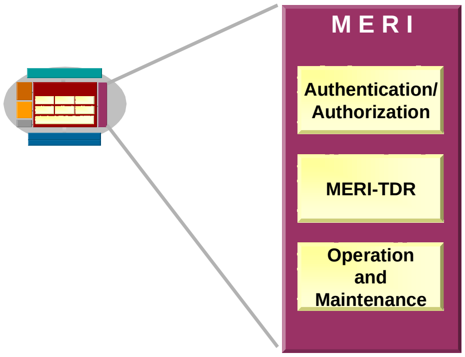
Location Studio generates log files to record transactions, and to enable fault analysis and billing mediation. Log files are to be periodically exported to a specified OSS server. The implementation of this is a standard part of the systems integration phase of Location Studio deployment.

Location Studio provides integrated Transaction Detail Record (TDR) capabilities. All service requests from Client applications generate a specific transaction log entry, stored in delimited flat text files with UTF-8 encoding (the logging system is globalized, allowing for localization). Log files are offloaded from the platform on a routine basis via scheduled FTP/RCP.

TDRs are provided for statistic analysis and billing mediation.

3.7 Middleware Expansion Request Interface (MERI)

Location Studio generates log files to record transactions, and to enable fault analysis and billing mediation. Log files are to be periodically exported to a specified OSS server. The implementation of this is a standard part of the systems integration phase of Location Studio deployment.



Location Studio supports integration with third-party toolkits using the MERI (Middleware Extension Request Interface) API. Examples of third-party toolkits are:

- Geo-server
- Mapping
- Routing
- Geo-coding
- Content manager

- Points-of-interest/landmarks
- Geo-coded content
- Zone service
- Point-to-polygon (zip code, community, city, country, …)

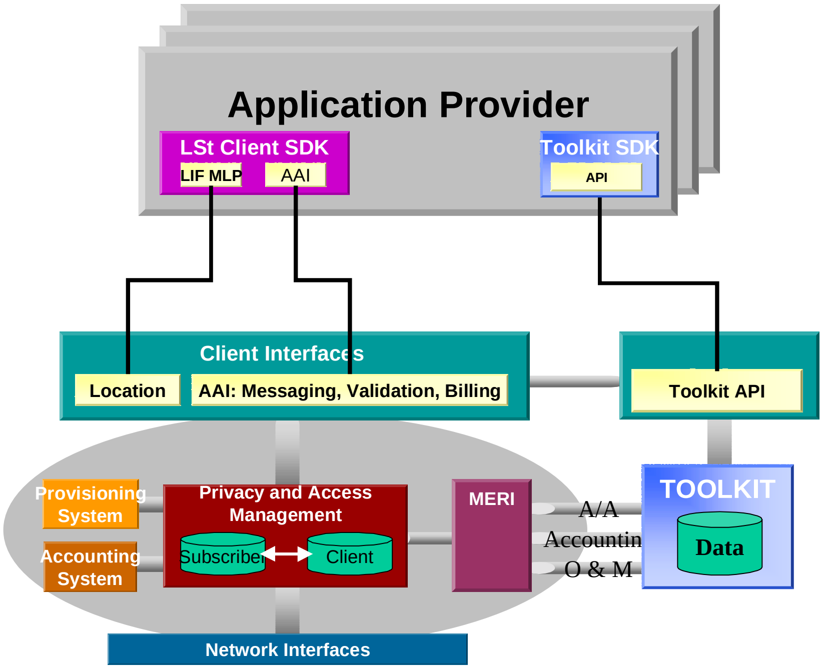
The MERI API extends core functions of Location Studio to complete toolkit transactions transparent to the underlying operator network infrastructure and requesting applications. These core functions include:

Client Authorization: the request type submitted by the Client is authorized against access privileges established within the Client profile in Location Studio. This allows maintaining profile data in one place only.

Accounting: The toolkit server may submit transaction result information to Location Studio, which will in turn generate an Extension-Transaction Detail Record (ETDR) with format, content and transfer mechanisms consistent with all other TDRs generated within Location Studio. A tracking ID will allow for correlating of external transactions with consolidated application-level billing records (such as ‘found 3 friends’, ‘found localized content’, …).

LBS surveillance: health and status monitoring functions are extended through the MERI to the toolkit application and platform to provide visibility to the network management system integrated to Location Studio. This allows a complete Location Based Service surveillance rather than monitoring third-party toolkits separately.

This integration is illustrated in the following diagram:



The benefits of integrating toolkits through the MERI API of Location Studio are:

- Single Client Profile to establish authorizations and access privileges.
- One format of TDRs and single-point of integration to operator billing and reporting systems.
- Single-point of integration to network management system providing visibility to health and status of toolkits along with other location infrastructure.
- Consolidation of micro-transactions to event-level billing.
- Consistent access methodology for applications, and compatibility with subscriber ID protection services (alias functions).
- Native API of the toolkit is preserved, so that applications previously integrated to the services do not need to adapt to a completely different interface.
- Simplifies transition to a consolidated API for all location services (such as the OGC OpenLS API, or a broader LIF API).

4. Use Cases

The following call flows illustrate how Location Studio facilitates the delivery of a premium-billed, location-intelligent services using either SMS or WAP as a bearer. This is a subscriber-initiated (“pull”) service and the key functionality required for this call flow is:

- Protect the anonymity of the subscriber at all times
- Allow for validation of the subscriber identity (will the operator support premium billing for this subscriber)
- Provide support for post-paid and pre-paid subscribers
- Support billing based on an event relevant to the subscriber (ie. obtained premium content) rather than on transactions measurable by the operator (location request, SMS message, content lookup, …), especially where multiple transactions may be required to complete one relevant service delivery
- Allow the Application Developer to define the specify the amount of the premium charge
- Support any combination of WAP and SMS for service invocation and content delivery

Premium service example: a mobile subscriber invokes a service to find the location of the nearest parking facility with space currently available. The subscriber is positioned by the LBS application and the obtained position is used to search a database of available parking spaces within a pre-defined radius of the subscriber’s reported location.

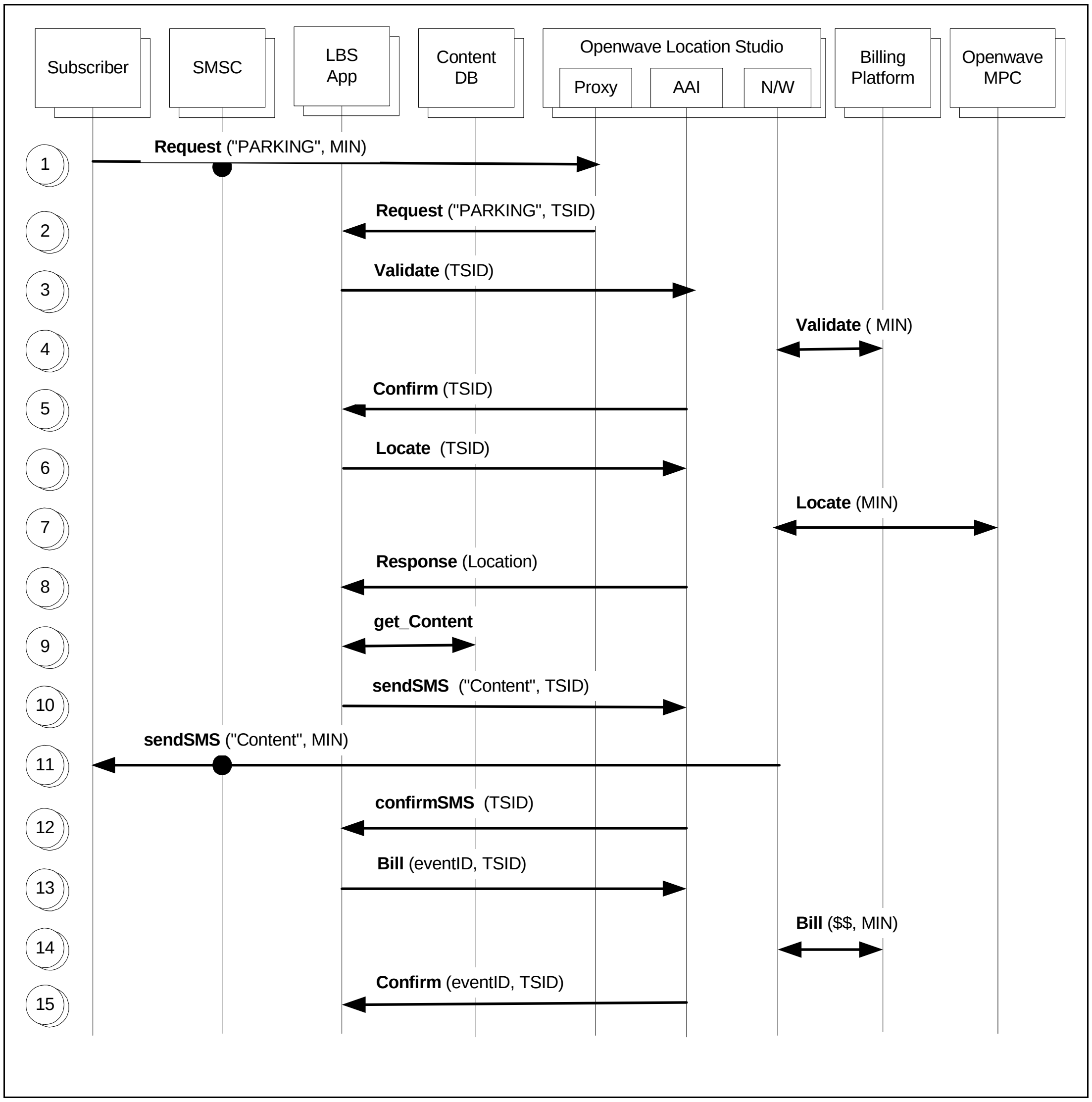
4.1 Call Flows Assumptions

The following assumptions are made:

- The Sample Call Flow below provides a high-level overview of functional interaction with Location Studio only, and does not deal with other aspects such as application authentication, subscriber privacy or quality of service issues
- The Application Developer is responsible for hosting its own database of parking facilities, and a real-time feed that provides parking capacity (simple full/available indicator) at each facility.
- This call flow assumes a North American CDMA network, and that the network is capable of providing location to the Openwave Location Manager Mobile Positioning Center (MPC).
- This call flow is equally valid in a GSM network, in which case Location Manager is configured as a Gateway Mobile Location Center (GMLC) and the mobile station is identified by its Mobile Station ISDN (MSISDN).
- The necessary integration work with the operator’s billing platform (including Pre-Paid system) interface has been completed, and supports the detailed actions.

Note: This call flow has been simplified to illustrate the example. More precise definition of service requests and required parameters may be found in the AAI Interface Control Document.

4.2 SMS Call Flow



1. A mobile subscriber originates an SMS message with the keyword “Parking” in the text field. The SMS command is addressed to a short code, which terminates within the Location Studio SMS Proxy and uniquely identifies the destination application (LBS App) for this service. The SMSC recognizes the mobile station by the Mobile Identification Number (MIN) and generates appropriate SMS bearer charging.

2. The Location Studio SMS Proxy substitutes the MIN with a Temporary Subscriber IDentifier (TSID), and forwards the keyword “Parking” and TSID to the LBS App.

3. The LBS App submits a validation request to Location Studio, using the validation service of the AAI, to ensure that the subscriber is authorized to use the service.

4. Location Studio (LSt) validates that the subscriber identified by the TSID is authorized to use the requested service (LBS App) and, if the subscriber is a pre-pay customer, it is possible to extend this validation to test the pre-pay billing platform to qualify the subscriber status.

5. LSt responds to the validation request indicating the subscriber is authorized, and has a positive billing status.

6. The LBS App submits a location service request via the AAI using the TSID to identify the subscriber.

7. LSt requests and receives the subscriber location from the Openwave *Location Manager* Mobile Positioning Center (MPC).

8. LSt responds to the location service request with the required subscriber location.

9. The LBS App uses the subscriber's location to search a content database for the nearest parking facilities that have available parking. The content database may be local to the LBS App (ie. in an Oracle spatial database), or it may be a remote database managed by a third-party content provider (or the operator).

10. The LBS App formats the available content as a text message and submits the text for SMS delivery to the subscriber using the messaging service of the AAI. The subscriber is once again identified in the request using the same TSID obtained from the SMS Proxy in step 2.

11. LSt submits the content received from the LBS app and formats it in an SMS text message to the SMSC for immediate delivery to the subscriber. The TSID ids used

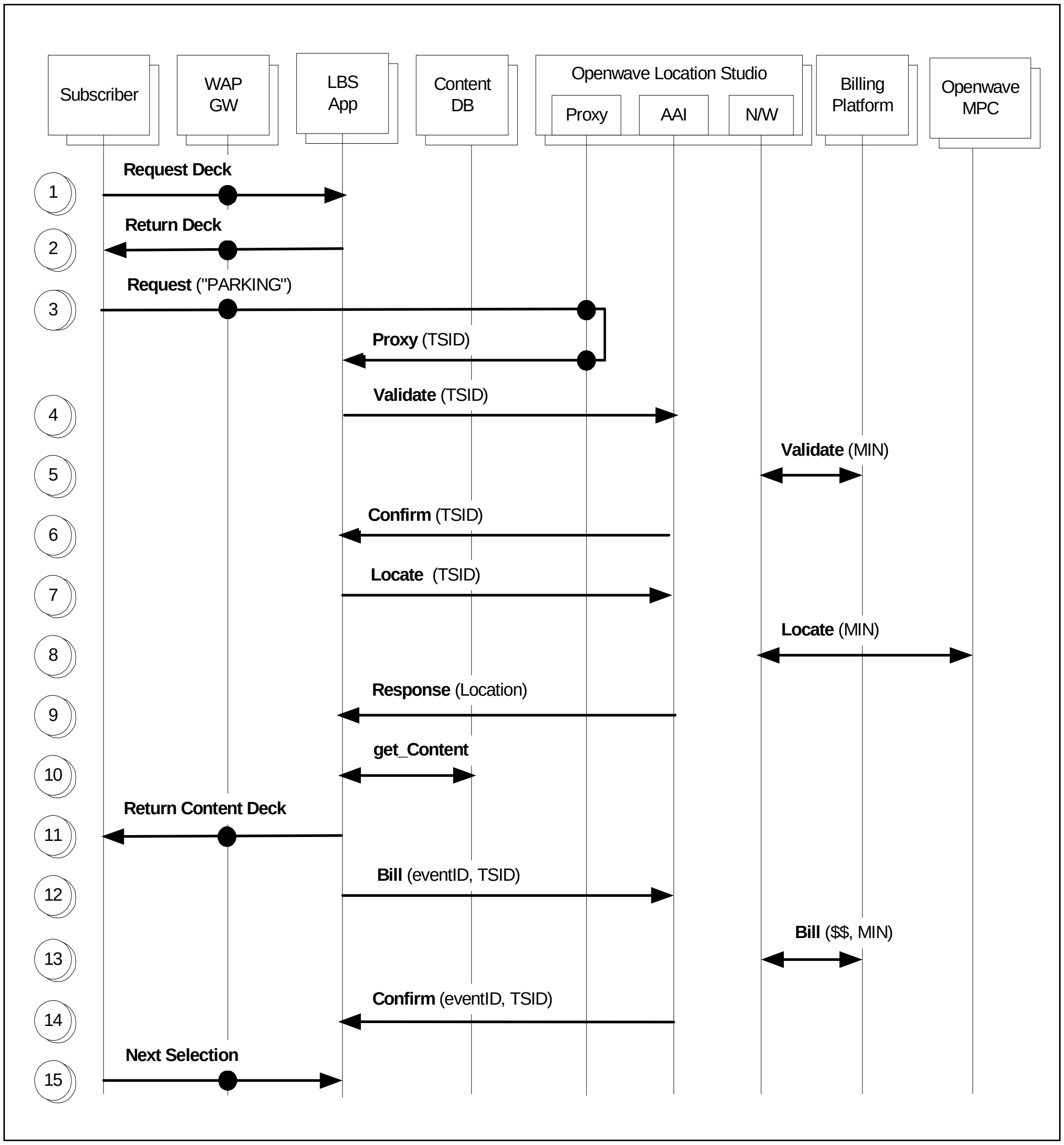
12. LSt confirms submission of the SMS message to the SMSC, but not receipt of the message by the subscriber.

13. Upon successful delivery of service to the subscriber the LBS App submits a billing request to LSt, along with an eventID, using the billing service of the AAI. The eventID indicates to the billing system the total service charge.

14. LSt processes the request and interacts with the Billing Platform to debit funds for pre-pay customers, or for a post-pay subscriber, to create a CDR for the event.

15. LSt confirms the successful billing event.

4.3 WAP Call Flow



1. A mobile subscriber originates a WAP session with the LBS Application.
2. A WML decks is presented to the subscriber with some cards that link to a service that requires a location update to complete, and some that do not require location information. The cards that require a location update link to the WAP Proxy in Location Studio.
3. The subscriber selects a card for the “Parking” service. The card contains a URL that terminates within the Location Studio WAP Proxy and contains parameters that indicate where to return the subscriber

WAP session when the proxy function is complete. Location receives the identify of the mobile station (MIN) from the WAP Gateway and generates a TSID for use by the LBS App for subsequent (time limited) transactions with Location Studio. The TSID is returned as a parameter in the URL that is re-directed to the LBS App.

4. The LBS App submits a validation request to Location Studio, using the validation service of the AAI, to ensure that the subscriber is authorized to use the service.
5. Location Studio (LSt) validates that the subscriber identified by the TSID is authorized to use the requested service (LBS App) and, if the subscriber is a pre-pay customer, it is possible to extend this validation to test the pre-pay billing platform to qualify the subscriber status.
6. LSt responds to the validation request indicating the subscriber is authorized, and has a positive billing status.
7. The LBS App submits a location service request via the AAI using the TSID to identify the subscriber.
8. LSt requests and receives the subscriber location from the Openwave *Location Manager* Mobile Positioning Center (MPC).
9. LSt responds to the location service request with the required subscriber location.
10. The LBS App uses the subscriber’s location to search a content database for the nearest parking facilities that have available parking. The content database may be local to the LBS App (ie. in an Oracle spatial database), or it may be a remote database managed by a third-party content provider (or the operator).
11. The LBS App formats the available content as a WML deck and returns the deck to the subscriber. As an alternative, or as an option within the deck, the LBS App may return the content formatted as a SMS text message, and may use the messaging service of the AAI to deliver the text message (not shown in this call flow).
12. Upon successful delivery of service to the subscriber the LBS App submits a billing request to LSt, along with an eventID, using the billing service of the AAI. The eventID indicates to the billing system the total service charge.
13. LSt processes the request and interacts with the Billing Platform to debit funds for pre-pay customers, or for a post-pay subscriber, to create a CDR for the event.
14. LSt confirms the successful billing event.
15. The subscriber continues navigation of the WML decks of the LBS Application. As in Step 2, some cards may require a location update to continue, in which case they are routed through the LSt WAP Proxy, and others simply interact directly with the LBS App and do not require use of the proxy.

5. Conclusion

Successfully deploying Location Based Services requires careful planning to ensure smooth deployment of initial services, and a cost effective strategy to enable the delivery of a broad spectrum of services. There is no single killer application that will ensure a profitable business model and the selection of location middleware can have a large impact on the business case for incremental service offerings.

In addition to facilitating lower cost of deployment, location middleware is an essential component for the total solution:

- The LCS Standards do not provide a comprehensive or efficient privacy management framework
- A single, carrier-controlled privacy profile is easier for customers to manage and understand, as well as for network operators to deploy

Current XML-based access interfaces defined within the standards bodies do not contemplate critical elements:

- Subscriber aliasing for anonymity
- SMS service invocation
- Billing and charging interfaces
- The delivery of geo-toolkits through the middleware layer provides:
- Access by applications to common services, such as: driving directions, mapping, and geo-coding
- A single-point of control for the operator to enable, or disable access to the geo-toolkit
- Transaction records to facilitate reconciliation (fee for use) with application providers
- Integration of LBS services with existing customer care and activation processes
- Subscription validation

Location Studio has been carefully designed, so that it fills in where the standards fall short. Location Studio is a proven middleware platform – deployed commercially today, and integrated with the application offerings of Openwave, and its partners through the local.Info Alliance program.

Author
Ron Poulin
Principal Product Manager
Openwave Systems Inc.

Ron.Poulin@openwave.com

Feedback

whitepaper.feedback@openwave.com

OPENWAVE®

Openwave Systems Inc.
1400 Seaport Boulevard
Redwood City
California 94063
U.S.A.
Corporate +1 650 480 8000
Europe +44 1442 458 800
Japan +81 3 5909 6100
http://www.openwave.com