Enabling location-based services through passive monitoring techniques:

Mobile positioning with the HINTON Locator probe

A White Paper from Telesoft Technologies

DX-HIN-GEN-MK-WP-32640-02

Where **innovative thinking**
meets **engineering excellence**

Contents

Executive Summary

The geographical location of mobile subscribers has become an important topic with profound implications for a wide range of applications, known generically as “Location-Based Services” (LBS). Alongside the commercial opportunity for LBS applications, legal and social obligations – such as lawful interception and intelligence-related data acquisition, and public Emergency E911/E112 services – also depend on the acquisition of subscribers’ geographical location information. These services can be extremely valuable, both for gathering intelligence and for the support of value added services (VAS). Moreover, the potential for such services has only recently started to be exploited, and the value associated with these is likely to increase significantly in the coming years. Analyst firm ABI Research predicts growth in commercial LBS from $111 million in 2008 to $2.2 billion by 2013.

In order to support LBS, the position of mobile devices must be determined accurately and consistently. It is possible to interrogate the parameters in mobile network signalling via the use of passive monitoring probe solutions. To achieve this, probes need to be deployed at the edge of the network, as close as possible to the radio interface used by mobile terminals for communication. There is a trade-off between the most accurate rendering of such data and the cost of deploying such systems as overlays into a mobile network.

There are a variety of techniques that can be used to provide information to support LBS. Each has different levels of accuracy, but there is also a cost associated with each. However, there are other techniques which, when combined, can generate resolution within a range of 100 – 500m, which is sufficient for a wide range of potential applications, including emergency service access under US E911 laws. Collectively, techniques which depend on data available over wired or physical connections are known as “network based”, in contrast to those that are made via direct interaction with the radio interfaces. Network-based techniques are not only much simpler and more cost effective to deploy, they also depend on information that is intrinsic to the mobile network. Mobile location data needs to be presented to equipment where it can be processed and accessed by applications.

In order to cost-effectively deploy and leverage the potential of LBS, a lightweight, passive solution that is capable of collecting location data from appropriate interfaces is required. The HINTON Locator meets this requirement, and leverages functionality inherent in the mobile network to capture location-related signalling information, allowing application developers and operators to use it to triangulate geographic position.

The HINTON Locator provides access to information that can support location techniques such as TA and CGI positioning, allowing application developers and operators to use it to triangulate geographic position. It is capable of acting as an external, network-based LMU to capture data from the Abis interface, and for intercepting information from the A-Interface.

The HINTON Locator from Telesoft Technologies provides a cost-effective, scalable platform that captures essential location information for the creation of valuable LBS. It can be layered onto an existing network and does not disrupt existing deployments. It offers future-proof technology, protecting existing investment and building long-term ROI.

Telesoft Technologies has decades of experience in the field of network monitoring and mobile signalling. Through the HINTON Locator, this expertise is available to assist the rapid deployment of LBS applications and support monetisation of key network assets in new and innovative ways.

Introduction

The geographical location of mobile subscribers has become an important topic with profound implications for a wide range of applications, known generically as “location-based services” (LBS). Alongside the commercial opportunity for LBS applications, legal and social obligations – such as lawful interception and intelligence-related data acquisition, and public Emergency E911/E112 services – also depend on the acquisition of subscribers’ geographical location information. These services can be extremely valuable, both for gathering intelligence and for the support of value added services (VAS). Moreover, the potential for such services has only recently started to be exploited, and the value associated with these is likely to increase significantly in the coming years.

In order to support LBS, the position of mobile devices must be determined accurately and consistently. As such, the mobile network must be equipped with resources that can determine the location of a mobile device in real time and present this data to applications that can process and act upon the information. This requires interaction with many of the elements of a GSM network and related technologies. There are two broad families of mobile network, governed by the 3GPP and 3GPP2 standards organisations. The 3GPP family is the dominant technology and includes standards such as GSM, GPRS, EDGE and UMTS and, in the future, LTE. 3GPP2 has adopted a broadly similar network architecture, but utilises a different radio access standard, based on CDMA and CDMA-2000 technology. Positioning information can be harvested from each of the main mobile technologies, although this paper will largely focus on the 3GPP family of GSM and its derivatives.

Positioning in mobile networks is a function of the location of the handset or terminal utilised by a subscriber, and the signalling that is used to measure signal strength and manage handover between cells conveys much of the information required to determine device location. Although information that can help determine location may be available, networks were not designed to automatically produce such information either to a high degree of accuracy, or in a format appropriate for LBS application support. It is possible to discover the parameters in mobile network signalling using passive monitoring probe solutions and, using sophisticated algorithms, determine the location of the terminal – and hence of the subscriber. In order to improve accuracy, it is essential to provide such location information to the highest degree of resolution. To achieve this, probes need to be deployed at the edge of the network, as close as possible to the radio access network (RAN) interface used by mobile terminals for communication. There is also a trade-off between the most accurate rendering of such data and the cost of deploying such systems as overlays into a mobile network. This paper discusses the techniques that can be cost-effectively leveraged to provide accurate location-based information, and proposes a solution that can be easily deployed by operators seeking to access location data, the HINTON Locator Probe.

Mobile Location Services – an Opportunity

Although the 3GPP standards body has avoided specification of specific services, they have provided a useful classification of categories of services that can be implemented by LCS Clients[1]. These include:

- Commercial LCS, or value added services (VAS);
- Internal LCS;
- Emergency LCS; and
- Lawful intercept LCS.

Commercial location services are typically revenue-generating services that offer value to a mobile subscriber based on their location. They are generally based around a “push” model, in which selected data is presented to mobile subscribers. This might be related to proximity to restaurants, for example, or special offers in local stores. Such services have implications for privacy, and additional policies and permissions have to be deployed in appropriate platforms in order to control access to services. These platforms are beyond the scope of the current paper.

Internal location services are primarily concerned with operations internal to the network, such as handover, although they may be concerned with reporting activities, such as traffic monitoring and capacity measurement.

Emergency location services are a vital element in the provision of emergency services to subscribers and are covered by legislation such as E.911 from the United States and E.112 from the European Union. These acts make provision for specific levels of accuracy in determining both horizontal and vertical position of mobile subscribers in order to assist in the provision of emergency assistance.

Lawful intercept location services form a specific category concerned with legally or officially sanctioned collection of data for use by law enforcement agencies and have become a vital element in the fight against crime and terrorism. Targets may be tracked individually or collectively via location tracking techniques.

Much of the growth in LBS has been associated with deployments to support emergency and lawful intercept applications. However, analysts have long predicted dramatic growth in the commercial sector. Commercial Mobile Location Services have been the poster child of value-added services enabled exclusively by mobile networks for some years. Despite optimistic forecasts from a number of analysts, the predicted market has not yet materialised. Nevertheless, there are increased grounds for optimism that the time for commercial LBS may finally have arrived.

Location based services categories	Standardized Service Types
Public Safety Services	Emergency Services
	Emergency Alert Services
Location-Sensitive Charging	
Tracking Services	Person Tracking
	Fleet Management.
	Asset Management
Traffic Monitoring	Traffic Congestion Reporting
Enhanced Call Routing	Roadside Assistance
	Routing to Nearest Commercial Enterprise
Location-Based Information Services	Traffic and Public Transportation
	City Sightseeing
	Localized Advertising
	Mobile Yellow Pages
	Weather
	Asset and Service Finding
Entertainment and Community Services	Gaming
	Find Your Friend
	Dating
	Chatting
	Route Finding
	Where-am-I?
Service Provider Specific Services	

Table 1: 3GPP Location Service Types

Increased penetration of advertising-funded mobile business models has led to greater acceptance of push or opt-in, services. Users are now more accustomed to being presented with data regarding potential services, providing that their privacy is protected. This stems both from new business models (such as that pursued by Blyk), as well as the now-ubiquitous Google advertisements. Subscribers are accustomed to seeing data presented according to their search preferences. This behaviour can be replicated in the mobile world, using familiar techniques such as SMS or via suitable mobile browsing portals. As a result, analyst firm ABI Research is predicting growth in commercial LBS from $111 million in 2008 to $2.2 billion by 2013[2]. This represents significant growth potential, as deployment moves from support of emergency infrastructure to commercial applications. Growth may be further stimulated by the emergence of passive positioning techniques that will reduce the cost of network deployments. Telesoft Technologies is at the forefront of initiatives in this marketplace.

There are many possibilities for commercial location services. These can be targeted towards individuals, offering specific goods, services and information, or towards groups and industry, providing telematic and tracking applications based on the movement of mobile devices. 3GPP has defined a range of generic service types[3], which are highlighted in Table 1.

Mobility Management, Cell Allocation and Control in GSM Mobile Networks

Mobile Network Architecture

Mobile networks can be divided into four basic domains, as illustrated in Figure 1, below:

- The mobile station (MS);
- The base station subsystem (BSS);
- The network and switching subsystem (NSS); and
- The operation and support subsystem (OSS).

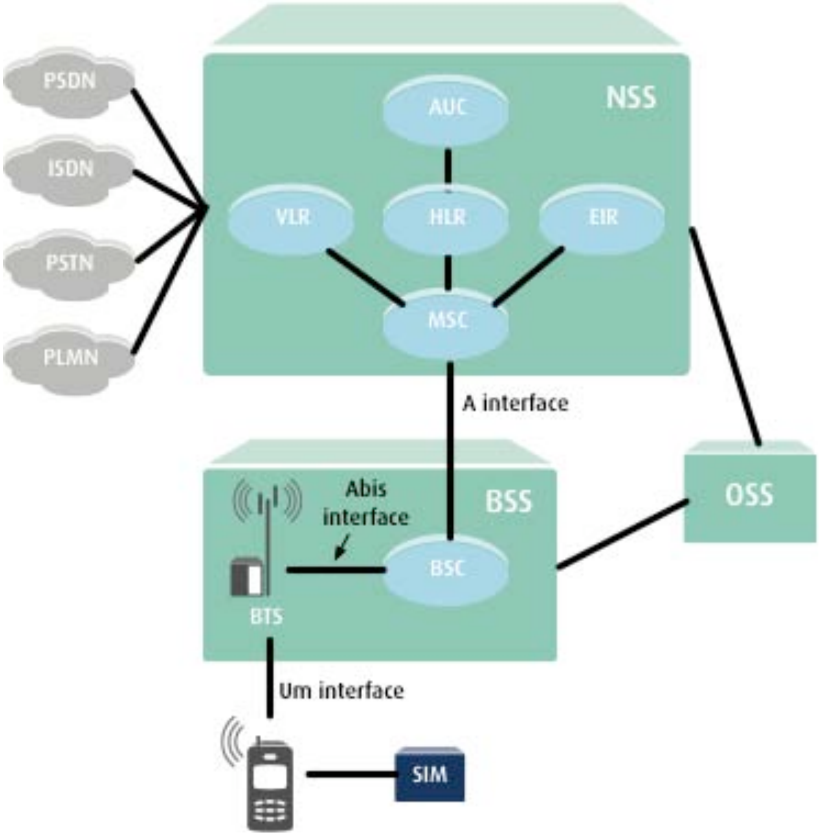

Figure 1: GSM Mobile Network Architecture

In all mobile specifications, the interface between two defined entities is given a label to assist standardisation efforts. Thus, although there are many such interfaces defined, there are three that can be leveraged to provide mobile location information:

- Interface between the mobile station and the BSS – the Um interface;
- Interface between the entities of the BSS – the Abis interface;
- Interface between the BSS and NSS – the A-interface.

A more complete explanation of basic mobile network architecture is provided in Appendix 1.

Mobility Management

Within the BSS domain, the base transceiver station (BTS) continuously transmits control information across what is known as a broadcast control channel (BCCH). When a mobile handset, or mobile station, is powered on, it will begin to scan all of the 125 available GSM-900 frequencies in search of a frequency correction burst signal. Once the BCCH frequency has been found and the frequency has been adjusted, the mobile station will "stay tuned" and listen for a further synchronization burst. This must be decoded in order to synchronize (in terms of clock signal) to the network. After successfully synchronizing frequency and time, the BCCH signal can be received and decoded, providing network identification and information about how the mobile should behave on the network. The BCCH never changes frequency – it stays in the same frequency constantly, like a beacon, transmitting information to the mobiles in a given cell. When the mobile station has found the strongest BCCH signal, it verifies this and, if permitted, “camps on” to the cell. It then obtains a BCCH allocation list (BA) of other BCCH signals in the area, and uses this to check the signal strength of the surrounding cells.

GSM mobile stations have two key background tasks:

- Continuously monitoring beacon power levels of neighbouring cell sites; and
- Maintaining a record of the six strongest neighbouring cells.

In “idle” mode, the action of continuously measuring the signal strength (or receive level) of the BCCH of neighbouring cells helps the mobile station to select the best serving cell. This scanning also aids cell handover procedures when a mobile station is active. The mobile station is said to be active when it is performing one of the following tasks:

- Location update;
- Receiving a call (mobile termination, or MT);
- Initiating a call (mobile origination, or MO); and
- Allocating a data channel (for packet-switched data or SMS).

The active measurement of neighbouring cell BCCH signal strength exists primarily for the network to manage handovers between cells, allowing the mobile station to transfer to a different BCCH at a higher signal level if the original diminishes. This underpins the whole concept of mobility – the ability of a mobile station to seamlessly maintain connectivity to the network. However, as a side effect, the reports contain valuable data on the radio frequencies and signal levels currently being measured by the mobile station. The data collected can be used for other applications, in addition to the control of handovers. These applications include:

- Cell RF planning;
- Monitoring quality of service (QoS) of the radio interface; and
- Determining MS position.

The role of the Base Station Subsystem

The BSS has a critical role to play in the mobile network. It also provides a key entry point for obtaining information that can be used to support LBS. There are several elements that are required to assist in positioning of mobile stations and which are produced as part of the standard activity of mobility management. As such, they require no invasive techniques for capture, but need to be collected by appropriate equipment.

On the network side of a transmitter (TRX) within the BSS, each cell is given a cell identity (CI). The location area code (LAI) is added to this by the BSC to create a unique cell global identity (CGI) code which can be seen at the A interface. Each TRX within the BSS will also have a unique terminal equipment number (TEI) that is used to communicate between the BSC and the TRX across the Abis interface.

Within each base-station there may be several base transceiver stations (BTS), each with one to sixteen transmitters (TRX). The air side of a transmitter (TRX) is identified by two unique data tags:

- Base station identity code (BSIC); and
- Absolute radio frequency channel number (ARFCN).

The BSIC allows mobile stations to discriminate between different cells transmitting their broadcast control channels (BCCHs) on the same frequency. The BSIC comprises two values: a network colour code (NCC); and a base station colour code (BCC). The combination of BCCH frequency and BSIC is used in GSM cellular radio systems to identify a cell for purposes such as handover. BCCH frequency and BSIC is normally unique within a local geographic area, but not necessarily unique within a network.

The mobile station is told of the BCCH frequencies of nearby cells via a BCCH allocation (BA) list. This saves hunting nearby cells for the information and allows it measure their signal strength (RXLEVEL) relative to the serving cell (see section 4.5). The BA list is sent out on the broadcast channel of each cell and is received by mobile stations in idle mode. It is also sent to each mobile station that is in active mode on a slow associated control channel (or SACCH) associated with the active traffic or data channel.

GSM Location Techniques

Positional Accuracy

There are a variety of techniques that can be used to provide information to support LBS. Each has different levels of accuracy, but there is also a cost associated with each. Positioning information can be characterised with varying degrees of accuracy to support a range of specific services. 3GPP has defined parameters that indicate the kinds of services that can be supported for a particular level of location resolution[3]. This is illustrated in Table 2.

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

Table 2: 3GPP Guidelines for Location-Based Services

The most accurate methods, capable of providing resolution at a granularity of <100m require significant investment, as noted by Liutkauskas et al[4] as they require measurements to be captured at the mobile station and directly across the radio interface. Moreover, the greatest resolution is only available through global positioning system (GPS) technology, which is not yet widely deployed in mobile stations. However, there are other techniques which, when combined, can generate resolution within a range of 100 – 500m, which is sufficient for a wide range of potential applications, including emergency service access under US E911 laws. Collectively, techniques which depend on data available over wired or physical connections are known as “network based”, in contrast to those that are made via direct interaction with the radio interfaces. Network-based techniques are not only much simpler and more cost effective to deploy, they also depend on information that is intrinsic to the mobile network.

The three primary network based measurement techniques are:

- Cell global identity;
- Handover / location area update; and
- Timing advance / RXLEV

For each technique, there are key variables that have to be obtained. Several interfaces provide measurement data for network-based location measurement within the GSM family of networks. The role of each is discussed in the following sections and is summarised in Table 3[5].

Measurement Technique	Mobile Station	Interface Surveyed	Positioning Method
Location Area Update	Passive	A / Abis	Location area update
Handover	Active	A / Abis	Handover area
Cell Global ID	Active	A	Cell global identity
TA-value	Active	Abis	Arc section
RXLEV-values	Active	Abis	Arc section

Table 3: Mobile Location Techniques

Cell Global Identity Positioning

Cell Global Identity (CGI) may also be referred to as Cell of Origin (COO) approximation and uses the cell value in which the mobile station is registered by identifying the cell identity (Cell ID) of the serving cell, from which the BTS concerned can be found. Once the cell identity is known, the mobile station can be located to a given cell[5]. It depends on the principle that each BTS has a fixed position and known properties such as signal strength. An area around the BTS can be calculated in which the handset can be located to receive signals of a given strength from the cell. This principle is illustrated in Figure 2.

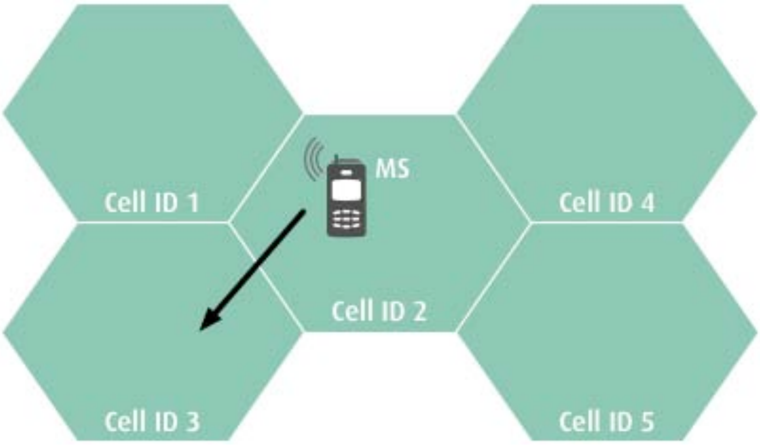

Figure 2: CGI / COO Positioning

Cell Global Identity positioning has varying degrees of accuracy, as the area calculated around the BTS is based on transmitted signal strength and the known signal attenuation (signal loss). These values allow calculation of the radius around the BTS. The final accuracy depends upon the network cell size, which can vary from a radius of 150m in an urban area up to 35km in a rural area. Given this variation, the method has relatively limited utility and is often used in combination with other methods. Nonetheless, it is a useful initial step to providing location-based information and can support a variety of applications.

The BTS often have Antennas that divide the 360 degrees into (usually 2, 3 or 4) segments. As a result the base station can limit the location of a mobile station to a smaller angular segment (180, 120 or 90 degrees) as illustrated in Figure 3[6]. The cell identity value is contained in Location Update signalling that passes across the A-interface towards the NSS.

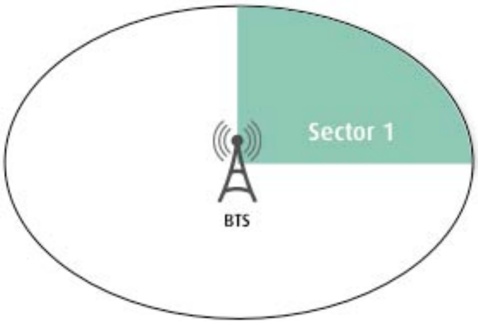

Figure 3: CGI and Sectoring

Location Area / Handover Update Positioning

A location area is a group of base stations. When a mobile station is switched on it determines it's location area and passes that information to the network so the network knows where to find it if a call is received. Whenever its location area changes the mobile station will update the network with its new location area. At the point of handover a 'handover event' takes place where two cell identities are available and the boundary of the two cells concerned can be determined. Although this can provide additional location information, it has the disadvantage of being a transitory event. The handover method is illustrated in Figure 4[6]. Handover and Location Area Update messages are presented across both the Abis and A-interfaces towards the NSS.

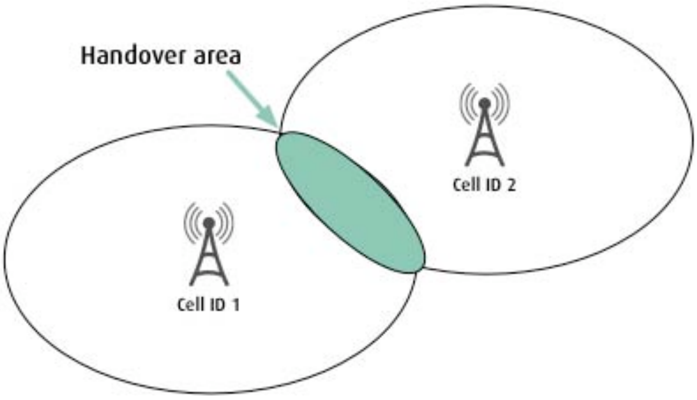

Figure 4: Positioning During Handover

Timing Advance Positioning

Timing advance (TA) values provide a measure of the distance of the mobile station from the serving cell. TA is a technique used to synchronise the signals between the mobile station and the BTS by ensuring that all bursts transmitted from the mobile station arrive at the BTS at the expected time. As distance between the two increases, the burst is sent earlier. The TA value indicates the time advance for the mobile station to send one signal burst and is limited to a resolution of approximately 550m[[5]]. Each 550m distance can be described as a TA step and the BSS assigns a TA value to a mobile station, based on calculated distance. A TA value of '0' thus implies that the mobile station is between 0 and 550m from the BTS, and a value of '2' suggests that it is between 1100 and 1650m from the BTS. Given the maximum radius of a BTS site of 35Km, each cell can be divided into 64 TA steps, as shown in table 4:

Timing Advance	**0**	**1**	**2**	**3**	**….**	**63**
Distance To BTS	**<550m**	**550-1100m**	**1100-1650m**	**1650-2200m**		**35Km**

Table 4: Correlation of Timing Advance Number to Distance of BTS from MS

Determination of the TA is a normally a function of the base station controller (BSC), but this function can be handled anywhere in the BSS, depending on the manufacturer.

Signal Strength Positioning

RXLEV, or Reception Level, is an indication of the signal strength at the mobile station. The mobile station is able to measure RXLEV values for both the serving BTS and up to six neighbouring sites. These are transmitted to the BSS domain during communication by the mobile station. The signal strength is resolved to within 1dBm as shown in table 5 below:

RXLEVEL	0	1	2	3	….	60
Distance To BTS	-110dBm	-109dBm	-108dBm	-107dBm		-48dBm

Table 5: Correlation of RXLEVEL Number to Signal Strength

By converting the RXLEV value into a measure of distance, calculation of the position of the mobile station can be made relative to each of the BTS sites involved. This provides information on the segment, or arc section, within the coverage circle around the BTS in which the mobile station is likely to be located. Combining measurement of several (up to 6) RXLEV values from different transmitters allows triangulation of the mobile station. This is a complex calculation because attenuation within a signal area may not be uniform due to obstructions.

TA and RXLEV positioning methods are complementary, allowing the resolution of location to within 150m under optimum conditions. The principle is illustrated in Figure 5 (below). Both RXLEV and Timing Advance information are only presented across the Abis interface between the BTS and base station controller (BSC).

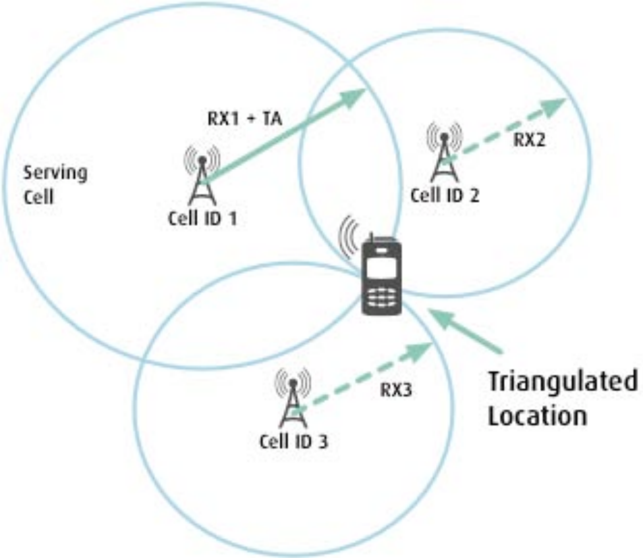

Figure 5: Combining TA and RXLEVEL positioning

Location Measurement Infrastructure

Mobile networks inherently produce mobile location information. However, that data needs to be presented to equipment where it can be processed and accessed by applications; it is not necessarily extracted by default. Location applications can be provided within a mobile network, but they can also be external to that network and operated by a third party. In this context, a differentiation can be made between Location Servers and Location Clients[1].

A location server (LCS) is responsible for collecting location information. Each LCS Server responds to requests from external clients to obtain and present location information to one or more Location Clients. There may be many components to the LCS. Location clients (LCS Clients) are comprised of any hardware or software equipment that initiates requests and interacts with a LCS for the purposes of obtaining location information for one or more mobile stations.

Positioning information is obtained from the access network (the RAN) and exchanged with the core network (the NSS). That is, the interfaces between the domains (Abis, A-interface). Therefore, the information can be collected by components that are integrated within the BSS domain, or they may be obtained via additional equipment that can be added to the network. In many cases, a device known as a location measurement unit (LMU) captures the required data. This can be a standalone entity, or integrated into the BTS. A standalone version can capture data from the Abis interface and present it to a second entity, the serving mobile location centre (SMLC). The SMLC exists to format and present location information to LCS clients, but it may also be associated with cell broadcast capabilities (CBC), which can be of assistance in emergency sessions[7]. This architecture is illustrated in Figure 6.

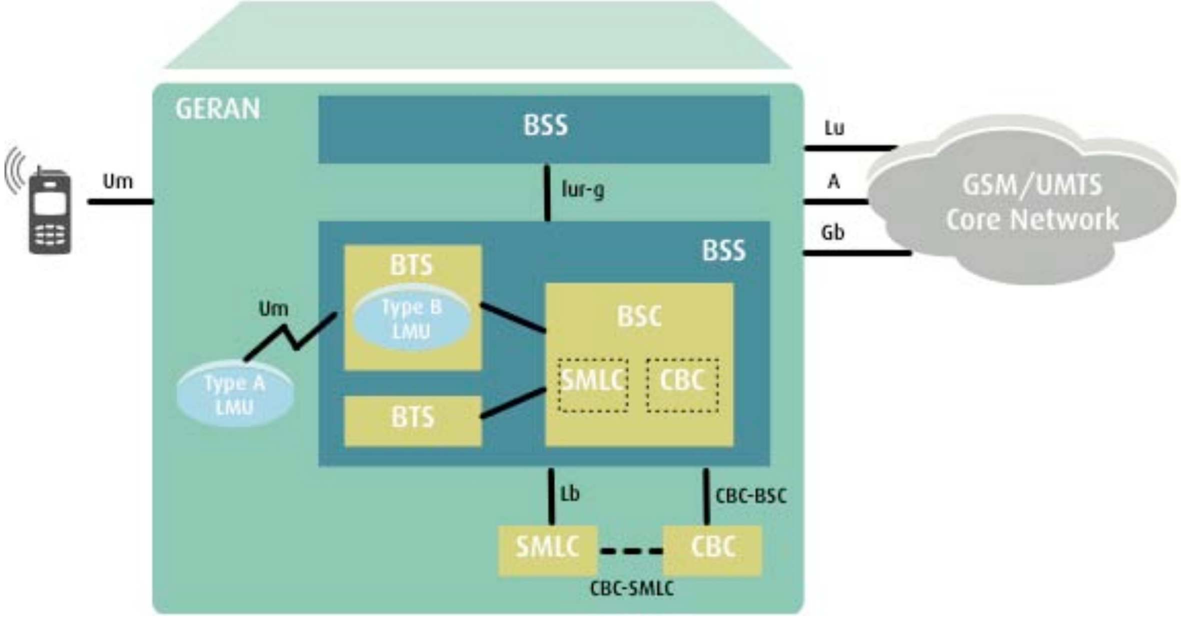

Figure 6: LCS Architecture

The SMLC may have responsibility for multiple LMU devices and presents the collated information to an additional device, the gateway mobile location centre (GMLC). This is the point of entry to the network for external LCS client applications and thus it is vital that accurate and timely information can be provided to this in response to requests from the LCS client[1]. It is further possible to provide data collected from the A-interface to the GMLC. This architecture is illustrated in Figure 7[1].

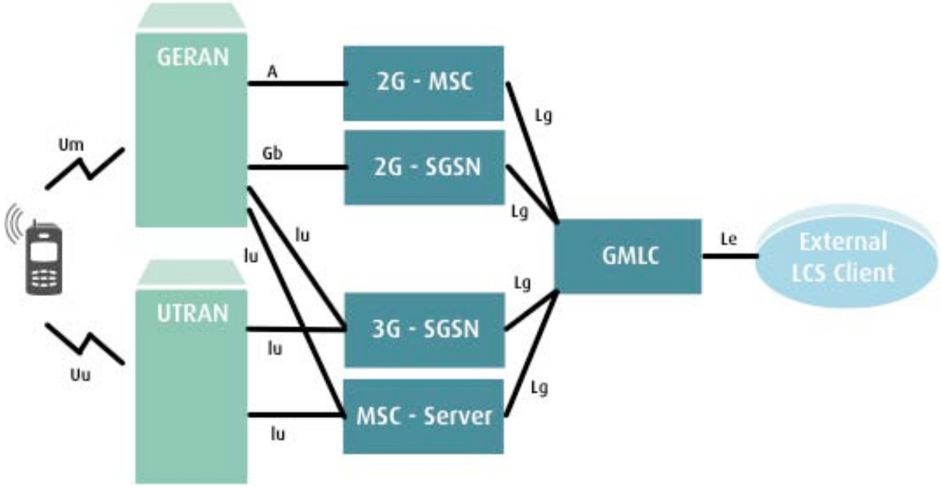

Figure 7: Overall LCS Architecture

The components of the LCS system can be deployed as an overlay to an existing mobile network, adding capabilities to support additional services as required. A common LMU architecture can support multiple LCS clients via the combination of the SMLC and GMLC. Although client software can be provided for mobile stations yielding increased levels of accuracy, this can be a costly and inefficient method of obtaining information, even though it may deliver the most accurate data. A compromise can be achieved by adding passive equipment to potential access points that already exist within the BSS and NSS domains. This is what an external LMU solution can deliver, particularly when combined with sophisticated passive monitoring techniques to ensure non-disruptive deployment.

HINTON Location Techniques

Although data to support LBS is available within the network, it needs to be extracted from the appropriate interface, formatted and presented via SMLC platforms to the LCS client. In the absence of widespread deployment of mobile stations with embedded GPS or other active radio telemetry technology, passive probe solutions provide the finest granularity of positioning available from the network to obtain detailed location data.

The Telesoft Technologies' HINTON Locator passively monitors the interfaces of the BSS and NSS domains in mobile networks using high-impedance termination. This provides access to location-related signalling information for processing by SMLC and GMLC platforms, and LCS clients, and is illustrated in Figure 8. The HINTON Locator may be connected to any mobile network, such as GSM, GPRS, EDGE, UMTS or CDMA, CDMA2000, and their derivatives, ensuring that the platform is future-proof as network migration proceeds, offering vital investment protection. The HINTON Locator leverages functionality inherent in the mobile network to capture location-related signalling information, allowing application developers and operators to use it to triangulate geographic position.

The HINTON Locator extracts relevant information from signalling parameters and presents the received data via an Ethernet API to middleware or applications for further processing. The data is aggregated and forwarded to third-party applications. Aggregation may be done locally at each monitoring site or centrally as network topology dictates. The HINTON Locator supports a wide range of physical interfaces (E1, T1, STM1, OC-3, Ethernet) as well as a comprehensive range of signalling protocols (including those used across the Abis and A-interfaces). It can also collect voice traffic from the A-interface directly, allowing for further creativity in application development, as well as supporting legally-enforced Lawful Intercept programmes.

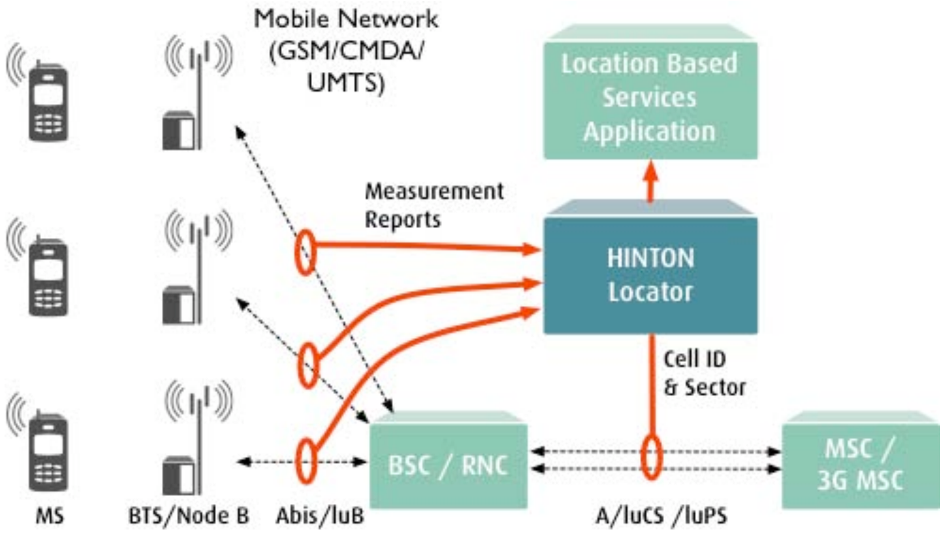

Figure 8: HINTON Locator System Architecture

This methodology allows sophisticated mobile subscriber applications to be developed, based on targeting geographic areas, using network information only. The vast majority of handsets, both in circulation and sold today, are still low specification non-GPS phones. Using network information avoids the need for any specialised handset capabilities and allows LBS to be offered to all subscribers, even those with the most basic handsets. Network location accuracy depends on many factors including density of base stations and interference from tall buildings, but typical results from the HINTON Locator in an urban area derive location data to an accuracy of 150-500m via triangulation of multiple BTS platforms from a handset. Monitoring data using a separate overlay system avoids network interference and allows enhancement and upgrade independent of the main network.

Conclusion

In order to cost-effectively deploy and leverage the potential of LBS, a lightweight, passive solution that is capable of collecting location data from appropriate interfaces is required. The captured information can support location techniques such as RXLEVEL, TA and CGI positioning. Such a device should be capable of acting as an external, network-based LMU to capture data from the Abis interface, and for intercepting information from the A-Interface. It should be able to interface seamlessly to the SS7 signalling conveyed over both interfaces and present it to SMLC and other LCS entities in a format that can rapidly be processed in response to location requests from an LCS client.

The HINTON Locator from Telesoft Technologies meets all of these requirements and provides a cost-effective, scalable platform that captures essential location information for the creation of valuable LBS. It can be layered onto an existing network and does not disrupt existing deployments. It offers future-proof technology, protecting existing investment and building long-term ROI.

The HINTON Locator can also be used to ensure compliance with legal requirements and Lawful Intercept regulations. At a time when the LBS market appears poised to – finally – deliver on its promise, the HINTON Locator can become a key enabler to help network operators and LBS application developers realise its potential.

Telesoft Technologies has decades of experience in the field of network monitoring and mobile signalling. Through the HINTON Locator, this expertise is available to assist the rapid deployment of LBS applications and support monetisation of key network assets in new and innovative ways. Please contact Telesoft Technologies Ltd for more information and to discuss your network requirements.

References

1. 3GPP TS 23.271 V7.9.0 "*3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional stage 2 description of Location Services (LCS) (Release 7)*"
2. ABI Research (2008) "*Location Based Platforms and Infrastructure*"
3. 3GPP TS 22.071 V8.0.0 "*3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Location Services (LCS); Service description; Stage 1 (Release 8)"*
4. Liutkauskas, V, Matulis, Pl štys, Kaunas University of Technology, "*Location Based Services"*
5. Schwieger, V. "*Positioning within the GSM Network*" in "Coastal Areas and Land Administration – Building the Capacity, 6th FIG Regional Conference, San José, Costa Rica 12 – 15 November 2007
6. Czommer, R, Ramm, K, Schwiege, V, (2006) "*Analyse de Ortungsverfahren*". Report within the project Do-iT, Working Practice 4.1, Institute for Applications of Geodesy to Engineering, University Stuttgart
7. 3GPP TS 43.059 V8.1.0 "*3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; Functional stage 2 description of Location Services (LCS) in GERAN (Release 8)"*

Glossary

Abis: *Signalling between BTS and BSC in GSM mobile networks*
A-Interface: *Signalling between BSC and MSC in GSM mobile networks*
ARFCN: *Absolute radio frequency channel number*
BCC: *Base station colour code*
BCCH: *Broadcast control channel*
BSC: *Base station controller*
BSIC: *Base station identity code*
BSS: *Base station subsystem*
BTS: *Base Transceiver Station*
CDMA: *Code division multiple access*
Class 5: *Central office switch in fixed networks, directly serving subscribers*
COO: *Cell of origin*
E1: *E carrier level one, 2.048 Mbit/s full duplex*
EDGE: *Enhanced data rates for GSM evolution*
EIR: *Equipment identity register*
GLMC: *Gateway mobile location centre*
GERAN: *GSM edge radio access network*
GPRS: *General packet radio service*
GPS: *Global positioning system*
GSM (X00): *Global system for mobile communications or groupe spéciale mobile, where X00 refers to the frequency band used*
HLR: *Home location register*
LBS: *Location based services*
LCS: *Location services*
LTE: *Long term evolution*
MO: *Mobile originated*
MS: *Mobile station*
MSC: *Mobile switching centre*
MT: *Mobile terminated*
NCC: *Network colour code*
NSS: *Network and switching subsystem*
OSS: *Operation and support subsystem*
QoS: *Quality of service*
RAN: *Radio access network*
RF: *Radio frequency*
RXLEV: *Reception level*
SACCH: *Slow associated control channel*
SMLC: *Serving mobile location centre*
SMS: *Short message service*
SS7: *Signalling system number 7*
TA: *Timing advance*
TEI: *Terminal Equipment Identifier*
UMTS: *Universal mobile telecommunications system*
UTRAN: *UMTS terrestrial radio access network*
VAS: *Value added services*
VLR: *Visitor location register*

Appendix A: Mobile Network Architecture

Architectural Basics

In order to access location information, an understanding of the topology of mobile networks is required. In this section, an overview of mobile network architecture is provided. Mobile networks can be divided into four basic domains, based on the GSM implementation, as illustrated in Figure 9 (below).

- The mobile station (MS);
- The base station subsystem (BSS);
- The network and switching subsystem (NSS); and
- The operation and support subsystem (OSS).

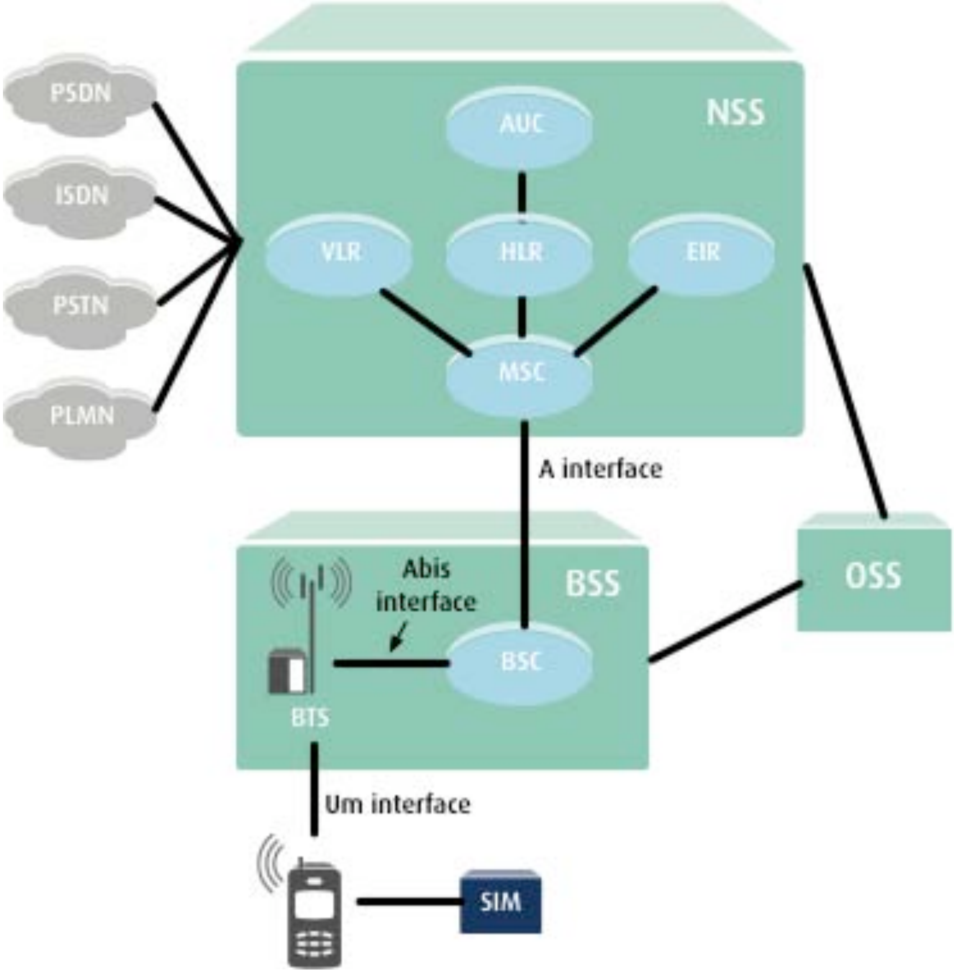

Figure 9: GSM Mobile Network Architecture

A mobile station is the term applied to the combination of the mobile equipment that is deployed together with the subscriber identity module (or SIM) card. The SIM card stores valuable subscriber information, allowing subscribers to easily change handset or access devices. The term mobile station is used because there is a range of devices in which the SIM card can be transported. These are usually mobile handsets, but can also include computers, dongle devices for mobile broadband access, and positioning equipment. This latter category is important for many commercial telemetry applications, such as fleet mobility.

The mobile station communicates via a radio interface to the BSS domain. This is often called the radio access network (RAN), and has evolved in conjunction with the release of new mobile standards. More recent versions include GERAN and UTRAN (GPRS edge radio access network and UMTS radio access network, respectively). However, the basic principles are the same and, for the purposes of this paper, the term RAN will be generically adopted. In all mobile specifications, the interface between two defined entities is given a label to assist standardisation efforts. Thus, although there are many such interfaces defined, there are three that can be leveraged to provide mobile location information:

- Interface between the mobile station and the BSS – the Um interface;
- Interface between the entities of the BSS – the Abis interface;
- Interface between the BSS and NSS – the A-interface.

The Um Interface

Um is a radio signalling interface that is responsible for the control of mobile stations. It is the responsibility of the base transceiver station (BTS) within the BSS domain to manage bi-directional communications with all active and inactive (but powered on) mobile stations within a cell area. The RAN is divided into cells, each of which contains a BTS – often known as a cell tower. A cell comprises the area around a BTS for which coverage may be provided. For simplicity, this is usually described as being circular, although the local topography influences the effective coverage. Using the concept of a circle, it can be seen that a mobile station will always be located at a given radius from the BTS, which gives rise to various location detection possibilities.

In order to provide 360° coverage within a given cell area, a BTS may deploy one or more transceiver devices (TRX). Each TRX device is allocated a sector within a particular cell and is given a cell Identity (CI), base station identity code (BSIC), absolute radio frequency channel number (ARFCN) and terminal equipment identity value (TEI) value. Where three such TRX devices are deployed, each has an effective arc of 120°. This is illustrated in Figure 10, below.

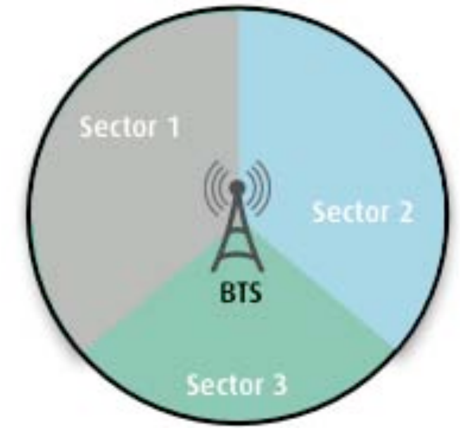

Figure 10: TRX and BTS Relationship

The Abis Interface

The BSS domain is divided into two entities, the base station controller (BSC) and the BTS. An individual BSC may control many hundreds of BTS platforms. The two are linked by a physical connection, which is usually based on E1 interfaces. A dedicated signalling protocol is conveyed over this interface, the Abis, which manages cellular traffic from within each cell site. Voice and data communications may be carried across this interface. The Abis interface is the nearest signalling interface to the radio access network. That is, it contains specialised information regarding the location and mobility of mobile stations that can be a valuable input to the creation of LBS. This information includes data on the signal strength of the mobile station (RXLEVEL) and the timing advance (TA). Both types of data can be used to calculate distance of the mobile station to the relevant BTS and are discussed at greater length in sections 4.4 and 4.5. GPRS packet data can also contain location information and is also carried over the Abis interface.

The A-Interface

Each base station controller is connected to the mobile switching centre (MSC) in the NSS via the A-interface. There may be multiple MSCs within a mobile network and they act in a similar way to a class 4 switch in a fixed network. The A-interface is a signalling connection, based on SS7, which manages voice traffic from the cellular access network. It is normally transported over E1 interfaces. In later revisions to the standards, a data overlay was implemented that effectively separated voice and data traffic at the

BSC level (i.e. GRPS). The A-interface includes details of location update and handover information that must be presented to the NSS in order to update the key databases that are located within the core (for example, the HLR, VLR and EIR). As such, it provides additional information that can be used for the creation and support of LBS.

Appendix B: Mobile Network Codes

Mobile Network Codes

A reference of various network codes:

ARFCN: *absolute radio frequency channel number* - the GSM900 spectrum uses ARFCN 1 to 124.
BCC: *base station colour code* – part of the BSIC – to discriminate between cells using the same frequencies during the cell selection and camping on process.
BSIC: *base station identity code* - a code broadcast in order to identify the NCC (Network Colour Code – 3bits) and the BCC (Base Station Colour Code – 3bits).
CGI: *cell global identity* - the concatenation of the LAI (Location Area Identity) and the CI (Cell Identity) and uniquely identifies a given cell.
CI: *cell identity* - a 16bit identifier. When combined with the LAI (Location Area Identity) or RAI (Routing Area Identity) the result is termed the CGI (Cell Global Identity).
LA: *location area* - is a group of cells (defined by the network provider) in which a mobile will be paged.
LAI: *location area identity* - comprised of the MCC (Mobile Country Code), MNC (Mobile Network Code) and the LAC (Location Area Code).
LAC: l*ocation area code* - uniquely identifies a LA (Location Area) within a PLMN (Public Land Mobile Network). It may range from 0 to 65,535.
MCC: *mobile country code* - a three digit number uniquely identifying a given country.
MNC - Mobile Network Code - a two or three digit number used to uniquely identify a given network from within a specified country.
NCC: network colour code – part of the BSIC - 3bits, to differentiate between operators
RAI: routing area identification - composed of the LAC (Location Area Code) and the RAC (Routing Area Code). It is used for paging and registration purposes.

Where innovative thinking
meets engineering excellence

telesoft TECHNOLOGIES

Telesoft Technologies Ltd,
Observatory House,
Blandford, Dorset DT 11 9LQ UK

T. +44 (0)1258 480 880
F. +44 (0)1258 486 598
E. sales@telesoft-technologies.com

Telesoft Technologies Inc.
Suite 601, 4340 Georgetown Square,
Atlanta GA 30338 USA

T. +1 770 454 6001
F. +1 770 452 0130
E. salesusa@telesoft-technologies.com

Telesoft Technologies Ltd,
Building FC-24, Sector 16A, Noida 201301,
Uttar Pradesh, India

T. +91 120 466 0300
F. +91 120 466 0301
E. salesindia@telesoft-technologies.com

DX-HIN-GEN-MK-WP-32640-02 20