

Mobile@Home—GSM services over wireless LAN

Martin Bäckström, Andreas Havdrup, Tomas Nylander, Jari Vikberg and Peter Öhman

What do you get when you combine mobile telephony with voice over IP (VoIP)? Mobile@Home. The solution is a new access network for mobile core networks that has the same role in the mobile network as GSM/EDGE and WCDMA radio access networks (GERAN/UTRAN) but makes use of unlicensed spectrum and IP-based broadband access networks. It is based on the 3GPP Generic Access Network (GAN) specification (formerly known as Unlicensed Mobile Access, UMA).

With Mobile@Home, end users can use their GSM terminals at home to access mobile services over wireless LAN (WiFi or Bluetooth). The solution minimizes operator investment by reusing the existing mobile core network and other support nodes.

In late 2003, Ericsson helped establish the Unlicensed Mobile Access (UMA) forum for this idea. The forum labored for nine months to produce a set of specifications that supported every major GSM service over unlicensed radio. The specifications were released in September 2004.

Just before the release of the first specification, UMA was included as a work item in the Third Generation Partnership Project (3GPP) under the name *Generic Access to A and Gb Interface* (GAAG). Within 3GPP, the UMA technology specification is called Generic Access Network or GAN. The GAN specifications have since been approved for inclusion in 3GPP Release 6 (Rel-6). All future work related to unlicensed mobile access will take place in 3GPP and will be coordinated with standardization and development of the GSM and UMTS networks.

Background

In 2000, Ericsson began investigating how unlicensed radio in a mobile handset could be used to access mobile network services. Not long afterward it developed a demo system to show that every major GSM service can indeed be supported over Bluetooth radio and an IP-access network.

Benefits of Mobile@Home

Operator benefits

Ericsson's Mobile@Home solution enables operators to explore new business opportunities including improved indoor coverage. This is especially interesting in North

BOX A, TERMS AND ABBREVIATIONS

3GPP	Third Generation Partnership Project	GPRS	General packet radio service	PAN	Personal area network
AAA	Authentication, authorization and accounting	GSM	Global system for mobile communications	PLMN	Public land mobile network
AKA	Authentication and key agreement	GUI	Graphical user interface	PS	Packet switched
AP	Access point	HBSC	Home BSC	RADIUS	Remote authentication dial-in user server/service
AUC	Authentication center	HLR	Home location register	SCCP	Signaling connection control part
BSC	Base station controller	HPLMN	Home PLMN	SEGW	Security gateway
BSSAP	Base station subsystem application part	HSN	Mobile@Home support node	SGSN	Serving GPRS support node
BSSMAP	Base station subsystem management application part	HSS	Home subscriber server	SIM	Subscriber identity module
CBC	Cell broadcast center	IEEE	Institute of Electrical and Electronics Engineers	SMLC	Serving mobile location center
CC	Call control	IETF	Internet Engineering Task Force	SMS	Short message service
CDMA	Code-division multiple access	IKE	IPsec key exchange	SS	Supplementary service
CGI	Cell global identity	IMS	IP Multimedia Subsystem	TCP	Transmission control protocol
CS	Circuit switched	IMSI	International mobile subscriber identity	UMA	Unlicensed mobile access
DHCP	Dynamic host configuration protocol	IP	Internet protocol	UMTS	Universal mobile telecommunications system
DNS	Domain name server/service	IPsec	IP security protocol	UNC	UMA network controller
DSL	Digital subscriber line	LAI	Location area identity	USIM	Universal SIM
DTAP	Direct transfer application part	MAC	Media access control	UTRAN	UMTS terrestrial radio access network
EAP	Extensible authentication protocol	MAP	Mobile application part	VoIP	Voice over IP
EDGE	Enhanced data rates for GSM evolution	MM	Mobility management	VPLMN	Visited PLMN
FQDN	Fully qualified domain name	MSC	Mobile services switching center	WCDMA	Wideband CDMA
GA-CSR	Generic access circuit-switched resource	MTP	Message transfer part	WiFi	Wireless fidelity (IEEE 802.11 wireless networking)
GAN	Generic access network	NAT	Network address translation/translator	WLAN	Wireless local area network (see also WiFi)
GANC	GAN controller	O&M	Operation and maintenance	Wm	An interface developed in 3GPP for interworking with WLAN
GERAN	GSM/EDGE radio access network	OSI	Open Systems Interconnection		
		OSS	Operation support system		

America where the majority of GSM networks operate on the 1900MHz spectrum and only limited coverage is provided in many residential areas. Thanks to Mobile@Home, operators can now deploy and extend local indoor coverage without affecting end-user behavior or sacrificing functionality. Indeed, Mobile@Home provides a seamless user experience between the operator and home networks.

Operators might also opt to deploy voice services over broadband access. There are currently several alternatives for doing so, but most of them require a personal computer, which severely limits interoperability, functionality and convenience. Mobile@Home, by contrast, combines the broadband network with the infrastructure of the mobile core network while preserving the role of the mobile handset. And because it reuses existing functionality in the mobile core network, such as charging, authentication and end-user administration, the impact of deploying Mobile@Home is limited to the configuration of the new access network.

End-user benefits

Ericsson's Mobile@Home solution guarantees a consistent end-user experience in WiFi and wide area radio domains. Each end-user handset has only one number, which works independently of access method and location.

Mobile@Home-enabled handsets come preconfigured and do not require any more end-user configuration than an ordinary GSM handset would. End users experience transparent functionality, seamless mobility between the two domains and two-way roaming and handover.

IP Multimedia Subsystem (IMS) services function equally well in the Mobile@Home network as in GERAN and UTRAN. Therefore, new services introduced through IMS for GERAN and UTRAN will be available in Mobile@Home with full end-user transparency and mobility.

Standards

The Mobile@Home solution is based on the 3GPP GAN standard, which was developed through a process that involved handset and network vendors to minimize the impact on mobile handsets by drawing on existing implementations. This approach reduces time to market, ensures interoperability between a wide range of handsets and networks, and promotes the commercial availability of handsets from multiple vendors.

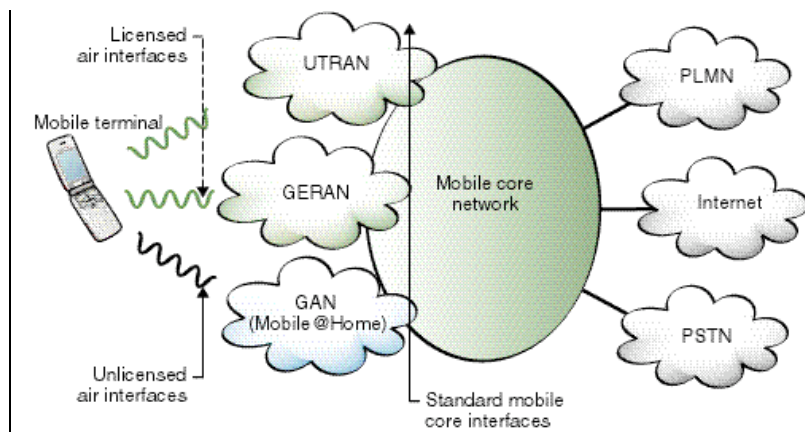
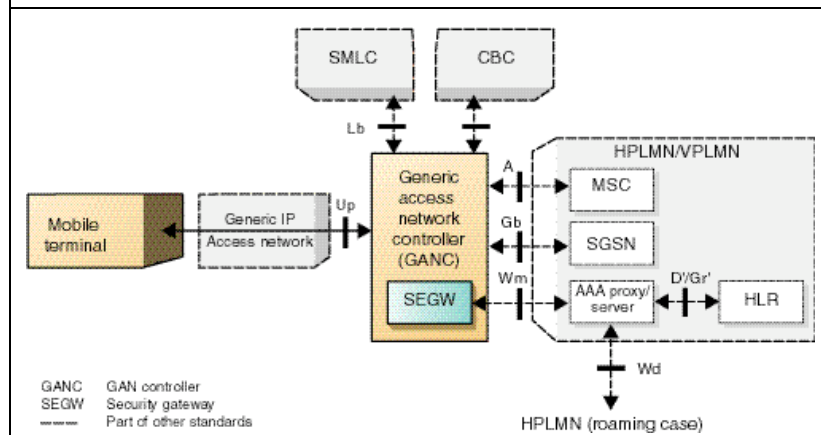


Figure 1
Ericsson Mobile@Home.

GAN overview

Figure 2 shows the GAN architecture. The *Up* interface, which is the heart of the standard, determines how a handset communicates with the network, represented by the generic access network controller (GANC), formerly the UMA network controller (UNC). The *Up* interface assumes that the handset is capable of exchanging IP packets

Figure 2
Architecture of the generic access network (GAN).



with the GANC as described in other standards – for example, the Bluetooth standard for personal area networks (PAN), the WiFi standard (IEEE 802.11), and a variety of broadband access standards (cable, xDSL, and so on). In other words, one may use a standard WiFi access point.

Figure 2 also shows that the GANC employs standard *A* and *Gb* interfaces to the mobile core network. As a consequence, the core network is not aware that the GANC represents a different type of access network. It treats the GANC as an ordinary GSM access network, permitting all major GSM services including IMS packet-based services.

An IPsec tunnel between the handset and the security gateway (SEGW) in the generic access network protects information sent over the *Up* interface. All traffic over the *Up* interface is sent inside this tunnel and switched or routed between the SEGW and GANC. The SEGW makes use of the *Wm* interface to an authentication, authorization and accounting (AAA) server. A subset of the *Wm* interface is used to authenticate users when the IPsec tunnel is being established. The GAN standard defines the functions and procedures needed in the *Up* interface

- to support seamless mobility (handover and roaming) between GAN and GSM and between GAN and WCDMA; and
- to provide access to services in the mobile core network.

Security

GAN security is based on the security mechanisms defined for the *Interworking WLAN IP Access* scenario (3GPP). The IPsec tunnel protects all control signaling and user plane traffic over the *Up* interface between the handset and the network. Therefore an IPsec tunnel must be established before the handset can communicate with the GANC. Using SIM or USIM credentials (similar to GERAN/UTRAN) the system authenticates the handset when the tunnel is being established. IETF specifications define the protocols for this procedure. They include IKEv2, EAP-SIM and EAP-AKA.

Allocation of the correct GANC

The access network between the handset and the GANC is based on internet protocols. In principle, this means the handset has access to different GANC nodes in the GAN. Discovery and registration procedures are used to allocate the best GANC for the handset in its current location. Discovery is used

between the handset and the Provisioning GANC, which is the initial point of contact in the GAN. The handset is either given the address of the Provisioning GANC or can derive the address from information in the SIM or USIM. The main tasks of the Provisioning GANC are to allow access to the GAN and to allocate a Default GANC to each handset. Allocation is based on subscription information in the Provisioning GANC and information provided by the handset during the discovery procedure. The best default GANC, for example, might be one that is close to the end user's residence.

The Default GANC is the handset's main point of contact in the GAN. Any time the handset tries to access the GAN from a new location, it must initiate registration with the Default GANC, providing information on the current GERAN or UTRAN cell. The Default GANC then determines which GANC can best serve the handset at its present location. If the Default GANC redirects the handset to a different Serving GANC, the handset will have to initiate registration with that GANC.

The Default GANC might also accept the registration and become the Serving GANC. Indeed, assuming the correct Default GANC has been allocated, this will be the regular outcome. Once the registration has been accepted, the Serving GANC returns relevant GAN system information to the handset over the established connection. This information is thus not broadcasted in the GAN. The GANC stores information about the handset for mobile terminating procedures, such as paging.

Ordinarily, the Serving GANC has a connection to the mobile services switching center (MSC), which controls the macro cell in which the user resides. This makes it easier to support handover between the GAN and macro network. The Serving GANC accepts all service requests from the handset. The handset stores the address of the GANC and information on the current cell. The next time the handset connects to the GAN in this macro cell, it sends its request directly to the Serving GANC. If the GANC reports a new location area, the handset sends a location update message via the GAN. The handset may then display a symbol to indicate that it is being served by the GAN (Figure 3). When this symbol is displayed, end users know that all originating and terminating traffic is being routed via the GAN.

Figure 3
The handset displays a symbol to indicate that it is being served by the GAN.



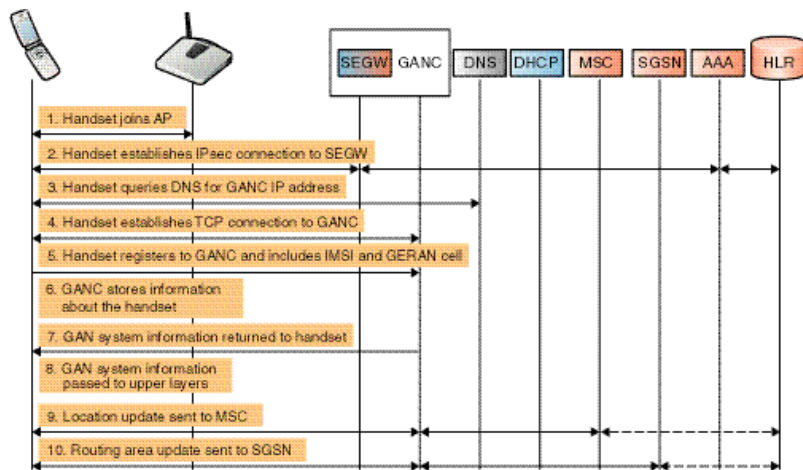


Figure 4
Rove-in example (see also Box B).

Rove-in and rove-out

The GAN standard uses the term *roving* to describe roaming between WiFi coverage and GERAN/UTRAN coverage. *Rove-in* means the handset has begun communicating actively using the protocols in the *Up* interface to serve the upper OSI layers in the handset (Box B). These upper layers include mobility management and support for SMS, call control and supplementary services.

Rove-out means the handset has stopped communicating via the protocols in the *Up* interface; instead, relevant GERAN/UTRAN protocols are used to serve the upper layers in the handset.

Transparent access to services in the mobile core network

The protocols in the *Up* interface provide transparent support for services in the mobile core network. All upper-layer messages are tunneled over the *Up* interface and interworked with existing mechanisms in the *A* and *Gb* interfaces.

GPRS support in GAN

The *Up* interface also transports GPRS control signaling and user-plane traffic. Specific procedures and design principles for GPRS support in GAN allow the network to support a very large number of handsets,

BOX B, ROVE-IN

Figure 4 shows an example of GAN rove-in; that is, of a handset that registers to a Default or Serving GANC. The handset in this example is in idle mode. At the outset it is attached to the network via GPRS and camped on a GERAN cell.

- **Step 1**
The handset joins an access point (AP) to gain IP connectivity.
- **Step 2**
Step 2 is dependent on SEGW address information contained in the handset. If the handset has the fully qualified domain name (FQDN) of the SEGW (for instance, ganc-segw.operator.com) it performs a DNS query in the public DNS to retrieve the IP address of the SEGW (not pictured). It then establishes the IPsec tunnel to the SEGW. As part of this procedure, the SEGW authenticates the handset using the *Wm*

interface to the AAA server. The SEGW also allocates an IP address to the handset from the DHCP server.

- **Step 3**
Step 3 is dependent on the GANC address information contained in the handset. If the handset has the FQDN of the GANC (for instance, ganc1.operator.com) it performs a DNS query via the IPsec tunnel in the private DNS to retrieve the IP address of the GANC.
- **Step 4**
The handset establishes the TCP connection to the GANC.
- **Step 5**
The handset initiates registration with the GANC. Among other things, the handset provides its international mobile subscriber identity (IMSI) and the GERAN cell identifier.
- **Step 6**
The GANC accepts registration from the

handset in its current location and stores all necessary information.

- **Step 7**
The GANC informs the handset that it has accepted the registration and transmits GAN system information.
- **Step 8**
The handset opts for rove-in; the relevant part of the system information is passed to its upper layers. In this example, the location area identity (LAI) indicated by the GANC differs from that of the last registered LAI.
- **Step 9**
The upper layers in the handset initiate location area update in the MSC (same procedure as for GERAN/UTRAN).
- **Step 10**
The upper layers in the handset initiate a routing area update in the SGSN (same procedure as for GERAN/UTRAN).

particularly as the GAN does not need to keep specific data on idle handsets in the GPRS part of the GANC. The GAN also supports flexible load distribution.

Location services

Several methods may be employed to determine the location of a handset registered to the GAN. These methods use information configured in the GAN and information received from the handset during registration. The handset informs the GANC where (that is, on which GERAN or UTRAN cell) it is camped. It also identifies the current WiFi or Bluetooth access point. The GANC can use an external database to map this data to the exact geographical location of the access point. The handset might also report the geographic location to the GANC. In addition, the security gateway sees the public IP address of the handset. In some situations, this information can be used to determine the geographic location of the handset and to check that the access point has not been moved. The handset might also include a street address in its registration request to the GANC; this information can be mapped to a geographic location using external databases.

Emergency services

Operators can stipulate whether emergency calls will be directed from handsets through GERAN/UTRAN or GAN. If the GANC indicates GERAN/UTRAN, and this coverage is available, emergency calls are placed

over GERAN/UTRAN and existing location-determination services are used. Otherwise, emergency calls are placed over the GAN. Location-determination mechanisms in the GAN are used to guide the core network in routing to the correct emergency center, and when requested to do so, to deliver more exact location information to the mobile core network.

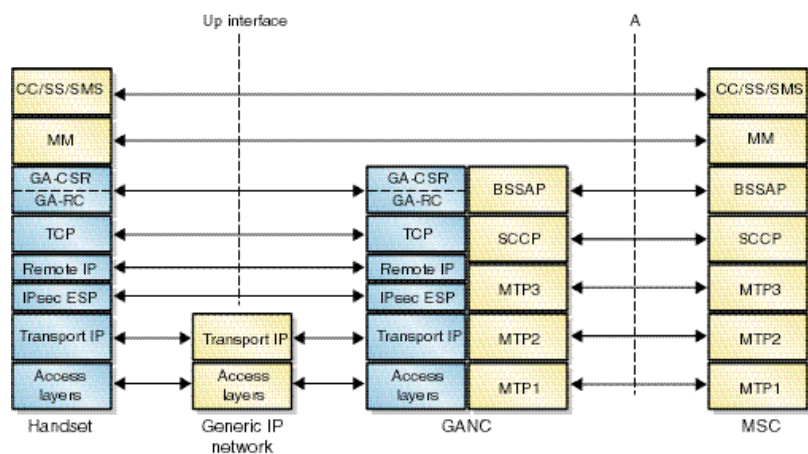
GAN protocol architecture

Figure 5 describes the protocol architecture of the GAN circuit-switched (CS) domain control plane. The new protocols defined in the GAN standard (generic access circuit-switched resources, GA-CSR, and below) serve mobility management and other upper OSI layers (in place of the GERAN and UTRAN radio resource-management protocols).

A TCP connection between the handset and GANC transports the protocols for the CS control plane using the IPsec tunnel between the handset and the SEGW.

The protocol layers above GA-CSR – mobility management (MM), call control (CC), supplementary services (SS), and SMS – are unmodified and transported transparently between the handset and the MSC. The protocols are tunneled in the GA-CSR protocol over the *Up* interface and transported using standard mechanisms over the *A* interface, which is the interface between the MSC and GANC. Signaling over the *A* interface complies with the base station system application part (BSSAP)

Figure 5
Circuit-switched control plane over the *Up* interface.



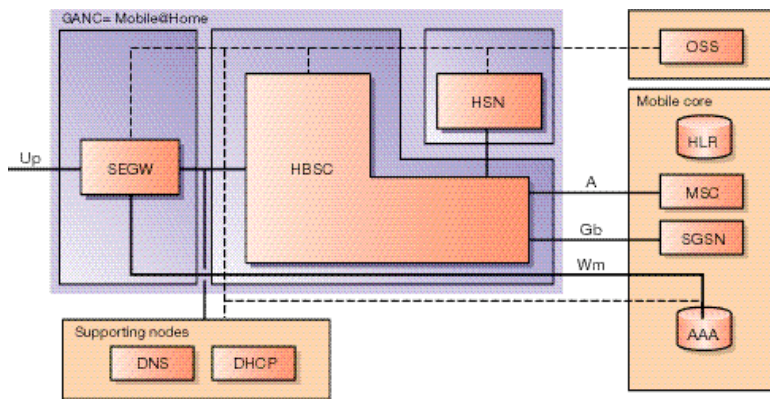


Figure 6
Mobile@Home network architecture.

protocol, which uses the message transfer part (MTP) and signaling connection control part (SCCP). BSSAP messages can be divided into two categories:

- transparent direct transfer application part (DTAP) messages sent between the handset and MSC; and
- non-transparent base station subsystem management application part (BSSMAP) messages sent between the GANC and MSC.

The GANC performs the necessary interworking between the BSSMAP and GANC protocols.

Control signaling and user-plane data for GPRS are interworked toward the SGSN in a similar way using standard *Gb* interface protocols and procedures.

Ericsson's Mobile@Home solution

Mobile@Home – Ericsson's solution for the GANC – is 100% compatible with UMA specifications and the GAN standard, and also offers some security enhancements. Figure 6 shows the main components, or nodes, of this solution: the HBSC, SEGW and HSN.

HBSC

The home base station controller (HBSC), the main node in the Mobile@Home solution, implements the three logical roles (Provisioning, Default and Serving) of the GANC and interworks with the handset

over the *Up* interface. It is based on a standard Ericsson base station controller (BSC) with the addition of IP connectivity for *Up* interface support. Therefore, the HBSC has inherited support for virtually every core network interface and signaling standard. In short, Ericsson designed and built the HBSC to have the carrier-class performance of its other radio access solutions.

The Mobile@Home solution can be deployed in several ways:

- Few centralized stand-alone HBSC nodes.
- Distributed stand-alone HBSC nodes.
- Integrated HBSC functionality in all or some (Ericsson) BSC nodes.

The latter approach has several obvious benefits: operators, for instance, do not need additional floor space or sites, because the necessary hardware and infrastructure (power, cooling, transmission, OSS connection, and so on) are already in place. In addition, when connected to the HBSC the handset uses existing BSC resources, such as transcoders. Because each handset uses either the GAN or GERAN there is no need for extra transcoders. The handsets can be redirected to the combined HBSC/BSC, which serves the macro network. This minimizes network signaling and the operation and maintenance (O&M) needed for handovers, because the handovers take place inside the same piece of hardware (the combined HBSC/BSC).

A stand-alone HBSC can be deployed without transcoders, reusing the transcoder pool from an existing BSC/TRC. Each

HBSC can be connected to several MSCs. Initially, one may thus deploy the Mobile@Home solution using only a few HBSC nodes.

HSN

The Mobile@Home support node (HSN) is an optional part of the Mobile@Home solution. It introduces a layered architecture that improves the management of information in large networks. Ordinarily, this node is placed in a central location where it is available to every HBSC in the Mobile@Home network. The HSN is used to centrally configure data for extended registration checks, triggering functions and location services.

Extended registration check

An extended registration check is used to control access to the GAN, for instance, by checking to see whether or not an access point or IP network has been blacklisted. It may also be used to enhance charging functions for the core network, so that specific cell rates solely apply to specific access points. The check can also trigger an information message to an external service node (for example, a presence server).

Location service functions

Location service functions maintain positioning information. If the handset is able to report its geographic location, this information can be provided to the HSN automatically during registration. Location information can also be provided per access point, or in some cases, per IP address. The address used for a subscription can be automatically translated into longitude and latitude. This information can be verified, for example, by using the serving mobile location center (SMLC) to retrieve the macro

network's cell position and comparing it with the stored position of the access point. If a discrepancy is detected the subscriber or operator is informed.

SEGW

The security gateway (SEGW), the termination point for the security part of the *U_p* interface on the network side, terminates the IPsec tunnel from the handset and forwards the IP packets of the unencrypted *U_p* interface to the HBSC. In the downlink, it receives unencrypted IP packets from the HBSC and routes and encrypts them in the IPsec tunnel specified by the destination IP address. The SEGW interworks with AAA servers via the RADIUS protocol to help authenticate IPsec tunnel establishment. In addition, by interworking with DHCP servers, it allocates IP addresses to the handset during IPsec tunnel establishment. The SEGW provides the security functions specified in the GAN standard. These include IKEv2, EAP-SIM, EAP-AKA and NAT traversal.

SEGWs may run in high-availability (hot standby) mode or *N+1* redundancy. This way, if one SEGW fails there is always spare capacity in the remaining SEGWs. Load on the SEGW is balanced by means of a separate load balancer or DNS round-robin functionality. In addition, Ericsson has developed enhanced functionality for security and for controlling and regulating load on the SEGWs.

Support and other nodes

AAA server

The Mobile@Home solution reuses the Ericsson AAA server that supports the same trusted security mechanism used in standard GSM systems – the EAP-SIM-based

TRADEMARKS

- Mobile@Home is a trademark of Telefonaktiebolaget LM Ericsson
- UNIX is a registered trademark of the Open Group
- Windows is a registered trademark of Microsoft Corporation

authentication mechanism. For handsets with USIM, it also supports authentication based on the EAP-AKA protocol.

The AAA server supports mobile application part (MAP) versions 2 and 3 for the retrieval of GSM, GPRS and UMTS authentication information. It uses standard MAP messages to request authentication data from the HLR/AUC/HSS. The Mobile@Home solution can use any standard AAA server that supports EAP-SIM and EAP-AKA, and has the necessary functionality for requesting authentication information from the HLR/AUC/HSS.

DNS and DHCP servers

The Mobile@Home solution can use any standard DNS or DHCP server. For optimum performance, it can be provided with the Ericsson IPWorks software package, which contains DNS and DHCP servers. IPWorks provides the carrier-class characteristics required of telecommunications systems: high capacity, availability, enhanced functionality, a user-friendly and secure O&M interface, extensive redundancy functions, statistics, and load balancing. In addition, IPWorks supports dynamic DNS and responds to DNS queries with a working and available IP address.

Mobile core network

Mobile@Home can connect to any mobile core network node provided the node uses standard interfaces.

Mobile@Home O&M

The Mobile@Home solution uses unlicensed radio frequencies. Therefore, to use it, operators need only configure static equipment, such as signaling terminals, A interface circuits, and Gb and IP interfaces. Terminals and access points may thus come and go

without the need for operation and maintenance or cell configuration or planning.

The HBSC is based on standard AXE, so customers that have an Ericsson OSS need only add one further BSC. After that, all alarm-handling, backups, software upgrades, and so on work as normal. Customers without an Ericsson OSS can manage the HBSC with an element manager running on Windows or UNIX. Windows-based element managers provide some support for handling alarms, collecting statistics and so forth.

Depending on the network scenario, the HBSC can be configured to appear (to the core network) as one or more GSM cells. For example, the selection of a cell global identity (CGI) for a handset attached to the GAN can be matched to the macro location area reported by the handset when it attached to the HBSC. This way, all emergency calls can be routed to the correct city or region.

Conclusion

Ericsson's Mobile@Home solution is not about new functionality or multimedia services. Instead, it is a new access network for the mobile core network. In short, it turns a mobile handset into a single personal communication device. When at home, the handset connects to services through WiFi and broadband connections but when on the move it uses GSM and WCDMA networks. Moreover, it provides seamless transition between the access networks.

Mobile@Home also enables operators to use existing network infrastructure to launch communication services over IP in end users' homes. And they can reuse their provisioning systems, billing systems and so on. For operators and end users alike, Mobile@Home is a clear step toward voice over WiFi through a converged network.

REFERENCES

- 1 3GPP TS 43.318, Generic Access to the A/Gb Interface; Stage 2
- 2 3GPP TS 44.318, Generic Access to the A/Gb Interface; Stage 3