

# Seamless Multimedia Network and Service Access Over All-IP

## Based Infrastructures:

## The EVOLUTE Approach

T. Dagiuklas<sup>a</sup>, C. Politis<sup>b</sup>, S. Grilli<sup>c</sup>, G. Bigini<sup>c</sup>, D. Sisalem<sup>d</sup>, Y. Rebahi<sup>d</sup> and R. Tafazolli<sup>b</sup>

<sup>a</sup> *Hellenic Open University, Greece*

<sup>b</sup> *University of Surrey, UK*

<sup>c</sup> *CEFRIEL, Italy*

<sup>d</sup> *FhG Fokus, Germany*

### Abstract

The concurrent use of the Wireless LAN technology is gaining a hold as a very cost-effective broadband competitor for the cellular networks in medium-range and enterprise areas (the so-called hot spots). There are many differences between these networking technologies, ranging from mobility support to user and service authentication, and a standardized cooperation model has not been yet developed.

The IST project EVOLUTE intends to provide to deeply analyze the problem and develop a suitable solution, in order to provide seamless real time multimedia services to users having any kind of terminal and connection in an all-over-IP network environment, where 3G Cellular Networks and WLAN Hot Spots are integrated, using a loose-coupling approach. EVOLUTE tries to integrate different AAA mechanisms in a scalable AAA architecture with a gateway between 3G and WLAN networks. SIM-based authentication is used for both WLAN and 3G network access. The service provisioning architecture in EVOLUTE is based on SIP and offers both a service creation platform that allows the separation between network and service provider, and an interaction to the AAA infrastructure for managing the service access. This paper presents the EVOLUTE approach associated with the AAA activities for getting access to the network and the services and the service provisioning mechanism.

**Keywords:** all-IP network, 3G-WLAN internetworking, AAA architectures, seamless multimedia services provisioning.

### Name and Contact of the corresponding authors:

Tasos Dagiuklas

Hellenic Open University,

Ag. Andreou Str.,

GR-26222 Patras,

Greece.

e-mail: [ntan@in.gr](mailto:ntan@in.gr)

Christos Politis and Rahim Tafazolli

Centre for Communication Systems Research (CCSR), University of Surrey,  
Guildford, GU2 7XH Surrey,  
United Kingdom.

Ph. +44 (0) 1483 689491

Fax. +44 (0) 1483 686011

e-mail. {c.politis, r.tafazolli}@eim.surrey.ac.uk

Sara Grilli and Glauco Bigini

Cefriel,

via Fucini 2,

20133 Milan,

Italy.

Ph. +39 0223954251

Fax +39 0223954451

e-mail: {grilli,bigini}@cefriel.it

Yacine Rebahi and Dorgham Sisalem

FOKUS - Institut fuer offene Kommunikationssysteme

Kaiserin-Augusta-Allee 31,

D-10589 Berlin,

Germany

email: {rebani,sisalem}@fokus.fraunhofer.de

# 1. INTRODUCTION

The market for wireless communication is rapidly growing and the future trends show the users' expectation in terms of mobility and multimedia services, with higher bandwidth and security, will dramatically increase. Both mobile operators and Internet Service Providers (ISP) foresee an increasing share of their revenues coming from new multimedia and value-added mobile services. Traditional ISPs show a rising interest in wireless technologies as a cost effective mobile alternative to standard wired Internet access in hot spot areas.

The mobile operators are planning to replace/subsidize their existing networks, switching from the current GSM and 2<sup>nd</sup> Generation (2G) cellular networks to the much more versatile and feature rich 3<sup>rd</sup> Generation (3G) cellular systems and UMTS (Universal Mobile Telecommunication System). Mobile telephony operators see in the WLAN technology a new way to increase their revenues by offering broadband wireless data and voice services at lower cost in selected areas.

The deployment of heterogeneous wireless access technologies necessitates the use of AAA mechanisms so that access is granted to users, allowing them to use multimedia services (i.e. streaming, multi-conference). User authentication, through WLANs, needs to issue a request towards a AAA server using protocols such as Radius or Diameter. To be more precise, the user presents his NAI which is of the form user@ realm. On the other hand, in 3G networks, a mobile subscriber needs to present his IMSI to be identified. A challenging issue regards the employment of a common scheme for user authentication regardless of the wireless technology used. Moreover, for the support of seamless communication in such a heterogeneous environment allowing terminal-unaware network access to the users, several aspects need to be considered: user authentication and authorization, service access and provisioning. The transition towards All-IP network architectures, gives the ability to the mobile users to access to rich multimedia services. SIP technology is the standardised method to build powerful services at both Internet and mobile domains. However, to secure access these services, roaming users must be equipped with AAA features. All these issues highlighted above have been addressed by research IST project EVOLUTE.

This paper presents and analyses the EVOLUTE architecture associated with network and service access in heterogeneous environment. The paper is organised as follows: Section 2 presents the All-IP network architecture characteristics within heterogeneous wireless environments and how EVOLUTE's All-IP network architecture is constructed; Section 3 presents different interworking scenarios regarding 3G and WLAN schemes and how EVOLUTE addresses the issue of interworking; Section 4 presents EVOLUTE AAA architecture, user and service authentication in hybrid wireless (3G and WLANs) environment; Section 5 highlights some simulation results associated with the EVOLUTE architecture and finally conclusions are presented at section 6.

## 2. All-IP NETWORK ARCHITECTURE AND THE EVOLUTE APPROACH

With 3G systems, just beginning to be deployed, it is necessary to consider how beyond 3G network architectures will evolve in order to include a much wider range of users, applications and economic deployment. There is no industry consensus on what “Systems beyond 3G”, will look like but as far as the next generation networks is concerned, concepts and ideas include the following [1], [2], [3]:

- Transition towards an “All-IP based network infrastructure
- Support of heterogeneous wireless technologies (i.e. UTRAN, Ad-hoc, WLANs)
- Seamless handover across both homogeneous and heterogeneous wireless access technologies
- QoS support on the IP layer
- Multilayer Mobility Management suitable to support fast mobile users that may access a wide range number of services with diverse characteristics
- Network access control of mobile users (i.e. deployment of AAA protocols that allow inter-domain network access control) regardless of heterogeneous wireless access network used
- Distributed AAA architecture for the dynamic establishment of trust relations in hybrid IPv4/IPv6 networks
- Secure access to multimedia services across different networking environments
- Use of policy-based mechanisms in order to determine QoS, accounting, and billing mechanisms for multimedia services
- Access to multimedia services in hybrid IPv4/IPv6 based networks

EVOLUTE addresses these concepts in the following ways [4]:

1. Use of WLANs and 3G wireless technologies
2. Integration of the above wireless technologies towards an IP-based network
3. Unified AAA access from both WLANs and UMTS
4. Seamless access to multimedia services
5. Service mobility support

To support seamless communication over heterogeneous networks and technologies, EVOLUTE has chosen an integrative approach, allowing the integration of different technologies using gateways between different protocols or relying on a unifying middleware such as the Internet protocol (IP), as illustrated in Figure 1 [4]. EVOLUTE objective is providing an integrated architecture supporting users roaming/moving between networks with different access control technologies and physical interfaces. Users will be able to combine services offered by the visited network provider, as well as by their home provider or a third-party provider, even if not a network carrier, into their own personal service environment. To achieve this goal, the following have been considered:

- *Roaming between different wireless networking technologies.* In the context of EVOLUTE, we mainly consider WLAN and 3G networks. This includes developing mechanisms for allowing seamless handover among

heterogeneous technologies vertical handovers between WLAN and 3G, as well as horizontal handovers inside WLAN networks, where low level mobility support is missing.

- *Roaming between networks with different access control technologies.* In the context of EVOLUTE this mainly involves AAA mechanisms for identifying and authorizing users accessing the 3G and WLAN networks.
- *Service provisioning for mobile users.* This includes the architecture for combining services offered by different providers in a secure and personalized manner.

### 3. 3G and WLAN Interworking

#### 3.1 Technologies Overview

3G will offer data rates ranging from 384 Kbps up to 2 Mbps on the frequencies 1885-2025 MHz and 2110-2200 MHz. The 3G Core Network supports both circuit-switched and packet-switched services. Spectral efficiency in 3G is about three – to four times higher than GPRS, however a major drawback is the 3G deployment [5]. Currently, GSM infrastructure has been deployed over 150 countries worldwide. At its early stages, 3G coverage will be inferior to that of GSM/GPRS in dense urban environments.

On the other hand, WLAN is a relative inexpensive technology. Today's WLAN technology is mainly revolving around IEEE standards. These standards are collectively referred to as "the 802.11 family". The vast majority of WLANs that have been currently deployed are based on the IEEE 802.11b standard supporting data rates up to 11 Mbps. It is expected that this technology will be replaced by its successors. For instance, the IEEE 802.11a,g that support data rates up to 54 Mbps. WLAN systems are increasingly used in homes, offices and indoor public areas. Mobile service providers are exploring opportunities to extend their service portfolios by providing limited, indoor WLAN public access (i.e. hotspot areas). The same basic configuration, that is a laptop computer with a WLAN adapter, can be used to gain access in indoor public and private environments. End-users can thus access their office environments without any noticeable change to the network performance [6].

Table 1 illustrates the main drivers and barriers for WLANs and 3G technologies, as they have been already identified and addressed by the UMTS Forum [7]. Table 2 makes a comparison between the two technologies in terms of network equipment, license cost, CAPEX (Capital Expenditure), Coverage and Speed. Based on the table highlights, it is evident that the two technologies can be complementary rather than competitive to each other. It is expected that 3G will benefit over WLAN in terms of mobility and connectivity. On the other hand, WLAN benefits over 3G in terms of throughput. Therefore, it is obvious that if the advantages of both technologies are combined, we will have a very powerful network covering the needs of the most demanding end-users. Operator's WLAN solutions may vary, but all of them combine the wide-area benefits of second- and third-generation mobile systems, including unlimited roaming and mobility, with increased throughput and capacity in hotspots via WLAN technologies. This combined architecture enables broadband mobile public access to the Internet and to corporate intranets with relatively small additional investment.

### 3.2 3G and WLAN Interworking Requirements and Scenarios

Many advantages may come from the interworking of 3G and WLAN in particular for mobile operators and WISPs; in fact they can both increase significantly their revenues from mobile data traffic and test new application at initial stage in public WLAN. Furthermore high-demand data traffic can be diverted from 3G to WLAN relieving potential network congestion. The basic requirements regarding the interworking between 3G and WLANs are the following:

1. **Business Model:** It has been recognised that the preferred operation model from both network providers and end-users point of view is the deployment of WLANs by a cellular operator.
2. **Partnership between the 3G and the WISP:** In the case of a 3G operator and a WISP, a roaming agreement must be established allowing the 3G subscribers to use WISP in order to access the Internet
3. Uniform billing and accounting between roaming partners must be handled.
4. **A single subscription** is used for both WLAN and 3G accesses.
5. Although the authentication procedure for UMTS is straightforward, there are various ways in order to perform user authentication within the WLAN access in such environment:
  - **SIM/USIM based authentication:** This means that the SIM/USIM card is also used to provide WLAN access to the roaming access. This necessities the use of a gateway that translates AAA WLAN access to 3G AAA access.
  - **SMS one-time password** login with optional payment using Premium Charged SMS. This means that one-time passwords over SMS can be used to authenticate the user.
  - **Network-level authentication** where Mobile IP is used in order to authenticate the user at the visited domain and the Home Agent (it can be configured by the provider)

The service provider value proposition for utilising integrated WLANs with cellular networks includes the following benefits for carrier as well as their subscribers:

1. Extension of current service offering by:
  - Integrating cellular data and WLAN solutions.
  - Positioning for voice phone service in hot spots.
  - Engaging enterprises with in-building solutions.
2. Improved bottom line with new revenue and lower churn:
  - The carrier provides improved in-building coverage by using intranet bandwidth instead of in-building cell sites to provide coverage.
  - Cross system/service integration features become a competitive advantage for the carriers offering Seamless Mobility services.
  - The cellular provider derives service revenue for authentication services, mobility services, and calls that do not use cellular bearer channels.
  - The cellular handset becomes an indispensable element.
  - The handset can operate with more functionality e.g. even as gateway.

- The subscriber increases his dependency on the handset
3. Payload traffic trade-off:
- Some calls will hand over from cellular channels to WLAN connections when subscribers enter these coverage areas.
  - Other calls will hand over to cellular bearer channels when people leave WLAN coverage areas.
  - A more integrated approach to data traffic will probably increase the use of data transferred over cellular systems.
  - As subscribers become more dependent on their much more useful handsets, they will call more and be called more, everywhere.

The most important schemes regarding WLAN interworking between 3G and WLANs are called loose coupling and tight coupling [8]. The following paragraphs describe the network architectures between the two schemes and makes a comparison outlining advantages and disadvantages.

### 3.2.1 Loose Coupling

A **loosely coupled** approach interworks 3G and WLAN access networks at the G<sub>i</sub> interface, as illustrated at Figure 2. The WLAN network is coupled with the cellular network in the operator's IP network. In this architecture, SIM/USIM-based authentication is supported in both the cellular and WLAN networks to gain access to the operator's services. In this approach, different mechanisms and protocols can handle mobility management and QoS in the 3G and WLAN networks. This architecture also supports integrated billing, via the Billing Mediator, into a common Billing System. The WLAN network may be owned by a third party, with roaming/mobility enabled via a dedicated connection between the operator and the WLAN network, or over an existing public network, such as the Internet.

### 3.2.2 Tight Coupling

For **tight coupling** the WLAN network is connected to the rest of the 3G core network in the same manner as other 3G radio access technologies (e.g. UTRAN, GERAN) using an I<sub>u</sub> - like interface, as illustrated in Figure 3. The I<sub>u</sub> interface is defined by the 3GPP RAN34 WG but it is not essential to be a compliant with the standard. In this way, the mechanisms for mobility, QoS and security of the 3G-core network can be reused. In this scenario, seamless roaming between 3G and WLAN access networks is feasible. It is unlikely that interworking between operators would be contemplated using the I<sub>u</sub> interface.

### 3.2.3 Comparisons of the two approaches

The choice between the aforementioned solutions for EVOLUTE architecture is mainly a trade-off between the required degree of modifications to standards and the seamlessness of the interworking and amount of infrastructure

commonality. Starting from these assumptions the most suitable architecture for EVOLUTE is Solution 2 – Loose Coupling because it is suitable for different WLAN technologies and has no impact on GGSN (Gateway GPRS Support Node) nodes, which would imply standardization effort. Furthermore it has one customer database and authentication procedure, which simplifies the handling of security, billing and customer management.

The most innovative aspect of Loose Coupling scenario is the design and specification of the AAA-HLR gateway architecture (SIM Access Gateway). The purpose of the SIM Access Gateway (SAG) is to translate the authentication and authorization mechanisms between a WLAN and a mobile network. Once a user with a SIM-attached device (mobile terminal, PDA, laptop etc) enters a WLAN domain he should be authenticated according to the WLAN signalling procedures but at the same time based on his SIM card subscription. In order to make this possible, the SIM Access Gateway will map the involved signalling during the authentication procedure between a WLAN and mobile network. Furthermore, the gateway will provide authorization procedures in order for the SIM user to be granted access to the WLAN services and vice versa.

## 4. EVOLUTE AAA architecture

### 4.1 Generic AAA Characteristics

In a heterogeneous wireless network environment, the primary challenge regards the adoption of an independent AAA access scheme, allowing the network to authenticate the users regardless the technology used. Other important issues concern the authorisation of the services while the users roams between WLANs and 3G and the ability to route the billing information that is related to the bandwidth usage. There are two primary types of roaming between 3G and WLAN networks [9]:

1. In the first case, a 3G users roams into a WLAN network. This means that the 3G operator will have some control over the user, or a public WLAN in a hot-spot area or an WLAN in a corporate environment.
2. In the second case, a WLAN user has the option to roam in a 3G network. This network can be either a 3G operator at home or a visited network somewhere.

In case the home provider employs a different AAA infrastructure than the one of the foreign provider, then a gateway is required to provide the necessary translation between the two protocols.

### 4.2 EVOLUTE AAA Architecture

In EVOLUTE, a business model that is called cooperative service has been adopted [4]. In this model, a user has a fixed subscription to one service provider and in the same time can access services from other providers as well. In this scenario, the home provider is distinguished from the other service providers. The home provider manages the user's data and profile and maintains information required to authenticate the user for using a certain service, and foreign provider, in which premises the user is currently located and which provides the user with the IP access, local services, such as local chatting or gaming groups, and the forwarding user's incoming and outgoing calls.

Thereby when a user enters a foreign network, the foreign network provider needs to execute AAA mechanisms for the following resources:

- 1. Internet Access:** This includes the access to the network transport resources. In order to ensure that only eligible users can access the network resources and receive an IP address, the AAA infrastructure must provide functions associated with the user authentication (e.g. it verifies that the user proves who he is claiming to be), the user authorization, (e.g. it verifies that the user is actually allowed to access the network) and the accounting of the network resources that are spent by the user.
- 2. Service access:** After receiving the IP connectivity pipe, the user might want to access to applications and services (i.e. media streaming, VoIP, Web browsing). In general, this request may involve either one or several content providers that have signed agreement with the network operator. In this case, the AAA infrastructure must provide the functions, that verify whether the user is allowed to access the requested service and provide accounting information of the service usage. Without loss of generality the main emphasis regarding the multimedia services has been given to SIP-based applications and services and the associated platforms. This is due to the fact that SIP is the platform to deploy multimedia services at both packet-based and 3G networks [10].
- 3. Local access control AAA protocols:** In the WLAN environments, 802.1x is used as an access control protocol for authenticating and authorizing the user between the end device and the base station [11]. The 802.1x protocol applies to the association of wireless hosts (suplicants) to Access Points (Authenticators) with a supporting authentication server (i.e. RADIUS, DIAMETER). Without loss of generality, a RADIUS-based AAA server has been employed due to the simplicity to be deployed in small number of networks/domains [12]. The 802.1x authentication process uses the Extensible Authentication Protocol (EAP) [13] between the Mobile Host and the authentication server. The Authenticator is configured with two logical access points to the LAN through a single physical LAN port, namely the controlled port and the uncontrolled port. The uncontrolled port allows an uncontrolled exchange between the authenticator and other systems of the LAN regardless of the system's authorization state. Normally, the uncontrolled port will only accept packets to establish authentication. In 802.1x, these are EAP over LAN (EAPOL) packets. The second logical access point allows an exchange between a system on a LAN and the authenticator services only if the system is authorized. Here so called Network Access Identifiers (NAI) are used to identify the users. In the case of 3G network, the authentication and authorization technology must be able to rapidly and uniquely identify the user for both network access and service access, using different kinds of identifiers such as USIM's (Universal Subscriber Identity Module) and IMSI (International Mobile Subscriber Identity). Without loss of generality, the IMSI identifier has been employed in EVOLUTE users. In 3G networks, network access authorization is accomplished using 3G AKA (Authentication Key Agreement), and the user data are managed, within the Core Network, by the VLR (Visited Location Register) and the HLR (Home Location Register), communicating over the MAP (Mobility Anchor Point) protocol.
- 4. Local AAA infrastructure:** This describes the protocols and components used in a network for realizing the AAA functionalities. For WLANs, RADIUS can be conveyed for carrying AAA requests and answers between

an AAA server and a SIP proxy, or base station. For 3G networks an infrastructure similar to what is currently being used for GSM is used based on a home subscription system (HSS).

5. **Inter-domain AAA exchange:** When a user roams into a foreign network, that network might need to contact the home provider of this user before providing him with access to the network resources and local services. Depending on the used networks there are three exchange scenarios: native IP networks, that use an AAA infrastructure for the exchange of AAA information between the involved providers, native 3G networks, which AAA exchange, heterogeneous networks, in which the AAA exchange should be provided between networks using different AAA infrastructures and protocols. In this last scenario the authentication of a user coming from a 3G provider in a native IP network, requires some interaction between the AAA infrastructure of the native IP network and that of the 3G networks. In EVOLUTE, this is accomplished through a gateway that translates the AAA protocols and information carried between the two worlds. A user wishing to access the services offered by the foreign network indicates its wish to use the service and gives the provider its network address identifier (NAI). This identity is forwarded from the access to the AAA server. If the NAI contains an IMSI, then the access request is forwarded to a gateway that translates the AAA request into the equivalent 3G AAA protocol request. This gateway might be pre-configured or might be dynamically searched for through some brokerage service. The access request might then be further forwarded over SS7 signalling to another 3G network (home network of the user) and replies to the request are forwarded back to the user over the gateway. In case the NAI does not include an IMSI then the AAA server tries to contact the home network of the user as identified by the NAI over the AAA infrastructure, i.e., either directly if a trust relation is available between the foreign and home network or through an AAA broker.

### 4.3 User Authentication

The most challenging part regarding user authentication concerns the scenarios where the user from WLAN access is authenticated in a 3G network. The entities involved in this scenario are the following, as illustrated in Figure 5:

1. **WLAN user:** The WLAN card is equipped with a SIM card in order to provide the subscriber credentials and executes securely sensible cryptographic calculations
2. **AP EAP Authenticator:** This entity is located at the WLAN AP and is responsible for authenticating the client by communicating with an AAA server (either DIAMETER or RADIUS). The WLAN authenticator handles the EAP interaction and initializes the EAP/SIM functionality. This is accomplished by encapsulating the EAP-SIM messages in either RADIUS-based or DIAMETER-based packets.
3. **AAA Server:** This server can be either based on RADIUS or DIAMETER. This server is able to process requests and provide AAA services for WLAN access. This server receives requests from SIM-based users acting as a Proxy redirecting the exchanged messages to and from the SAG.
4. **Service Access Gateway (SAG):** It resides between the WLAN island and the 3G network. Its main functionality is to authenticate and authorize the WLAN users in the 3G network. The SAG comprises of the following subsystems:
  - Reception of EAP-SIM information from the WLAN

- Proxying of the AAA messages from the WLAN-AAA server. These messages can be based either on RADIUS or DIAMETER framework. Without loss of generality, the described architecture presents the use of RADIUS.
- Integration of the EAP server in order to respond to the commands received by the WLAN user.
- Mapping of AAA (RADIUS or DIAMETER) to the corresponding 3G one (MAP)

The EAP/SIM authentication is used to employ session key distribution for the signalling and data encryption using the 3G (which is similar to the GSM one) subscription [14]. Under this framework, the user is authenticated by an AAA server that supports EAP. Figure 6 illustrates the MSC using the EAP/SIM Authentication procedure.

- According to the EAP-SIM authentication procedure, the authenticator sends the EAP-Req-identity message towards the client requesting his identity.
- Upon the reception of the EAP-Req-Identity message, the client responds with an EAP-Resp-Identity message including the IMSI (IMSI@realm), which is used to identify the user within the GSM network.
- This message is encapsulated in a RADIUS Access Request and is sent towards the SAG.
- The SAG replies by sending towards the user the EAP-Req-SIM-Start message and the user responds by sending the EAP-Resp-SIM-Start that contains the AT\_NOTICE\_MT field, which includes a random number NONCE\_MT.
- Upon the reception of the above message, the SAG contacts the HLR authentication server in order to obtain GSM triplets (RAND, XREWS, Kc).
- Subsequently, the SAG sends the EAP-Req-SIM-challenge that contains the RAND challenges and a message authentication attribute AT\_MAC encapsulated within a RADIUS message.
- Upon the reception of the above message, the user runs the GSM authentication algorithm in the SIM card and then verifies whether the calculated MAC is identical with the received one. If it does not match, the user ignores the EAP packet. Otherwise, the user responds by sending an EAP-Resp-SIM-Challenge message containing the MAC-SRES response.
- The AP, encapsulates the above message within a RADIUS message and is sent towards the SAG.
- The SAG verifies the validity of the response and responds with an EAP success inside the RADIUS Access Accept that is sent towards the WLAN AP.

#### 4.4 Service Authorization

In order to provide multimedia (without loss of generality, SIP services have been considered in EVOLUTE network architecture), the user needs to be authenticated again. This authentication procedure regards user's profile and preferences in order to grant access to the services offered by the network provider. This information can be retrieved whenever, the users requires access to multimedia services. This can be handled using the LDAP for instance. Prior to describing the steps associated with service authorisation, the following assumptions have been made:

- The user has a subscription with the 3G network operator/provider
- There is a trust relationship between WLAN network and the 3G operator, allowing the user to roam between WLANs and 3G networks
- The network operator is also a service provider
- There is a trust relationship between the foreign and home SIP proxies. This means that the SIP requests that are issued in the foreign are not authenticated by the home SIP proxy.
- The user is allowed to access any service requested after he has been authenticated.

Figure 7 illustrates the steps associated with service authorisation:

- The user get access to the network according to the procedure described in section 4.3
- The Foreign SIP Proxy supports HTTP Digest for the user authentication [15]. This means that the user uses the SIP address as username and IMSI as password. It is assumed that the user's SIP is of the form "SIP:user@home\_service\_provider". The SIP proxy extracts from this SIP address, the expression "user@home\_service\_provider" which will be used within the AAA request as a NAI
- The AAA server receives the SIP proxy's request and forwards it to the Gateway
- The SAG requires verifying whether the received NAI has the form of "IMSI@home\_network". If not, it will check the database to verify whether there is a URL associated with the IMSI included in the password and whether this SIP URL matches the one used as username. If they match, the SAG sends a AAA success message towards the AAA server which in turn forwards it to the Foreign SIP Proxy.
- The Home SIP Proxy sends a 200 OK message, which is forwarded by the Foreign SIP Proxy to the user. This ends the registration phase.

## 5. Multimedia service provisioning

### 5.1 Architecture

The EVOLUTE architecture will allow a user to access a set of multimedia services deployed in an IP network regardless of the heterogeneous type of the access network used. EVOLUTE infrastructure will allow a user to access a set of multimedia services deployed in an IP network regardless of the type of the access network used. Two types of services will be provided:

1. **Home services:** These services are offered by the home SIP provider of the user such as call handling features or auto dialling.
2. **Local services:** These are services provided by a SIP provider owned by the provider of the IP access at the foreign network. This could be a network provider, a coffee shop or an airport for example. The services provided here are more of location based services such as information about local shops or movies, access to a local PSTN gateway which offer cheap access to the PSTN at that location or chat and gaming sessions with people who are geographically close to the user –i.e., in the same coffee shop or Mall.

When aiming at providing communication services for mobile users in a seamless manner one needs to consider different sources of heterogeneity:

1. **End devices:** End devices might have different capabilities like supported compression styles for example.
2. **Applications:** This involves reaching some communication between applications using different protocols such as enabling an instant messaging session between a SIMPLE and an ICQ application.
3. **Internet Access:** In this scenario all communicating end devices have direct access to the Internet and can thereby access all services provided over the Internet transparently. An interesting case here might be when moving from a high bandwidth environment to a low bandwidth one. In this case some adjustment of the used service might be required. This can take the form of changing the compression style to one with a lower rate or closing a video connection and using only audio in a conferencing scenario for example. These changes can be triggered by the end systems or by the network that might add transcoders for example.
4. **Heterogeneous Access:** This involves a communication scenario in which the communicating end devices are attached to network of different technologies such as a communication between a PSTN and an Internet user. This requires the addition of gateways in between the technologies to translate from the one form to the other.

The proposed EVOLUTE architecture for multimedia service provisioning depicted in Figure 8 and is based on SIP protocol. This architecture consists of the following components:

1. **Service platform:** This component is the core provisioning part, supporting signal handling and routing. For SIP based services this would be a SIP proxy receiving SIP messages and routing them to the appropriate destination and executing a needed intelligent services.
2. **Service management:** This includes the intelligence needed to control the behaviour of the service platform and coupling the different components constituting the service provisioning platform. This includes providing the platform administrator with the necessary interface for adding new functionalities and configuring the interaction between the different supported service components.
3. **Personalized services:** This includes managing the profiles of the users, which govern how a service should be executed for a certain user. That is, such profiles might be CPL scripts dictating that all calls coming from some caller should be rejected or that all messages should be forwarded to a message-to-SMS gateway at certain times of the day.
4. **AAA:** This is the interface of the platform to an AAA infrastructure. This interface is used to authenticating users requesting some services and authorizing the service usage.
5. **Transcoder:** This is an entity that is used to translate the content sent by one user into a form understood by another. This might be for example a voice to text transcoder allowing a hearing impaired person to communicate with another user with only a voice capable end device.
6. **Unified messaging:** This includes services such as voicemail system, translation services and text to fax for example.

7. **Instant Messaging and Presence:** One of the most widely used application in the Internet is instant messaging. This for of near real time communication allows textual communication as well as sending information to users in an asynchronous manner. Presence and notification on the other hand allow the user to subscribe to certain events and to get notified when this even occurs.
8. **Application and protocol gateway:** These are components that are dedicated to the translation between different protocols and applications. This includes a SIP to SS7 gateway as well as a SIMPLE to YAHOO for example. In the first case the gateway would allow the communication between a VoIP user and a PSTN user. In the second one, it would allow a user using SIP messaging to communicate with a user using the YAHOO messaging application.
9. **Streaming servers:** This includes the servers that provide the audio and video streaming.

Two service scenarios have been considered using the EVOLUTE architecture: Instant Messaging and Video Streaming from the WLAN. The MSC flow for these two services are described below:

1. **Instant Messaging:** In the instant messaging scenario, the message flow scenarios is the following, as illustrated in Figure 9 :
  - User A is equipped with PDA-based MSN messenger to get access to the network. User and service authorisation takes place according to the procedures described in paragraphs 4.2 and 4.3 respectively.
  - The chat session starts. The SIP/IM Gateway handles the routing of SIMPLE messages within the session.
  - After some time, User A wants to move out of the WLAN network and intends to use his mobile phone to continue the chat. He then sends to User B his mobile phone number and tears down the session.
  - User A will receive on his mobile a SMS message with a header containing User B's SIP address and a body which is the content of the message. User A can keep chatting by replying to his friend's message. Another way to respond back to User be is to write a new SMS message
2. **Video Streaming from the WLAN:** A user from a WLAN is initiating a video streaming session as illustrated in Figure 10
  - The user enters in the WLAN and performs the SIP registration, required for updating the user's location and notifying him about some events. He got successfully the access to the network and to the multimedia service.
  - Once the server registers him, he receives an Instant message where there is an RTSP URL.
  - His SIP/RTSP integrated client automatically reads the RTSP URL and request the movie to the RTSP server. Since the movie is free of charge only for the WLAN users, the RTSP server has to check whether this user is really allowed to view the movie.
  - The RTSP server uses HTTP digest authentication to ask the mobile host for credential. The mobile host will send a token containing the required credential to the RTSP server.
  - The RTSP server checks if the user is authorized for viewing the movie by sending a RADIUS request to the local AAA server. When the RTSP server receives a positive answer from the AAA server, it provides the service.

## 6. EVOLUTE ARCHITECTURE SIMULATIONS

The architecture design and specification phase is followed by an evaluation and simulation phase. In this phase many aspects of the planned architecture are tested, in terms of simulation studies and message flow analyses. Not all the aforementioned architecture components will be considered for the simulation and analysis studies, but only those in which a technology choice is needed, or a better understanding of the basic component interaction is required before implementation. Particular emphasis has been given on the AAA simulations and IEEE 802.1x evaluation.

In this section, we study and simulate IEEE 802.1x applicability for the H2 case, by considering a pre-authentication scheme for fast handoffs [17], [18]. The 802.1x protocol applies to the association of wireless hosts/MT to APs with a supporting authentication server (e.g. Radius). The 802.1x authentication process uses EAP between the MT and the authentication server. The basic 802.1x architecture is described further on.

- ü The AP requests an identity from the MT.
- ü The MT sends its identity to the AP.
- ü The AP forwards the information to the AAA server via EAP.
- ü The AAA server and the MT have an EAP authentication dialog. The authentication dialog between the MT and the AAA server must be negotiated between them as part of EAP dialog. The authentication dialog between the MT and the Authentication Server is carried in EAP frames. The EAP frames are carried as EAPOL in 802.1x, and as EAP attributes in Radius. It should be noted that mutual authentication eliminates rogue APs.
- ü If the dialog is successful, the MT and the AAA server share a session key.
- ü The AAA server sends the session key to the AP in a Radius attribute as a part of Radius accept message.
- ü The AP enables its controlled port for the MT.

Consecutively, we discuss and analyze a fast inter-AP handoff scheme. In the scheme, a MT performs authentication procedures not only for the current AP but also for neighbouring APs, when it handoffs. Figure 11 shows the basic components involved in the pre-authentication. Since IEEE 802.1x provides a network port access control scheme, this is more scalable than others. The supplicant system (MT and AP) is an entity at one end of the point-to-point LAN segment that is being authenticated by the authenticator attached to the other end of the link. The authenticator system (adjacent AP and AAA server) facilitates authentication of the entity attached to the other end of the link via the authentication server. The authenticator controlled port is in the unauthorized state; therefore the authenticator makes use of the uncontrolled port to communicate with the supplicant, using EAPOL and EAP to communicate with the AAA server. The innovation here is that MT authenticates with several APs during the scanning process, so that when association is required, the MT is already authenticated.

Figure 12 shows the key distribution in IEEE 801.x for the H2 case. Despite a MT sends an authentication request to the AAA server, the latter sends multiple authentication responses to all APs within that frequent handoff region. The FHR is a set of adjacent APs. It is determined by factors such as location of APs in a WLAN service area and

users' movement pattern. By definition, the FHR is comprised of APs, which MTs are likely to move shortly. Although, there are a lot of APs in a public WLAN, the movement ratio between different APs is not the same (depending on geographical profile/location, velocity of users, QoS contracts i.e. applications type and services class etc). In order to take these factors into account and evaluate the pre-authentication process for HiperLAN/2 systems, we use the FHR selection algorithm described in [17]. After having received responses, all APs except the current one keep the authenticated information until the specific timer has expired. If there is no handoff during that period, the information expires and the MT should perform re-authentication when a handoff occurs.

Figure 14 shows the re-authentication message flow after handoff. We assume that the adjacent AP belongs to the FHR. If a MT hands off to the adjacent AP, no further message exchanges are needed (due to pre-authentication). In the 802.1x model, the controlled port changes into an authorized port after authentication. However, in the pre-authentication scheme, the port in ready state can change imminently to authorised state just by checking the identifier of the MT, without further interaction with the AAA server.

Finally, we compare the handoff delay for the fast handoff scheme as proposed in [17] and for different service classes. The total delay during handoff can be measured by the summation of all the delays across the wired and wireless links [18].

Figure 14 shows the average handoff delay when the AAA server is located in the local domain. It can be seen that the average delay is lower when the pre-authentication scheme is used rather than the BE (Best Effort) class/user (normal handoff process). Additionally, users belonging to CO (Conversational) class have lower delays compared to users in other classes, e.g. ST (Streaming) or IN (Interactive). Figure 15 shows the simulation results in the remote AAA server case. Here the pattern is similar to the one in Figure 14. However, the average handoff delay is approximately 20, 25 and 30 msec higher than the delays for IN, ST and CO class users respectively. Therefore, the proposed pre-authentication scheme based on the IEEE802.1x protocol for H2 (WLAN) systems is more appropriate for multimedia services and other delay sensitive applications.

## 7. CONCLUSIONS

This paper has presented an All-IP network architecture integrating heterogeneous wireless technologies: 3G and WLANs. The loose coupling approach has been adopted for the interworking between WLANs and 3G, where the WLAN network is coupled with the cellular network in the operator's IP network. SIM-based authentication is used for both wireless technologies in order to perform unified user access by considering that the user profile data are stored at the cellular network. This necessitates the introduction of a AAA gateway that translates WLAN AAA messages (RADIUS) to the corresponding 3G AAA (MAP) messages. Service authentication is performed on the user's profile and preferences in order to grant access to the services offered by the network provider. This information can be retrieved whenever, the users requires access to multimedia services

## **ACKNOWLEDGMENTS**

This work has been performed in the framework of the IST-2001-32449 project EVOLUTE, which is partly funded by the European Union. The authors would like to acknowledge the contribution of their colleagues from Intracom S.A., FhG Fokus, Alcatel-SEL, Motorola UK, University of Surrey, CERFRIEL and Telia.

## REFERENCES

- [1] J. De Vriendt, P. Lainé, C. Lerouge and Xiaofeng Xu, "Mobile Network Evolution: A Revolution on the Move", *IEEE Communications Magazine*, Vol. 40, pp., April 2002.
- [2] Y.Kim, B.Jang Jeong, J.Chung, Chan-Soo Hwang, J.S. Ryu, Ki-Ho Kim, and Y.Kyun Kim, "Beyond 3G: Vision, Requirements, and Enabling Technologies", *IEEE Communications Magazine*, Vol. 41, March 2003, pp. 120-124.
- [3] WWRF WG-3 White Paper
- [4] EVOLUTE Architecture Specification, Deliverable 2.1
- [5] D. Wisely et al, *IP for 3G: Networking Technologies for Mobile Communications*, John Wiley, 2002.
- [6] R. Van Nee et al, "New High-Rate Wireless LAN standards", *IEEE Communications Magazine*, Vol.40, pp. , December1999.
- [7] UMTS Forum, *Report 22: Impact and Opportunity: Public WLANs and 3G Business Models*, 2002
- [8] A. Salkintzis et al, "WLAN-GPRS Integration for Next Generation Mobile Data Networks", *IEEE Wireless Communications*, Vol. 9, pp. 112-124, October 2002.
- [9] Y. Rebahi and D. Sisiale, "AAA Management in the Internet for Wireless and 3G users", *WWRF#7 meeting*, Eindhoven, Netherlands, December 2002.
- [10] H. Sinnreich and A. B. Johnston, *Internet Communications Using SIP*, John Wiley, 2002.
- [11] *IEEE Standards for Local and Metropolitan Area Networks: "Port based Network Access Control"*, *IEEE Standard 802.1X-2001*, June 2001.
- [12] IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), June 2000.
- [13] IETF RFC 2284, The Extended Authentication Protocol (EAP), March 1998.
- [14] H. Haverinen, J. Salowey, "EAP SIM authentication", *Internet Draft*, December 2002.
- [15] IETF RFC 2069, HTTP Authentication: Basic and Digest Access Authentication, June 1999.
- [16] IETF RFC 2326, Real Time Streaming Protocol, April 1998
- [17] Sangheon Pack and Yanghee Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN based on IEEE 802.1x Model, " *IFIP TC6 Personal Wireless Communications 2002*, Singapore, October 2002.
- [18] EVOLUTE Architecture Simulation, Deliverable 2.2
- [19] N. Akhtar, M. Georgiades, C. Politis, R. Tafazolli "SIP-based End System Mobility Solution for All-IP Infrastructures", *IST Mobile & Wireless Communications Summit 2003*, 15-18th June 2003, Aveiro, Portugal.

FIGURES

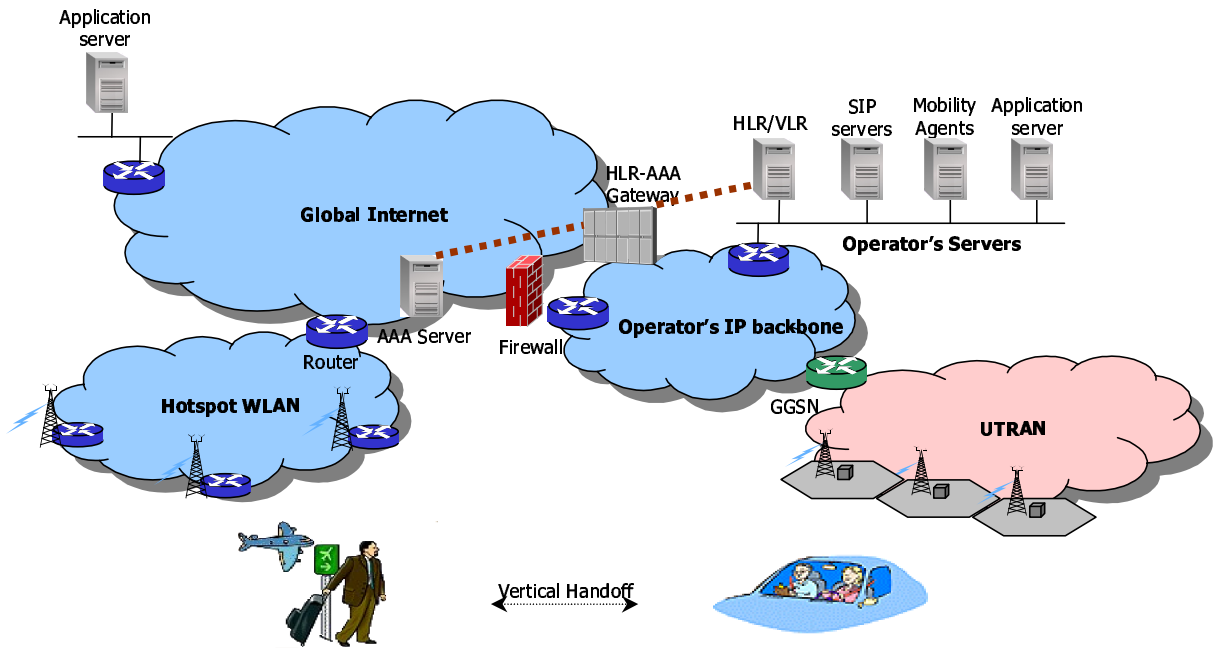


Figure 1 - EVOLUTE IP-based network architecture.

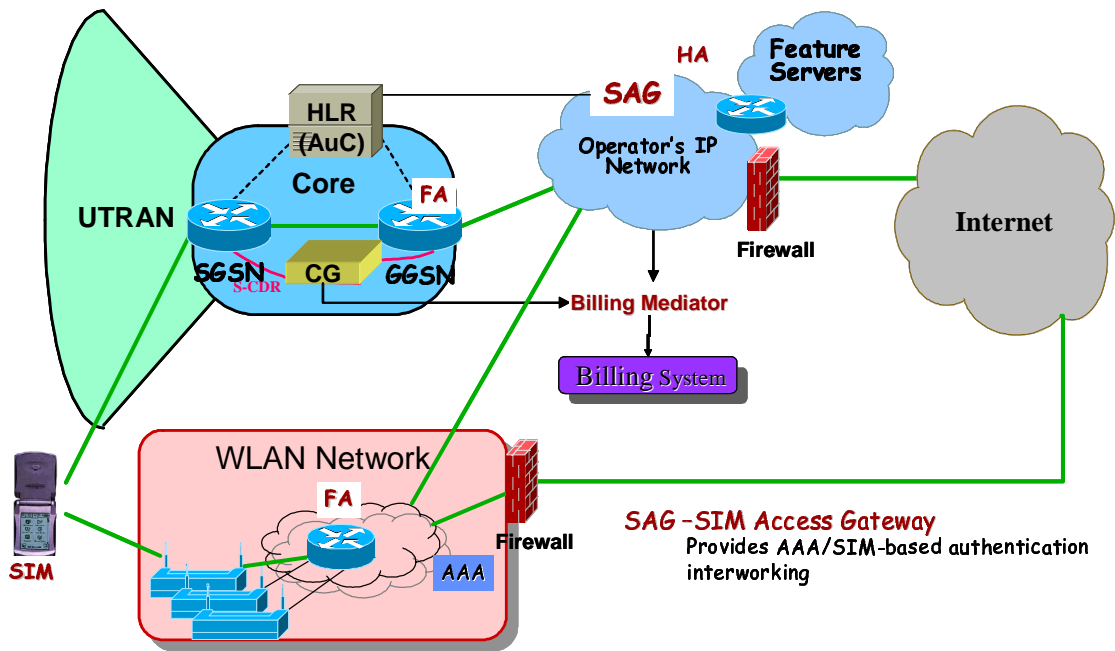


Figure 2 - Loose Coupling scenario

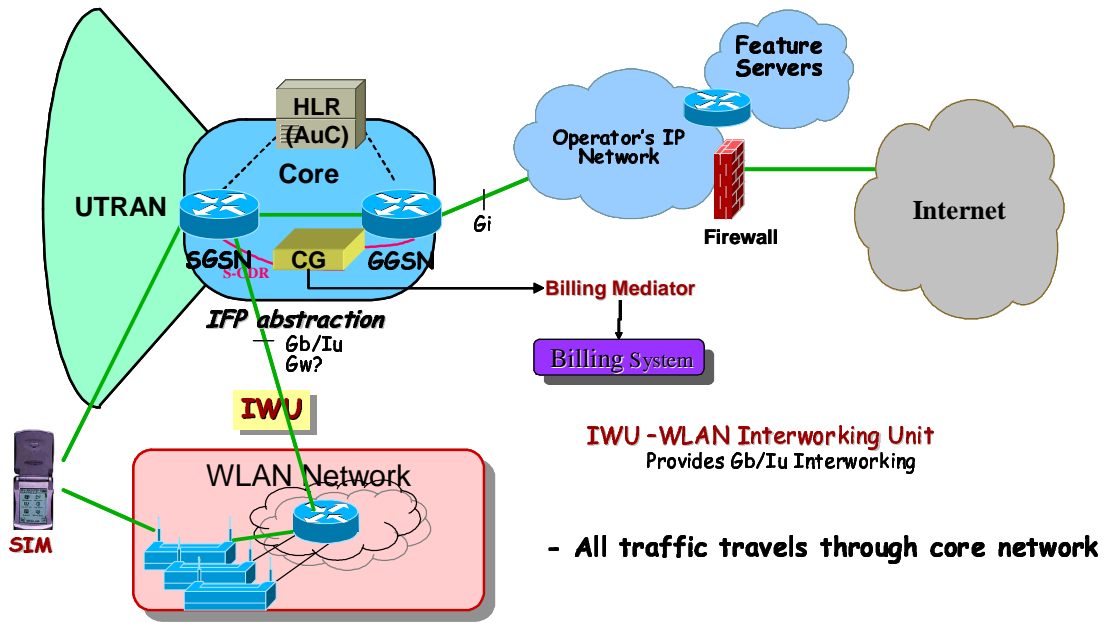


Figure 3 - Tight coupling scenario

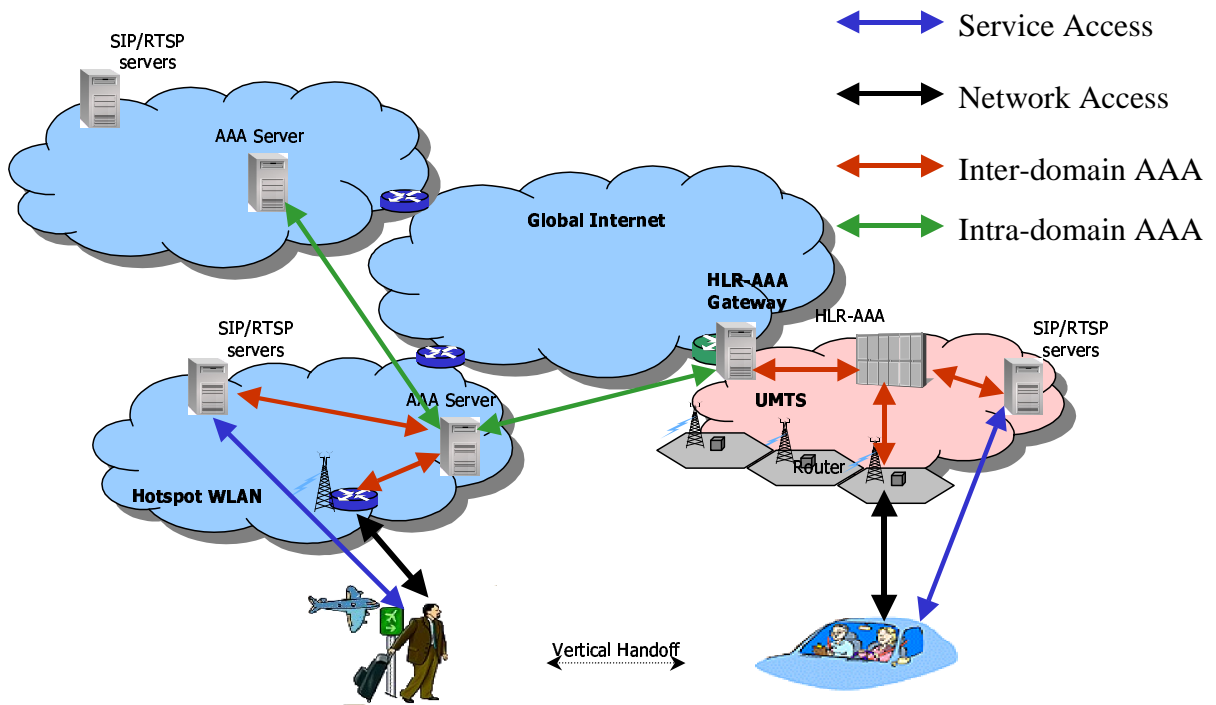


Figure 4 - EVOLUTE AAA architecture for supporting heterogeneous environments

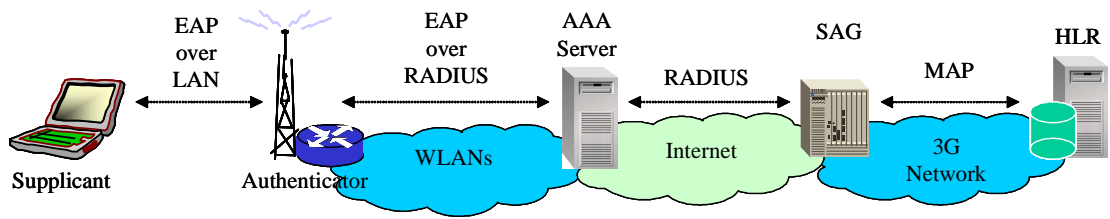


Figure 5 – WLAN user authentication and authorisation using the SAG

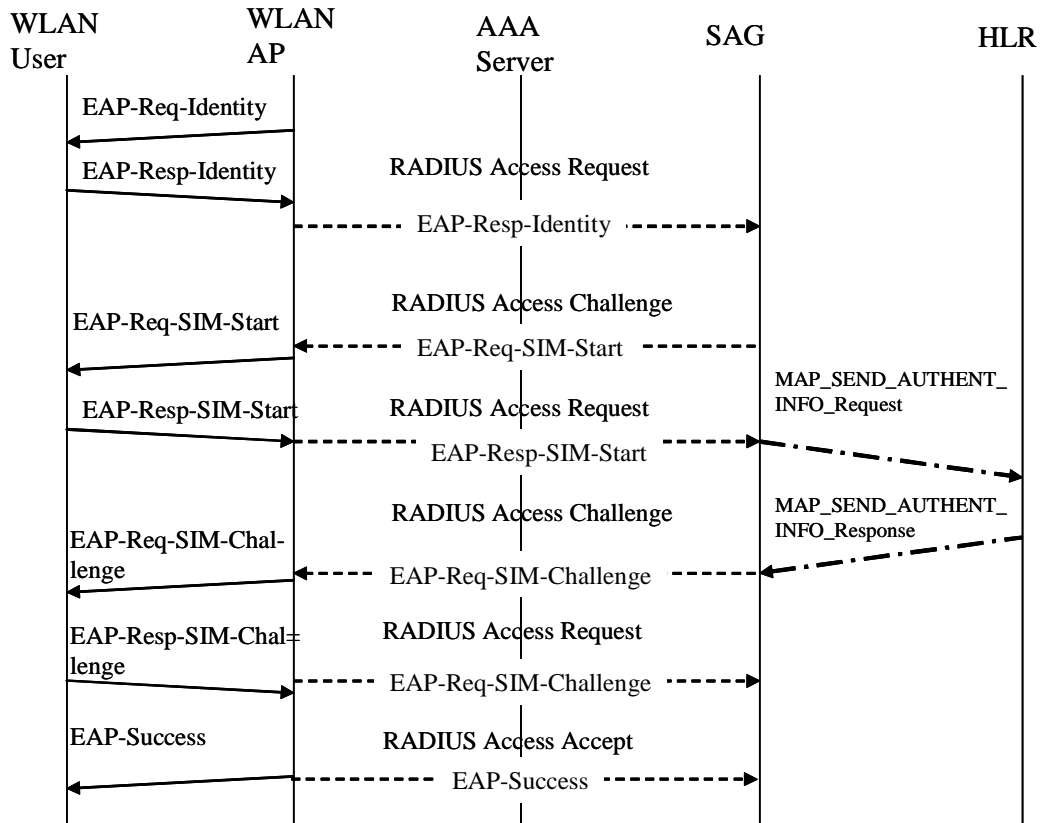


Figure 6 – MSC authentication WLAN user within a 3G network

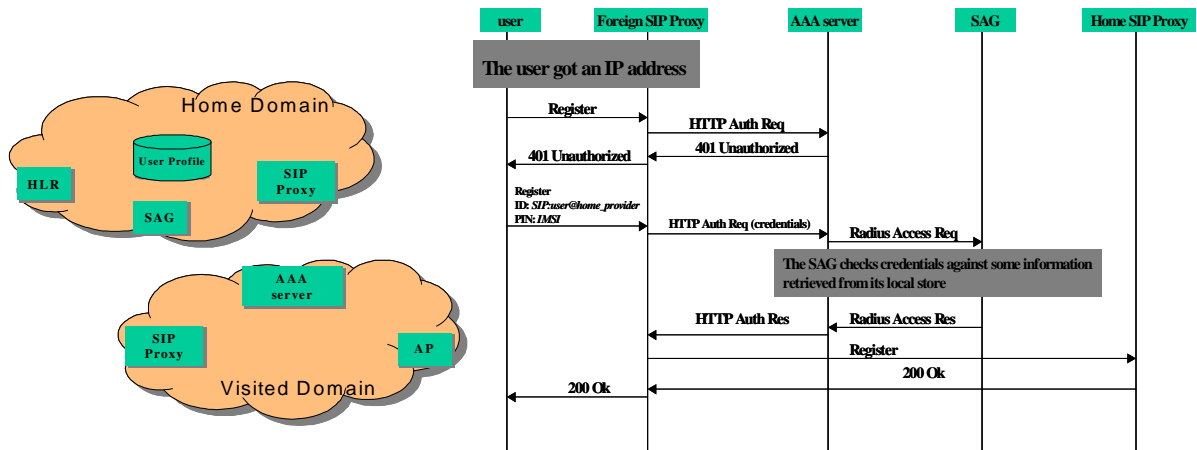


Figure 7: Service Authentication

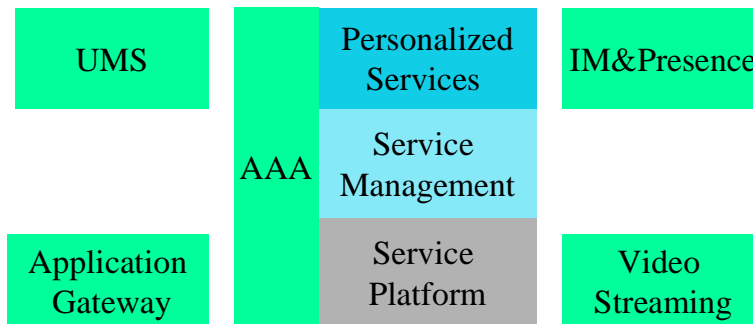


Figure 8 : EVOLUTE Service Provisioning Infrastructure

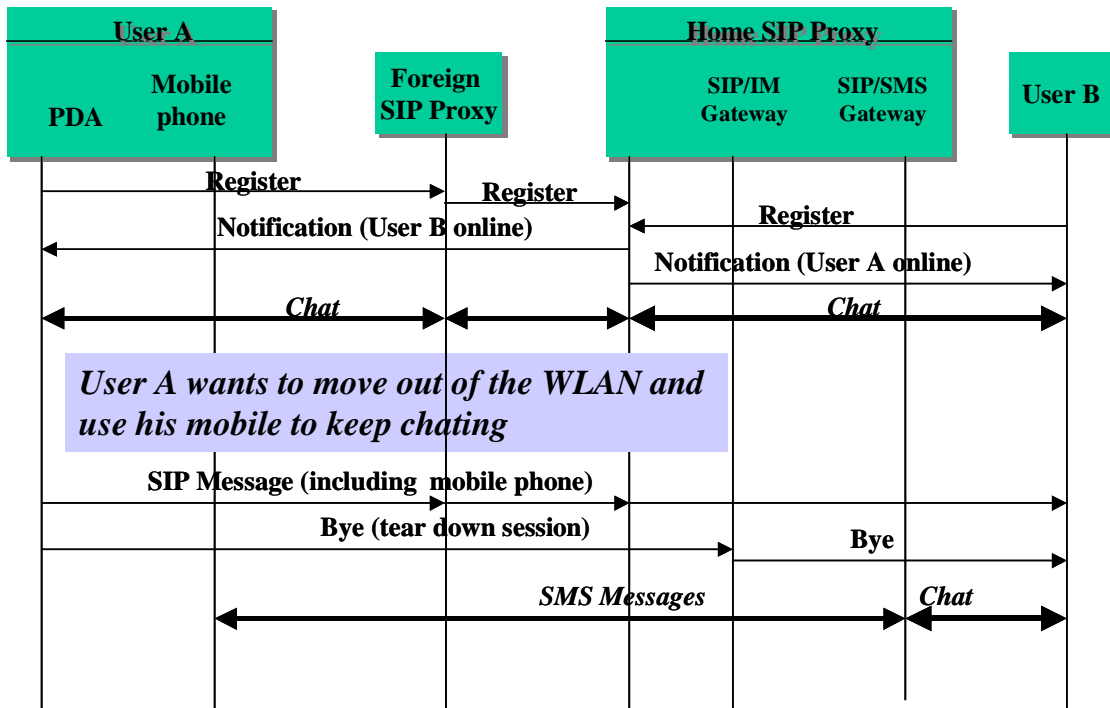


Figure 9 –IM MSC Flow

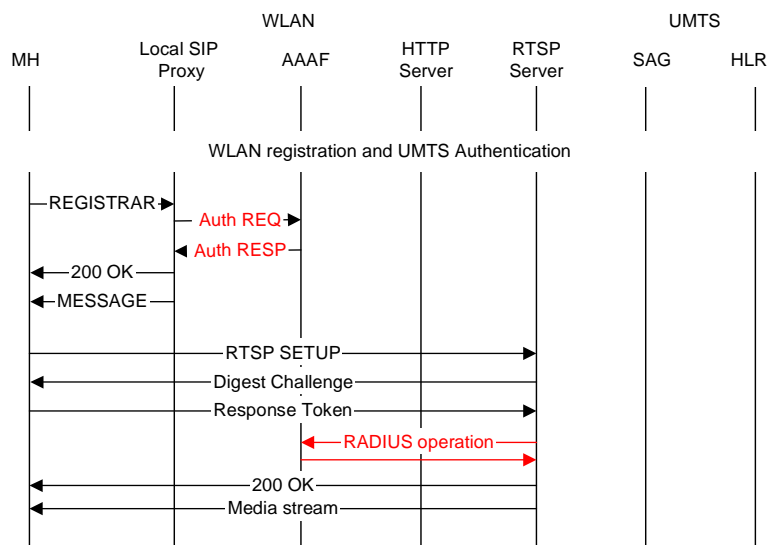


Figure 10: Video Streaming in WLAN

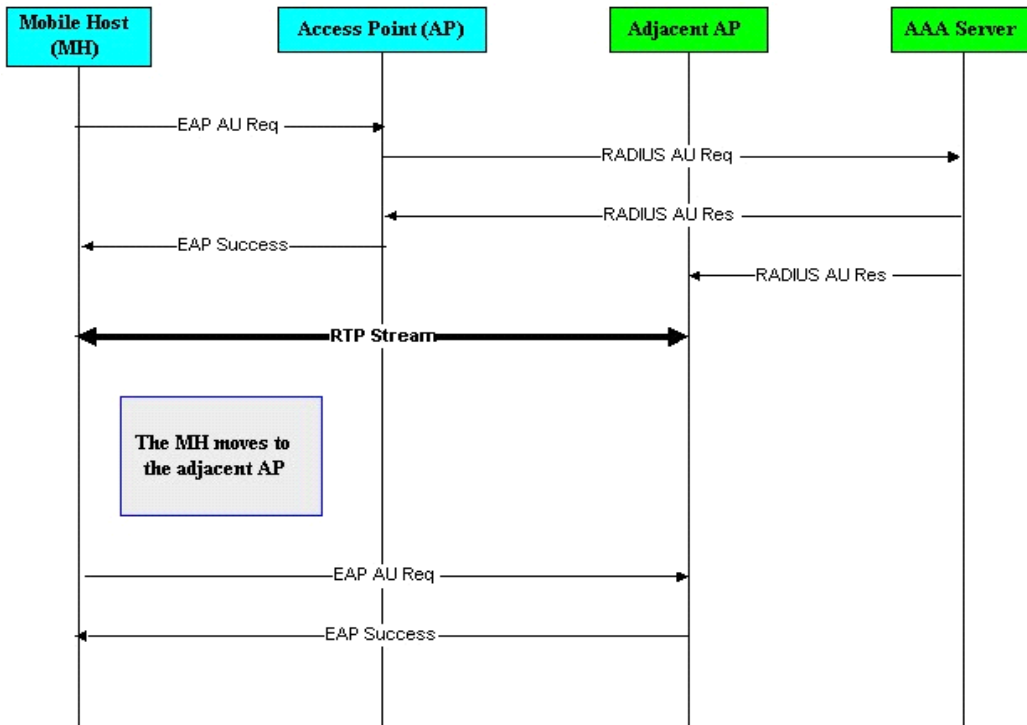


Figure 11: Pre-authentication scheme for fast handoff in H2

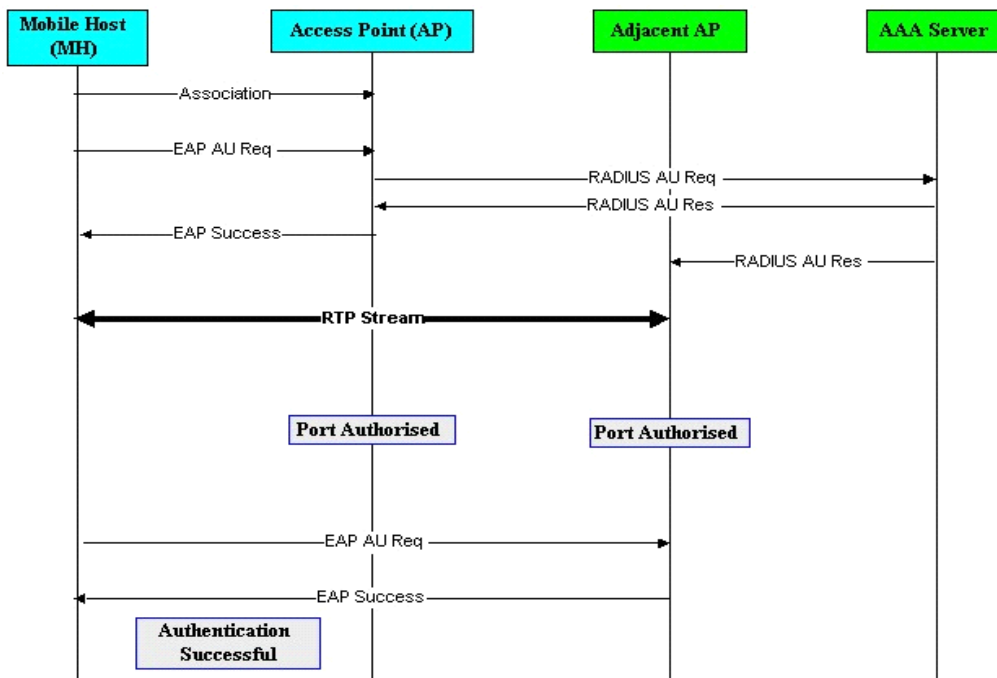


Figure 12: Message exchanges before handoff

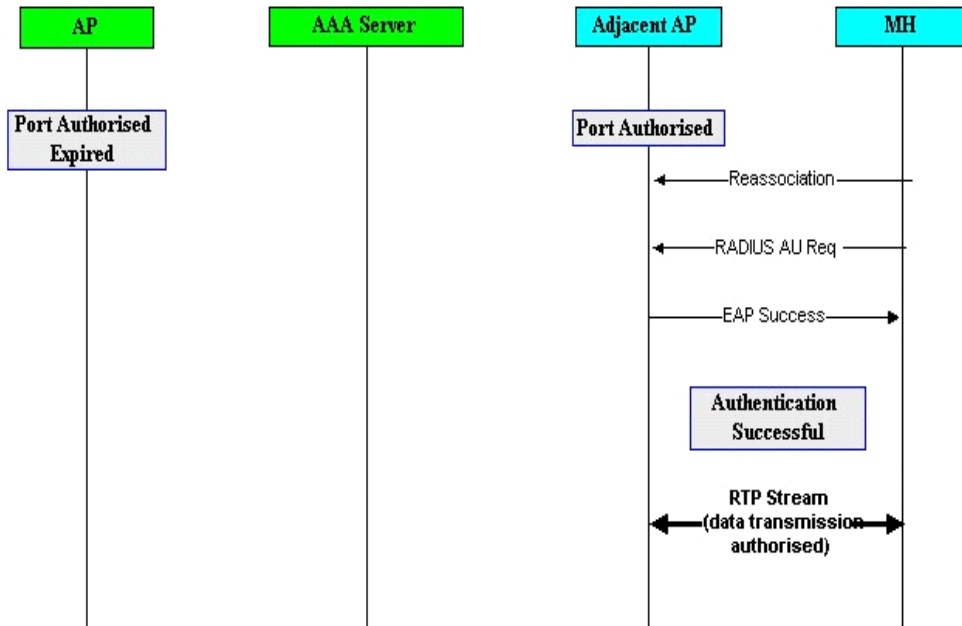


Figure 13: Message exchanges after handoff

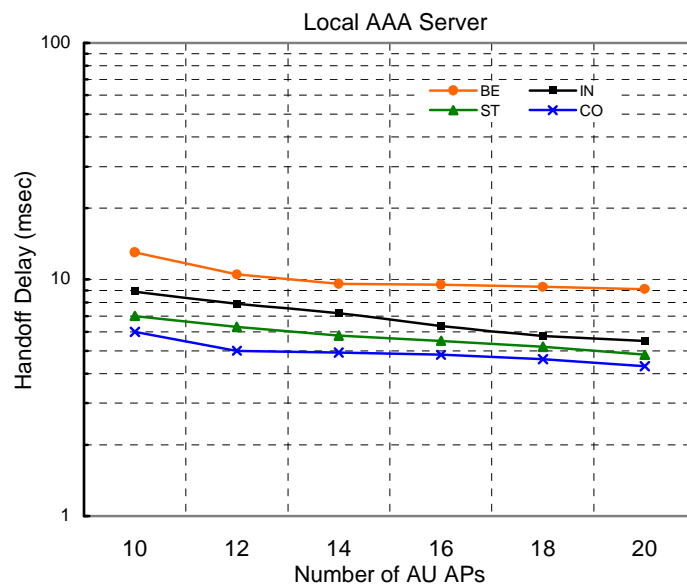


Figure 14: Handoff delay for pre-authenticated H2 APs (Local AAA server)

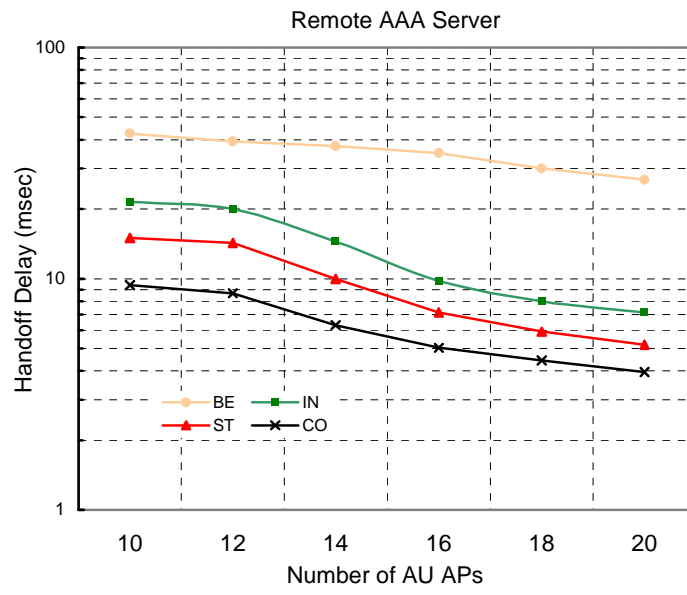


Figure 15: Handoff delay for pre-authenticated H2 APs (Remote AAA server)

TABLES

	Wireless LAN	3G
<b>Drivers</b>	<ul style="list-style-type: none"> <li>§ Low price for access technology and terminal equipment</li> <li>§ Expected low price of use for public access</li> <li>§ Technology is available and performance visible</li> <li>§ Simple configuration</li> </ul>	<ul style="list-style-type: none"> <li>§ Area-wide coverage</li> <li>§ "Convenience " (no gap in media)</li> <li>§ Roaming</li> <li>§ Suitable for mass market (only mobile phone required)</li> </ul>
<b>Barriers</b>	<ul style="list-style-type: none"> <li>§ Security</li> <li>§ Restricted freedom of movement</li> <li>§ Problematic installation on devices, login problems</li> <li>§ Niche solution (business users)</li> </ul>	<ul style="list-style-type: none"> <li>§ Expected high prices – no cost control</li> <li>§ Technology still not available (time of availability still unknown), performance not yet proven</li> <li>§ Lack of availability vis-a-vis terminal equipment</li> <li>§ Limitation due to mobility of the devices (display, input)</li> </ul>

**Table 1: Drivers and Barriers for UMTS and WLANs (source: UMTS Forum)**

Technology	WLANs	3G
<b>Network Equipment</b>	IEEE 802.11 b already deployed. Forthcoming IEEE 802.11a, 802.11 g with higher bandwidth	Rolling out of WCDMA networks in Europe and Asia has been slow down with many commercial launches delayed to 2004
<b>End User Equipment</b>	802.11 b already available	3G end-user equipment is at entry/testing level. WCDMA devices are available commercially in Japan
<b>License Cost</b>	Operator access to unlicensed WLANs	Licenses are paid through license auctions or awarded after national 'beauty contest'
<b>CAPEX</b>	3000 Euros: 42% for the WLAN AP, and 58% for the E1/DSL Lines (ASSUMPTIONS: 18 MHz spectrum, capacity 5,5 Mbps). 50-100 times less expensive than 3G	100,000 Euros: 20% equipment, 80% construction./installation (ASSUMPTIONS: 15 MHz spectrum, total capacity 4,5 Mbps, 45 users)
<b>Speed</b>	11 Mbps to 54 Mbps	384 Kbps to 2 Mbps
<b>AAA Access</b>	802.1x, RADIUS/DIAMETER	SIM/AKA, HLR/SS7

**Table 2: Comparisons between 3G and WLAN**