

PRD SE. 27



Title: Services, Ease of Use, and Operator Considerations
in Interworked WLAN-Cellular Systems

Version: 3.0.0

Date: 28th of May 2003

GSM MoU Association Classifications

Non - Binding
Non – Core

Security Classification Category*:		
Unrestricted - Industry		X

Information Category:	WLAN
------------------------------	------

Unrestricted

This document is subject to copyright protection. The GSM MoU Association (“Association”) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice. Access to and distribution of this document by the Association is made pursuant to the Regulations of the Association.

© Copyright of the GSM MoU Association 2003

Document History

Version	Date	Brief Description
2.0.0	13 th of February 2003	This document provides descriptions of various aspects of the provisioning and use of services in Interworked WLAN – Cellular Systems. This version was put forward for approval by SerG#50.
2.0.1	8 th of April 2003	The document was been reclassified as Unrestricted – Industry and is to be resubmitted for approval
3.0.0	22 nd May 2003	Approved by SerG.
Changes Since Last Version The original document had an incorrect security classification and therefore had to be changed. The document on approval will be classified as Unrestricted – Industry.		

Table of Contents

References	4
Definitions	4
1. Introduction	5
2. Scope	5
3. User, System and Service Scenarios	5
3.1 WLAN-Cellular System Scenarios	5
3.2 User Scenarios	8
3.3 Service Scenarios	8
4. User Experience Processes	9
4.1 Configuration of User Device	10
4.2 Network Detection	10
4.3 Network Selection	11
4.4 Network Login/Logoff	12
4.5 Security Information	14
4.6 Services Selection	14
4.7 Service Sign-On / Sign-Off	15
4.8 Continuity of User Experience	15
5. Use Cases & User Interface	16
5.1 Example Use Cases	16
5.2	16
5.3 Pre-pay Subscription Using A Scratch Card	16
5.4 Login/Logoff with Radius	21
5.5 Login/Logoff with EAP/SIM	25
6. Operator Considerations - Technical	27
6.1 Service Provisioning	27
6.2 Service Control	27
6.3 Charging Information	28
6.4 Authentication	28
6.5 Roaming	29
6.6 Network Agnostic Applications	29
6.7 Others	30
7. Operator Considerations - Business	30
7.1 Introduction, Scope and Concepts	30
7.2 Background	30
7.3 Mobile Operators and WLAN	31
7.4 Market	31
7.5 User's Expectations	33
7.6 Competition	33
7.7 Relationship to 3GPP Specifications	33
7.8 The Proposition	33
7.9 Business Models	35
7.10 Architecture Choices	48
7.11 Decision Tree	51

References

- [1] GSM Association PRD AA.39
- [2] 3GPP TR 22.934 v1.0.0 “Feasibility Study on 3GPP System to WLAN Interworking”
- [3] GSMA WLAN Task Force Document “Roaming Functionality for WLAN Operators”, Sami Ala-Luukko, Sonera Corp.

Definitions

AAA	Access, Authorisation and Accounting
AC	Access Controller
AP	Access Point
HPLMN	Home Public Land Mobile Network
HWLAN	Home Wireless LAN
Inter-System Handover	Handover of an active connection between systems (e.g. 3GPP to WLAN or vice versa)
Inter-System Roaming	Roaming between two systems of different type (i.e. a 3GPP use registering onto a WLAN)
Intra-System Roaming	Roaming between two systems of the same standard (i.e. WLAN to WLAN or 3GPP to 3GPP)
lu	Interconnection point between the RNS and Core Network. It is also considered as a reference point. The lu will be implemented as one or more physical interfaces.
MS	Mobile Station
MVNO	Mobile Virtual Network Operator
PLMN	Public Land Mobile Network
SLA	Service Level Agreement
(U)SIM	3GPP (Universal) Subscriber Identity Module
VPLMN	Visited Public Land Mobile Network
VWLAN	Visited Wireless LAN
WISP	Wireless Internet Service Provider

1. Introduction

This document provides descriptions of various aspects of the provisioning and use of services in Interworked WLAN – Cellular Systems. The service aspects include Network Detection, Network Selection, Logging in and out of the Network, presentation of Charging information etc. and address both the user and operator perspectives. These descriptions are expected to lead to user friendly and operator efficient implementations of Interworked WLAN-Cellular Services.

The document is organized as follows. The User and System Parameters that affect the Ease of Use are first listed and described. The Processes that are involved in the User Experience are then described. Then, a number of Use Cases are described, together with the User Interface for each of these Use Cases. The relevant Terms and Icons are identified. Then, the issue of Continuity of User Experience as the User traverses across the WLAN – Cellular Networks is described. Finally, the Operator aspects, such as Service Provisioning, Consolidated Billing are addressed, followed by Conclusions and Recommendations.

Annex A of this document examines the market, players, drivers and issues for cellular operators entering the WLAN market. The Annex also highlights the advantages and disadvantages of various architecture choices in available in integrating a WLAN system with an operator's cellular network.

2. Scope

The scope of this document is to cover the ease of use aspects of Interworked WLAN-Cellular system services from both the user and operator perspectives. This document is related to and builds on other documents generated by GSMA WLAN Task Force as well as 3GPP Technical Standards Groups. For example, the GSMA document AA.39 deals with "User Scenarios", and describes various User States (in terms of Network coverage) and User Experiences in each User State. The present document builds on the AA.39 and goes into the next level of detail in terms of User Experience, not only when the User is in a particular State, but also when the User transitions from one State to another. Similarly, 3GPP TSG SA has produced a Technical Report TR 22.934, which deals with feasibility of WLAN-3GPP Interworking. Specifically, a number of Interworking Scenarios have been defined, with each Interworking Scenario being capable of providing a set of service types. The present document relates to TR 22.934 in the sense that the services identified in this document would be mapped into one of the 3GPP Interworking Scenarios.

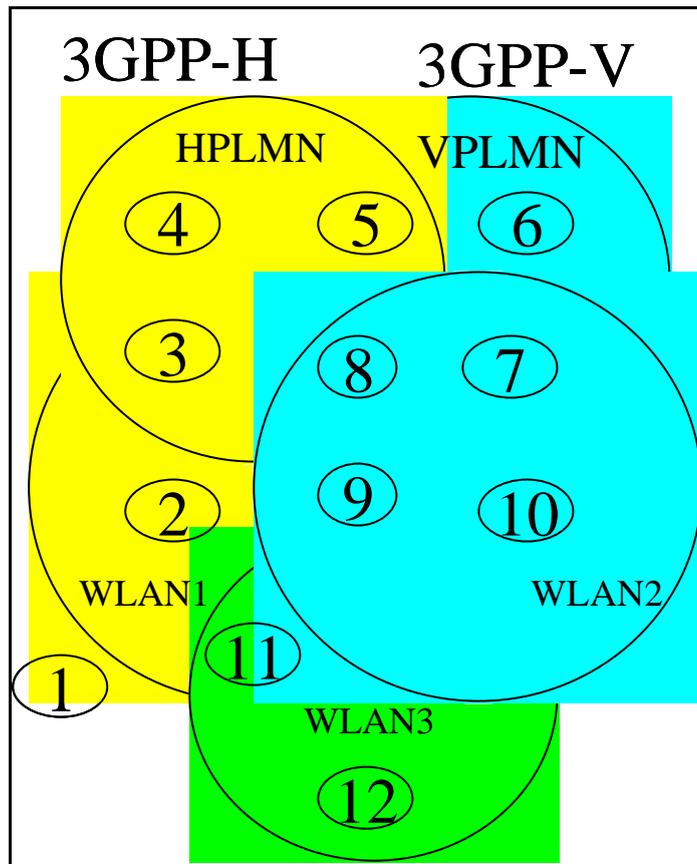
It is expected that this document would be useful for both operators and vendors in order to help create and deliver user friendly and operator efficient services in Interworked WLAN-Cellular Systems. It is also expected to provide inputs to the activities of 3GPP Technical Standards Group SA2.

3. User, System and Service Scenarios

The User Experience in a WLAN – Cellular System depends upon a number of parameters belonging to the User as well as the System. These are now described.

3.1 WLAN-Cellular System Scenarios

The following User States (in terms of the Network Coverage) are taken from PRD AA.39 [1].



Assumptions:

WLAN1 is owned by and interworked with home network 3GPP-H (HPLMN)

WLAN2 is owned by and interworked with cellular roaming partner network 3GPP-V(VPLMN). It may be preferred or non-preferred, or blocked for use by a subscriber of the home network

WLAN3 is an independent visited network, which is not owned by any cellular network, but can be interworked with one or more cellular networks; It may be preferred or non-preferred, or blocked for use by a subscriber of the home network.

State	Description	WLAN Coverage	3GPP PLMN Coverage
1	Switch on	No coverage	No coverage
2	Single network WLAN coverage	Coverage only available from WLAN1(s)	No coverage
3	Overlapping 3GPP & WLAN coverage	Single network coverage	Home network coverage
4	Single network 3GPP-H coverage (HPLMN)	No coverage	Home network coverage
5	Multiple networks 3GPP coverage	“ “	Coverage from home network and other operator(s)
6	Network(s) 3GPP-V coverage (VPLMN)	“ “	Coverage from visited network(s) only
7	Overlapping 3GPP &	Coverage only available from	Coverage from visited network

	WLAN coverage	WLAN2(s)	only
8	Multiple 3GPP & Multiple WLANs	WLAN1(s) & WLAN2(s) Note: May also include WLAN 3 (Not Illustrated)	Coverage from Home and Visited Networks
9	Multiple WLAN coverage	Coverage available from WLAN1(s) & WLAN2(s)	No coverage
10	Single WLAN network coverage	Coverage only available from WLAN2(s)	No coverage
11	Multiple WLAN coverage	Coverage available from WLAN1 & WLAN3	No coverage
12	Single independent WLAN(s) coverage	Coverage only available from WLAN3(s)	No coverage

Table 1 - Description of User States

Of the 12 coverage states, States 1, 4, 5 & 6 do not have any WLAN coverage. The remaining states, namely 2, 7 through 12, represent joint coverage by WLAN(s) and Cellular Network(s).

3.1.1. WLAN-Cellular Interworking Scenarios

The following list of interworking scenarios is taken from 3GPP TR 22.934 v1.0.0 [2] and simplified descriptions are given.

Interworking Scenario 1 - Common Billing and Customer Care

The customer receives one bill from the mobile operator for the usage of both 3GPP and WLAN access services. Integrated Customer Care allows for simplified service offering from both operator and subscriber's perspective.

Interworking Scenario 2 - 3GPP system based Access Control and Charging

Authentication, authorization and accounting are provided by the 3GPP system. The security level of these functions applied to WLAN is in line with that of the 3GPP system.

Interworking Scenario 3: Access to 3GPP system PS based services

This scenario allows the operator to grant access to some or all of the 3GPP system PS based services (e.g. IMS based services, location based services, instant messaging, presence based services, MBMS) through the WLAN access. However, there is no service continuity and there are no handovers.

Interworking Scenario 4: Service Continuity

This scenario provides some or all of the 3GPP system PS services (those provided in Scenario-3) as the user moves to WLAN via handovers. However, the quality of service may vary and there may be loss of packets during the handover.

Interworking Scenario 5: Seamless Services

This scenario provides continuity of some or all of the 3GPP system PS services (those provided in Scenario-4) in a manner minimizing aspects such as data loss and break time during the handovers.

3.2 User Scenarios

The following are examples of User Devices for Interworked WLAN-Cellular Systems.

- Laptop with WLAN device
- Laptop with WLAN device & GSM Phone
- Laptop with WLAN device including SIM card
- Laptop with combined WLAN+GPRS device (including SIM)
- PDA with WLAN device
- PDA with WLAN device incl. SIM
- Smart Phone with WLAN device

Notes:

1. WLAN devices can be either be integrated into the laptop/PDA/smart Phones or can be accessories such as PCMCIA cards or Compact Flash cards.
2. SIM card readers can be integrated into the WLAN device, or the reader can be external to the WLAN device.

Each of these devices may be based on different Operating Systems such as:

- Microsoft family (Windows 98, XP, ME, Windows 2000, Pocket PC 2000/02)
- MacOS
- Unix
- Linux
- Symbian
- Palm O/S

Some Commercial Examples:

- Laptop with WLAN card: Linksys WPC11
- Laptop with WLAN card including SIM card: Nokia C110/C111 Wireless LAN Card with SIM Services module
- PDA with WLAN modem: Palm m500 with 802.11b WLAN module from Xircom
- Combined WLAN+GPRS card (including SIM): Nokia D211 GPRS WLAN Card

3.3 Service Scenarios

3.3.1. Access/Connectivity Services

User Experience depends upon the selected Access Service, such as those listed below:

1. Local Services
 - a. Access to Local Operator Services (such as Airport/Flight/Hotel/Movie/Bill Information)
 - b. Local Access to the Public Internet
 - c. Access to Corporate Intranet services

2. Roaming Access to Home Network services
 - a. Packet Switched (PS) Services
 - (i.) Operator's WAP portal content including Location based services
 - (ii.) Access to corporate Intranet Services
 - (iii.) Remote access to the Public Internet
 - b. Interactive Multimedia Service (IMS)
 - c. Circuit Switched (CS) Services
3. Seamless Services (as the user moves from one User state to another)
 - a. Continuity of Services (with possible change of service attributes such as Data Rates)
 - b. Transparency of Services (which is Continuity of Services with no change of service attributes)
 - c. Lossless Handovers (with no loss of data as user moves across User States)

3.3.2. Data Services

1. Web Browsing
2. Email
3. FTP
4. Streaming
5. VoIP
6. Instant Messaging
7. Chat
8. SMS
9. MMS
10. IMS
11. Location Based Services
12. Broadcast services
13. Multicast services
14. Telemetry
15. IP-Video Calls

4. User Experience Processes

While the specific User Experience depends upon selected User & System Parameters, User Experience can be broken down into a number of common User Processes. These are listed below and described in this section.

- User Device Configuration
- Network Detection
- Network Selection
- Network Login
- Service Selection
- Service Sign-in
- Service Sign-out
- Network Logout

The following terms will be used in the present document. [3].

Term	Description
Roaming Service	Provision of Wireless connection service to the Internet for Customers of another company, Roaming Company. It is limited to WLAN (Wi-Fi) technology.
WLAN	Wireless Local Area Network
Roaming Agreement	Agreement between two parts to enable end users of each to utilize the other parts network using their home account service provider authentication parameters.
Roaming Company	The Company, which has entered a Roaming Alliance.
Home Network Company	Roaming Company contracting to provide the Service to its own Customers.
Visited Network Company	Roaming Company providing the Roaming service to the Customer or End-user of the Roaming Company.

4.1 Configuration of User Device

The User Equipment that is capable of WLAN and Cellular services is likely to be more sophisticated than the present day WLAN-alone or Cellular-alone User Devices. Accordingly, it is very important that the Software and Hardware configuration as well as Upgrades be as user friendly and simple as possible. The ease of use in this regard may strongly affect the user acceptance and wide spread use of the services.

4.2 Network Detection

The detection of available networks (when using WLAN) is done with the WLAN card and its driver software.

The WLAN card detects the available networks transparently to the user. The WLAN card searches the air interface and detects the available networks by reading the information from the air interface (for example, reading the SSID in 802.11b). The WLAN card detects only

available networks which are supported by the card and which passes a minimal signal requirements.

After the Networks are detected, they are either displayed to the user for manual selection or in any automatic mode they are matched to defined known networks to be recognized by the equipment for the network selection.

The network detection process continues until the user requests to connect, or until a network is selected in any automatic login mode.

One different scenario is when the user selects to connect only to one specific network, The WLAN searches only the specific network, it will not detect any other and continue until it detects and connects to specific one.

4.3 Network Selection

This section discusses the scenario where the user equipment detects several available networks, so that the user has to select one of the networks.

4.3.1. Preference settings

The following configurable global parameters:

Network selection mode – manual, automatic, semi-automatic (home, office etc.)

If network selection mode is semi-automatic then the user can either use the defaults or set the selection policy. It is possible that the equipment will propose several alternative semi-automatic policies optimizing price, quality or other parameters.

Per-network: encryption mode and encryption key where relevant, private/ office or unsupported network identification (e.g. SSID), black list of network identifiers (e.g. SSIDs).

4.3.2. Manual network selection

When the equipment is brought up, it displays a list of all available networks. Various types of information (with configurable level of details) is associated with each item in the list (e.g. network radio type, quality, supported/unsupported, cost). A connect button pops out when at least one network is available. The user selects one item from the above list, and pushes the connect button. The equipment now proceeds to the login process (unless otherwise configured). The login process is described later.

Another type of manual selection is a predefined network. The user defines a specific network to connect to. The WLAN card connects only to the specific network, without searching and displaying any other information to the user.

4.3.3. Automatic and Semi-automatic network selection

The equipment detects all available network, when the equipment detects at least one available network, it either pops a connect button, or connects automatically (depending on the login configuration). The network is chosen according to the default selection policy in the

automatic mode, or according to the user pre-configured semi-automatic mode (e.g. cost). The following list describes a few automatic network selections modes:

- Automatic: priority list ordered as: LAN interface (for services), Home private AP, Corporate AP, HPLMN WLAN, VPLMN WLAN, interworked WLAN, GPRS interface.
- Cost semi-automatic: ordered WLAN networks list according to a predefined updated cost parameter, can be cost per traffic, cost per login duration or cost per calendar day.
- Performance semi-automatic: 802.11a, 802.11b, GPRS etc, additional information can be used if exists.
- User determined predefined order list: The user defines a list of networks to be selected according to priority. A user can define several lists such as Home, Corporate etc.
- Additional category can be Free networks: Any Access Point, which connects to the internet without needing to identify and login.

4.4 Network Login/Logoff

After the network selection is completed, the login process begins. When the login process completes successfully, a configurable connect indicator is displayed. Information in the indicator can include connected network identification, radio interface number, connected link, speed, connected time, traffic send, traffic received, etc.

In case the selected network is a Free network, The equipment connects to the internet automatically and notify the user whether to login to the cellular network server (for services etc).

4.4.1. Preference setting

Login – automatic or manual (orthogonal to automatic or manual network selection).

If automatic login is selected, then the user should configure whether the login process starts automatically once a network is selected, or user triggered.

Supported login schemes (EAP, etc) – could be automatically set, but also manually.

4.4.2. Manual login

The login process is completely manual. The process begins after a network is selected, and the user pushes the connect button. The user then must enter his user name and password. The login process depends on the authentication method, which may be

- Radius based
- EAP/SIM based
- Certificate based

The Radius based Authentication method may be Browser based or Specific Client Software based. Some example procedures with some of these methods are included in a later section on Use Cases.

4.4.3. Automatic login

When the user selects the automatic login process, the process is completely user-transparent (except maybe the initial push of the connect button). After a network is selected, the user presses the connect button (configurable), and the equipment logs in to the selected network. If login fails, the equipment moves on to try and login to the next network (this time there is no need to push the connect button). When the login succeeds, the connected network information is displayed.

The automatic login user experience is the same for Radius and EAP/SIM authentication procedures; the equipment automatically inserts and sends the username/ID and password if needed.

A temporary user ID can be used transparently to the user, the equipment login using the current temporary ID, then receives the next temporary ID, which will be used for the next login process.

4.4.4. Manual Logoff

After the login process is complete successfully, a logoff button pops-out (this could be either a customize logoff button, in scenarios where the equipment intercepts the logoff screen, and replaces it with a unified looking screen – usually in the automatic login, or the original hotspot logoff screen).

Pushing the logoff button gives the user an acknowledgment, and turns off the connect indication. Pressing the logoff button doesn't turn background processes in the equipment, such as network detection. A scenario where the equipment logs in automatically (without displaying the pop-up connect button) might create a loop. Equipments must always display the pop-up connect button after the logoff button is pushed.

4.4.5. Automatic logoff

Automatic logoff happens when the equipment detects an inactivity timeout on the radio interface (the timeout is configurable). Shutting down the equipment also triggers automatic logoff.

4.4.6. Network & Service Access Control

The User Experience is directly affected by the type and method of Access Control provided by the Network as well as User Device. These aspects are now detailed.

- Network Authentication

Network Authentication is the process whereby the user device (Laptop or PDA) determines that it is connected to the intended network. This authentication is critical in cases where a “man in the middle” cryptographic attack could occur. Network authentication can be achieved by several techniques but most commonly via SSL using X400 certificates signed by a trusted root authority.

The Network Authentication management process is provided by the carrier and includes maintaining a database of key Network elements including SSID, network X400 certificates, network security keys (if required) preferred network lists and barred network lists. Some of the customer's WLANs may be outside of the carrier's range of influence (a home or SOHO network for example) but nonetheless are part of the customer's experience and should be smoothly integrated therein.

- User Authentication

User Authentication is the process whereby the Customer is authenticated to the carrier. If the WLAN network is owned/operated by the carrier, then Network Authentication could be synonymous with User Authentication. However, they may be

different in a roaming environment. Many approaches to user authentication have been identified of which a few are discussed below.

- Username/Password based – A UserName/Password is sent by the user to a AAA server where it is checked against a database containing authorized subscribers. Typically the Username and Password are sent via SSL or some other secure tunnel to protect against unauthorized use. One time passwords developed from tokens, etc add an additional level of protection.
- SIM Based – SIM based authentication uses the cellular SIM, attached to the Laptop or PDA. The SIM is challenged with a RAND and is authenticated if and only if the proper response value is returned. There are several variations to this approach including not actually having the SIM on the Laptop or PDA but using a SIM equipped mobile phone to certify the legitimacy of the subscriber.
- Certificate Based – Certificate based authentication is where the user has an X400 based certificate installed on the Laptop or PDA. The technique used is the same as the one that the client uses to authenticate the network, except it is the server that is authenticating the client. A key disadvantage of this approach is one of scale. It is very complex to manage unique signed keys on every client.

- Service Authorization

Service Authorization is the process of managing the privileges for the subscribers. Based on rate plan, user groups, etc, each subscriber (or class of subscribers) may have different available services. This management function enables these various functions at for each subscriber.

4.5 Security Information

The User Experience is governed by the indication the User has regarding the type and level of security associated with the Network, Radio Link etc. This information will facilitate the user in making informed choices regarding the security of the application he/she is about to launch.

4.6 Services Selection

A list of the available services per subscriber is defined in the HLR or possibly in a different provisioned DB. The list is a part of the user profile. The list may also be stored in the User Device.

The Network may also wish to offer services that the user is not currently a subscriber of. In such a case, it may be possible for the User to subscribe to such services after login.

After User login, the list of user's available services as well as any additional services that the network may wish to offer to the user appear on the User Device's display, either as icons or as a list. This list may be generated by procedures involving the User Device and the Network Data Base. The procedure may also take into account the limitations and scope of the interconnecting network as well as User Device capabilities.

Remark: Some services might be accessed directly through the Internet with no specific access control and with no provisioning through the Cellular WLAN server other than manual login to the application, these services list will not be sent to the equipment to be displayed automatically, it can be done in other ways.

4.7 Service Sign-On / Sign-Off

Services, which are provisioned for WLAN users and are controlled by the network, can be sign-on and off by simply clicking the Icon on the equipment. The access control is done by the network.

Services which are controlled by username/password to the application itself, and are provisioned directly to the application DB with no connection to the WLAN system, are accessed directly by the user by clicking an Icon with the URL or using a shortcut, following by entering the username/password as requested by the application/service.

4.8 Continuity of User Experience

The User Experience in an Interworked WLAN-Cellular System depends not only on the User Experience in a WLAN Hot Spot and Cellular Wide Area Network, but also on the User Experience as the user traverses between the WLAN hot spot and the Cellular WAN. For example, the User Experience across these two Networks is affected by the Radio Link Characteristics, such as Data Rates, Quality of Service, Mobility, Security and Billing. It is also affected by the continuity of availability of services across the two networks. In addition, the User Experience across the two networks is also affected by the User Device Form factors for which a particular service may have been optimized.

As such, it is convenient and perhaps necessary to address all these factors under a concept, that may be termed as 'Continuity of User Experience'. At a high level, Continuity of User Experience may be seen as a generalized Quality of Service across multiple networks, multiple user devices and multiple service environments as well as multiple network hierarchies. It brings together all the technical issues encountered in producing an acceptable and enjoyable user experience in an Interworked WLAN-Cellular System.

4.8.1. WLAN to WLAN Transition

The user experience during WLAN to WLAN transition is configurable to either be transparent or needs a user approval.

In case of user approval, when the equipment decides it needs to move to a different WLAN, it pops up an approval button asking the user to approve the transition. After the approval the equipment login to the other WLAN according to the login process described above. If the login is configured for automatic, it is transparent to the user.

In case a transparent is configured, the whole process is transparent to the user other than the fact that the name of the connected network changes on the Icon.

Note that the equipment physical IP address changes during the transition. The user experience in terms of applications running depends on the Interworking scenarios as explained in Section 3.1.1.

5. Use Cases & User Interface

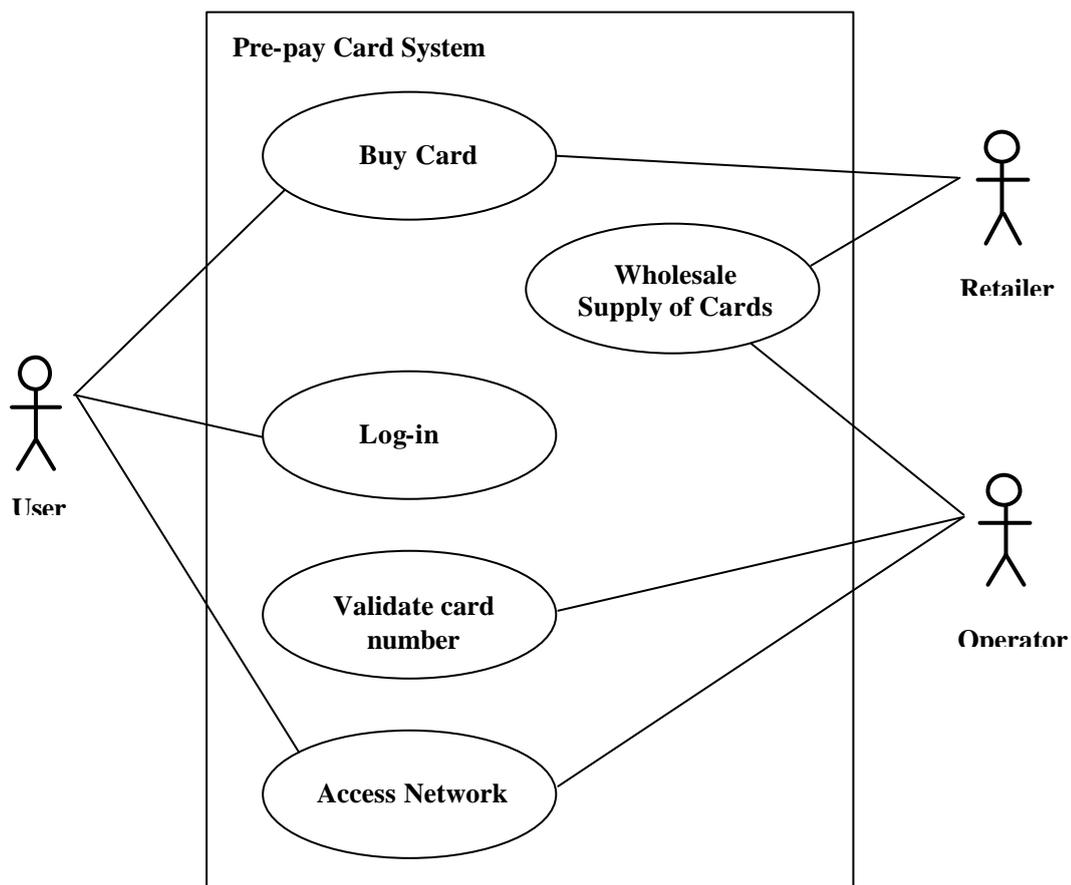
5.1 Example Use Cases

- Pre-pay Subscription using a Scratch card
- Login/Logoff with Radius
- Login/Logoff with EAP/SIM
- Web Browsing
- Corporate Intranet access
- Home WAP service
- SMS

5.2

5.3 Pre-pay Subscription Using A Scratch Card

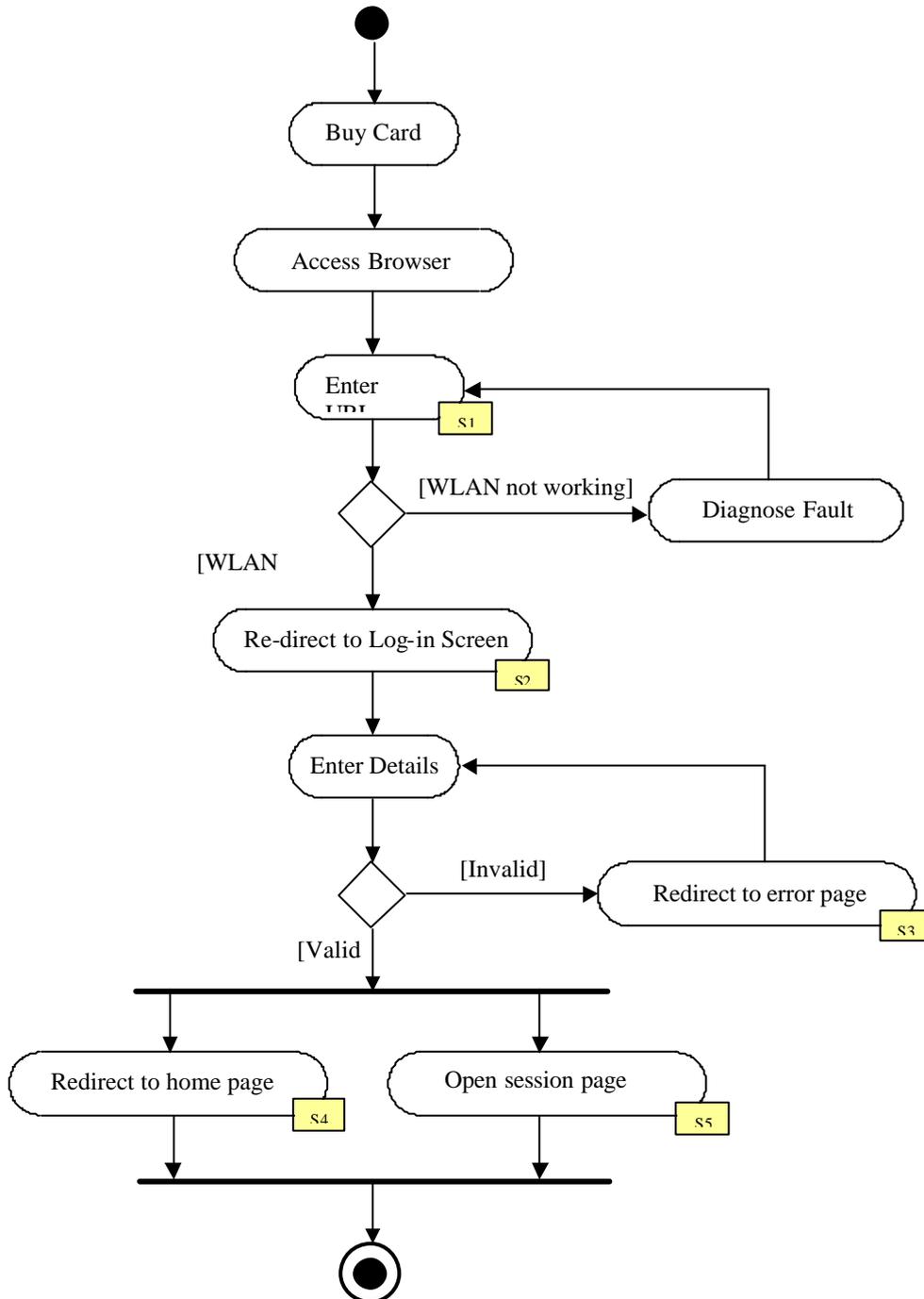
5.3.1. UML Use Case Diagram



Use Case Name:	Pre-pay Subscription Using A Scratch Card
Ref:	UC1
Version:	1.0

Last Modified:	21JUN02
Activity Diagram related to:	A1

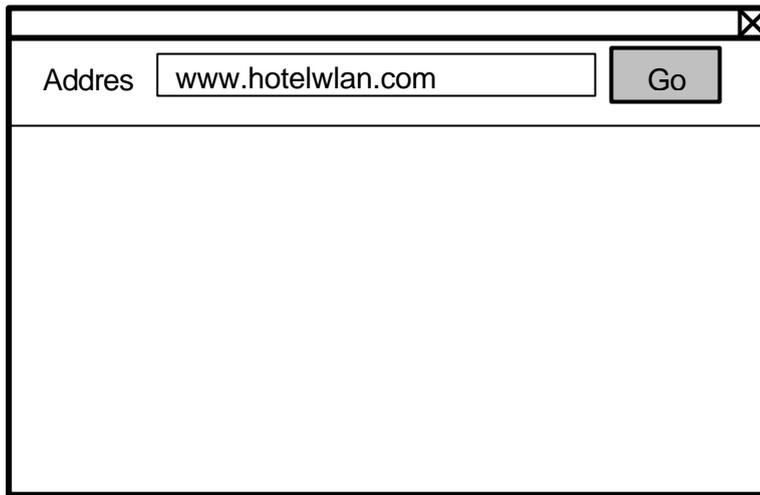
5.3.2. UML Activity Diagram



Activity Diagram:	Pre-pay Subscription Using A Scratch Card
Ref:	A 1
Version:	1.0

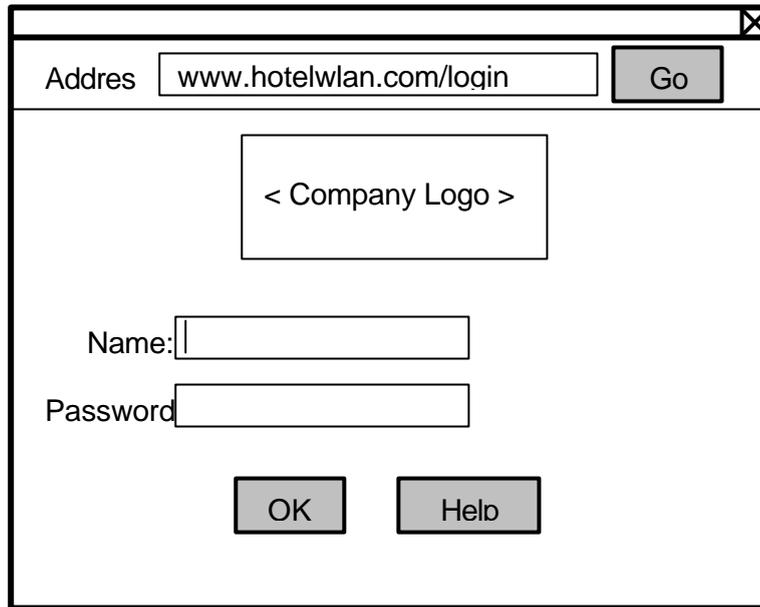
Last Modified:	21JUN02
Use case related to:	A1

Relevant Screen Shots



Screen Name:	Standard web browser	
Ref:		
Version:		
Last Modified:		
Activity Diagram used in:		
Control	Text/Graphic	Action
URL input field	Defined by browser	Input URL
Initiate button	Defined by browser	Initiate browser look-up of URL

Login Page



Screen Name:	Login page	
Ref:	S2	
Version:	1.0	
Last Modified:	21JUN02	
Activity Diagram used in:	A1	
Control	Text/Graphic	Action
Name input field	Name:	Entry on text for user name
Password input field	Password:	Entry on text for user password
OK button	OK	Initiates validation of user details
Help button	Help	Launches to separate help window screen ref: 7

5.3.3. Relevant Terms & Icons

Terminology

The following is an example of what would be in a spreadsheet or database

Term	Description	Control(s)	Alias(s)	Used in
Log-in	Log in to WLAN	Title	Login, Logon	S1
OK	Initiates action(s)	Button	Start, Do, Ok, Okay	Most
Help	Initiates help screen	Button, Title	Uh?	Most
Name	User or account name	Label		S1
Password	User's or account's password	Label	Passcode	S1
...				

Graphics

Graphic	Description	Control(s)	Alias(s)	Used in
	Save icon	Button		S87
	Print icon	Button		S78

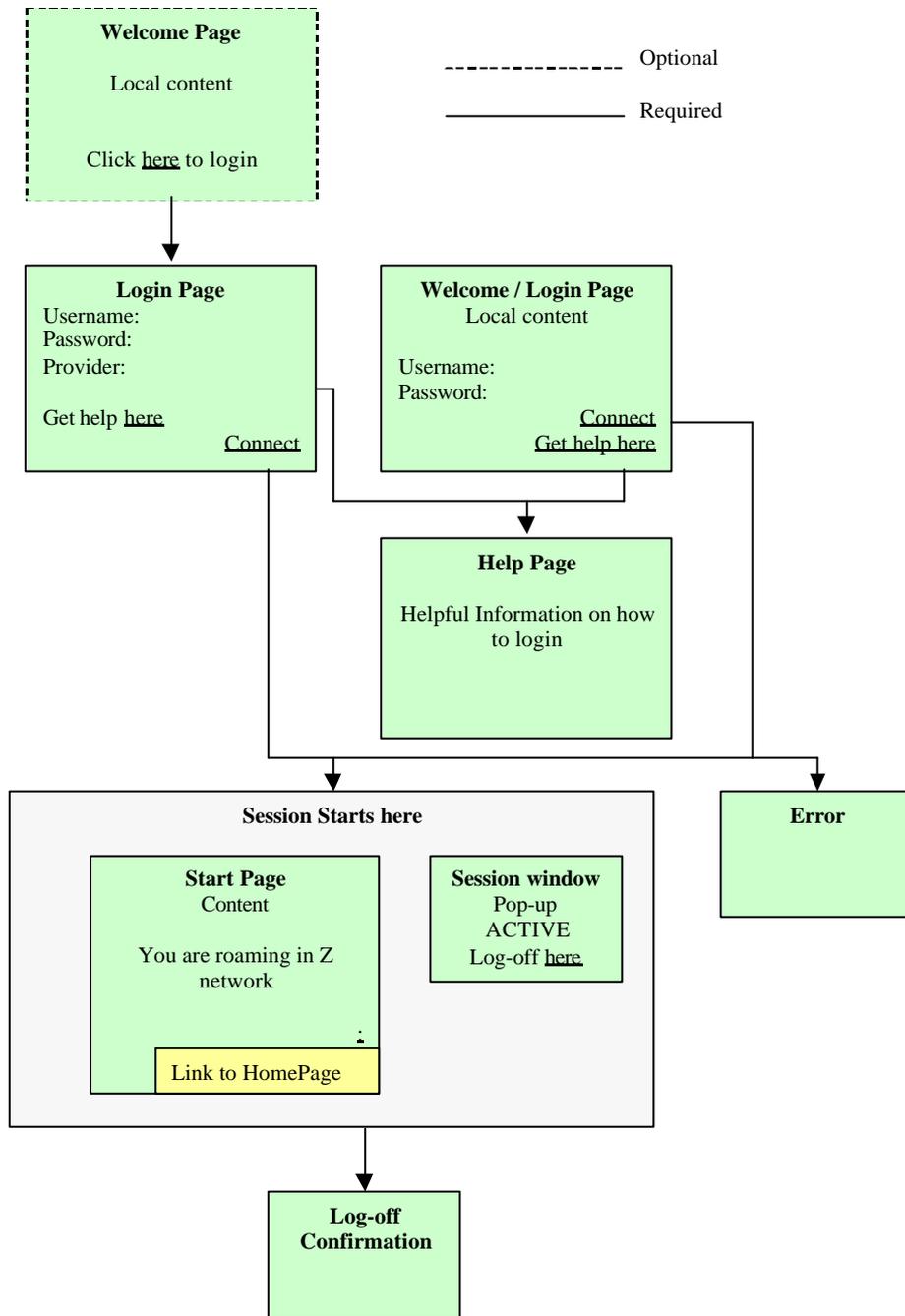
5.4 Login/Logoff with Radius

Given below is an example procedure, which illustrates the various steps involved in a typical Login/Logoff process [3]. Other variations are possible. For example, the login process may be based on a Web browser or on a specific client software for Interworked WLAN-Cellular operation. The following example assumes browser based login/logoff process.

1. Customer opens the WEB browser and communicates via access equipment installed at the location with server controlling the visited network.
2. The visited network sends a Login page to the customer
3. Customer logs in to visited network by inserting username, password and provider to the Login page.
4. The username shall be entered in format username@realm or the login page adds @ sign and the provider to the end of the username (In case of the drop down box).
5. Visited network will recognize the realm and will proxy the request to Roaming Partner. Local validation is ignored and authentication request is routed to home network authentication server.
6. The home network receives the authentication request and authenticates the user.
7. Home network sends an authentication response to the visited network Radius server.
8. If the authentication in home network was successful, the visited network enables customer session.
9. Customer receives a login acknowledge.

10. Visited network starts session statistics recording and sends Radius Accounting Start message to the home network.

5.4.1. UML Activity Diagram



Welcome Page

The user might be directed to a Welcome page provided by the visited Network. The Welcome Page is the first page that is presented to the user during URL redirection. Welcome page is optional and may contain local content, branding, and link to the logon page.

Login Page

The user shall login at the Login page provided by the visited network by automatic re-direct.

Following fields are required to the each operator roaming login page:

- **User ID.** Username is the same as in the home network. The length is max 32 characters including the realm. At least characters @, #, *, %, \$ are not allowed in the User ID field. The character “ ” is not allowed in the username but is used in the suffix. (@ shall not be part of the user ID but possible to enter in the user ID field as specified below).
- **Provider.** As a maximum, the user shall enter a suffix to the username indicating Home Network using [user@realm](#). It is recommended that the realm represent the domain.
- **Password** is the same as in the home network. The length is max 32 characters. (note: To secure password SSL is required.)
- **Connect** button is required. To be connected user has to press connect button.
- It is recommended that one of the two following alternatives shall be available for choice of provider:
- Alternative 1:
The user selects provider by provided drop-down list. Provider identifies whose customer the user is.
Technically HTML/Login page adds @realm after the username.
- Alternative 2:
The user adds the @ sign and realm after username to the username field.

Each Network Provider decides which alternative to be chosen.

Welcome / Login Page

The Login Page and the Welcome Page may be the same page.

Help Page

Help-page shall be available for the end user provided by the visited network Company. The help page content shall at least include:

- login procedure for roaming environment
- logoff procedure

Start Page

The V-WLAN shall support the Start Page functionality. Upon successful authentication of a roaming customer, the V-WLAN **shall** redirect the customer to the Start Page.

The two following alternatives are recommended:

- Alternative 1:
Redirect the roaming customer to the HWLAN Start-page. This can be implemented by informing the Roaming Partner on URL to be used for respective roaming profile or Exchange URLs for start-page via Radius.
- Alternative 2:
Redirect the roaming customer to the V-WLAN Start-page.
Link to the H-WLAN Start-page shall be available.

Each WLAN Operator decides which alternative to be chosen.

Error Window

If login fails an Error message Window shall appear. The Error message is required and delivered by the visited network.

Log-off

After successful login a Session Window with connection status and log-off are required to be provided by the visited Network. The log-off function shall preferably be provided through a popup window that allows the End User to click a log-off button. The window shall be a known URL for the user and difficult to close.

Both implicit and explicit log-off capabilities are required to be provided by the visited network. Session must end even though the End User does not explicitly log-off. Absence time-out should be set at maximum 5 minutes.

Log-off Confirmation

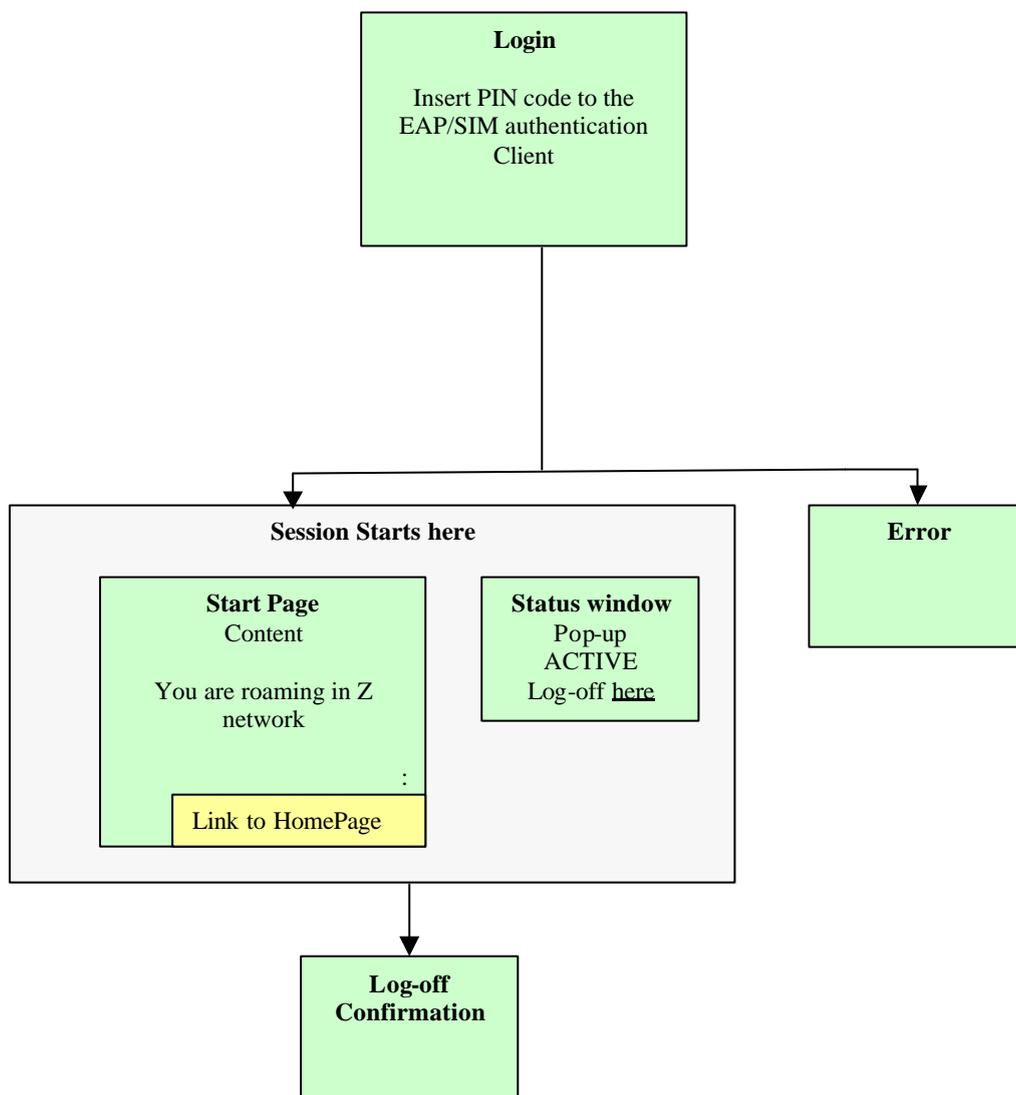
Log-off confirmation page shall preferably be shown after successful log-off. The Log-off Confirmation Page is for explicit log-offs and delivered by the visited network. The page is intended to provide confirmation to the customer that they have been logged off and shall contain session statistics in regards to the user's closed session.

5.5 Login/Logoff with EAP/SIM

This sequence gives only an overview to login because the EAP/SIM standardisation is not yet finalised. (See EAP/GSMSIM [IETF: draft-haverinen-pppext-eap-sim]), the actual process includes mutual authentication not described here [3].

1. Customer opens a client and selects EAP/SIM authentication.
2. User inserts the PIN code to the client (can be configured to insert it only once per equipment used).
3. IMSI or temporary ID is sent over the air interface to the AP (access point) and AP sends it to the AC (Access Controller).
4. AC realises that SIM authentication is required and sends authentication request to the AS (Authentication server).
5. AS receives IMSI from AC (or retrieved IMSI from the temporary D) and sends MAP SendAuthenticationInfoArg to the SS7 network (AS has a SS7 interface). This message includes IMSI as a parameter.
6. This message is routed to the correct HLR in the SS7 network.
7. HLR responses with the MAP SendAuthenticationInfoRes to the AS. (Rand, Sres and Kc).
8. AS sends Rand with the Radius protocol to the AC.
9. AC sends Rand to the terminal and SIM card
10. SIM card calculates the Sres from the Rand using Ki.
11. Calculated Sres is sent to the AC.
12. AC sends Sres to the AS.
13. AS compares the HLR sent Sres to the Sres calculated in the SIM card, if these match AS continues according to the following paragraphs, if does not match access is denied.
14. AS sends MAP UpdateLocationArg to the HLR.
15. HLR sends MAP InsertSubscriberDataArg to the AS. This includes the user's service profile.
16. AS responses to the HLR with the MAP InsertSubscriberDataRes
17. HLR responses with the MAP UpdateLocationRes
18. AS verifies the user's service profile received from the HLR includes WLAN service activated, AS sends Radius Access-Accept or Access-Reject message to the AC.
19. If the authentication was successful, visited network enables customer session.

5.5.1. UML Activity Diagram



Login Page

SIM based solution does not have Login page. PIN code is inserted to the EAP/SIM authentication Client.

PIN code insertion can be configured for MUST insert PIN each login process, each time the SIM is inserted or once per equipment used.

Welcome Page

In EAP/SIM based roaming there is no Welcome page

Help Page

The Help page like in the Radius roaming cannot exist. However Help page features may be part of the Start page.

Start Page

The V-WLAN shall support the Start Page functionality. Upon successful authentication of a roaming customer, the V-WLAN shall redirect the customer to the Start Page.

The two following alternatives are recommended:

- Alternative 1:
Redirect the roaming customer to the H-WLAN Start-page. This can be implemented by informing the Roaming Partner on URL to be used for respective roaming profile.
- Alternative 2:
Redirect the roaming customer to the V-WLAN Start-page.
Link to the H-WLAN Start-page shall be available.

Each WLAN Operator decides which alternative to be chosen.

Start Page may include link to the Help page

Status Window

The EAP/SIM client can provide status window or the visited network can provide it.

Error Window

If login fails an Error message Window shall appear. The Error message is required and delivered by the visited network.

Log-off

After successful login an EAP/SIM Client has to include session information with connection status and log-off button.

Explicit log-off capability is required to be provided by the EAP/SIM Client. Visited Network is responsible for the ending of the Session in case that the End User does not explicitly log-off. Absence time-out should be set at maximum 5 minutes.

Log-off Confirmation

Log-off confirmation is shown after successful log-off. The Log-off Confirmation is presented by the EAP/SIM Client and it is for explicit log-offs. It is intended to provide confirmation to the customer that they have been logged off and it shall contain session statistics in regards to the user's closed session.

6. Operator Considerations - Technical

6.1 Service Provisioning

The service provisioning is done in the HLR as any other user's service provisioning. A specific service is defines as WLAN service. Optionally other connected user services can be defined using the user profile in the HLR, services such as Location Based Services etc.

6.2 Service Control

Service control can be done in two main ways:

- Traffic service control - The traffic from the equipment is controlled by the network.
- Application control - the application/service controls the usage by the user entering a username/password when accessing the service.

6.3 Charging Information

Billing and Charging management is the process of integrating the WLAN billing functions into the overall customer billing systems. The user experience on WLAN is substantially different than on current GSM data networks, and consequently the billing may be different.

Specifically, billing can be based on amount of data transported, QoS, duration of connection, type of data transferred or a combination of any or all of these. The carrier's Billing and Charging system will convert the session metrics into an appropriate CDR that will be integrated into the carriers network. This must be done in a manner that is understandable to the customer to avoid billing surprises. Integration with prepaid billing must also be accommodated including a mechanism for presenting billing information to the customer.

Charging information could include:

- Local timestamp of login – Time stamp of the Laptop/device
- Duration – Time duration from login to current time/logout time.
- Logout reason – such as: normal specific logout, no activity timeout, network disconnection, handover to a different network/interface etc.
- Total Traffic sent/received – Total number of bytes sent/received from the device since it logged in.
- Traffic sent/received for equipment management – Traffic sent/received for system usage such as keep alives, billing information etc. This traffic might not be charged.
- Interface Type – which interface is being used, such as: WLAN, GPRS, LAN (Ethernet), dialup modem etc.
- Network ID – identifies the connected network.
- Location information – such as AP MAC address used for location translation etc.
- Free Access – identifies whether the connection is free, for example home WLAN network, corporate AP etc, can include whether a login process was needed.
- Temporary user name used for login,
- Constant username/IMSI – if known.
- Charging Record ID.
- Network services activation/use
- Prepaid information.

6.4 Authentication

The issue of authentication is addressed partly in terms of architecture as described in section 7.10.

There are two basic ways of authenticating the user:

- SIM based and
- non-SIM based.

SIM based authentication and service authorization with the HLR: - there are a number of proprietary proposals to do this. SIM based authentication methods build on the existing authentication methods of the operators and typically require small software changes to the HLR. Additionally each user will need to acquire either a WLAN card that has a SIM card reader or an alternative SIM card reader to attach to the PC.

Non-SIM based authentication techniques fall into three categories:

- username/password,

- one time password systems (which are really variants of username/password) and
- digital certificates.

One time passwords adopt the same authentication method as username and password except the password is generated on login request for the specific user and then sent, typically, to the mobile phone.

Since username/password systems are essentially the same as used by ISPs for dial-up these are easy to adopt but will require additional investment.

Digital certificate authentication does not seem to be very popular because of the additional support activity required in operating such a mechanism.

Non-SIM based authentication techniques require a new database to manage users (i.e. in addition to the HLR).

6.5 Roaming

Given that a significant segment of mobile phone users roam, there is a significant interesting in supporting roaming. This is true both for GSM operators and WISPs.

WISPs are working with WECA on a model called WISPr (WISP roaming) to support roaming WLAN users. This is based on exchange of data between RADIUS servers, it also includes the possibility of an intermediary to act as a clearing house.

GSM operators already have efficient and successful roaming support both in terms of technical solutions and roaming agreements that has been operational for many years. Clearly this is advantageous for GSM operators and operators should seek to capitalise on this capability and experience.

GSM to non-GSM roaming, however, proves to be a complex issue with respect to authentication and settlement, since the authentication mechanisms adopted by WISPs are typically username/password which would require interworking between GSM mechanisms and Internet mechanisms. Additionally WISPs will tend to use the AAA which will require some effort to integrate with GSM TAP procedures.

Operators may still have a competitive advantage in this area because the operators have pre-existing roaming agreements and arrangements and it is probably easier and quicker to negotiate and integrate than to build from scratch

6.6 Network Agnostic Applications

Whilst the different levels of coupling and authentication are discussed above there are a great many more issues to do with mobility and seamless service presentation whilst reselecting access network type.

The basic requirements for Mobility range from :-

- Automated attachment to "best" or "preferred" network according to a preset configuration
- Total access solution where the user is unaware of what network they use, and when different network types are reselected even whilst in the middle of data communications.

At this stage it is clear that item (1) Automated attachment is sought and that a total access solution is not.

6.7 Others

A number of other considerations are of importance to operators and warrant further investigation. They include Service Logging, Consolidated Billing, Control of Unauthorized Access and Fraudulent Users, Software Updates for User Equipments and Customer Care.

7. Operator Considerations - Business

7.1 Introduction, Scope and Concepts

This section examines the market, players, drivers and issues for cellular operators entering the WLAN market. The annex also highlights the advantages and disadvantages of various architecture choices in available in integrating a WLAN system with an operator's cellular network.

7.2 Background

The rapidly evolving IT world has seen the following basic trends:

- Share of laptops is growing as people move from desktops to laptops. More and more consumers are buying a laptop in preference to a desktop due to convenience and space.
- More and more networking is required from applications but the access mechanism is moving from wired connections to wireless. This has been enabled through the introduction of 802.11b equipment.
- Email is seen by many as essential and access to it globally is increasingly important (cf. the growth of Hotmail and Yahoo Mail services for example).
- The world of networking (of any variety) is rapidly converging on the Internet Protocol as its choice. This is due to the reduced costs, ease of interconnection, flexibility of the network and the vast skill base.

However, the shift to higher revenue generating data services for mobile Operators has not been easy.

- Broadband access from the mobile has been promised for a long time, GPRS has failed to deliver it, and 3G is not ready yet.
- The development of compelling applications for use on a mobile phone has been slow due to the very different requirements to traditional IT platforms.
- Mobile Operators' desire to increase ARPU from data services is still there but, with the exception of SMS, has not yet been realised to any large degree.

7.2.1. WLAN-Cellular Environments [1]

There are a number of different possible operating environments where interworking of the 3GPP and the WLAN systems may be desired. The 3GPP Wide Area Network operates universally in Public, Corporate, or Residential environments. WLANs may also be deployed in any of these environments. The environments and some of their characteristics may be summarized as follows:

The "Public" environment includes all areas where there is unrestricted public presence, including outdoor areas, streets, transportation centers, retail stores, hotels, restaurants and public spaces and lobbies in major civic buildings. Here, for example, the WLAN operator is expecting general access and will likely have a set of system policies and equipment suitable for 3GPP – WLAN interworking.

The “Corporate” environment includes offices and factories where the users are restricted to employees of the business. Restricted visitor access may also be accommodated in this environment. The Corporate WLAN operator is providing service primarily for internal uses, and access to other networks may be screened (i.e. with a “firewall”). There may be several WLANs deployed within the corporation, not all of which need to be interworked with 3GPP. Thus, interworking between Corporate WLAN and 3GPP may involve some different policies and techniques than for other environments.

The “Residential” environment includes individual homes and apartments where the users are restricted to the residents and their guests. Here, the WLAN owner and user are most likely the same. However, in a multi-tenant building, there may be a single WLAN (i.e. owned by the landlord) serving many users. The interworking of residential WLAN with 3GPP may involve some different policies than for other environments.

7.3 Mobile Operators and WLAN

Why should mobile operators be considering launching public WLAN networks?

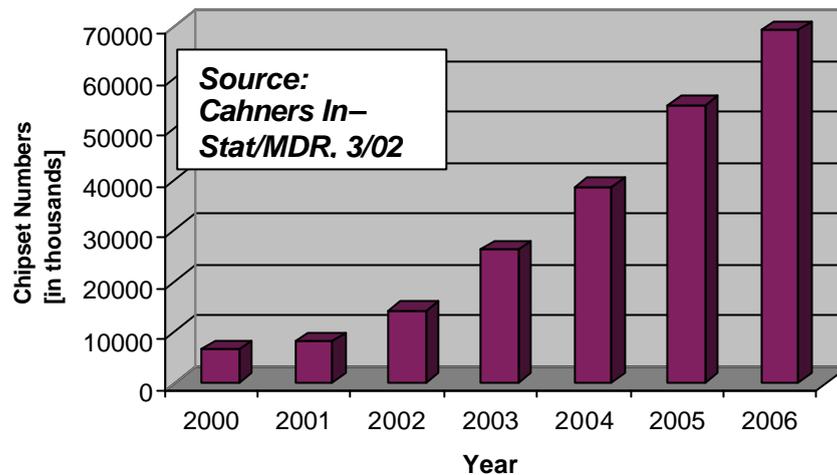
Mobile Operators are already expert in wireless network deployment, operation and management. WLAN is a wireless network deployment opportunity. While WLAN is fundamentally a lot less complex than GSM, a well designed, scalable network shares many of the requirements of a GSM deployment. There are few organisations in the world better placed to do it well than mobile operators.

- Mobile operators have a large existing customer base which they can profile to locate good candidates to offer a WLAN service too (simply looking at the movement of individual subscribers will be a good indication of business users, as will revenue).
- Mobile Operators have a well-known brand. This will be a key factor in the deployment of WLANs because those Operators are seen as trustworthy in the eyes of end consumers.
- A well designed WLAN network is not inexpensive. However, it is cheaper to deploy than a 2.5G/3G network and mobile Operators have the resources to invest in this technology. As discussed above, the skills to design and implement a WLAN network are readily available to mobile Operators, as the process is very similar to building and operating a mobile network.
- Mobile Operators already have very sophisticated and comprehensive billing and customer care systems. These are significant investments that start-up WISPs will simply not have. This allows mobile Operators to immediately offer a "value added" service.

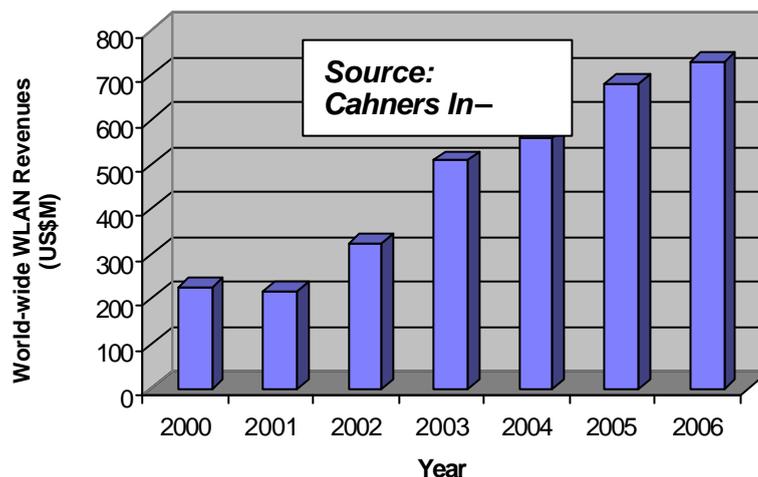
7.4 Market

The volume – and hence value – of the public WLAN market will be driven by factors such as: the number of WLAN-enabled locations, the number of WLAN-enabled devices and the traffic patterns of public WLAN users. The prospects for WLAN opportunities, World-wide, in Europe and the US are highlighted in the following statistics and forecasts.

The following graph shows that in 2000, when 802.11b chipsets became fully available, more than 6 million WLAN chipsets were sold. An increase, to over 69 million in 2006, is forecast.



World-wide chipset revenues have dropped by 4% from a World-wide total of over \$226.4 million in 2000, to \$216.9 million in 2001. This is attributed to the resulting erosion of chipset prices, however the forecast is for continuing growth in revenues to \$703.2 million in 2006.



Recent studies of WLAN activity in regional markets (i.e. Europe and the US) also point to rapid growth in the sector:

- The number of World-wide WLAN hot spots at the end of 2001 was 6,300. Hot spots could reach 114,200 by 2006, with 17 million users generating revenues in the region of \$7.3 billion. By 2006, over 20 million people in Europe will use public WLAN services in 90,000 hot spot locations
- There will be around 75 million WLAN-enabled devices in Europe by 2006, the current number of devices in Europe is 1 million. Whilst in the US, network interface cards that support WLAN access will reach 18 million by 2004. Revenues for the US WLAN market will reach almost \$2 billion in 2004.

(Sources: BWCS, "Wireless LANs and the threat to Mobile Revenues".
 Analysys Research, "Public WLAN services could equal 7% of 2.5G/3G data revenue in 2006", 2001.
 The Phillips Group, "Wireless LANs: US market demand and opportunity assessment", 2000).

The key market for WLAN hotspot access currently is the business traveller. This may change but for the moment:

- 93% of business users have said that they would be interested or very interested in using WLAN in airports.
- 61% of business users would rather use WLAN in hotels, airports and restaurants than 3G everywhere.
- If a WLAN was available at airports effective working time would increase from 19 minutes to 30 minutes.

(Source: BWCS, Study among business travellers at Heathrow Airport, May 2001).

Of the current uses of the WLAN, the biggest was email following by applications and Internet

(Source: Cahners In-Stat Group, June 2000).

7.5 User's Expectations

Users (Consumers) are looking for the following qualities in wireless networking technologies:

- Adequate speed for smooth working
- Easy to use
- Automatic connection for wherever they are i.e. a high degree of mobility in terms of widespread coverage is not relevant to a user if they spend most of their time in a hotel, airport etc.)
- Reliable, good quality service
- Secure access to corporate intranets and email
- Value for money
- A single bill for service.

7.6 Competition

WISPs are starting up rapidly all around the world with more and more regulators opening up the 2.4GHz band for public WLAN operations. The key issue for Operators is that this market can have the following impact on their business:

- Take valuable short term revenue away from mobile.
- Devalue the 2.5G/3G value proposition for pure data access.
- Allow value added services to be developed which are not available to be offered by mobile Operators.

7.7 Relationship to 3GPP Specifications

Current work in 3GPP SA1 is developing a Stage 1 description that this work should feed into Ref 3GPP TS 22.934 - Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking (setting out requirements).

7.8 The Proposition

WLAN technologies are being rapidly implemented by vendors for mass-market utilisation. The most prevalent technology being IEEE 802.11b offering user data rates in excess of 5Mbit/s over a cell radius of up to 100m. Implementation in PC cards costing less than \$50 and access point devices of less than \$100 are common. Operation network equipment can be bought from as little as \$800 and yet offers operational network qualities for management and reliability. Many terminal manufacturers are integrating IEEE 802.11b technology into their products at no apparent extra costs. This makes WLAN a key enabler for early mobile

data deployment and this annex discusses many of the options around the WLAN business opportunity.

WLAN entry offers a powerful tactical solution in the Operator’s service portfolio, in that it:

- Provides a valuable stepping-stone for revenue generation, in advance of delivering full 3G services.
- With the voice market approaching saturation, the WLAN usage model provides a mechanism for revenue creation from data services.
- The market forecasts indicate that opportunities for early return of investment will potentially come from initially acquiring ‘niche’ location hot spots, for example airports.
- From a strategic perspective, integration of the WLAN infrastructure with the cellular infrastructure will maximise the customer touch points and hence cross- and up- sell opportunities.

7.8.1. The Potential Threat to 2.5G/3G Services

For the Mobile Operator, there is potential disruption to 2.5G/3G services from WLAN. The public WLAN market offers significant opportunities for a variety of new entrants encouraged by low capital costs that reduce the initial risks and provide profitable return within 4 to 5 years of entry. WLANs will enable MVNOs, Mobile Operators, Fixed Line Operators, middleware vendors (e.g. IBM) and other sector entrants to operate without 3G licences. In addition, WLAN services potentially cannibalising an Operator’s 3G services may be an issue. Careful definition of services must be made so as to minimise this disruption as 2.5G/3G service offer ubiquitous coverage where as WLAN is hotspot based. Until laptops are always on they will be operated in a static mode where hot-spot deployment will be appropriate – when they are always on then 2.5G/3G will enable constant synchronisation and “instant” access across an operators coverage footprint.

However, rather than being viewed as a threat, WLAN services can be viewed as a potentially huge opportunity by Operators to add to their services portfolios. High–end data service users (typically Corporate Consumers) will want the speed offered by WLAN, but the mobility provided by 3G. The Operator offering both 3G and WLAN infrastructure and services is ideally placed to fulfil Consumer needs, without initially needing to resort to commercial agreements and revenue sharing models to offer interoperability. However, this position will change, as it becomes necessary to provide wider interoperability. The Operator will also be better able to preserve Quality of Service by owning the hand over control between the two network infrastructures.

Overall WLAN appears a very interesting proposition but the service proposition requires very careful thought to avoid confusing the customer and in order to yield the best continued service across all access technologies operated.

7.8.2. Summary: Rationale for Offering Public WLAN Access

From a Mobile Operator’s perspective, there are a number of key benefits in providing a Public WLAN service. These benefits are summarised below.

<p>Operator is well–placed to exploit market</p> <ul style="list-style-type: none"> • Public wireless networks delivery and support are a core competence • Existing large Customer base • Strong, established brand • Resources in place to support new infrastructure with business processes geared to communications service launch 	<p>Allows Operator to Address Consumer’s Current Mobility Requirements</p> <ul style="list-style-type: none"> • Clear understanding by the Consumer of the ‘on the move’ solution • The ‘Roaming’ Corporate Consumer requires the following ‘basic’ services addressed by WLAN: email, Internet access and VPN access.
--	---

<ul style="list-style-type: none"> Existing Operational and support systems (i.e. billing, Customer care etc.) Roaming agreements and interoperability experience means operators are well placed to capitalise in this market. 	
<p>Effective Adoption of a Tactical Position</p> <ul style="list-style-type: none"> WLAN services offered as an extension of the Operator's service portfolio Via the WLAN solution, the Consumer will be engaged and prepared for evolution to full 3G services The Operator will ultimately be able to offset operating costs and provide value added services by offering seamless interoperability between 3G and WLAN services. 	<p>A Shorter Term ROI is Forecast for WLAN Services</p> <ul style="list-style-type: none"> The lower cost of entry into the WLAN market and forecast ROI periods of 4–5 years are advantageous to Operators seeking to rapidly recoup investment costs. Despite the absolute small size of the public WLAN market, it represents a significant proportion of the revenue achievable from high-speed mobile data services.

WLAN authentication is one of the key aspects of operation of a WLAN network. If the operators are successful in getting SIM based authentication methods adopted then the operators will be in a strong position. Indeed it may become realistic for operators to provide authentication services alone, without necessarily supporting the infrastructure.

7.9 Business Models

There is a great deal of latitude in terms of roles and integration options within a WLAN Operator scenario. For the purposes of consistency, five key roles are defined within the WLAN value chain. These roles are described in the following sections. The key issues faced by each of the adopted roles within the value chain are also included in the form of a 'SWOT' outline. These outlines form the basis for developing more detailed value chain models

7.9.1 Value Chain

The diagram below illustrates the value chain and outlines where the roles referred to in subsequent sections fit in.

The following key roles are explored in more detail later in this annex:

- Operator (see section 7.9.2)
- Service Provider (see section 7.9.3)
- Aggregator (see section 7.9.4)
- Broker (see section 7.9.5)
- Hot spot owner (see section 7.9.6)
- Property owner (see section 7.9.7)

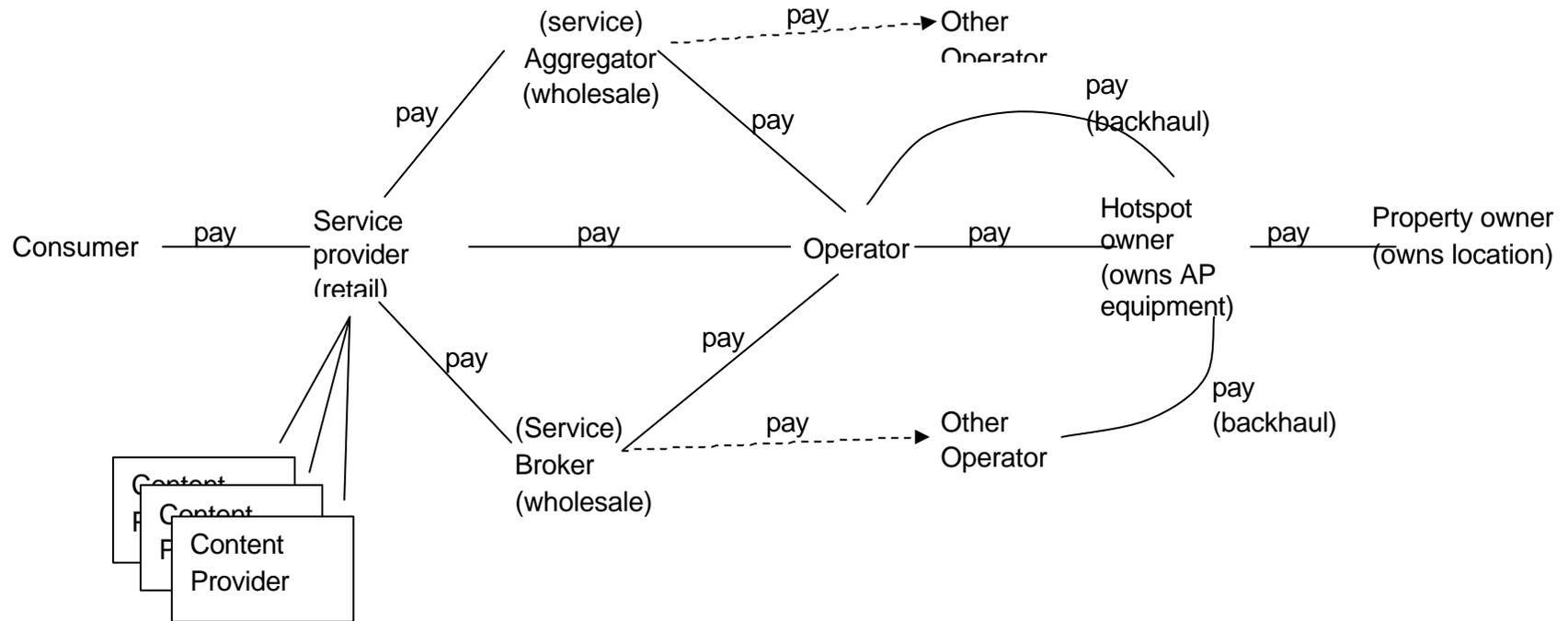
The following roles have also been identified in the value chain illustrated below, but are not deemed as key to the context of this annex:

- Consumer – In the context of this annex this is the end recipient of the service, this could be a residential customer, corporate, an individual within a corporate entity, a third party etc. [See also 0].
- Content Provider – Provides content and other related content provision services (e.g. content delivery, content aggregation etc) primarily to the Service Provider.

Notes on 'Key Roles in the WLAN Value Chain' Scheme shown below:

Within the scheme shown in the figure below, a WISP would typically function as Operator, Service Provider and Hot Spot Owner.

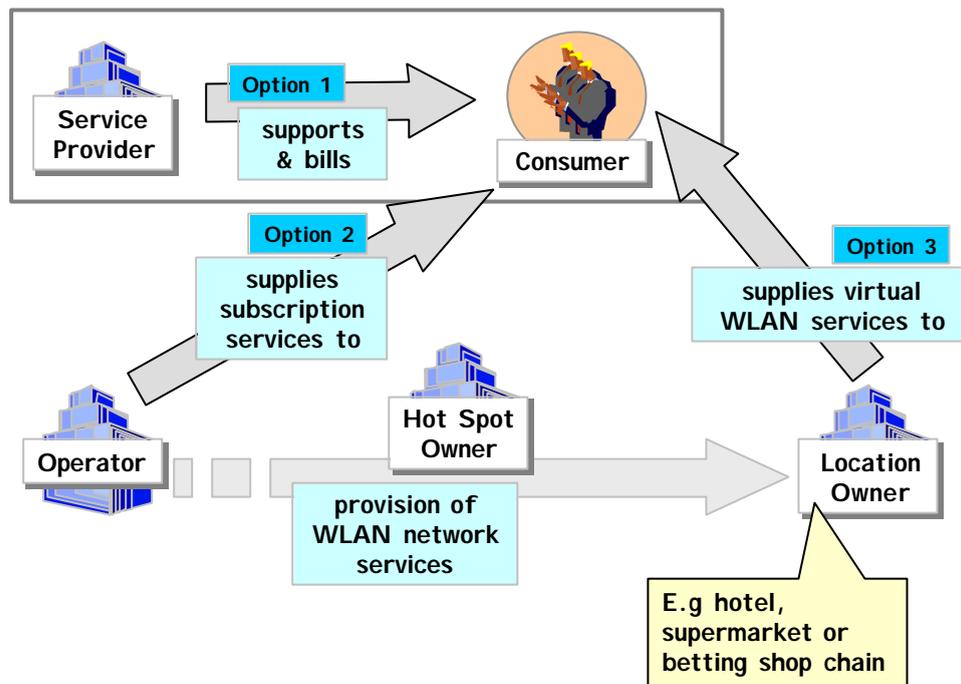
The Operator in practice might in addition operate as a combination of Service Provider, Aggregator and/or Hot Spot Owner.



Key Roles in the WLAN Value Chain

9.9.1.1 The Role of the Consumer

In the scheme shown above (i.e. *Key Roles in the WLAN Value Chain*) the Consumer (i.e. the end user of the services) is shown in the relationship that is anticipated to be the most prevalent i.e. acquiring services directly from, and being billed by, the Service Provider. However, it should be noted that the Consumer might also have direct relationships with the Operator, Hot Spot Owner and Location Owner.

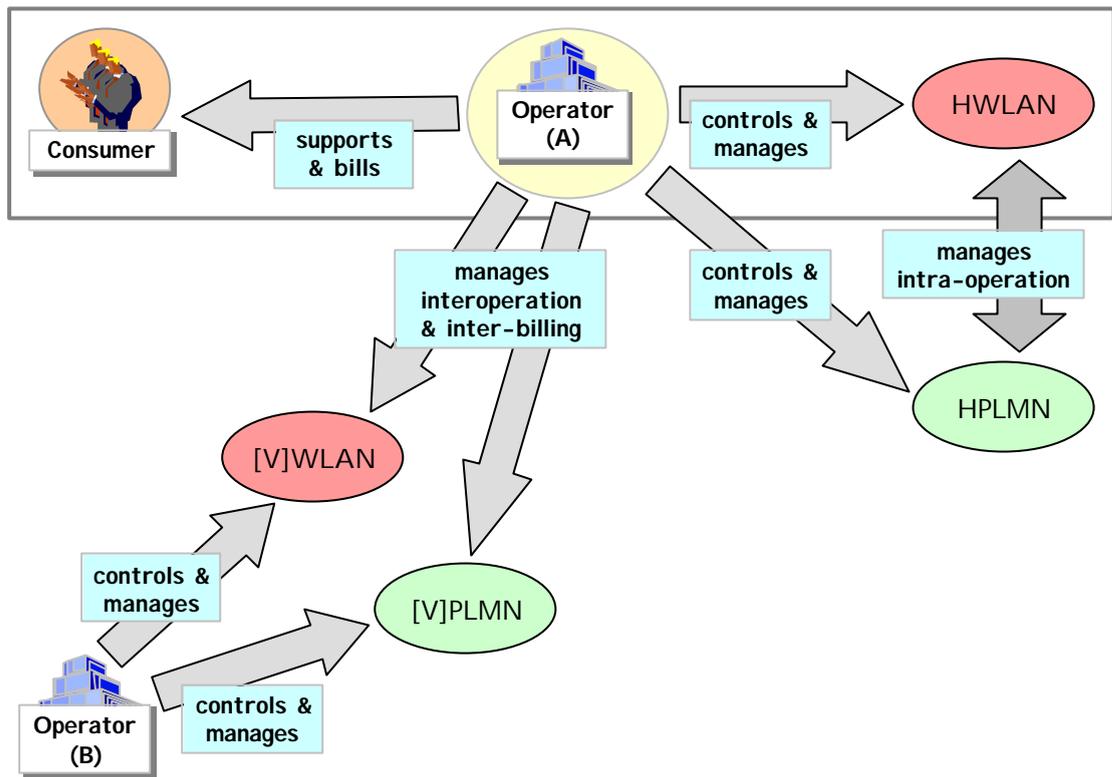


The Role of the Consumer

7.9.2. Operator

Profile:

The primary role of the Operator is that of owning and running the WLAN network infrastructure, providing network management and control functions, support and directly billing the customer (Consumer). It should be noted that the Operator might also adopt a combination of other roles within the value chain, such as Hot Spot Owner, Service Provider and/or Aggregator.



Examples of the mobile operators acting in a operator role are currently the most common, as typified by Telia HomeRun and Sonera amongst others.

Key Issues: From the perspective of an existing ‘cellular’ Operator

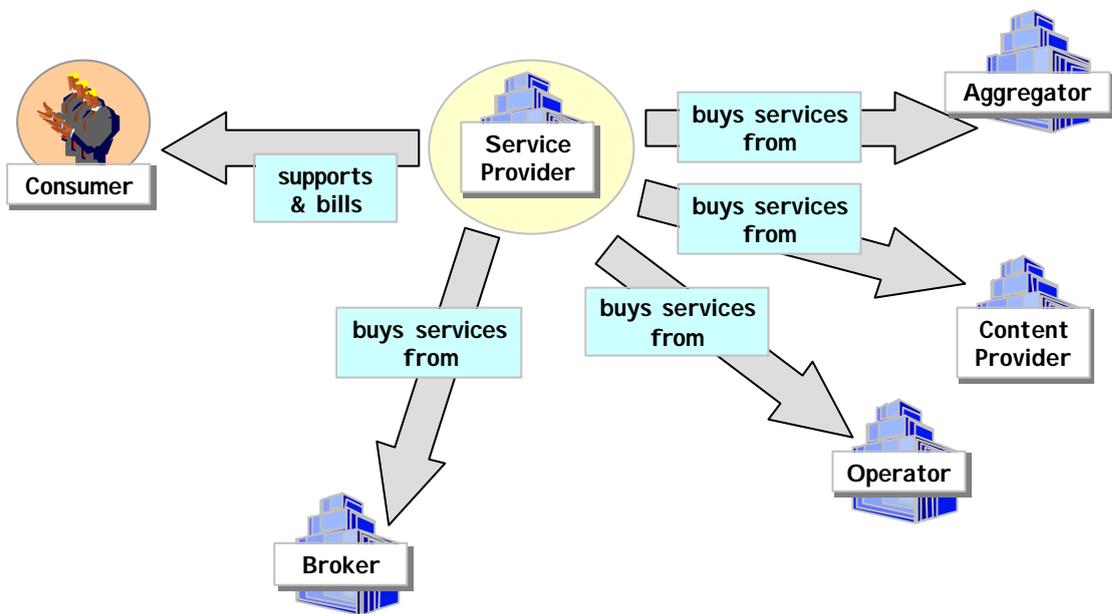
<p>Strength:</p> <ul style="list-style-type: none"> • WLAN model plays to key strengths of Operator, i.e. need to have effective service launch, authentication, reliability, competitive, ease of use, etc. • Large base of existing customers; has network and billing relationship with customer. • Fully integrated model, opportunity for cross- and up-sell of services to WLAN Customer base and offer unified billing of services to customer. • Can retain maximum percentage of revenue if supporting fully integrated (i.e. end-to-end) model. • Well-placed to acquire prime sites. 	<p>Weakness:</p> <ul style="list-style-type: none"> • Network infrastructure and operating costs. • Potentially confusing strategy, i.e. should customer perceive WLAN as a tactical solution prior to the arrival of full 3G services? • Customer segment is ill-defined.
<p>Opportunity:</p> <ul style="list-style-type: none"> • Potential new channel for services. • Provides early 3G-like services for 	<p>Threat:</p> <ul style="list-style-type: none"> • Licence exemption and low barrier to entry may undermine 3G investments.

<p>customers, which Operators should define.</p> <ul style="list-style-type: none"> • Provision of better personalisation/profiling, in particular for high-value customers. 	<ul style="list-style-type: none"> • Potential cannibalisation of 3G investment, i.e. competitiveness of WLAN services could act to de-value future 3G services. • Transitory, 'commoditised' nature of WLAN.
---	---

7.9.3. Service Provider

Profile:

The Service Provider buys services, typically from an Operator, Content Provider, Aggregator and Broker and sells on to customer. The Service Provider is responsible for billing customer.



Key Issues: From the perspective of an existing Service Provider organisation

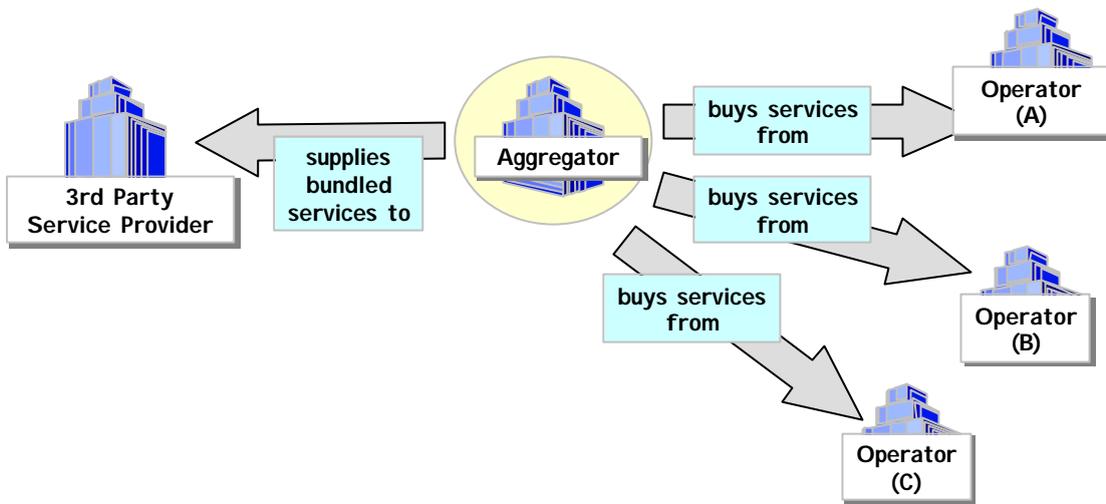
<p>Strength:</p> <ul style="list-style-type: none"> • No infrastructure needed to operate • Existing billing relationship with customer. • Able to 'shop around' to broker best rates from Operator. • Flexibility 	<p>Weakness:</p> <ul style="list-style-type: none"> • No infrastructure, reliance on alliances • WLAN model offers little or no customer relationship to Service Provider.
<p>Opportunity:</p> <ul style="list-style-type: none"> • Ability to secure best services and offer them via SP-owned platform. • Potential to offer developed least cost routing capability. 	<p>Threat:</p> <ul style="list-style-type: none"> • Relatively reactive role in value chain.

- New channel for value added services.

7.9.4. Aggregator

Profile:

The Aggregator buys services from several Operators and sells bundled/unified services onto 3rd party.



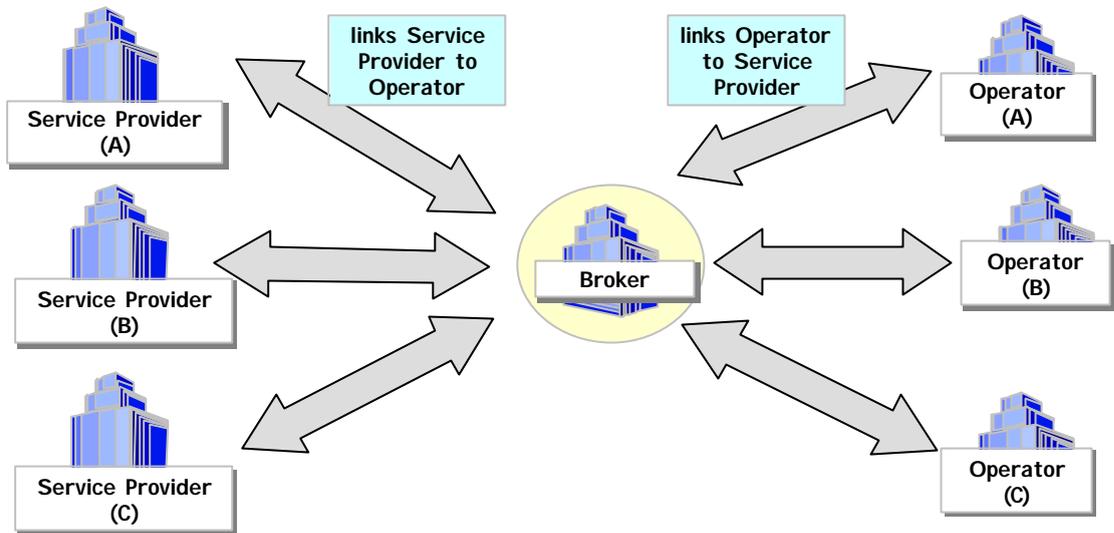
Key Issues: Aggregator

<p>Strength:</p> <ul style="list-style-type: none"> • Ability to deliver most effective route to 3rd party Service Provider. • Independent status provides capability to provide better coverage. • No requirement to acquire sites • Wholesale billing. 	<p>Weakness:</p> <ul style="list-style-type: none"> • No control of integration and management of infrastructure, making customer-oriented SLAs potentially difficult.
<p>Opportunity:</p> <ul style="list-style-type: none"> • Spot marketing/buying of services as a means to aggressively obtaining best value for service. 	<p>Threat:</p> <ul style="list-style-type: none"> • Potentially vulnerable to large ISPs entering new market.

7.9.5. Broker

Profile:

The Broker links Operator(s) to Service Provider(s) within a wholesale commission-based model. Envisaged as a predominantly commercial arrangement, a physical 'broker hub' may exist in the integrated architecture.



Key Issues: Broker

<p>Strength:</p> <ul style="list-style-type: none"> • Market agility, best placed to offer best value deals for 3rd party Service Providers and Operators. • No associated infrastructure overheads, operating responsibilities etc. • No billing responsibility with consumer • No need to bid to acquire sites. 	<p>Weakness:</p> <ul style="list-style-type: none"> • As an outsourced service is vulnerable to cost cutting exercises, i.e. could potentially be perceived as an overhead. • No tangible/tradable assets.
<p>Opportunity:</p> <ul style="list-style-type: none"> • Potential to acquire best players in negotiations. • Opportunity to influence 	<p>Threat:</p> <ul style="list-style-type: none"> • Network operators and Aggregator • Vulnerable to being 'squeezed' out of the value chain • Market may be too small or become too consolidated to support Broker role.

7.9.6. Hotspot Owner

Profile:

The Hotspot Owner provides the access point equipment, installs it and provides access to the operator. The Hotspot owner also negotiates with the property owner to acquire the site. An example profile could be an airport lounge. The lounge operator (e.g. SAS, United or British Airways) could install the equipment and then lease capacity to one or more operators.

Key Issues: Hotspot Owner

<p>Strength:</p> <ul style="list-style-type: none"> • Ability to sell to more than one operator • Owns the infrastructure and can choose to manage it itself or lease management • No billing responsibility with consumer • 	<p>Weakness:</p> <ul style="list-style-type: none"> • Must be in a clearly useful hotspot otherwise additional costs to operator may not be recouped • Needs good relationships with the property owner
<p>Opportunity:</p> <ul style="list-style-type: none"> • Can acquire a dominant influence if right hotspots are acquired • Many key hotspots are still available 	<p>Threat:</p> <ul style="list-style-type: none"> • • Loss of key hotspots to other players •

7.9.7. Property Owner

Profile:

The Property Owner owns the property/land into which the access points are installed. An example profile would be StarBucks or Marriot hotels.

Key Issues: Property Owner

<p>Strength:</p> <ul style="list-style-type: none"> • Owns the physical location • Direct access to the customers • Absolute control over installed equipment and deals made 	<p>Weakness:</p> <ul style="list-style-type: none"> • Location may not be a prime site (i.e. the addition of WLAN may not lead to significant increase in revenue) • Needs to promote the service
<p>Opportunity:</p> <ul style="list-style-type: none"> • Increase revenue from business travellers largely eroded by use of mobile phones • Short term differentiation • Customers likely to remain within property for longer 	<p>Threat:</p> <ul style="list-style-type: none"> • Coverage could be made available from another property • May be pressured into exclusive agreements with WLAN providers

7.9.8. Key Business Questions

Some of the key questions to be addressed are:

• **Who are the key players in the value chain?**

The hub-based nature and low entry point of the WLAN architecture will further increase the competitive landscape with new market entrants. There may well be a number of profiles of new market entrant, from the traditional ISP, ASP/BSP and ERP/middleware organisations such as IBM or Cisco. ‘Hot Spot Owner’ entrants with specific sector experience may seek to diversify by focusing on operating in a niche market (e.g. banks, hotel chains, oil rigs, betting shops). These new, niche market entrants will be offering customers vertical segment-specific services, adopting Service Provider roles in the value chain – owning the sites and customers, but not necessarily the infrastructure to deliver the service.

PA Consulting has considered a number of WLAN Operator models and believe that WLAN may mimic the cellular model, where one Operator installs WLAN nodes in all the ‘hot spots’. Alternatively, one Operator might focus on particular areas such as hotel chains or airports. The extreme case is one in which each building has its own WLAN system. Within this potentially fragmented landscape, ‘Consolidator’ roles may emerge. PA Consulting predicts that companies such as AT&T and AOL will take on the role of consolidation; building a core network to link cellular and the disparate WLAN systems together to form a seamless service for the consumer.

As incumbents with established customer bases, extensive experience in network roll-out and management and trust in security of access, the Operators, are well placed to negotiate deals with new players (particularly in the early stages when the competition centres around acquisition of ‘hot spots’).

‘Themed’ hot spots, where the profile of the consumer may be better predicted potentially offer strong opportunities for cross- and up-sell of services for both Operator and Location Owner. For example, handset upgrades, or hotel room upgrades/discounts. The brand element will clearly play an important part in the formation of new alliances of this kind.

• **Is the ‘hot spot’ revenue model clearly developed?**

Consumers use wireless systems differently, depending on their location and how static they are likely to be, i.e. on the move (walking, driving) or in a hotel room or airport. There is an element of conjecture in the modelling of usage in various WLAN scenarios, as to date few high-data-rate services are available (although early adopter implementations, such as Telia’s, offer some insight). Early modelling of revenue potential, for different ‘hot spot’ locations and scenarios, will clearly be important in determining which locations and alliances will yield most value for the Operator. Several hot spot types, together with key points to consider are highlighted in the table below:

LocationType	Key Features
Airport (A)	<ul style="list-style-type: none"> • High volume of customers of the right profile for uptake of data services • potentially high growth volume • Within this more static location, usage likely to involve high-data-rate applications • Ability to target corporate user via business lounges • ‘Business lounge’ contract deal provides potential for International/global presence for Operator, i.e. covering business lounges in all major airports around the world.

LocationType	Key Features
	<ul style="list-style-type: none"> • Controlled environment, interference from other sources (microwave, Bluetooth etc.) potentially more manageable within airport location • Acquisition costs likely to be high with high degree of competition for acquiring this category of hot spot • CRM potential poor • Limited opportunity to sell value added services
Hotel (H)	<ul style="list-style-type: none"> • Medium volume of customers, relatively low growth in volume • Within this more static location, usage likely to involve high-data-rate applications • Contract deal provides potential for International/global presence for Operator, i.e. covering hotel chains in major cities around the world. • Relatively uncontrolled environment, potential interference from other sources (microwave, Bluetooth etc.) • Acquisition costs likely to be high with high degree of competition for acquiring this category of hot spot (though not as high as 'public' hot spots) • CRM potential poor • Limited opportunity to sell value added services
(Residential or Commercial) Managed Services Apartment (M)	<ul style="list-style-type: none"> • CRM potential good, opportunity to target high-value corporate customer segment with personalised/sector-specific services. • Offers good opportunity for cross- and up- sell of services • Relatively static customer volumes, however potential for larger ARPU per consumer • Reduced control of environment, leading to potential for interference from other sources within this more fragmented infrastructure
Sports Stadium (S)	<ul style="list-style-type: none"> • Mass market • Ad-hoc customer base • Advertising opportunity • Asymmetric communications

• **What are the challenges for CRM when offering WLAN services?**

In keeping with other operating and support environments, in the WLAN interoperability model, Operators are faced with the task of identifying the customer and using this

information to manage customer contracts and profitability. Within the WLAN/Cellular interoperability model, integrating back office systems with front office customer facing elements may be more challenging.

Since within the WLAN/Cellular interoperability model, the question of customer ownership may not always be clear. It may be, for example, that the Operator will not have a direct customer-facing role (i.e. the billing responsibility may belong to the Hot Spot Owner - who in this case may not be the Operator themselves - or Service Provider).

The ability of the Operator to track customers will largely depend on two factors:

- **The nature of the WLAN transaction**

For example, the use of WLAN in airports, hotels etc, where access is initiated by PIN number, does not require the consumer to establish a relationship with the Operator (or indeed the Service Provider). Ultimately, full WLAN/Cellular interoperability will enable the customer information to be captured by subscription (leading to a fully integrated service offering, for example unified billing, preferential access etc.).

The counter argument to the 'anonymous access' approach is that in this 'tactical' deployment phase, the transitory, essentially anonymous, customer access enables support and operating costs to be kept to a minimum. This is particularly true if the Hot Spot Owner is not the Operator, or the Consumer is able to self-provision the WLAN service via Internet access. It does however result in a more complicated SLA model.

- **The status of ownership within the value chain.**

If the Operator is acting purely as an Operator, i.e. providing network access and management capability, within the relationship, access to Consumer data may not be possible or appropriate.

Interspersing a number of layers between the Operator and the Consumer (i.e. Service Provider, Hot Spot Owner) highlights the general challenge for mobile Operators, particularly those transcending International boundaries; that of establishing 'network brand' loyalty.

- **What is the impact on existing billing systems of WLAN services?**

Working on the premise that the Mobile Operator had a direct relationship with the customer and therefore bills the Customer, there are still potentially a range highly divergent pricing structures to be considered.

The current WLAN deployments, as exemplified by Telia's HomeRun Service, allow for simple, pre-paid billing for timed out access to a single service. The medium term (or Phase 1) goal will be billing systems capable of supporting multi-access via a single bill, single Customer care system, support number etc. Phase 2 allows for single authentication and a truly seamless service.

Key areas to investigate are:

- Unlike voice which is a relatively easy application to charge for, in the case of post pay data services access, how would a Consumer understand what they are being charged for? How would an itemised bill look?
- Will billing platforms offer sufficient flexibility and agility to the Operators to enable them to modify pricing structures to reflect market changes and competition?
- Within a sophisticated seamless charging model, will the Operator be required to support micro-charging?

- With new entrants potentially able to enter the WLAN value chain (e.g. credit card organisations, utilities, supermarkets), will Operators be able to charge for more than the bit pipe?

7.10 Architecture Choices

When rolling out a WLAN network it is necessary to decide what architecture is required. In this case there are essentially three options of how to integrate the WLAN and the operators cellular network:

- not coupled,
- loose coupled and
- tight (or flexible) coupled.

In the sections that follow each of the given architectures are described and the benefits and challenges of each are presented. In all cases only two authentication schemes are covered: RADIUS based and SIM based. RADIUS is available now and is widely adopted by WISPs. SIM based is likely to be another 6 to 12 months before being widely available.

7.10.1. No Coupling

In this architecture the WLAN and the PLMN are operated as separate entities but combined bills are possible, even if only added at the final printing stage. Typically customer care will be handled by a separate team (due to the different nature of support required). The primary link between the WLAN and PLMN lies in the brand.

In this model the user is authenticated onto the WLAN via the user of a username/password scheme via the RADIUS AAA server. In the PLMN case the network uses traditional HLR based authentication.

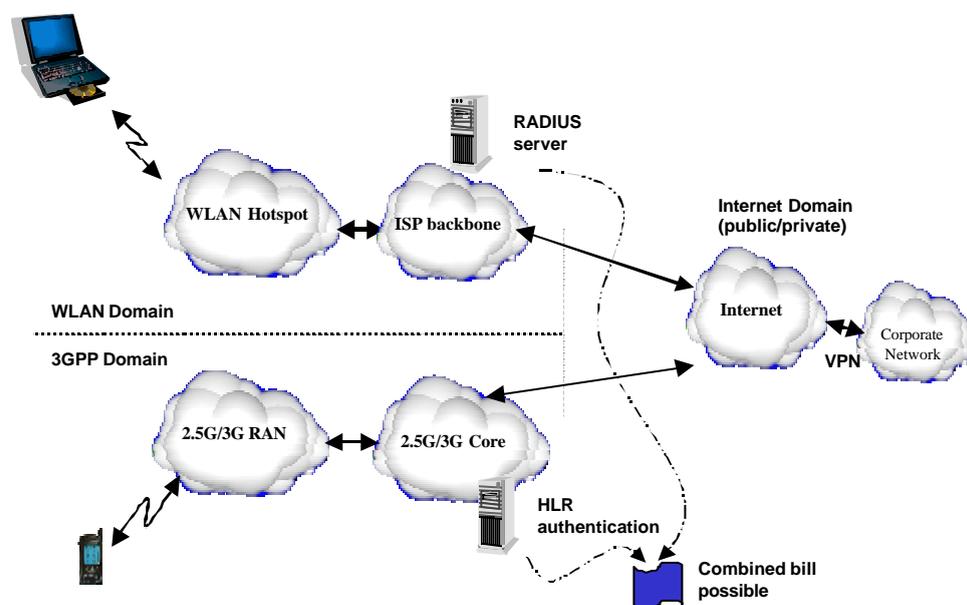


Figure A1 : WLAN and PLMN Not Coupled

Pros	Cons
<ul style="list-style-type: none"> • Easy to implement and can be deployed now • Compatible with WISPs systems • Combined billing can differentiate GSM operators from WISPs 	<ul style="list-style-type: none"> • Known issues with RADIUS • Services must be developed separately for WLAN access and PLMN access • Combined bills require some integration work between billing systems

Table A2: Pros and Cons of No-Coupling Model

In this case the user of the WLAN and mobile will not normally be able to use the same services unless the content provider provides both a cellular variant and an Internet variant which are integrated at the backend. (The content provider is not shown in the diagram for clarity.)

7.10.2. Loose Coupling

Loose coupling allows the WLAN hotspot to authenticate the user against the home network's home location register and authentication centre. It also allows more centralised billing functionality than is possible with the no-coupling model.

Customer care functions can be integrated or separated as required.

Pros	Cons
<ul style="list-style-type: none"> • Easy to provide an combined bill • Single authentication source for mobile users (HLR/AuC) • Bills can be generated from the local WISP or the home network operator • Ability to offer some services over both bearers, providing scope for personalisation • Operator differentiation potential for those who can couple • Customer retention 	<ul style="list-style-type: none"> • Integration may be complex (especially given sensitivity of exposing the HLR to the Internet) • Solutions not yet available • No seamless operation of services

Table A3: Pros and Cons of a Loosely Coupled Architecture

The ability to offer services such as unified messaging will encourage customers not to churn to other providers quite so readily. In the no coupled model there is no real reason for a customer to use any one providers network.

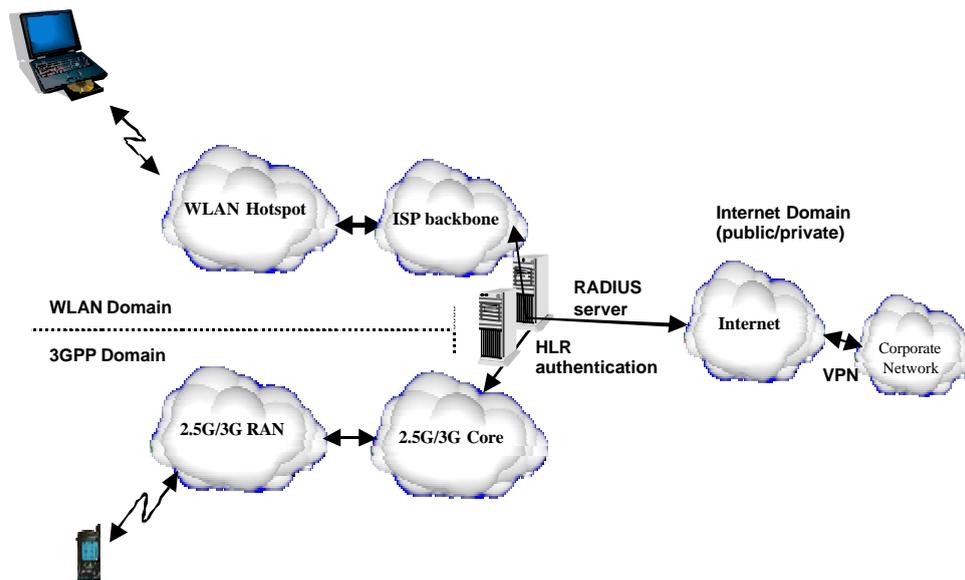


Figure A2 : WLAN and PLMN Loosely Coupled

Bills can be generated from the interworking functions on the WISP side or on the network operator side. It is probable that operators will choose to provide the billing functionality on their side. However, reconciliation can be performed against the record emanating from the visited WISP hotspot.

7.10.3. Tightly Coupled

In the tightly (or flexibly) coupled solution the WLAN access point couples directly into the cellular operators access network. This can be achieved at a number of points with differing integration costs and implications ranging from coupling at the radio base station through to coupling at the radio access networks of the WISP and the mobile network operator interact in such a way that a handover between WLAN and 3GPP environments is possible.

In figure 3 a mobile data user can operate either within the WLAN context or in the 2.5/3G RAN context. In either the authentication (of at least) the operator's customers is against the home network's HLR. Data services will be operational both on the PLMN and on the WLAN and it is possible through the integration of signalling between the WLAN and the 2.5/3G RAN to switch traffic across access networks.

Authentication is still via the authentication interworking system.

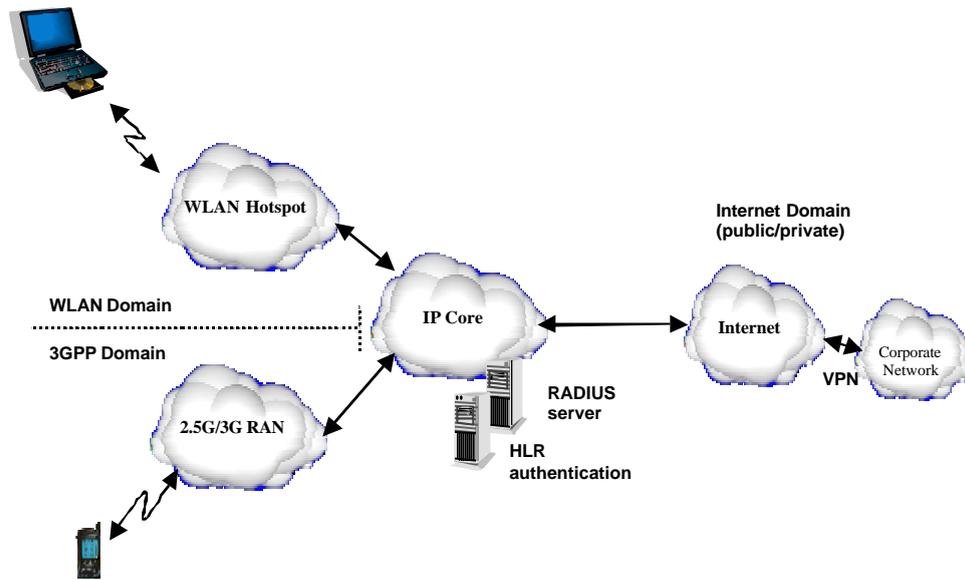


Figure A3: WLAN and PLMN Tightly Coupled

Pros	Cons
<ul style="list-style-type: none"> • Fully seamless operation for Consumer • WLAN just another bearer for mobile network operator services • Can assist in capacity planning by providing broadband access at lower cost than 3G • Potential for single device usage 	<ul style="list-style-type: none"> • Not likely to be available until after 3GPP Release 6 (earliest 2004) • Unclear at this stage how important handover of services/sessions is going to be

Table 4: Pros and Cons of the Tightly Coupled Architecture

7.11 Decision Tree

In this annex a number of options have been presented and it is difficult to view all the options together. To help in this regard the following decision tree is presented which allows a clear view of the issues on one page.

