The Multimedia Mobile Access Communication Systems Promotion Council

Chairman of ETSI Project Broadband Radio Access Networks
Jamshid Khun-Jush, Dr.-Ing.
Ericsson Eurolab Deutschland GmbH
Ericsson Research, Corporate Unit
Neumeyerstr. 50
D-90411 Nürnberg
Germany
Tel: +49 911 2551260 / Fax +49 911 2551961
Email: jamshid.khun-jush@eed.ericsson.se

Chairman of High Speed Wireless Access Committee of MMAC-PC
Masahiro Umehira, Dr.
Wireless Systems Innovation Laboratory
NTT Network Innovation Laboratories
Yokosuka
Japan
Tel: +81-468-59-3547 FAX: +81-468-55-1497
Email: umehira@wslab.ntt.co.jp

Chairman of IEEE 802.11
Stuart J. Kerry, Mr.
Philips Semiconductors, Inc
San Jose
USA
Tel: +148 408 474 7356 FAX: +148 408 474 7247
Email: stuart.kerry@philips.com

To: Niels Andersen, Chairman of 3GPP SA

Cc: Kevin Holley, Chairman of 3GPP SA1, Puuskari Mikko, Chairman of 3GPP SA2, Michael Walker, Chairman of 3GPP SA3

Date: 13th September 2002

Subject: Liaison statement about new Wireless LAN Interworking Group (WIG)

Dear Niels,

It is with great pleasure to inform you that MMAC HSWA, ETSI Project BRAN and IEEE 802.11 have jointly created a group to work on the issues related to 3G and other public access networks interworking. The group has been given the name WIG (Wireless LAN Interworking Group).

WIG has adopted the following scope:

- To be an integral part in the production of a generically applicable interworking standard for WWAN (Wireless Wide Area Network) and other public networks. The standard is to be applicable for IEEE 802.11 family, MMAC HiSWAN family and ETSI HIPERLAN/2
- To be the point of resolution for ETSI, IEEE and MMAC on issues related to interworking with WWAN and other public networks.
- To be the single point of contact for the above-mentioned WLAN standards on questions related to interworking with WWAN and other public networks.

The WLAN Interworking Group will deploy a joint email reflector given below and is available for subscription. This reflector is currently being maintained by ETSI/BRAN. The document areas will be open for members of IEEE, ETSI and MMAC only. If you are interested in these documents we then request information about how we can share relevant documents between our organisations.

WIG@list.etsi.fr

Subscription can be made via the "E-mail Archives - BRAN" window in the BRAN part of the ETSI portal http://portal.etsi.org/bran (click on the +/- icon to join the list) or by sending a request to BRANsupport@etsi.fr
For additional information please make contact with one of the following persons below:

- Takashi Aramaki, Takashi.Aramaki@YRP.MCI.MEI.CO.JP, Liaison officer for the MMAC HSWA.

- TK Tan, tktan@ieee.org, Chairman of the WNG SC at IEEE 802.11

- Thomas Haslestad, Thomas.Haslestad@Telenor.com, Rapporteur of the 3G Interworking Group at ETSI Project BRAN.

Best Regards

Stuart J. Kerry, Jamshid Khun-Jush & Masahiro Umehira

European Telecommunications Standards Institute **BRAN30d135r1**
BRAN #30
1st to 4th October 2002
ETSI, Sophia Antipolis
France

Source: Siemens, France Telecom, Panasonic
Title: Proposed WIG Baseline Document, Version 0.1
Date: 3rd October 2002
Document for: Discussion
Agenda item: WIG (Wireless Interworking Group)

Note: Although this document is based on BRAN 3GIWG material, no claim is made that it represents the views of any body within ETSI or any broader group of companies. It is an individual contribution, whose purpose is to encourage discussion and debate on the way forward for WLAN interworking.

Summary

Recently, mobile business professionals have been looking for an efficient way to access corporate information systems and databases remotely through the Internet backbone. However, the high bandwidth demand of typical office applications, such as large email attachment downloading, often calls for very fast transmission capacity. Further, certain hot spots, like airports and railway stations are a natural place to use these services. However, in these places the time available for information download is typically fairly limited.

In the light of above there clearly is a need for a public wireless access solution that could cover the demand for data intensive applications and enable smooth on-line access to corporate data services in hot spots and would allow a user to roam from a private, micro cell network (e.g. a WLAN Network) to a public (e.g. cellular) network.

Together with high data rate cellular access, WLAN Technologies have the potential to fulfil end user demands in hot spot environments. WLAN hotspots offer a possibility for cellular operators to offer additional capacity and higher bandwidths for end users without sacrificing the capacity of the cellular users, as WLANs typically operate on unlicensed frequency bands. Furthermore, interworking solutions enable operators to utilize the existing cellular infrastructure investments and well established roaming agreements for WLAN network subscriber management and billing.

This document is input to the process of developing a single global standard which will support this type of interworking between WLAN networks and public networks, which is not specific to any WLAN technology, or tied to any single public network architecture.

[SMc: Some of this new text may want to go into section 2]

During the summer of 2002, the following standardisation bodies; ETSI BRAN, IEEE 802.11 and MMAC HSWA arrived at a trilateral agreement to generate this global standard and have name the group to undertake this work as WIG (WLAN Interworking Group)

1.1 WIG scope

The scope for WIG, which was ratified at the initial WIG meeting, states that the purpose of the group is:

- To be an integral part in the production of a generically applicable interworking standard for WWAN and other public networks. The standard is to be applicable for IEEE 802.11 family, MMAC HiSWAN family and ETSI HIPERLAN/2

- To be the point of resolution for ETSI, IEEE and MMAC on issues related to interworking with WWAN and other public networks.

- To be the single point of contact for the above mentioned WLAN standards on questions related to interworking with WWAN and other public networks.

1.2 Objective

It is the objective of this document to be the WIG working document. By nature of the WIG scope, this document does not cater for any particular WLAN technology. This level of detail is outside the scope of WIG and shall be described within separate documents produced within each of the member standardisation groups.

To further illustrate the goal of this document, hotspot technology located within Japan would use this document in conjunction with a specific MMAC HSWA document detailing all aspects of interworking that affect HiSWANa technology.

Comments on this document should be addressed to the authors:
Stephen McCann (editor), Siemens/RMR, stephen.mccann@roke.co.uk
Franck Lebeugle, France Telecom, franck.lebeugle@rd.francetelecom.com
Cheng Hong, Panasonic, hcheng@psl.com.sg
Or to the WIG mailing list:
WIG@list.etsi.fr

Contents

Summary 1

1 Introduction 4
1.1 WLAN Interworking Concept 4
1.2 Document Scope 5
1.3 Document Status 6
1.4 Release Structure 7

2 References 7

3 Definitions symbols and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 9

4 Reference Architecture 9

5 Authentication (L*s* Interface) 11
5.1 Authentication Functions 13
5.1.1 Authentication Functions 13
5.1.2 Attendant 13
5.1.3 MT Authenticator 13
5.2 Backwards Compatibility with RADIUS and CHAP 14

6 Authorisation (L*p* Interface) 15
6.1 Authorisation Functions 16
6.1.1 Authorisation Function 16
6.1.2 Authoriser 16
6.2 Policy Control Functions 16

7 Accounting (L*a* Interface) 17
7.1 Accounting Functions 18
7.1.1 Accounting Function 19
7.1.2 Resource Monitor 19

8 User Data Forwarding 19

Annex A (Informative): Requirements 20
A.1 Security and Authentication 20
A.1.1 Authentication Requirements 20
A.1.2 Network Security Requirements 20
A.1.3 Roaming Requirements 21
A.1.4 Summary Requirements on L*s* 21
A.2 Charging and Accounting 21
A.2.1 Accounting Requirements 22
A.2.2 Charging Requirments 22
A.2.3 Summary Requirements on L*a* 22
A.3 Authorisation 23
A.3.1 Authorisation Requirements 23
A.3.2 Summary Requirements on L*p* 23

Annex B (Informative): Technology Overview 23

2 Introduction

2.1 WLAN Interworking Concept

The scenario under consideration is that of a mobile user connecting directly to the Internet via a WLAN access network. The WLAN access network leverages roaming agreements with different service providers to which the user is subscribed for control plane functions such as authentication and billing. User plane data is sent directly out across the Internet to the correspondent node participating in a data session.

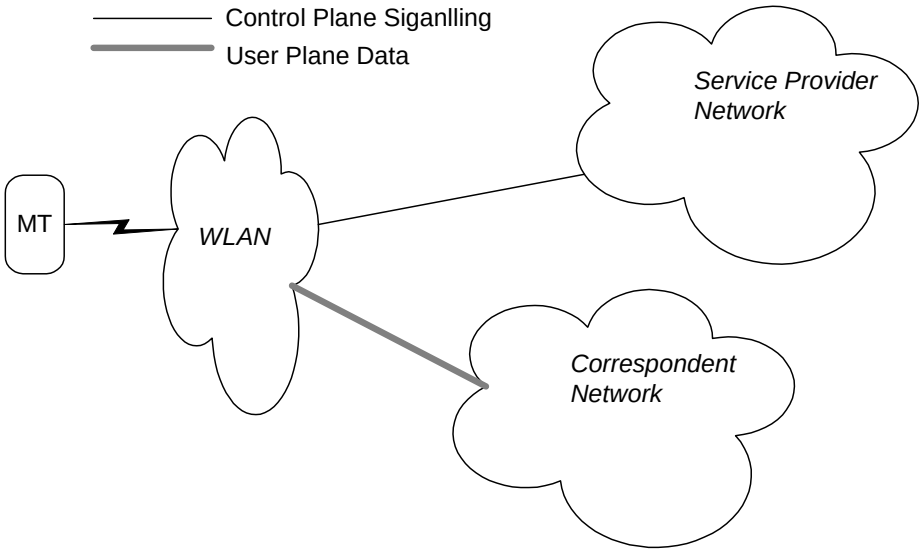

Figure 1. Overview of Network Entities

Within Figure 1, the following entities are identified:

- WLAN Access Network: incorporates multiple WLAN access points and the wired connectivity between them
- Service Provider Network: maintains user subscription and identity information, and is always the same for a given user.
- Correspondent Network: the destination/source network for the user plane traffic travelling to and from the MT.

There can be many independent access networks, service provider networks, and correspondent networks all connected together in an arbitrary manner and owned or operated by different administrations. For example, if the access network is owned by a different operator to that of the service provider network for a particular user, the access network takes on the role as visited network for that user. It is important to identify organisational boundaries in order to derive requirements for protocols used between the Access Network and the external networks. Such issues may include additional security requirements.

The Service Provider Network and the Correspondent Network could be combined for a given mobile, for example, in an Service Provider's mobile core network, but for the purposes of the following discussion and in order to avoid constraining any final architecture it is easier to describe them as logically separate. In particular, the separation of user and control plane traffic at the AN boundary has major implications for the functionality required in the access network itself.

2.2 Document Scope

The scope of the following document is to define the interface between the WLAN and the Service Provider and Correspondent Networks, at the so-called W.2 interface (see Figure 2). Figure 2 provides a high level view of the different functional groups considered within the following document, and the interfaces between them.

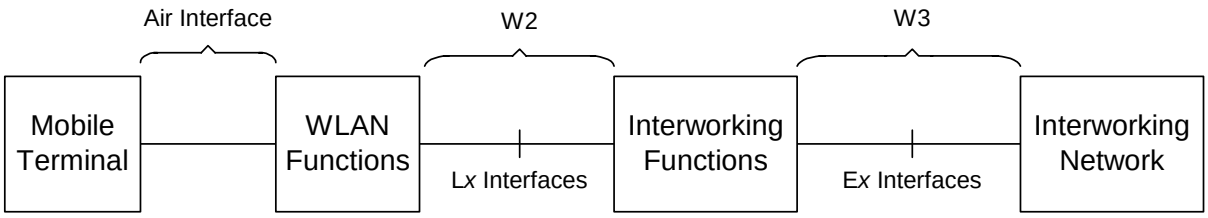

Figure 2. Overview of Interface Types

The WLAN Functions represent WLAN specific features, which communicate via standard protocols with functions in external networks. This communication is carried out across the W.2 interface, the standardisation of which is the focus of this document. The emphasis of the W.2 interface is to hide all WLAN specific features behind a single generic interface that can be used by external networks to support any kind of WLAN technology. Since the WLAN and external networks communicate with each other for a variety of different reasons, e.g. authentication, accounting etc. the W.2 interface is subdivided into a series of L interfaces to represent each different type of interaction.

In order for the inter-operation between WLAN functions and external network functions, interworking functions may be required to map between the protocol specified for the W.2 interface and those used within external service provider networks. The W3 interface provides the interworking from the standard defined for the L interface to another standard used by the external network. The definition of the protocols across the W3 interface (i.e. the E*x* protocols) is not within the scope of this standard, but may be defined by other standardisation bodies concerned with interworking WLANs to their specific technology e.g. 3GPP may define a set of E*x* protocols for interworking with UMTS. Different variant E*x* protocols may be applicable for different interworking scenarios (e.g. for different service provider network types).

A further representation of the relationship between the W interfaces described in this document and existing WLAN standards is given in Figure 3. This shows the WLAN standards as defining lower layer standards for the air interface (between MT and WLAN access network). Different WLAN standards may have different detailed scopes, in terms of which layers of the protocol stack are defined or required by them, and also in how much they define the system architecture, either inside the terminal or within the access network (e.g. between “access points” and “access servers”).

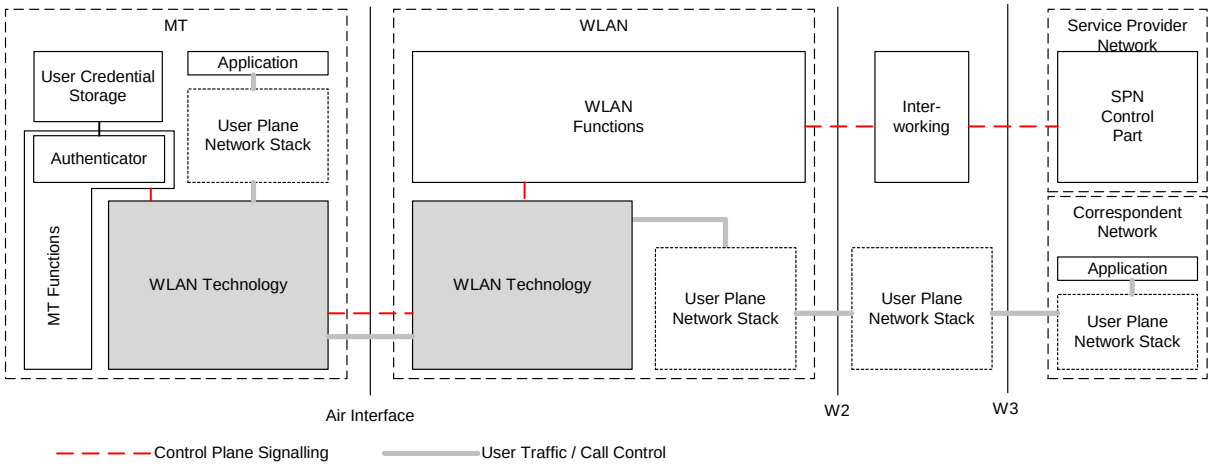

Figure 3. Scope of Existing WLAN specifications

The technology differences between these standards, as well as these differences in scope, are all intended to be hidden behind the W.2 interface. It is up to the individual WLAN standardisation or other body to describe how any particular WLAN technology should be deployed or configured (possibly in conjunction with other standards) to support the W.2 interface functionality.

2.3 Document Status

It is assumed that the interworking specifications will be developed in stages, with an initial release covering basic functionality (mainly authentication and authorisation related functions), and subsequent releases covering more sophisticated functionality (such as mobility management between networks, or QoS handling). The release structure is described in more detail in section 2.4. As mentioned above, this current document considers only functionality for the first release ("R1").

Because this document is supposed to be generically applicable to all WLAN standards, it does not consider any specific WLAN technology or refer to any standards body (except for the purpose of example). Nor will this document (or future iterations) have the status of an official standard in its own right. Instead, implementation of the interworking interface defined here for a given WLAN standard will include the following steps:

1. Adoption of the W.2 interface defined by this document by the standardisation body.
2. [Possibly] development of new additional WLAN technology-specific functions to enable the W.2 functionality to be supported inside the WLAN access network, in a way that does not impact W.2 itself.
3. [Possibly] other changes or refinements to the existing WLAN standard.

It is expected that all these steps will be carried out separately by the individual WLAN standardisation bodies concerned. The precise mechanism for step (1) may have implications for the appropriate structure for this documents (e.g. regarding references, terminology and so on) which are still to be determined.

This current document is based primarily on existing material developed within ETSI BRAN as part of the Hiperlan/2 – 3G Interworking group ("3GIWG") activities [1], but with the following changes:

- Changed language to be WLAN-generic rather than BRAN/Hiperlan/2 specific.
- Removed material on Hiperlan/2 internal mechanisms to support W.2 functionality, and replaced with information on what generic assumptions have been made on the underlying WLAN technology.
- Merging of requirements from several sources, retaining only requirements that apply at W.2.
- Where appropriate, listing of open issues where options are still to be defined or selected.

2.4 Release Structure

The member standardisation groups have agreed to produce this document in a two stage release to assist the market in produce interworking equipment in realistic timescales.

The first release (R1) is concerned with the establishing of functionality to provide a secure authentication scheme through the network to be interworked. It further establishes an architectural baseline for the interworking concept.

The next stage (R2) is to provide the support for functionality such as service integration, mobility and QoS differentiation support.

R1 supports the following functionality within the indicated sections:

- Authentication
- Authorisation
- Policy
- Simple Accounting

For R1, the method of communicating the Policy information will be stated, but the use of such information will only be fully described within R2. The main goal at R1 is to clarify the distinction between authorisation and policy control.

The scope of R2 is not fixed currently. However, typical functionality to be included might be:

- Mobility and Handover
- Quality of Service (QoS), and more generally other Policy capabilities
- Location Based Services
- Management

3 References

Note: No WLAN technologies are referenced as this document is a technology neutral standard, except for the initial ETSI reference that is the basis of this work.

[1] ETSI TR 101 957 v1.1.1 (2001-08): *Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Requirements and Architectures for Interworking between HIPERLAN/2 and 3rd Generation Cellular Systems*

[2] L. Blunk, J. Vollbrecht: *PPP Extensible Authentication Protocol (EAP)*, RFC 2284, March 1998

[3] P. Calhoun, at al: *Diameter Base Protocol*, draft-ietf-aaa-diameter-07, July 2001-09-24

[4] P. Calhoun, et al: *Diameter NASREQ Application*, draft-ietf-aaa-diameter-nasreq-09, March 2002

[5] T. Hiller, G. Zorn: *Diameter Extensible Authentication Protocol (EAP) Application*, draft-ietf-aaa-eap-00, June 2002

[6] P. Calhoun, et al: *Diameter CMS Security Application*, draft- ietf-aaa-diameter-cms-sec-04, March 2002

[7] J. Arkko, H. Haverinen: *EAP AKA Authentication*, draft-arkko-pppext-eap-aka-04, June 2002

[8] Microsoft Developer Network, *Windows 2000 EAP API*, August 2000

[9] B. Aboba, D. Simon: *The EAP Keying Problem*, draft-aboba-pppext-key-problem-01, February 2002

[10] C. Rigney, et al: *Remote Authentication Dial In User Service (RADIUS)*, RFC 2058, January 1997

[11] W. Simpson: *PPP Challenge Handshake Authentication Protocol (CHAP)*, RFC 1994, August 1996

[12] D. Durham et al.: *The COPS (Common Open Policy Service) Protocol*, RFC 2748, January 2000

[13] 3GPP TS 29.207 v5.10 (2002-09): *Policy Control over Go interface (Release 5)*

[14] Aboba, B., Arkko, J. and D. Harrington: *Introduction to Accounting Management*, RFC 2975, October 2000

[15] Arkko et al, *Diameter Accounting Extensions*, draft-ietf-aaa-diameter-accounting-01, March 2001

4 Definitions symbols and abbreviations

4.1 Definitions

WLAN Access Network: incorporates multiple WLAN access points and the wired connectivity between them

Accounting: process of monitoring the resource usage of a user in order to allow cost allocation, auditing and billing.

Authentication: process of exchanging information between two endpoints for the purposes of verifying their identity.

Authorisation: process of determining whether a user is allowed to access the services of a network, and what level of service they are able to request.

Correspondent Network: the destination/source network for the user plane traffic travelling to and from the MT.

Home AAA (AAAH): logical function within the loose coupling architecture that provides AAA functions to support subscribers who have a permanent relationship with that network

NOTE 1: Whether the subscriber is directly using a WLAN access network under the same administrative control as the AAAH, or is roaming on another operator's network, it is assumed that the AAA transactions are eventually handled by the AAAH, possibly via one or more intermediaries.

Mobile Terminal (MT): end system equipment providing the interface towards human beings through a set of applications

NOTE 2: The MT includes, among other things, the functions and protocols necessary to provide and handle the communication to the WLAN access network, as well as against other networks, services, and applications.

Mobility: ability of an MT to be used in different network environments, within a single and in different administrative domains, with minimum user intervention

User Identifier: the permanent identity of the user typically stored on a secure token such as a smart card or SIM, and usually transferred in NAI format.

Policy: relates to any special treatment that should be applied to a packet, beyond the choice between dropping it or forwarding it with best efforts service

Roaming: ability of an MT to connect to their service provider via third party owned access networks.

Service Provider Network: maintains user subscription and identity information, and is always the same for a given user

4.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3G Project Partnership
AAA	Authentication, Authorization and Accounting
AAAH	Home AAA
AKA	Authentication and Key Agreement
AP	Access Point
AVP	Attribute Value Pair
CHAP	Challenge Handshake Authentication Protocol
CMS	Cryptographic Message Syntax
CN	Correspondent Network
COPS	Common Open Policy Service
EAP	Extensible Authentication Protocol
HSS	Home Subscriber server
IETF	Internet Engineering Task Force
IP	Internet Protocol
IWF	InterWorking Function
MT	Mobile Terminal
NAI	Network Access Identifier
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SIM	Subscriber Identity Module
SPN	Service Provider Network
UMTS	Universal Mobile Telecommunication System
WLAN	Wireless Local Area Network

5 Reference Architecture

The following introduces a proposed reference architecture for interworking WLANs with external networks for public access. It identifies the functions required within the network and the interfaces between them.

Within the WLAN there are a number of functions that are required in order to support public access operation. These functions are logically grouped under the heading of WLAN functions, but this is not intended to constrain the location of these functions in terms of actual network implementations. For example, some functions may be supported within the AP whilst others are distributed amongst other network nodes.

The reference architecture is shown in Figure 4. The terminology used in naming the different functions tries to follow IETF conventions where possible but does not mandate the use of any particular transport infrastructure within the SPN.

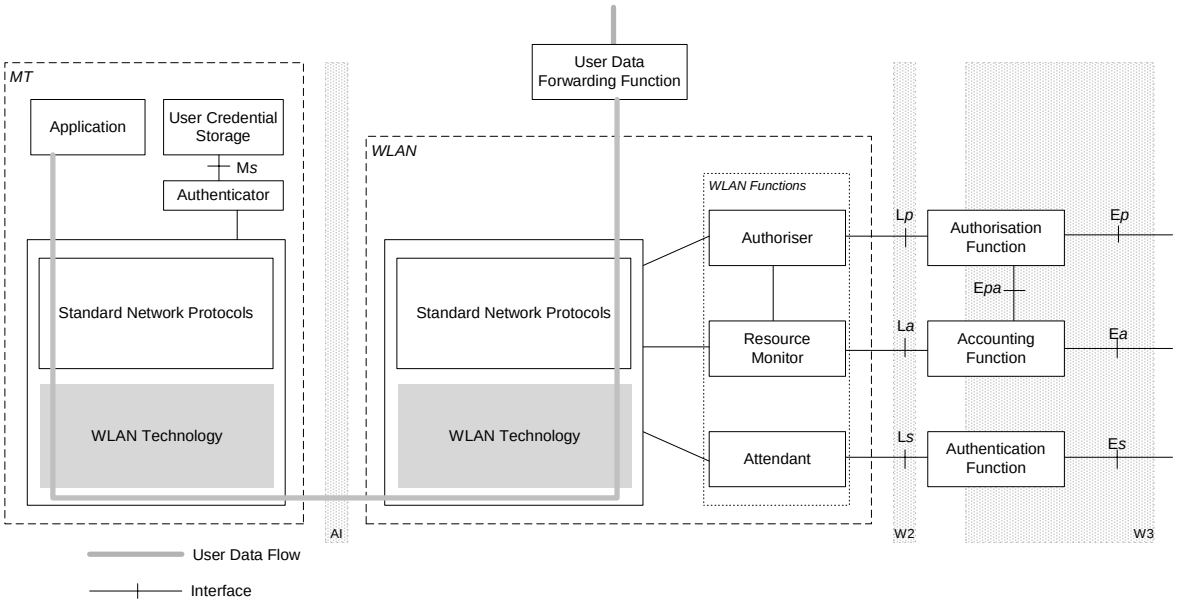

Figure 4. Reference Architecture

The interfaces are labelled as follows: -

- L interfaces pass across the W.2 interface. These are the interfaces that are proposed for standardisation within the current scope of the reference architecture. The L interfaces are required to run over a transport infrastructure that may vary depending on the scenario.
- M interfaces are internal interfaces within the MT. These interfaces are considered as reference points and are not proposed for standardisation, however specific reference to the interface M*s* is made below.
- E interfaces pass across the W3 interface. These interfaces are not proposed for standardisation within the reference architecture.

Within these categories of interfaces, the letters following the first letter indicate the type of function(s) the interface is used by. The convention is as follows:

- *a* interfaces are used by accounting functions
- *p* interfaces are used by authorization functions
- *s* interfaces are used by authentication mechanisms
- *o* interface are used by policy control mechanisms (note, since these interfaces are R2 functionality, they are not illustrated in Figure 4)

Although not all of the interfaces identified within the reference architecture will be specified, it is useful to identify these interfaces separately in order to determine what information needs to be exchanged across the standardised interfaces.

The reference architecture supports the following functional groups, each of which is described in further detail in the indicated sections: -

- Authentication (section 6): authenticates the user with the network and vice versa.
- Authorisation (section 7): checks user privileges and determines what basic (IP) services users are allowed to access. In addition, policy may be used to provide finer-grained control of the way to provide the service to the user. This type of policy control is not a release 1 function, however.
- Accounting (section 8): monitors resource consumption for auditing and billing purposes
- User Data Forwarding (section 9): forwards user traffic to and from the MT.

6 Authentication (Ls Interface)

Authentication provides a way for the access network to validate the identity of a user that wishes to access the WLAN network. The mechanism for authentication is undertaken through the exchange of logical keys or certificates between the MT, the users service provider network, and the WLAN.

In the public access environment, mutual authentication of a user and the user's service provider network is carried out end-to-end between the MT and the authentication server within the service provider network, for example an AAAH or HSS. The protocol used end-to-end to achieve authentication is the Extensible Authentication Protocol (EAP)[2]. EAP is a desirable choice since it can support a wide range of different authentication mechanisms (for example, encapsulating the native authentication protocols of the WLAN technology in question), it can be used with remote authentication servers, and it is already being widely adopted as an authentication solution. The protocol stacks either side of the air and W.2 interfaces are illustrated in Figure 4.

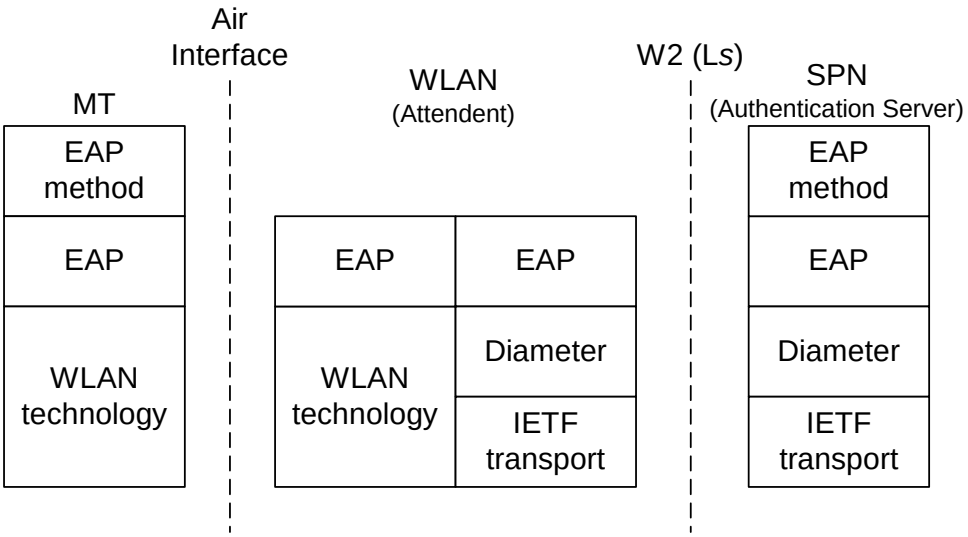

Figure 5. Protocol Stacks at the Air and Ls Interfaces

Diameter[3] is the protocol used for transporting the EAP messages across W.2, and as such it is possible for a number of Diameter proxies to be present between the WLAN and the AAAH. EAP can be transported in Diameter via the use of the NASREQ[4] or EAP [5] applications. Data confidentiality and integrity can be provided through the use of the CMS application [6].

EAP can conceptually be divided into two parts: the first part is the generic transport i.e. the format of the packet and the header contents, whilst the second part is concerned with defining how different authentication mechanisms are carried by the EAP packets. These definitions are referred to as EAP methods, and include authentication mechanisms such as UMTS AKA[7].

The authentication procedure is illustrated in Figure 6.

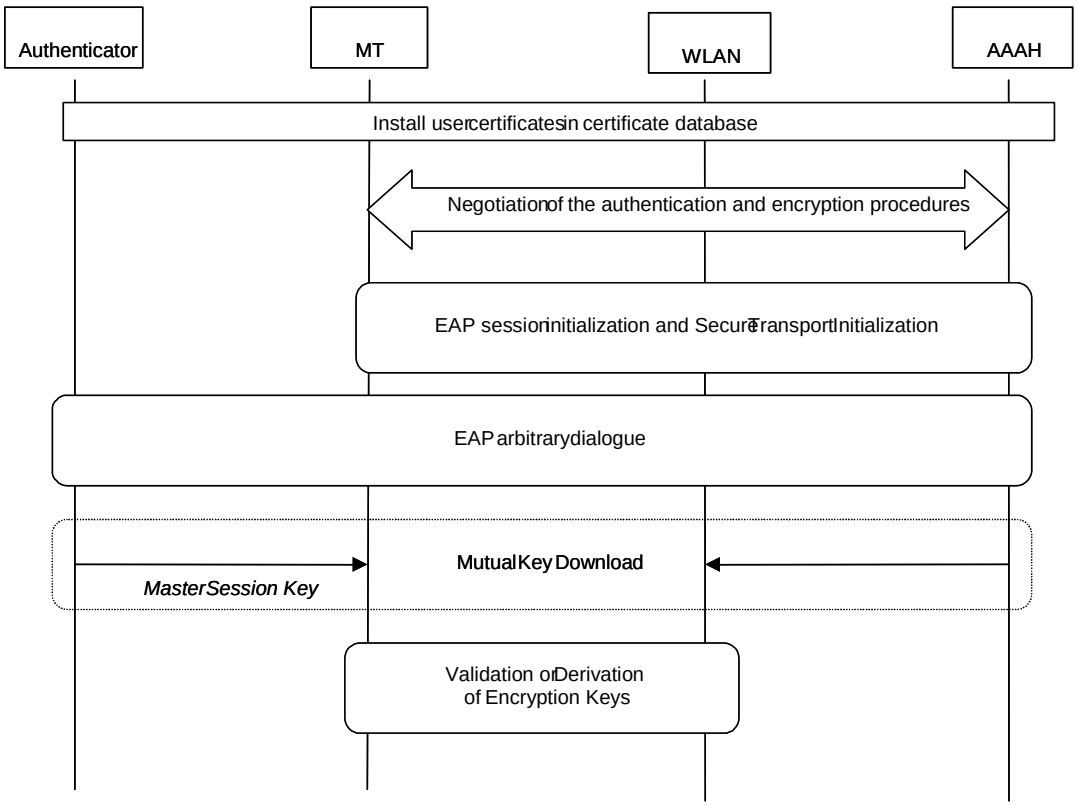

Figure 6. EAP with Mutual Key Download

Authentication consists of the following procedures:

- **Negotiation of the authentication and encryption procedures**

During association with an AP, the MT and the AP carry out link capability exchanges to negotiate which cipher suite to use etc. and optionally (depending on the technology) some form of encryption across the air interface may be initiated.

- **EAP Session Initialisation and Secure Transport Establishment**

In order to verify the identity of the user, the AAAH server that maintains authentication information for that user must be determined and a secure transport to that server initiated. The domain name of the service provider is determined from NAI information provided by the MT and a secure Diameter session is initiated to the corresponding AAAH. It is preferable for the NAI information disclosed to the network to be of the form anonymous@domain_name in order to protect the true identity of the user. During this establishment of secure transport to the AAAH, the service provider network may verify the identity of the access network.

- **Arbitrary EAP Dialogue**

The AAAH conducts an EAP exchange with the MT according to the EAP method deployed by the service provider. The specification of which EAP method should be used for interworking with different systems is out of the scope of this work. This allows the MT and AAAH to exchange whatever authentication is required to carry out mutual authentication. As a side effect of this authentication process, a shared master key is established at the MT and the AAAH. This master key is used to generate a master session key using a derivation algorithm specified by the EAP method.

User credential information is maintained at the MT in a secure device such as a SIM or a smart card. The Authenticator function present on the MT is responsible for interfacing to the user credential storage device for the purposes of authentication.

The 3G IWG is not concerned with the definition of the EAP method. The authentication mechanism chosen by the service provider and supplied on the MT is out of the scope of this standardisation work. Note, information

received from the EAP method does not have to be used in the same way by all WLAN technologies, but they should all utilise a common interface.

- **Mutual Key Download**

At the AAAH, the master session key is passed down the stack to the AAA transport protocol via a standard EAP_API, such as those defined in [8]. The master session key is passed from the AAAH to the AP using suitable AAA transport, in this case Diameter. At the MT, the master session key is simply passed down from the EAP method to the link layer. The master session key is then known to both the AP and the MT, and used according to the needs of the specific WLAN technology. Guidelines and issues associated with key download are described in [9].

- **Encryption Key Derivation or Validation**

The master session key known at the AP and the MT is used in a technology dependent way to either validate capability exchanges and previously established encryption keys, or used to generate a new encryption key. In the latter case, encryption may also be initiated across the air interface if not previously established.

6.1 Authentication Functions

The functions identified within the reference architecture for supporting authentication are as follows:

6.1.1 Authentication Functions

The Authentication Function is responsible for authenticating the MT, using subscription information associated with the user. The Authentication Function may be an interworking gateway between different authentication protocols, or the users actual home AAA server, but in either case the interface between it and the WLAN will be the same. It is possible for communication between the WLAN and the SPN to pass through a number of AAA proxies.

6.1.2 Attendant

The Attendant communicates with the MT to exchange credentials for authenticating the network and the MT. The Attendant does not have direct access to the information needed to verify the user credentials, so passes the request to the Authenticator. The Attendant is expected to be able to establish secure channels for the purposes of exchanging the authentication information.

If any of the internal interfaces used for authentication purposes become visible, they must also be protected from external interference.

The Attendant maintains information including the following: -

- Secure Link Information: the WLAN should set up secure links to the user's service provider network in order to exchanges authentication information with external network functions and requires data such as secure link keys. The establishment of secure transport will allow the service provider network to verify the identity of the WLAN.
- MT Authentication Information: the WLAN needs to maintain information indicating the authentication state associated with the MT, and any key information downloaded to the WLAN by the authentication server for the purposes of verifying or deriving encryption keys.

6.1.3 MT Authenticator

The details of the MT internal implementation are not considered in this specification. However, it is required to support many different authentication scenarios (e.g. with many different core network types) and each of these implies a particular type of user credentials and possibly storage of credentials. It is therefore helpful to separate the functionalities of:

- Support of the protocol carrying authentication-related messages – this protocol runs between the MT and WLAN over the air interface and is then relayed by the WLAN over the L interfaces. Therefore the protocol used has to be considered within the scope of this specification to ensure that W.2 can support the transportation of this protocol and associated information.
- Management of the user information within the MT, including triggering the protocol over the air interface and so on. This will be at least partly specific to the type of core network that is being connected to; for example, tight security coupling to the UMTS R5 CN would imply the use of a UICC.

In order to separate these two functionalities, we introduce the concept of a local Authenticator function within the MT. The Authenticator function interfaces to a UICC, or SIM, or other user information management functions, via the M*s* interface. This interface will not be realised by a protocol; however, the sequence of events and semantics of data transferred over this interface should be defined as part of the reference architecture. These can then be mapped to specific information flows in particular interworking scenarios.

The Authenticator is responsible for retrieving client credentials and using them in the authentication process between the MT and the WLAN. This function is intended to hide the specifics of the WLAN implementation from the user credential management function, and allows different implementations of these functions to be used as desired.

6.2 Backwards Compatibility with RADIUS and CHAP

Several existing WLAN systems currently utilise RADIUS[10] for transporting authentication information to backend servers in the service provider network. Some of these systems may use EAP, while others may use 'legacy' authentication protocols (e.g. variants of CHAP[11]).

The current working assumption is that a newly developed Ls interface should be based on the Diameter protocol, since this provides enhanced functionality compared to RADIUS. There are two basic aspects to interworking a Diameter based system with existing RADIUS based networks:

1. Interwork from a (legacy) RADIUS WLAN to a (WIG) Diameter SPN.
2. Interwork from a (WIG) Diameter WLAN to a (legacy) RADIUS SPN.
3. In some roaming cases, both of these may be needed[1].

All of these cases essentially reduce to the question of Diameter-RADIUS interworking.

If the higher layer authentication exchange is based on an EAP message exchange (for any EAP method), then a trivial interworking device can be placed at the edge of the WLAN network that simply encapsulates the EAP messages into Diameter (see Figure 7).

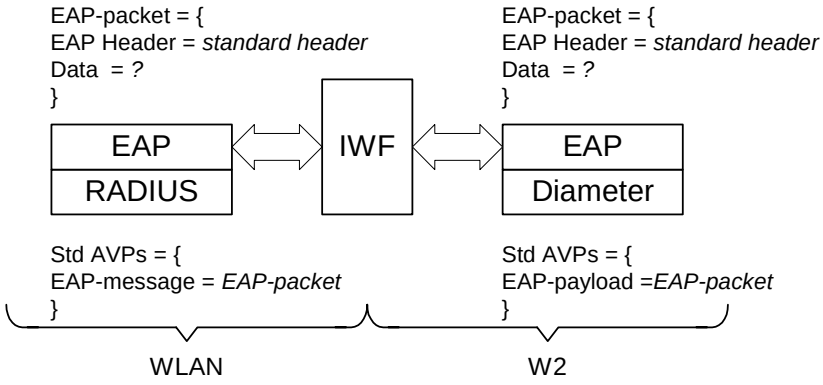

Figure 7: Diameter-RADIUS Interworking for EAP

If the higher layer authentication protocol is based on a different, such as CHAP, the IWF must be more complex. There are a number of options for handling this situation:

1. Carry the CHAP information directly in Diameter AVPs. The implications of this are that any additional information elements that need to be exchanged end-to-end that cannot be transported by pre-defined Diameter AVPs will need to have new AVPs defined. The transparency of what information is being transported between the MT and the AAAH is lost. This would not comply with a W.2 definition that mandated an EAP application for Diameter.
2. Carry CHAP in new EAP method. The EAP method would need to be defined, but the actual authentication method used is transparent to Diameter and the W.2 interface.

[1] An alternative is for RADIUS traffic to be routed directly.

Note in either of the above cases, the AAAH must support the CHAP authentication mechanism, and must be able to interpret the information provided by the Diameter messages or new EAP method. Alternatively, another IWF can be placed at the edge of the SPN to interwork directly from the W.2 interface to the SPN internal authentication mechanisms.

It is possible to consider RADIUS as an alternative protocol for use across W.2; however, there are a number of implications for the use of RADIUS that need to be considered (see [3]), not least:

- RADIUS does not support re-authentication initiated by the SPN
- Transport security has no confidentiality
- RADIUS does not protect data objects passed through it, and is open to man in the middle attacks.

Thus a number of security requirements outlined in A.1 are not satisfied. The former issue may also cause an issue for W.2 compliant SPNs that expect to be able to re-authenticate users on request. The request will reach the IWF at the edge of the WLAN, and cannot be converted into an equivalent RADIUS message.

7 Authorisation (L*p* Interface)

Authorisation is used to determine whether a user is allowed to access the services of the access network, and what level of service they are able to request. Subscription information is stored in the user's service provider network, and can be downloaded to the access network when the user has been authenticated. Alternatively, the WLAN may choose to request per-session authorisation from the service provider network as and when session requests are received from the MT.

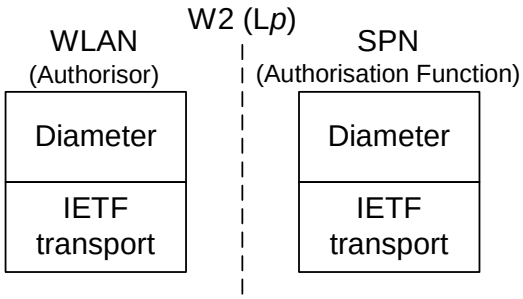

Figure 8. Protocol Stacks at the Lp Interface

Diameter has been selected for use across L*p* to transport the authorisation information. For the purpose of this document and the W.2 interface definition, we restrict the scope of 'authorisation' to the enabling/disabling of particular packet streams to and from the MT; in other words, authorisation can be encapsulated as a set of packet filter rules, in which case existing Diameter applications probably support the AVPs necessary.

Authorisation information may be "pushed" into the WLAN by the service provider after authentication has completed, and any time after that when the policy associated with the user changes. Alternatively (or in combination with), the WLAN may dynamically request authorisation decisions from the SPN on service requests received from the MT if the WLAN is not able/permitted to authorise a particular service request.

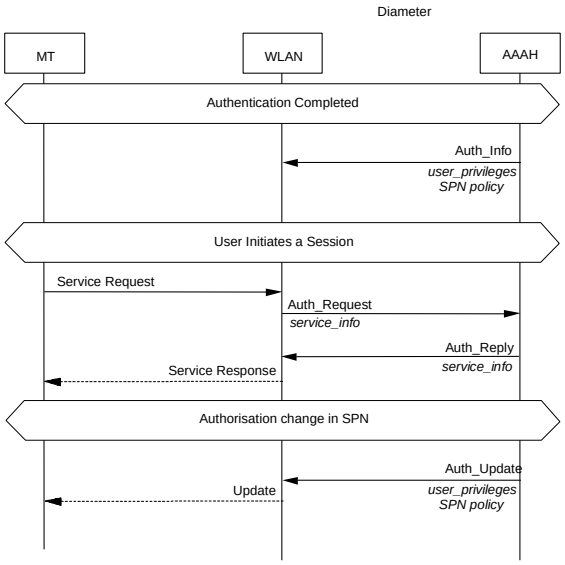

Figure 9. Authorisation

Closely related to authorisation function, policy information may be provided about how to provision a particular authorised service in the WLAN. For the purpose of this document, and the definition of the W.2 interface, policy information relates to any special treatment that should be applied to a packet, beyond the choice between dropping it or forwarding it with best efforts service. Policy control is outlined in section 7.2.

7.1 Authorisation Functions

7.1.1 Authorisation Function

The Authorisation function enables the service provider network to indicate to the access network and user whether the user is authorised to use the requested services and resources based on its subscription and network relationships. Policy information regarding the provisioning of the service is not included in the function. The subscription information is managed by the service provider with whom the user is registered. The authorisation function is also responsible for updating the access network of MT's authorisation state in case of any change in subscription or network status. The authorisation state of the MTs may be used by WLAN internal network functions for admission control purposes.

7.1.2 Authoriser

The authoriser maintains authorisation state of users connected to the AP, and may provide information to the policy control functions, the Policy Enforcement and the Policy Decision function, to control access to the WLAN network and the core network. Information regarding user authorisation state is provided by the authorisation function.

7.2 Policy Control Functions

Figure 10 depicts the services that involved in the communication between two terminals. It is obvious that the inter-working function needs to coordinate the WLAN Bearer Service and the External Bearer Service according to the user's subscription information. From the diagram, it is clear that a translation and control function is necessary at the WLAN gateway, since this is the start of the WLAN Bearer service, and the junction of WLAN Bearer and External Bearer services. To this end, an interface is needed for conveying user related policy information to the WLAN. This policy information would be at a harmonized layer, and is therefore WLAN independent. The control function at the WLAN is responsible for interpreting the information, and localizing the decisions based on the requirements of the specific WLAN technology utilized.

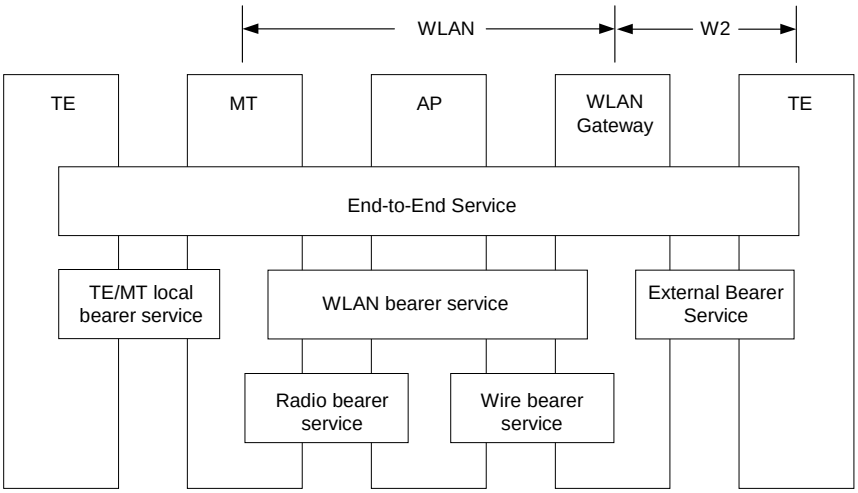

Figure 10: WLAN Policy Control

The transport protocol for the policy control functions could be COPS[12] as shown in Figure 11, since it is widely used for the policy control in other systems as well. This would allow the reuse of the techniques developed at the SPN, e.g. the Go interface at 3GPP[13].

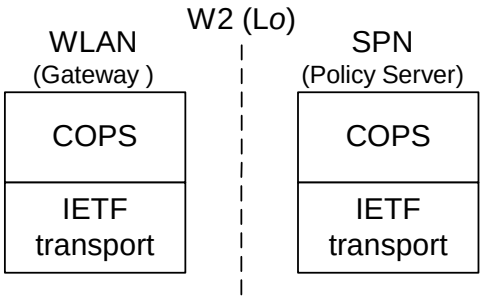

Figure 11: Lo Interface

8 Accounting (L*a* Interface)

Accounting is a user plane function that monitors the resource usage of a user in order to allow cost allocation, auditing and billing. The accounting is carried out according to a series of accounting and resource monitoring metrics, which are derived from policy and network management information.

Accounting information is collected by the WLAN and passed to the SPN where the information is used to support other accounting functions such as billing. The information must be passed securely across W.2 in order to ensure that no intermediate nodes can modify the information. The protocol stacks either side of the W.2 interface are illustrated in Figure 12.

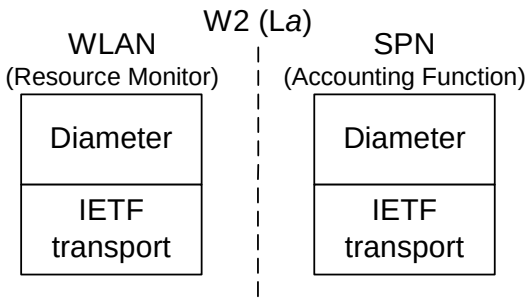

Figure 12. Protocol Stacks at the La Interface

Diameter is the protocol used for transporting the accounting information due to its support for secure transmission and extensibility to support the transfer of accounting records.

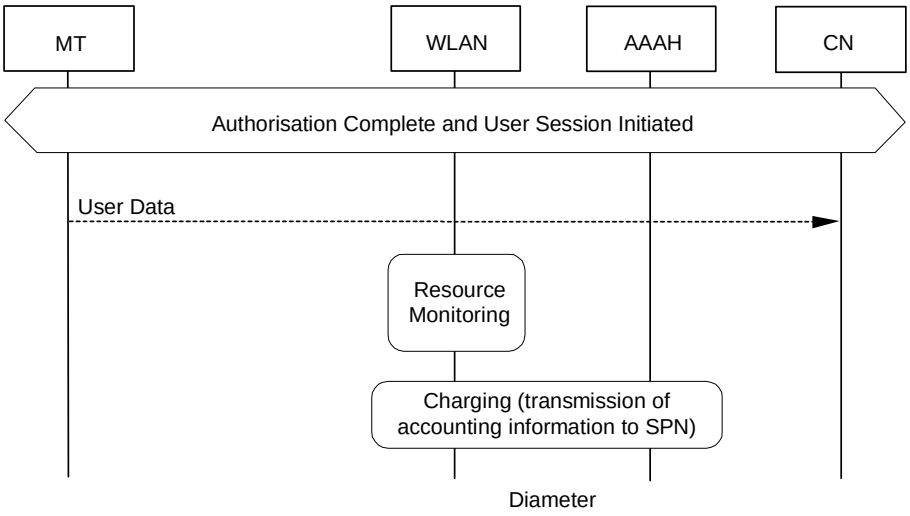

Figure 13. Accounting

Resource Monitoring is initiated within the WLAN after authentication/authorisation and once the user has initiated some user plane data sessions. The SPN may indicate what type of accounting should be performed for a particular user as part of the authorisation information, but this is optional and default accounting configurations should be used when this information is not passed to the WLAN.

Accounting information can be passed to the SPN in a number of modes:
- Realtime: to support hot billing and pre-paid services, accounting records associated with a session might be sent an a regular basis whilst the session is ongoing
- Per-session: this is the more usual mode where summary accounting records associated with a session are sent once the session has terminated
- Batch: the WLAN may store a series of records associated with a number of sessions and send them to the SPN in one transaction periodically.

The modes above can all be used simultaneously depending on the policy associated with particular session/service types and the policy associated with the user. The above modes will impact the amount and frequency of data sent across W.2.

8.1 Accounting Functions

The functions identified within the reference architecture for supporting accounting are as follows:

8.1.1 Accounting Function

The accounting function processes information passed to it from the WLAN and performs operations such as the summarisation of results and the generation of session records. This information may then be forwarded to other accounting functions within the network, for example a billing function.

8.1.2 Resource Monitor

The resource monitor is a user plane function responsible for measuring the resources consumed by a user when they are sending data via the WLAN. This function provides per user resource usage information for the purposes of billing, auditing, etc, although aggregated resource usage information could be monitored as well.

This information can be periodically sent to the Accounting Function or sent more rapidly if real-time accounting is supported and required by the service provider. The WLAN may monitor the following type of information:-

- Volume of traffic sent: this metric counts the number of packets or bytes sent by the user.
- Duration of the session: this metric is concerned with how long the session lasted.
- Bandwidth consumption: this metric could be concerned with measuring a user's peak bandwidth, their average bandwidth usage etc.
- Quality of Service provided: this metric records the QoS provided to a user's traffic flows.

As well as providing this data to the remote SPN for billing and auditing purposes, aspects of this information may also be passed to other local WLAN functions in order to provide better information on which to, for example, admission control decisions (although this is strictly a R2 function, and is not mentioned in further detail within this release).

9 User Data Forwarding

User Data Forwarding is concerned with transporting the user data to and from the MT across the WLAN to the correspondent network. It is represented in the reference architecture by the User Data Forwarding function and may be an IP router or an Ethernet switch.

Annex A (Informative): Requirements

The following Annex proposes some requirements associated with the Release 1 functionality that should be considered for the W.2 interface.

Note: it is not clear whether this document should include requirements on the W.2 interface. If it does, the following requirements present a starting point. The requirements section should not include WLAN-technology specific requirements, or requirements which are met at upper layers (except as background material).

A.1 Security and Authentication

The following section provides security related requirements that should be supported by the WLAN and the W.2 interface in order to provide a secure service.

A.1.1 Authentication Requirements

The following requirements are concerned with authentication of the user and network, and require support from both the WLAN technology and the W.2 interface.

SR01 It shall be possible for a user to continue to authenticate via the service provider network.

- This is a fundamental requirement for public access systems, and the WLAN and W.2 interface should support the relaying of user authentication information to the service provider network

SR02 It shall be possible to prevent intruders from obtaining unauthorised access to the network by masquerading as authorised users.

- Authentication of the user identity via a shared or private secret is considered sufficient to meet this requirement

SR03 It shall be possible for network providers to authenticate users at any time, such as when the user first enters the network and while the user is using the network

- Re-authentication procedures must be available between the AAAH and the MT, so support for this signalling is required across both W.2 and across the air interface

SR04 It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key.

SR05 Is shall be possible for the user to challenge the identity of the service provider network to which they are attached.

- The use of mutual authentication between the MT and SPN is necessary to meet this requirement

Note: protection of the permanent user identity is assumed to be the responsibility of the higher layer authentication protocols

A.1.2 Network Security Requirements

The following requirements are general security requirements that must be supported by the WLAN. Requirements that impact W.2 are also identified.

PR01 It shall be possible to detect and prevent the fraudulent use of the network. Audit logs of security related events will need to be produced.

- The WLAN must be able to determine whether a user accessing resources in the network is really who they say they are. This is a requirement on the AP, since this is the point of entry into the network through which all the traffic passes.

SR06 It shall be possible to prevent intruders from restricting the availability of services by logical means.

- The WLAN needs to provide adequate protection against Denial of Service attacks, such as limiting the rate at which the AP can accept and process attach and authentication requests

SR07 It shall be possible to protect against unauthorised modification of user traffic.

- Encryption of traffic across the air interface is needed to address this requirement. Across W.2, security mechanisms may also be deployed in order to encrypt user data across the network.

SR08 It shall be possible for the network to authenticate the origin of user traffic, signalling data and control data.

- As for SR08, since the MT and the AP, or the WLAN and the SPN/CN will share common keying information for data protection.

SR10 It shall be possible to protect against unauthorised modification of certain signalling data and control data including replay attacks.

- As for SR08.

SR11 It shall be possible to protect the confidentiality of certain signalling data and control data, including any data concerning the location of the user.

- As for SR08.

SR12 It shall be possible to protect the confidentiality of user traffic, including key refresh and multicast aspects.

- As for SR08.

A.1.3 Roaming Requirements

The following are the roaming requirements that are necessary to support public access systems.

SR13 It shall be possible for a user to connect to APs not operated by their service provider.

SR14 It shall be possible for the visited network to validate that the service provider network accepts responsibility for attaching the user.

- A trust context between the AN and the SPN must be established across W.2 within which authentication, authorisation and accounting procedures can take place. The protocols used to support control plane signalling to the SPN must be capable of establishing such a context or utilising a pre-existing one.

SR15 It shall be possible for the service provider network to validate that the user has attached to the visited network and used the resources reported.

- See SR14.

A.1.4 Summary Requirements on Ls

From the above requirements, it can be seen that the Ls interface must provide the following functionality:
- Support for relaying authentication signalling exchanges securely between WLAN and the SPN
- Support for transport of re-authentication signalling exchanges
- Support for key download from SPN to WLAN
- Establishment of trust relationship between SPN and AN

A.2 Charging and Accounting

The following sections outline requirements for the W.2 interface with regard to support for accounting and charging functionality. Accounting is defined as the process of collecting resource usage measurements within

the WLAN and apportioning charges for joint service between interworking an/or co-operating service/network providers. Charging is the function whereby access/session information is formatted and transferred from the WLAN to the SPN in order to make it possible to determine usage for which the subscriber may be billed.

Charging and Accounting functions require no direct support at the air interface.

A.2.1 Accounting Requirements

The following are requirements on the WLAN resource monitoring function regarding the functionality that it is required to support.

AR1 The accounting system must be able to handle Intra-domain accounting

- Where intra-domain accounting process involves the collection of information on resource usage within an administrative domain, for use within that domain. In intra-domain accounting, accounting packets and session records typically do not cross administrative boundaries and can be used to bill the user directly for services.

AR2 The accounting system must be able to handle Inter-domain accounting

- Inter-domain accounting process involves the collection of information on resource usage within an administrative domain, for use within another administrative domain. In inter-domain accounting, accounting packets and session records will typically cross administrative boundaries.

AR3 The accounting information must be of common format, due to the Intra-and Inter-domain accounting. For the sake of efficiency, the accounting record format used to transport the accounting information must be compact

- This format will need to be carried by the protocol used across W.2.

AR4 A standard accounting record format must be able to encode metrics commonly used to determine the user's bill. Since these metrics change over time, the accounting record format must be extensible so as to be able to add future metrics as they come along. The record format must support both standard metrics as well as vendor-specific metrics. The metrics must include all information expected by the 3G network for billing purposes.

- The L*a* protocol will also need to be able to easily adapt to changes in accounting record format that it is expected to transport.

AR5 Real time accounting and hot billing must be supported; due to it is a necessity in order to support fraud detection and risk management.

AR6 Accounting metric information must be maintained across node/network re-start.

A.2.2 Charging Requirements

The following charging requirements should also be supported at W.2.

AR7 Information about user charges shall be handled by the access/session contractor's equipment and/or by individual provider's equipment. Automatic transfer of information between the users' and the providers' equipment may be needed.

AR8 Accounting information that traverses administrative domain boundaries must be transferred securely.

A.2.3 Summary Requirements on L*a*

From the requirements above, it can be seen that the L*a* interface must support the following functionality:
- Secure transport of accounting information between the WLAN and the SPN
- Support for batch and real-time accounting messages
- Support for accounting record format and extensibility to cope with modifications to this format

A.3 Authorisation

Authorisation allows policy information related to the authenticated subscriber to be accessed by the WLAN for the purposes of controlling what WLAN network resources the user has access to.

A.3.1 Authorisation Requirements

PR01 It shall be possible for an AP to cause an immediate termination of the access provided to a user on instruction from the Core Network.

- If authorisation is revoked, the WLAN is expected to terminate the user's session immediately.

PR02 Authorisation should occur only after successful authentication.

PR03 The authorisation function should be able to identify the authenticated user to the service provider network and WLAN.

- This is to support correlating authorisation requests with authenticated users.

PR04 The authorisation function should be able to be carried out at different level, user level or application/service level, i.e. it should be able to authorise a user to use only certain services.

PR05 The authorisation function should be able to be initialised from either the service provider network or the WLAN.

- This is to support the two modes of operation, either authorisation information can be "pushed" into the WLAN by the service provider after authentication and on policy status changes in the SPN, or the WLAN may actively request authorisation decisions from the SPN on a per-user request basis.

PR06 Authorisation should support prompt status updating by allowing unsolicited messages.

In order to have a better understanding of the authorisation function, the information involved in the signalling can be identified as including the following:

- The authenticated identifier of the terminal to be authorised.
- The WLAN the authorised terminal currently stays in.
- The service type to be authorised. For inter-working, two more types needs to be defined, General Internet access, and Home Network Service access. Other service types defined in NASREQ could also be attached to this, but they may not be requirements for inter-working.
- The time the terminal is allowed to use the service. This could be stated as a single fixed time or as recurring times.
- The number of times the terminal is allowed to access the service.

A.3.2 Summary Requirements on L*p*

From the requirements above it can be seen that the L*p* interface must support the following functionality:
- Secure transport of authorisation information
- SPN initiated messages to pass information to the WLAN
- Dynamic retrieval of authorisation information from the SPN by the WLAN
- Flexible and extensible support for required authorisation parameters (but not so flexible as to replace policy aspects).

Annex B (Informative): Technology Overview

To be decided: if the WIG documentation should include information about the other standards or types of network with which this generic interworking standard could be used.

This would include two classes of network:
- ***WLAN and similar networks;***
- ***Public networks.***

If so, each participating body should probably propose informative text, including references to the relevant standards. The text would include description of how the W.2 functionality is actually supported, respectively:

- ***How the WLAN functionality (lower layers) enables W.2 to be implemented;***
- ***What interfaces within the public network are interworked with W.2.***