3GPP TSG SA WG3 Security — S3#29
San Francisco, USA 15 - 18 July 2003

Tdoc ⌘S3-030362

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**CRNum**	⌘ **rev**	**-**	⌘	Current version:	**0.5.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Alignment with WLAN architecture definition		
Source:	⌘	Ericsson		
Work item code:	⌘	WLAN	***Date:*** ⌘	16/06/2003
Category:	⌘	**F**	***Release:*** ⌘	Rel-6
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	Current version of TS 33.234 only reflects architecture for scenario 2. Scenario 3 defines more interfaces which will have some implications in SA3. It is needed then to allign TS 33.234 with TS 23.234 with the interfaces and nodes SA3 will work on. Also, requirements related to current tunneling issues are not covered yet in this specification.
Summary of change:	⌘	Network diagram and nodes descriptions in chapters 4.1.1 and 4.1.2 modified. Only the relevant interfaces for SA3 are shown. Requirements added in chapter 4.2
Consequences if not approved:	⌘	TS 33.234 inconsistent with SA2 specification (TS 23.234).

Clauses affected:	⌘	4.1 Security architecture and Roles				
		Y	**N**			
Other specs affected:	⌘	□	□	Other core specifications	⌘	
		□	□	Test specifications		
		□	□	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

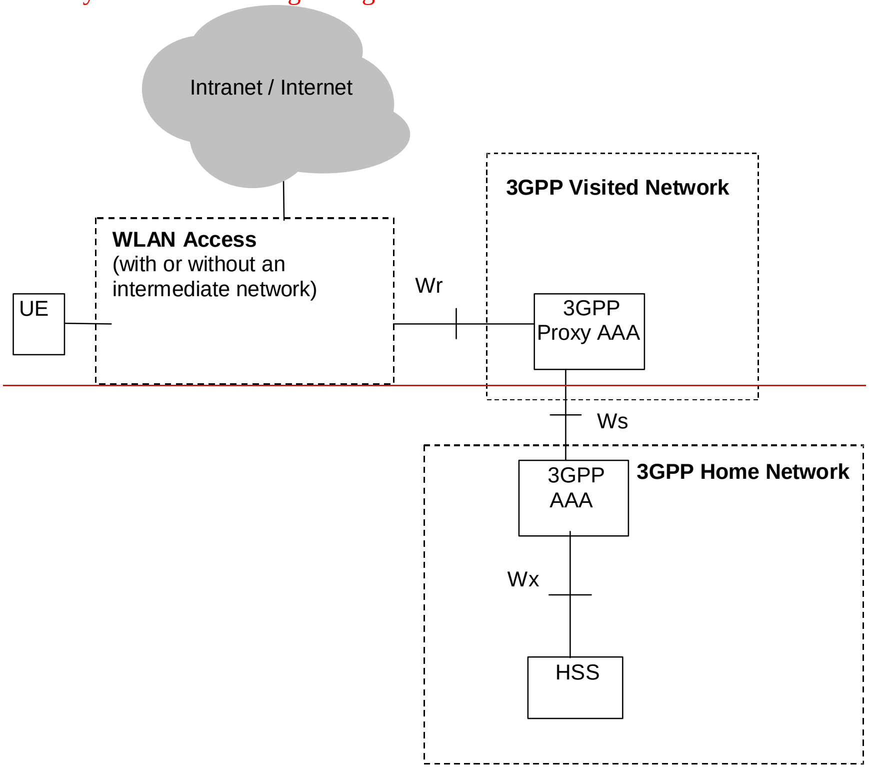
*** BEGIN SET OF CHANGES ***

4.1 Security architecture and Roles

Note: the pictures in this chapter may contain a shaded area, which surrounds the entities for scenario 3.

4.1.1 Non roaming WLAN interworking Reference Model

The home network is responsible for access control and tunnel establishment. ~~The Wx interface is intra-operator. The 3GPP network interfaces to, WLANs, via the Wr interface.~~
~~The 3GPP proxy AAA relays access control signalling to the home 3GPP AAA server via the Ws interface.~~



~~**Figure 4.1 Access Control Reference Model**~~

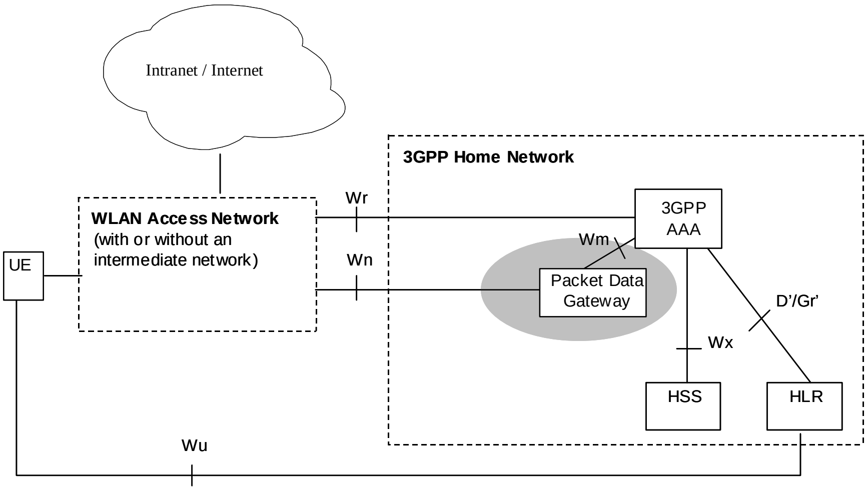


Figure 4.1 Non roaming reference model

4.1.2 Roaming WLAN Interworking Reference Model, access to HPLMN services

The home network is responsible for access control, although the VPLMN may take part in tunnel establishment (if one of the end points is the WAG).

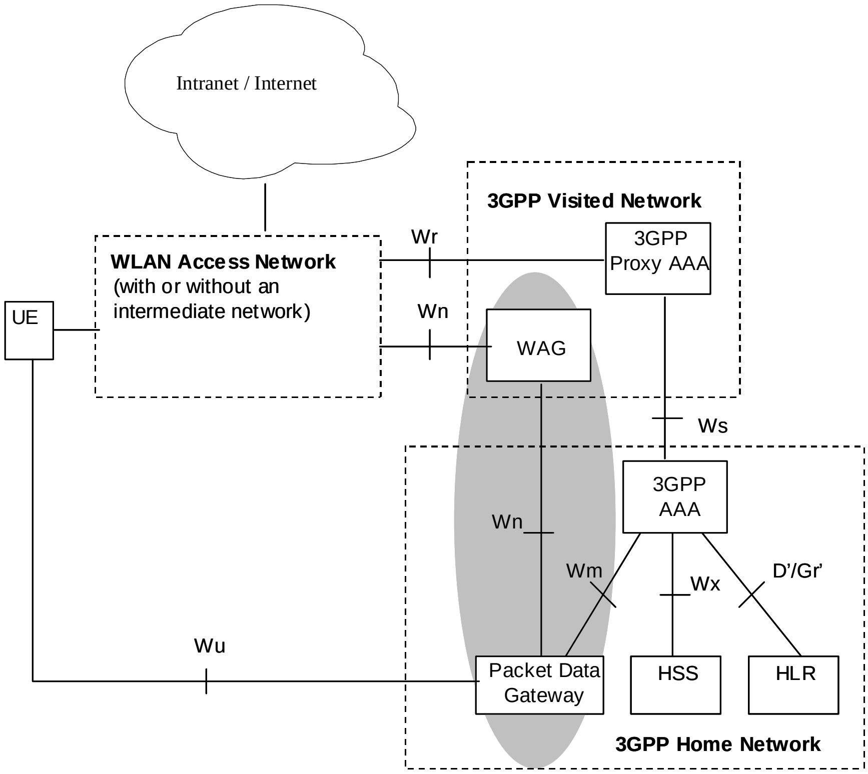


Figure 4.2 Roaming reference model, services in the HPLMN

4.1.3 Roaming WLAN Interworking Reference Model, access to VPLMN services

The home network is responsible for access control, but the authorization decision of tunnel establishment will be taken by the 3GPP proxy AAA based on own information plus information received from the home network. The VPLMN will take part in tunnel establishment (either the WAG or the PDGW).

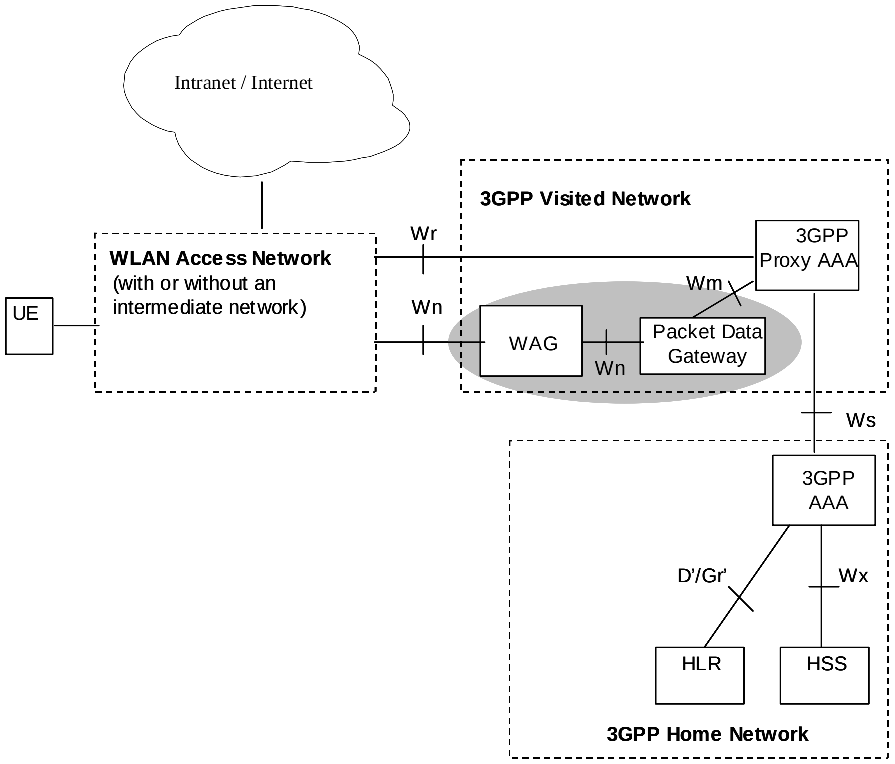


Figure 4.3 Roaming reference model, services in the VPLMN

4.1.4~~2~~ Network elements

The list below describes the access control related functionality in the network elements of the 3GPP-WLAN interworking reference model:

- The **WLAN-UE,** equipped with a UICC (or SIM card), for accessing the WLAN interworking service).
  - May be capable of WLAN access only
  - May be capable of both WLAN and 3GPP System access.
  - May be capable of simultaneous access to both WLAN and 3GPP systems

  [Editors note: definition of simultaneous access still TBA with SA1- LS in S3 030169] Reply to SA2 in S3-030188 provides some clarification

  - May be a laptop computer or PDA with a WLAN card, UICC (or SIM card) card reader, and suitable software applications,
  - May be functionally split over several physical devices, that communicate over local interfaces e.g. Bluetooth, IR or serial cable interface.

[Editors Note: All these alternatives must be carefully studied from a security perspective.]

- The **AAA proxy** represents a logical proxying functionality that may reside in any network between the WLAN and the 3GPP AAA Server. These AAA proxies are able to relay the AAA information between WLAN and the 3GPP AAA Server.
  The number of intermediate AAA proxies is not restricted by 3GPP specifications. The AAA proxy functionality can reside in a separate physical network node, it may reside in the 3GPP AAA server or any other physical network node.
- The **3GPP AAA server** is located within the 3GPP network. The 3GPP AAA server :

- Retrieves authentication information from the HLR/HSS of the 3GPP subscriber's home 3GPP network;
- Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies.

Communicates authorisation information to the WLAN potentially via AAA proxies.

- The **Packet Data Gateway (PDGW)** enforces tunnel authorization and establishment with the information received from the 3GPP AAA via the Wm interface.

*Note: The **WLAN Access Gateway (WAG)** responsibilities for security issues are related to tunnel establishment but this decision is pending to be taken.*

4.1.5 Reference points description

Wr

The reference point Wr connects the WLAN Access Network to the 3GPP Network (i.e. the 3GPP AAA Proxy in the roaming case and the 3GPP AAA server in the non-roaming case). The main purpose of the protocols implementing this interfaces is to transport authentication and keying information (WLAN UE - 3GPP network), and authorization information (WLAN AN – 3GPP network). The reference point has to accommodate also legacy WLAN Access Networks and thus should be Diameter or RADIUS based.

Wx

This reference point is located between 3GPP AAA Server and HSS. The main purpose of the protocols implementing this interface is communication between WLAN AAA infrastructure and HSS, and more specifically the etrieval of authentication vectors, e.g. for USIM authentication, and retrieval of WLAN access-related subscriber information from HSS. The protocol is either MAP or Diameter based.

D'/Gr'

This optional reference point is located between 3GPP AAA Server and pre-R6 HLR/HSS. The main purpose of the protocol implementing this interface is communication between WLAN AAA infrastructure and HLR, and more specifically the retrieval of authentication vectors, e.g. for USIM authentication, from HLR.. The protocol is MAP-based.

Wn

The definition of this reference point is for further study

Wm

This reference point is located between 3GPP AAA Server and Packet Data Gateway. The functionality of this reference point is to retrieve tunnelling attributes and UE's IP configuration parameters from/via Packet Data Gateway.

Ws

The reference point Ws connects the 3GPP AAA Proxy to the 3GPP AAA Server. This interface is similar to Wr, its main purpose is to transport authentication, authorization and related information in a secure manner.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

4.2.6 UE-initiated tunneling

The security features that are expected in a tunnel from the UE to the VPLMN or HPLMN will be:

- Data origin authentication and integrity must be supported.
- Confidentiality must be supported.
- The 3GPP network has the ultimate decision to allow tunnel establishment, based on:
    - The level of trust in the WLAN AN and/or VPLMN
    - The capabilities supported in the WLAN UE
    - Whether the user is authorized or not to access the services (in the VPLMN or HPLMN) the tunnel will give access to.
- The 3GPP network, in the setup process, decides the characteristics (encryption algorythms, protocols,...) under which the tunnel will be established.
- Keys used for tunnel establishment must be obtained from keying material previously obtained in user authentication.

Note: Authorization for the tunnel establishment is decided by the 3GPP AAA and enforce by the PDGW or WAG. Whether this authorization information is protected or not is FFS.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security — S3#29 **S3-030362att**
15 - 18 July 2003
San Francisco, USA

Title:	**DRAFT** LS on authorization information
Release:	Rel-6
Work Item:	3GPP-WLAN interworking
Source:	SA3
To:	SA2
Cc:	

Contact Person:

Name:	David Mariblanca
Represented company:	Ericsson
Tel. Number:	+34 646004736
E-mail Address:	david.mariblanca@ericsson.com

Attachments: None

1. Overall Description:

SA3 is analyzing SA2 TS 23.234 v1.10.0 in order to find out what kind of security impacts scenario 3 will carry to the current architecture. In chapter 5.5.1, it is written: *"Service authorization information shall be protected"*, which may lead to different interpretations.

2. Actions:

SA3 would like SA2 to clarify and specify more in detail what kind of protection is required for service authorization information.

3. Date of Next SA3 Meeting:

SA3#30	6th Oct – 10th Oct 2003	Portugal