3GPP TSG SA WG3 Security — S3#31 **S3-030676**
18 - 21 November 2003
Munich, Germany

3GPP TSG-SA WG2 meeting #35 **Tdoc S2-033813**
Bangkok, 27th – 31st October 2003

Title:	LS on Tunnel Establishment and Security Association
Release:	Rel-6
Work Item:	3GPP-WLAN interworking
Source:	SA2
To:	SA3
Cc:	

Contact Person:

Name:	Nicolas Martiquet
Represented company:	Orange
Tel. Number:	+33 1 45 29 51 69
E-mail Address:	nicolas.martiquet@rd.francetelecom.com

Attachments: None

1. Overall Description:

SA2 are currently studying the W-APN resolution and tunnel establishment issue under the working assumption of end-to-end tunnels as stated in the last SA plenary.

One possible architectural solution that was identified during SA2#35 is to introduce a new function called W-APN Resolution Gateway. This function would then be in charge of tunnel establishment signalling with the WLAN UE, including resolving the W-APN and authentication and authorisation of the WLAN UE (in cooperation with the AAA Sever). Therefore, there would be no exchange of tunnel establishment messages between the WLAN UE and the PDG, offering the possibility that policies at the WAG could by default block packets to the PDG from entering the inter-PLMN backbone.

On completion of the tunnel establishment signalling, security parameters derived during the tunnel establishment would be sent to the WLAN UE and the PDG. At this point, new policy would be applied at the WAG to allow tunnel data packets to flow towards the PDG. The UE could then begin sending tunnel data packets.

The main interest of this solution is to have the possibility of preventing packets from being sent to the PDG itself across the inter-PLMN backbone before the user is authenticated and authorised. Such packets would be allowed only towards the W-APN Resolution Gateway. In addition, the solution requires only one tunnel establishment procedure and so minimises the time taken for tunnel establishment.

However, the solution relies on the assumption that it is possible to separate the tunnel establishment and tunnel data handling into separate nodes, noting that these nodes are both in 3G networks, and not linked over the public internet. Additionally, no decision has been made on whether the W-APN Resolution Gateway would be located in the VPLMN or HPLMN and therefore these nodes may not necessarily be in the same PLMN.

This assumption needs feedback from SA3 in order to make sure that these mechanisms do not compromise the tunnel security, in particular the fact that tunnel data needs to be sent towards a different node from the node involved in the tunnel establishment and key agreement.

Additionally, SA2 would welcome feedback on

- the security advantages offered by protecting the PDG before user authentication/authorisation in the way described above
- whether the W-APN Resolution Gateway would become a single point of failure.

The corresponding proposed reference model and signalling flow have not been agreed by SA2 yet, however they are shown for information in the annex of this Liaison Statement.

2. Actions:

SA2 kindly request SA3 to evaluate the assumption above and to provide feedback to SA2.

3. Date of Next SA2 Meeting:

SA2#36	24th – 28th November 2003	New York – USA
SA2#37	12th – 16th January 2004	Innsbruck - Austria

4. Annex:

Proposed reference model update

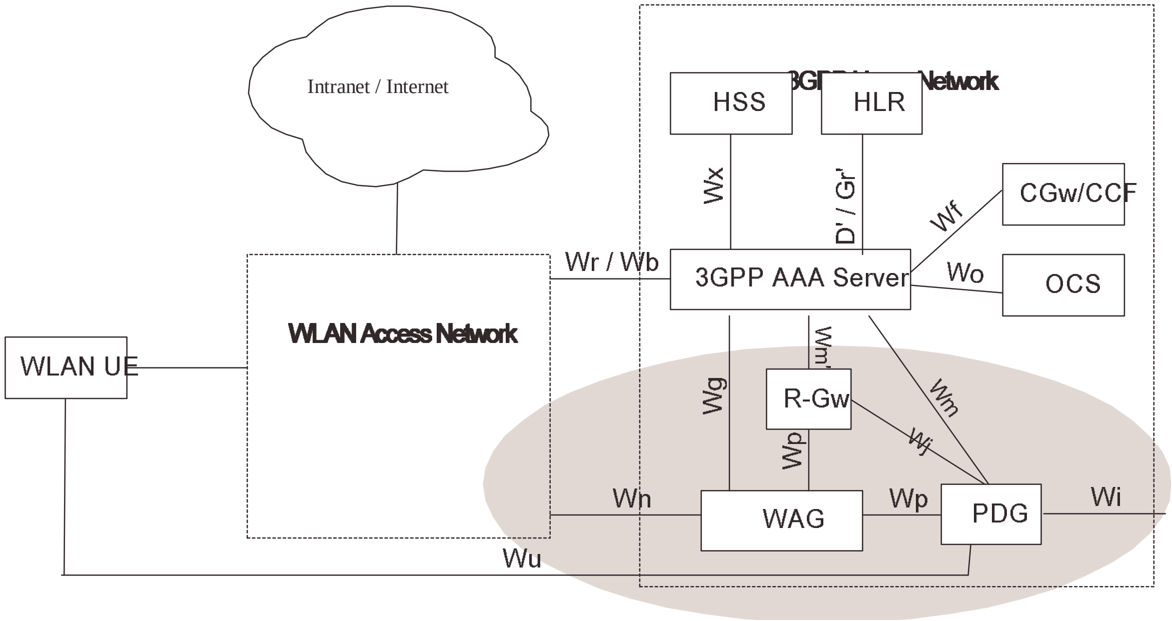


Figure 6.1 Non Roaming Reference Model.

The shaded area refers to scenario 3 functionality

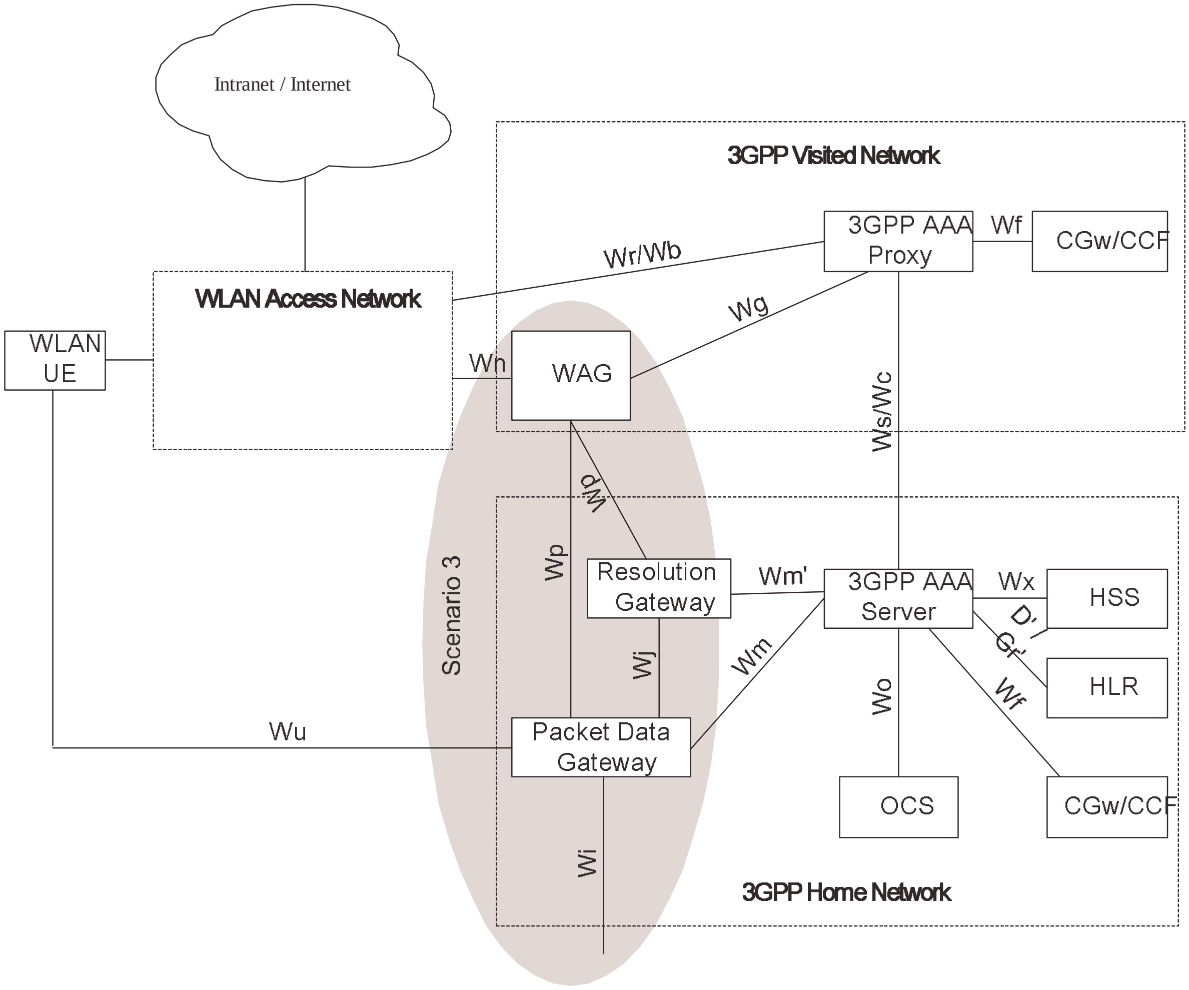


Figure 6.2a. Roaming Reference Model- 3GPP PS based services provided via the 3GPP Home Network (the shaded area refers to scenario 3 functionality)

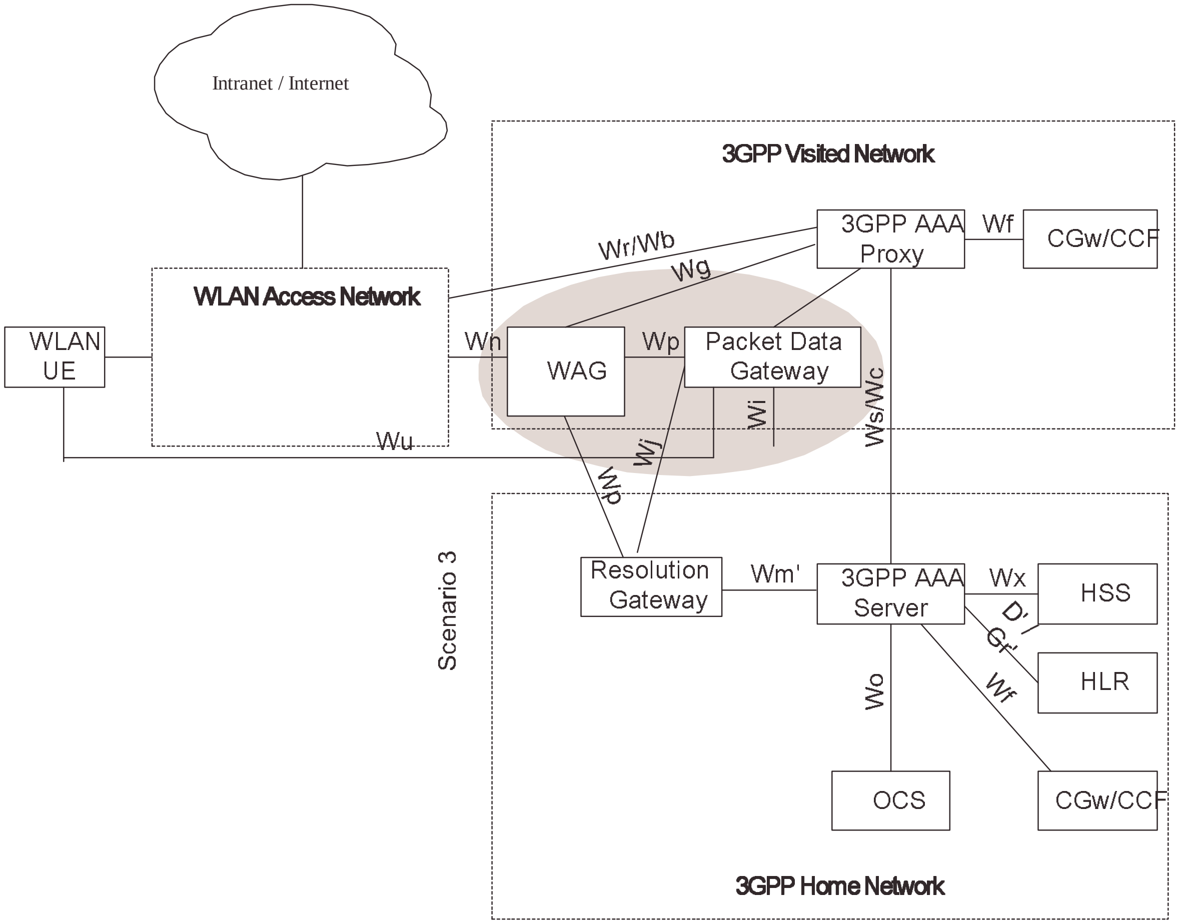


Figure 6.2b. Roaming Reference Model- 3GPP PS based services provided via the 3GPP Visited Network (the shaded area refers to scenario 3 functionality)

Description of W-APN Resolution gateway

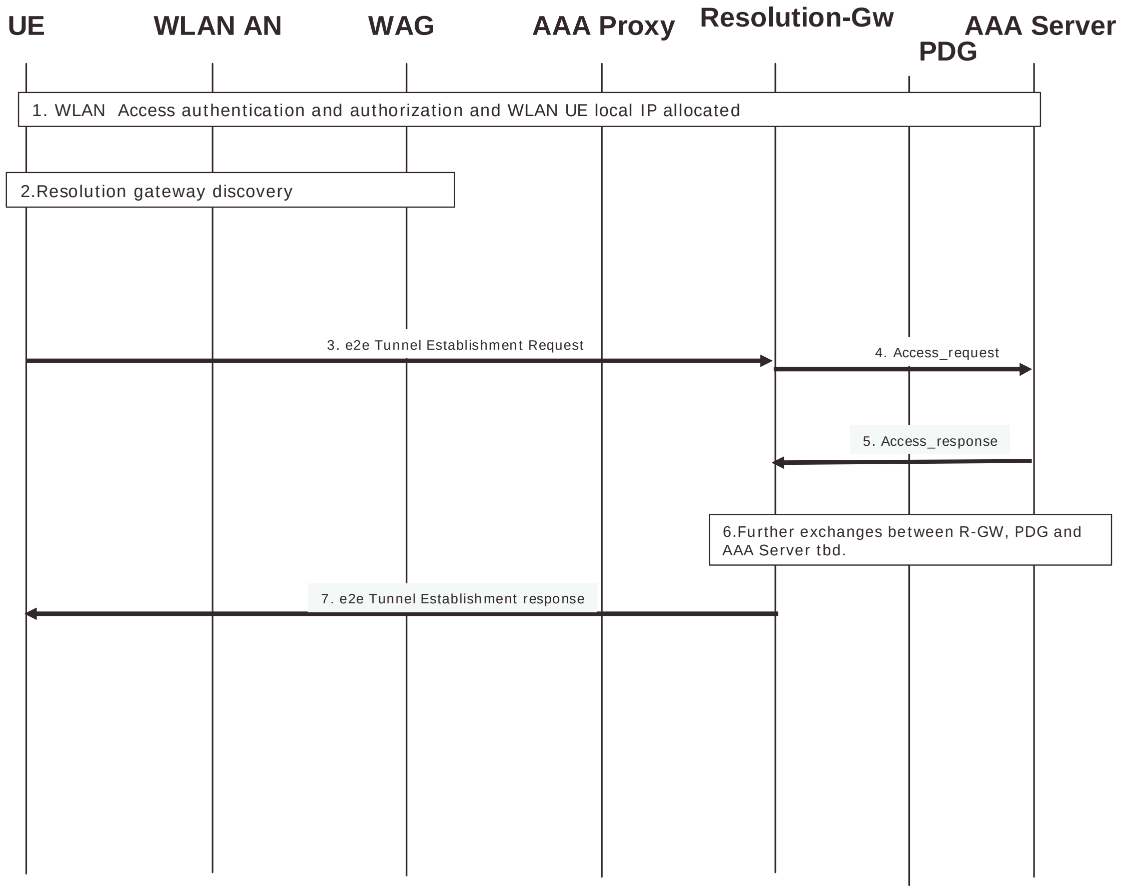
The W-APN resolution gateway

- Process the service request from the UE, interact with 3GPP AAA server to resolve and authorize a PDG for the WLAN UE.

- Help tunnelling establishment between the UE and the authorized PDG

Main message flow interaction:

The R-GW refers to the W-APN Resolution Gateway.


UE
WLAN AN
WAG
AAA Proxy
Resolution-Gw
PDG
AAA Server
1. WLAN Access authentication and authorization and WLAN UE local IP allocated
2.Resolution gateway discovery
3. e2e Tunnel Establishment Request
4. Access_request
5. Access_response
6.Further exchanges between R-GW, PDG and AAA Server tbd.
7. e2e Tunnel Establishment response

1. The user is authenticated and authorised for basic WLAN access. If the user has Scenario 3 access, then they will be provided with access to the VPLMN.
2. When the user decides to access a service, the WLAN UE builds the requested W-APN associated to the service requested by the user. The W-APN Resolution Gateway is pre-configured in the WLAN UE.
3 The WLAN UE sends a tunnel establishment request to the W-APN Resolution Gateway, including the requested W-APN.
4. The W-APN Resolution Gateway sends a service authorization request to the 3GPP AAA Server, including the requested W-APN and user identity from the tunnel establishment request. Additional exchanges between the WLAN UE and the 3GPP AAA Server (via the W-APN Resolution Gateway) may be required to complete authentication of the user.
5. The 3GPP AAA Server authorizes the service to the WLAN UE and sends the authorized PDG address to the W-APN Resolution Gateway.
6. (option1) The 3GPP AAA Server informs the W-APN Resolution Gateway that the user is authorized to be served by a PDG, and the related security /tunneling information is also included (These information can be include in the step5). The W-APN Resolution Gateway then includes the necessary information requests allocation of the necessary tunnel resources at the PDG (e.g. SPI or port number allocation) .

(option 2) The 3GPP AAA Server push to the selected PDG with the information indicating that the user is authorized to access the service through it, together with related security/tunneling attributes or information. The address of the W-APN Resolution Gateway is also included then the PDG can respond to the correct W-APN Resolution Gateway in step7, So, the W-APN Resolution Gateway does not need to retrieve or understand the security parameters, so the answer from the PDG to the WLAN UE can be encrypted, to avoid the Resolution gateway to be trusted.

7. The W-APN resolution Gateway (or the PDG answering through the W-APN Resolution Gateway) responses to the WLAN UE, including the PDG address and tunnel attributes, and security parameters to the WLAN UE.

After this, the tunnel between PDG and the WLAN UE is established, and the W-APN Resolution Gateway is no longer involved in further interaction between them.