3GPP TSG SA WG3 Security — S3#36 *Tdoc ⌘S3-040959*
November 23 – 26, 2004

Shenzhen, China

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **048** ⌘**rev** **-** ⌘ Current version: **6.2.1** ⌘

*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:	⌘	Removal of word “scenario”
Source:	⌘	Samsung and Nokia
Work item code:	⌘	WLAN
Date:	⌘	09/11/2004
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:	⌘	In SA3#35 meeting, LS S3-040701from SA2 recommends to replace the work “scenario” with an alternate word in TS 33.234, because it is just the term to distinguish possible steps in developing/deploying I-WLAN.
Summary of change:	⌘	To replace the word “scenario” with alternate words simailar to TS 23.234 and TS 22.234.
Consequences if not approved:	⌘	TS 33.234 is not aligned with the TS 22.234 and TS 23.234

Clauses affected:	⌘	3.1, 4.1.1, 4.1.2, 4.1.3, 5.1.1, 5.1.6, 5.1.8, 5.2.1, 5.2.2, 5.3.1, 6.1.5, 6.2.1, 6.2.2, 6.3.1, 6.3.2, 6.5, Annex E
Other specs affected:	⌘	Y N ☐ X Other core specifications ☐ X Test specifications ☐ X O&M Specifications
	⌘	
Other comments:	⌘	

*** BEGIN SET OF CHANGES ***

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

WLAN coverage: an area where wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.

WLAN-UE: user equipment to access a WLAN interworking with the 3GPP system, including all required security functions.

WLAN Direct IP Access: Access to an IP network is direct from the WLAN AN.

WLAN 3GPP IP Access: Access to an IP network via the 3GPP system

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

4.1.1 Non roaming WLAN interworking Reference Model

The home network is responsible for access control and tunnel establishment.

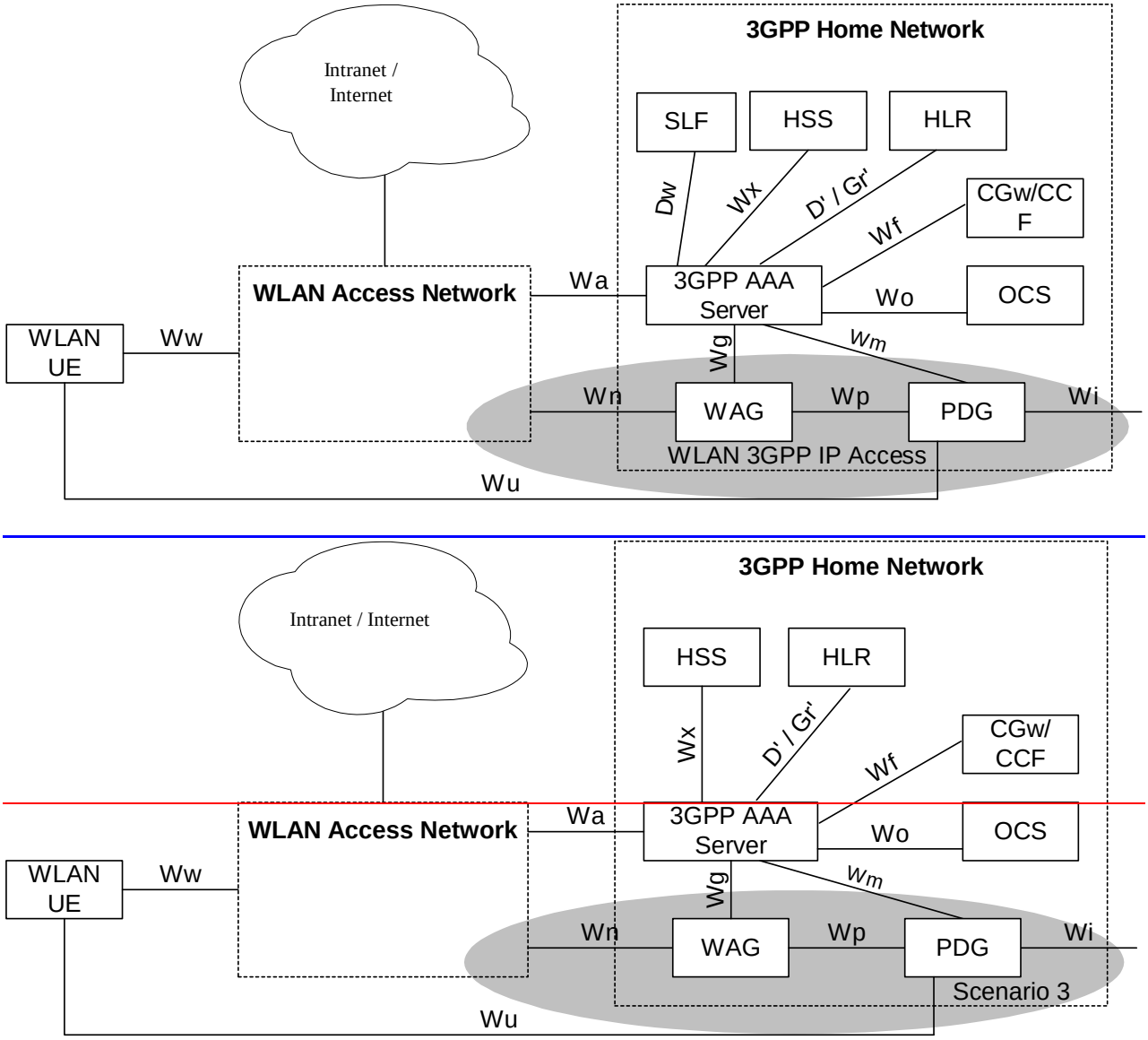
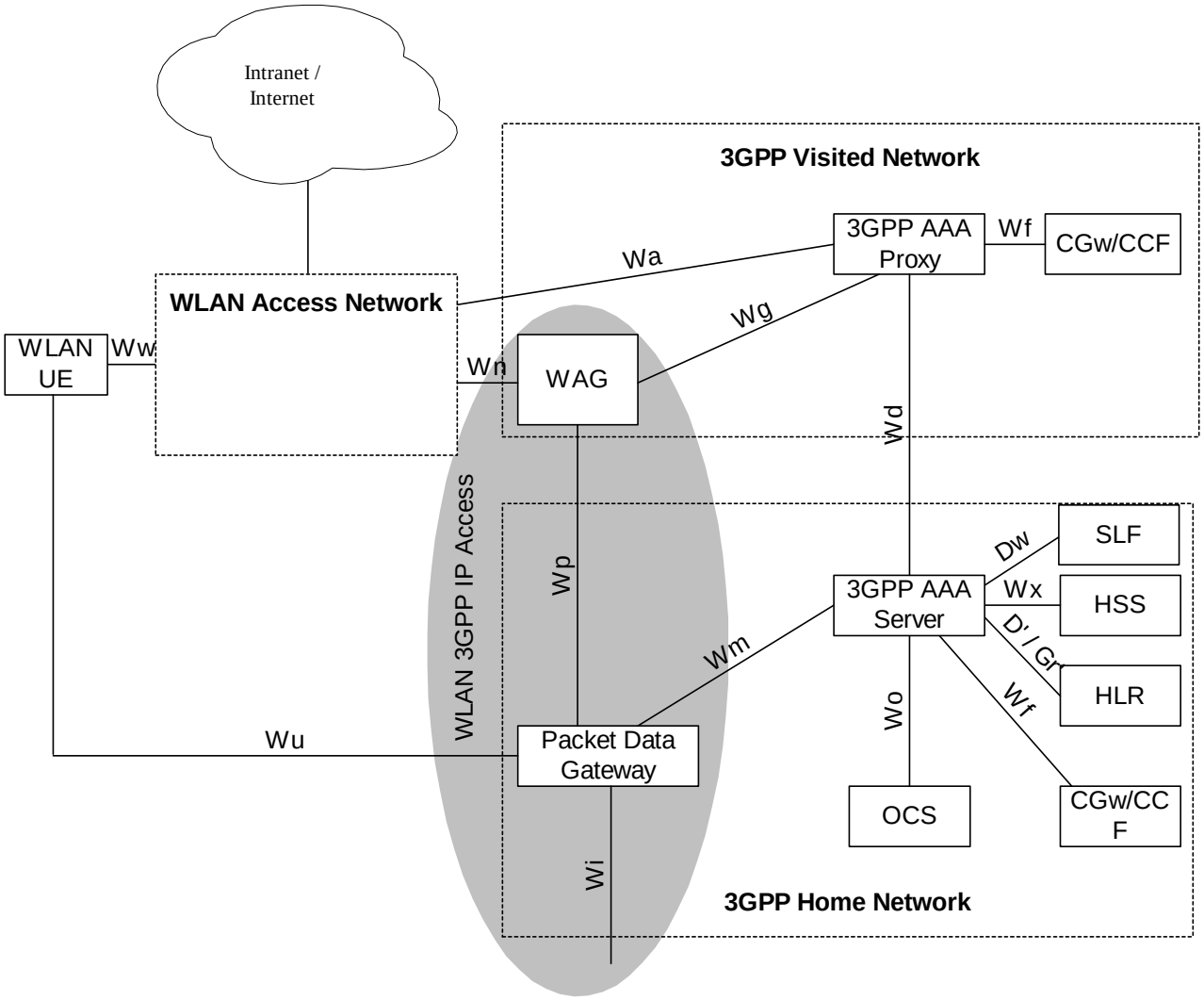


Figure 1: Non-roaming reference model (the shaded area refers to ~~scenario 3~~WLAN 3GPP IP Access functionality)

4.1.2 Roaming WLAN Interworking Reference Model, access to HPLMN services

The home network is responsible for access control and tunnel establishment. The traffic is routed through the visited network (using the WAG).


Intranet / Internet
3GPP Visited Network
3GPP AAA Proxy
Wf
CGw/CCF
Wa
WLAN Access Network
Wg
WLAN UE
Ww
Wn
WAG
Wd
WLAN 3GPP IP Access
Wp
SLF
Dw
3GPP AAA Server
Wx
HSS
D'/Gr'
Wm
HLR
Wo
Wf
Wu
Packet Data Gateway
OCS
CGw/CCF
Wi
3GPP Home Network

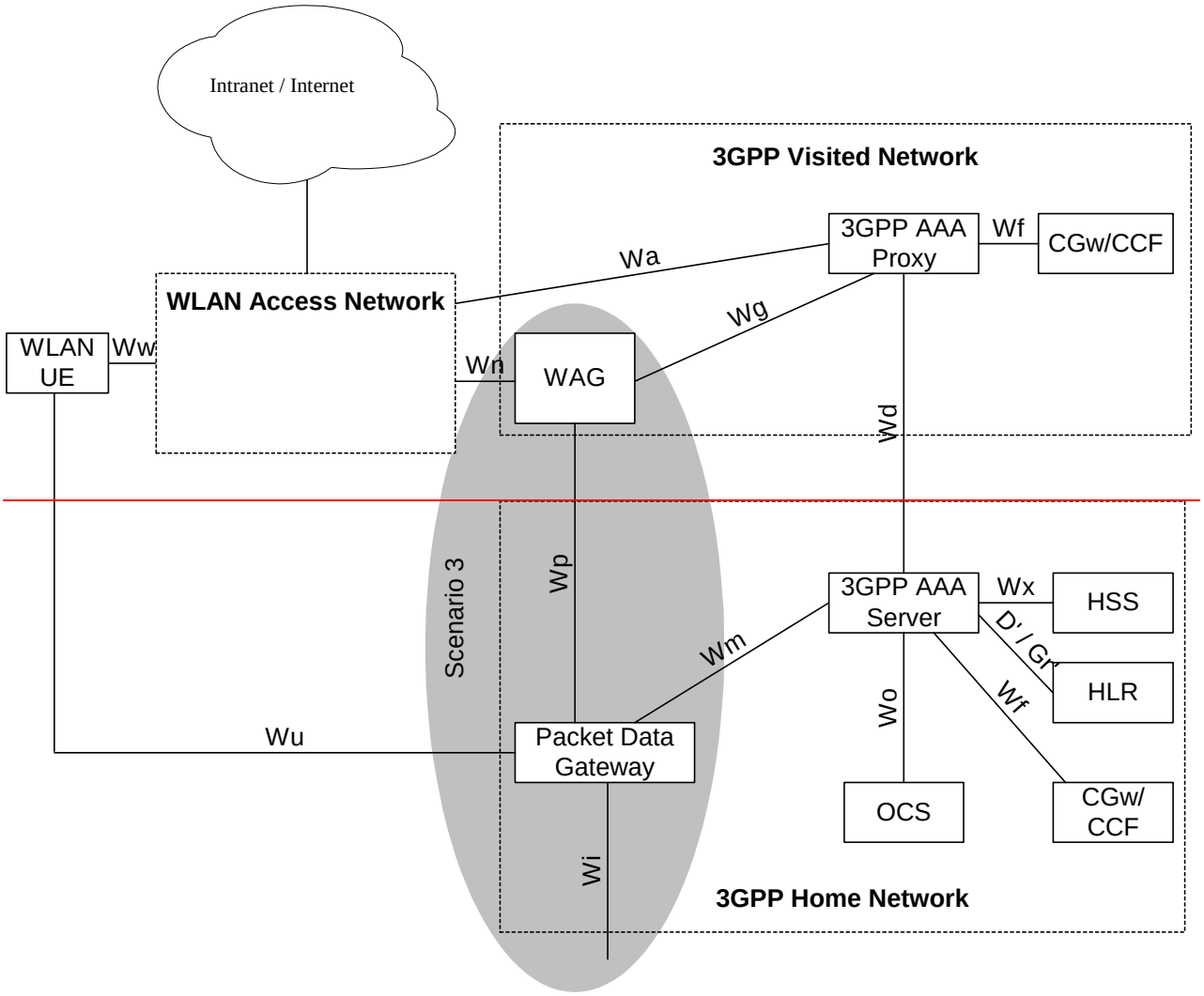
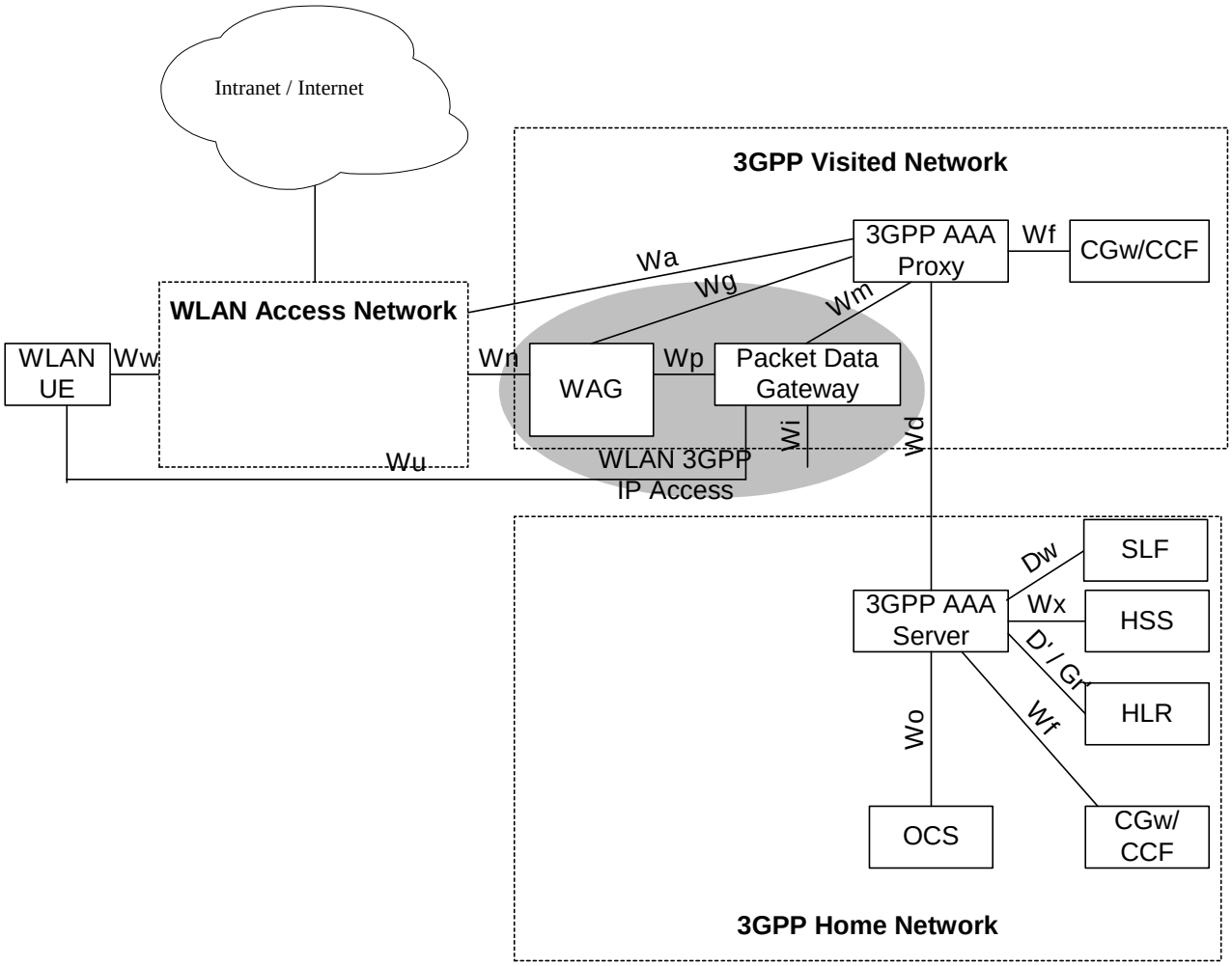


Figure 2: Roaming reference model - 3GPP PS based services provided via the 3GPP Home Network (the shaded area refers to ~~scenario 3~~WLAN 3GPP IP Access functionality)

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).


Intranet / Internet
3GPP Visited Network
3GPP AAA Proxy
Wf
CGw/CCF
Wa
Wg
Wm
WLAN Access Network
WLAN UE
Ww
Wn
WAG
Wp
Packet Data Gateway
Wi
Wd
Wu
WLAN 3GPP IP Access
Dw
SLF
3GPP AAA Server
Wx
HSS
D' / Gr'
HLR
Wo
Wf
OCS
CGw/ CCF
3GPP Home Network

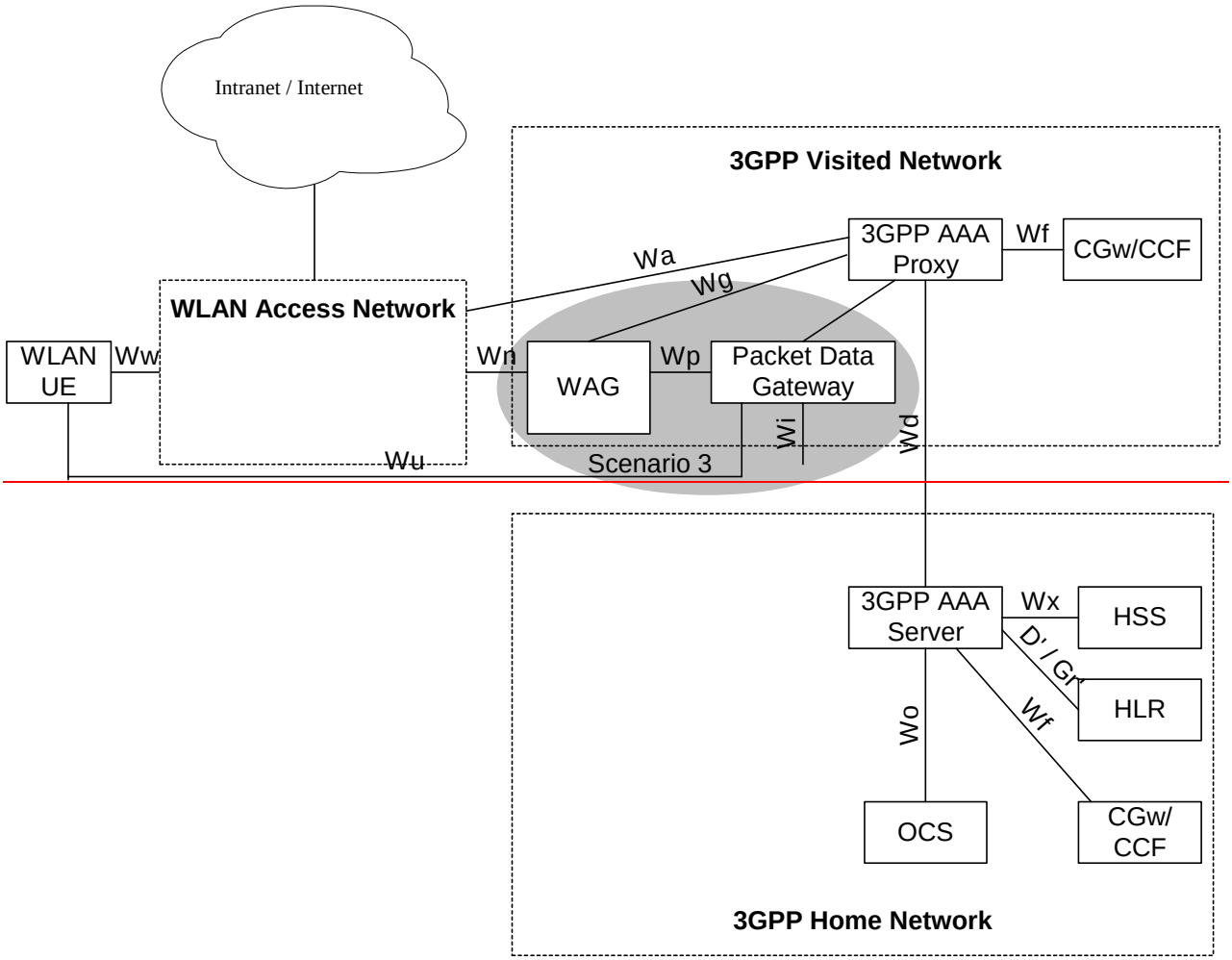


Figure 3: Roaming reference model - 3GPP PS based services provided via the 3GPP Visited Network (the shaded area refers to ~~scenario 3~~WLAN 3GPP IP Access functionality)

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

4.2.6 UE-initiated tunnelling

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 algorithms, protocols) under which the tunnel will be established.

NOTE: Authorization for the tunnel establishment is decided by the 3GPP AAA and enforced by the PDG~~W~~ or WAG. Whether this authorization information is protected or not is FFS.

Working assumptions:

1. The security mechanisms used in context with the IP tunnel in ~~scenario 3~~WLAN 3GPP IP Access are to be independent of the link layer security in ~~scenario 2~~WLAN Direct IP Access.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.1.1 End to End WLAN Access Authentication (~~Scenario 2~~WLAN Direct IP Access)

WLAN access authentication signalling is executed between WLAN-UE and 3GPP AAA Server. This authentication signalling shall be independent on the WLAN technology utilised within WLAN Access network. WLAN authentication signalling for 3GPP-WLAN interworking shall be based on Extensible Authentication Protocol (EAP) as specified in RFC 2284 (ref. [3]).

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.1.6 User Identity Privacy in WLAN Access

User identity privacy (Anonymity) is used to avoid sending any cleartext permanent subscriber identification information which would compromise the subscriber's identity and location on the radio interface, or allow different communications of the same subscriber on the radio interface to be linked.

User identity privacy is based on temporary identities (pseudonyms or re-authentication identities). The procedures for distributing, using and updating temporary identities are described in ref. [4] and [5]. Support of this feature is mandatory for implementation in the network and WLAN UE. The use of this feature is optional in the network, but mandatory in the WLAN UE.

The AAA server generates and delivers the temporary identity and/or the re-authentication identity to the WLAN-UE as part of the authentication process. The WLAN-UE shall not interpret the temporary identity; it shall just store the received identifier and use it at the next authentication. Clause 6.4 describes a mechanism that allows the home network to include the user's identity (IMSI) encrypted within the temporary identity.

When the WLAN-UE receives one temporary identity issued by the AAA server, it shall use it in the next authentication. The WLAN-UE can only use the permanent identity when there is no temporary identity available in the WLAN-UE. A temporary identity is available for use when it has been received in last authentication process. Temporary identities received in earlier authentication processes have to be cleared in the WLAN-UE or marked so that they can only be used once. If the WLAN-UE does not receive any new temporary identity during a re-authentication procedure, the WLAN-UE shall use a previously unused pseudonym, if available, for the next full re-authentication attempt.

If the WLAN-UE receives from the AAA server more than one temporary identity (a pseudonym and a re-authentication identity), in the next authentication procedure, it will use the re-authentication identity, so that the AAA server is able to decide either to go on with a fast re-authentication or to fallback to a full re-authentication (by requesting the pseudonym to the WLAN-UE). This capability of decision by the AAA server is not possible if the WLAN-UE sends the pseudonym, since the AAA server is not able to request the re-authentication identity if it decides to change to fast re-authentication.

For tunnel establishment in ~~scenario 3~~WLAN 3GPP IP Access, fast re-authentication may be used for speed up the procedure. In this case, the WLAN-UE shall use the fast re-authentication identities (as long as the re-authentication identity has been received in the last authentication process).

An exception is when the full authentication is being performed for tunnel establishment in ~~scenario 3~~WLAN 3GPP IP Access, in which case the IMSI may be sent even if identity privacy support was activated by the home network. In this situation, the authentication exchange is performed in a protected tunnel which provides encryption and integrity protection, as well as replay protection.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.1.8 Security Association Management for UE-initiated tunnels (~~Scenario 3~~WLAN 3GPP IP Access)

The tunnel endpoints, the UE and the PDG, are mutually authenticated when setting up the tunnel.

The tunnel set-up procedure results in security associations, which are used to provide confidentiality and integrity protection, as required according to sections 5.2 and 5.3, for data transmitted through the tunnel.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.2 Confidentiality protection

5.2.1 Confidentiality protection in ~~scenario 2~~WLAN Direct IP Access

Confidentiality protection in the WLAN AN link layer is required. The specification of this feature is, however, out of scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the confidentiality protection shall be as specified in ref. [6].

The home network (AAA server) has to be able to send key material to the WLAN AN, as input for the encryption procedure, in a confidential and integrity protected way (for detailed requirements cf. [27]).

5.2.2 Confidentiality protection in ~~scenario 3~~WLAN 3GPP IP Access

It shall be possible to protect the confidentiality of IP packets sent through a tunnel between the UE and the PDG.

5.3 Integrity protection

5.3.1 Integrity protection in ~~scenario 2~~WLAN Direct IP Access

Integrity protection in the WLAN AN link layer is required. The specification of this feature is, however, out of scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the integrity protection shall be as specified in ref. [6].

The home network (AAA server) has to be able to send key material to the WLAN AN, as input for the integrity protection mechanism, in a confidential and integrity protected way (for detailed requirements cf. [27]).

5.3.2 Integrity protection in ~~scenario 3~~WLAN 3GPP IP Access

The integrity of IP packets sent through a tunnel between the UE and the PDG shall be protected.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.1.5 Mechanisms for the set up of UE-initiated tunnels (~~Scenario 3~~WLAN 3GPP IP Access)

- The WLAN UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPSec security associations.
- Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG.
- EAP-AKA within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a USIM.
- EAP-SIM within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a SIM and no USIM.
- A profile for IKEv2 is defined in section 6.5.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.2 Confidentiality mechanisms

6.2.1 Confidentiality mechanisms in ~~scenario 2~~WLAN Direct IP Access

The link layer confidentiality mechanisms are outside the scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the confidentiality mechanisms of IEEE 802.11i [6] shall be used. It is specified in ref. [4] and [5] how the key material required for the link layer confidentiality mechanism is obtained from the master session key MSK. The generation of MSK is defined in ref. [4] and [5] as well. The use of ref. [4] and [5] in the context of 3GPP is specified in section 6.1 of this document.
When the key derivation is finished in the AAA server, the key material shall be sent to the WLAN AN via the Wa and Wd (in case of roaming) interfaces.

6.2.2 Confidentiality mechanisms in ~~scenario 3~~WLAN 3GPP IP Access

The confidentiality of IP packets sent through a tunnel between the UE and the PDG, if required, shall be protected by IPSec ESP (RFC 2406 [30]). A profile for IPSec ESP is defined in section 6.6.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.3 Integrity mechanisms

6.3.1 Integrity mechanisms in ~~scenario 2~~WLAN Direct IP Access

The link layer integrity mechanisms are outside the scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the integrity mechanisms of IEEE 802.11i [6] shall be used. It is specified in ref. [4] and [5] how the key material required for the link layer integrity mechanism is obtained from the master session key MSK. The generation of MSK is defined in ref. [4] and [5] as well. The use of ref. [4] and [5] in the context of 3GPP is specified in section 6.1 of this document.
When the key derivation is finished in the AAA server, the key material shall be sent to the WLAN AN via the Wa and Wd (in case of roaming) interfaces.

6.3.2 Integrity mechanisms in ~~scenario 3~~WLAN 3GPP IP Access

The integrity of IP packets sent through a tunnel between the UE and the PDG shall be protected by IPSec ESP (RFC 2406 [30]). A profile for IPSec ESP is defined in section 6.6.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.5 Profile of IKEv2

IKEv2, as specified in ref. [29], contains a number of options, where some are not needed for the purposes of this specification and others are required. IKEv2 is therefore profiled in this section. When IKEv2 is used in the context of this specification the profile specified in this section shall be supported.
Access to services offered by the HPLMN (~~scenario 3~~WLAN 3GPP IP Access) follows a VPN-like approach. In ref. [31] it can be found a set of recommendations of IKEv2 profiles, suitable for VPN-like solutions. On the other hand, ref. [33] sets rules and recommendations for individual algorithms support. Following recommendation from both papers, the below two profiles shall be supported by the PDG and the WLAN-UE:

First cryptographic suite:

- Confidentiality: 3DES in CBC mode;
- Pseudo-random function: HMAC-SHA1;
- Integrity: HMAC-SHA1-96;
- Diffie-Hellman group 2 (1024-bit MODP), mandatory for IKEv2 according to ref. [33].

Second cryptographic suite:

- Confidentiality: AES with fixed key length in CBC mode. The key length is set to 128 bits;
- Pseudo-random function: AES-XCBC-PRF-128;
- Integrity: AES-XCBC-MAC-96.
- Diffie-Hellman group 2 (1024-bit MODP), mandatory for IKEv2 according to ref. [33]

For NAT traversal, the NAT support of IKEv2 shall be supported as specified in section 2.23 of [29].

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

Annex E: (informative): Alternative Mechanisms for the set up of UE-initiated tunnels (WLAN 3GPP IP Access ~~Scenario 3~~)

Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing. The text in section 6.1.5 reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in this Annex. They may be replace the current working assumption in section 6.1.5 of the main body if problems with the working assumptions arise. Otherwise, this annex will be removed before the TS is submitted for approval.

E.1 IKE with subscriber certificates

- The UE and the PDG use IKE, as specified in [rfc2409], in order to establish IPsec security associations.
- Public key signature based authentication with certificates, as specified in [rfc2409], is used in order to authenticate the PDG and the UE.

- A profile for IKE is defined in section 6.5.

E.2 IKEv2 with subscriber certificates

- The UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPSec security associations.
- Public key signature based authentication with certificates, as specified in [ikev2], is used in order to authenticate the PDG and the UE.
- A profile for IKEv2 is defined in section 6.5.

*** END SET OF CHANGES ***