Technical Specification Group Services and System Aspects
Meeting #28, 06 - 08 June 2005,
Quebec, Canada

TSGS#28(05)0339

Source: **SA WG2**

Title: **CRs to TS 23.234: Various Technical Corrections (WLAN) (Rel-6)**

Document for: **Approval**

Agenda Item: **7.2.3**

SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers Cur	SA2 Doc	WI	Clauses affected
SP-050339	23.234	0122	1	Rel-6	F	Correction to Wn Reference Point	6.4.0	S2-050859	WLAN	6.3.7
SP-050339	23.234	0124	2	Rel-6	F	User authentication for tunnel establishement	6.4.0	S2-051415	WLAN	7.9
SP-050339	23.234	0125	-	Rel-6	F	Mandating Immediate Purging	6.4.0	S2-051086	WLAN	6.3.1.2
SP-050339	23.234	0126	1	Rel-6	F	Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages	6.4.0	S2-051353	WLAN	7.2

3GPP TSG SA WG2 meeting #45
Beijing, China, 4th – 8th April 2005

Tdoc ⌘S2-050859

CR-Form-v7

CHANGE REQUEST

⌘ **23.234** **CR** **0122** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

*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 **X**

Title:	⌘	Correction to the definition of the Wn Reference Point
Source:	⌘	SA WG2
Work item code:	⌘	WLAN
Date:	⌘	31/03/2005
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:	⌘	Analysis by CT4 on the text in TS 29.234 related to Wn has led to the conclusion that it should be clarifed that the specific method to implement this Reference Point is out of scope of 3GPP. CT4 have agreed a CR to 29.234 removing the description of the Wn reference point from Stage 3. The change proposed in this CR brings 23.234 in line with CT4's analysis and the changes made to 29.234.
Summary of change:	⌘	Text added in 6.3.7 to clarify that it is out of scope of 3GPP to specify the method to implement Wn.
Consequences if not approved:	⌘	Stage 2 specifications will be inconsistent with Stage 3 regarding the Wn Reference Point.

Clauses affected:	⌘	6.3.7

		Y	N		
Other specs Affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

<< Changed section >>

6.3.7 Wn reference point

The Wn reference point applies to WLAN 3GPP IP Access.

This is the reference point between the WLAN Access Network and the WAG. This interface is to force traffic on a WLAN UE initiated tunnel to travel via the WAG. There can be several different ways to implement this interface as shown in Annex C. The specific method to implement this interface is subject to local agreement between the WLAN AN and the PLMN and is out of the scope of this Release of 3GPP specifications.

3GPP TSG-SA WG2 Meeting #46 **S2-051415**
Athens, Greece. 9th to 13th May 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.234** **CR** **0124** ⌘ **rev** **2** ⌘ Current version: **6.4.0** ⌘

*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 **X**

Title:	⌘	User authentication for tunnel establishement
Source:	⌘	SA WG2
Work item code:	⌘	W-LAN
Date:	⌘	29/04/2005
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change:	⌘	It is unclear in the current specification whether the EAP AKA/ EAP-SIM based authentication is always necessary for WLAN 3GPP IP Access. Although this clarification has already been made by the approved CR S2-042503, This CR provides more clarity on the tunnel establishment procedure.
Summary of change:	⌘	Add explanatory text in section 7.9 to clarify that the WLAN Access Authentication and Authorisation procedure described in step 1 is not always necessary.
Consequences if not approved:	⌘	The relatioship between WLAN Direct access and WLAN 3GPP IP access remains unclear.

Clauses affected:	⌘	7.9

Other specs Affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

Be noted that the coresponding stage 3s are realy for this procedure. See the following qoutation.
=== Qoutation from 3GPP TS 23.008 ===

3B.5.5 Access Independence Flag

The Access Independence Flag is defined in 3GPP TS 29.234 [63]. It enables operators to authenticate a subscriber accessing the I-WLAN by WLAN 3GPP IP Access independently of a previous WLAN 3GPP Direct WLAN Access. The parameter takes either of the following values:

- Allow access to WLAN 3GPP IP Access independently of a previous WLAN 3GPP Direct Access.
- Prohibit access to WLAN 3GPP IP Access independently of a previous WLAN 3GPP Direct Access.

****** First modified section ******

7.9 W-APN resolution and Tunnel establishment

This information flow presents the generic message exchange necessary in order to resolve the selected W-APN and establish a WLAN UE-Initiated tunnel for WLAN 3GPP IP Access purposes.

As a prerequisite of these procedures it is necessary to perform the following:

1. WLAN Access Authentication and Authorisation and provisioning of the WLAN UE's local IP address.

   Note: The authentication and authorization for WLAN Direct IP access and WLAN 3GPP IP access may be performed independently according to the home operator's policy. (For example, the WLAN Access Authentication and Authorisation procedure can be skipped when the home operator allows.)

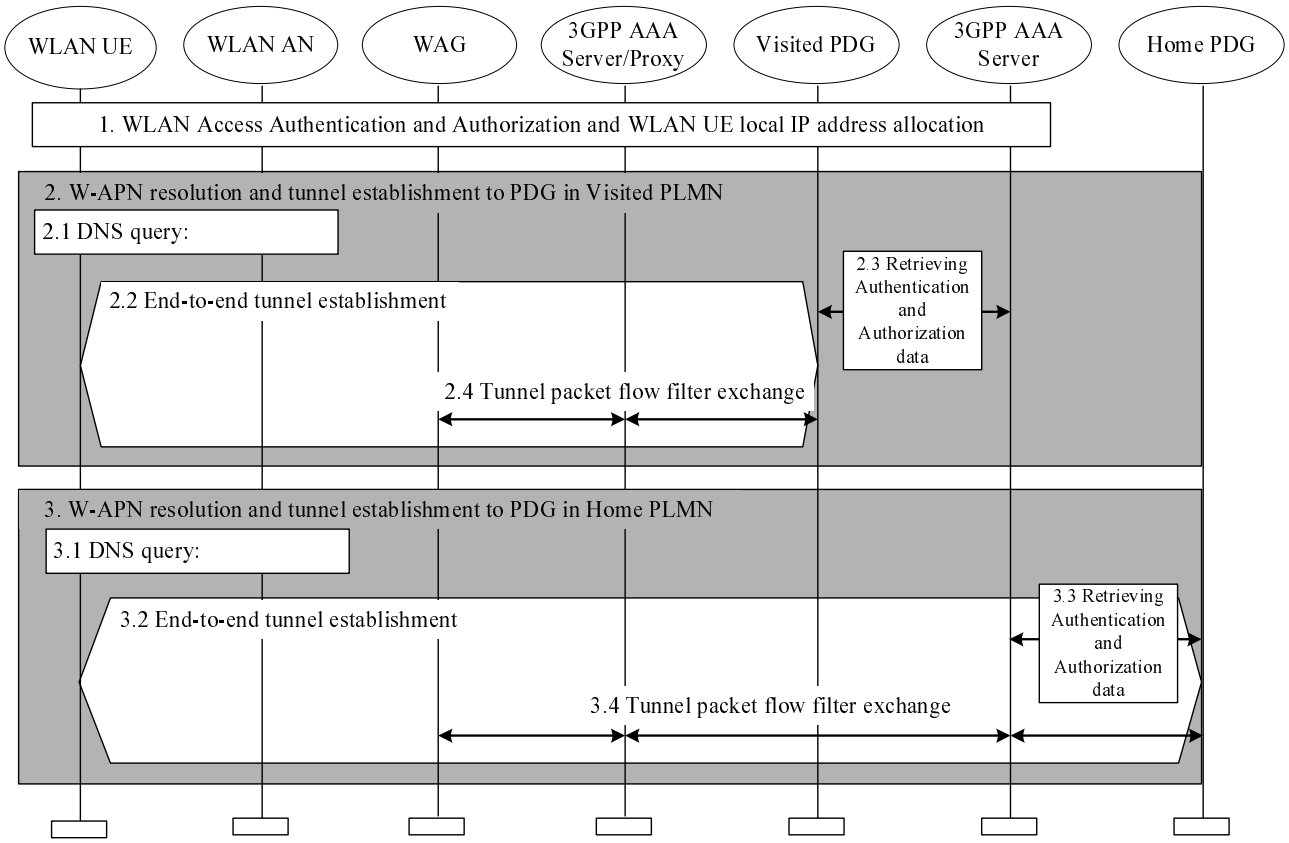


Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

When the user decides that he wants to access a service, the WLAN UE selects the W-APN network ID associated to the service requested by the user.

A detailed description of the W-APN resolution and the WLAN UE-Initiated Tunnel Establishment is given below.

2. Depending on internal configuration, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in VPLMN.

Note: The configuration of the WLAN UE regarding W-APNs can be controlled by e.g. USIM Application Toolkit-based mechanisms.

2.1 WLAN UE constructs an FQDN using the W-APN Network Identifier and VPLMN ID as the Operator Identifier and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the VPLMN according to standard DNS

procedures.
If the VPLMN does not support the W-APN, then the DNS query returns a negative response. In this case, the WLAN UE continues with step 3.

2.2 The WLAN UE selects a PDG from the list received in step 2.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address. If a PDG is finally selected, the establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.

2.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN via the 3GPP AAA Proxy for authorization of the WLAN UE for the W-APN being requested by the WLAN UE and to retrieve the information required for the mutual authentication part of the tunnel establishment. As a result of successful mutual authentication the 3GPP AAA Server registers itself at the HSS (WLAN registration procedure). This action may be omitted, if the 3GPP AAA Server is already registered at the HSS.
The 3GPP AAA Server shall be able to check that the user requesting the tunnel establishment has been already successfully WLAN Access Authorized. Based on operator policy it shall be possible to turn this check on and off. The check may be based on the user's subscription data, e.g. the user's subscribed services. If the check is not successful, the tunnel establishment request is rejected.
If the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, the 3GPP AAA Server shall send a rejection message to the PDG and then the tunnel establishment shall be rejected by the PDG.
The 3GPP AAA Server shall provide PDG with the subscribed Charging Characteristics or W-APN Charging Characteristics. If it is not possible to establish the tunnel with any of the PDGs received from step2.1, or the tunnel establishment failure reason is that the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, then the WLAN UE continues with step 3.

2.4 During the tunnel establishment procedure, the PDG and the WAG exchange information via the 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA Proxy requests the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA Proxy decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of users, WAG capabilities, roaming agreement policy, etc).

3. Depending on internal configuration, or due to the failure of step 2.1 or 2.3, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in HPLMN.

3.1 WLAN UE constructs an FQDN using W-APN Network Identifier and the HPLMN ID as the Operator Identifier, and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the HPLMN according to standard DNS procedures.

3.2 The WLAN UE selects a PDG from the list received in step 3.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address. If a PDG is finally selected, establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.

3.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN for authorization of the WLAN UE for the W-APN being requested by the WLAN UE and to retrieve the information required for the mutual authentication part of tunnel establishment. As a result of successful mutual authentication the 3GPP AAA Server registers itself at the HSS (WLAN registration procedure). This action may be omitted, if the 3GPP AAA Server is already registered at the HSS. The 3GPP AAA Server shall be able to check that the user requesting the tunnel establishment has been already WLAN Access Authorized. Based on operator policy it shall be possible to turn this check on and off. The check may be based on the user's subscription data, e.g. the user's subscribed services. If the check is not successful, the tunnel establishment request is rejected.
If the WLAN UE is not allowed to use a Home PDG to access the given W-APN according to his subscription, the 3GPP AAA Server shall send a rejection message to the PDG and then the tunnel establishment shall be rejected by the Home PDG. The 3GPP AAA Server shall provide the PDG with the WLAN UE's remote IP address, received from the HSS, when static remote IP address allocation is used.
The 3GPP AAA Server shall provide PDG with the subscribed Charging Characteristics or W-APN Charging Characteristics.

3.4 During the tunnel establishment, the PDG and the WAG exchange information via the 3GPP AAA Server and 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA Server requests to the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA Server decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of user, WAG capabilities, roaming agreement policy, etc). The applied filtering policy is communicated to the Home-PDG.

3GPP TSG-SA WG2 Meeting #46
Athens, Greece, 9-13th May 2005.

Tdoc ⌘S2-051086

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.234** **CR** **0125** ⌘**rev** **-** ⌘ Current version: **6.4.0** ⌘

*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 **X**

Title:	⌘	Mandating Immediate Purging
Source:	⌘	SA WG2
Work item code:	⌘	WLAN
Date:	⌘	8/05/2005
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change:	⌘	During SA2#45 meeting it was agreed that the immediate purging of a user from the WLAN AN is a mandatory function that shall be supported by all WLAN ANs. An LS (S2-050945) was sent out to the other working groups to notify them that this function is mandatory and not optional. This view of SA2 is inline with the requirement received from SA1 in S2-050981. Accoding to the current version of TS 23.234 this is an optional function of WLAN ANs.
Summary of change:	⌘	This CR makes the immediate purging of a user from the WLAN AN a mandatory function of WLAN ANs.
Consequences if not approved:	⌘	The specification will contradict the SA1's and SA2's current understanding.

Clauses affected:	⌘	6.3.1.2

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 29.234, TS 33.234
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

****** Start of changes ******

6.3.1.2 Functionality

The functionality of the reference point is to transport AAA frames:

- Carrying data for authentication signalling between WLAN UE and 3GPP Network.
- Carrying data for authorization (including the authorization information update) signalling between WLAN AN and 3GPP Network. These data may include a well-defined identification of the WLAN AN.
- Carrying charging signalling per WLAN user to enable offline and/or online charging. To minimize the requirements put on the WLAN Access Network, the use of online charging over Wa is optional and depends on the agreement between the operators of the WLAN AN and the 3GPP PLMN.
- Enabling the identification of the operator networks amongst which the roaming occurs.
- Carrying keying data for the purpose of radio interface integrity protection and encryption.
- May carry Routing Enforcement information from the PLMN to ensure that all packets sent to/from the WLAN UE for PS based services are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case) appropriately.
- ~~When such functionality is supported by the WLAN AN, p~~Purging a user from the WLAN access for immediate service termination
- Providing access scope limitation information to the WLAN based on the authorised services for each user (for example, IP address filters)

****** End of changes ******

3GPP TSG-SA WG2 Meeting #46
Athens, Greece, 9-13th May 2005.

Tdoc ⌘S2-051353

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.234** **CR** **0126** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

*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 **X**

Title:	⌘	Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages
Source:	⌘	SA WG2
Work item code:	⌘	WLAN
Date:	⌘	8/05/2005
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

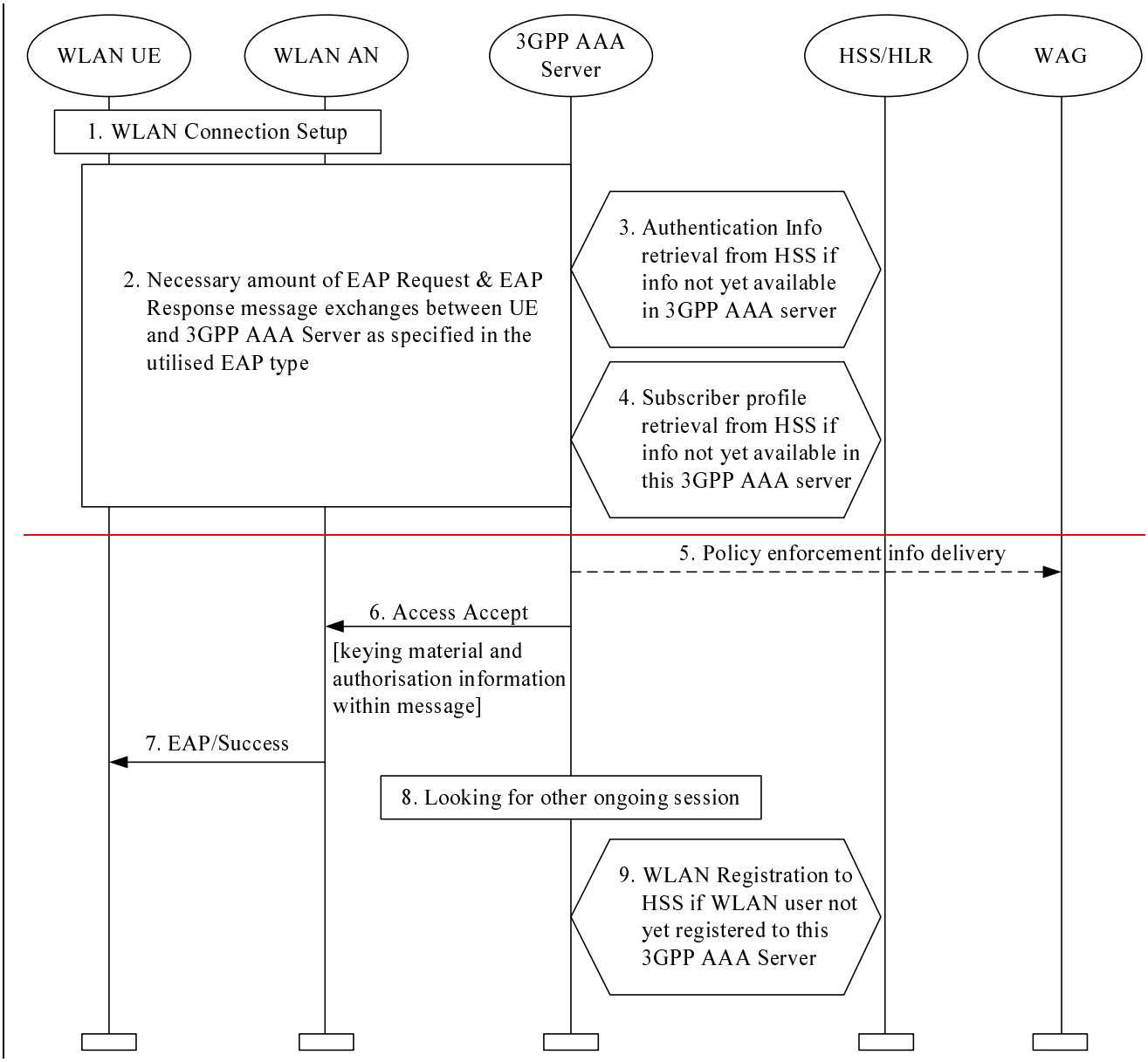
Reason for change:	⌘	A new authentication attemp during an ongoing WLAN direct IP access session can happen due to pre-authentication or to create simultanous WLAN direct IP access sessions. The first one (pre-authentication) is a valid authentication attemp that should be allowed, while the other one may be invalid that should not be allowed. SA3 has identified that based on EAP messaging there is no way to indentify whether a new authentication attempt is a pre-authentication when it has same MAC addresses as the ongoing WLAN Access session, but with different WLAN radio networks information. In SA3 it has been agreed (S3-050181) that the Diameter/RADIUS accounting start message can be used to detect that a WLAN Direct IP Access session is created.
Summary of change:	⌘	The Diameter/RADIUS accounting start messages are used to detect start of a WLAN Direct IP Access session instead of EAP messages. In this way pre-authenication can be allowed, while the fraud simultanous WLAN Direct IP Access sessions can be stopped.
Consequences if not approved:	⌘	The specification will not be suitable to distinguish between pre-authentication and fraud simultanous WLAN Direct IP Access sessions. There will be a contradiction between TS 23.234 and TS 33.234.

Clauses affected:	⌘	7.2
Other specs affected:	⌘	Other core specifications ⌘ Test specifications O&M Specifications
Other comments:	⌘	

Y	N	
	X	Other core specifications
	X	Test specifications
	X	O&M Specifications

****** Start of changes ******

7.2 WLAN Access Authentication and Authorisation


WLAN UE
WLAN AN
3GPP AAA Server
HSS/HLR
WAG
1. WLAN Connection Setup
2. Necessary amount of EAP Request & EAP Response message exchanges between UE and 3GPP AAA Server as specified in the utilised EAP type
3. Authentication Info retrieval from HSS if info not yet available in 3GPP AAA server
4. Subscriber profile retrieval from HSS if info not yet available in this 3GPP AAA server
5. Policy enforcement info delivery
6. Access Accept
[keying material and authorisation information within message]
7. EAP/Success
8. Looking for other ongoing session
9. WLAN Registration to HSS if WLAN user not yet registered to this 3GPP AAA Server

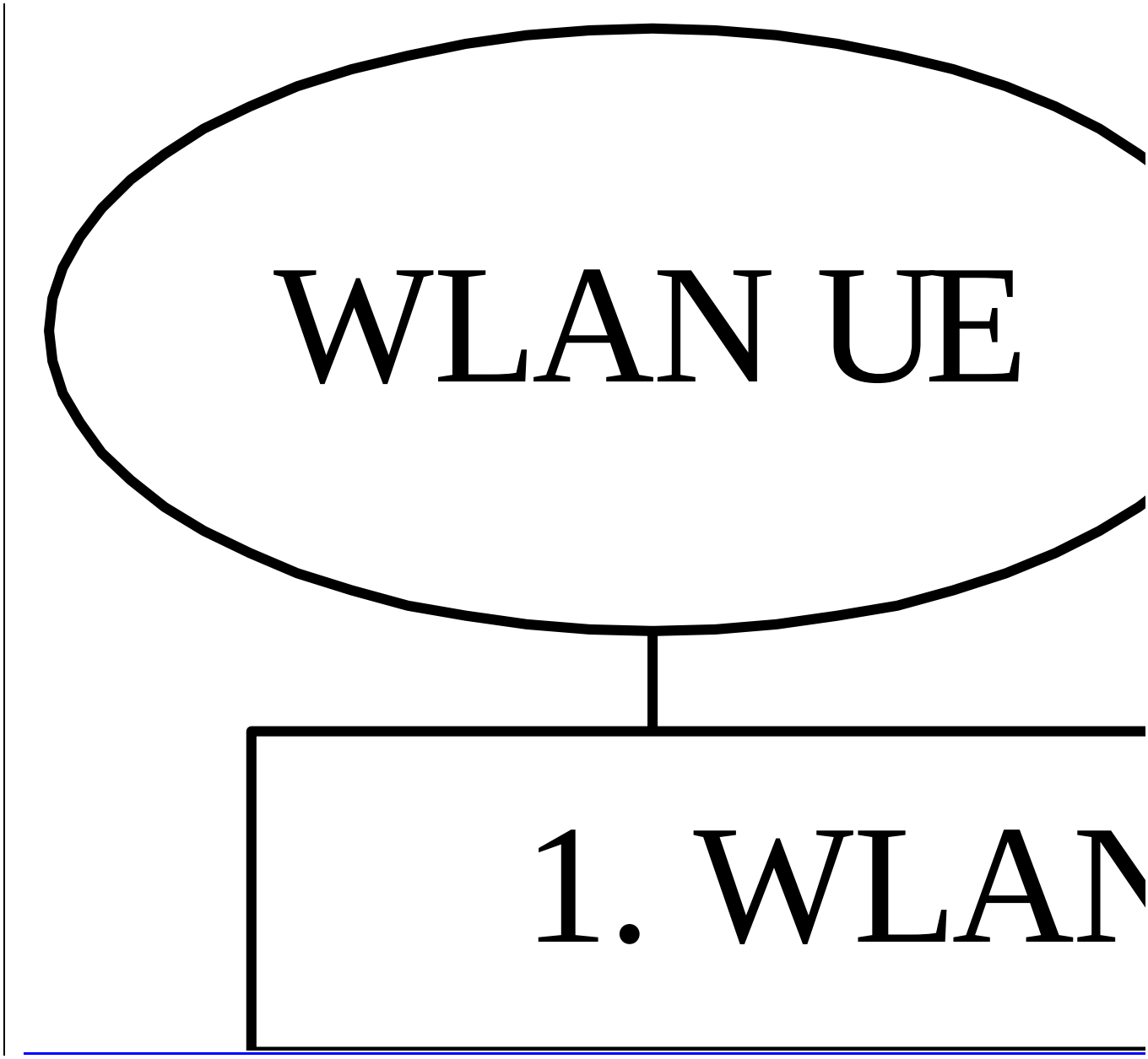


Figure 7.2: Authentication and authorisation procedure

1. WLAN connection is established with a WLAN technology specific procedure (out of scope for 3GPP).

2. The EAP authentication procedure is initiated in WLAN technology specific way.
   All EAP packets are transported over the WLAN interface encapsulated within a WLAN technology specific protocol.
   All EAP packets are transported over the Wa reference point.
   A number of EAP Request and EAP Response message exchanges is executed between 3GPP AAA Server and WLAN UE. The amount of round trips depends e.g. on the utilised EAP type. Information stored in and retrieved from HSS may be needed to execute certain EAP message exchanges.

3 Information to execute the authentication with the accessed user is retrieved from HSS. This information retrieval is needed only if necessary information to execute the EAP authentication is not already available in 3GPP AAA Server. To identify the user the *username* part of the provided NAI identity is utilised. During the information retrieval the HSS/HLR checks if there is a 3GPP AAA Server already registered to serve for the user. In case the HSS/HLR detects that another 3GPP AAA Server has already registered for this user, it shall provide the current 3GPP AAA Server with the previously registered 3GPP AAA Server address. The authentication signalling is then routed to the previously registered 3GPP AAA Server.

4 Subscribers WLAN related profile is retrieved from HSS. This profile includes e.g. the authorisation information and permanent identity of the user. Retrieval is needed only if subscriber profile information is not already available in 3GPP AAA Server.

5. Optionally, the 3GPP AAA Server (or the 3GPP AAA Proxy in roaming case) may send the policy enforcement information to the WAG in the PLMN that the WLAN UE selected in case VPLMN is to allocate the local IP Address for the WLAN UE.

NOTE 1: Additional process, such as allocating the IP address, may be necessary during or before this step to be performed.

6 If the EAP authentication and authorisation was successful, then 3GPP AAA Server sends Access Accept message to WLAN. In this message 3GPP AAA Server includes EAP Success message, keying material derived from the EAP authentication as well as connection authorisation information (e.g. NAS Filter Rule or Tunnelling attributes) to the WLAN.
WLAN stores the keying material and authorisation information to be used in communication with the authenticated WLAN UE.

NOTE 2: In the roaming case, authorisation information is passed from 3GPP AAA Server to 3GPP AAA Proxy in the form of Local service identifiers (see section 6.5).

7 WLAN informs the WLAN UE about the successful authentication and authorisation with the EAP Success message.

8 The 3GPP AAA server receives an accounting start message from the WLAN AN.

~~8~~9 At this point the 3GPP AAA server considers that a new authenticated session is started and it checks its validity. ~~The 3GPP AAA Server checks i~~If there is a different previously established authentication session of the WLAN user, e.g., a session that uses a different WLAN UE or roaming in a different WLAN AN or in a different VPLMN~~. If yes then~~ , the 3GPP AAA Server shall close the previously established session ("Session abort procedure" over Wa) to avoid multiple WLAN direct IP access sessions

~~9~~10 3GPP AAA Server registers the WLAN users 3GPP AAA Server to the HSS. In registration messages the subscriber is identified by his permanent identity. This registration is needed only if the subscriber is not already registered to this 3GPP AAA Server~~.~~

****** End of changes ******