Technical Specification Group Services and System Aspects **TSGS#27(05)0142**
Meeting #27, 14 - 17 March 2005,
Tokyo, Japan

Source: **SA WG3**

Title: **Ten CRs to TS 33.234 (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CRs were agreed by SA WG3 and are presented to TSG SA for approval.

TSG SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Work item
SP-050142	33.234	051	-	Rel-6	Wu Reference Point Description	F	6.3.0	S3-050014	WLAN
SP-050142	33.234	052	1	Rel-6	Replacing PDGW with PDG	D	6.3.0	S3-050161	WLAN
SP-050142	33.234	055	1	Rel-6	Clarification on EAP-AKA(SIM) description in 3GPP IP access authentication and authorization	D	6.3.0	S3-050158	WLAN
SP-050142	33.234	056	2	Rel-6	Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation	F	6.3.0	S3-050178	WLAN
SP-050142	33.234	057	1	Rel-6	Clarifying the status that can’t be changed in the security requirement of WLAN-UE split	F	6.3.0	S3-050159	WLAN
SP-050142	33.234	058	2	Rel-6	WLAN AN providing protection against IP address spoofing	F	6.3.0	S3-050180	WLAN
SP-050142	33.234	059	1	Rel-6	Clarification on the handling of simultaneous sessions	F	6.3.0	S3-050151	WLAN
SP-050142	33.234	060	2	Rel-6	Removal of editors' notes	D	6.3.0	S3-050160	WLAN
SP-050142	33.234	061	1	Rel-6	Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages	F	6.3.0	S3-050181	WLAN
SP-050142	33.234	063	1	Rel-6	Adding verification method of PDG certification by OSCP protocol	F	6.3.0	S3-050177	WLAN

3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050014

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**051**	⌘**rev**	**-**	⌘	Current version:	**6.3.0** ⌘

*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:	⌘	Wu Reference Point Description			
Source:	⌘	SA WG3			
Work item code:	⌘	WLAN	***Date:***	⌘	10/01/2005
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:	⌘	The security mechanism on Wu is very important for WLAN 3GPP IP Access. However, there is no description of Wu interface in the reference points description clause.
Summary of change:	⌘	Add the description of the Wu reference point in clause 4.1.5.
Consequences if not approved:	⌘	The description of reference points is not complete according to the reference model.

Clauses affected:	⌘	4.1.5

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

Other comments:	⌘	

*** BEGIN OF CHANGE ***

4.1.5 Reference points description

Wa

The reference point Wa 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 [23], [24] or RADIUS [15], [26] 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 retrieval 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

This reference point is located 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. The specific method to implement this interface is subject to local agreement between the WLAN AN and the PLMN.

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.

Wd

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

Wu

The reference point Wu is located between the WLAN UE and the Packet Data Gateway. It represents the WLAN UE-initiated tunnel between the WLAN UE and the Packet Data Gateway. On Wu interface WLAN UE and Packet Data Gateway run IKEv2 protocol to establish IPsec tunnel and protect user data packets transmitted.

*** END OF CHANGE ***

3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050161

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR 052**	⌘ **rev**	**1**	⌘ Current version:	**6.3.0** ⌘

*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:	⌘	Replacing PDGW with PDG		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	24/02/2005
Category:	⌘	**D**	***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:	⌘	The term Packet Date Gateway is sometimes abbreviated to PDGW in TS 33.234. However, the abbreviation is PDG in definitions and abbreviations clause.
Summary of change:	⌘	Replace all PDGW with PDG to keep term conformance.
Consequences if not approved:	⌘	Term abbreviations are not aligned in TS 33.234

Clauses affected:	⌘	4.1.3, 4.1.4 and 4.2.6

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

Other comments:	⌘	

*** BEGIN OF FIRST CHANGE ***

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~~PDG).

*** END OF FIRST CHANGE ***

*** BEGIN OF SECOND CHANGE ***

4.1.4 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;

NOTE: Definition of simultaneous access is specified in TS 23.234 [13].

  - 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, Infrared or serial cable interface;
- 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~~PDG)** 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.

*** END OF SECOND CHANGE ***

*** BEGIN OF FINAL CHANGE ***

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 ~~PDGW~~ PDG 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 WLAN 3GPP IP Access are to be independent of the link layer security in WLAN Direct IP Access.

*** END OF FINAL CHANGE ***

3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050158

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234 CR 055** ⌘**rev** **1** ⌘ Current version: **6.3.0** ⌘

*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:	⌘	Clarification on EAP-AKA(SIM) description in 3GPP IP access authentication and authorization.
Source:	⌘	SA WG3
Work item code:	⌘	WLAN
Date:	⌘	07/02/2005
Category:	⌘	**D**
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:	⌘	In Figure 7A and 7B (tunnel authentication and authorization), only EAP-AKA is showed in the message flows, but EAP-SIM is neglected, although there are some explainary texts below. Our changes make specification more clear and simple to understand.
Summary of change:	⌘	Modification of figures and coressponding texts on tunnel authentication description.
Consequences if not approved:	⌘	Potential misunderstanding of description of tunnel authentication and authorization flows.

Clauses affected:	⌘	6.1.5.1, 6.1.5.2

Other specs affected: ⌘

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

Other comments: ⌘

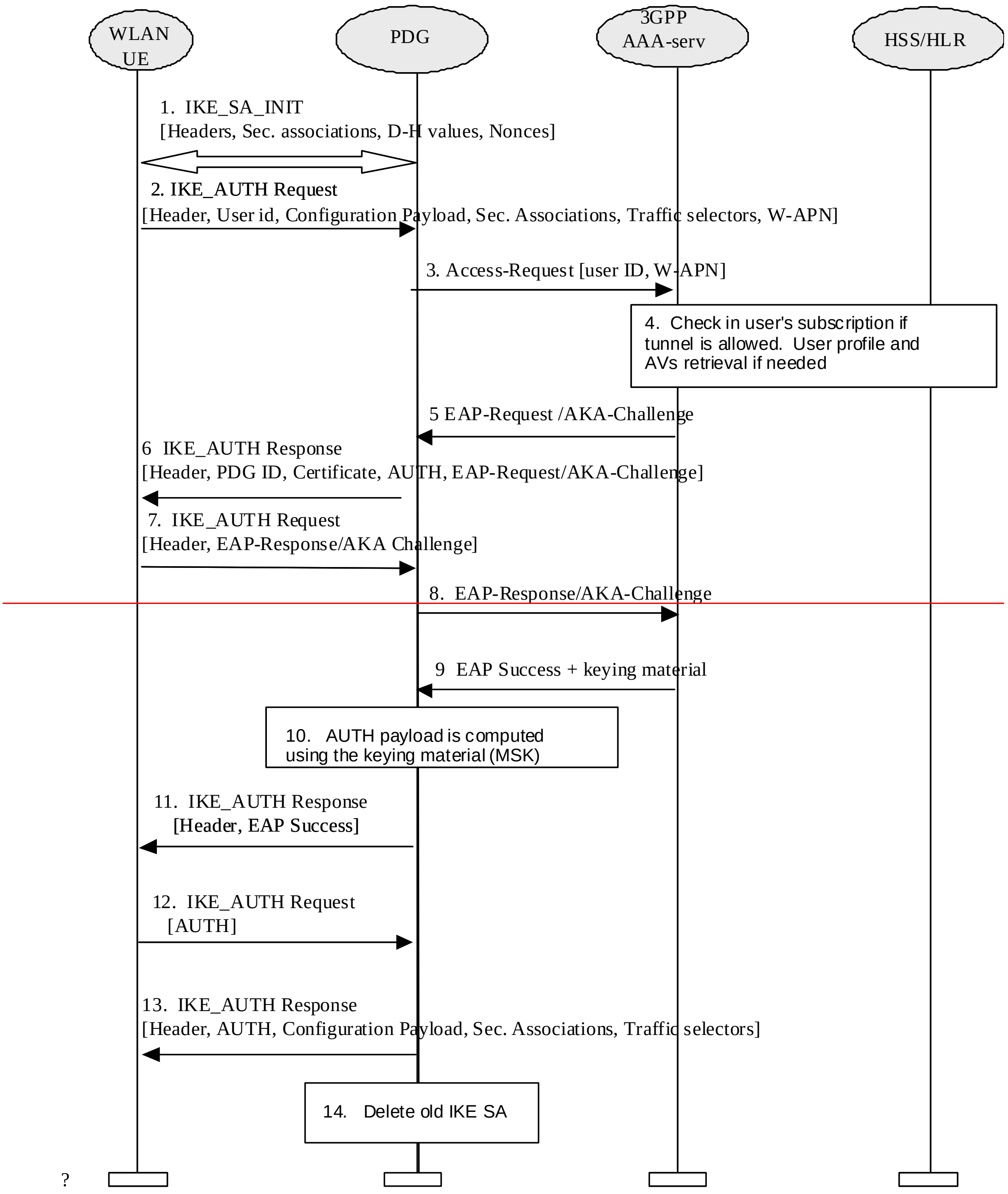
*** BEGIN SET OF CHANGES ***

6.1.5.1 Tunnel full authentication and authorization

The tunnel end point in the network is the PDG. As part of the tunnel establishment attempt the use of a certain W-APN is requested. When a new attempt for tunnel establishment is performed by the WLAN UE, the WLAN UE shall use IKEv2 as specified in ref. [29]. The EAP messages carried over IKEv2 shall be terminated in the AAA server, which communicates with the PDG via Wm interface, implemented with Diameter. Then the PDG shall extract the EAP messages received from the WLAN UE over IKEv2, and send them to the AAA server over Diameter (the opposite for messages sent from the AAA server). The WLAN UE shall use the Configuration Payload of IKEv2 to obtain the Remote IP address.

The sequence diagram is shown in figure 7A. The EAP message parameters and procedures regarding authentication are omitted since they are already described in this technical specification. Only decisions and processes relevant to this EAP-IKEv2 procedure are explained.

As the WLAN UE and PDG generated nonces are used as input to derive the encryption and authentication keys in IKEv2, replay protection is implemented as well. For this reason, there is no need for the AAA server to request the user identity again using the EAP AKA or EAP SIM specific methods (as specified in ref. [4] and ref. [5]), because the AAA server is certain that no intermediate node has modified or changed the user identity.


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Configuration Payload, Sec. Associations, Traffic selectors, W-APN]
3. Access-Request [user ID, W-APN]
4. Check in user's subscription if tunnel is allowed. User profile and AVs retrieval if needed
5 EAP-Request /AKA-Challenge
6 IKE_AUTH Response
[Header, PDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge]
7. IKE_AUTH Request
[Header, EAP-Response/AKA Challenge]
8. EAP-Response/AKA-Challenge
9 EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Configuration Payload, Sec. Associations, Traffic selectors]
14. Delete old IKE SA
?

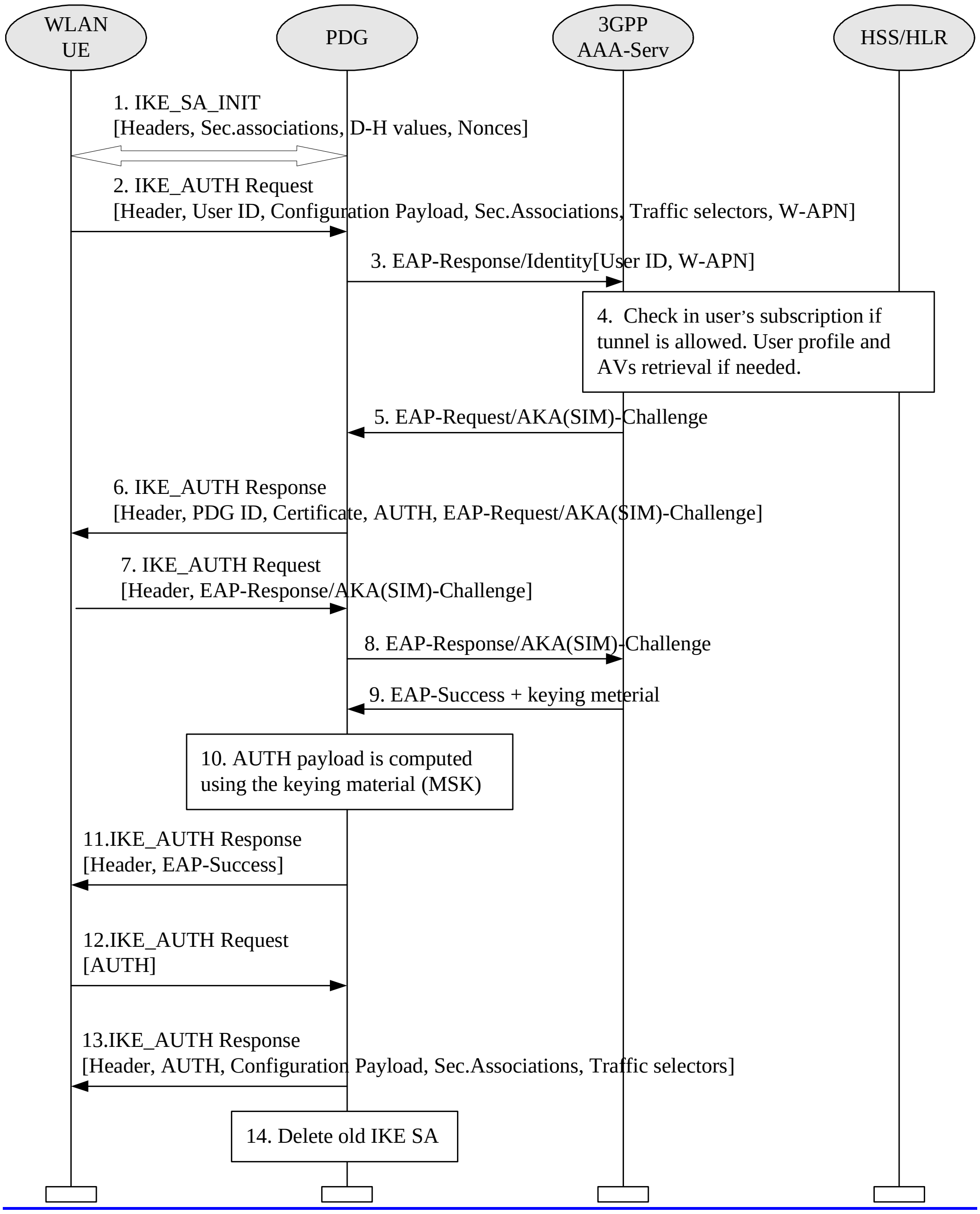

WLAN UE
PDG
3GPP AAA-Serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec.associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User ID, Configuration Payload, Sec.Associations, Traffic selectors, W-APN]
3. EAP-Response/Identity[User ID, W-APN]
4. Check in user's subscription if tunnel is allowed. User profile and AVs retrieval if needed.
5. EAP-Request/AKA(SIM)-Challenge
6. IKE_AUTH Response
[Header, PDG ID, Certificate, AUTH, EAP-Request/AKA(SIM)-Challenge]
7. IKE_AUTH Request
[Header, EAP-Response/AKA(SIM)-Challenge]
8. EAP-Response/AKA(SIM)-Challenge
9. EAP-Success + keying meterial
10. AUTH payload is computed using the keying material (MSK)
11.IKE_AUTH Response
[Header, EAP-Success]
12.IKE_AUTH Request
[AUTH]
13.IKE_AUTH Response
[Header, AUTH, Configuration Payload, Sec.Associations, Traffic selectors]
14. Delete old IKE SA

Figure 7A: Tunnel full authentication and authorization

1. The WLAN UE and the PDG exchange the first pair of messages, known as IKE_SA_INIT, in which the PDG and WLAN UE negotiation cryptographic algorithms, exchange nonces and perform a Diffie_Hellman exchange.

2. The WLAN UE sends the user identity (in the Idi payload) and th'e W-APN information (in the Idr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The WLAN UE omits the AUTH parameter in order to indicate to the PDG that it wants to use EAP over IKEv2. The user identity shall be compliant with Network Access Identifier (NAI) format specified in RFC 2486 [14], containing the IMSI or the pseudonym. The identity in NAI format generated from the IMSI is described in ref. [4] and ref. [5], depending on the type of EAP method to be used (EAP SIM or EAP AKA). The WLAN UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address.

Editors note: The control of simultaneous sessions in the EAP authentication has to be possible as in WLAN access authentication. Nevertheless, it is needed to study in detail how the parameters to perform this control have to be transferred in EAP/IKEv2. For example, the VPLMN id could be included in the NAI (see TS 23.234 [13], section 5.3.4)

3. The PDG sends the Access Request message with an empty EAP AVP to the AAA server, containing the user identity and W-APN. The PDG shall include a parameter indicating that the authentication is being performed for tunnel establishment, as indicated in reference [37]. This will help the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The AAA server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the AAA server) and determines the EAP method (SIM or AKA) to be used, according to the user subscription and/or the indication received from the WLAN UE. The AAA server checks in user's subscription if he/she is authorized to establish the tunnel.

~~In this sequence diagram, it is assumed that the user has a USIM and EAP AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification~~

5. The AAA server initiates the authentication challenge. The user identity is not requested again, as in a normal authentication process, because there is the certainty that the user identity received in the EAP Identity Response message has not been modified or replaced by any intermediate node. The reason is that the user identity was received via an IKEv2 secure channel which can only be decrypted and authenticated by the end points (the PDG and the WLAN UE).

6. The PDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the WLAN UE (in the IKE_SA_INIT exchange). It completes the negotiation of the child security associations as well. The EAP message received from the AAA server (EAP-Request/AKA-Challenge or EAP-Request/SIM-Challenge) is included in order to start the EAP procedure over IKEv2.

7. The WLAN UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message.

8. The PDG forwards the EAP-Response/AKA-Challenge message or EAP-Response/SIM-Challenge message to the AAA server.

9. When all checks are successful, the AAA server sends an EAP success and the key material to the PDG. This key material shall consist of the MSK generated during the authentication process. When the Wm interface (PDG-AAA server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in ref. [23].

   If the W-APN is not active, the AAA server will mark it as "active".

   If the AAA server detects that the W-APN is active in other PDG, it will send an indication to that PDG requesting to delete the IKE SA of the W-APN.

Editor's note: Registration procedure, including transport of parameters needed to perform simultaneous access control, should be performed in order to update registration status in HSS and fetch the necessary data to the AAA server, but this still needs to be studied in detail.

10. The MSK shall be used by the PDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified in ref. [29]. These two first messages had not been authenticated before as there were no key material available yet. According to ref. [29], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

11. The EAP Success message is forwarded to the WLAN UE over IKEv2.

12. The WLAN UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDG.

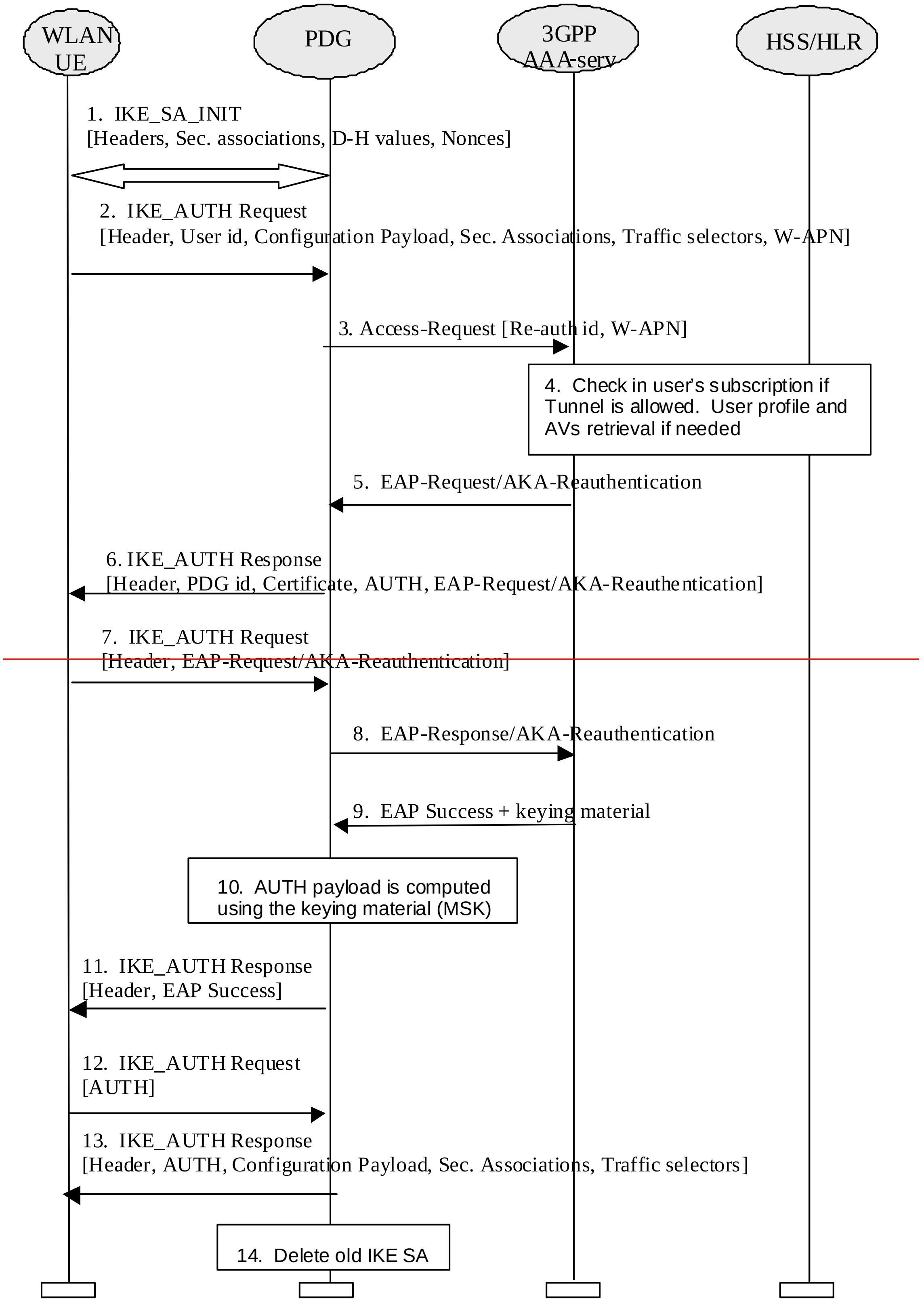
13. The PDG checks the correctness of the AUTH received from the WLAN UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The PDG shall send the assigned Remote IP address in the configuration payload (CFG_REPLY), if the WLAN UE requested for a Remote IP address through the CFG_REQUEST. Then the AUTH parameter is sent to the WLAN UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

14. If the PDG detects that and old IKE SA for that W-APN already exists, it will delete the IKE SA and send the WLAN UE an INFORMATIONAL exchange with a Delete payload, as specified in reference [29], in order to delete the old IKE SA in WLAN UE.

6.1.5.2 Tunnel fast re-authentication and authorization

This process is very similar to the tunnel full authentication and authorization. The only difference is that EAP fast re-authentication is used in this case.

The sequence diagram is shown in figure 7B. The EAP message parameters and procedures regarding fast re-authentication are omitted since they are already described in this technical specification. Only decisions and processes relevant to this EAP-IKEv2 procedure are explained.


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Configuration Payload, Sec. Associations, Traffic selectors, W-APN]
3. Access-Request [Re-auth id, W-APN]
4. Check in user's subscription if Tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Reauthentication
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Reauthentication]
7. IKE_AUTH Request
~~[Header, EAP-Request/AKA-Reauthentication]~~
8. EAP-Response/AKA-Reauthentication
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Configuration Payload, Sec. Associations, Traffic selectors]
14. Delete old IKE SA

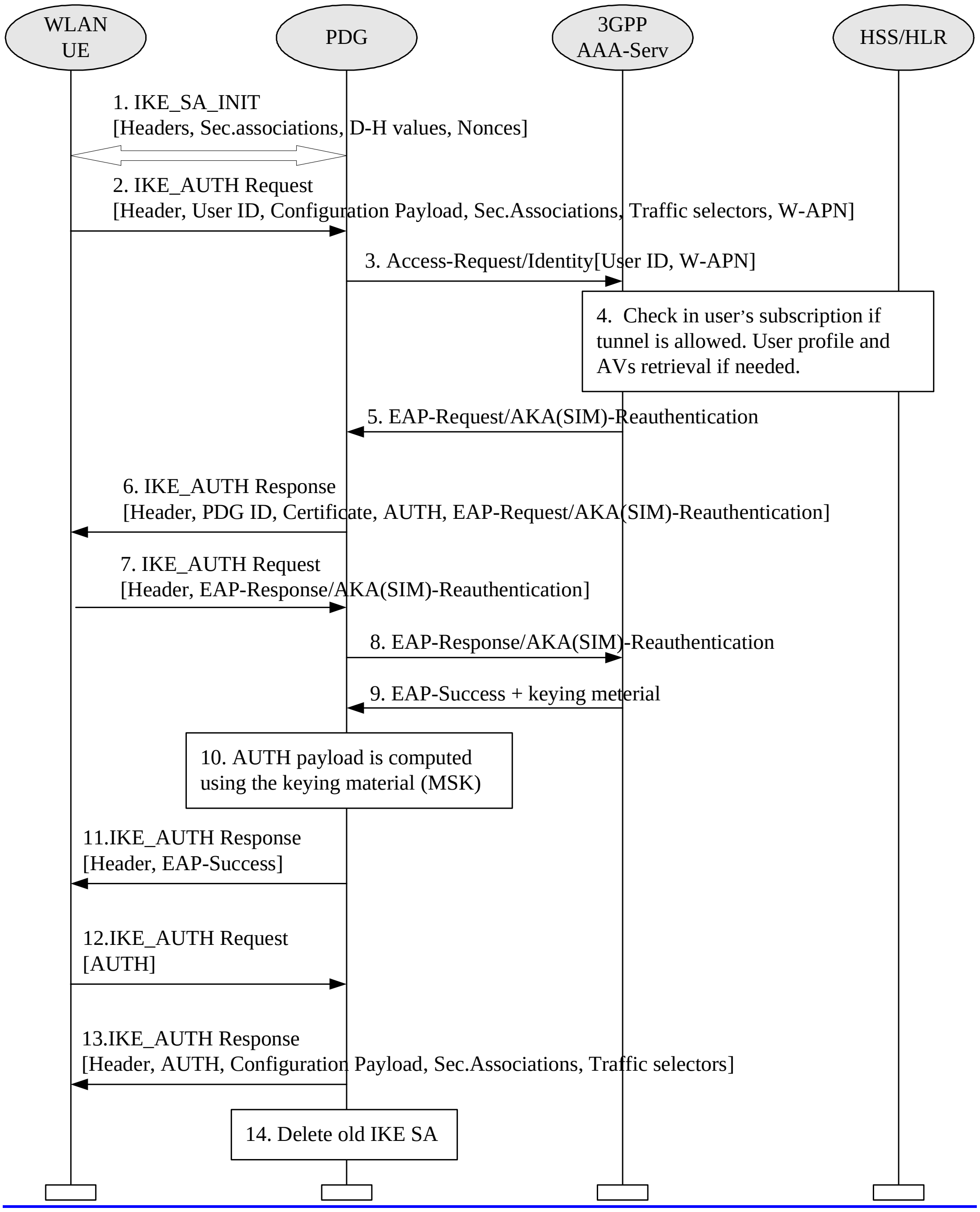

WLAN UE
PDG
3GPP AAA-Serv
HSS/HLR
1. IKE_SA_INIT [Headers, Sec.associations, D-H values, Nonces]
2. IKE_AUTH Request [Header, User ID, Configuration Payload, Sec.Associations, Traffic selectors, W-APN]
3. Access-Request/Identity[User ID, W-APN]
4. Check in user's subscription if tunnel is allowed. User profile and AVs retrieval if needed.
5. EAP-Request/AKA(SIM)-Reauthentication
6. IKE_AUTH Response [Header, PDG ID, Certificate, AUTH, EAP-Request/AKA(SIM)-Reauthentication]
7. IKE_AUTH Request [Header, EAP-Response/AKA(SIM)-Reauthentication]
8. EAP-Response/AKA(SIM)-Reauthentication
9. EAP-Success + keying meterial
10. AUTH payload is computed using the keying material (MSK)
11.IKE_AUTH Response [Header, EAP-Success]
12.IKE_AUTH Request [AUTH]
13.IKE_AUTH Response [Header, AUTH, Configuration Payload, Sec.Associations, Traffic selectors]
14. Delete old IKE SA

Figure 7B: Tunnel fast re-authentication and authorization

1. The WLAN UE and the PDG exchange the first pair of messages, known as IKE_SA_INIT, in which the PDG and WLAN UE negotiation cryptographic algorithms, exchange nonces and perform a Diffie_Hellman exchange.

2. The WLAN UE sends the re-authentication identity (in the Idi payload) and the W-APN information (in the Idr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The WLAN UE omits the AUTH parameter in order to indicate to the PDG that it wants to use EAP over IKEv2. The re-authentication identity used by the WLAN UE shall be the one received in the previous authentication process. The WLAN UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address.

3. The PDG sends the Access Request message with an empty EAP AVP to the AAA server, containing the re-authentication identity and W-APN. The PDG shall include a parameter indicating that the authentication is being performed for tunnel establishment, as indicated in ref. [37]. This will help the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The AAA server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the AAA server) and determines the EAP method (SIM or AKA) to be used, according to the user subscription. The AAA server checks in user's subscription if he/she is authorized to establish the tunnel.

~~In this sequence diagram, it is assumed that the user has a USIM and EAP AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification.~~

5. The AAA server initiates the fast re-authentication challenge.

6. The PDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the WLAN UE (in the IKE_SA_INIT exchange). It completes the negotiation of the child security associations as well. The EAP message received from the AAA server (EAP-Request/AKA-Reauthentication or EAP-Request/SIM-Reauthentication) is included in order to start the EAP procedure over IKEv2.

7. The WLAN UE checks the authentication parameters and responds to the fast re-authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message.

8. The PDG forwards the EAP-Response/AKA-Reauthentication message or EAP-Response/SIM-Reauthentication message to the AAA server.

9. When all checks are successful, the AAA server sends an EAP success and the key material to the PDG. This key material shall consist of the MSK generated during the fast re-authentication process. When the Wm interface (PDG-AAA server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in ref. [23].

   If the W-APN is not active, the AAA server will mark it as "active".

   If the AAA server detects that the W-APN is active in other PDG, it will send an indication to that PDG requesting to delete the IKE SA of the W-APN.

10. The MSK shall be used by the PDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified in ref. [29]. These two first messages had not been authenticated before as there were no key material available yet. According to ref. [29], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

11. The EAP Success message is forwarded to the WLAN UE over IKEv2.

12. The WLAN UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDG.

13. The PDG checks the correctness of the AUTH received from the WLAN UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The PDG shall send the assigned Remote IP address in the configuration payload (CFG_REPLY), if the WLAN UE requested for a Remote IP address through the CFG_REQUEST. Then the AUTH parameter is sent to the WLAN UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

14. If the PDG detects that and old IKE SA for that W-APN already exists, it will delete the IKE SA and send to the WLAN UE an INFORMATIONAL exchange with a Delete payload, as specified in reference [29], in order to delete the old IKE SA in WLAN UE.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050178

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**056**	⌘**rev**	**2**	⌘	Current version:	**6.3.0** ⌘

*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:	⌘	Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation.			
Source:	⌘	SA WG3			
Work item code:	⌘	WLAN	***Date:***	⌘	22/01/2005
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:	⌘	There is no description about threat of user accessing each other in link layer and corresponding security requirements of user traffic segregation in current specification.
Summary of change:	⌘	Adding threat of user accessing each other in link layer and security requirement of user traffic segregation. Some editorial corrections is also included.
Consequences if not approved:	⌘	Specification is not complete.

Clauses affected:	⌘	C.1, C.2.2.2				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN OF CHANGE1 ***

C.1 Security for Public WLAN Access

These questions related to security in the 3GPP-WLAN architecture, must be addressed:

- What needs to be protected? i.e. what are the assets, and to whom are they valuable?
- What trust relations can be assumed? i.e. who can trust whom, and to what degree? The Trust Model is described in Annex B.
- What are possible attacks against the assets, how can they be performed, and what is done to detect/prevent them?

In section ~~3~~ C.2 the relevant ~~assents~~ assets and threats to those assets are identified. Section ~~4~~ C.3 contains examples of possible attacks. Countermeasures are not discussed in this ~~contribution~~ section but the threats and specific attacks should be taken into consideration when defining security mechanisms for 3GPP-WLAN interworking.

*** END OF CHANGE1 ***

*** BEGIN OF CHANGE2 ***

C.2.2.2 User Data and Privacy

The user expects that the data he sends/receives while accessing to WLAN services, ~~and~~ personal information (such as identity, which services he/she uses or where he/she is located at a given time) is kept away from unauthorised parties, and data stored in his/her WLAN UE is not accessed by unauthorized user.

The following threats are relevant:

- An attacker obtains the information that the user sends/receives while accessing to WLAN services. This includes user credentials transferred during the authentication phase, as well as any other data (e.g. documents) exchanged once the user has gained access to the WLAN services. The attacker might know or not who the user is;
- An attacker manipulates or substitutes the information that the user sends/receives while accessing to WLAN services. The attacker might know or not who the user is;
- An attacker analyses the information sent/received by users (even if it is mostly concealed) in order to derive some personal information about the users (such as which services they are using or where they are located at a given time).
- An attacker obtains information about the user (permanent identity etc.) and traces where and when the user has been accessing WLAN services.
- An attacker (also a legal user) accesses the user's WLAN UE in link layer without the user's permission.

In some situations, such as public hotspots, it is considered a real threat that users can access each other in link layer directly. It is recommended to segregate user traffic at AP and access controller in WLAN AN to protect assets of users and operator.

*** END OF CHANGE2 ***

3GPP TSG SA WG3 Security — S3#37 ***Tdoc ⌘S3-050159***
Sophia Antipolis, France 21 - 25 February 2005

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**057**	⌘**rev**	**1**	⌘	Current version: **6.3.0** ⌘

*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:	⌘	Clarifying the status that can't be changed in the security requirement of WLAN-UE split		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	10/01/2005
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:	⌘	The meaning of "status" isn't clear in clause 2 in 4.2.4.2. The status was meant to be powering on/off status as agreed in the conference calls in August 2004.
Summary of change:	⌘	State directly the status is powering on/off status.
Consequences if not approved:	⌘	There may be misunderstanding of the meaning of "status".

Clauses affected:	⌘	4.2.4.2

Other specs affected: ⌘

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

Other comments: ⌘

*** BEGIN OF CHANGE ***

4.2.4.2 Generic security requirements on local interface

The security functionality required on the terminal side for WLAN-3G interworking may be split over several physical devices that communicate over local interfaces. The UICC or the SIM card may reside in a 3GPP UE (acting as a (U)SIM "server") and be accessed by a WLAN-UE through Bluetooth, Infrared or a USB (Universal Serial Bus) cable or some other similar wired or wireless interconnect technology (acting as the (U)SIM "client"). This would facilitate the user to get simultaneous WLAN and 3GPP access with the same (U)SIM. If this is the case, then the following requirements shall be satisfied:

1. Any local interface shall be protected against eavesdropping, attacks on security-relevant information. This protection may be provided by physical or cryptographic means. For cryptographic means, the encryption key length shall be at least 128 bits.

2. The endpoints of a local interface should be authenticated and authorised. The authorisation may be implicit in the security set-up. Keys used for local interface transport security shall not be shared across local interface links. Each local interface shall use unique keys.

3. The involved devices shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.

4. The device without (U)SIM shall not be allowed to change the status of the device with (U)SIM, ~~e.g~~i.e. to reset it, or to switch its power on or off.

5. The (U)SIM holding device shall allow the user to shut off sharing of (U)SIM feature.

*** END OF CHANGE ***

3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050180

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**058**	⌘**rev**	**2**	⌘	Current version:	**6.3.0**	⌘

*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:	⌘	WLAN AN providing protection against IP address spoofing		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	25/02/2005
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:	⌘	For WLAN Direct IP Access there exists potential IP address spoofing attack if the charging is based on IP address. It's WLAN AN's duty to defeat this kind of attack.
Summary of change:	⌘	Add a description of IP address spoofing attack against WLAN AN in the Annex C3.3.
Consequences if not approved:	⌘	WLAN provider may not be aware of this threat of IP address spoofing attack against WLAN Direct IP Access.

Clauses affected:	⌘	Annex C3.3				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN OF CHANGE ***

C.3.3 Attacks at the WLAN AN Infrastructure

Attacks can be performed at the WLAN AN infrastructure, e.g. Access Points (AP), the LAN connecting the APs, Ethernet switches etc. To perform any type of attacks "inside" the WLAN AN, the attacker needs access to the network in some way. For ordinary wired networks, an attacker needs to somehow hook up to the wires to get access. The WLAN AN is partially a wired network, and an attacker may hook up to that part of the network. In public spaces the APs and corresponding wired connections may be physically accessible by attackers. Simply connecting a laptop to the wired LAN "behind" the APs may give the attacker free access to WLAN services as well as access to other user's data and signalling traffic.

Depending on where charging data is collected, an attacker with access to the wired LAN of the WLAN AN can also interfere with the charging functions. If the volume based charging model is applied, an attacker could e.g. inject packets with any chosen source or destination MAC and IP addresses, just to increase a user's bill.

For WLAN Direct IP Access if the charging is based on IP address, there exists a threat of IP address spoofing attack against the WLAN AN, which may generate incorrect accounting message for users.

NOTE: 3GPP suggest WLAN operators not to use IP address based accounting; unless there are sufficient countermeasures implemented against IP address spoofing attack in the WLAN AN.

*** END OF CHANGE ***

3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 22 - 25 February 2005

Tdoc ⌘S3-050151

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**059**	⌘**rev**	**1**	⌘	Current version:	**6.3.0** ⌘

*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:	⌘	Clarification on the handling of simultaneous sessions		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	02/02/2005
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:	⌘	In SA3#36 the handling of simultaneous sessions in WLAN 3GPP IP access (formerly called scenario 3) was introduced in TS 33.234. However, the description of the actions to be taken by the 3GPP network were not clear enough, for example how the PDG shall behave. Furthermore, the mechanism currently described sets the maximum number of sessions to one, thus preventing it to be extended to more simultaneous sessions if the home operators decides it.
Summary of change:	⌘	The 3GPP network procedures (behaviour of the PDG and AAA server) are explained in more detail. The mechanism is explained in a flexible way so that more than one simultaneous session is possible. The number of simultaneous sessions will be configured by the home operator.
Consequences if not approved:	⌘	Lack of clear enough descriptions may lead to interoperability problems.

Clauses affected:	⌘	5.7, 6.1.5.1, 6.1.5.2				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	29.234, 24.234
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

5.7 Simultaneous access control

The home network operator needs to be aware of how the user is accessing the WLAN network. If the user is making the SIM or UICC card available for several devices that have WLAN access capabilities, the home network operator may decide, at any time, to allow or bar t he access of two or more network devices simultaneously.

WLAN direct IP access

The control of simultaneous sessions in WLAN direct IP access can be performed, under some circumstances, using the MAC address of the user's device.

After a number of successful authentications, if a subsequent authentication attempt is being performed by another device, the MAC address will be different and the AAA server will be able to detect it. However, this mechanism has some limitations. One of them is that if the two devices are accessing two different WLAN access points (assuming that a WLAN access point has a independent control of MAC address space), the MAC address of one of them can be spoofed and made equal to the other one. This is a fraud situation the home network should avoid. However, it may happen that the user is accessing other WLAN access point and a pre-authentication is performed in this new access point. In this case there is no fraud attempt. Then, in this situation (same MAC addresses, different WLAN radio networks) the AAA server will not be able to distinguish between a legal and a fraud situation and shall not reject the authentication process.

WLAN 3GPP IP access

The control of simultaneous sessions in WLAN 3GPP IP access has to be performed in a different way than in WLAN direct IP access as in this case the MAC addresses cannot be trusted by the home network and may not be available.

The user gets connected to the 3GPP network using the W-APNs. When a W-APN is activated by the user, an IKEv2 exchange will be initiated and, if successful, an IKE SA and an IPsec SA will be established.

The IKEv2 procedure is authenticated using EAP SIM or EAP AKA, so the AAA server has to be contacted in order to perform this authentication. Then the AAA server will be aware of the fact that a new W-APN is going to be activated.

The mechanism to control simultaneous sessions is to limit the number of W-APNs to be activated by the user and ~~allow only one~~ control the number of IKEv2 security associations per W-APN. The home operator shall configure, by subscription, the Maximum Number of IKE SAs per W-APN. With this mechanism, it is ensured that only as many devices as defined by the Maximum Number~~avoided that two or more devices~~ make use of the same subscription to access the 3GPP network, because each device will have to activate a W-APN (and use a different IKE SA and IPsec SA). ~~The AAA server shall keep a flag (e.g. active yes/no) for every W-APN and check this flag when a IKE SA establishment attempt is received. If the W-APN is already active, the AAA server will instruct the PDG to delete the old IKE SA and proceed to establish the new IKE SA.~~

Since one IKE SA allows to establish multiple IPsec SAs, and the establishment of a new IPsec SA (under the same IKE SA) does not imply to contact the AAA server, the PDG shall reject more than one IPsec SA per IKE SA. This measure forces the WLAN UE to setup a new IKE SA if the WLAN UE wants to setup a new IPsec SA, hence making the AAA server aware of this establishment attempt and enforcing the authorization mechanism specified previously.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.1.5.1 Tunnel full authentication and authorization

The tunnel end point in the network is the PDG. As part of the tunnel establishment attempt the use of a certain W-APN is requested. When a new attempt for tunnel establishment is performed by the WLAN UE, the WLAN UE shall use IKEv2 as specified in ref. [29]. The EAP messages carried over IKEv2 shall be terminated in the AAA server, which communicates with the PDG via Wm interface, implemented with Diameter. Then the PDG shall extract the EAP messages received from the WLAN UE over IKEv2, and send them to the AAA server over Diameter (the opposite for messages sent from the AAA server). The WLAN UE shall use the Configuration Payload of IKEv2 to obtain the Remote IP address.

The sequence diagram is shown in figure 7A. The EAP message parameters and procedures regarding authentication are omitted since they are already described in this technical specification. Only decisions and processes relevant to this EAP-IKEv2 procedure are explained.

As the WLAN UE and PDG generated nonces are used as input to derive the encryption and authentication keys in IKEv2, replay protection is implemented as well. For this reason, there is no need for the AAA server to request the user identity again using the EAP AKA or EAP SIM specific methods (as specified in ref. [4] and ref. [5]), because the AAA server is certain that no intermediate node has modified or changed the user identity.

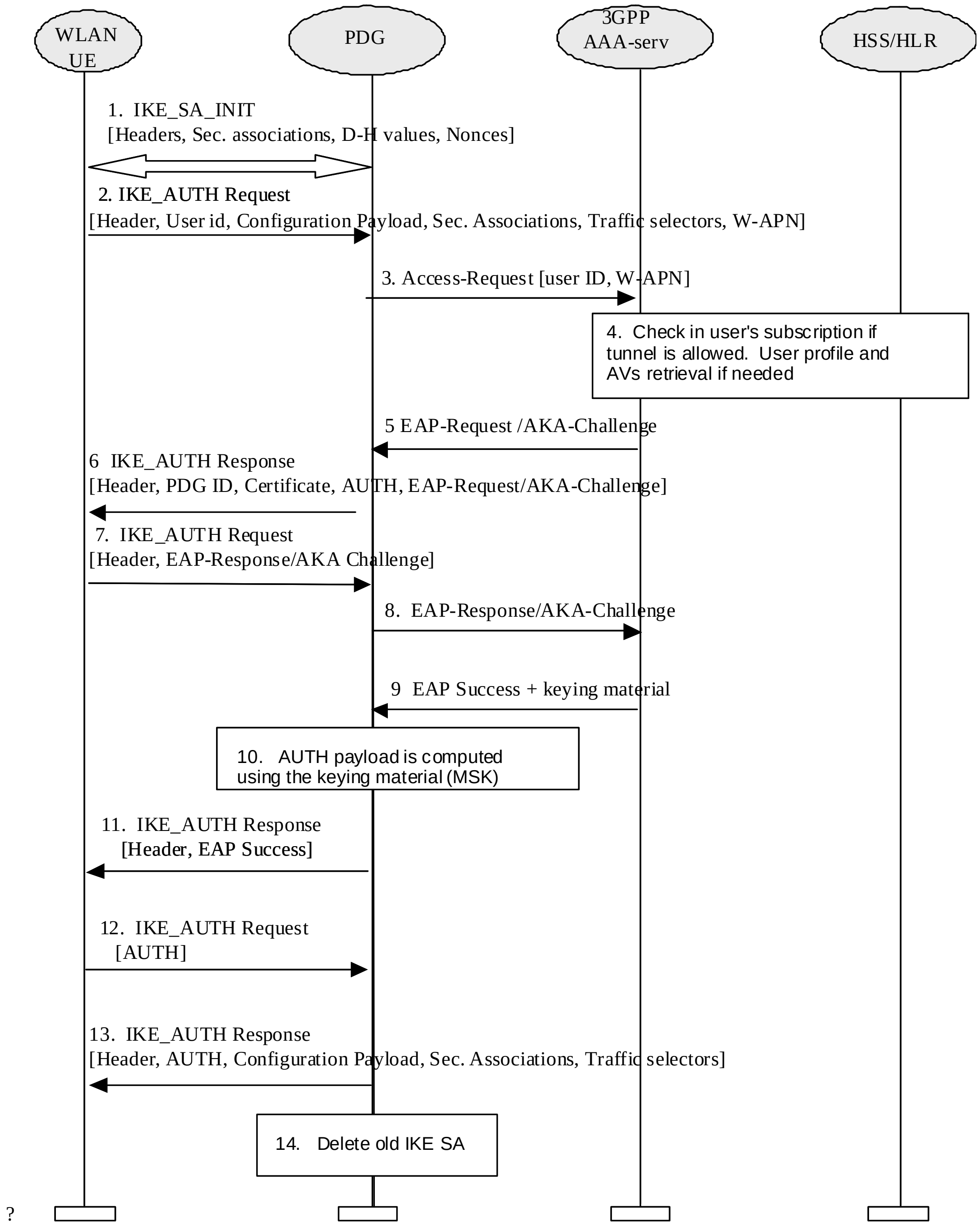

WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Configuration Payload, Sec. Associations, Traffic selectors, W-APN]
3. Access-Request [user ID, W-APN]
4. Check in user's subscription if tunnel is allowed. User profile and AVs retrieval if needed
5 EAP-Request /AKA-Challenge
6 IKE_AUTH Response
[Header, PDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge]
7. IKE_AUTH Request
[Header, EAP-Response/AKA Challenge]
8. EAP-Response/AKA-Challenge
9 EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Configuration Payload, Sec. Associations, Traffic selectors]
14. Delete old IKE SA
?

Figure 7A: Tunnel full authentication and authorization

1. The WLAN UE and the PDG exchange the first pair of messages, known as IKE_SA_INIT, in which the PDG and WLAN UE negotiation cryptographic algorithms, exchange nonces and perform a Diffie_Hellman exchange.

2. The WLAN UE sends the user identity (in the Idi payload) and the W-APN information (in the Idr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The WLAN UE omits the AUTH parameter in order to indicate to the PDG that it wants to use EAP over IKEv2. The user identity shall be compliant with Network Access Identifier (NAI) format specified in RFC 2486 [14], containing the IMSI or the pseudonym. The identity in NAI format generated from the IMSI is described in ref. [4] and ref. [5], depending on the type of EAP method to be used (EAP SIM or EAP AKA). The WLAN UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address.

Editors note: The control of simultaneous sessions in the EAP authentication has to be possible as in WLAN access authentication. Nevertheless, it is needed to study in detail how the parameters to perform this control have to be transferred in EAP/IKEv2. For example, the VPLMN id could be included in the NAI (see TS 23.234 [13], section 5.3.4)

3. The PDG sends the Access Request message with an empty EAP AVP to the AAA server, containing the user identity and W-APN. The PDG shall include a parameter indicating that the authentication is being performed for tunnel establishment, as indicated in reference [37]. This will help the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The AAA server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the AAA server) and determines the EAP method (SIM or AKA) to be used, according to the user subscription and/or the indication received from the WLAN UE. The AAA server checks in user’s subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification

5. The AAA server initiates the authentication challenge. The user identity is not requested again, as in a normal authentication process, because there is the certainty that the user identity received in the EAP Identity Response message has not been modified or replaced by any intermediate node. The reason is that the user identity was received via an IKEv2 secure channel which can only be decrypted and authenticated by the end points (the PDG and the WLAN UE).

6. The PDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the WLAN UE (in the IKE_SA_INIT exchange). It completes the negotiation of the child security associations as well. The EAP message received from the AAA server (EAP-Request/AKA-Challenge is included in order to start the EAP procedure over IKEv2.

7. The WLAN UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message.

8. The PDG forwards the EAP-Response/AKA-Challenge message to the AAA server.

9. When all checks are successful, the AAA server sends an EAP success and the key material to the PDG. This key material shall consist of the MSK generated during the authentication process. When the Wm interface (PDG-AAA server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in ref. [23].

   ~~If t~~The counter of IKE SAs for that W-APN is ~~not active~~stepped up. If the maximum number of IKE SAs for that W-APN is exceeded, the AAA server ~~will mark it as "active".~~shall send an indication to the PDG that established the oldest active IKE SA (it could be the same PDG or a different one) to delete the oldest established IKE SA. The AAA server shall update accordingly the information of IKE SAs active for the W-APN.

   ~~If the AAA server detects that the W-APN is active in other PDG, it will send an indication to that PDG requesting to delete the IKE SA of the W-APN.~~

Editor's note: Registration procedure, including transport of parameters needed to perform simultaneous access control, should be performed in order to update registration status in HSS and fetch the necessary data to the AAA server, but this still needs to be studied in detail.

10. The MSK shall be used by the PDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified in ref. [29]. These two first messages had not been authenticated before as there were no key material available yet. According to ref. [29], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

11. The EAP Success message is forwarded to the WLAN UE over IKEv2.

12. The WLAN UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDG.

13. The PDG checks the correctness of the AUTH received from the WLAN UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The PDG shall send the assigned Remote IP address in the configuration payload (CFG_REPLY), if the WLAN UE requested for a Remote IP address through the

CFG_REQUEST. Then the AUTH parameter is sent to the WLAN UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

14. If the PDG detects that and old IKE SA for that W-APN already exists, it will delete the IKE SA and send the WLAN UE an INFORMATIONAL exchange with a Delete payload, as specified in reference [29], in order to delete the old IKE SA in WLAN UE.

6.1.5.2 Tunnel fast re-authentication and authorization

This process is very similar to the tunnel full authentication and authorization. The only difference is that EAP fast re-authentication is used in this case.

The sequence diagram is shown in figure 7B. The EAP message parameters and procedures regarding fast re-authentication are omitted since they are already described in this technical specification. Only decisions and processes relevant to this EAP-IKEv2 procedure are explained.

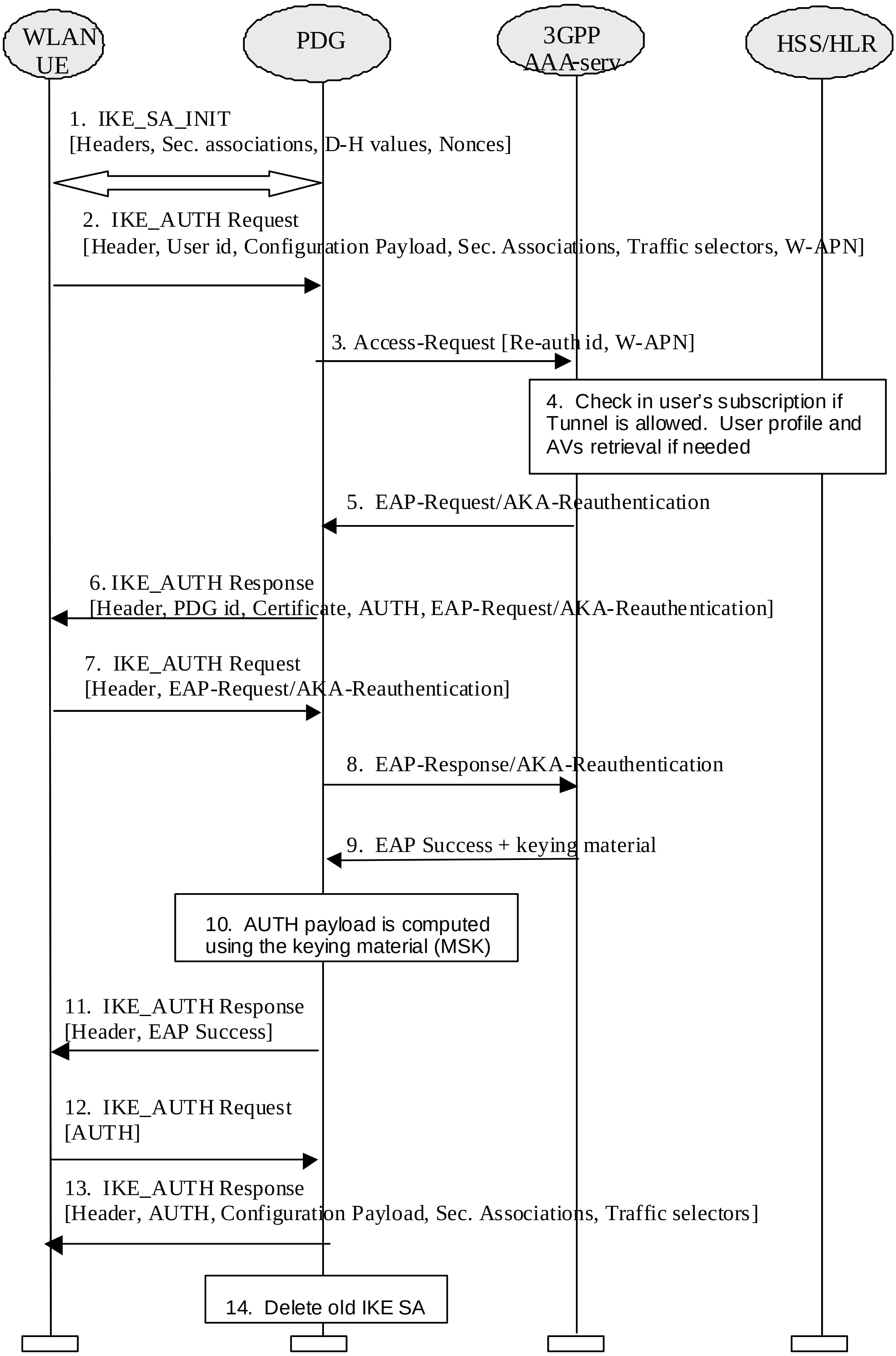

WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Configuration Payload, Sec. Associations, Traffic selectors, W-APN]
3. Access-Request [Re-auth id, W-APN]
4. Check in user's subscription if Tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Reauthentication
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Reauthentication]
7. IKE_AUTH Request
[Header, EAP-Request/AKA-Reauthentication]
8. EAP-Response/AKA-Reauthentication
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Configuration Payload, Sec. Associations, Traffic selectors]
14. Delete old IKE SA

Figure 7B: Tunnel fast re-authentication and authorization

1. The WLAN UE and the PDG exchange the first pair of messages, known as IKE_SA_INIT, in which the PDG and WLAN UE negotiation cryptographic algorithms, exchange nonces and perform a Diffie_Hellman exchange.

2. The WLAN UE sends the re-authentication identity (in the Idi payload) and the W-APN information (in the Idr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations.

The WLAN UE omits the AUTH parameter in order to indicate to the PDG that it wants to use EAP over IKEv2. The re-authentication identity used by the WLAN UE shall be the one received in the previous authentication process. The WLAN UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address.

3. The PDG sends the Access Request message with an empty EAP AVP to the AAA server, containing the re-authentication identity and W-APN. The PDG shall include a parameter indicating that the authentication is being performed for tunnel establishment, as indicated in ref. [37]. This will help the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The AAA server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the AAA server) and determines the EAP method (SIM or AKA) to be used, according to the user subscription. The AAA server checks in user's subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification.

5. The AAA server initiates the fast re-authentication challenge.

6. The PDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the WLAN UE (in the IKE_SA_INIT exchange). It completes the negotiation of the child security associations as well. The EAP message received from the AAA server (EAP-Request/AKA-Reauthentication is included in order to start the EAP procedure over IKEv2.

7. The WLAN UE checks the authentication parameters and responds to the fast re-authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message.

8. The PDG forwards the EAP-Response/AKA-Reauthentication message to the AAA server.

9. When all checks are successful, the AAA server sends an EAP success and the key material to the PDG. This key material shall consist of the MSK generated during the fast re-authentication process. When the Wm interface (PDG-AAA server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in ref. [23].

   ~~If t~~The counter of IKE SAs for that W-APN is ~~not active~~ stepped up. If the maximum number of IKE SAs for that W-APN is exceeded, the AAA server ~~will mark it as "active"~~shall send an indication to the PDG that established the oldest active IKE SA (it could be the same PDG or a different one) to delete the oldest established IKE SA. The AAA server shall update accordingly the information of IKE SAs active for the W-APN.

   ~~If the AAA server detects that the W-APN is active in other PDG, it will send an indication to that PDG requesting to delete the IKE SA of the W-APN.~~

10. The MSK shall be used by the PDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified in ref. [29]. These two first messages had not been authenticated before as there were no key material available yet. According to ref. [29], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

11. The EAP Success message is forwarded to the WLAN UE over IKEv2.

12. The WLAN UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDG.

13. The PDG checks the correctness of the AUTH received from the WLAN UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The PDG shall send the assigned Remote IP address in the configuration payload (CFG_REPLY), if the WLAN UE requested for a Remote IP address through the CFG_REQUEST. Then the AUTH parameter is sent to the WLAN UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

14. If the PDG detects that and old IKE SA for that W-APN already exists, it will delete the IKE SA and send to the WLAN UE an INFORMATIONAL exchange with a Delete payload, as specified in reference [29], in order to delete the old IKE SA in WLAN UE.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050160

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**060**	⌘**rev**	**2**	⌘	Current version:	**6.3.0**	⌘

*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:	⌘ Removal of editors' notes		
Source:	⌘ SA WG3		
Work item code:	⌘ WLAN	***Date:***	⌘ 09/02/2005
Category:	⌘ **D**	***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:	⌘ There are still some editor’s notes in TS 33.234, which can be removed from Rel-6.
Summary of change:	⌘ Remove the editor’s notes.
Consequences if not approved:	⌘ Outdated editors information left in the TS

Clauses affected:	⌘	3.1, 4.2.4.3, 4.2.5, 6.1.1, 6.1.2, 6.1.5.1			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	Any enhancements, identified by SA3,to SIM Access Profile developed in BLUETOOTH SIG , will be addressed by 3GPP and the Bluetooth SIG in R7.			

*** BEGIN OF CHANGE ***

3.1 Definitions

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

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards.

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.

Local interface: an interface between the devices that may conform to the WLAN UE, normally one device with WLAN capabilities and one UICC or SIM card holding device.

Temporary identity: an identity given by the home network to the WLAN UE, used to identify the user temporarily, normally in one authentication process lifetime. In this TS it refers to a pseudonym or a re-authentication identity.

Tunnel: it refers to an IPsec security association used in WLAN 3GPP IP access to protect the communications from the WLAN UE to the 3GPP network. It is preceded by an IKE negotiation.

W-APN: WLAN Access Point Name – identifies an IP network and a point of interconnection to that network (Packet Data Gateway).

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

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

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.

~~Editors note: This WLAN-UE definition needs to be reflected in related specifications.~~

*** NEXT CHANGE ***

4.2.4.3 Communication over local interface via a Bluetooth link

For SIM access via a Bluetooth link, the SIM Access Profile developed in BLUETOOTH SIG forum may be used. See [22].

~~Editor note: The version of the SIM Access Profile specification in the reference needs to be updated, if SA3 decides that a new version is required.~~

*** NEXT CHANGE ***

4.2.5 Link layer security requirements

~~Editors note: This section is FFS, LS (S3-030167) sent to SA2 group on 1) the need for requiring 802.11i in TS 23.234. SA2 to explain the impact (if any) a change of technology from 802.11i to WPA would have on the standardisation work. 2) SA2 to study the architectural impacts of implementing protection on Wa interface 3) SA2 to Investigate the importance of specifying specific WLAN technologies to be used for the WLAN access network.~~

Most WLAN technologies provide (optional) link-layer protection of user data. Since the wireless link is likely to be the most vulnerable in the entire system, 3GPP-WLAN interworking should take advantage of the link layer security provided by WLAN technologies. The native link-layer protection can also prevent against certain IP-layer attacks.

*** NEXT CHANGE ***

6.1.1 USIM-based WLAN Access Authentication

USIM based authentication is a proven solution that satisfies the authentication requirements from section 4.2. This form of authentication shall be based on EAP-AKA (ref. [4]), as described in section 6.1.1.1. For the case of WLAN-UE Functional Split, see section 4.2.4.

~~Editor's note: also see section 4.2.4 on WLAN-UE Functional Split.~~

*** NEXT CHANGE ***

6.1.2 GSM SIM based WLAN Access authentication

SIM based authentication is useful for GSM subscribers that do not have a UICC with a USIM application. This form of authentication shall be based on EAP-SIM (ref. [5]), as described in section 6.1.2.1. This authentication method satisfies the authentication requirements from section 4.2, without the need for a UICC with a USIM application. For the case of WLAN-UE Functional Split, see section 4.2.4.

~~Editor's note: Also see section 4.2.4 on WLAN UE split.~~

*** NEXT CHANGE ***

6.1.5.1 Tunnel full authentication and authorization

The tunnel end point in the network is the PDG. As part of the tunnel establishment attempt the use of a certain W-APN is requested. When a new attempt for tunnel establishment is performed by the WLAN UE, the WLAN UE shall use IKEv2 as specified in ref. [29]. The EAP messages carried over IKEv2 shall be terminated in the AAA server, which communicates with the PDG via Wm interface, implemented with Diameter. Then the PDG shall extract the EAP messages received from the WLAN UE over IKEv2, and send them to the AAA server over Diameter (the opposite for messages sent from the AAA server). The WLAN UE shall use the Configuration Payload of IKEv2 to obtain the Remote IP address.

The sequence diagram is shown in figure 7A. The EAP message parameters and procedures regarding authentication are omitted since they are already described in this technical specification. Only decisions and processes relevant to this EAP-IKEv2 procedure are explained.

As the WLAN UE and PDG generated nonces are used as input to derive the encryption and authentication keys in IKEv2, replay protection is implemented as well. For this reason, there is no need for the AAA server to request the user identity again using the EAP AKA or EAP SIM specific methods (as specified in ref. [4] and ref. [5]), because the AAA server is certain that no intermediate node has modified or changed the user identity.

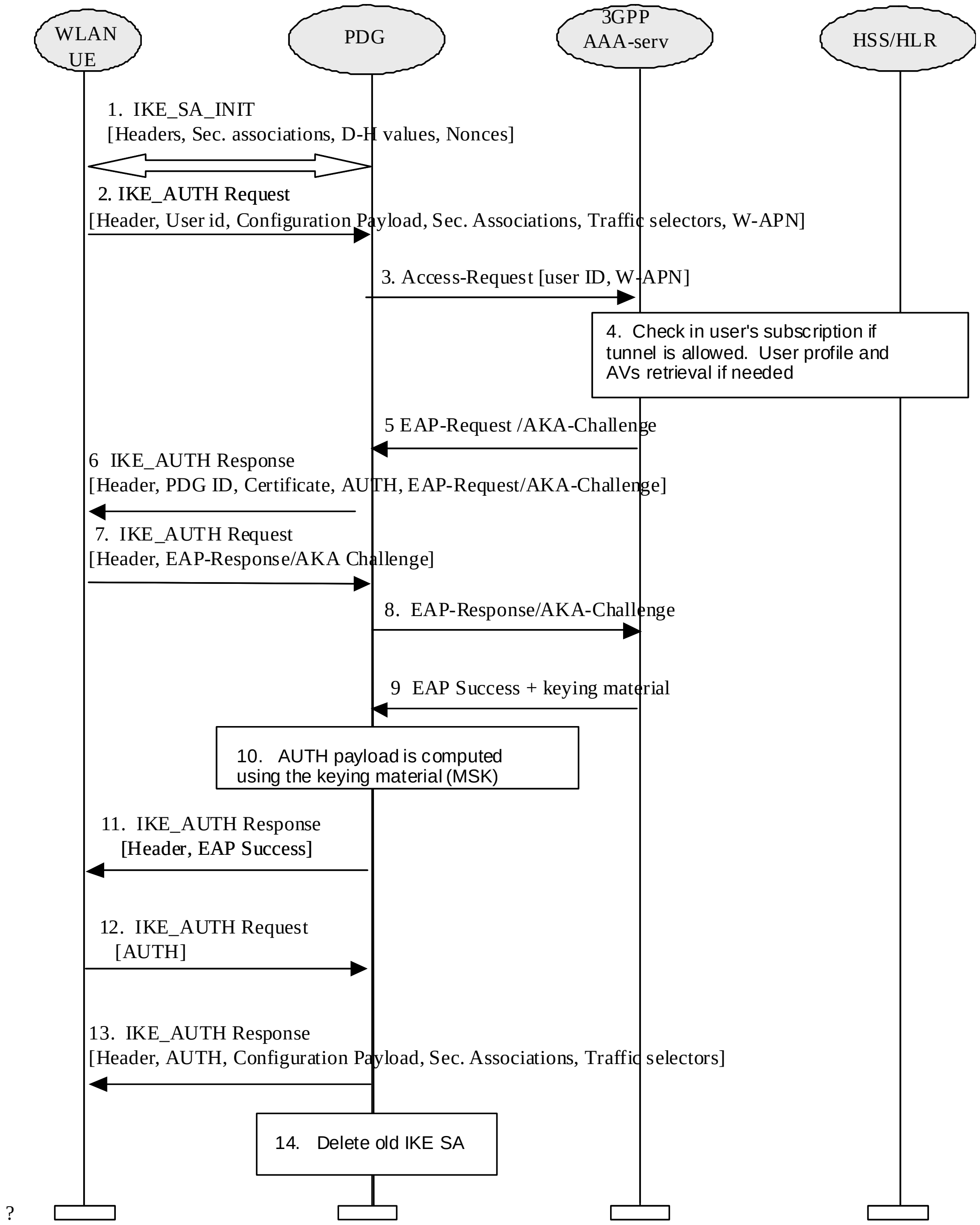

WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Configuration Payload, Sec. Associations, Traffic selectors, W-APN]
3. Access-Request [user ID, W-APN]
4. Check in user's subscription if tunnel is allowed. User profile and AVs retrieval if needed
5 EAP-Request /AKA-Challenge
6 IKE_AUTH Response
[Header, PDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge]
7. IKE_AUTH Request
[Header, EAP-Response/AKA Challenge]
8. EAP-Response/AKA-Challenge
9 EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Configuration Payload, Sec. Associations, Traffic selectors]
14. Delete old IKE SA
?

Figure 7A: Tunnel full authentication and authorization

1. The WLAN UE and the PDG exchange the first pair of messages, known as IKE_SA_INIT, in which the PDG and WLAN UE negotiation cryptographic algorithms, exchange nonces and perform a Diffie_Hellman exchange.

2. The WLAN UE sends the user identity (in the Idi payload) and the W-APN information (in the Idr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The WLAN UE omits the AUTH parameter in order to indicate to the PDG that it wants to use EAP over IKEv2. The user identity shall be compliant with Network Access Identifier (NAI) format specified in RFC 2486 [14], containing the IMSI or the pseudonym. The identity in NAI format generated from the IMSI is described in ref. [4] and ref. [5], depending on the type of EAP method to be used (EAP SIM or EAP AKA). The WLAN UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address.

~~Editors note: The control of simultaneous sessions in the EAP authentication has to be possible as in WLAN access authentication. Nevertheless, it is needed to study in detail how the parameters to perform this control have to be transferred in EAP/IKEv2. For example, the VPLMN id could be included in the NAI (see TS 23.234 [13], section 5.3.4)~~

3. The PDG sends the Access Request message with an empty EAP AVP to the AAA server, containing the user identity and W-APN. The PDG shall include a parameter indicating that the authentication is being performed for tunnel establishment, as indicated in reference [37]. This will help the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The AAA server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the AAA server) and determines the EAP method (SIM or AKA) to be used, according to the user subscription and/or the indication received from the WLAN UE. The AAA server checks in user's subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification

5. The AAA server initiates the authentication challenge. The user identity is not requested again, as in a normal authentication process, because there is the certainty that the user identity received in the EAP Identity Response message has not been modified or replaced by any intermediate node. The reason is that the user identity was received via an IKEv2 secure channel which can only be decrypted and authenticated by the end points (the PDG and the WLAN UE).

6. The PDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the WLAN UE (in the IKE_SA_INIT exchange). It completes the negotiation of the child security associations as well. The EAP message received from the AAA server (EAP-Request/AKA-Challenge is included in order to start the EAP procedure over IKEv2.

7. The WLAN UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message.

8. The PDG forwards the EAP-Response/AKA-Challenge message to the AAA server.

9. When all checks are successful, the AAA server sends an EAP success and the key material to the PDG. This key material shall consist of the MSK generated during the authentication process. When the Wm interface (PDG-AAA server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in ref. [23].

   If the W-APN is not active, the AAA server will mark it as "active".

   If the AAA server detects that the W-APN is active in other PDG, it will send an indication to that PDG requesting to delete the IKE SA of the W-APN.

~~Editor's note: Registration procedure, including transport of parameters needed to perform simultaneous access control, should be performed in order to update registration status in HSS and fetch the necessary data to the AAA server, but this still needs to be studied in detail.~~

10. The MSK shall be used by the PDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified in ref. [29]. These two first messages had not been authenticated before as there were no key material available yet. According to ref. [29], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

11. The EAP Success message is forwarded to the WLAN UE over IKEv2.

12. The WLAN UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDG.

*** END OF CHANGE ***

3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050181

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**061**	⌘ **rev**	**1**	⌘	Current version:	**6.3.0**	⌘

*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:	⌘ Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages		
Source:	⌘ SA WG3		
Work item code:	⌘ WLAN	***Date:*** ⌘	5/02/2005
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:	⌘ In WLAN direct IP access if there is an ongoing WLAN Access session for the subscriber there is no way to distinguish whether a new authentication attempt is valid when it has same MAC addresses as the ongoing WLAN Access session, but with different WLAN radio networks information, because it may be a request of setting up a simultaneous session or a pre-authentication.
Summary of change:	⌘ The Diameter/RADIUS accounting start message can be used to detect that a WLAN Direct IP Access session is created. In the case described above if there is an accounting start message sent from WLAN AN after the new authentication procedure completes, this simultaneous session is a fraud one and should be stopped.
Consequences if not approved:	⌘ There is still no method to distinguish simultaneous session from pre-authentication in WLAN direct IP access if the new authentication attempt has same MAC addresses as the ongoing WLAN Access session, but with different WLAN radio networks information, so that there may exist a fraud simultaneous session if the new authentication attempt isn't a pre-authentication.

Clauses affected:	⌘	5.7, 6.1.1, 6.1.2, a new added section 6.1.6			
		Y	**N**		
Other specs affected:	⌘	X		Other core specifications	⌘ 23.234, 24.234
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

*** BEGIN OF CHANGE ***

5.7 Simultaneous access control

The home network operator needs to be aware of how the user is accessing the WLAN network. If the user is making the SIM or UICC card available for several devices that have WLAN access capabilities, the home network operator may decide, at any time, to allow or bar t he access of two or more network devices simultaneously.

WLAN direct IP access

The control of simultaneous sessions in WLAN direct IP access can be performed, under some circumstances, using the MAC address of the user's device.

After a number of successful authentications, if a subsequent authentication attempt is being performed by another device, the MAC address will be different and the AAA server will be able to detect it. However, this mechanism has some limitations. One of them is that if the two devices are accessing two different WLAN access points (assuming that a WLAN access point has a independent control of MAC address space), the MAC address of one of them can be spoofed and made equal to the other one. This is a fraud situation the home network should avoid. However, it may happen that the user is accessing other WLAN access point and a pre-authentication is performed in this new access point. In this case there is no fraud attempt. Then, in this situation (same MAC addresses, different WLAN radio networks) the AAA server should check if there is a AAA accounting start message sent from WLAN AN after the authentication procedure completes. If there is such accounting start message and the number of simultaneous sessions for the subscriber has already been reached, it is considered to be a fraud attempt and the AAA server should send a message to WLAN AN to stop this simultaneous session.~~will not be able to distinguish between a legal and a fraud situation and shall not reject the authentication process.~~

*** NEXT CHANGE ***

6.1.1.1 EAP/AKA Procedure

The EAP-AKA authentication mechanism is specified in ref. [4]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.

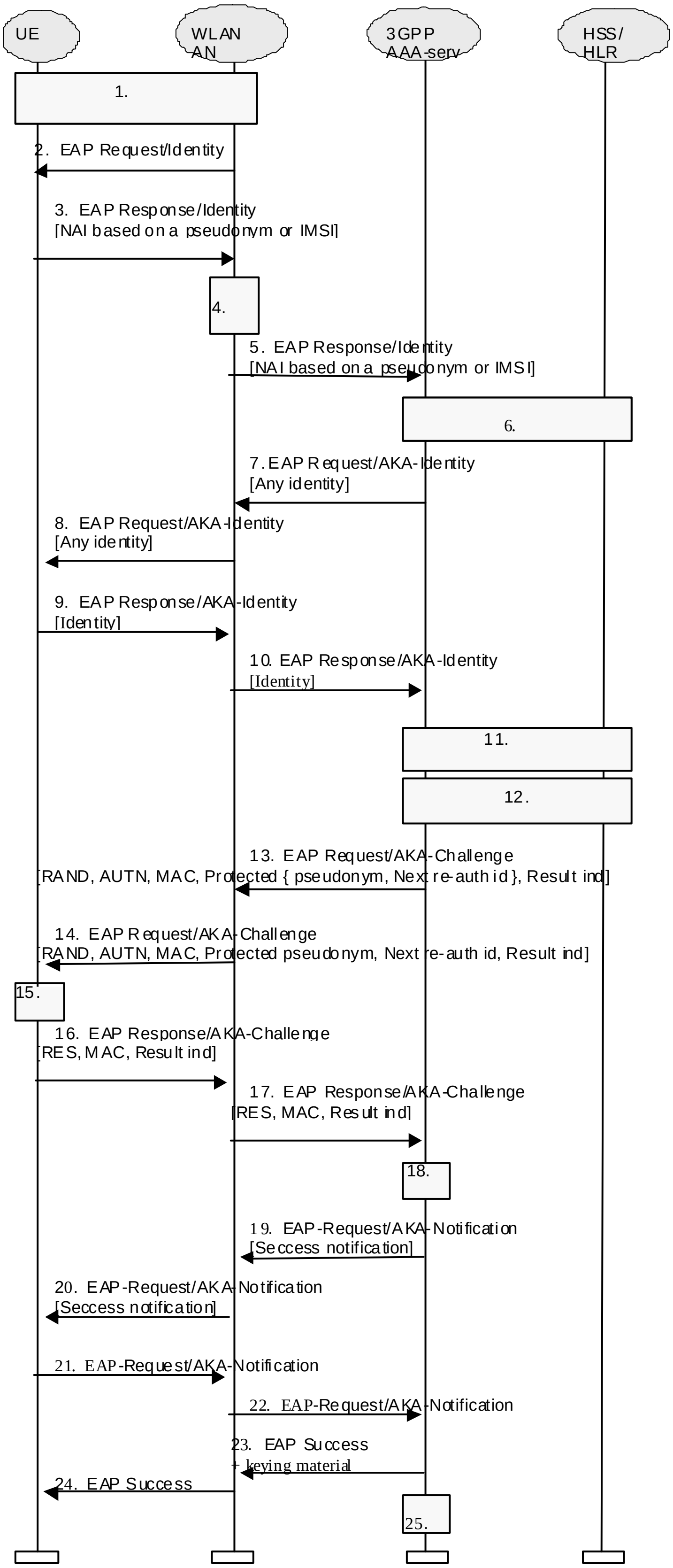

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6.
7. EAP Request/AKA-Identity [Any identity]
8. EAP Request/AKA-Identity [Any identity]
9. EAP Response/AKA-Identity [Identity]
10. EAP Response/AKA-Identity [Identity]
11.
12.
13. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Protected { pseudonym, Next re-auth id }, Result ind]
14. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Protected pseudonym, Next re-auth id, Result ind]
15.
16. EAP Response/AKA-Challenge [RES, MAC, Result ind]
17. EAP Response/AKA-Challenge [RES, MAC, Result ind]
18.
19. EAP-Request/AKA-Notification [Seccess notification]
20. EAP-Request/AKA-Notification [Seccess notification]
21. EAP-Request/AKA-Notification
22. EAP-Request/AKA-Notification
23. EAP Success + keying material
24. EAP Success
25.

Figure 4: Authentication based on EAP AKA scheme

1. A connection is established between the WLAN-UE and the WLAN-AN, using a Wireless LAN technology specific procedure (out of scope for this specification).

2. The WLAN-AN sends an EAP Request/Identity to the WLAN-UE.

   EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

3. The WLAN-UE sends an EAP Response/Identity message. The WLAN-UE sends its identity complying with Network Access Identifier (NAI) format specified in RFC 2486. NAI contains either a pseudonym allocated to the WLAN-UE in previous authentication or, in the case of first authentication, the IMSI.

NOTE 1: Generating an identity conforming to NAI format from IMSI is defined in EAP/AKA [4].

4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI. The routing path may include one or several AAA proxies (not shown in the figure).

NOTE 2: Diameter referral can also be applied to find the AAA server.

5. The 3GPP AAA server receives the EAP Response/Identity packet that contains the subscriber identity. The identifier of the WLAN radio network, VPLMN Identity and the MAC address of the WLAN-UE shall also be received by the 3GPP AAA server in the same message.

6. 3GPP AAA Server identifies the subscriber as a candidate for authentication with EAP-AKA, based on the received identity. The 3GPP AAA Server then checks that it has an unused authentication vector available for that subscriber . If not, a set of new authentication vectors is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required.

   The HSS/HLR shall check if there is a 3GPP AAA server already registered to serve for this subscriber In case the HSS/HLR detects that another 3GPP AAA server has already registered for this subscriber, it shall provide the current 3GPP AAA server with the previously registered AAA server address. The authentication signalling is then routed to the previously registered 3GPP AAA server with Diameter-specific mechanisms, e.g., the current 3GPP AAA server transfers the previously registered AAA server address to the AAA proxy or the WLAN AN, or the current 3GPP AAA server acts as a AAA proxy and forwards the authentication message to the previously registered 3GPP AAA server.

NOTE 3: It could also be the case that the 3GPP AAA Server first obtains an unused authentication vector for the subscriber and, based on the type of authenticator vector received (i.e. if a UMTS authentication vector is received), it regards the subscriber as a candidate for authentication with EAP-AKA.

7. The 3GPP AAA server requests again the user identity, using the EAP Request/AKA Identity message. This identity request is performed as the intermediate nodes may have changed or replaced the user identity received in the EAP Response Identity message, as specified in ref. [4]. However, this new request of the user identity can be omitted by the home operator if there exist the certainty that the user identity could not be changed or modifies by any means in the EAP Response Identity message.

8. The WLAN AN forwards the EAP Request/AKA Identity message to the WLAN UE.

9. The WLAN UE responds with the same identity it used in the EAP Response Identity message.

10. The WLAN AN forwards the EAP Response/AKA Identity to the 3GPP AAA server. The identity received in this message will be used by the 3GPP AAA server in the rest of the authentication process. If an inconsistency is found between the identities received in the two messages (EAP Response Identity and EAP Response/AKA Identity) so that the user profile and authentication vectors previously retrieved from HSS/HLR are not valid, these data shall be requested again to HSS/HLR (step 6 shall be repeated before continuing with step 11).

NOTE 4: In order to optimise performance, the identity re-request process (the latter four steps) should be performed when the 3GPP AAA server has enough information to identify the user as an EAP-AKA user, and before user profile and authentication vectors retrieval, although protocol design in Wx interface may not allow to perform these four steps until the whole user profile has been downloaded to the 3GPP AAA server.

11. 3GPP AAA server checks that it has the WLAN access profile of the subscriber available. If not, the profile is retrieved from HSS. 3GPP AAA Server verifies that the subscriber is authorized to use the WLAN service.

Although this step is presented after step 6 in this example, it could be performed at some other point, however before step 14. (This will be specified as part of the Wx interface.)

12. New keying material is derived from IK and CK., cf. [4]. This keying material is required by EAP-AKA, and some extra keying material may also be generated for WLAN technology specific confidentiality and/or integrity protection.

    A new pseudonym and/or re-authentication ID may be chosen and protected (i.e. encrypted and integrity protected) using EAP-AKA generated keying material.

13. 3GPP AAA Server sends RAND, AUTN, a message authentication code (MAC) and two user identities (if they are generated): protected pseudonym and/or protected re-authentication id to WLAN-AN in EAP Request/AKA-Challenge message. The sending of the re-authentication id depends on 3GPP operator's policies on whether to allow fast re-authentication processes or not. It implies that, at any time, the AAA server decides (based on policies set by the operator) to include the re-authentication id or not, thus allowing or disallowing the triggering of the fast re-authentication process.

    The 3GPP AAA Server may send as well a result indication to the WLAN UE, in order to indicate that it wishes to protect the success result message at the end of the process (if the outcome is successful). The protection of result messages depends on home operator's policies.

14. The WLAN-AN sends the EAP Request/AKA-Challenge message to the WLAN-UE.

15. The WLAN-UE runs UMTS algorithm on the USIM. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of synch, terminal initiates a synchronization procedure, c.f. [4]. If AUTN is correct, the USIM computes RES, IK and CK.

    The WLAN UE derives required additional new keying material from the new computed IK and CK from the USIM, checks the received MAC with the new derived keying material.

    If a protected pseudonym and/or re-authentication identity were received, then the WLAN-UE stores the temporary identity(s) for future authentications.

16. The WLAN UE calculates a new MAC value covering the EAP message with the new keying material. WLAN-UE sends EAP Response/AKA-Challenge containing calculated RES and the new calculated MAC value to WLAN-AN.

    The WLAN UE shall include in this message the result indication if it received the same indication from the 3GPP AAA server. Otherwise, the WLAN-UE shall omit this indication.

17. WLAN-AN sends the EAP Response/AKA-Challenge packet to 3GPP AAA Server

18. The 3GPP AAA Server checks the received MAC and compares XRES to the received RES.

19. If all checks in step 18 are successful, the 3GPP AAA Server shall send the message EAP Request/AKA-Notification, previous to the EAP Success message, if the 3GPP AAA Server requested previously to use protected successful result indications. This message is MAC protected.

20. The WLAN AN forwards the message to the WLAN-UE.

21. The WLAN-UE sends the EAP Response/AKA-Notification.

22. The WLAN AN forwards the EAP Response/AKA-Notification message to the 3GPP AAA server. The 3GPP AAA Server shall ignore the contents of this message

23. The 3GPP AAA Server sends the EAP Success message to WLAN-AN (perhaps preceded by an EAP Notification, as explained in step 20). If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection then the 3GPP AAA Server includes this keying material in the underlying AAA protocol message (i.e. not at the EAP level). The WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.

24. The WLAN-AN informs the WLAN-UE about the successful authentication with the EAP Success message. Now the EAP AKA exchange has been successfully completed, and the WLAN-UE and the WLAN-AN share keying material derived during that exchange.

25. ~~If there is no other ongoing WLAN Access session for the subscriber detected by the 3GPP AAA server, and the WLAN registration for this subscriber is not performed previously, then the 3GPP AAA server shall initiate the WLAN registration to the HSS/HLR. Otherwise, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN access network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for old sessions. If it is the same subscriber but with a different MAC address, or with a different VPLMN identity or with different radio network information that is received than in any ongoing session, the 3GPP AAA server then considers that the authentication exchange is related to a new WLAN Access session. It shall terminate an old WLAN Access session after the successful authentication of the new WLAN Access session, based on the policy whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded. The exception in this process is when the MAC addresses (the old one and the new one) are equal and the WLAN radio network information received is different from the old one. In that case the authentication process continues normally.~~The procedure of WLAN registration for this subscriber is described in clause 6.1.6.

The authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN-UE after a network request. In that case, the EAP AKA process will be terminated as specified in ref. [4] and an indication shall be sent to HSS/HLR.

*** NEXT CHANGE ***

6.1.2.1 EAP SIM procedure

The EAP-SIM authentication mechanism is specified in ref. [5]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.

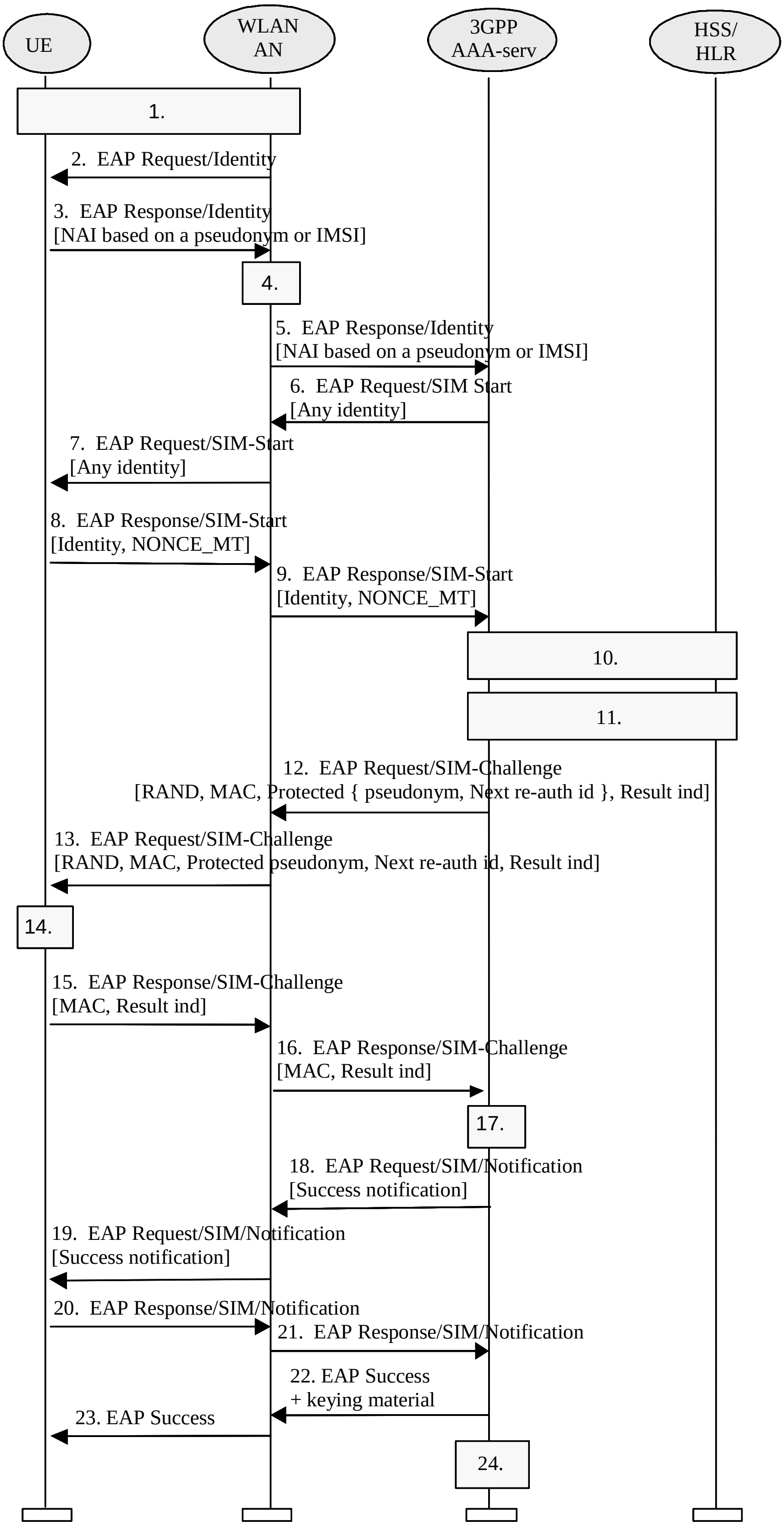

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6. EAP Request/SIM Start [Any identity]
7. EAP Request/SIM-Start [Any identity]
8. EAP Response/SIM-Start [Identity, NONCE_MT]
9. EAP Response/SIM-Start [Identity, NONCE_MT]
10.
11.
12. EAP Request/SIM-Challenge [RAND, MAC, Protected { pseudonym, Next re-auth id }, Result ind]
13. EAP Request/SIM-Challenge [RAND, MAC, Protected pseudonym, Next re-auth id, Result ind]
14.
15. EAP Response/SIM-Challenge [MAC, Result ind]
16. EAP Response/SIM-Challenge [MAC, Result ind]
17.
18. EAP Request/SIM/Notification [Success notification]
19. EAP Request/SIM/Notification [Success notification]
20. EAP Response/SIM/Notification
21. EAP Response/SIM/Notification
22. EAP Success + keying material
23. EAP Success
24.

Figure 5: Authentication based on EAP SIM scheme

1. A connection is established between the WLAN-UE and the WLAN-AN, using a Wireless LAN technology specific procedure (out of scope for this specification).

2. The WLA-AN sends an EAP Request/Identity to the WLAN-UE.

   EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

3. The WLAN-UE sends an EAP Response/Identity message. The WLAN-UE sends its identity complying with the Network Access Identifier (NAI) format specified in RFC 2486. NAI contains either a pseudonym allocated to WLAN-UE in previous authentication or, in the case of first authentication, the IMSI.

NOTE 1: Generating an identity conforming to NAI format from IMSI is defined in EAP/SIM.

4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI. The routing path may include one or several AAA proxies (not shown in the figure).

NOTE 2: Diameter referral can also be applied to find the AAA server.

5. The 3GPP AAA server receives the EAP Response/Identity packet that contains the subscriber identity. The identifier of the WLAN radio network, VPLMN Identity and the MAC address of the WLAN-UE shall also be received by the 3GPP AAA server in the same message.

6. The 3GPP AAA Server, identifies the subscriber as a candidate for authentication with EAP-SIM, based on the received identity, and then it sends the EAP Request/SIM-Start packet to WLAN-AN. The 3GPP AAA server requests again the user identity. This identity request is performed as the intermediate nodes may have changed or replaced the user identity received in the EAP Response Identity message, as specified in ref. [5]. However, this new request of the user identity can be omitted by the home operator if there exist the certainty that the user identity could not be changed or modified by any means in the EAP Response Identity message.

NOTE 3: It could also be the case that the 3GPP AAA Server first obtains an authentication vector for the subscriber and, based on the type of authenticator vector received (i.e. if a GSM authentication vector is received), it regards the subscriber as a candidate for authentication with EAP-SIM.

7. WLAN-AN sends the EAP Request/SIM-Start packet to WLAN-UE

8. The WLAN-UE chooses a fresh random number NONCE_MT. The random number is used in network authentication. The WLAN UE includes the same user identity it used in the EAP Response Identity message.

   The WLAN-UE sends the EAP Response/SIM-Start packet, containing NONCE_MT and the user identity, to WLAN-AN.

9. WLAN-AN sends the EAP Response/SIM-Start packet to 3GPP AAA Server. The identity received in this message will be used by the 3GPP AAA server in the rest of the authentication process. If an inconsistency is found between the identities received in the two messages (EAP Response Identity and EAP Response/SIM Start) so that any user data retrieved previously from HSS/HLR are not valid, these data shall be requested again to HSS/HLR.

10. The AAA server checks that it has available N unused authentication vectors for the subscriber. Several GSM authentication vectors are required in order to generate keying material with effective length equivalent to EAP-AKA. If N authentication vectors are not available, a set of authentication vectors is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required.

    Although this step is presented after step 9 in this examples, it could be performed at some other point, for example after step 5, however before step 12. (This will be specified as part of the Wx interface).

    The HSS/HLR shall check if there is a 3GPP AAA server already registered to serve for this subscriber. In case the HSS/HLR detects that another 3GPP AAA server has already registered for this subscriber, it shall provide the current 3GPP AAA server with the previously registered AAA server address. The authentication signalling is then routed to the previously registered 3GPP AAA server with Diameter-specific mechanisms, e.g., the current 3GPP AAA server transfers the previously registered AAA server address to the AAA proxy or the WLAN AN, or the current 3GPP AAA server acts as a AAA proxy and forwards the authentication message to the previously registered 3GPP AAA server.

11. The AAA server checks that it has the WLAN access profile of the subscriber available. If not, the profile is retrieved from HSS/HLR. 3GPP AAA Server verifies that the subscriber is authorized to use the WLAN service.

    Although this step is presented after step 10 in this example, it could performed at some other point, however before step 18. (This will be the specified as part of the Wx interface).

12. New keying material is derived from NONCE_MT and N Kc keys. This keying material is required by EAP-SIM, and some extra keying material may also be generated for WLAN technology specific confidentiality and/or integrity protection.

    A new pseudonym and/or a re-authentication identity may be chosen and protected (i.e. encrypted and integrity protected) using EAP-SIM generated keying material.

    A message authentication code (MAC) is calculated over the EAP message using an EAP-SIM derived key. This MAC is used as a network authentication value.

    3GPP AAA Server sends RAND, MAC, protected pseudonym and protected re-authentication identity (the two latter in case they were generated) to WLAN-AN in EAP Request/SIM-Challenge message. The sending of the re-authentication id depends on 3GPP operator's policies on whether to allow fast re-authentication processes or not. It implies that, at any time, the AAA server decides (based on policies set by the operator) to include the re-authentication id or not, thus allowing or disallowing the triggering of the fast re-authentication process.

    The 3GPP AAA Server may send as well a result indication to the WLAN-UE, in order to indicate that it wishes to protect the success result message at the end of the process (if the outcome is successful). The protection of result messages depends on home operator's policies.

13. The WLAN sends the EAP Request/SIM-Challenge message to the WLAN-UE.

14. WLAN-UE runs N times the GSM A3/A8 algorithms in the SIM, once for each received RAND.

    This computing gives N SRES and Kc values.

    The WLAN-UE derives additional keying material from N Kc keys and NONCE_MT.

    The WLAN-UE calculates its copy of the network authentication MAC with the newly derived keying material and checks that it is equal with the received MAC. If the MAC is incorrect, the network authentication has failed and the WLAN-UE cancels the authentication (not shown in this example). The WLAN-UE continues the authentication exchange only if the MAC is correct.

    The WLAN-UE calculates a new MAC with the new keying material covering the EAP message concatenated to the N SRES responses.

    If a protected pseudonym and/or re-authentication identity were received, then the WLAN-UE stores the temporary identity(s) for future authentications.

15. WLAN-UE sends EAP Response/SIM-Challenge containing calculated MAC to WLAN-AN.

    The WLAN-UE shall include in this message the result indication if it received the same indication from the 3GPP AAA server. Otherwise, the WLAN-UE shall omit this indication.

16. WLAN-AN sends the EAP Response/SIM-Challenge packet to 3GPP AAA Server.

17. 3GPP AAA Server compares its copy of the response MAC with the received MAC.

18. Once the comparison in step 17 is successful, the 3GPP AAA Server shall send the message EAP Request/SIM/Notification, previous to the EAP Success message, if the 3GPP AAA Server requested previously to use protected success result indications. The message EAP Request/SIM/Notification is MAC protected.

19. The WLAN AN forwards the message to the WLAN-UE.

20. The WLAN-UE sends the EAP Response/SIM/Notification.

21. The WLAN AN forwards the EAP Response/SIM/Notification message to the 3GPP AAA server. The 3GPP AAA Server shall ignore the contents of this message.

22. The 3GPP AAA Server sends the EAP Success message to WLAN-AN (perhaps preceded by an EAP Notification, as explained in step 20). If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection, then the 3GPP AAA Server includes this derived keying material in the underlying AAA protocol message. (i.e. not at EAP level). The WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.

23. WLAN-AN informs the WLAN-UE about the successful authentication with the EAP Success message. Now the EAP SIM exchange has been successfully completed, and the WLAN-UE and the WLAN_AN may share keying material derived during that exchange.

24. ~~If there is no other ongoing WLAN Access session for the subscriber detected by the 3GPP AAA server, and the WLAN registration for this subscriber is not performed previously, then the 3GPP AAA server shall initiate the WLAN registration to the HSS/HLR.~~

~~Otherwise, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN access network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for old sessions. If it is the same subscriber but with a different MAC address, or with a different VPLMN identity, or with different radio network information that is received than in any ongoing session, the 3GPP AAA server then considers that the authentication exchange is related to a new WLAN Access session. It shall terminate an old WLAN Access session after the successful authentication of the new WLAN Access session, based on whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded. The exception in this process is when the MAC addresses (the old one and the new one) are equal and the WLAN radio network information received is different from the old one. In that case the authentication process continues normally.~~The procedure of WLAN registration for this subscriber is described in clause 6.1.6.

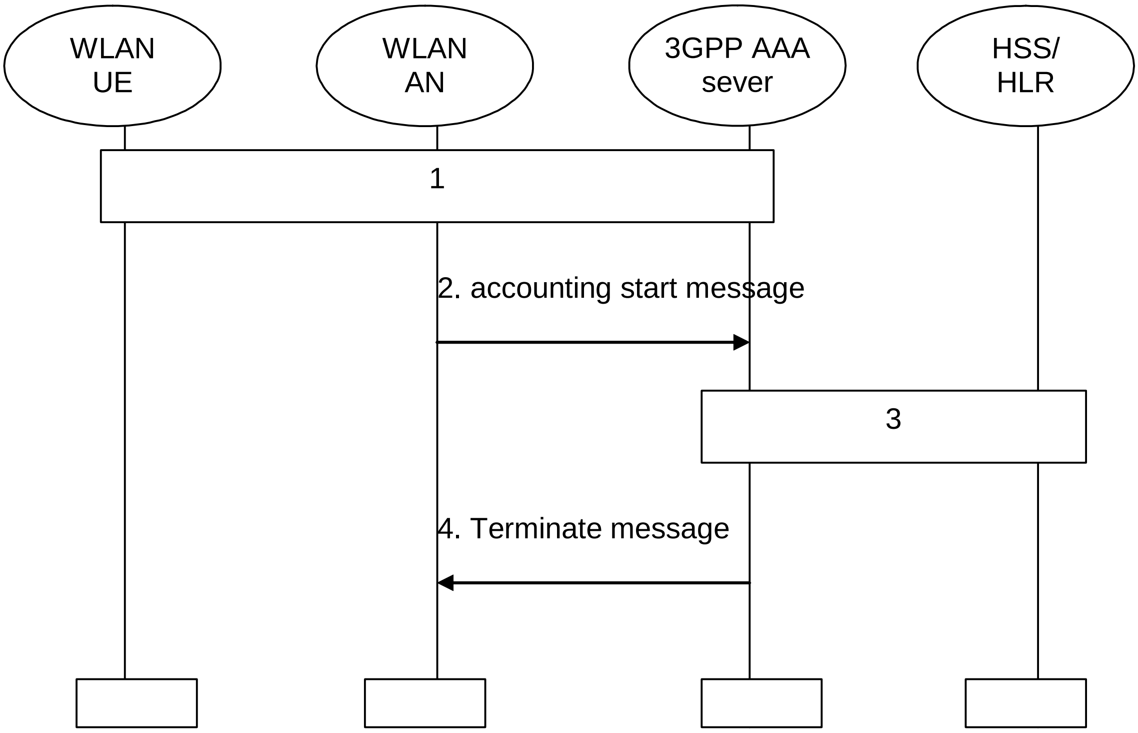
NOTE 4: The derivation of the value of N is for further study.

The authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN-UE after a network request. In that case, the EAP SIM process will be terminated as specified in ref. [5] and an indication shall be sent to HSS/HLR.

*** NEXT CHANGE ***

6.1.6 WLAN Direct IP Session Start

This section describes how to use AAA accounting start message to detect a fraud simultaneous session in WLAN Direct IP Access.



EAP/AKA or EAP/SIM procedure completes.

1. 3GPP AAA server receives an accounting start message from WLAN AN.

2. 3GPP AAA server verifies that a corresponding authentication procedure has been completed. If there is no other ongoing WLAN Access session for the subscriber detected by the 3GPP AAA server, and the WLAN registration for this subscriber is not performed previously, then the 3GPP AAA server shall initiate the WLAN registration to the HSS/HLR. Otherwise, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN access network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for old sessions. If it is the same subscriber but with a different MAC address, or with a different VPLMN identity or with different radio network information that is received than in any ongoing session, the 3GPP AAA server then considers that the authentication exchange is related to a new WLAN Access session. It shall terminate an old WLAN Access session after the successful authentication of the new WLAN Access session, based on the policy whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded. If the MAC addresses (the old one and the new one) are equal and the WLAN radio network information received is different from the old one, the new session is considered to be a fraudulent one.

3. If in step 3 the new session is considered to be a fraudulent one, 3GPP AAA server terminates the new session.

*** END OF CHANGE ***

3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050177

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**063**	⌘**rev**	**1**	⌘	Current version:	**6.3.0** ⌘

*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:	⌘	Adding verification method of PDG certification by OSCP protocol	
Source:	⌘	SA WG3	
Work item code:	⌘	WLAN	***Date:*** ⌘ 22/01/2005
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:	⌘	Certificates are used by the UE to authenticate the PDG. The current specification mandates the usage of OCSP for certificate revocation handling of PDG certificates. However, at the time when the UE needs to verify the PDG it has not yet access to the revocation server. Hence, it might not be possible for the UE to use the OCSP when it is actually needed. Furthermore, the OMA OCSP profile is currently not covered by the specification.
Summary of change:	⌘	We suggest add a reference to the OMA OCSP profile. Furthermore, we suggest adding a note to section 6.6A explaning how OCSP can be used to check PDG certificate status in WLAN interworking.
Consequences if not approved:	⌘	It is unclear how OCSP is supposed to be used in WLAN interworking.

Clauses affected:	⌘	2, 6.6A			
		Y	**N**		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

*** BEGIN OF CHANGE1 ***

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 22.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".

[2] 3GPP TR 23.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition".

[3] IETF RTC 3748: "Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-13, October 2004: "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)". IETF Work in progress

[5] draft-haverinen-pppext-eap-sim-14, October 2004: "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)". IETF Work in progress

[6] IEEE 802.11i-2004: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - LAN/MAN - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications-Amendment 6: MAC Security Enhancements".

[7] RFC 2716, October 1999: "PPP EAP TLS Authentication Protocol".

[8] SHAMAN/SHA/DOC/TNO/WP1/D02/v050, 22-June-01: "Intermediate Report: Results of Review, Requirements and Reference Architecture".

[9] ETSI TS 101 761-1 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 1: Basic Data Transport".

[10] ETSI TS 101 761-2 v1.2.1C: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer".

[11] ETSI TS 101 761-4 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 4 Extension for Home Environment".

[12] ETSI TR 101 683 v1.1.1: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview".

[13] 3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[14] RFC 2486, January 1999: "The Network Access Identifier".

[15] RFC 2865, June 2000: "Remote Authentication Dial In User Service (RADIUS)".

[16] RFC 1421, February 1993: "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures".

[17] Federal Information Processing Standard (FIPS) draft standard: "Advanced Encryption Standard (AES)", November 2001.

[18] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[19] IEEE P802.1X/D11 June 2001: "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".

[20] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[21] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[22] CAR 020 SPEC/0.95cB: "SIM Access Profile, Interoperability Specification", version 0.95VD.

[23] draft-ietf-aaa-eap-08.txt, June 2004: "Diameter Extensible Authentication Protocol (EAP) Application". IETF Work in progress

[24] RFC 3588, September 2003: "Diameter base protocol".

[25] RFC 3576, July 2003: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".

[26] RFC 3579, September 2003: "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)".

[27] draft-ietf-eap-keying-02.txt, June 2004: "EAP Key Management Framework". IETF Work in progress

[28] E. Barkan, E. Biham, N. Keller: "Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication", Crypto 2003, August 2003.

[29] draft-ietf-ipsec-ikev2-16.txt, September 2004: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998: "IP Encapsulating Security Payload (ESP)".

[31] draft-ietf-ipsec-ui-suites-06.txt, April 2004: "Cryptographic Suites for IPsec". IETF Work in progress

[32] draft-ietf-ipsec-udp-encaps-09.txt, May 2004: "UDP Encapsulation of IPsec Packets". IETF Work in progress

[33] draft-ietf-ipsec-ikev2-algorithms-05.txt, April 2004: "Cryptographic Algorithms for use in the Internet Key Exchange Version 2". IETF Work in progress

[34] RFC 2104, February 1997: "HMAC: Keyed-Hashing for Message Authentication".

[35] RFC 2404, November 1998: "The Use of HMAC-SHA-1-96 within ESP and AH".

[36] RFC 2548, March 1999: " Microsoft Vendor-specific RADIUS Attributes".

[37] draft-mariblanca-aaa-eap-lla-01.txt, June 2004: "EAP lower layer attributes for AAA protocols".

[38] RFC 3279, April 2002: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[39] RFC 3280, April 2002: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[40] 3GPP TS 27.007: "Technical Specification Group Terminals; AT command set for User Equipment (UE)".

[41] ETSI TS 102.310: "Smart Cards; Extensible Authentication Protocol support in the UICC".

[42] ETSI TS 102.221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[43] ”Online Certificate Status Protocol Mobile Profile” Open Mobile Alliance OMA-WAP-OCSP V1.0. URL: http://www.openmobilealliance.org/

*** END OF CHANGE1 ***

*** BEGIN OF CHANGE2 ***

6.6A Profile for PDG certificates

Certificates used for authentication of the PDG shall meet the following profile of RFC 3280 [39].

a) The certificate shall be encoded in DER format.

b) The version shall be 2 ("v3").

c) The certificate serial number shall meet the requirements in RFC 3280 [39], section 4.1.2.2.

d) The signature algorithm shall be "sha1WithRSAEncryption" [38], and the RSA public key used for signing shall not be longer than 2048 bits.

e) The issuer name shall not be empty.

f) The validity period shall meet the requirements in RFC 3280 [39], section 4.1.2.5.

f) The subject name may be empty in PDG certificates and shall not be empty in CA certificates.

g) The subject public key shall use algorithm "rsaEncryption" (RFC 3279 [38]), and the RSA public key shall not be longer than 2048 bits.

h) The issuerUniqueID or subjectUniqueID fields shall not be present.

i) The SubjectAltName extension shall be present if this is a PDG certificate, and shall contain at least one dNSName component.

j) The BasicConstraints extension shall be present if this is a CA certificates with "CA" flag asserted. The pathLenConstraint may be present.

k) CA certificates should contain the NameConstraints extension with appropriate dNSName components in the permittedSubtrees field.

l) The KeyUsage extension shall be present in all certificates. The keyCertSign bit shall be set in CA certificates, and digitalSignature bit shall be set in PDG certificates.

m) The CRLDistributionPoint extension may be present, and shall not be marked critical. At least one of the distribution points should use HTTP for retrieving the CRL.

n) The AuthorityInformationAccess extension may be present with id-ad-ocsp access method, and shall not be marked critical.

o) Other extensions should not be used; if they are, they shall not be marked as critical.

p) The total length of a certificate shall not exceed 2000 bytes.

Certificate processing requirements:

a) UE shall send one or more CERTREQ payloads with encoding value 4 (X.509 certificate - Signature).

b) IKEv2 Certificate encoding value shall be 4 (X.509 certificate - Signature).

c) UE shall not assume that any except the first IKEv2 CERT payload is ordered in any way.

d) UE shall support paths of at least four certificates (self-signed CA certificate, intermediate CA 1, intermediate CA 2, PDG certificate).

e) PDG shall not send paths containing more than four certificates.

f) UE shall be prepared to receive irrelevant certificates, or certificates they do not understand.

g) UE shall be able to process certificates (for e.g. chain building) even if naming attributes are unknown.

h) UE shall support both UTCTime and GeneralizedTime encoding for validity time.

i) UE shall check the validity time, and reject certificates that are either not yet valid or are expired.

j) UE shall support processing of the BasicConstraints, NameConstraints, and KeyUsage extensions.

k) UE may check the validity of the certificates using CRLs or OCSP [43]. Support for CRLs is optional. Support for OCSP is mandatory.

NOTE: A WLAN UE that initiates 3GPP IP Access according to the tunnel full authentication and authorization procedure, may want to check the validity of the PDG certificate, but it might not gain access to the OCSP server. This situation can be handled in the following way: After the UE initiated tunnel is successfully established and before user data is transmitted in the tunnel, the UE sends an OCSP request message to OCSP server. When the UE receives the OCSP response, it checks the certificate status. If the certificate of PDG is valid, the UE will allow user data to be transmitted to the PDG in the tunnel. If the certificate is not valid, the UE may terminate the tunnel that just was established.

*** END OF CHANGE2 ***