3GPP TSG SA WG3 Security — S3#36
Shenzhen, China 23 - 26 November 2004

Tdoc ⌘S3-041153

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**040**	⌘ **rev**	**2**	⌘	Current version:	**6.2.1**	⌘

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

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

Title:	⌘	Control of simultaneous sessions in WLAN 3GPP IP access
Source:	⌘	SA WG3
Work item code:	⌘	WLAN
Date:	⌘	20/10/2004
Category:	⌘	**C**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	A mechanism to control simultaneous sessions in WLAN 3GPP IP access (formerly called scenario 3) is needed in order to prevent fraud situations, for example where the user gives access to its (U)SIM from several devices that authenticate on behalf of the user and get access to the 3GPP network.
Summary of change:	⌘	This paper reflects the changes needed in the TS 33.234 to introduce the mechanism. It basically consists of having a flag for every W-APN in the 3GPP AAA server to indicate if it is already active or not, i.e. if an IKE security association has already been set up or not. If a certain W-APN is active and a new W-APN setup request is received in the AAA server, the request is rejected.
Consequences if not approved:	⌘	Potential fraud situations may happen, where a user gives access to this (U)SIM to several devices.

Clauses affected:	⌘	3.1, 5.7 (new), 6.1.5.1, 6.1.5.2				
		Y	**N**			
Other specs affected:	⌘	X		Other core specifications	⌘	23.234, 24.234
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

3.1 Definitions

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

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

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

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

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

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

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

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.7 Simultaneous access control

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 IKEv2 security associations per W-APN. With this mechanism, it is 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.

*** END SET OF CHANGES ***

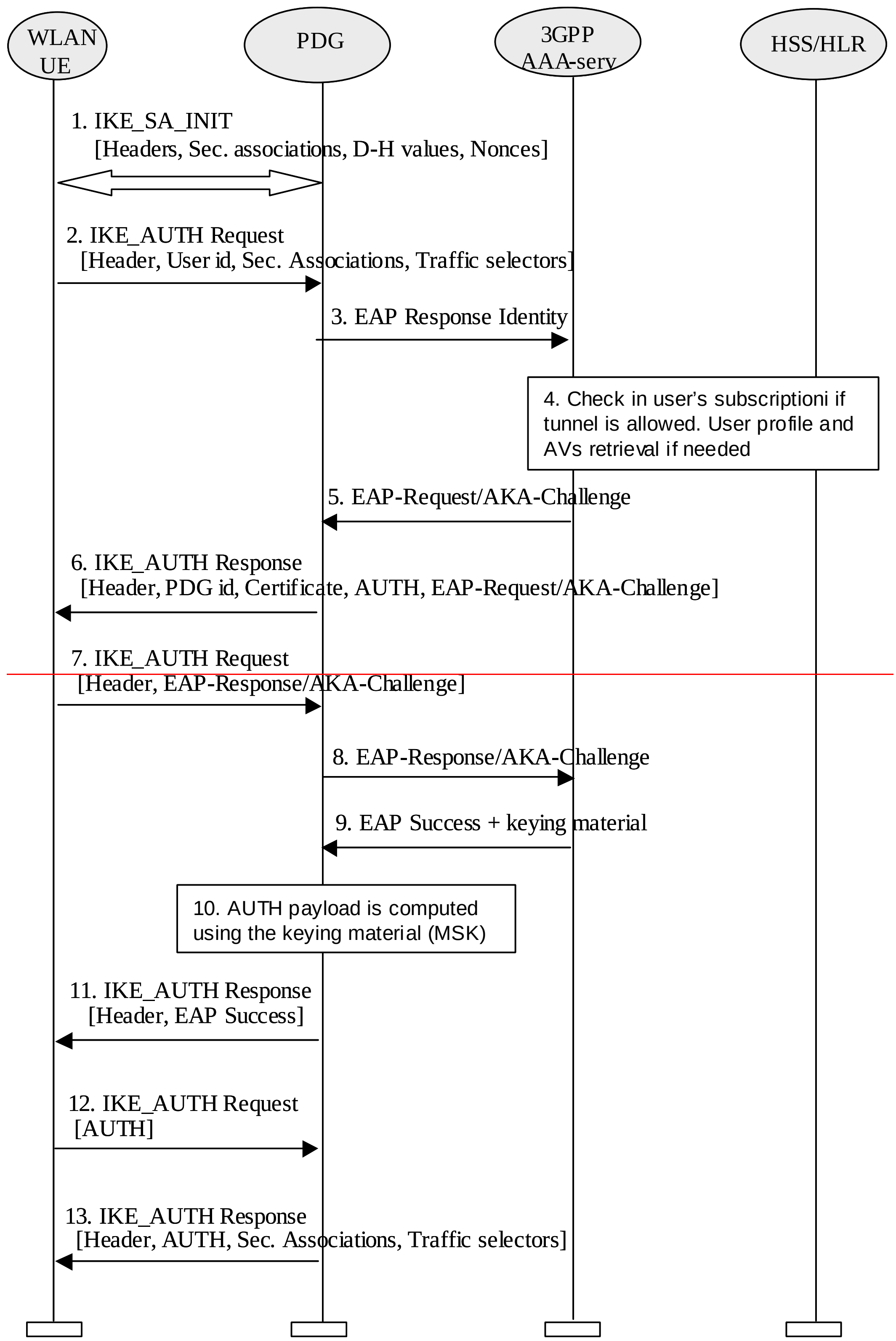
*** BEGIN SET OF CHANGES ***

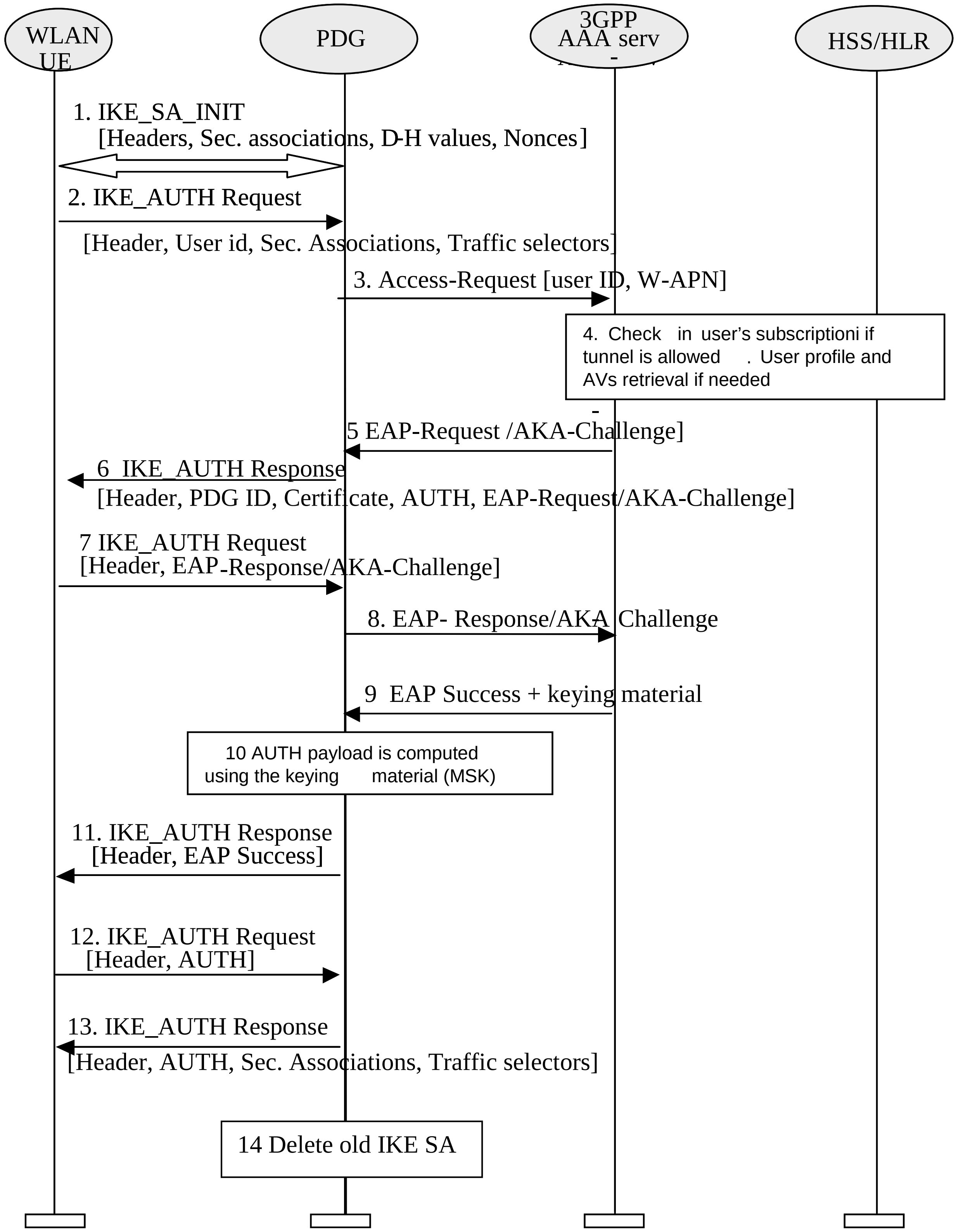
6.1.5.1 Tunnel full authentication and authorization

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 sequence diagram is shown in this chapter. 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 [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, Sec. Associations, Traffic selectors]
3. EAP Response Identity
4. Check in user's subscriptioni 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, Sec. Associations, Traffic selectors]



WLAN UE
PDG
3GPP AAA server
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. Access-Request [user ID, W-APN]
4. Check in user's subscriptioni 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
[Header, AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]
14 Delete old IKE SA

Sequence of events:

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 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 ref [14], containing the IMSI or the pseudonym. The identity in NAI format generated from the IMSI is described in ref. [4] and [5], depending on the type of EAP method to be used (EAP SIM or EAP AKA).

~~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)~~

Editors' note: W-APN should be sent in this step, because in TS 23.234 [13], there is following sentence; "The WLAN-UE shall include the W-APN and the user identity in the initial tunnel establishment request." One possibility is to include the W-APN in the IDr parameter in the IKE_AUTH phase, but this has to be studied in detail.

3. The PDG sends the Access Request ~~EAP Response identity 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 ref. [32]. 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 [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.

Editors 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. This AUTH parameter is sent to the WLAN UE together with the security associations and rest of 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 ref. [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.

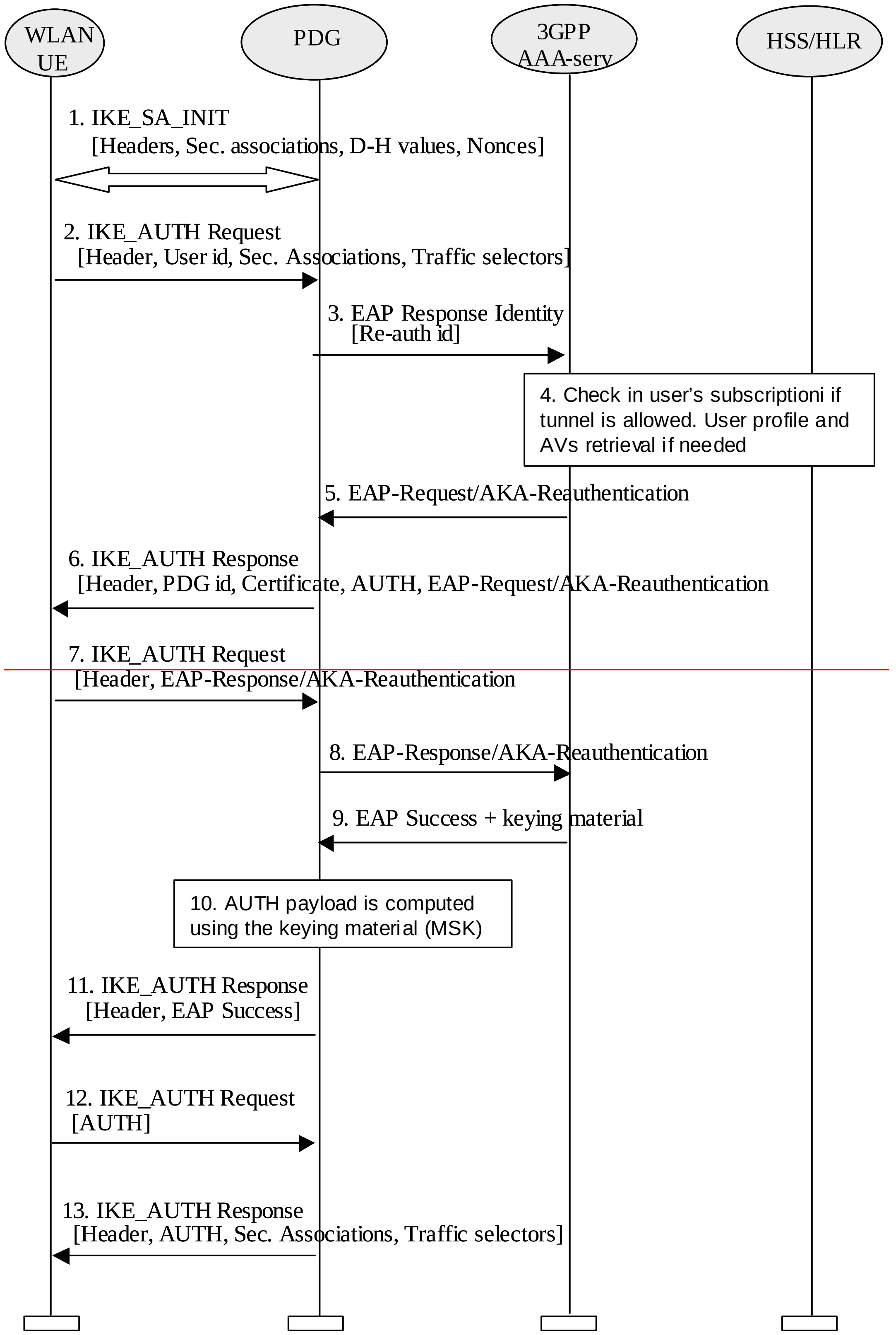
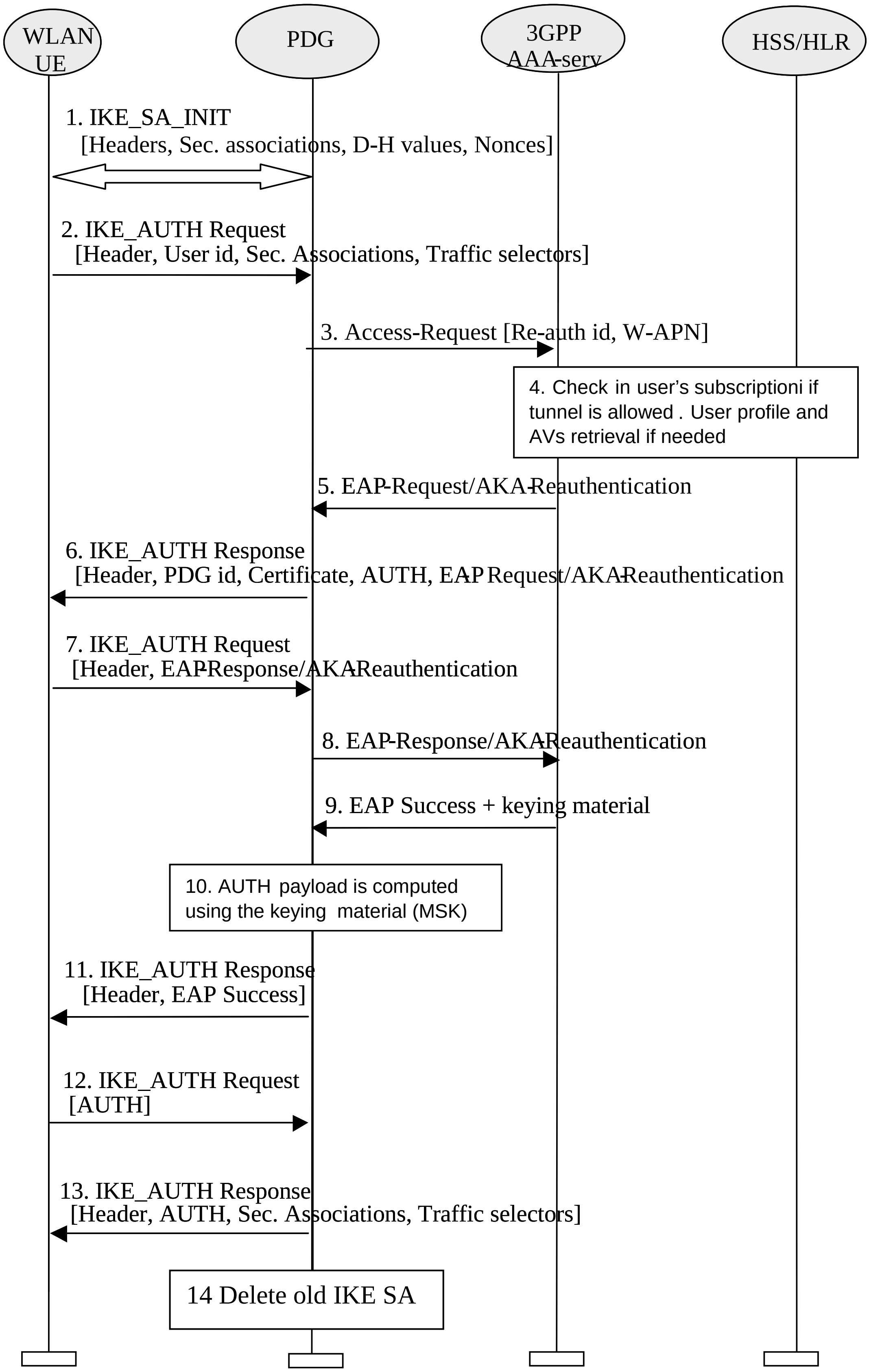


Figure 7B: Tunnel fast re-authentication and authorization


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, Sec. Associations, Traffic selectors]
3. Access-Request [Re-auth id, W-APN]
4. Check in user's subscriptioni 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-Response/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, Sec. Associations, Traffic selectors]
14 Delete old IKE SA

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 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.

3. The PDG sends the Access Request ~~EAP Response identity~~ 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 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. This AUTH parameter is sent to the WLAN UE together with the security associations and rest of 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 ref. [29], in order to delete the old IKE SA in WLAN UE.

*** END SET OF CHANGES ***