3GPP TSG SA WG3 Security — S3#35
St. Paul's Bay, Malta 5 - 8 October 2004

Tdoc S3-040748

CR-Form-v7.1

CHANGE REQUEST

⌘	33.234	CR	022	⌘	rev	-	⌘	Current version:	6.2.0	⌘

*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:	⌘	Control of simultaneous accesses in scenario 3
Source:	⌘	Ericsson
Work item code:	⌘	WLAN
Date:	⌘	28/09/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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:	⌘	Ericsson has submitted a discussion paper where the use of VPLMN identification and WLAN access network identification is analysed. The conclusion is that for scenario 3 these parameters can only be sent by the WLAN UE as the IPsec tunnel is end to end and makes it impossible to be sent by intermediate nodes. However, these parameters, if sent by the WLAN UE, are not authenticated so the AAA server cannot trust them in order to control simultaneous sessions.
Summary of change:	⌘	Removal of editor's notes in WLAN 3GPP IP access authentication, where the use of WLAN AN id and VPLMN id is left FFS.
Consequences if not approved:	⌘	Trusting in the VPLMN id and WLAN AN id may lead to fraud situations as they can be spoofed by the WLAN UE.

Clauses affected:	⌘	6.1.5.1

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		24.234, 29.234
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

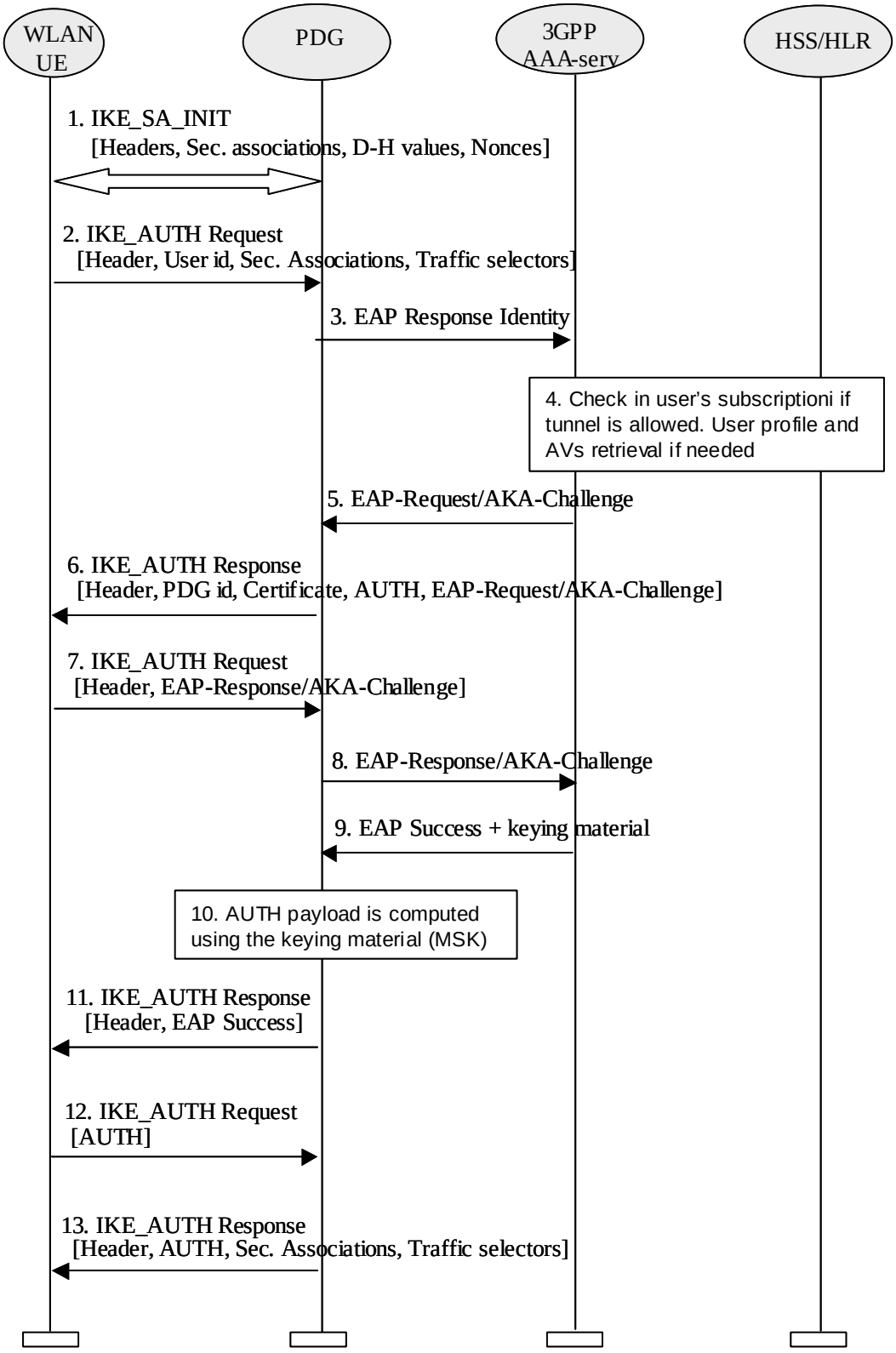
***** BEGIN SET OF CHANGES *****

6.1.5.1 Tunnel full authentication and authorization

The tunnel end point in the network is the PDG. 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.



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 is for further study.~~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 EAP Response identity message to the AAA server, containing the user identity. 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]

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

*** END SET OF CHANGES ***