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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Removal of editors' notes
Source:	⌘	NOKIA, BT
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Consequences if not approved:	⌘	Outdated editors information left in the TS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

Other specs affected:	Y	N		
⌘		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.

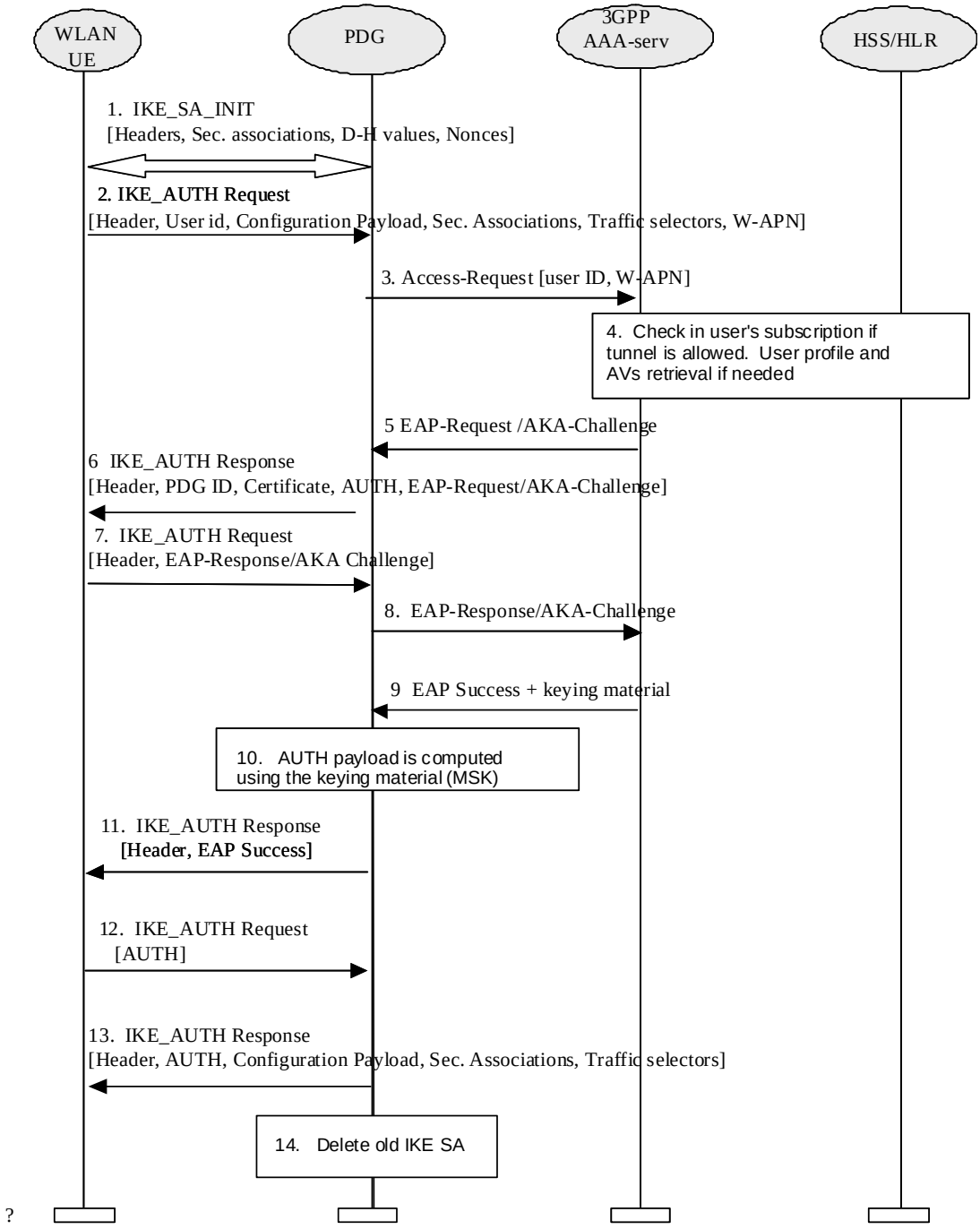

Figure 7A: Tunnel full authentication and authorization

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 ***