3GPP TSG SA WG3 Security — S3#35 *Tdoc ⌘S3-040770*
October 5 – 8, 2004, St Paul's Bay, Malta

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** CR **035** ⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Multiple Tunnels establishnemt with different PDG
Source:	⌘	Samsung
Work item code:	⌘	WLAN
Date:	⌘	23/06/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Multiple tunnels establishment procedure with different PDG is not mentioned in the specification. Multiple tunnels to the different PDG for different W-APN is needed as when the UE wants to access different services simultaneously. Procedure for multiple tunnel establishment for different PDG using IKEv2 is defined in this CR.
Summary of change:	⌘	Add feature on multiple tunnel establishment procedure with a different PDG.
Consequences if not approved:	⌘	No method defined to initiate and establish multiple tunnels with the different PDG for the different W-APN.

Clauses affected:	⌘	6.1.5.5

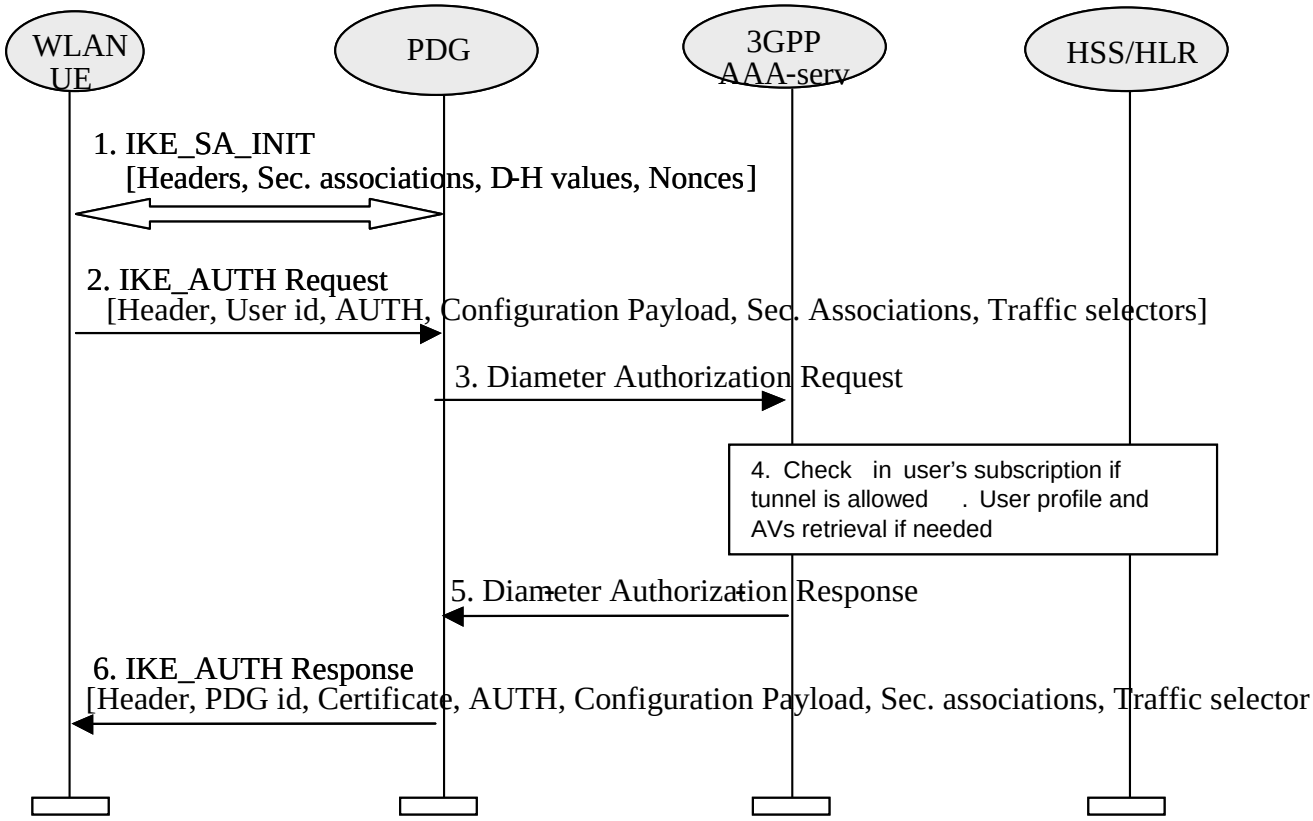
	Y	N		
Other specs Affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

*** BEGIN SET OF CHANGES ***

6.1.5.5 Subsequent Tunnel establishment with different PDG

The WLAN UE shall initiate subsequent tunnel with the different PDG for different W-APN.



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 generates the AUTH parameter with the latest MSK obtained as a result of the previous tunnel establishment procedure. 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). The WLAN UE shall send the configuration payload (CFG_REQUEST) with the IKE_AUTH to request for a Remote IP Address from the PDG.

Editors note: (1)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 ref. [33] section 5.3.4) (2) W-APN should be sent in this step, because in [33], 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 Diameter authorization message to the AAA server, containing the user identity and the W-APN.

4. The AAA server shall fetch the user profile and authorization vectors from HSS/HLR (if these parameters are not available in the AAA server). The AAA server checks in user's subscription if he/she is authorized to establish the tunnel. The AAA Server verifies that the user requesting the tunnel establishment has been already successfully authenticated for any previous tunnel establishment procedure.

5. The AAA server sends Diameter Response message to intimate whether UE is authorized to establish the tunnel and also includes the key material. This key material shall consist of the MSK generated during the previous 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].

6. The PDG verifies the AUTH parameter with the received MSK from the AAA server and 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). 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 rest of IKEv2 parameters and the IKEv2 negotiation terminates. It completes the negotiation of the child security associations as well.

*** END SET OF CHANGES ***