3GPP TSG SA WG3 Security — S3#34 *Tdoc ⌘S3-040493*
Acapulco, Mexico 6 - 9 July 2004

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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:	⌘	IPsec tunneling establishment procedures
Source:	⌘	NTT DoCoMo
Work item code:	⌘	WLAN
Date:	⌘	06/06/2004
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:

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:	⌘	Although the scenario 3 tunnel establishment procedure is specified in TS 23.234, it is understood that the security specific part of this procedure is left to SA3. That is, SA3 is responsible for specifying the detailed call flows for the encryption key exchange and the EAP-SIM/AKA authentication before establishing IPsec security associations. For the purpose of the stage3 work progress (e.g. protocol design of the Wu, Wm, or Wg reference point), the procedures should be clarified.
Summary of change:	⌘	IPsec tunneling establishment procedures is added.
Consequences if not approved:	⌘	Lack of necessary information for Stage3 work progress.

Clauses affected:	⌘	6.1.5

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

Other comments:	⌘	

*** BEGIN SET OF CHANGES ***

6.1.5.1 UE-initiated tunnels set up with EAP/AKA procedure

The UE-initiated tunnels set up uses the IKEv2 in ref [29] and The EAP-AKA in ref. [4]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.

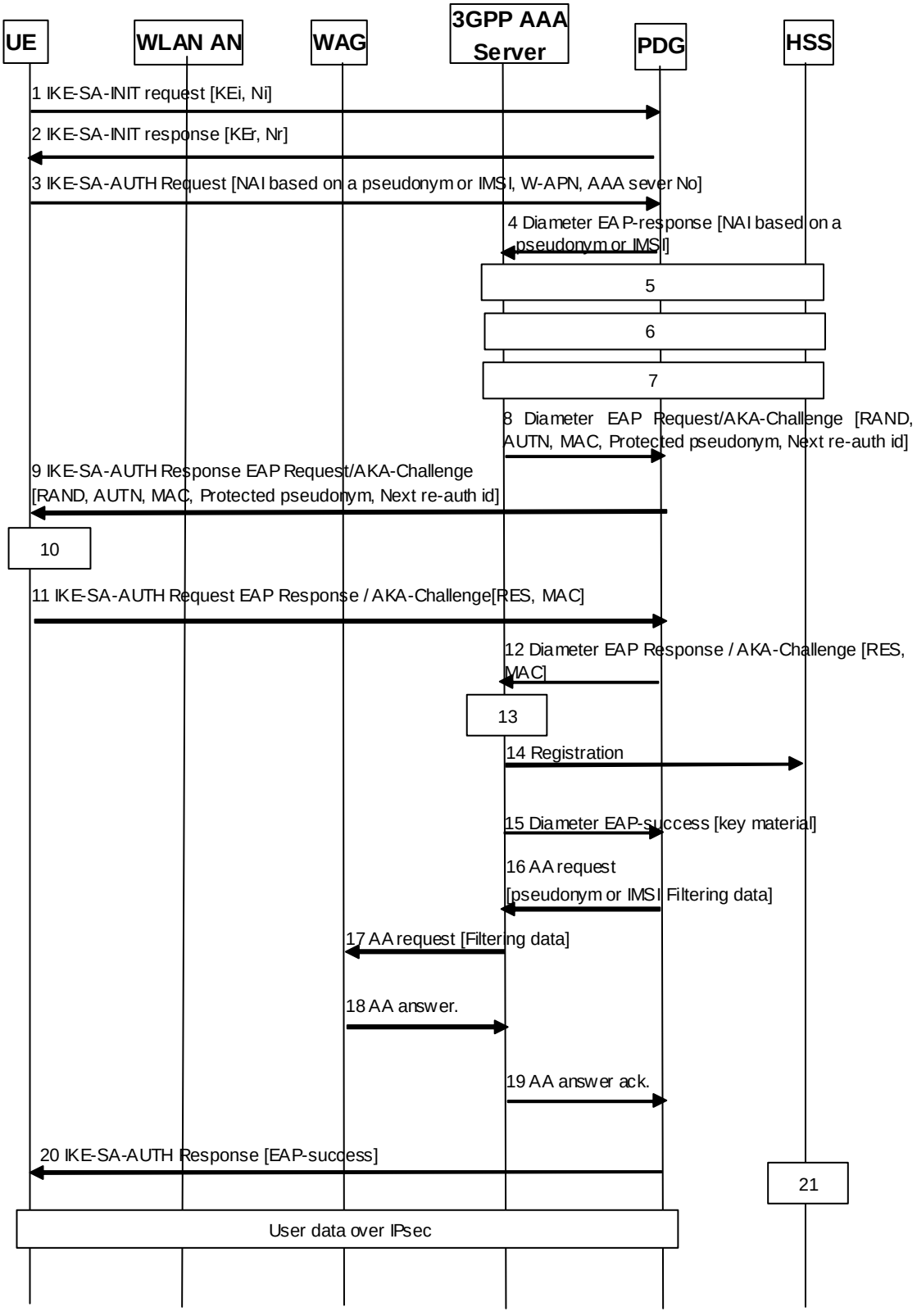

Figure 8: UE-initiated tunnels set up with EAP/AKA procedure

1. The WLAN-UE sends a IKE-SA-INT message to the PDG with KEi and Ni. The PDG generates cipher key and integrity key for IKE-SA-AUTH procedures.

2. The PDG sends a IKE-SA-INT message to the PDG with KEr and Nr. The WLAN UE generates cipher key and integrity key for IKE-SA-AUTH procedures.

3. The WLAN-UE sends a IKE-SA-AUTH Request message to the PDG. The WLAN-UE sends its identity complying with Network Access Identifier (NAI) format specified in RFC 2486, and W-APN. NAI contains either a temporary identifier (pseudonym) allocated to the WLAN-UE in previous authentication or, in the case of first authentication, the IMSI. If the identity is temporary identity, the WLAN-UE also sends the 3G AAA Sever number which allocated the temporary identity.

4. The PDG sends EAP Response/Identity message to the 3GPP AAA with the NAI. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI and the 3G AAA Sever number if the number is needed. The routing path may include one or several AAA proxies (not shown in the figure). 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.

5. 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.

6. 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.

7. New keying material is derived from IK and CK., cf. [4]. This keying material is required by EAP-AKA, and keying material is generated for IPsec confidentiality and integrity protection. A new pseudonym may be chosen and protected (i.e. encrypted and integrity protected) using EAP-AKA generated keying material.

8. 3GPP AAA Server sends RAND, AUTN, a message authentication code (MAC) and two user identities (if they are generated): protected pseudonym and/or re-authentication id to the PDG 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.

9. The PDG sends IKE-SA-AUTH Response message with the EAP Request/AKA-Challenge message to the WLAN-UE.

10. 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 was received, then the WLAN-UE stores the pseudonym for future authentications.

11. The WLAN UE calculates a new MAC value covering the EAP message with the new keying material. WLAN-UE sends IKE-SA-AUTH Request message with EAP Response/AKA-Challenge containing calculated RES and the new calculated MAC value to the PDG.

12. The PDG sends the EAP Response/AKA-Challenge packet to the 3GPP AAA Server.

13. The 3GPP AAA Server checks the received MAC and compares XRES to the received RES. If successful, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN radio 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 the old sessions (skip step 14).

14. Otherwise, the AAA server considers that the authentication exchange is related to a new scenario-3 session. In this case the AAA server shall contact the HSS for a decision. The AAA server shall inform to the HSS of the WLAN-UE's MAC address, the VPLMN Identity, as well as the identifier of the WLAN radio network used.

15. If all checks in step 13 are successful, then 3GPP AAA Server sends the EAP Success message to the PDG. The 3GPP AAA Server includes this keying material for IPsec confidentiality and integrity protection in the underlying

AAA protocol message (i.e. not at EAP level). The PDG stores the keying material to be used in communication with the authenticated WLAN-UE.

16. The PDG sends the AA request message including filtering policy information in AAA protocol to the AAA sever.

17. The AAA sever sends the AA request message to the WAG.

18. The WAG sets filtering policy and sends the AA answer message of acknowledgement to the AAA sever.

19. The AAA sever sends the AA answer message to the PDG.

20. The PDG informs the WLAN-UE about the successful authentication with the EAP Success message with in IKE-SA-AUTH response message. Now the IKE-SA-AUTH exchange with EAP AKA exchange has been successfully completed, and the WLAN-UE and the PDG share keying material derived during that exchange.

21. If the same subscriber but different MAC address, or VPLMN identity or the radio network information is received than in any ongoing session, then the registration is related to a new scenario-3 session. The HSS shall close an old scenario-3 session by indicating to the 3GPP AAA server of the old session to terminate the session, based on the policy whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded.

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.

6.1.5.2 UE-initiated tunnels set up with EAP/SIM procedure

Note: This is FFS.

6.1.5.3 Fast re-authentication mechanisms in UE-initiated tunnels set up

When authentication processes have to be performed frequently, it can lead to a high network load especially when the number of connected users is high. Then it is more efficient to perform fast re-authentications. Thus the re-authentication process allows the WLAN-AN to authenticate a certain user in a lighter process than a full authentication, thanks to the re-use of the keys derived on the previous full authentication.

6.1.5.3.1 UE-initiated tunnels set up with EAP/AKA fast re-authentication procedures

The implementation of EAP/AKA must include the fast re-authentication mechanism described in this chapter, although its use is optional and depends on operator's policies, which shall be enforced by the AAA server by means of sending the re-authentication identity in any authentication process. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.

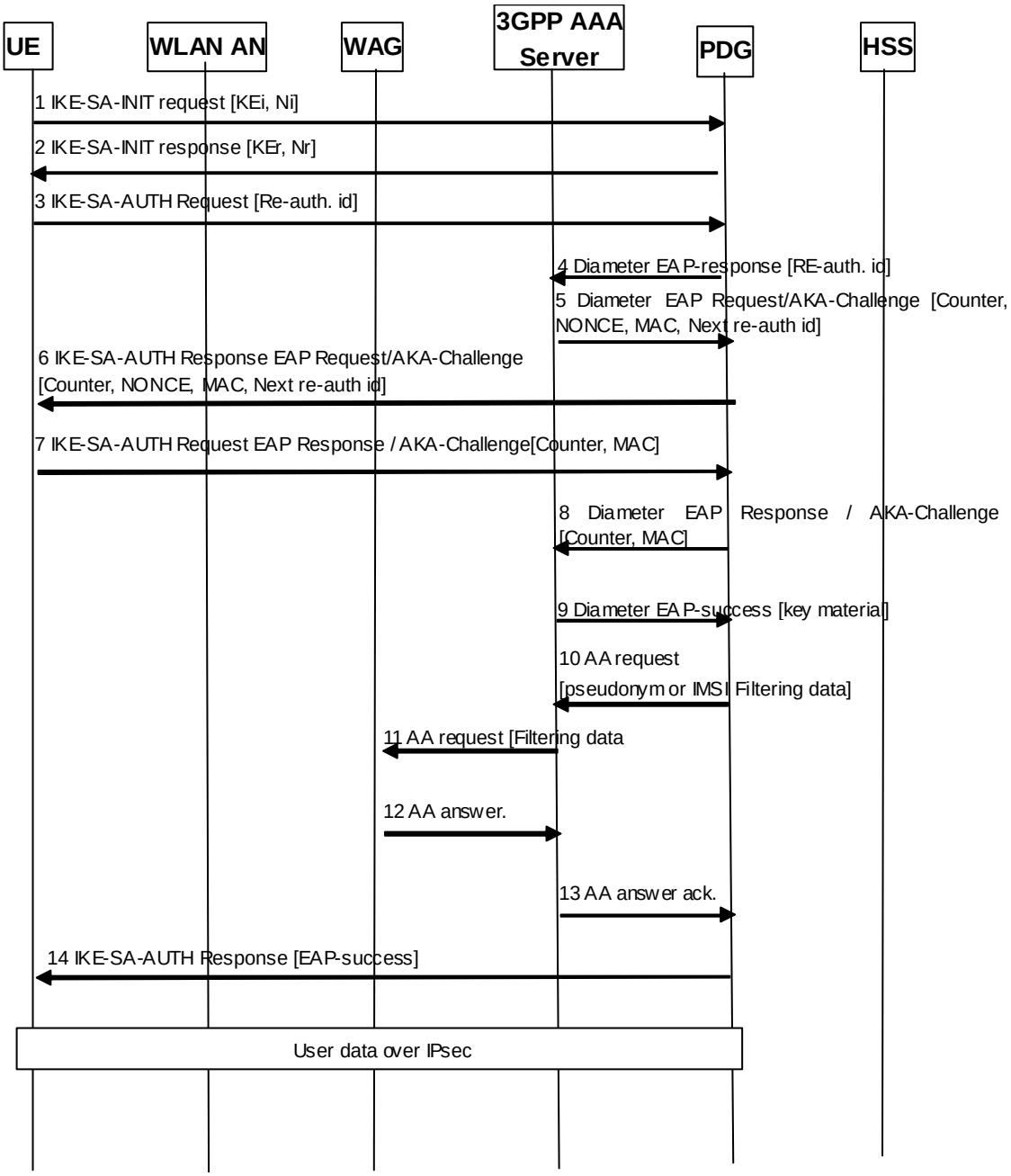

Figure 9: UE-initiated tunnels set up with EAP/AKA fast re-authentication procedures

1. The WLAN-UE sends a IKE-SA-INT message to the PDG with KEi and Ni. The PDG generates cipher key and integrity key for IKE-SA-AUTH procedures.

2. The WLAN-UE sends a IKE-SA-INT message to the PDG with KEr and Nr. The WLAN UE generates cipher key and integrity key for IKE-SA-AUTH procedures.

3. The WLAN-UE sends a IKE-SA-AUTH Request message containing a re-authentication identity (this identity was previously delivered by AAA server in a full authentication procedure) to the PDG.

4. The PDG sends EAP Response/Identity to the AAA server.

5. The AAA server initiates the Counter (which was initialized to one in the full authentication process) and sends it in the EAP Request message, together with the NONCE, the MAC (calculated over the NONCE) and a re-

authentication id for a next fast re-authentication. If the AAA server is not able to deliver a re-authentication identity, next time the WLAN-UE shall force a full-authentication (to avoid the use of the re-authentication identity more than once).

6. The PDG sends IKE-SA-AUTH request message with the EAP Request message to the WLAN-UE.

7. The WLAN-UE verifies that the Counter value is fresh and the MAC is correct, and it sends IKE-SA-AUTH with the EAP Response message with the same Counter value (it is up to the AAA server to step it up) and a calculated MAC.

8. The PDG sends the EAP response message to the AAA server.

9. The AAA server verifies that the Counter value is the same as it sent, and the MAC is correct, and sends an EAP Success message.

10. The PDG sends the AA request message including filtering policy information in AAA protocol to the AAA sever.

11. The AAA sever sends the AA request message to the WAG.

12. The WAG sets filtering policy and sends the AA answer message of acknowledgement to the AAA sever.

13. The AAA sever sends the AA answer message to the PDG.

14. The PDG informs the WLAN-UE about the successful authentication with the EAP Success message with in IKE-SA-AUTH response message.

The re-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.

6.1.5.3.2 UE-initiated tunnels set up with EAP/SIM fast re-authentication procedures

Note: This is FFS.

*** END SET OF CHANGES ***