

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 Radio Access Network Core Network

Title:	# Wm interface description		
Source:	# Ericsson		
Work item code:	# WLAN	Date:	# 22/06/2004
Category:	# F	Release:	# Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	# Wm interface (PDG-AAA server) is not yet defined. The purpose of this CR is to start with the definition of the interface for tunnel establishment purposes in scenario 3.
Summary of change:	# A new subchapter will be included specifying the procedures between the PDG and the AAA server, and how key derivation and delivery is performed in order to authenticate the tunnel in scenario 3.
Consequences if not approved:	# Scenario 3 not possible to implement, tunnel establishment not defined.

Clauses affected:	# 6.1.5 and 2		
Other specs affected:	#	Y	N
	#	X	<input type="checkbox"/>
	#	<input type="checkbox"/>	X
	#	<input type="checkbox"/>	X
Other comments:	#		

*** BEGIN SET OF CHANGES ***

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 22.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".
- [2] 3GPP TR 23.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition".
- [3] draft-ietf-eap-rfc2284bis-06.txt, October 2003: "PPP Extensible Authentication Protocol (EAP)".
- [4] draft-arkko-pppext-eap-aka-11, October 2003: "EAP AKA Authentication".
- [5] draft-haverinen-pppext-eap-sim-~~12~~[13](#), ~~October~~ [April 2003](#)[2004](#): "EAP SIM Authentication".
- [6] IEEE Std 802.11i/D7.0, October 2003: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".
- [7] RFC 2716, October 1999: "PPP EAP TLS Authentication Protocol".
- [8] SHAMAN/SHA/DOC/TNO/WP1/D02/v050, 22-June-01: "Intermediate Report: Results of Review, Requirements and Reference Architecture".
- [9] ETSI TS 101 761-1 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 1: Basic Data Transport".
- [10] ETSI TS 101 761-2 v1.2.1C: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer".
- [11] ETSI TS 101 761-4 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 4 Extension for Home Environment".
- [12] ETSI TR 101 683 v1.1.1: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview".
- [13] 3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".
- [14] RFC 2486, January 1999: "The Network Access Identifier".
- [15] RFC 2865, June 2000: "Remote Authentication Dial In User Service (RADIUS)".

- [16] RFC 1421, February 1993: "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures".
- [17] Federal Information Processing Standard (FIPS) draft standard: "Advanced Encryption Standard (AES)", November 2001.
- [18] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".
- [19] IEEE P802.1X/D11 June 2001: "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".
- [20] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".
- [21] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".
- [22] CAR 020 SPEC/0.95cB: "SIM Access Profile, Interoperability Specification", version 0.95VD.
- [23] draft-ietf-aaa-eap-03.txt, October 2003: "Diameter Extensible Authentication Protocol (EAP) Application".
- [24] RFC 3588, September 2003: "Diameter base protocol".
- [25] RFC 3576, July 2003: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".
- [26] RFC 3579, September 2003: "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)".
- [27] draft-ietf-eap-keying-01.txt, November 2003: "EAP Key Management Framework".
- [28] E. Barkan, E. Biham, N. Keller: "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Crypto 2003, August 2003
- [29] draft-ietf-ipsec-ikev2-~~12~~13.txt, ~~January~~-~~March~~ 2004, "Internet Key Exchange (IKEv2) Protocol"
- [30] RFC 2406, November 1998, "IP Encapsulating Security Payload (ESP)"
- [31] draft-ietf-ipsec-ui-suites-04.txt, August 2003, "Cryptographic Suites for IPsec"
- [32] [draft-mariblanca-aaa-eap-lla-00.txt, May 2004, "EAP lower layer attributes for AAA protocols"](#).

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.1.5.1 Tunnel authentication and authorization

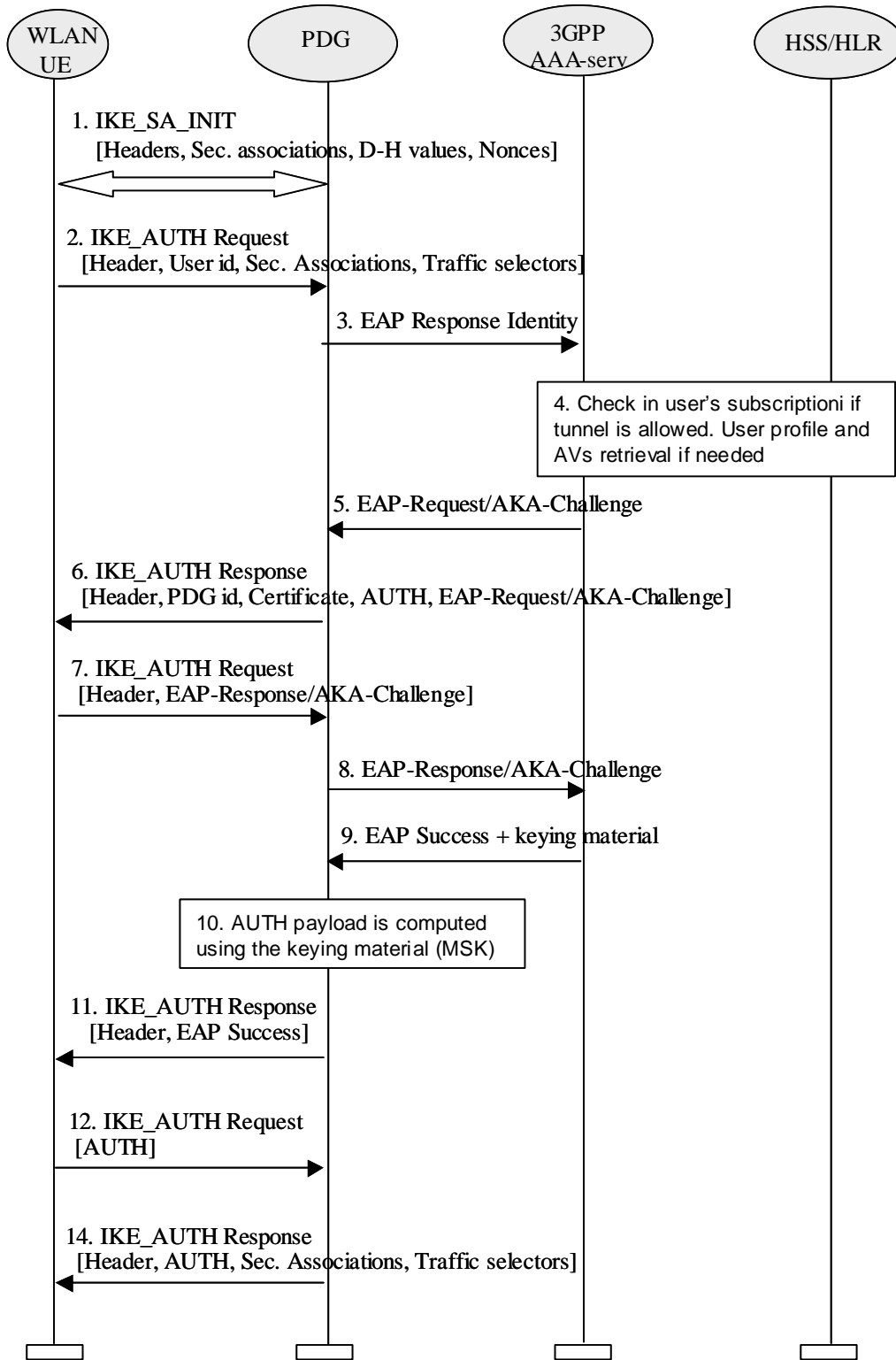
The tunnel end point in the network is the PDG. When a new attempt for tunnel establishment is performed by the WLAN UE, the WLAN UE shall use IKEv2 as specified in ref. [29]. The EAP messages carried over IKEv2 shall be terminated in the AAA server, which communicates with the PDG via Wm interface, 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 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

When the WLAN UE sends the user identity, it may use the IMSI even if identity privacy support has been selected by the home network (by means of sending a temporary identity in the previous authentication). The reason is that IKEv2 provides integrity protection and encryption in the IKE_AUTH messages where the user identity is sent.

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 negotiate 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. 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).
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]
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, using its own copy of the MSK, shall take it 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 ***