3GPP TSG-SA WG3 Security #33
Beijing, China, 10-14 May 2004

Tdoc ⌘S3-040275

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	EAP in IKEv2
Source:	⌘	Nokia, Ericsson
Work item code:	⌘	WLAN
Date:	⌘	03/05/2004
Category:	⌘	**C**
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:	⌘	IKEv2 is a component of IPsec used for performing mutual authentication and establishing and maintaining security associations for IPsec ESP and AH. In addition to supporting authentication using public key signatures and shared secrets, IKEv2 also supports EAP authentication, but it requires the use of public key signatures to authenticate responder. However, EAP-SIM and EAP-AKA can be used to provide responder authentication in IKEv2 completely based on EAP.
Summary of change:	⌘	Adding support for mutual EAP-SIM and EAP-AKA authentication in IKEv2.
Consequences if not approved:	⌘	Public key signatures should be used for responder authentication and public key infrastructure should be deployed.

Clauses affected:	⌘	2 and 6.1.5

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

Other comments:	⌘	

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, October 2003: "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 Cryptoanalysis of GSM Encrypted Communication", Crypto 2003, August 2003.

[29] draft-ietf-ipsec-ikev2-~~12~~13.txt, March~~January~~ 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-eronen-ipsec-ikev2-eap-auth-00.txt, February 2004, "Extension for EAP Authentication in IKEv2".

*** NEXT CHANGE***

6.1.5 Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

- The WLAN UE and the PDG use IKEv2, as specified in [~~ikev2~~29], in order to establish IPSec security associations.
- ~~Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG.~~ Depending on the WLAN UE, either EAP-AKA or EAP-SIM within IKEv2, as specified in [32], is used to authenticate the PDG
- EAP-AKA within IKEv2, as specified in [~~ikev2, section 2.16~~32], is used to authenticate WLAN UEs, which contain a USIM.
- EAP-SIM within IKEv2, as specified in [~~ikev2, section 2.16~~32], is used to authenticate WLAN UEs, which contain a SIM and no USIM.
- A profile for IKEv2 is defined in section 6.5.

Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3. The text in this section reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in Annex E. They may replace the current working assumption in this section if problems with the working assumption arise. Otherwise, Annex E will be removed before the TS is submitted for approval. The above points on the use of IKEv2 are dependent on the analysis of the open issues on legacy VPN clients and key management; in particular, the use of EAP-AKA and EAP-SIM will be studied.

*** END OF CHANGE***