3GPP TSG SA WG3 Security — S3#32 *Tdoc ⌘S3-040103*
Edinburgh, UK 9 - 13 February 2004

CR-Form-v7

Pseudo-CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.8.0** ⌘

*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:	⌘	Link layer keys generation from EAP SIM/AKA procedures
Source:	⌘	Ericsson, Siemens, Nokia
Work item code:	⌘	WLAN ***Date:*** ⌘ 12/01/2004
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:	⌘	In TS 33.234 it is needed to explain how the EAP SIM/AKA procedures derive keys which are used later on in WLAN access network link layer security
Summary of change:	⌘	Since the authentication using EAP SIM/AKA procedures is considered secure enough for WLAN interworking authentication, the derivation of keys from these processes for link layer security in the WLAN access network avoids a separate method for this purpose and gives a sufficient security level
Consequences if not approved:	⌘	Key derivation and delivery not explained in TS 33.234. TS not consistent.

Clauses affected:	⌘	5 Security features and 6 Security mechanisms

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

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: " Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking;".

[2] 3GPP TR 23.934: "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~~2~~.0, ~~March 2002~~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 101 761-4v1.3.1B "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 "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: "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: "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] SIM Access Profile, Interoperability Specification, version 0.95VD - d. Document no. CAR 020 SPEC/0.95cB

[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.txt, January 2004, “Internet Key Exchange (IKEv2) Protocol”

[30] RFC 2406, November 1998, “IP Encapsulating Security Payload (ESP)”

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.2 Confidentiality protection

[Editor’s note: This section shall deal with what confidentiality protection that is provided between different nodes both inter domain, intra domain and the WLAN-UE. It shall justify the selected mechanisms (hop-by-hop or end-to-end) and protection at different layers]

5.2.1 Confidentiality protection in scenario 2

~~*Text to be added*~~

Confidentiality protection in the WLAN AN link layer is required. The specification of this feature is, however, out of scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the confidentiality protection shall be as specified in ref. [6].

The home network (AAA server) has to be able to send key material to the WLAN AN, as input for the encryption procedure, in a confidential and integrity protected way (for detailed requirements cf. [27]).

5.2.2 Confidentiality protection in scenario 3

It shall be possible to protect the confidentiality of IP packets sent through a tunnel between the UE and the PDG.

5.3 Integrity protection

[Editor's note: This section shall deal with what integrity protection that is provided between different nodes both inter domain, intra domain and the WLAN-UE. It shall justify the selected mechanisms (hop-by-hop or end-to-end) and protection at different layers]

5.3.1 Integrity protection in scenario 2

~~*text to be added*~~

Integrity protection in the WLAN AN link layer is required. The specification of this feature is, however, out of scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the integrity protection shall be as specified in ref. [6].

The home network (AAA server) has to be able to send key material to the WLAN AN, as input for the integrity protection mechanism, in a confidential and integrity protected way (for detailed requirements cf. [27]).

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.2 Confidentiality mechanisms

6.2.1 Confidentiality mechanisms in scenario 2

~~*Text to be added*~~

The link layer confidentiality mechanisms are outside the scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the confidentiality mechanisms of IEEE 802.11i (ref. [6]) shall be used. It is specified in ref. [4] and [5] how the key material required for the link layer confidentiality mechanism is obtained from the master session key MSK. The generation of MSK is defined in ref. [4] and [5] as well. The use of ref. [4] and [5] in the context of 3GPP is specified in section 6.1 of this document.

When the key derivation is finished in the AAA server, the key material will be sent to the WLAN AN via the Wa and Wd (in case of roaming) interfaces.

6.2.2 Confidentiality mechanisms in scenario 3

The confidentiality of IP packets sent through a tunnel between the UE and the PDG, if required, shall be protected by IPsec ESP [rfc2406]. A profile for IPsec ESP is defined in section 6.6.

6.3 Integrity mechanisms

6.3.1 Integrity mechanisms in scenario 2

~~*Text to be added*~~

The link layer integrity mechanisms are outside the scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the integrity mechanisms of IEEE 802.11i (ref. [6]) shall be used. It is specified in ref.[4] and [5] how the key material required for the link layer integrity mechanism is obtained from the master session key MSK. The generation of MSK is defined in ref. [4] and [5] as well. The use of ref. [4] and [5] in the context of 3GPP is specified in section 6.1 of this document.

When the key derivation is finished in the AAA server, the key material will be sent to the WLAN AN via the Wa and Wd (in case of roaming) interfaces.

6.3.2 Integrity mechanisms in scenario 3

The integrity of IP packets sent through a tunnel between the UE and the PDG shall be protected by IPsec ESP (ref. [30])~~[rfc2406]~~. A profile for IPsec ESP is defined in section 6.6.