3GPP TSG SA WG3 Security — S3#33 *Tdoc ⌘S3-040418*
Beijing, China 10 - 14 May 2004

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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Extension of IKEv2 and IPsec profiles
Source:	⌘	Ericsson, Nokia
Work item code:	⌘	WLAN
Date:	⌘	03/05/2004
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:	⌘	Additional algorithms are added in order to avoid problems in case an algorithm is broken and to provide more flexibility in implementations
Summary of change:	⌘	the extension of the profile to one more algorithm, and the specification of the Diffie-Hellman group
Consequences if not approved:	⌘	Only one algorithm for confidentiality and integrity in IKEv2 and IPsec may reduce too much the implementation options. Furthermore, to have one more algorithm gives an alternative if any of them gets broken in future.

Clauses affected:	⌘	2, 6.5, 6.6			
Other specs affected:	⌘	Y / N	Other core specifications	⌘	24.234
		X /	Other core specifications		
		/ X	Test specifications		
		/ X	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: "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.txt, January 2004, “Internet Key Exchange (IKEv2) Protocol”

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

[31] draft-ietf-ipsec-ui-suites-~~04~~05.txt, ~~August~~ April ~~2003~~2004, “Cryptographic Suites for IPsec”

[32] draft-ietf-ipsec-ikev2-algorithms-04.txt, September 2003, “Cryptographic Algorithms for use in the Internet Key Exchange Version 2”

[33] RFC 2104, February 1997, “HMAC: Keyed-Hashing for Message Authentication”

[34] RFC 2404, November 1998, “The Use of HMAC-SHA-1-96 within ESP and AH”

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.5 Profile of IKEv2

IKEv2, as specified in ref. [29], contains a number of options, which are not all needed for the purposes of this specification. IKEv2ESP is therefore profiled in this section. When IKEv2 is used in the context of this specification the profile specified in this section shall be supported.

Access to services offered by the HPLMN (scenario 3) follows a VPN-like approach. In ref. [31] it can be found a set of recommendations of IKEv2 profiles, suitable for VPN-like solutions. On the other hand, ref. [32] sets rules and recommendations for individual algorithms support. Following recommendation from both papers, the below two profiles shall be supported by the PDG and the WLAN-UE:

First cryptographic suite:

- Confidentiality: 3DES in CBC mode
- Pseudo-random function: HMAC-SHA1
- Integrity: HMAC-SHA1-96
- Diffie-Hellman group 2 (1024-bit MODP), mandatory for IKEv2 according to ref. [32]

Second cryptographic suite:

- Confidentiality: AES with fixed key length in CBC mode. The key is set to 128 bits.
- Pseudo-random function: AES-XCBC-PRF-128
- Integrity: AES-XCBC-MAC-96
- Diffie-Hellman group 2 (1024-bit MODP), mandatory for IKEv2 according to ref. [32]

~~The reasons to choose this one are the advantages of AES and its current support by the home network (AAA server) and the UE to for EAP SIM/AKA.~~

~~Editor's note: an example of a profile of IKE, which may be useful to study when writing this section, can be found in TS 33.210, section 5.4.~~

6.6 Profile of IPsec ESP

IPsec ESP, as specified in ref. [30], contains a number of options which are not all needed for the purposes of this specification. IPsec ESP is therefore profiled in this section. When IPsec ESP is used in the context of this specification the profiles specified in this section shall be supported. Rules and recommendations in ref. [31] and [32] have been followed, as in case of IKEv2.

~~As for IKEv2, ref. [31] is used for the profile of IPsec ESP:~~

First cryptographic suite

- Confidentiality: 3DES in CBC mode
- Integrity: HMAC-SHA1-96. The key length is 160 bits, according to ref. [33] and [34]
- Tunnel mode must be used

Second cryptographic suite

- Confidentiality: AES with 128-bit keys in CBC mode. The key length is set to 128 bits.
- Integrity: AES-XCBC-MAC-96
- Tunnel mode must be used

~~The reasons to choose this one are the same as in the case of IKEv2.~~

It shall be possible to turn off security protection (confidentiality and/or integrity) in the tunnel (for example high trust between the 3GPP network operator and the WLAN access provider). This means that tranform IDs for encryption ENCR_NULL and NONE for integrity shall be allowed to negotiate, as specified in ref. [29]

Editor's note: an example of a profile of IPsec ESP, which may be useful to study when writing this section, can be found in TS 33.210, section 5.3.

*** END SET OF CHANGES ***