

## CHANGE REQUEST

33.234 CR 025 rev 2 Current version: 6.2.0

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

<b>Title:</b>	Clean up of not completed chapters		
<b>Source:</b>	SA WG3		
<b>Work item code:</b>	WLAN	<b>Date:</b>	07/10/2004
<b>Category:</b>	F	<b>Release:</b>	Rel-6
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> of the following releases: <i>Ph2</i> (GSM Phase 2) <i>R96</i> (Release 1996) <i>R97</i> (Release 1997) <i>R98</i> (Release 1998) <i>R99</i> (Release 1999) <i>Rel-4</i> (Release 4) <i>Rel-5</i> (Release 5) <i>Rel-6</i> (Release 6) <i>Rel-7</i> (Release 7)

<b>Reason for change:</b>	TS 33.234 still contains some chapters which at the beginning were created in order to insert some text later on, but that have not been filled. This lack of specifications for these chapters has happened because of two reasons: the issue is not under SA3 responsibility, or lack of SA3 interest for the issue. This CR proposes some text to close the chapters
<b>Summary of change:</b>	The main change is in the 'Link layer requirements' chapter. The proposal is to remove the questions and write some summary of the state of the art. The requirements are removed as SA3 is not in charge of this issue, but it corresponds to IEEE instead
<b>Consequences if not approved:</b>	TS 33.234 will contain some chapters not completed

<b>Clauses affected:</b>	2, 4.2.5						
<b>Other specs affected:</b>	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
<b>Other comments:</b>							

\*\*\* 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] IETF RTC 3748: "Extensible Authentication Protocol (EAP)".
- [4] draft-arkko-pppext-eap-aka-12, April 2004: "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)". IETF Work in progress
- [5] draft-haverinen-pppext-eap-sim-13, April 2004: "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)". IETF Work in progress
- [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".~~ [IEEE 802.11i-2004 IEEE Standard for Information technology - Telecommunications and information exchange between systems - LAN/MAN - Specific requirements - Part 11: Wireless LAN Medium Access Control \(MAC\) and Physical Layer \(PHY\) specifications-Amendment 6: MAC Security Enhancements](#)
- [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-08.txt, June 2004: "Diameter Extensible Authentication Protocol (EAP) Application". IETF Work in progress
- [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-02.txt, June 2004: "EAP Key Management Framework". IETF Work in progress
- [28] E. Barkan, E. Biham, N. Keller: "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Crypto 2003, August 2003.
- [29] draft-ietf-ipsec-ikev2-14.txt, May 2004: "Internet Key Exchange (IKEv2) Protocol".
- [30] RFC 2406, November 1998: "IP Encapsulating Security Payload (ESP)".
- [31] draft-ietf-ipsec-ui-suites-06.txt, April 2004: "Cryptographic Suites for IPsec". IETF Work in progress
- [32] draft-ietf-ipsec-udp-encaps-09.txt, May 2004: "UDP Encapsulation of IPsec Packets". IETF Work in progress
- [33] draft-ietf-ipsec-ikev2-algorithms-05.txt, April 2004: "Cryptographic Algorithms for use in the Internet Key Exchange Version 2". IETF Work in progress
- [34] RFC 2104, February 1997: "HMAC: Keyed-Hashing for Message Authentication".
- [35] RFC 2404, November 1998: "The Use of HMAC-SHA-1-96 within ESP and AH".
- [36] RFC 2548, March 1999: "Microsoft Vendor-specific RADIUS Attributes".
- [37] draft-mariblanca-aaa-eap-lla-01.txt, June 2004: "EAP lower layer attributes for AAA protocols".

\*\*\* END SET OF CHANGES \*\*\*

\*\*\* BEGIN SET OF CHANGES \*\*\*

## 4.2.5 Link layer security requirements

Editors note: This section is FFS, LS (S3-030167) sent to SA2 group on 1) the need for requiring 802.11i in TS 23.234. SA2 to explain the impact (if any) a change of technology from 802.11i to WPA would have on the standardisation work. 2) SA2 to study the architectural impacts of implementing protection on Wa interface 3) SA2 to Investigate the importance of specifying specific WLAN technologies to be used for the WLAN access network.

Most WLAN technologies provide (optional) link-layer protection of user data. Since the wireless link is likely to be the most vulnerable in the entire system, 3GPP-WLAN interworking should take advantage of the link layer security provided by WLAN technologies. The native link-layer protection can also prevent against certain IP-layer attacks.

~~In order to set the bar for allowed WLAN protocols, 3GPP should define requirements on link layer security. The existing and work-in-progress WLAN standards can then be evaluated based on these requirements.~~

Areas in which relevant requirements ~~are~~should be defined are:

- Confidentiality and integrity protection of user data;
- Protection of signalling;
- Key distribution, key freshness validation and key ageing.

These requirements are out of scope of 3GPP. IEEE has defined the security requirements and features for the link layer in WLAN access networks, see ref. [6]. Other WLAN access technologies are not excluded to be used although not described here.

### ~~4.2.5.1 Confidentiality and integrity protection of user data~~

- ~~— Can user data be sent in the clear or is some kind of protection required?~~
- ~~— Is it enough to integrity protect user data or should it be encrypted as well?~~
- ~~— How strong must the WLAN security protocols be? Compare e.g. WEP, TKIP and CCMP in the case of 802.11 WLAN.~~

### ~~4.2.5.2 Protection of signalling~~

- ~~— What implications on 3GPP WLAN security does it have if the WLAN control signalling is unprotected? (Currently 802.11 management frames are not protected by 802.11i).~~

#### ~~4.2.5.3 — Key distribution, key freshness validation and key ageing~~

- ~~— Can encryption keys generated during EAP authentication be used directly as encryption keys for the link layer or must there be a handshake between UE and AP to e.g. ensure freshness? (Like the 4 way handshake of 802.11i).~~
- ~~— What are the security implications of not having a UE-AP key handshake?~~

\*\*\* END SET OF CHANGES \*\*\*