

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:	# Deletion of editor's note Wa interface security
Source:	# Ericsson
Work item code:	# WLAN Date: # 07/07/2004
Category:	# F C Release: # Rel-6
<p>Use <u>one</u> of the following categories:</p> <p>F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p>	
<p>Use <u>one</u> of the following releases:</p> <p>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)</p>	

Reason for change:	# In SA3#33 meeting, BT provided an useful document to track the editor's note in TS 33.234. This CR, together with a discussion paper, proposes the removal of one editor's note, that questions the security of Wa interface, and the introduction of normative text justifying the security mechanisms for Wa interface. The reasons for the removal are arguments for the change are explained in the discussion paper Security of the Wa interface is not currently addressed in the specification.
Summary of change:	# Removal of editor's note "Threats on the Wa interface are not clear yet, so protection on this interface is for further study." Addition Specification of security mechanisms for RADIUS and Diameter protection in the Wa interface.
Consequences if not approved:	# The editor's note may indicate uncertainties in the security of the Wa interface, which in the discussion paper are proven to not exist. Lack of security specifications for the Wa interface may lead to non-secure or incompatible implementations.

Clauses affected:	# 2.4.2.2, 5.1.3								
Other specs affected:	<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 # <input 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 # <input type="checkbox"/>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Y	N								
<input type="checkbox"/>	<input checked="" type="checkbox"/>								
Y	N								
<input type="checkbox"/>	<input checked="" type="checkbox"/>								

O&M Specifications

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

*** 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 Cryptanalysis of GSM Encrypted Communication", Crypto 2003, August 2003.
- [29] draft-ietf-ipsec-ikev2-13.txt, March 2004: "Internet Key Exchange (IKEv2) Protocol".
- [30] RFC 2406, November 1998: "IP Encapsulating Security Payload (ESP)".
- [31] draft-ietf-ipsec-ui-suites-05.txt, April 2004: "Cryptographic Suites for IPsec".
- [32] draft-ietf-ipsec-udp-encaps-08.txt, February 2004: "UDP Encapsulation of IPsec Packets".
- [33] draft-ietf-ipsec-ikev2-algorithms-04.txt, September 2003: "Cryptographic Algorithms for use in the Internet Key Exchange Version 2".
- [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"](#)

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

4.2.2 Signalling and user data protection

- The subscriber should have at least the same security level for WLAN access as for his current cellular access subscription.
- 3GPP systems should support authentication methods that support protected success/failure indications.

Editors note: It is for further study if this is possible.

- The selected WLAN (re-) authentication mechanisms for 3GPP interworking shall provide at least the same level of security as [33.102] for USIM based access.
- The selected WLAN (re-) authentication mechanism for 3GPP interworking shall provide at least the same level of security as [43.020] for SIM based access.
- Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material.
- 3GPP systems should provide the required keying material with sufficient length and the acceptable levels of entropy as required by the WLAN subsystem.

Editors note: LS (S3-030166) sent to IEEE 802.11-task group i on their requirements over key length and entropy of keying material

- Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks.
- Protection should be provided for WLAN authentication data and keying material on the Wa, Wd and Wx interfaces.
- The WLAN technology specific connection between the WLAN-UE and WLAN AN shall be able to utilise the generated session keying material for protecting the integrity of an authenticated connection.

Editor's note: ~~Threats on the Wa interface are not clear yet, so protection on this interface is for further study.~~

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.1.3 Transport of WLAN Access authentication signalling between the WLAN access network and the 3GPP AAA proxy server

WLAN Authentication signalling shall be transported over the Wa reference point by standard mechanisms, which are independent on the specific WLAN technology utilised within the WLAN Access network. The transport of Authentication signalling over Wa reference point shall be based on standard Diameter [23], [24] or RADIUS [15], [26] protocols.

When the Wa reference point is based on Diameter, it shall be protected with IPsec if there is no physical protection between the WLAN Access network and the 3GPP AAA proxy/server (the support of IPsec for Diameter is mandatory as stated in ref. [24]).

NOTE: In case of RADIUS based Wa reference point, protection is achieved by means of RADIUS standard procedures. Furthermore In particular, the attribute MS-MPPE-Recv-Key (see ref. [36]) provides extra protection to of the keying material derived in the 3GPP AAA server and sent to the WLAN Access network.

*** END SET OF CHANGES ***