

CHANGE REQUEST

33.234 CR **CRNum** # rev **-** # Current version: **0.4.0**

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:	# Transport of Authentication Signalling in 3G-WLAN		
Source:	# Nokia		
Work item code:	# WLAN	Date:	# 30/04/2003
Category:	# C	Release:	# Rel-6
	<i>Use one of the following categories:</i> 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 .		<i>Use one of the following releases:</i> 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:	# SA2 has made an email decision about the Ws interface. References to CN1's TS 29.234 and definition for Wx interface are missing.
Summary of change:	# - Ws interface added - references to TS 29.234 added - Wx interface definition added
Consequences if not approved:	#

Clauses affected:	# 2, 4.1.1, 4.2.2, 5.1.3, 5.1.4 (new), 5.1.5 (new)			
Other specs affected:	#	#	Other core specifications #	
	#	#		Test 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: " 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] RFC 2284, March 1998, "PPP Extensible Authentication Protocol (EAP)".
- [4] draft-arkko-pppext-eap-aka-06, November 2002, "EAP AKA Authentication".
- [5] draft-haverinen-pppext-eap-sim-07, November 2002, "EAP SIM Authentication".
- [6] IEEE Std 802.11i/D2.0, March 2002, "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 TR 21.905: "Vocabulary for 3GPP Specifications"
- [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)", September 2001
- [18] 3GPP TS 23.003: "Numbering, addressing and identification"
- [19] IEEE P802.1X/D11, March 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 29.234: "3GPP System to WLAN Interworking"](#).

Next modified section

4.1.1 Reference Model

The home network is responsible for access control. The Wx interface is intra-operator. The 3GPP network interfaces to other 3GPP networks, [and WLANs](#), ~~and intermediate networks~~ via the Wr interface.

The 3GPP proxy AAA relays access control signalling to the home 3GPP AAA server [via the Ws interface](#).

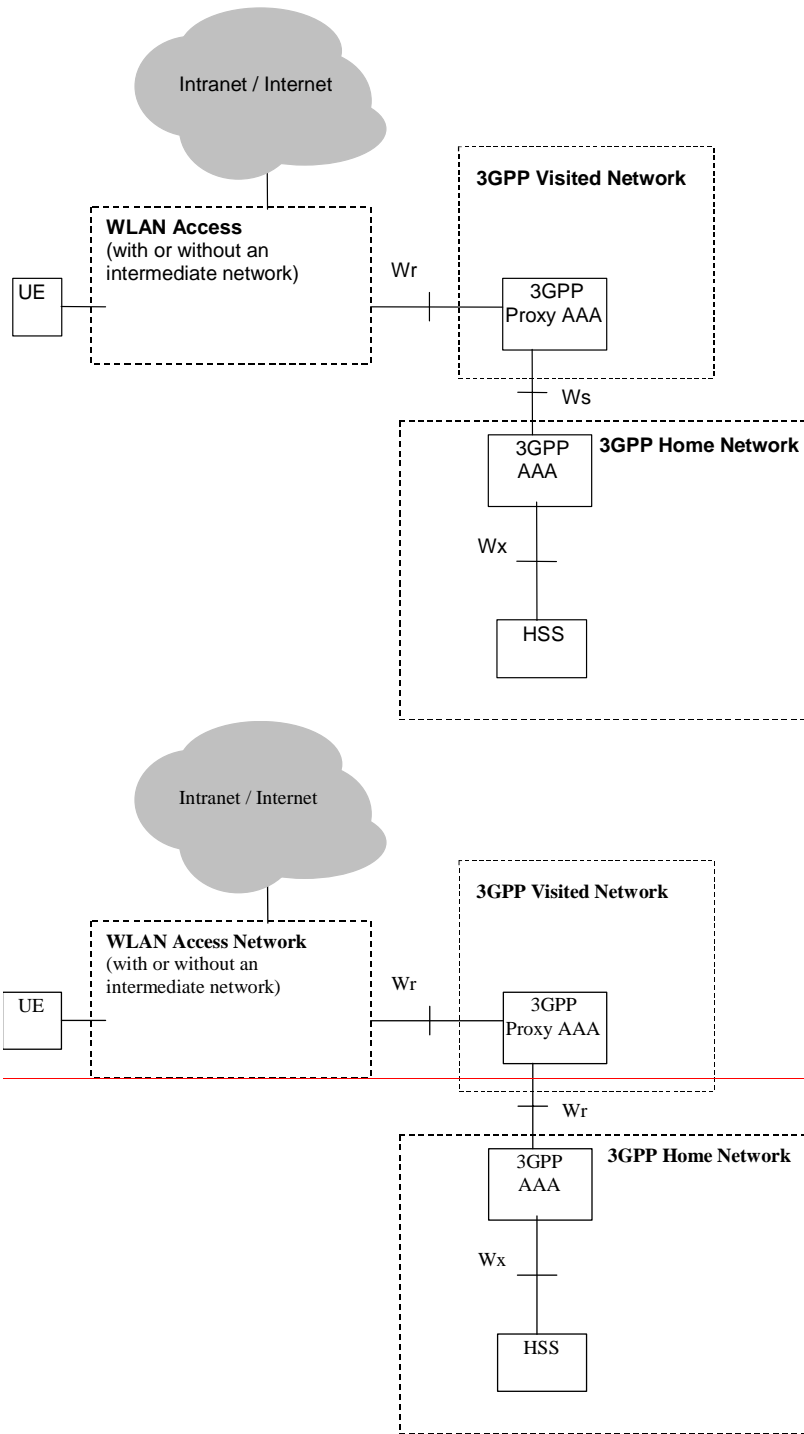


Figure 4.1 Access Control Reference Model

Next modified section

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 not compromise the security offered by the interworking WLAN subsystems.
- 3GPP systems should support authentication methods that support protected success/failure indications. Editors note: FFS 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 Wr, [Ws](#) and [Wx](#) interface
- 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.

Next modified section

5.1.3 Transport of authentication signalling between the WLAN access network and the 3GPP [AAA proxy server](#)~~network~~

WLAN Authentication signalling shall be transported over Wr 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 Wr reference point shall be based on standard Diameter or RADIUS protocols [as specified in \[21\]](#).

Next modified section

[5.1.4 Transport of authentication signalling between the 3GPPP AAA proxy server and the 3GPP AAA server](#)

[WLAN Authentication signalling shall be transported over Ws reference point by standard mechanisms. The transport of Authentication signalling over Ws reference point is specified in \[21\].](#)

Next modified section

5.1.5 Transport of authentication signalling between the 3GPP AAA server and the HSS

WLAN Authentication signalling shall be transported over Wx reference point by standard mechanisms. The transport of Authentication signalling over Wx reference point is specified in [21].