3GPP TSG SA WG3 Security — S3#31 **Tdoc ⌘S3-030735**
Munich, Germany 18 - 21 November 2003

CR-Form-v7

CHANGE REQUEST

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

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:	⌘	Editorial changes and informative annex in TS 33.234
Source:	⌘	Ericsson
Work item code:	⌘	WLAN
Date:	⌘	06/11/2003
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:	⌘	Some RFCs and internet drafts have been updated since chapter 2 'References' was updated for the last time. In other to keep consistency with the rest of the documents versions, the chapter has to be updated. In ther other hand, an informative annex about EAP keying framework is introduced in informative annex A.3
Summary of change:	⌘	Some items in the reference list are updated New subchapter in informative Annex A.3
Consequences if not approved:	⌘	Documents referenced in chapter 2 do not show the right version, or other useful documents are missing

Clauses affected:	⌘	2 References			
		Y	**N**		
Other specs affected:	⌘	□	□	Other core specifications	⌘
		□	□	Test specifications	
		□	□	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: " 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, ~~RFC 2284, March 1998~~October 2003, "~~PPP ~~Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-~~06~~11, ~~November~~October 2003~~2~~, "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-~~07~~12, ~~November~~October 2003~~2~~, "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 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~~2~~.txt, ~~June~~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”.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

4.1.5 Reference points description

Wr

The reference point Wr connects the WLAN Access Network to the 3GPP Network (i.e. the 3GPP AAA Proxy in the roaming case and the 3GPP AAA server in the non-roaming case). The main purpose of the protocols implementing this interfaces is to transport authentication and keying information (WLAN UE - 3GPP network), and authorization information (WLAN AN – 3GPP network). The reference point has to accommodate also legacy WLAN Access Networks and thus should be Diameter [23,24] or RADIUS based [15,26].

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

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

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 [23,24] or RADIUS [15,26] protocols.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

A.3 IETF

A.3.1 Key Generation and EAP Methods

Reference [27] discusses the security aspects of EAP methods generating keys, distributing them to access points via AAA protocols such as Diameter EAP [23], and using them in establishing link-layer security.

A.3.~~1~~2 Co-Existence of RADIUS and Diameter

While Diameter does not share a common protocol data unit (PDU) with RADIUS [15], considerable effort has been expended in enabling backward compatibility with RADIUS, so that the two protocols may be deployed in the same network. Initially, it is expected that Diameter will be deployed within new network devices, as well as within gateways enabling communication between legacy RADIUS devices and servers. This capability, described in [23], enables Diameter support to be added to legacy networks, by addition of a gateway or proxy speaking both RADIUS EAP [15, 26] and Diameter EAP [23, 24].

RADIUS is currently widely used protocol in WLAN environments. At the same time RADIUS is missing several features, such as server initiated messages and may not operate with the highest possible security turned on. Diameter is a better protocol, but it is not very widely deployed yet. Therefore, gradual migration from RADIUS to Diameter seems to be one potential way to go further.

It seems reasonable to start from an initial model of the AAA network where most or all of the access points implement only RADIUS, and a core which uses Diameter but is capable of talking to the RADIUS-only capable access points. This would mean that leaf AAA proxies should support both RADIUS and Diameter. As Diameter-capable access points are inserted to the network, they can be taken into use immediately. An advantage of placing the RADIUS/Diameter-capable nodes on the leafs of the network is that it becomes easier to take advantage of the features found in Diameter. For instance, even accounting may be more reliable if only the first hop is run in RADIUS but the traversal of the access provider, roaming consortium, and home operator proxies is done via DIAMETER.

The actual translation gateway must be able to run both RADIUS and Diameter protocols. The [24] extension defines a framework for the protocol conversion, where the RADIUS attribute space is included into Diameter, which eliminates the need to perform many attribute translations. However, some explicit translations between RADIUS and Diameter attributes must be made, like translating vendor specific and accounting information.

Some Diameter related messages cannot be translated during the communication with RADIUS client, such as messages initiated by Diameter server. Interoperability between RADIUS and DIAMETER in the presence of some of the non-standard RADIUS extensions has not been specified.

The gateway needs to add RADIUS application layer security mechanisms towards RADIUS, and IPsec or TLS towards Diameter. Given the use of the hop-by-hop security mechanisms, this translation can be performed without the knowledge of the original sender of the message. RADIUS requires pre-shared keys, while Diameter can take advantage of either IKE or TLS.

In addition, the translation gateway must secure attribute data towards the home server using Diameter CMS techniques (when the RFC is published). That is, end-to-end security mechanisms can be employed between the translation proxy and the home server, but not between the RADIUS-only access point and the translation proxy.
Diameter – RADIUS compatibility mode should support both protocols along with the necessary translation mechanisms in order to enable the use of RADIUS-only access points. Such translation should occur as near the leaves of the network as possible. As not all functions can be translated in full, some loss of functionality occurs for those devices, which use RADIUS.

It is possible to use IPSec in those cases where RADIUS is used, as currently required in RFC 2869bis. This may help to eliminate some of the vulnerabilities of RADIUS. In addition, 3GPP may adopt the use of RFC 2869bis and corresponding Diameter counterpart as the standard for running EAP over AAA protocols.

*** END SET OF CHANGES ***