3GPP TSG SA WG3 Security — SA3#35 **S3-040722**
October 5-8, 2004
St Paul's Bay, Malta

Source: **BT Group**
Contact: **Colin Blanchard colin.blanchard@bt.com**
Title: **Resolving the editors notes in Wireless Local Area Network (WLAN) interworking security 3GPP TS 33.234**

Document for: **Discussion and decision**
Agenda Item: **6.10**

1. Introduction

The current version of Wireless Local Area Network (WLAN) interworking security 3GPP TS 33.234 V6.1.0 (2004-06) as amended by CR's agreed at SA3#34, contains a number of editor's notes, which need to be resolved to allow them to be removed from TS33.234. This contribution provides a summary of these editors' notes and their current status in 3GPP or IEEE802.11.

2. Draft action Plan

TS33.234 Para. Ref.	**Editors note content**	**Status**
3.1	Editors note: This WLAN-UE definition needs to be reflected in related specifications.	Still to be done
4.2.2	"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	We have an interim informal reply: Original Message From: Hepworth, Eleanor [mailto:eleanor.hepworth@roke.co.uk] Sent: 06 July 2004 14:17 To: Myers,AD,Andrew,XSG1 MYERSAD R; Blanchard,CW,Colin,XSG1 R Subject: RE: WIEN Study Group and 3GPP Open Issues *Colin, Andrew,* *I am currently in the process of final preparations for the next IEEE meeting, and I'm a bit stuck on exactly what one of the SA3 issues is* *(Apologies for not sorting this out at one of the audio conferences).On the keying material question, SA3 are asking for clarification of keying material length and entropy. The IEEE802.11i standard states that this should be 256 bits, and the EAP-AKA and EAP-SIM draft both advocate using the top 32 bytes of the MSK as the PMK for 802.11i. In addition, the frequency that the keying material should be refreshed (i.e. the PMK timeout) can be configured by the authentication server. Please could you just confirm exactly what information further to this is required by SA3, or is it just an official response that provides the above information?* Does SA3 need any further clarification?
TS33.234	**Editors note content**	**Status**

Para. Ref.		
4.2.4.2	Editors note: It was agreed at SA3#31 that for WLAN interworking, modification of EAP parameters on the Bluetooth interface will cause EAP to fail in the network or on the USIM. It was therefore agreed to remove the "undetected modification" requirement from this TS.	Suggest that this is deleted
4.2.4.3	"For SIM access via a Bluetooth link, the SIM Access Profile developed in BLUETOOTH SIG forum may be used. See [22]." Editor note: The version of the SIM Access Profile specification in the reference needs to be updated, if SA3 decides that a new version is required.	Review after new text from"(U)SIM Security Re-use" CR's to TS33.234 have been agreed
4.2.6	"Working assumptions The security mechanisms used in context with the IP tunnel in scenario 3 are to be independent of the link layer security in scenario 2." Editor's note: The independence requirement is not for security reasons. If the solution developed implies significant inefficiencies then this would be reported to SA WG2 for possible revision of this independence requirement.	Suggest that this is deleted
5.1.6	Editor's note: The use of PEAP with EAP/AKA and EAP/SIM is currently under consideration. If PEAP is used, the temporary identity privacy scheme provided by EAP/AKA and EAP/SIM is not needed.	Suggest that this is deleted as no contributions have been received by SA3 , even though PEAP-TLS is built into Windows XP
5.4	Visibility and configurability Editor's note: This section shall contain what the subscriber shall be able to configure and what is visible for the subscriber regarding the actual protection the subscriber is provided with. And 4.2.5 Link layer security requirements Editors note:	Presentation IEEE 802.11 WIEN – SG (WLAN Interworking with External Networks – Study Group). 13th July 2004 *"3GPP does not specify any level of link layer security and permit interoperability to WEP, WPA and 802.11i (WPA2) networks indiscriminately. However, these technologies do not provide any indication of security to the user. Additionally, no decisions are made from a 3GPP network perspective on the behaviour of the accessed network in terms of the link layer security in place, i.e. a WLAN Access Network is treated as a black box into which 3GPP pass the keys required for link layer encryption.* *Can the SG provide a view on:*

	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.	*–Whether there is a need for indicating a security level to the user* *–The possible impacts of "support vs non-support" of a security indicator within a device when requested by a 3GPP network e.g. the 3GPP network may refuse connection based on this information."* This group is now in the formal process of becoming a Task Group. If agreed by IEEE, the group will be known as IEEE 802.11u. While there appears to be interest providing no formal response to SA3 can be provided at this time
6.1.3	EAP support in Smart Cards Editors note: LS (S3-030187/ S1-030546) from SA1 has stated, "There are requests from operators for a secure SIM based WLAN authentication solution". SA3 has SA1 in an LS (S3-030306) if this request is confirmed. The input paper to SA3 on this can be found at: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_28_Berlin/Docs/ZIP/S3-030198.zip	The argument in SA3 seems to go something like this" *The weakness that putting EAP on the UICC addresses is not present in EAP/AKA. We have EAP/SIM in the specification to allow the use of existing SIM cards. If we have to have new UICCs to put EAP on them, we may as well go for EAP.AKA, which does not require EAP on the UICC. Even if we went for EAP on UICC, the ME's would have to have EAP in them anyway to work with existing UICC's, leading to a double implementation of EAP."* Unless a WLAN operator makes a statement that they want to continue using EAP/SIM e.g. simpler AuC etc and are not prepared to accept the security risks and require a solution, then I suggest we delete the editors note and advise 3GPP T3 and ETSI SCP to reconsider their work on EAP on the UICC
6.1.5	Mechanisms for the set up of UE-initiated tunnels (Scenario 3) Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3. The text in this section reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in Annex E. They may replace the current working assumption in this section if problems with the working assumption arise. Otherwise, Annex E will be removed before the TS is submitted for approval. The above points on the use of IKEv2 are dependent on the analysis of the open issues on legacy VPN clients and key management; in particular, the use of EAP-AKA and EAP-SIM will be studied.	Suggest that this is deleted as no contributions have been received
6.6	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. Future editions of this specification will define additional profiles.	Suggest that this is deleted as no contributions have been received

Annex E: informative	"Alternative Mechanisms for the set up of UE-initiated tunnels (Scenario 3)" Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing. The text in section 6.1.5 reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in this Annex. They may be replace the current working assumption in section 6.1.5 of the main body if problems with the working assumptions arise. Otherwise, this annex will be removed before the TS is submitted for approval.	Suggest that this is deleted, along with the Annex as no contributions have been received