3GPP TSG SA WG3 Security — S3#33 **S3-040283**
10 - 14 May 2004
Beijing, China

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 V6.0.0 (2004-03)**

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 V6.0.0 (2004-03) 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 a framework for agreeing actions both within 3GPP and IEEE802.11. A similar proposal will be made to The Wireless Interworking with External Networks Study Group (WIEN SG) of IEEE 802.11 when they meet on 13th May 2004.

2. Draft action Plan

		3GPP			**IEEE 802.11**		
TS33.234 Para. Ref.	**Editors note content**	**CR required for TS33.234**	**Guidance in TR33.900**	**LS to IEEE to be drafted**	**CR to 802.11i**	**Guidance**	**LS to 3GPP to be drafted**
3.1	Editors note: This WLAN-UE definition needs to be reflected in related specifications.	√	X	X			
4.1.4	Editors note: Definition of simultaneous access still TBA with SA1- LS in S3 030169] Reply to SA2 in S3-030188 provides some clarification	√	X	X			
4.1.4	Editors note: All these alternatives must be carefully studied from a security perspective	Delete	X	X			

		3GPP			IEEE 802.11		
TS33.234 Para. Ref.	**Editors note content**	**CR required for TS33.234**	**Guidance in TR33.900**	**LS to IEEE to be drafted**	**CR to 802.11i**	**Guidance**	**LS to 3GPP to be drafted**
4.2.2	"3GPP systems should support authentication methods that support protected success/failure indications." Editors note: It is for further study if this is possible.	√ Related to use of PEAP	X	X			
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 ubsystem." Editors note: LS (S3-030166) sent to IEEE 802.11-task group i on their requirements over key length and entropy of keying material	N/A	N/A	√			
	"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.	√	X	X			

		3GPP			IEEE 802.11		
TS33.234 Para. Ref.	**Editors note content**	**CR required for TS33.234**	**Guidance in TR33.900**	**LS to IEEE to be drafted**	**CR to 802.11i**	**Guidance**	**LS to 3GPP to be drafted**
4.2.4	"The UE functional split shall be such that attacking the CS or PS domain of GSM or UMTS by compromising the device providing the WLAN access is at least as difficult as attacking the CS or PS domain by compromising the card holding device" Editors note: The requirement is fulfilled if at least the master keys for EAP-AKA and EAP-SIM, as specified in [4] and [5], are computed either on the card or in the card holding device. Editor's note: The termination point of EAP is for further study e.g. if EAP-AKA and EAP-SIM shall terminate in the TE e.g. laptop computer. The decision on the termination point shall take into account the requirements in this subsection.}. LS sent to Bluetooth Architecture Review Board (BARB), Bluetooth CAR group and Bluetooth Security Expert Group in S3-030780.	√	X	√			

		3GPP			IEEE 802.11		
TS33.234 Para. Ref.	**Editors note content**	**CR required for TS33.234**	**Guidance in TR33.900**	**LS to IEEE to be drafted**	**CR to 802.11i**	**Guidance**	**LS to 3GPP to be drafted**
4.2.4.2	“The involved devices shall be protected against avesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.” 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.	Delete editors note	X	X			
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.	Delete editors note	X	X			

		3GPP			IEEE 802.11		
TS33.234 Para. Ref.	**Editors note content**	**CR required for TS33.234**	**Guidance in TR33.900**	**LS to IEEE to be drafted**	**CR to 802.11i**	**Guidance**	**LS to 3GPP to be drafted**
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.	Delete editors note	X	X			

		3GPP			IEEE 802.11		
TS33.234 Para. Ref.	**Editors note content**	**CR required for TS33.234**	**Guidance in TR33.900**	**LS to IEEE to be drafted**	**CR to 802.11i**	**Guidance**	**LS to 3GPP to be drafted**
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.	√	X	X			
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.	√ Related to 4.2.2	X	√			
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.	√ Need CR to define behaviour	X	√			

		3GPP			IEEE 802.11		
TS33.234 Para. Ref.	**Editors note content**	**CR required for TS33.234**	**Guidance in TR33.900**	**LS to IEEE to be drafted**	**CR to 802.11i**	**Guidance**	**LS to 3GPP to be drafted**
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	√	X	√			
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	Delete editors note	X	X			

	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.						
6.5	The reasons to choose this one are the advantages of AES and its current support by the home network (AAA server) and the UE to for EAP SIM/AKA. Editor's note: An example of a profile of IKE, which may be useful to study when writing this section, can be found in TS 33.210, section 5.4.	Delete editors note	X	X			
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.	Delete editors note	X	X			

		3GPP			IEEE 802.11		
TS33.234 Para. Ref.	**Editors note content**	**CR required for TS33.234**	**Guidance in TR33.900**	**LS to IEEE to be drafted**	**CR to 802.11i**	**Guidance**	**LS to 3GPP to be drafted**
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.	√	X	X			