3GPP TSG SA WG3 #30 **S3-030739**

18-21 November 2003

Munich, Germany

Agenda Item:	6.11 WLAN inter-working
Source:	Ericsson
Title:	Split WLAN-UE: Integrity protection on local interface
Document for:	Discussion and decision

1. Introduction

SA3 needs to decide whether integrity protection shall be required on the local interface between a Laptop and a UE.

2 Background

In our TS 33.234 on WI WLAN Inter-working, the split WLAN UE may use a Bluetooth link between the Laptop and the UE. Today Bluetooth only provides protection as encryption. No integrity protection is supported in Bluetooth today.

In addition, the Bluetooth forum has developed a profile named “SIM Access Profile” which was specified in order to get SIM/UICC access from an external device. This SIM Access Profile protocol does not provide any protection.

3. Discussion

It could be considered whether the short communication distance in Bluetooth, should be considered as a physical connection.

In the Ericsson paper in [4], where termination of EAP-AKA and EAP-SIM protocols are discussed, a number of man-in-the-middle attacks on the local interface are described and discussed, and the consequences in the Laptop, 3GPP UE and the network, that these attacks will have.

If SA3 still decides that integrity protection is required, then Ericsson proposes to add this to the SIM Access Profile protocol instead of Bluetooth baseband. Making a change in the Bluetooth baseband would be more difficult to implement and it would take many years before these kind of products supporting this new Bluetooth base-band, would be out on the market.

4. Proposals

SA3 needs to take a decision on whether integrity protection shall be added to the local interface.

Ericsson does not see the need to add integrity protection on the local interface between the Laptop and the 3GPP UE and proposes therefore to delete the requirement on integrity protection in TS 33.234.

5. References

[1] SIM Access Profile, Interoperability Specification, version 0.95VD - d. Document no. CAR 020 SPEC/0.95cB.

[2] 3GPP TS 33.234 V0.4.0 “Wireless Local Area Network (WLAN) Interworking Security”.

[3] S3-030xxx “Split WLAN UE: Termination of EAP-AKA/SIM”, from Ericsson to SA3#31.

3GPP TSG-SA3 Meeting #31
Munich, Germany, 18th-21th November, 2003

Tdoc ⌘DocNumber

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.7.0** ⌘

*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:	⌘	Delete requirement on integrity protection on local interface
Source:	⌘	Ericsson
Work item code:	⌘	WLAN Interworking
Date:	⌘	01/05/2003
Category:	⌘	**C**
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:	⌘	A local Bluetooh link can be used between a TE and MT, in order to allow a WLAN client in a TE to access the UICC or SIM in a 3GPP UE. Bluetooth does not support integrity protection. In TS 33.234 we have currently a requirement on the local interface in the case of WLAN UE Functionality Split. Considering the short communication distance in Bluetooth, Ericsson does not see any reasons for requiring integrity protection on the encrypted SIM access data. Therefore Ericsson proposes to delete such requirement from TS 33.234.
Summary of change:	⌘	Delete requirement on integrity protection when a local Bluetooth link is used between a TE and MT.
Consequences if not approved:	⌘	Bluetooth does not support integrity protection. If we don't delete this requirement from TS 33.234, we need to require the Bluetooth forum where Bluetooth is developed, to add integrity protection.

Clauses affected:	⌘	4.2.4.1

Other specs affected: ⌘	Y	N		⌘
			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.

4.2.4 WLAN-UE Functional Split

4.2.4.1 General

In the case when the WLAN-UE, equipped with a UICC (or SIM card), for accessing the WLAN interworking service, is functionally split over several physical devices, that communicate over local interfaces e.g. Bluetooth, IR or serial cable interface, then is shall be:

- Possible to re-use existing UICC and GSM SIM cards; and

[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 }.

4.2.4.2 Security requirements on local interface

The security functionality required on the terminal side for WLAN-3G interworking may be split over several physical devices that communicate over local interfaces. If this is the case, then the following requirements shall be satisfied:

- Any local interface shall be protected against eavesdropping~~, undetected modification~~ attacks on security-relevant information. This protection may be provided by physical or cryptographic means.
- The endpoints of a local interface should be authenticated and authorised. The authorisation may be implicit in the security set-up.
- The involved devices shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.

[Editor's note: New work item approved at SA3#28" U(SIM) Security Reuse by Peripheral Device on local Interfaces" (S3-030307). The Local interface" undetected modification" requirement - cryptographic requirement for short range e.g. Bluetooth is FFS pending the completion of this WI]