

Agenda Item: 6.11 WLAN inter-working
Source: Ericsson
Title: Split WLAN-UE: SIM Access Profile protocol in Bluetooth forum
Document for: Discussion and decision

1. Introduction

Ericsson presented a document in S3-030251 to SA3 #28, which presented a proposal for split WLAN-UE where SIM access could be provided from a 3GPP UE to an external device as Laptop, by the use of the SIM Access Profile protocol via a Bluetooth link. In this paper (S3-030251) a number of proposals on changes to the SIM Access Profile protocol were presented, in order to better suite the usage model of a split WLAN UE in simultaneous WLAN and GSM/UMTS access.

Ericsson proposes that SA3 discuss each proposal presented in this paper and takes a decision in order to progress the work in Bluetooth forum. Ericsson has separate discussions paper on [Split WLAN UE: Termination of EAP-AKA/SIM protocol] and [Split WLAN-UE: Integrity protection on local interface] for this SA3 meeting.

2. Discussion

2.1 Information required by an external WLAN client from a UICC or SIM card inserted into a 3G/2G UE

A WLAN client residing in an external device (e.g. Laptop) would require the following information from a UICC or SIM card inserted into a 3G/2G UE:

- The knowledge of whether a GSM SIM or UICC card is inserted.
- Read IMSI from a GSM or USIM application;
- Send authentication challenge requests to the GSM and USIM application.
- Receive authentication challenge responses from the GSM and USIM application.

To Ericsson knowledge, these requirements are possible to fulfill already today with the SIM Access Profile, and would not require any further changes.

2.2 New requirements on SIM Access Profile

The following issues are discussed in separate papers from Ericsson in this meeting:

- Termination of EAP-AKA and EAP-SIM in split WLAN UE;
- Need for integrity protection on local interface with a Bluetooth link between the UE and the Laptop;

and agreements from these discussions shall be communicated to the Bluetooth forum, if the SIM Access Profile protocol is impacted.

In addition, it is proposed that the following new requirements on the SIM Access Profile shall be communicated as well:

- Allow a 2G/3G UE to access a 2G or 3G network and simultaneously allow a SIM Access Profile connection to an external TE via a BLUETOOTH link, in order to provide SIM/UICC access to a WLAN client running in a TE (e.g. Laptop).
- The 3G/2G UE shall be required to be switched on and a SIM/UICC card shall be powered on, in order to allow and accept a request from a TE to establish a SIM Access Profile connection.
- It shall NOT be possible from a TE (e.g. laptop) to reset, power on or off a SIM/UICC card inserted into a 3G/2G UE, as the SIM/UICC is already in use for GSM or UMTS access in the 2G/3G UE. Therefore it is proposed that the following features in the SIM ACCESS PROFILE shall NOT be supported in the new version of the specification:
 1. Reset SIM or USIM in the 2G/3G UE;
 2. Power on the SIM or USIM in the 2G/3G UE;
 3. Power off the SIM or USIM in the 2G/3G UE.
- PIN or password in Bluetooth:

In BLUETOOTH a PIN or password of 16 characters is required today. This is not so user friendly. We encourage the usage of an improved pairing proposed by the BLUETOOTH SIG Security Expert Group to be used by the 'SIM Access Profile'. An improved pairing would allow a shorter PIN or password without providing less security.

3. Proposals

Ericsson proposes to send an LS with the requirements in this paper to the Bluetooth Architecture Review Board (BARB) and the CAR groups, asking them to develop a new version of the SIM Access Profile for a split WLAN UE in work item WLAN Inter-working in 3GPP.

4. 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] S3-030251 SIM access via 'SIM Access Profile' and Bluetooth link, from Ericsson in SA3 #28.
- [4] S3-030xxx Split WLAN UE: Termination of EAP-AKA/SIM protocol, from Ericsson.
- [5] S3-030xxx Split WLAN-UE: Integrity protection on local interface, from Ericsson.