3GPP TSG SA WG3 Security — S3#32 **S3-040083**

09 - 13 February 2004

Edinburgh, Scotland, UK

Title: **WLAN BT alternatives**

Source: **Nokia**

Document for: **Discussion and decision**

Agenda Item: **6.10**

1 Introduction

This contribution provides Nokia view of the pros and cons of different alternatives for accessing smart card over Bluetooth for WLAN authentication.

2 Discussion

Currently SA3 is discussing three different alternatives.

2.1 Alternative 1 (BT SAP enhanced to allow WLAN authentication without shutting down GSM radios)

(-) it is not acceptable to pass Kc keys from the card holding device to the laptop but instead direct access to raw triplets should be prevented. irect access would enable a malicious piece of software (running on the laptop) to retrieve triplets from the SIM card.

(-) SAP is a general smart card access profile that is designed for giving control to all smart card features for an external device. SAP is not specific to GSM SIMs. Technical feasibility of having two devices control the smart card at the same time should be proven -- currently it is not clear if this is even possible. Mutual exclusion and alternating access would probably have to be used

(-) WLAN authentication requires several round trips to the smart card: PIN code, running the A3/A8 algorithm, in UMTS possibly another round to synchronize sequence number. Hence, it would be very hard to implement mutual exclusion between the laptop and the local GSM functions -- WLAN laptop would have to keep control for a long time before smart card could be released back to GSM functions.

(-) SAP is designed to routing smart card related requests between smart card the BT SAP client. Performing other things besides low-level request routing, such as EAP-SIM related key calculations, by the card holding device does not seem to fit in the SAP profile. SAP leans itself towards solutions where all actual computations would be performed by the smart card (rather than the card holding device). This is not an acceptable restriction.

2.2 Alternative 2 (EAP peer implemented by card holding device

(+) a very good level of security, since all EAP-SIM and EAP-AKA calculations are performed by the card holding device or the smart card rather than the laptop. Laptop never processes raw triplets.

(+) EAP-SIM network authentication is performed by card holding device, so a malicious piece of software running on the laptop cannot get any information from the SIM because it won't pass network authentication.

(+) general support for any EAP method, so the solution would not be specific to to a certain EAP-SIM/EAP-AKA version or to any particular EAP method.

(+) enable new EAP authentication appliances that can be accessed over BT, regardless of EAP method. (EAP key chain)

(+) this alternative is neutral with regard to whether EAP peer is implemented by the card holding device or the smart card

(+)/(-) Even running EAP-SIM or EAP-AKA re-authentication requires the presence of the card holding device, so sharing a subscription or using an outdated re-authentication state by the laptop is not possible. On the other hand, re-authentication is not as fast as in other alternatives, because the use of the bluetooth link is required.

2.3 Alternative 3 (A3/A8 and EAP MSK derivation performed by card holding device, rest of EAP peer implemented by laptop)

(+) the laptop will not get raw Kc keys, so some of the security problems of alternative 1 are avoided

(+)/(-) EAP SIM and EAP AKA re-authentication is performed by the laptop without consulting the smart card at all, which may improve reauthentication performance. On the other hand, the re-authentication procecure no longer ensures that the laptop is in posession of the smart card. Sharing of subscription until re-authentication state exprises may be possible.

(-) this solution is specific to certain versions of EAP-SIM and EAP-AKA. Other EAP methods are not supported at all. If EAP-SIM or EAP-AKA is updated, then the BT profile also needs to be updated.

(-) EAP-SIM network authentication is performed by the laptop, so a malicious piece of software running on the laptop can make the card holding device calculate EAP-SIM master keys for chosen triplets and nonce values that are easier to break the SIM. This may enable the malicious piece of software to mount attacks against the SIM

3 Consideration of the BT replay attack identified by Orange

The attack identified by Orange, Eric Gaunther, is due to the lack of replay protection over the Bluetooth local link. Instead of changing how EAP-SIM and EAP-AKA use random numbers and MACs, the integrity protection should be added to make every messages transmitted over BT unique and verifiable. So a corresponding solution would be to make sure there is replay protection in the usage of BT.

Currently the alternative 2 and 3 are equally weak against the identified attack. However adding integrity protection seems requires further function from the SIM access profile can provide, choosing alternative 3 for would not simplify the development in BT community.

4 Proposal

Based on our discussion, it is concluded that the alternative 2 seems to be a better approach with more advantages, compared to alternative 1 and 3. It is proposed to this SA3 meeting to adopt the approach for 3GPP-WLAN UE split, and proceed with Bluetooth community.