3GPP TSG SA WG3 Security — S3#34 **S3-040571**
6 - 9 July 2004
Acapulco, Mexico

Source: **Nokia**

Title: **Comments to S3-040467: WLAN: Justification for the introduction of a WLAN application (Gemplus)**

Document for: **Discussion and decision**

Agenda Item:

Abstract

This contribution provides more justification for the introduction of WLAN application.
It is already clear a requirement to use old UICC, meaning the ME needs to support EAP anyway. Do we need to duplicate the function in UICC? What's Gemplus' proposal to ME based EAP function? Replace it or as another option?

1. Introduction

At SA3#33 Beijing meeting Gemplus presented S3-040351 contribution on WLAN application. It was considered necessary to have more explanation of the justification for creating this functionality over the use of EAP-AKA with USIM. This contribution provides more justification for the introduction of this proposal.

2. Spreading of vulnerabilities between WLAN and GSM/GPRS domains

S3-040351 [1] proposed WLAN application as an alternative to the combination of countermeasures based on Special RAND and functional split of EAP-SIM/AKA, this proposal offers a higher security level to prevent attacks on vulnerabilities between WLAN and GSM/GPRS domains.

Special RAND
The Special RAND is a ME-based mechanism; the UICC is not involved in the decision to perform the authentication command according to the Special RAND value sent by the Home Network. The Special RAND mechanism assumes the use of a trusted device. So, in case of ME not implementing the Special RAND mechanism or a hacked ME then there is no separation of domains. A WLAN application in UICC cannot help to mitigate the attack launched by a hacked ME either. The Home Network has no guarantee of the interpretation of the Special RAND by the ME since the HN has no information on the ME capability of the user's UE.
In case of usage of a WLAN application, the Home Network knows if a WLAN application is present on the user's UE since the HN knows the capabilities of the UICC. The Home Network controls the level of security associated to WLAN access request.

Moreover, SA3 have not yet selected Special RAND mechanism for A5/2 protection. So, the availability of special RAND mechanism is not guaranteed to prevent spreading of vulnerabilities between WLAN and GSM/GPRS domains.

Split UE
With WLAN application the session keys Kc, CK or IK are always protected whatever the type of split UE since these session keys never leave the UICC.

Independent key sets
The use of independent key sets for WLAN application guarantees the separation of GSM/GPRS, UMTS and WLAN domains. This can be handled by the ME anyway. The WLAN key sets are not stored in UICC due to the backward compatibility of using old smart card, so store in UICC seems unnecessary.

The WLAN application offers higher security level than the EAP-SIM with SIM and also than EAP-AKA with USIM.

3. Justification for creating WLAN application over the use of EAP-AKA with USIM

WLAN application proposes additional features which improve the security level.

Control of the IMSI-based user identity
When the network does not recognize the temporary identifier used by the WLAN UE, the network requests the WLAN UE to sent the IMSI-based user identity.
A WLAN application allows controlling the sending of the IMSI-based user identity; it determines when to use temporary identifier (pseudonym) instead of the IMSI, e.g. the pseudonym should be used whenever it is available. A fake AP can pretend not recognizing the pseudonym and ask such UICC to send its IMSI, because it is the network to request the IMSI and not controlled by the UICC.

So, the Home Network controls the management of the IMSI sending since it is implemented on the UICC. Moreover, the Home Network has the possibility to change this management by means of OTA mechanism.

Storage of the new keying material
New keying material is derived during USIM-based WLAN Access Authentication.

New keying material
On EAP-AKA full authentication, a Master Key (MK) is derived from the UMTS AKA values (CK and IK keys) and the subscriber identity. The Master Key is fed into a Pseudo-Random number Function (PRF), which generates separate keys:

- The Transient EAP Keys (TEKs) for protecting EAP-AKA packets
  - **K_encr** (128 bits): Encryption key to be used with AT_ENCR_DATA attribute
    K_encr is involved in the ciphering of the user identity
  - **K_aut** (128 bits): Authentication key to be used with AT_MAC attribute
    K_aut is involved in MAC computations covering EAP messages
- Master Session Key (MSK) for link layer security
- Extended Master Session Key (EMSK) for other purposes

On fast re-authentication:

- The same TEKs shall be used for protecting EAP packets
- A new MSK and a new EMSK shall be derived from the original MK and new values exchanged in the fast re-authentication.

In case of WLAN pre-authentication procedure, the WLAN UE needs to do the authentications with many APs and agree one MK with each AP before hand, which can't be all stored in UICC anyway, since it's unclear how many APs available.

EAP-AKA with the USIM according to TS 33.234 [2]

The USIM sends RES, CK and IK to the device hosting the UICC, which computes the Master Key (MK) and derives the new keying material from MK.

Attacks on the device hosting the UICC can allow the retrieval of K_encr involved in the ciphering of the user identity and K_aut involved in MAC computations and checks covering EAP messages.

WLAN application:

The WLAN application computes the new keying material, it checks and computes MAC on EAP messages and deals with the ciphering of the user identity. The UICC does not reveal the Master Key (MK) and the Transient EAP Keys (K_encr and K_aut).

So, WLAN credentials for WLAN access authentication are not revealed in clear in unprotected environment, the WLAN application provides a higher security level than EAP-AKA with USIM.

How to manage the authentication policy for pre-Rel 6 terminal and network, and how to update such policy in terminal side?

4. EAP support in the UICC

ETSI SCP produced ETSI TS 102 310 “Extensible Authentication Protocol support in the UICC [3].

This specification enables the UICC to provide support of different EAP methods, ensuring interoperability between the UICC and any terminal, independently of their respective manufacturers. Examples of EAP methods are EAP-SIM, EAP-AKA, EAP-TLS.

So, the WLAN application could be based on “EAP support in the UICC” specification, 3GPP T3 group could specify the EAP-SIM/AKA methods involved in the 3GPP WLAN access authentication.

5. Conclusion

The use of a WLAN application offers a higher security level and the standardization of this application is not an issue.

We kindly recommend SA3 to adopt WLAN application and send LS to SA1 for consultation and to T3 to ask them to work on WLAN application.

6. References

[1] TD S3-040351, “WLAN application”, Gemplus

[2] 3GPP TS 33.234, “Wireless Local Area Network (WLAN) Interworking security”, Rel-6

[3] ETSI TS 102 310, “Extensible Authentication Protocol support in the UICC”, Rel-6, v1.1.0 (2004-04)