3GPP TSG SA WG3 Security — S3#26 **S3-020639**

19 – 22 November 2002

Oxford, UK

Source: **Siemens**

Title: **WLAN-3G interworking security requirements relating to a functional split on the terminal side**

Document for: **Discussion**

Agenda Item: **7.9 (WLAN inter-working)**

Abstract

It is proposed to add security requirements to TS 33.234 which relate to scenarios for WLAN-3G interworking where the required security functions are split between several devices, e.g a SIM-card in a mobile phone and a laptop. The inclusion of such security requirements is considered useful as such scenarios may be commonly used in the future, and security may be compromised if the proposed requirements are not fulfilled. It is not the purpose of this contribution to advocate or recommend the use or the standardisation in 3GPP of such scenarios.

---

1. UE functional split scenarios in WLAN access

The methods for WLAN-3G interworking, which have been proposed so far in 3GPP, are based on the use of SIM or USIM functionality. These include EAP/SIM and EAP/AKA, and methods based on one-time-password using SMS.

I order to be able to use the existing authentication infrastructure for GSM and UMTS, many operators are expected to prefer solutions which allow access to WLAN using the same SIM or USIM functionality which is used for access to GSM or to the CS and PS domains of UMTS. This SIM or USIM functionality resides on a SIM card / UICC which is inserted in a mobile phone. On the other hand, the WLAN Network Interface Card and the corresponding driver SW today typically reside in a separate device, e.g. a laptop. The phone would not know anything about WLAN specifics, and the laptop would not require any GSM security functionality. This is not an obstacle to the use of SIM or USIM-based methods for WLAN-3G interworking as long as the device providing WLAN access can access the SIM/USIM in the mobile phone via an appropriate interface, which may be provided by e.g. Bluetooth, IrDa or cable. The scenario (for which no originality is claimed) is depicted in the following figure 1. The use of EAP/SIM in such a scenario is sketched in the Appendix.

Figure 1

The use of such a functional split is outside the scope of 3G standards, and therefore also the “local interface” from the above figure 1 is not subject to 3GPP standardisation. However, the use of such a scenario may result in a severe compromise of security unless appropriate care is taken. It is therefore proposed that 3GPP should set minimal security requirements for the use of such a UE functional split scenario. The next section proposes corresponding security requirements.

2. Security requirements for UE functional split scenarios in WLAN access

It is proposed to include the following text in TS 33.234 v020, section 4.2:

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

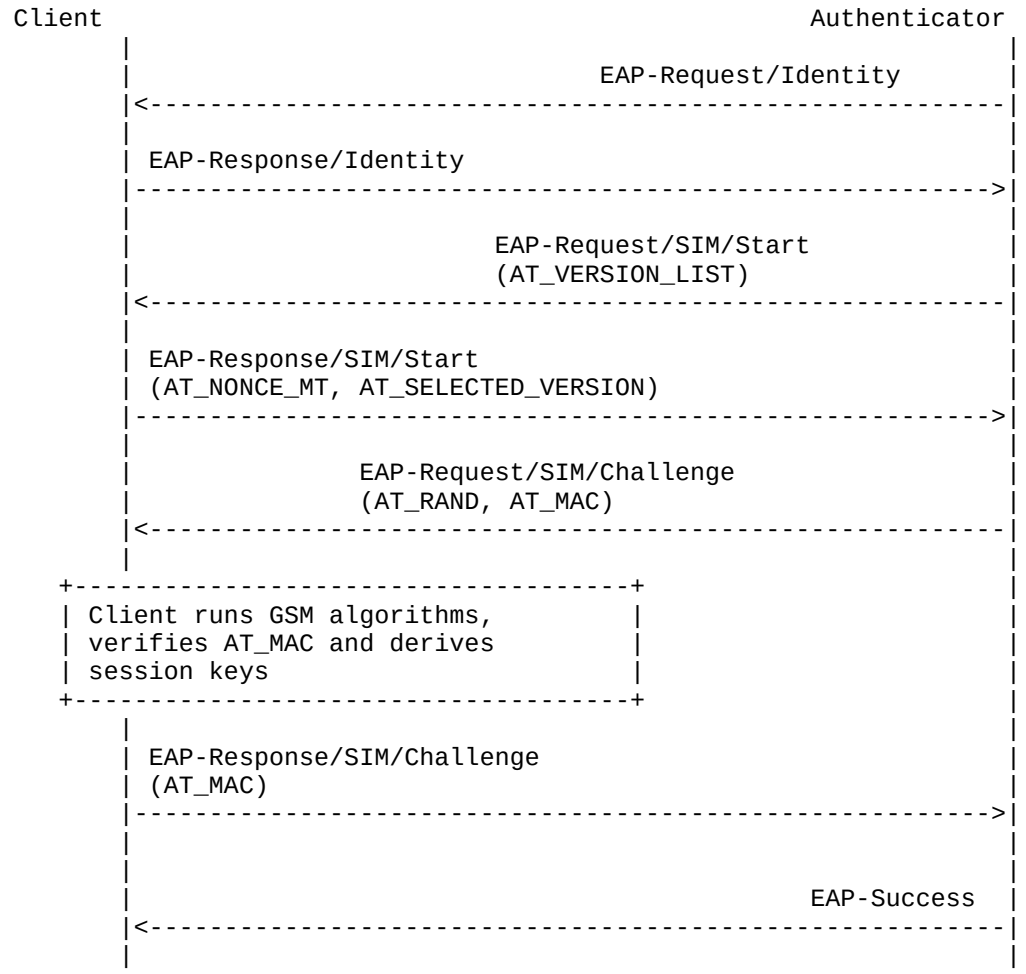
- Any local interface carrying security-relevant information must be adequately protected against eavesdropping and undetected modification. This protection may be provided by physical or cryptographic means.
- The endpoints of a local interface must be authenticated and authorised. The authorisation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

Conclusions

The functional split on the terminal side for WLAN-3G interworking described in this contribution may become practically quite relevant. While the standardisation of such scenarios is outside the scope of 3GPP, it is felt necessary to include pertinent security requirements in TS 33.234 in order to ensure that the use of such scenarios does not generate additional security risks

Appendix:

The UE functional split scenario for WLAN-3G interworking is illustrated for the case of EAP/SIM. The following figure 2 is taken from the latest IETF draft on EAP/SIM [draft-haverinen-pppext-eap-sim-06.txt]. A scenario for WLAN-3G interworking, where client functions are split between a laptop and a mobile phone with a SIM card inserted, may be realised in many different ways. By way of example, we assume that all the functions needed to access the WLAN, i.e. the WLAN network interface card and the driver SW, and to execute the EAP/SIM protocol reside on the laptop, with the exception of the GSM algorithms which reside in the SIM in the phone. So, only the function in the box in figure 2 below labelled “ Client runs GSM algorithms ” would require the support of the SIM in the phone. The laptop would send a challenge RAND over the local interface (as in figure 1 above) and receive the authentication response SRES and the cipher key Kc back over the local interface. Depending on the key length required, this challenge-response procedure would be repeated two or three times. In this way, the mobile phone can remain completely free of WLAN-specific functionality. Of course, in principle the other functions in the box in figure 2 below labelled “ verifies AT_MAC and derives session keys ” could also be executed in the mobile phone or even on the SIM-card, but that would imply WLAN-specific functionality in the in the mobile phone or on the SIM-card, and may therefore be less desirable.



EAP/SIM full authentication procedure

Figure 2