3GPP TSG SA WG3 Security — S3#32 **S3-040048**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item: 6.10 WLAN inter-working

Source: Ericsson

Title: Split WLAN UE: Termination of EAP-AKA/SIM protocol

Document for: Discussion and decision

1. Introduction

In SA3 #31 discussions paper were presented in S3-030738 and S3-030747 on where to terminate the EAP-AKA/SIM protocol in the case of a WLAN UE split configuration. It was decided to postpone the decision to the next SA3 #32.

2 Background

At SA3 #31 three different alternatives were presented in S3-030747 from Siemens, where:

Alternative 1: all functions of an EAP peer are executed on the WLAN access device, with the exception of the functions executed by the SIM or USIM, which are defined in GSM 03.20 and 3G TS 33.102

Alternative 2: all functions of an EAP peer are executed on the card holding device, with the exception of the functions executed by the SIM or USIM as specified in GSM 03.20 and 3G TS 33.102.

Alternative 3: the card holding device computes the master key for EAP-SIM and EAP-AKA from the GSM and UMTS session keys, the remaining functions of an EAP peer outside the card are executed in the WLAN access device.

Alternative 1 was precluded already in SA3 #31, while no conclusion was made between Alternative 2 and Alternative 3. Also the requirement on integrity protection on the local interface was removed from the TS 33.234.

Furthermore after the SA3 #31 meeting, a potential attack was sent out by Orange in [5], on the SA3 reflector where an attacker by recording the traffic on the local interface between the TE and MT and also the traffic between the WLAN AP and TE, could replay the same traffic from a false AP to a TE and from a false MT to the same TE and by this, could succeed in connecting the TE to a false AP.

3. Discussion

This chapter provides some examples of how Alternative 2 and 3 could be implemented with either a new updated version of the SIM Access Profile or potentially a new profile based on RFCOMM in Bluetooth forum.

The intention from Ericsson with this WLAN UE split and simultaneous WLAN and GSM/GPRS access has been to only allow certain operations on the SIM or UICC card when accessed from an external device via Bluetooth, as reading parameters from the card (e.g. IMSI) and handle authentication challenges and responses on the card, when accessed from an external device.

Some concerns has been raised that the UE does not know or cannot distinguish between whether the external device is GSM or WLAN device. By differentiating the commands for WLAN and GSM access (depending on how you update the SIM Access Profile or define a new profile), the 3GPP UE could simply block certain operations from the external device towards the SIM/USIM. If the external device claims it's an AKA for WLAN access, but it's actually for GSM access, then as long as the MT does not give out the CK and IK to the external device, but a hash key as MK or MSK, as in alternative 2 and 3 in Siemens paper S3-030737, an attacker would not achieve anything with this kind of attack, as it can not re-use the key in GSM access. If the external device claims it's an AKA for GSM access by using the

existing SIM Access Profile, then the MT could simply block certain operations, if it already has simultaneous GSM/GPRS access. It should not be a problem to do these kinds of implementations in the MT.

3.1 Alternative 3: Termination of EAP-AKA/SIM in TE except MK derivation

3.1.1 Potential Functionality split in EAP-AKA/SIM

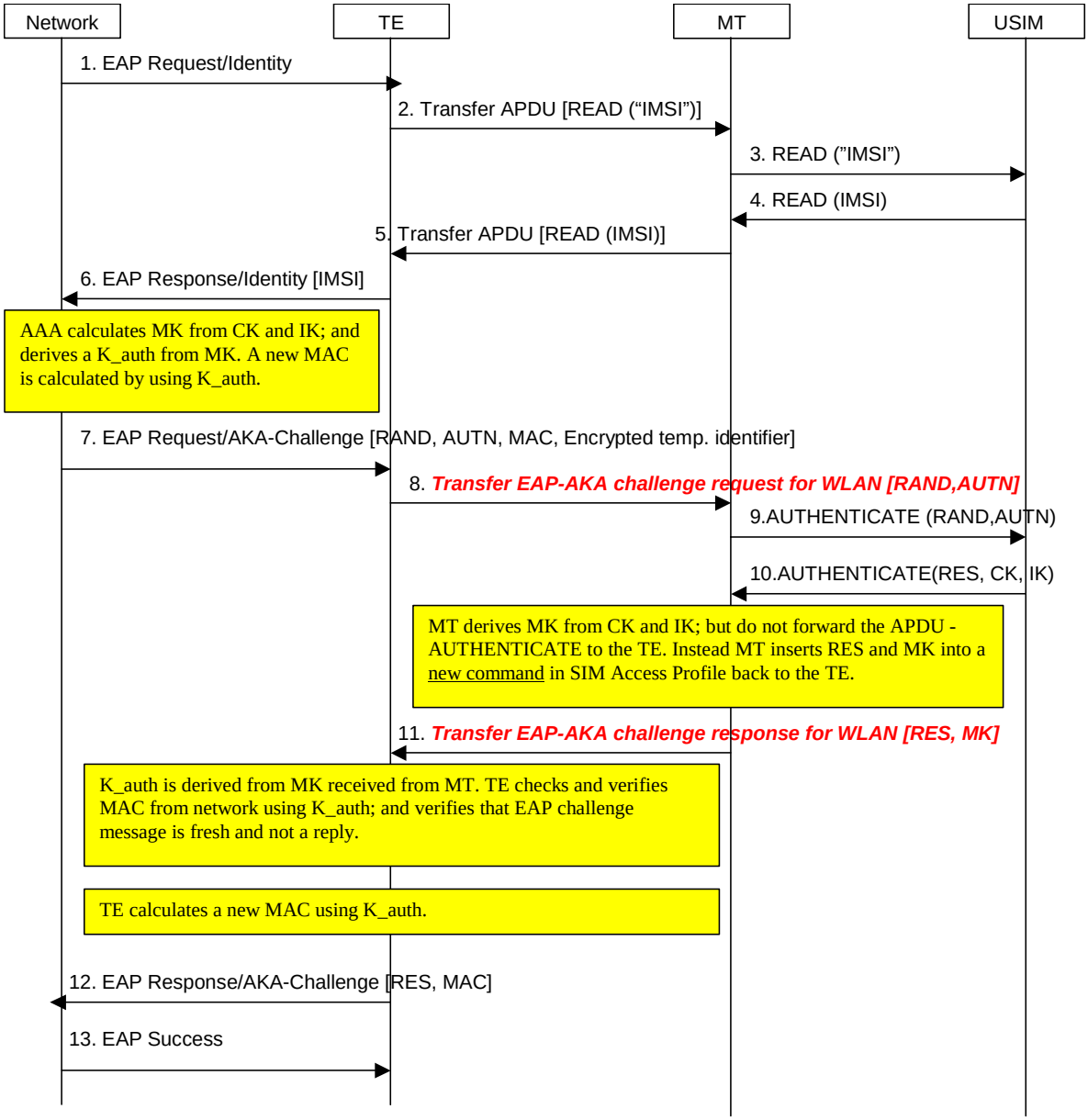
At full authentication and re-authentication, access to a SIM or a UICC is required and therefore the TE needs to contact the (U)SIM in the 3GPP UE via a Blutooth link. It could be visioned that a full authentication does not take place frequently, if the operator is enabling fast re-authentication in his network.

In Alternative 3, when a fast re-authentication takes place, then there is no need for the TE to contact the (U)SIM in the 3GPP UE via a Bluetooth link in alternative 3. This would save signaling on the Bluetooth link between the TE and MT and also power consumption in the MT.

3.1.2 Signaling flows

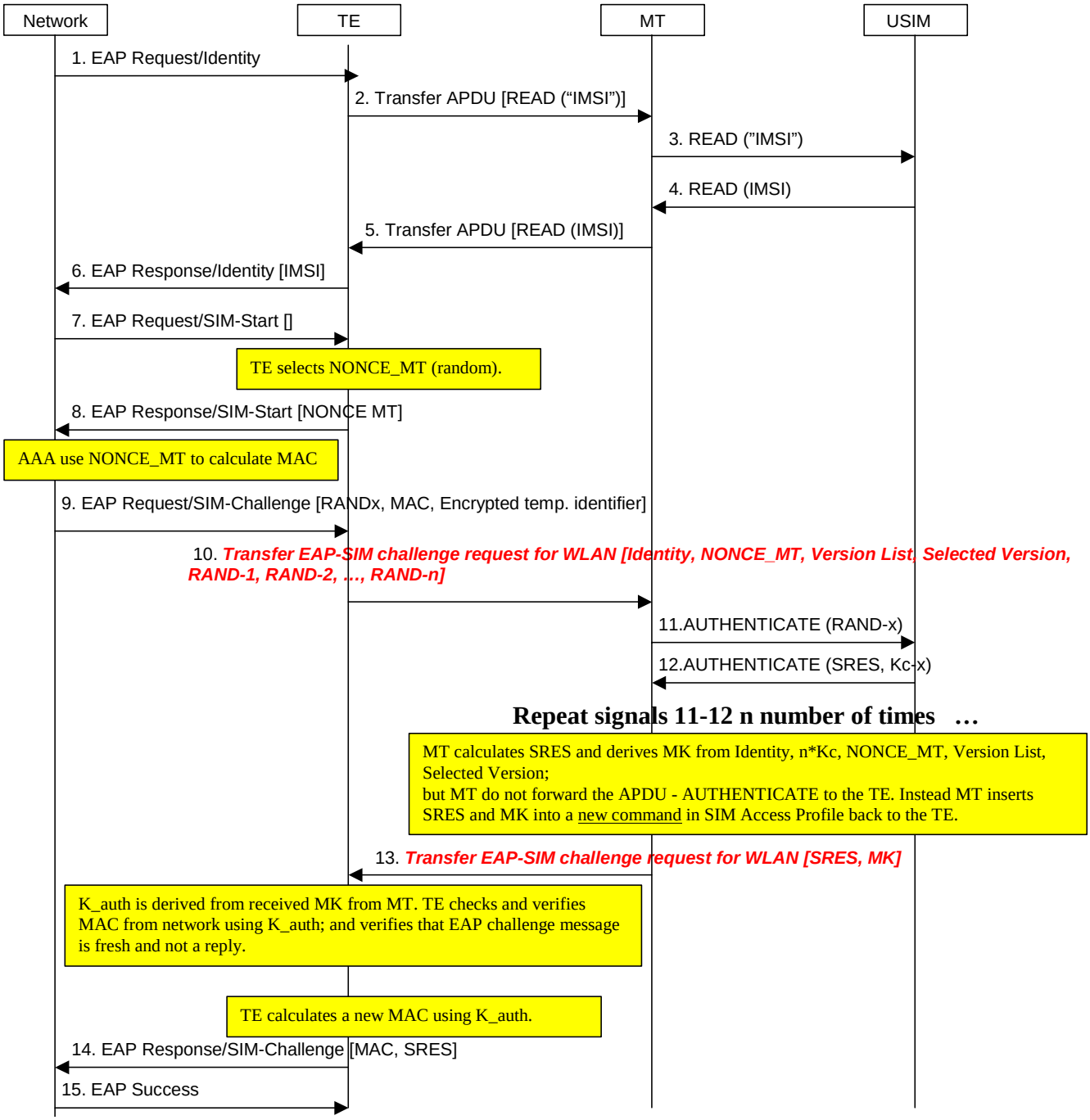
The following signaling flows shows examples of how the functionality in EAP-AKA and EAP-SIM can be split between the TE and MT. This flow presents a potential proposal on how to update the SIM Access Profile protocol to achieve Alternative 3.

3.1.2.1 Full authentication with EAP-AKA



Red and bold parts are new commands in the SIM Access Profile protocol.

3.1.2.2 Full authentication with EAP-SIM



Red and bold parts are new commands in the SIM Access Profile protocol.

3.1.3 Potential attacks

Regarding the attack from Orange in reference [5], when EAP-SIM is used, the NONCE_MT in EAP-SIM can not prevent from these kinds of attacks in Alternative 3 in WLAN UE split, as the TE allocates the NONCE_MT value but the MT calculates the MK using the NONCE_MT has input.

Also with EAP-AKA this kind of attack is possible, as EAP-AKA do not support the NONCE_MT parameter.

3.2 Alternative 2: Termination of EAP-AKA/SIM in MT

3.2.1 Potential Functionality split in EAP-AKA/SIM

As EAP-AKA/SIM terminates in the MT in this alternative, the TE needs to contact the MT via Bluetooth at each full and fast re-authentication, even if no (U)SIM access is required.

Also according to chapter 5.1.7 in TS 33.234, the following text implies that the WLAN UE may be able to initiate a new re-authentication procedure. These kind of requirements can be difficult to support if the WLAN radio is located in the TE and the EAP-AKA/EAP-SIM protocols terminates in the MT. On the other hand these requirements are optional to support in the WLAN UE:

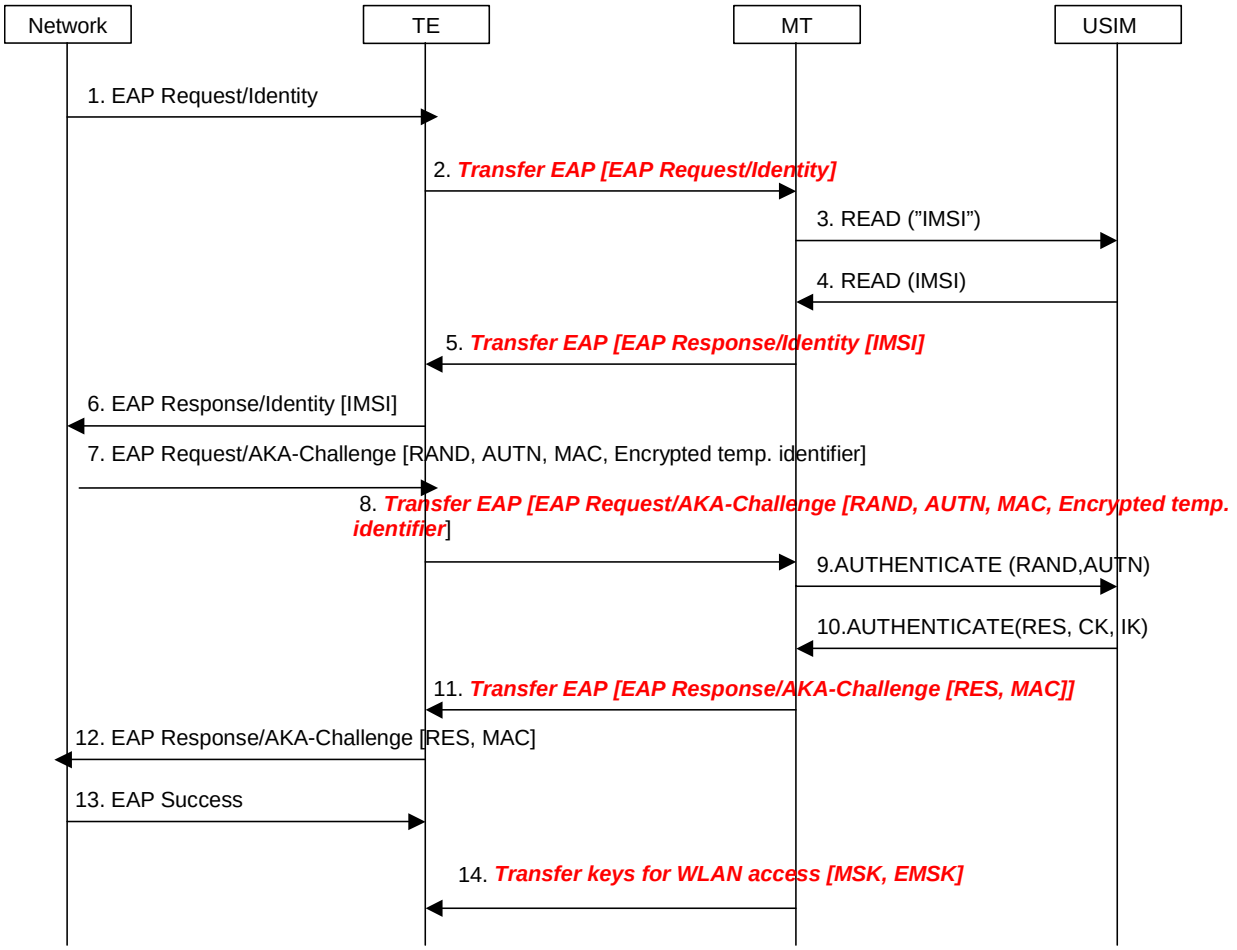
NOTE:

> …
>
> *The WLAN UE may initiate the 802.1x/AAA re-authentication process for example upon moving to a new access point. [Monica: unclear to me in WLAN-UE split when EAP terminates in MT how the MT detects that it has moved to a new access point.] The WLAN UE may also initiate the 802.1x/AAA re-authentication periodically; however it is out of the scope [Monica: Why is it out of scope?] how the WLAN UE determines the frequency of periodic 802.1x/AAA re-authentications.*
>
> …

3.2.2 Signalling flows

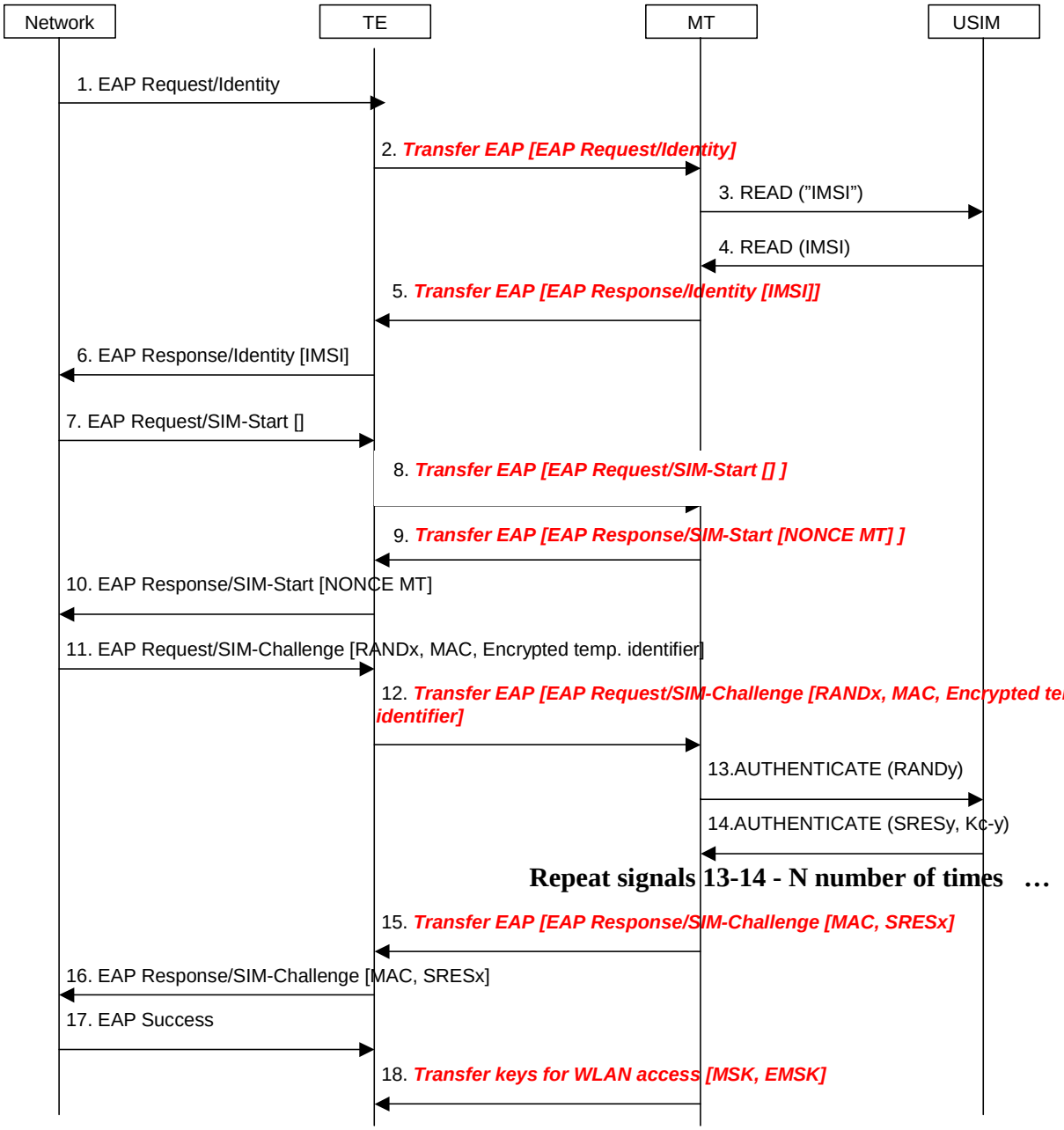
The following signaling flows shows examples of when EAP-AKA and EAP-SIM terminates in the MT. This flow presents a potential proposal on how to update the SIM Access Profile protocol or potentially define a new profile to achieve Alternative 2.

3.2.2.1 Full authentication with EAP-AKA



Red and bold parts are new commands in the SIM Access Profile protocol or potentially included in a new profile in Bluetooth.

3.2.2.2 Full authentication with EAP-SIM



Red and bold parts are new commands in the SIM Access Profile protocol or potentially included in a new profile in Bluetooth.

3.2.3.3 Potential attacks

Regarding the attack from Orange in reference [5], integrity protection would be required on the local interface between the MT and TE, so that the TE can be ensure that the EAP-messages in EAP-AKA/SIM do originate from a real MT.

4. Conclusions

If the attack described by Orange is considered as a serious one by SA3 that needs to be resolved, then alternative 2 and 3 can be considered as secure, only if integrity protection is provided on the local interface between TE and MT in both alternatives.

In Alternative 3, replay attacks will not be prevented by the NONCE_MT parameter in EAP-SIM, as the TE allocates the NONCE_MT value but the MT calculates the MK, using the NONCE_MT has input. Also with EAP-AKA this kind of attack is possible, as EAP-AKA do not support the NONCE_MT parameter.

Of course the seriousness of the Orange attack could be discussed. A false AP could of course send fake user data as WEB pages to the user, which is not aware that it is attached to a false AP. But the user will not get charged with these kinds of attacks. Also the opened vulnerability does allow you to move an attack to another location and not just the original compromised AP place.

5. Proposals

SA3 needs to take a decision on whether EAP-AKA and EAP-SIM shall terminate in the TE or the MT, update TS 33.234 accordingly and send an LS to the Bluetooth forum.

Either of Alternative 2 and Alternative 3 is acceptable to Ericsson.

If the attack presented by Orange shall be solved, then integrity protection needs to be added to the local interface between the TE and MT.

6. 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] S3-030747 Pseudo-CR to TS 33.234 on Requirements on UE split, from Siemens.

[4] S3-030780 LS on SIM Access Profile in split WLAN-UE to Bluetooth- BARB, -SIG and -CAR groups.

[5] Paper on ‘A man-in-the-middle attack using Bluetooth in a WLAN interworking environment’, by Eric Gauthier from Orange, sent out on SA3 e-mail reflector.