3GPP TSG SA WG3 #30 **S3-030738**

18-21 November 2003

Munich, Germany

Agenda Item:	6.11 WLAN inter-working
Source:	Ericsson
Title:	Split WLAN UE: Termination of EAP-AKA/SIM protocol
Document for:	Discussion and decision

1. Introduction

The user can get WLAN access with either a SIM card or UICC card. The 3GPP network will initiate protocols as EAP-AKA and EAP-SIM to authenticate the WLAN UE with a SIM or UICC card will be used for mutual authentication by the 3GPP network and the WLAN UE.

When the WLAN UE is split between two physical devices (i.e. Laptop and 3GPP UE), SA3 needs to decide where the EAP-AKA and EAP-SIM procedures shall be terminated. This paper discusses whether EAP-AKA and EAP-SIM protocols should be terminated in the Laptop or in the 3GPP UE.

The term "local interface" refers to the interface between a Laptop and a 3GPP UE. The discussion in this paper is based on the assumption of a Bluetooth link between the Laptop and the 3GPP UE; and that "SIM Access Profile" is used to provide SIM/UICC access to an external physical device.

Note that when the term 3GPP UE is used, the intention is to terminate EAP-AKA and EAP-SIM in the terminal itself and not on the smart card.

2 Background

In SA2, different scenarios have been defined in the WI WLAN Inter-working. It is expected that scenario 2 and 3 from TS 23.234, will be in REL-6.

Scenario 2 in WLAN Inter-working

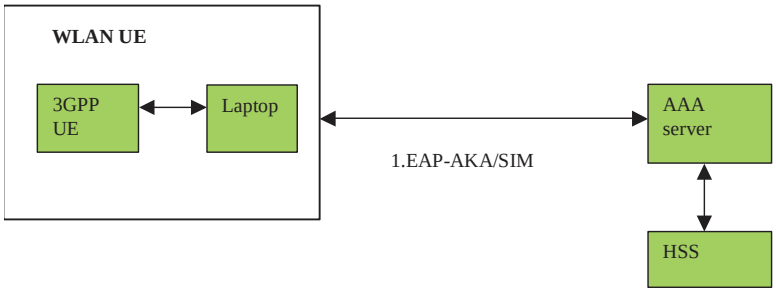


Figure 1

In scenario 2, a successful EAP-AKA and EAP-SIM between the network and WLAN UE is required, in order for the WLAN UE to get WLAN access. EAP-AKA/SIM takes only place in the Link Layer.

Scenario 3 in WLAN Inter-working

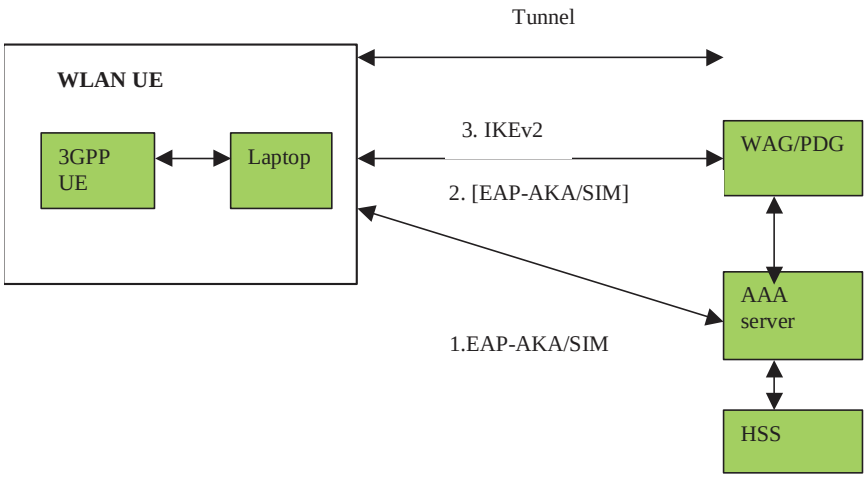


Figure 2

In scenario 3, an 3GPP operator can offer 3GPP services to the user via WLAN access. To achieve this, a tunnel between the 3GPP network and the WLAN UE needs to be established. Two different solutions are currently discussed in SA2, 1) Tunnel switching and 2) End-to-end tunnelling. These two solutions do not have impact on the discussion in this paper.

In SA3 #30, Siemens and Nokia presented contributions on how to secure the tunnel and a number of working assumptions were made like:

- Use IPsec ESP to protect the tunnels between UE and PDG required by scenario 3.
- The **security mechanisms used in context with the IP tunnel in scenario 3 are to be independent of the link layer security in scenario 2**.
- SA WG3 will concentrate their further study on IKE and IKEv2.

This discussion is still ongoing in SA3.

3. Discussion

3.1 Background on security in Bluetooth and SIM Access Profile

In the scenarios discussed in this paper, we assume a Bluetooth link between the Laptop and the 3GPP UE, which provides protection as encryption. Note that Bluetooth does not provide any integrity protection.

The “SIM Access Profile” does not provide any security.

3.2 Assumptions

This paper is based on a number of assumptions.

For scenario 2:

- EAP-AKA and EAP-SIM in the Link layer is only used for user authentication to provide WLAN access to the user.
- Security key(s) produced at EAP-AKA and EAP-SIM at the Link Layer, will not be taken into use by the WLAN-UE or the network.

For scenario 3:

- EAP-AKA and EAP-SIM in the Link layer is only used for user authentication to provide WLAN access to the user.
- Security key(s) produced at EAP-AKA and EAP-SIM at the Link Layer, will not be taken into use by the WLAN-UE or the network.
- The Tunnel established between the 3GPP network and the WLAN UE, terminates in the Laptop;
- An additional EAP-AKA and EAP-SIM procedure will take place at tunnel establishment This EAP-AKA and EAP-SIM procedure at tunnel establishment, is separate from the one taking place in the Link Layer;
- The security keys produced at EAP-AKA and EAP-SIM, will be used by the Laptop to secure the IP-sec tunnel between the Laptop and the 3GPP network. It is expected that an encryption key and integrity key are required in the Laptop and network to protect an IP-sec tunnel.

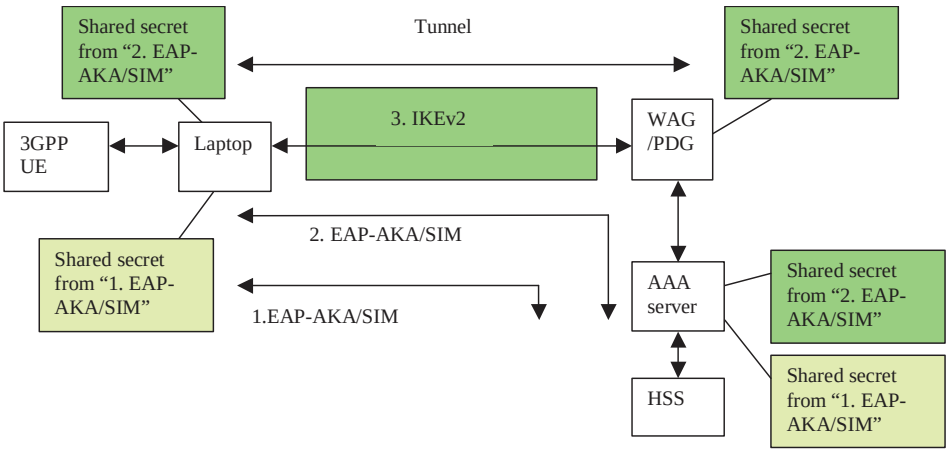
3.4 Termination of EAP-AKA/SIM in split WLAN UE

3.4.1 Termination of EAP-AKA/SIM in the Laptop

In this proposal, the EAP-AKA and EAP-SIM procedure towards the network terminates in the Laptop. The 3GPP UE is not aware of the EAP-AKA and EAP-SIM protocols. After the completion of the EAP-AKA and EAP-SIM procedures, the security keys are stored in the Laptop.

The SIM-ME interface described in TS 31.102 and 11.11 will be extended from the UE to the Laptop. The APDU's specified in these technical specifications, will be carried by the SIM Access Profile protocol specified in [1].

In scenario 2 and scenario 3, the security key(s) will always be sent from the 3GPP UE to the Laptop in an APDU (e.g. SRES and Kc; or RES, CK, IK) when EAP-SIM and EAP-AKA takes place.



3.4.1.1 Trust model

The 3GPP network trust that the Laptop can establish a secured tunnel with the 3GPP network.

The 3GPP operator also trust that the Laptop can securely terminate EAP-AKA and EAP-SIM protocols in the Laptop, and handle these protocols with the 3GPP network.

The 3GPP UE trust that the Laptop can handle the information the 3GPP UE sends to the Laptop.

The 3GPP operator and the Laptop trust that the 3GPP UE can authenticate towards a SIM or UICC on behalf of the Laptop and provide user identity as IMSI to the Laptop.

The 3GPP operator has trust in the SIM and UICC card.

3.4.1.2 Security aspects

3.4.1.2.1 Attacks on the RAND, AUTN, RES, or the SRES

In the EAP-AKA and EAP-SIM protocols, parameters as RAND, AUTN, RES are protected by a separate MAC in the EAP-AKA and EAP-SIM protocols. If EAP-AKA and EAP-SIM terminates in the Laptop, this MAC will NOT be used on the local interface between the Laptop and UE, to protect the RAND, AUTN, RES or SRES.

Attacks on RAND and AUTN, in the Laptop or on the local interface, will cause that the authentication will fail on the USIM. The consequences will be that the user either will not get any WLAN access or the tunnel establishment between the network and Laptop would fail.

Attacks on the SRES or RES, in the Laptop or on the local interface, will cause that the authentication will fail in the network. The consequences will be that the user either will not get any WLAN access or the tunnel establishment between the network and Laptop would fail.

Introduction of integrity protection on the local interface would mean that the Laptop and UE can detect the attacks on the local interface and discard the messages, which fails the integrity check. The consequence will be that timer expiration in the network and the Laptop would take place, and trigger retransmissions of the EAP-messages. After a number of failed retransmissions the consequences will be that the user either will not get any WLAN access or the tunnel establishment would fail. So the consequence would be the same as if integrity protection was not supported.

3.4.1.2.2 Attacks on the security keys in Scenario 3

The security keys produced at EAP-AKA and EAP-SIM will be transferred from the UE to the Laptop, in a APDU carried by the SIM Access Profile. These security keys will be encrypted by Bluetooth on the local interface.

For an attacker to get hold of the security keys sent from the 3GPP UE to the Laptop, an attacker must break the Bluetooth cipher. Integrity protection protects only against man-in-the-middle attacks, which results in corrupted keys and tunnel establishment failure.

The security keys can also be attacked in the Laptop, which also results in corrupted keys. The consequences will be that the tunnel establishment will fail.

In EAP-SIM a number of challenges towards the SIM takes place, and all the Kc values from these challenges are hashed into a new Kc value in the Laptop, to be used to protect the tunnel with the 3GPP network. The most serious attack with terminating EAP-SIM in the Laptop, is that an attacker in the Laptop can take the RAND and Kc values, and display those publicly.

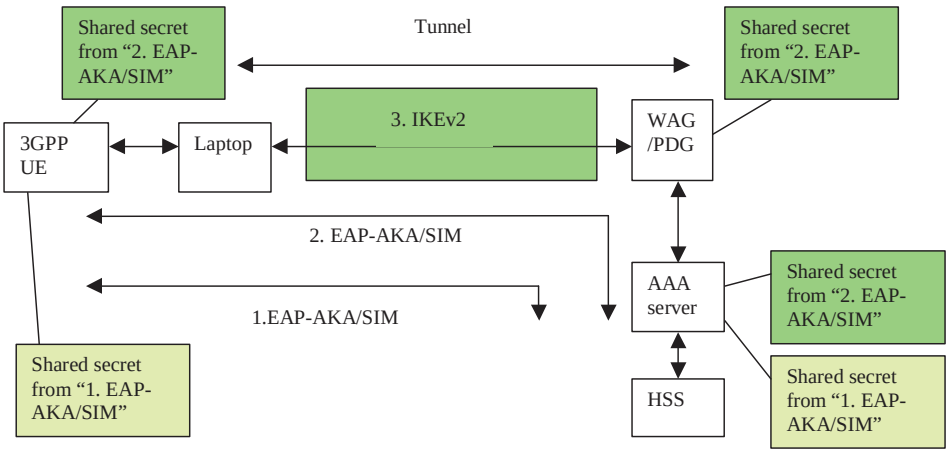
3.4.2.3 Impacts on SIM Access Profile protocol

EAP-AKA and EAP-SIM termination in the Laptop, would have the following impacts on the SIM Access Profile protocol in [1]:

- None.

3.4.3 Termination of EAP-AKA/SIM in the 3GPP UE

In this proposal EAP-AKA and EAP-SIM terminates in the3GPP UE. The EAP-AKA and EAP-SIM procedures will be completely transparent to the Laptop. After the completion of EAP-AKA and EAP-SIM, the security keys are stored in the 3GPP UE. These security keys, needs to be transferred from the UE to the Laptop over the local interface.



3.4.3.1 Trust model

In this proposal, the 3GPP operator has more trust in the 3GPP UE than the Laptop.

On the other hand, the 3GPP network trust that the Laptop can establish a secured tunnel with the 3GPP network.

The 3GPP operator also trust that the 3GPP UE can securely terminate EAP-AKA and EAP-SIM protocols in the 3GPP UE, and handle these protocols with the 3GPP network.

The 3GPP UE trust that the Laptop can handle the information the 3GPP UE sends to the Laptop.

The 3GPP operator and the Laptop trust that the 3GPP UE can authenticate towards a SIM or UICC on behalf of the Laptop and provide user identity as IMSI to the Laptop.

The 3GPP operator has trust in the SIM and UICC card.

3.4.3.2 Security aspects

3.4.3.1.1 Attacks on RAND, AUTN, RES, SRES

In the EAP-AKA and EAP-SIM protocols, a MAC protects the RAND, AUTN, RES and SRES. As the EAP-AKA and EAP-SIM protocol terminates in the 3GPP UE, this MAC will provide protection for the RAND, AUTN, RES and SRES on the local interface as well. This is an advantage compared to the termination of EAP-AKA/SIM protocols in the Laptop, when no integrity protection is provided on the local interface.

Attacks on the RAND and AUTN in the Laptop or on the local interface, will be detected by the 3GPP UE by the MAC, which will simply discard the messages. Expiration of timers will initiate retransmissions of EAP-AKA/SIM messages.

Attacks on the SRES or RES in the Laptop or on the local interface, will be detected by the network by the MAC provided by EAP-AKA and EAP-SIM. The network will attempt to re-authenticate the WLAN UE a number of times before determine that the user authentication has failed. When user authentication is deemed as failed, the user will not get WLAN access or the tunnel establishment between the 3GPP network and the Laptop will fail.

3.4.3.1.2 Attacks on security key(s) in Scenario 3

The security keys from the SIM/USIM at EAP-AKA/SIM, are stored in the 3GPP UE, as EAP-AKA/SIM terminates in the 3GPP UE. These keys need to be transferred from the 3GPP UE to the Laptop, to be used to secure the tunnel between the Laptop and network. A new command needs to be defined in the SIM Access Profile protocol to carry these security keys from the 3GPP UE to the Laptop.

If a MAC was introduced to protect the security keys by the 3GPP UE, the Laptop would be able to detect an attack on the local interface. If the security keys are attacked the tunnel establishment will fail. For an attacker to get hold of the security keys on the local interface, he needs to break the Bluetooth cipher.

The Laptop manufactures needs to ensure that the security keys will not be attacked them-selves in the Laptop. Otherwise the tunnel establishment will fail. The question is how severe such an attack on the security keys on the local interface or in the Laptop is considered? Is it a big threat if the tunnel establishment fails?

In EAP-SIM a number of challenges towards the SIM takes place, and all the Kc values from these challenges are hashed into a new Kc value by the 3GPP UE. The new hashed Kc value needs to be transferred by the 3GPP UE to the Laptop, to be used to protect the tunnel with the 3GPP network. An attacker in the Laptop can get hold of the new hashed Kc value together with the RAND, and display them publicly.

3.4.3.3 Impacts on SIM Access Profile protocol

EAP-AKA and EAP-SIM termination in the 3GPP UE, would have the following impacts on the SIM Access Profile protocol in [1]:

- A new command needs to be defined to carry EAP-AKA/SIM messages between the Laptop and UE;
- A new command needs to be defined to carry security keys from the 3GPP UE to the Laptop;

3.4.3.4 Impacts on 3GPP UE

3GPP UE is required to support EAP-AKA and EAP-SIM protocols.

3.4.4 Other issues related to key management in the Laptop for both proposals

Other issue related to key management in the Laptop:

- With EAP-SIM and a GSM SIM card, only an encryption key (Kc), is available. An Integrity key needs to be derived from Kc as well. This key derivation function needs to be defined for the Laptop.

4. Conclusions

The 3GPP operator needs to have trust in the Laptop, in order for the user to get WLAN access and also that the Laptop has the capability to secure an IP-sec tunnel with the 3GPP network. If this would fail in the Laptop because of malicious software, then the user simply would not get the services from the 3GPP operator via WLAN access. This should not been seen as a major threat as the user will not get charged.

Adding integrity protection to the local interface could help the Laptop and UE to detect man-in-the-middle attacks on the local interface, but once again the consequence with these attacks will be that the user will not get WLAN access or the tunnel establishment will fail. The Bluetooth cipher protects the security keys from eavesdropping. Currently today, there exists no practical attack on the Bluetooth cipher.

EAP-AKA and EAP-SIM termination in 3GPP UE would provide some more security, as RAND, AUTN, RES and SRES are protected by a MAC, on the local interface between the Laptop and 3GPP UE

As the security key(s) from the SIM/USIM at EAP-AKA and EAP-SIM procedures needs to be transferred to the Laptop to be used to secure the IP-sec tunnel with either solution, the actual termination of the EAP-AKA and EAP-SIM protocols would not have any impact on the transfer of the security key(s) to the Laptop.

The main issue seems to be the case when EAP-SIM terminates in the Laptop and the threat exists that an attacker in the Laptop can get hold of the RAND and Kc, and distribute these publicly.

5. Proposals

SA3 needs to take a decision on whether EAP-AKA and EAP-SIM shall terminate in the Laptop or the 3GPP UE. This issue needs to be solved in order to proceed this work on split WLAN UE and finalise the requirement in the TS on split WLAN UE.

The main issue from this analyze seems to be the case when EAP-SIM protocol terminates in the Laptop and the threat exists that an attacker in the Laptop can get hold of the RAND and Kc, and distribute these publicly . SA3 needs to consider whether this is seen as a major threat. If so, then it should be considered to terminate EAP-AKA and EAP-SIM in the 3GPP UE. If this is not seen as a major threat, then Ericsson proposes to terminate EAP-AKA and EAP-SIM in the Laptop. (Note that in the use case when an external smart card reader is connected to a Laptop, EAP-AKA and EAP-SIM needs to terminate in the Laptop).

It should be mentioned that the WLAN UE may support either EAP-AKA or EAP-SIM, or both procedures, as there today exists no requirement on the WLAN UE regarding support of these protocols in TS 33.234. Also one should remember that the operator has the capability in the future to migrate from EAP-SIM to EAP-AKA, if it is felt that this is necessary.

It is proposed that TS 33.234 is updated with the decision taken in this meeting.

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”.