3GPP TSG SA WG3 Security — S3#34 **S3-040562**

6 - 9 Jul 2004

Acapulco, Mexico

Title:	**Binding Scenario Information to Mutual EAP Authentication**
Source:	**Nokia**
Document for:	**Discussion/Decision**
Agenda Item:	
Work Item:	**WLAN**

1 Introduction

The current version of 3GPP TS 33.234 [1] specifies in section 6.1.5 that public key certificates are used to authenticate the PDG. S3-040275 (EAP in IKEv2) [2] proposed that single authentication mechanism, EAP-IKEv2 with EAP-SIM/AKA[4], is used to authenticate the network. The S3-040372 [3] pointed out that there are few possible man in the middle (MITM) attacks against the solution, which was proposed in the S3-040275. This paper discusses two mechanisms to prevent MITM attacks, when the EAP-IKEv2 is used in the WLAN interworking.

2 Discussion

The S3-040372 presented several possible solutions to prevent MITM attacks. In the 3GPP TS 33.234, public key certificates are used to authenticate the PDG. The use of public key certificates is a rather complex solution, because certificates require at least minimal public key infrastructure (PKI). The minimal PKI would contain the certificate authority (CA), manual certificate handling and a mechanism to check the status of certificate (e.g. LDAP and certificate revocation lists).

The following subsections presents two mechanisms to bind WLAN scenario information to EAP-SIM or EAP-AKA authentication. These solutions can be used to prevent MITM attacks instead of public key certificates and the PKI.

2.1 The Enhanced Network Access Identifier (NAI)

In this mechanism, the necessary scenario information is bound to network access identifier (NAI). The current format of NAI is specified in chapter 14.2 of 3GPP TS 23.003 [5] and it is:

wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org

where:

- mnc<MNC> and mcc<MCC> identify the home network.

For example: If MNC = 15 and MCC = 234 then realm part of NAI is "wlan.mnc015.mcc234.3gppnetwork.org"

The enhanced NAI shall contain WLAN scenario information and possible visited network information and it use the following format:

wlan<SCEN>.vmnc<VMNC>.vmcc<VMCC>.mnc<MNC>.mcc<MCC>.3gppnetwork.org

where:

- wlan<SCEN> identifies the WLAN scenario. The possible values could be wlan-scen2, wlan-scen3-hn, wlan-scen3-vn

- vmnc<VMNC> and vmcc<VMCC> identify the visited network. This part is omitted, when it is home network situation.

- mnc<MNC> and mcc<MCC> identify the home network.

For example: If visited network scenario 3 is used, the visited network is MNC =23 and MCC=123 and the home network is MNC =15 and MCC=234 then realm part of NAI is "wlan-scen3-vn.vmnc023.vmcc123.mnc015.mcc234.3gppnetwork.org"

The actual EAP-AKA and EAP-SIM authentication procedures are specified in chapter 6.1 of 3GPP TS 33.234. A malicious visited network PDG and a malicious WLAN AP can modify a NAI in the EAP Response/Identity message, but they cannot modify the same identity, when the AAA server request identity again in the latter phase. See steps 7-10 in the chapter 6.1.1.1 in the 3GPP TS 33.234 and steps 6-9 in the chapter 6.1.2.1 in the 3GPP TS 33.234. If MITM does not modify NAI, but pretends to be a different network element then the AAA server will notice that the request came from the wrong source according to the received NAI.

2.2 Special RAND

The special RAND mechanism was already presented in S3-040372 [3] and S3-040288 [6].

In this mechanism, the WLAN scenario information is bound to the special RAND value. The special RAND contains the encryption algorithms restriction vector context field (EARV_Context) and EARV_Value_bits. They can be used to indicate the WLAN scenario and visited/home network situation. The UE can detect the fraud from the received EARV if a malicious visited network PDG pretends to be a home network PDG or a malicious WLAN AP pretends to be a PDG. The malicious network element cannot change RAND, because AKA would fail.

The format of EARV_Context and EARV_Value_bits has presented in updated version of "Introducing the special RAND mechanism as a principle for GSM/GPRS" [8].

3 EAP-IKEv2 Standardization Status

S3-040372 highlighted that EAP-IKEv2 [4] is in contradiction to the current IKEv2 draft [7]. However, EAP-IKEv2 should be considered as an extension to IKEv2 as SCTP support was for the IKEv1. In the design of IKEv2, mutual authentication of EAP was not considered very carefully, because legacy authentication methods typically support only a user authentication. The mutual authentication of EAP was discussed in the later phase of design of IKEv2 and the consensus was that mutual EAP authentication can provide extensible responder authentication for IKEv2 without public key signatures. The EAP-IKEv2 Internet draft was written, because it was not wanted to delay standardization of IKEv2.

The standardization of EAP-IKEv2 is progressing well. The current draft is -03 and the first one (-00) was published in February 2004.

4 Conclusions

This paper has presented that EAP-IKEv2 that EAP-SIM or EAP-AKA authentication can be used to provide secure network authentication without public key certificates. The S3-040372 presented two different MITM attack scenarios, but they are solved by the enhanced NAI and special RAND mechanisms.

We propose that the EAP-IKEv2 with the EAP-SIM/AKA is used to provide mutual authentication and either NAI or special RAND is used to provide protection against the MITM attacks.

5 References

[1] 3GPP TS 23.234, 3GPP system to Wireless Local Area Network (WLAN) interworking security, version 6.1.0

[2] S3-040275, EAP in IKEv2, Nokia and Ericsson

[3] S3-040372, Comments on S3-040275 (Ericsson, Nokia) and S3-040288 (Nokia) relating to PDG authentication using IKEv2 in scenario 3, Siemens

[4] EAP IKEv2 Method (EAP-IKEv2), IETF Internet draft, <http://www.ietf.org/internet-drafts/draft-tschofenig-eap-ikev2-03.txt>

[5] 3GPP TS 23.003, Numbering, addressing and identification, version 6.3.0.

[6] S3040288, Introducing the special RAND mechanism with GSM/GPRS and WLAN separation, Nokia]

[7] Internet Key Exchange (IKEv2) Protocol, IETF Internet draft, <http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-14.txt>

[8] S3-040xxx, S3#34, Updated version of "Introducing the special RAND mechanism as a principle for GSM/GPRS"