**3GPP TSG SA WG3 Security — SA3#35** **S3-040701**
**October 5-8, 2004**
**St Paul's Bay, Malta**

**3GPP TSG-SA WG2 meeting #41** **Tdoc S2-042951**
**Montreal, Canada, 16th – 20th August 2004**

**Title:** Reply LS on Binding Scenario Information to Mutual EAP Authentication
**Release:** Rel-6
**Work Item:** WLAN

**Source:** SA2
**To:** SA3, CN1, CN4
**Cc:**

**Contact Person:**
**Name:** Osok Song
**Tel. Number:** +82 31 279 5840
**E-mail Address:** **osok.song@samsung.com**

**Attachments:** S3-040672/S2-042440

---

**1. Overall descriptions**

SA2 thanks SA3 for its liaison statement about enhanced NAI for EAP-AKA (S3-040672/S2-042440).

SA2 recognized the following concerns on the method proposed in the LS.

EAP-AKA is used in two different situations; authentication for WLAN access (stated as scenario 2 in S3-040672) and authentication during tunnel setup (stated as scenario 3 in S3-040672). In the former case, EAP messages are routed via AAA servers, so NAI decoration is required. But in the latter case, EAP messages are transported directly between a WLAN UE and a PDG, so no NAI decoration is required.
SA2 acknowledges that the main purpose of the proposal in the LS is not EAP message routing but solving the security problem (i.e. Man-In-The-Middle attack). However, the enhanced NAI and the decorated NAI contains overlapping information about VPLMN identity when it is used for WLAN access authentication.

Decoration of the realm part of NAI is done according to the current version of EAP-AKA Internet-Draft and RFC 2486bis. SA2 thinks that the proposal from SA3 to decorate the realm part of the NAI needs to be checked against these documents.

Also using the word of 'scenario' is not recommended, because it is just the term to distinguish possible steps in developing/deploying I-WLAN. Please note that the word 'scenario' has been removed from TS 23.234.

**2. Actions:**

**To SA3, CN1 and CN4**

SA2 kindly asks SA3, CN1 and CN4 to consider the concerns stated above for their decisions.

**To CN4**

SA2 kindly asks CN4 to check whether it is possible to decorate the realm part of the NAI as described in the attached LS S3-040672 without conflicting with the relevant IETF documents.

**3. Date of Next TSG SA WG2 Meetings:**

| | | |
|---|---|---|
| TSG-SA2 Meeting #42 | 11-15 October 2004 | Sophia Antipolis, France |
| TSG-SA2 Meeting #43 | 15-19 November 2004 | Seoul, Korea |

**3GPP TSG-SA WG2 meeting #41** **Tdoc S2-042440**
**Montreal, Canada, 16th – 20th August 2004**

**3GPP TSG SA WG3 Security — S3#34** **S3-040672**
**July 6 - 9, 2004**
**Acapulco, Mexico**

**Title:** LS on Binding Scenario Information to Mutual EAP Authentication
**Release:** Rel-6
**Work Item:** WLAN

**Source:** SA3
**To:** SA2
**Cc:** CN4

**Contact Person:**
**Name:** Dajiang Zhang
**Tel. Number:** +86 13901168924
**E-mail Address:** **Dajiang.zhang@nokia.com**

**Attachments:** S3-040372, S3-040562, S3-040275

---

**1. Background:**

In SA3#33 meeting, contribution S3-040372 was presented in order to show an attack against WLAN users. Basically, this attacks consists of that a compromised WLAN access point can simulate a PDG towards the user and act like an access point towards the AAA server. As the AAA server has no way to be aware of this attack, the user will be authenticated for scenario 3 while the AAA server believes the user is using scenario 2.
In order to solve this attack, there exist currently some solutions. The accepted solution in the IETF, which is mandatory in IKEv2, see draft-ietf-ipsec-ikev2-14.txt, and which has also been incorporated in TS 33.234 v610 is the use of a certificate to authenticate the network (the PDG) towards the user. This will make it impossible for an attacker to simulate a PDG by means of compromising an access point.

**2. Discussion:**

In SA3#34 meeting, the discussion paper S3-040562 was presented, in which it is proposed to use a modified version of the NAI in order to convey information of the scenario for which authentication is being performed. This solution will help to prevent man-in-the-middle attacks as the one described in S3-040372, and can be seen as an alternative to the use of certificates to authenticate the PDG.

The enhancement of the NAI works as follows:

The current format of NAI is specified in chapter 14.2 of 3GPP TS 23.003 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"

It should be noted that the discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3 and SA3 has not yet agreed to replace the solution in TS 33.234 v610 with the solution proposed in S3-040562, even if SA2 confirms its feasibility. But SA2 is nevertheless contacted at this stage because the deadline for Release 6 is approaching fast, and a response to an LS sent from the next SA3 meeting would probably come too late to be considered for Release 6.

It should also be noted that there is ongoing work at the IETF to address the problems, which the modified NAI proposal in S3-040562 tries to solve, but by different means, cf. draft-eronen-ipsec-ikev2-eap-auth-01 and draft-arkko-eap-service-identity-auth-00.

**3. Actions:**

SA3 kindly asks SA2 to study the feasibility of using enhanced NAI and provide to response in order to take a decision on the mechanism to be used.

**4. Date of Next TSG SA WG 3 Meetings:**

| | | |
|---|---|---|
| TSG-SA3 Meeting #35 | 5-8 October 2004 | Malta |
| TSG-SA3 Meeting #36 | 23-26 November 2004 | Shenzhen, China |

**3GPP TSG-SA WG3 Security #33**
**Beijing, China, 10-14 May 2004**

***Tdoc ⌘S3-040275***

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

***Proposed change affects:*** | UICC apps⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | EAP in IKEv2 |
| ***Source:*** | ⌘ | Nokia, Ericsson |
| ***Work item code:*** | ⌘ | WLAN |
| ***Date:*** | ⌘ | 03/05/2004 |
| ***Category:*** | ⌘ | **C** |
| ***Release:*** | ⌘ | Rel-6 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*

| | |
|---|---|
| *2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | IKEv2 is a component of IPsec used for performing mutual authentication and establishing and maintaining security associations for IPsec ESP and AH. In addition to supporting authentication using public key signatures and shared secrets, IKEv2 also supports EAP authentication, but it requires the use of public key signatures to authenticate responder. However, EAP-SIM and EAP-AKA can be used to provide responder authentication in IKEv2 completely based on EAP. |
| ***Summary of change:*** | ⌘ | Adding support for mutual EAP-SIM and EAP-AKA authentication in IKEv2. |
| ***Consequences if not approved:*** | ⌘ | Public key signatures should be used for responder authentication and public key infrastructure should be deployed. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 2 and 6.1.5 |

| | | Y | N | | |
|---|---|---|---|---|---|
| ***Other specs affected:*** | ⌘ | | X | Other core specifications | ⌘ |
| | | | X | Test specifications | |
| | | | X | O&M Specifications | |
| ***Other comments:*** | ⌘ | | | | |

# 2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.


[1] 3GPP TR 22.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".

[2] 3GPP TR 23.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition".

[3] draft-ietf-eap-rfc2284bis-06.txt, October 2003: "PPP Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-11, October 2003: "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-12, October 2003: "EAP SIM Authentication".

[6] IEEE Std 802.11i/D7.0, October 2003: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[7] RFC 2716, October 1999: "PPP EAP TLS Authentication Protocol".

[8] SHAMAN/SHA/DOC/TNO/WP1/D02/v050, 22-June-01: "Intermediate Report: Results of Review, Requirements and Reference Architecture".

[9] ETSI TS 101 761-1 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 1: Basic Data Transport".

[10] ETSI TS 101 761-2 v1.2.1C: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer".

[11] ETSI TS 101 761-4 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 4 Extension for Home Environment".

[12] ETSI TR 101 683 v1.1.1: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview".

[13] 3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[14] RFC 2486, January 1999: "The Network Access Identifier".

[15] RFC 2865, June 2000: "Remote Authentication Dial In User Service (RADIUS)".

[16] RFC 1421, February 1993: "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures".

[17] Federal Information Processing Standard (FIPS) draft standard: "Advanced Encryption Standard (AES)", November 2001.

[18] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[19] IEEE P802.1X/D11 June 2001: "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".

[20] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[21] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[22] CAR 020 SPEC/0.95cB: "SIM Access Profile, Interoperability Specification", version 0.95VD.

[23] draft-ietf-aaa-eap-03.txt, October 2003: "Diameter Extensible Authentication Protocol (EAP) Application".

[24] RFC 3588, September 2003: "Diameter base protocol".

[25] RFC 3576, July 2003: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".

[26] RFC 3579, September 2003: "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)".

[27] draft-ietf-eap-keying-01.txt, November 2003: "EAP Key Management Framework".

[28] E. Barkan, E. Biham, N. Keller: "Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication", Crypto 2003, August 2003.

[29] draft-ietf-ipsec-ikev2-~~12~~13.txt, March~~January~~ 2004, "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998, "IP Encapsulating Security Payload (ESP)".

[31] draft-ietf-ipsec-ui-suites-04.txt, August 2003, "Cryptographic Suites for IPsec".

[32] draft-eronen-ipsec-ikev2-eap-auth-00.txt, February 2004, "Extension for EAP Authentication in IKEv2".

*** NEXT CHANGE***

## 6.1.5 Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

- The WLAN UE and the PDG use IKEv2, as specified in [~~ikev2~~29], in order to establish IPSec security associations.
- ~~Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG.~~ Depending on the WLAN UE, either EAP-AKA or EAP-SIM within IKEv2, as specified in [32], is used to authenticate the PDG
- EAP-AKA within IKEv2, as specified in [~~ikev2, section 2.16~~32], is used to authenticate WLAN UEs, which contain a USIM.
- EAP-SIM within IKEv2, as specified in [~~ikev2, section 2.16~~32], is used to authenticate WLAN UEs, which contain a SIM and no USIM.
- A profile for IKEv2 is defined in section 6.5.

Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3. The text in this section reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in Annex E. They may replace the current working assumption in this section if problems with the working assumption arise. Otherwise, Annex E will be removed before the TS is submitted for approval. The above points on the use of IKEv2 are dependent on the analysis of the open issues on legacy VPN clients and key management; in particular, the use of EAP-AKA and EAP-SIM will be studied.

*** END OF CHANGE***

**3GPP TSG SA WG3 Security#33** **S3-040372**
**10 – 14 May, 2004**
**Beijing, China**

**Agenda Item:** **6.10 WLAN**

**Source:** **Siemens**

**Title:** **Comments on S3-040275 (Ericsson, Nokia) and S3-040288 (Nokia) relating to PDG authentication using IKEv2 in scenario 3**

**Document for:** **Discussion and decision**

**Abstract**

*The current version of TS 33.234 specifies in section 6.1.5 that "Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG." S3-040275 (EAP in IKEv2) by Ericsson and Nokia proposes a CR to replace this sentence by "Depending on the WLAN UE, either EAP-AKA or EAP-SIM within IKEv2, as specified in [32], is used to authenticate the PDG ". While it is correct to say that the use of certificates may be superfluous because EAP-SIM and EAP-AKA provide mutual authentication, there are several problems with this proposed CR which are addressed in this comment.*

# 1 Man-in-the middle attacks when not using certificate-based authentication of responder (server) in IKEv2

### 1.1 Impersonation of a PDG (scenario 2) by a WLAN AP (scenario 2)

When EAP-AKA or EAP-SIM are used for authentication of the PDG in IKEv2, this gives only the assurance to the UE that the PDG is authorised by the EAP AAA server to receive the EAP session keys. On the other hand, draft-ietf-ipsec-ikev2-13 mandates the use of public key signature based authentication with certificates. This can give additional assurances to the UE, depending on the semantics of the certificate of the responder. In more detail:

For 3G-WLAN interworking, EAP-AKA and EAP-SIM are meant to be used for both, scenario 2 (IP connectivity over WLAN, EAP over IEEE 802.1X) and scenario 3 (IPsec tunnel between UE and Packet Data Gateway, set up using IKEv2+EAP ). It is quite plausible that scenario 3 should come with higher security guarantees for the user than scenario 2 because the user is more likely to trust services provided by his home operator, reached through a PDG, than services provided by a WLAN access network.

But a rogue, or compromised, WLAN AP can impersonate a PDG, as follows: the EAP session key is the MSK from EAP-AKA and EAP-SIM, which is delivered from the EAP AAA server to the WLAN AP (in scenario 2) as well as to the PDG (in scenario 3). Hence the AUTH payload in IKEv2 is computed from MSK, and any attacker who can impersonate a WLAN AP, authorised to participate in scenario 2, towards the EAP AAA server, can obtain the MSK, and consequently compute the AUTH payload and impersonate the PDG towards the UE. But WLAN APs may be assumed to be much more vulnerable than PDGs in the 3GPP operator's home network, making an attack more likely.

### 1.2 Impersonation of a PDG in the home network by a PDG in a visited network

TS 23.234 allows PDGs to also reside in a visited network. Then a PDG in a visited network may also receive the EAP keys MSK from the EAP AAA server in the user's home network. In the same way as described in section 1.1, the PDG in the VN could impersonate a PDG in the home network without the user or the EAP AAA server in the home network knowing. However, it should be noted that UMTS does not allow the user to authenticate the PS or CS access network either, so, if the security objective is only to connect the user securely to any 3GPP network, then there is no problem, but if the security goal is to, in addition, assure the user that he is connected to the home network then the possibility of impersonation of a PDG by another PDG needs to be addressed. This is to be decided by operators.

# 2. Countermeasures against Mitm attacks

**2.1 Use of public key signatures based authentication with certificates**

This is the approach mandated in draft-ietf-ipsec-ikev2-13. The implicit semantics of the certificate could be as follows: the certificate may be verified with a root key which is only used to sign certificates of PDGs of the user's home operator. The UE is pre-configured to use only this root key in the context of scenario 3. In this way, the user knows that he is setting up an IPsec tunnel to the home operator, and not to somebody in control of a WLAN AP.

**2.2 Secure context-information in EAP-SIM or EAP-AKA**

EAP-SIM or EAP-AKA could be enhanced to securely carry context information between UE and EAP AAA server, which ensures that an AP or a PDG in a visited network cannot present two different contexts, one to UE and another to the EAP AAA server. E.g. in the attack in section 1.1, the AP pretends to the UE to be an authorised entity in the context of scenario 3, while the AP is (correctly) known to the EAP AAA server only as an authorised entity in the context of scenario 2.

An example of how to enhance EAP-SIM or EAP-AKA is contained in TS S3-040288 (Introducing the special RAND mechanism with GSM/GPRS and WLAN separation) by Nokia. This contribution proposes to change TS 43.020 to extend the special RAND mechanism to also separate WLAN scenario 2 from WLAN scenario 3 (cf. section C.4 of S3-040288), for the case of EAP-SIM. The proposal could be easily extended to also provide this separation for EAP-AKA, probably requiring a change to TS 33.102. The proposal does not necessitate any changes to the IETF specifications of EAP-SIM or EAP-AKA. Using the mechanism in S3-040288, one can prevent the attack described in section 1.1, but not the one in section 1.2. But it seems plausible, that, by introducing new EARV values, also PDGs in the home and the visited networks could be distinguished, if required.

Please also note that it is up to the operator to implement the special RAND mechanism, and a decision not to implement it would not cause any interoperability problems. Therefore, if PDG authentication is to be based on EAP-SIM or EAP-AKA rather than on certificates, a note should be added to TS 33.234 as a warning that measures against the Mitm attacks described in section 1 of this contribution need to be in place.

Another example, how to prevent the described Mitm attacks, is given in draft-arkko-eap-service-identity-auth-00 which is a generalised mechanism than those proposed in Section 11.4 of draft-tschofenig-eap-ikev2-03.txt. There, it is proposed that integrity-protected information about the authenticator (AP or PDG) is included in EAP messages.

# 3. Non-compliance with IKEv2 standard

The proposal in S3-040275 is in contradiction to draft-ietf-ipsec-ikev2-13, which is likely to evolve into the IKEv2 standard. It should be noted that draft-eronen-ipsec-ikev2-eap-auth-00.txt (reference [32] in S3-040275) addresses the issue of mutual authentication of initiator and responder in IKEv2 without using certificates, in situations when the EAP method already provides mutual authentication. But this draft is still work in progress.

Furthermore, it has to be clear from TS 33.234, exactly what has to be done by the PDG and the UE to perform authentication. The sentence *" Depending on the WLAN UE, either EAP-AKA or EAP-SIM within IKEv2, as specified in [32], is used to authenticate the PDG "* seems not sufficient, as the referenced draft [32] offers four alternative solutions, without making a decision for one. For interoperability reasons, no more than one of these alternatives shall be selected by 3GPP.

# 4. Proposal

It is proposed to only accept S3-040275 if

- the man-in-the-middle attacks described in section 1 are satisfactorily addressed, and a corresponding note is added to TS 33.234, how it is addressed;
- the issues arising from non-compliance with the IKEv2 standard are resolved.

**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"