3GPP TSG SA WG3 Security — S3#21 **S3-010650**

27 - 30 November, 2001

Sophia Antipolis, France

Source: Alcatel
Title: Comments on draft-arkko-pppext-eap-aka-00.txt
Document for: Discussion
Agenda item:

J. Arkko
Ericsson
H. Haverinen
Nokia

Internet Draft
Document: draft-arkko-pppext-eap-aka-00.txt
Expires: December 2001

May 2001

EAP AKA Authentication

Status of this Memo

Abstract

This document specifies an Extensible Authentication Protocol (EAP) mechanism for authentication and session key distribution using the UMTS AKA authentication mechanism. AKA is based on symmetric keys, and runs in a UMTS Subscriber Identity Module, a smart card like device. AKA provides also backward compatibility to GSM authentication, making it possible to use EAP AKA for authenticating both GSM and UMTS subscribers.

Table of Contents

1. Introduction and Motivation

This document specifies an Extensible Authentication Protocol (EAP) mechanism for authentication and session key distribution using the UMTS AKA authentication mechanism [1]. The Universal Mobile Telecommunications System (UMTS) is a global third generation mobile network standard.

AKA is based on challenge-response mechanisms and symmetric cryptography. AKA runs in a UMTS Subscriber Identity Module (USIM), a smart card like device. AKA provides also backwards compatibility to the GSM authentication mechanism [2]. Compared to the GSM mechanism, AKA provides substantially longer key lengths and the authentication of the server side as well as the client side.

The introduction of AKA inside EAP allows several new applications. These include the following:

- The use of the AKA also as a secure PPP authentication method in devices that already contain an USIM.

- The use of the third generation mobile network authentication infrastructure in the context of wireless LANs and IEEE 801.1x technology through EAP over Wireless [3, 4].

- Relying on AKA and the existing infrastructure in a seamless way with any other technology that can use EAP.

AKA works in the following manner:

- The USIM and the home environment have agreed on a secret key beforehand.

- The actual authentication process starts by having the home environment produce an authentication vector, based on the secret key and a sequence number. The authentication vector contains a random part RAND, an authenticator part AUTN used for authenticating the network to the USIM, an expected result part XRES, a session key for integrity check IK, and a session key for encryption CK.

- The RAND and the AUTN are delivered to the USIM.

- The USIM verifies the AUTN, again based on the secret key and the sequence number. If this process is successful (the AUTN is valid and the sequence number used to generate AUTN is within the correct range), the USIM produces an authentication result, RES and sends this to the home environment.

- The home environment verifies the correct result from the USIM. If the result is correct, IK and CK can be used to protect further communications between the USIM and the home environment.

When verifying AUTN, the USIM may detect that the sequence number the network uses is not within the correct range. In this case, the USIM calculates a sequence number synchronization parameter AUTS and sends it to the network. AKA authentication may then be retried with a new authentication vector generated using the synchronized sequence number.

For a full specification of the AKA algorithms and how the cryptographic values AUTN, RES, IK, CK and AUTS are calculated, see reference [1].

It is also possible that the home environment delegates the actual authentication task to an intermediate node. In this case the authentication vector or parts of it are delivered to the intermediate node, enabling it to perform the comparison between RES and XRES, and possibly also use CK and IK.

[Alcatel] Add a statement “Such a delivery MUST be done in a secure manner.”.

In the third generation mobile networks, AKA is used both for radio network authentication and IP multimedia service authentication purposes. Different user identities and formats are used for these; the radio network uses the International Mobile Subscriber Identifier (IMSI), whereas the IP multimedia service uses the Network Access Identifier (NAI) [5].

2. Conventions used in this document

The following terms will be used through this document:

AAA protocol

Authentication, Authorization and Accounting protocol

AAA server

In this document, AAA server refers to the network element that resides on the border of Internet AAA network and GSM network.

[Alcatel] What is the exact purpose of such a precise location of the AAA server ? The AAA server could well be located within the mobile operator’s network.

AKA

Authentication and Key Agreement

AuC

Authentication Centre. The mobile network element that can

authorize subscribers either in GSM or in UMTS networks.

EAP

Extensible Authentication Protocol [6].

GSM

Global System for Mobile communications.

NAI

Network Access Identifier [5].

AUTN

Authentication value generated by the AuC which together with the RAND authenticates the server to the client, 128 bits [1].

AUTS

A value generated by the client upon experiencing a synchronization failure, 112 bits.

RAND

Random number generated by the AuC, 128 bits [1].

RES

Authentication result from the client, which together with the RAND authenticates the client to the server, 128 bits [1].

SQN

Sequence number used in the authentication process, 48 bits [1].

SIM

Subscriber Identity Module. SIM cards are smart cards distributed by GSM operators.

SRES

The authentication result parameter in GSM, corresponds to the RES parameter in UMTS aka, 32 bits.

USIM

UMTS Subscriber Identity Module. These cards are smart cards Similar to SIMs and are distributed by UMTS operators.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [8]

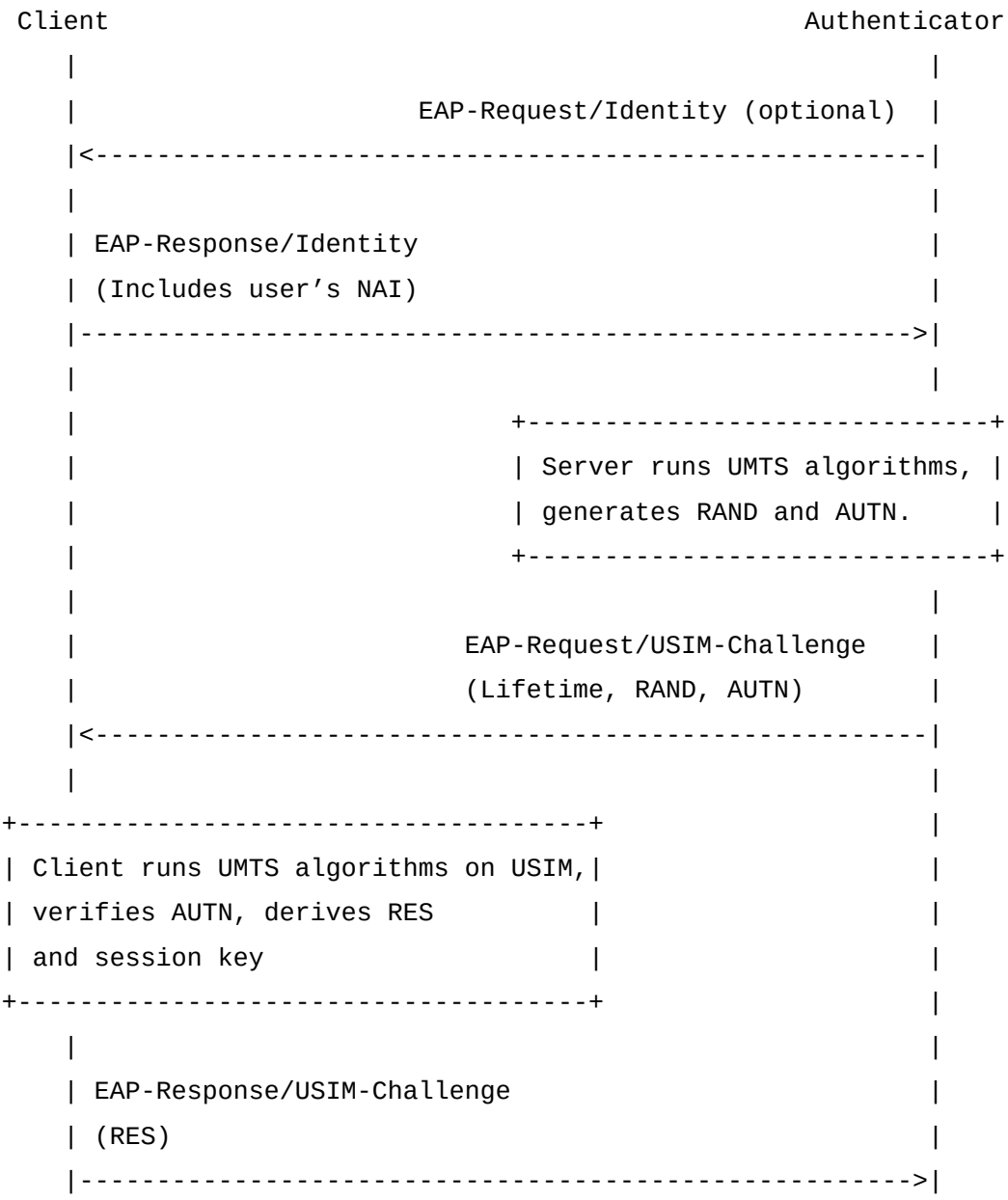
3. Protocol Overview

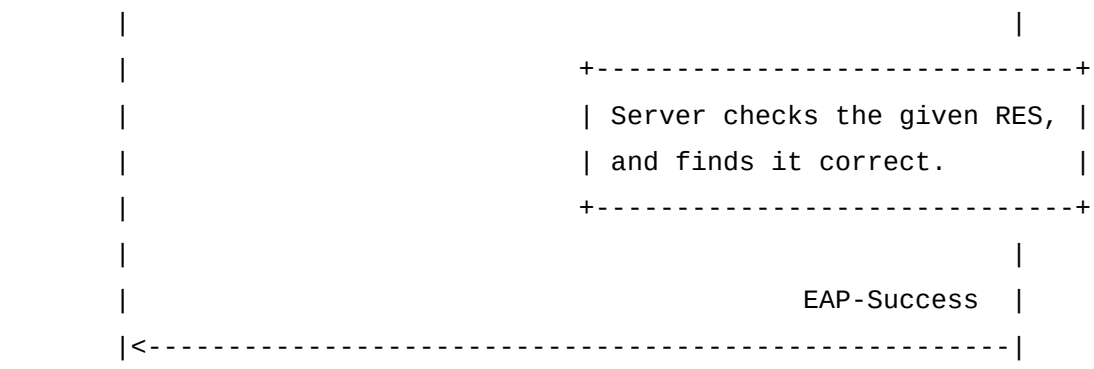
The EAP AKA uses two roundtrips to authorize the user and generate session keys. The authenticator typically communicates with the user's AAA server using an AAA protocol. (The exact AAA communications are outside the scope of this document, however.)

The below message flow shows the basic successful authentication case with the EAP AKA. As in other EAP schemes, first an identity

request/response message pair is exchanged. (For this particular EAP protocol, the identity request is defined to be optional, to shorten the authentication process to a minimal one.)

Next, the authenticator starts the actual AKA protocol by sending an EAP-Request/USIM-Challenge message. This message contains a random number and an authorization vector. The client runs the AKA algorithm (perhaps inside an USIM) and verifies the AUTN. If this is successful, the client is talking to a legitimate authenticator and proceeds to send the EAP-Response/USIM-Challenge. This message contains a result parameter that allows the authenticator in turn to verify that the client is a legitimate one.

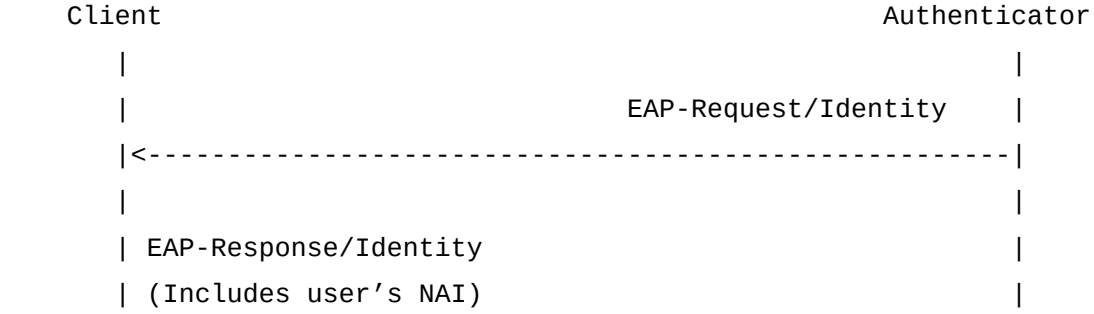

Client
Authenticator
EAP-Request/Identity (optional)
EAP-Response/Identity
(Includes user's NAI)
Server runs UMTS algorithms,
generates RAND and AUTN.
EAP-Request/USIM-Challenge
(Lifetime, RAND, AUTN)
Client runs UMTS algorithms on USIM,
verifies AUTN, derives RES
and session key
EAP-Response/USIM-Challenge
(RES)

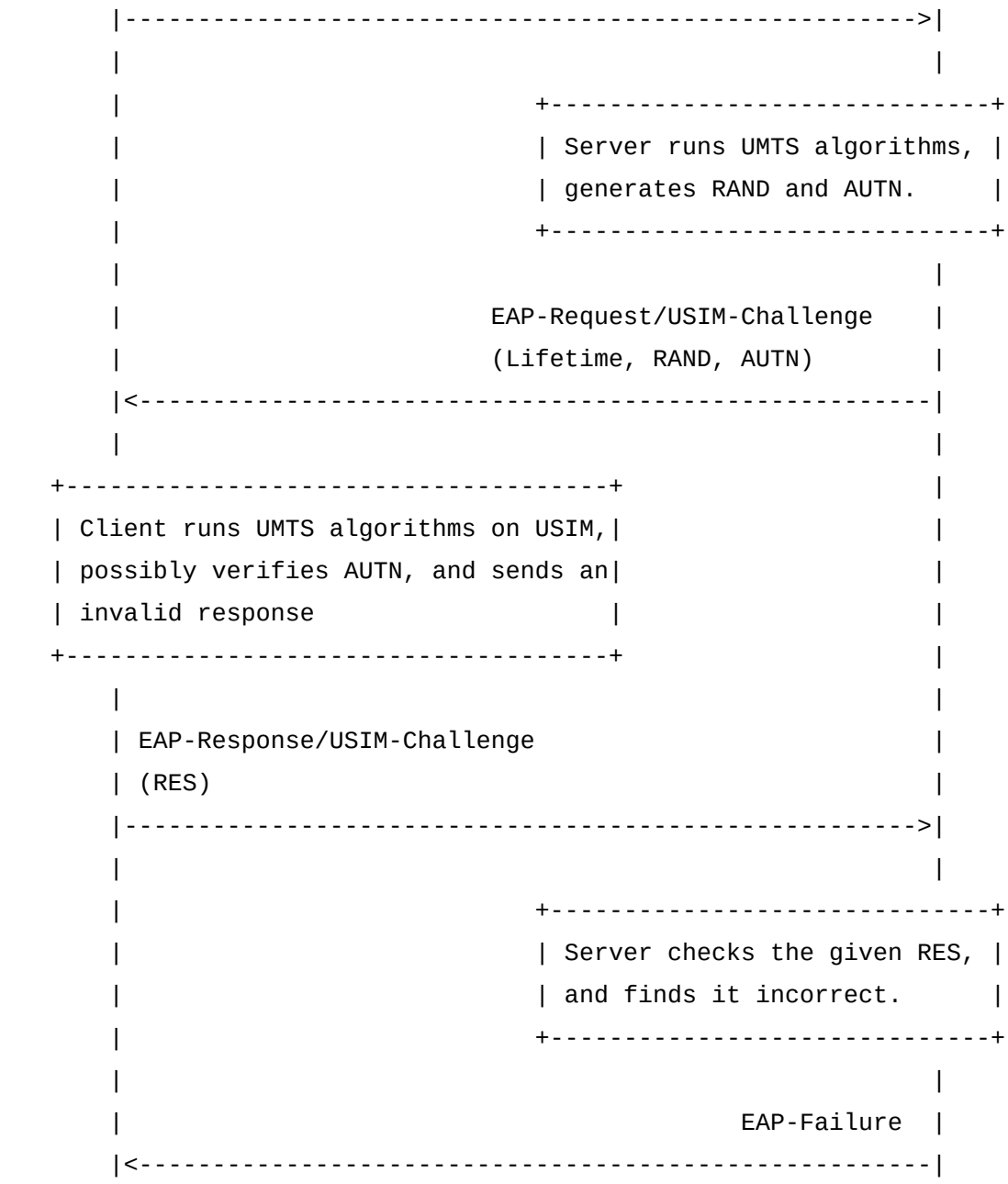


When EAP AKA is run in the GSM compatible mode, the message flow is otherwise identical to the message flow below except that the AUTN parameter is not included in EAP-Request/USIM-Challenge packet.

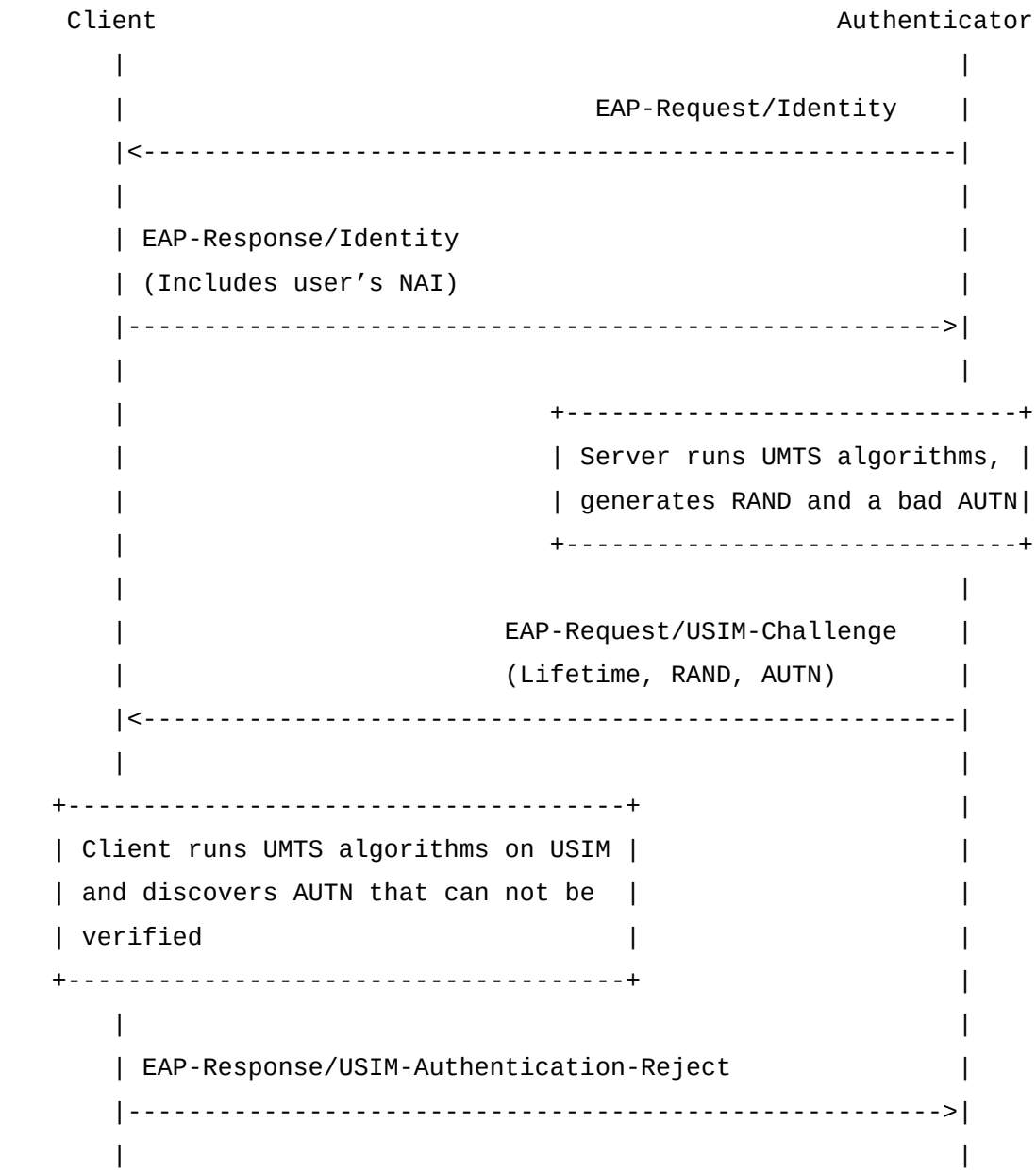
An optional lifetime may be associated to the challenge message. This specifies the server side’s limit on how long the ciphering and integrity keys generated as a part of the authentication process can be used. (The use of such keys is outside the scope of this document.)

The second message flow shows how the Authenticator rejects the Client due to failed authentication. The same flow is also used in the GSM compatible mode, except that the AUTN parameter is not included in the EAP-Request/USIM-Challenge packet.

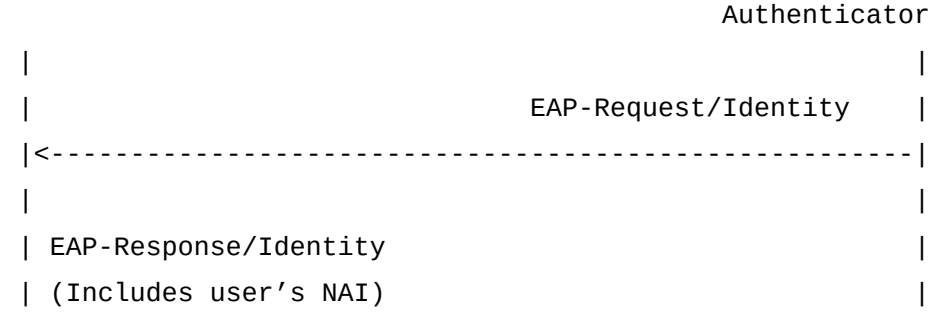


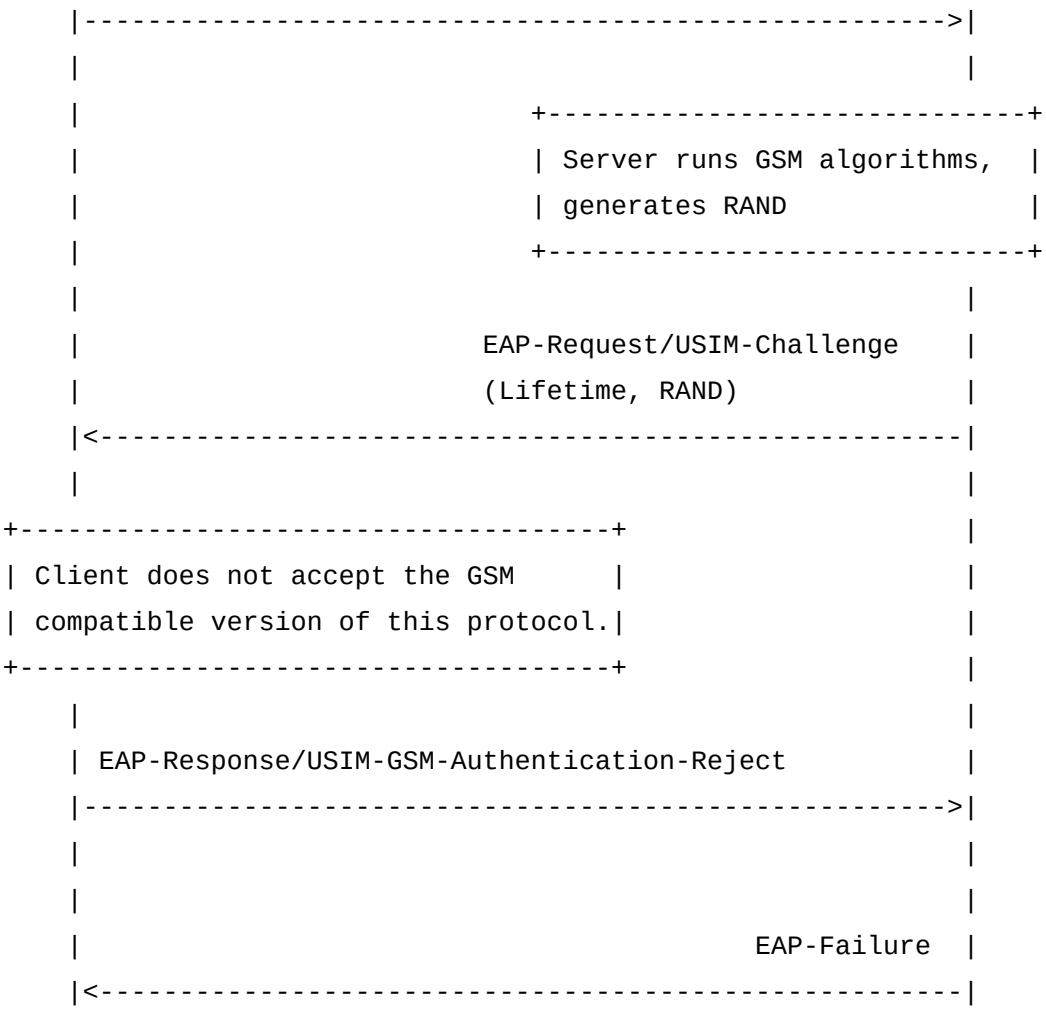


The next message flow shows the client rejecting the AUTN of the Authenticator. This flow is not used in the GSM compatible mode.

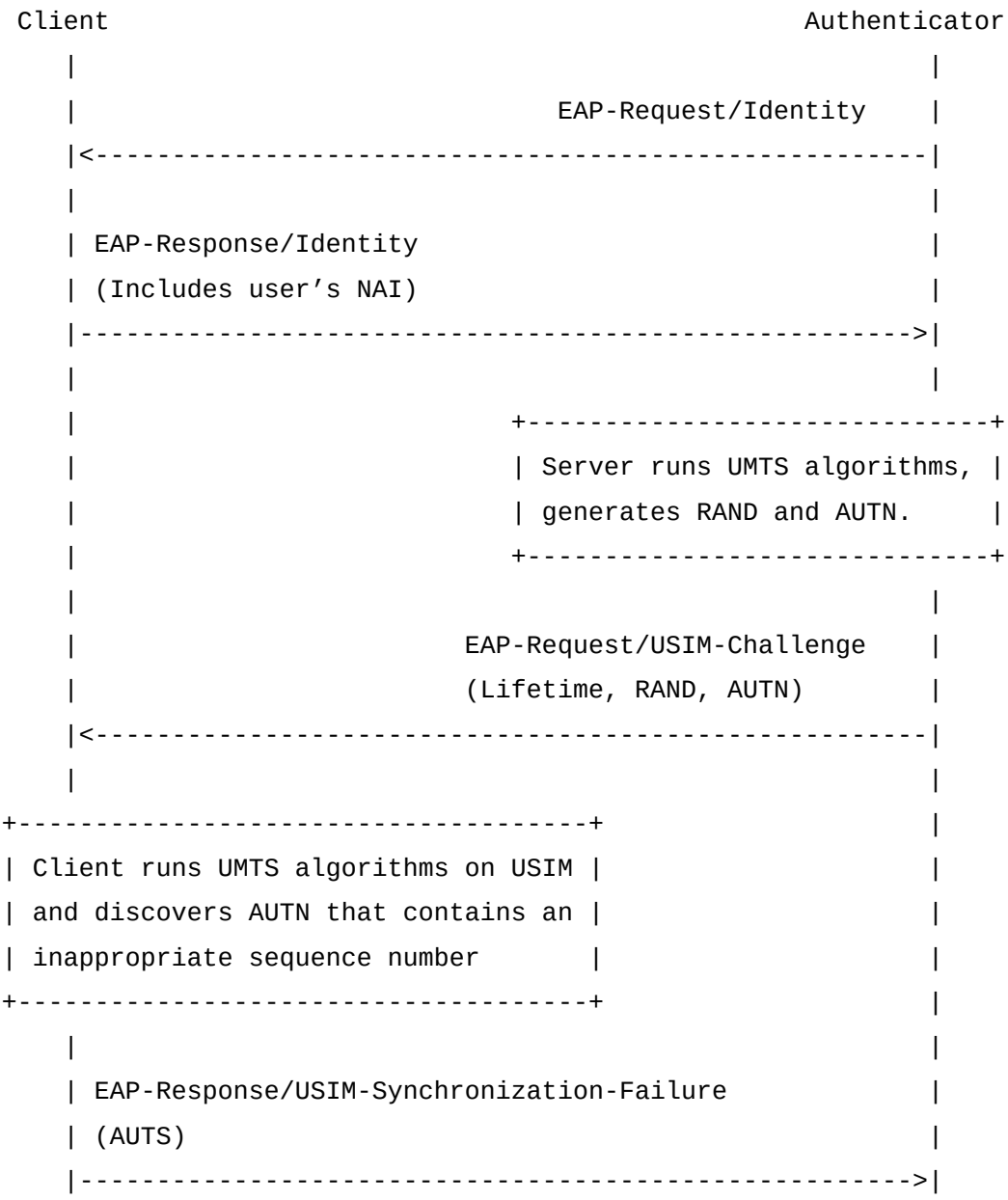

Client
Authenticator
EAP-Request/Identity
EAP-Response/Identity
(Includes user's NAI)
Server runs UMTS algorithms,
generates RAND and a bad AUTN
EAP-Request/USIM-Challenge
(Lifetime, RAND, AUTN)
Client runs UMTS algorithms on USIM
and discovers AUTN that can not be
verified
EAP-Response/USIM-Authentication-Reject

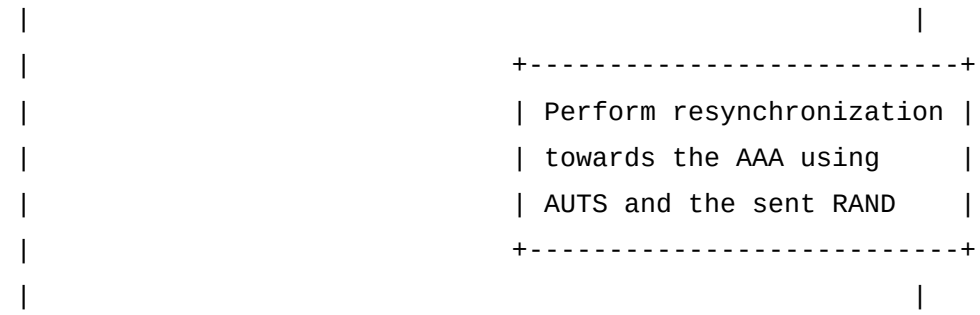
Networks that are not UMTS aware use the GSM compatible version of this protocol even for UMTS subscribers. In this case, the AUTN parameter is not included in the EAP-Request/USIM-Challenge packet. If a UMTS capable client does not want to accept the use of the GSM compatible mode, the client can reject the authentication with the EAP-Response/USIM-GSM-Authentication-Reject message, as shown in the following figure:





The AKA uses shared secrets between the Client and the Authenticator together with a sequence number to actually perform an authentication. In certain circumstances it is possible for the sequence numbers to get out of sequence. Here’s what happens then:


Client
Authenticator
EAP-Request/Identity
EAP-Response/Identity
(Includes user's NAI)
Server runs UMTS algorithms,
generates RAND and AUTN.
EAP-Request/USIM-Challenge
(Lifetime, RAND, AUTN)
Client runs UMTS algorithms on USIM
and discovers AUTN that contains an
inappropriate sequence number
EAP-Response/USIM-Synchronization-Failure
(AUTS)



After the resynchronization process takes place in the server and AAA side, the process continues by the server side sending a new EAP-Request/USIM-Challenge message.

4. Messages

4.1. EAP-Response/Identity

In the beginning of EAP authentication, the Authenticator issues the EAP-Request/Identity packet to the client. The client responds with EAP-Response/Identity, which contains the user's identity. The formats of these packets are specified in [6].

The EAP AKA mechanism uses the NAI format [5] as the identity. In order to facilitate the use of the existing cellular roaming infrastructure, the EAP AKA client transmits the user's IMSI within the NAI in the EAP Response/Identity packet. The NAI is of the format "0imsi@realm". In other words, the first character is the digit zero (ASCII 0x30), followed by the IMSI, followed by the @

character and the realm. The IMSI is an ASCII string that consists of not more than 15 decimal digits (ASCII values between 0x30 and 0x39) as specified in [9].

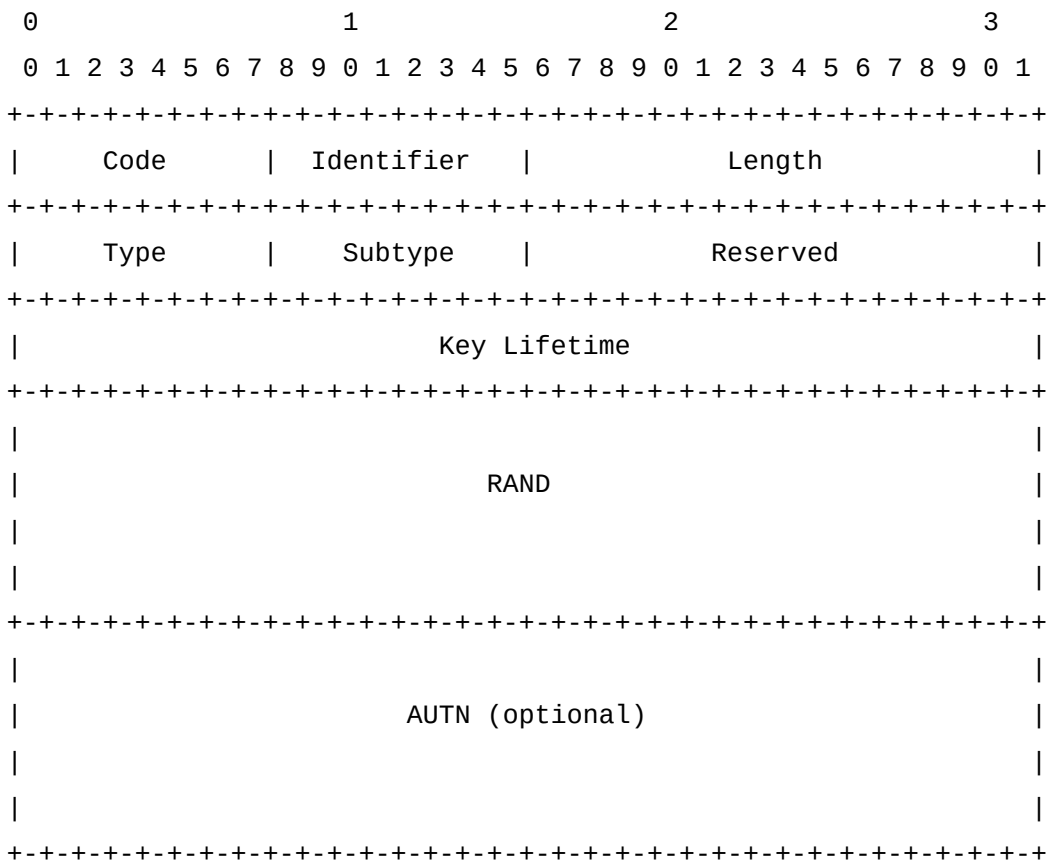
The AAA network routes AAA requests to the correct AAA server using the realm part of the NAI. Because cellular roaming can be used with EAP AKA, the AAA request can be routed to an AAA server in the

visited network instead of the server indicated in the NAI realm. The operators need to agree on this special AAA routing in advance. It is recommended that operators should reserve the realm portion of NAI used with EAP AKA to UMTS and GSM subscribers only, so that exactly the same realm is not used with other authentication methods. This convention makes it easy to recognize that the NAI identifies a UMTS or GSM subscriber of this operator, which may be useful when configuring the routing rules in the visited AAA networks.

In the EAP AKA protocol, the EAP-Request/Identity message is optional when applicable. If the client can positively determine that it has to authenticate, it MAY send an unsolicited EAP-Response/Identity to the authenticator with an Identifier value it has picked up itself. The client MUST NOT send an unsolicited EAP-Response/Identity if it has already received an EAP-Request/Identity packet. The client MUST send an EAP-Response/Identity to all received EAP-Request/Identity packets, using the Identifier value in the EAP-Request/Identity. If the authenticator receives an unsolicited EAP-Response/Identity, it SHOULD process the packet as if it had requested it. If the authenticator receives an EAP-Response/Identity with an incorrect Identifier value in response to the first EAP-Request/Identity it has sent to the client, then the authenticator SHOULD still accept the EAP-Response/Identity packet.

4.2. EAP-Request/USIM-Challenge

The format of the EAP-Request/USIM-Challenge packet is shown below.



The semantics of the fields is described below:

Code

1 for Request

Identifier

See [6]

Length

The length of the EAP Request packet.
44, if AUTN is included (UMTS AKA).
28, if AUTN is excluded (GSM compatible mode).

Type

TBD

Subtype

1 for USIM-Challenge

Reserved

Set to zero when sending, ignored on reception.

Key lifetime

This expresses how long the cipher and integrity keys may be used. This value is expressed in seconds, and the value of zero means they may be used indefinitely.

RAND

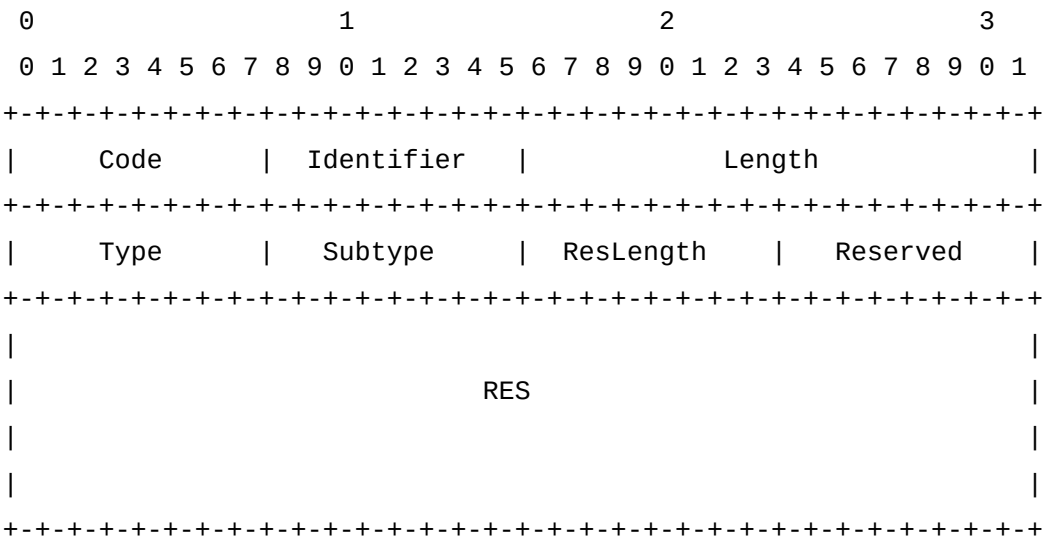
The AKA RAND parameter, 16 bytes (128 bits).

AUTN

The AKA AUTN parameter, 16 bytes (128 bits).

4.3. EAP-Response/USIM-Challenge

The format of the EAP-Response/USIM-Challenge packet is shown below.



The semantics of the fields is described below:

Code

2 for Response

Identifier

See [6]

Length

The length of the EAP Response packet, 12..40.

Type

TBD

Subtype

1 for USIM-Challenge

ResLength

This is the length of the RES parameter in bits. According to the specification [10] this parameter can vary between 32 and 128 bits. In the GSM compatible mode, the RES field contains the GSM SRES parameter which is always 32 bits long.

Reserved

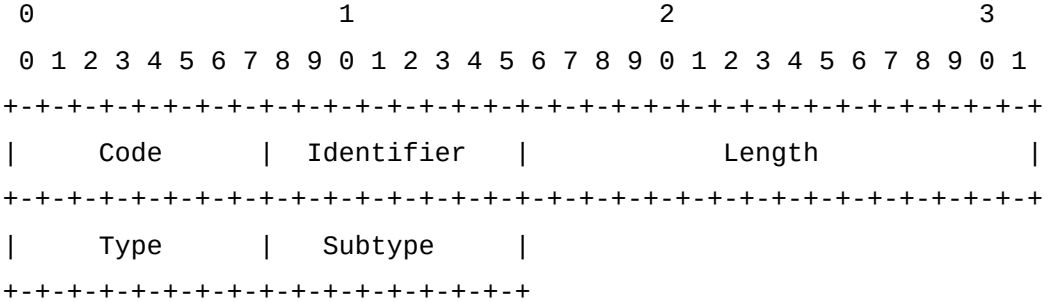
Set to zero when sending, ignored on reception.

RES

The AKA RES parameter, 32..128 bits. The Length parameter specifies the total length of the payload and identifies ~~the~~ at the same time indirectly also the size of the RES in bytes. The ResLength field identifies the exact length in bits. The sender may pad the RES with zero bits and bytes where necessary. In the GSM compatible mode, the RES field contains the GSM SRES parameter.

4.4. EAP-Response/USIM-Authentication-Reject

The format of the EAP-Response/USIM-Authentication-Reject packet is shown below.



The semantics of the fields is described below:

Code

2 for Response

Identifier

See [6]

Length

The length of the EAP Response packet, 12.

Type

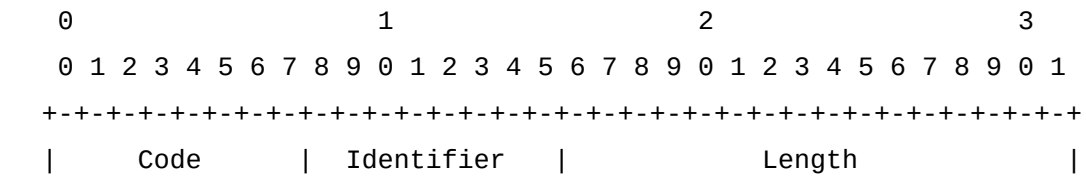
TBD

Subtype

2 for USIM-Authentication-Reject

4.5. EAP-Response/USIM-GSM-Authentication-Reject

The format of the EAP-Response/USIM-GSM-Authentication-Reject packet is shown below.



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |   Subtype     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The semantics of the fields is described below:

Code

2 for Response

Identifier

See [6]

Length

The length of the EAP Response packet, 6.

Type

TBD

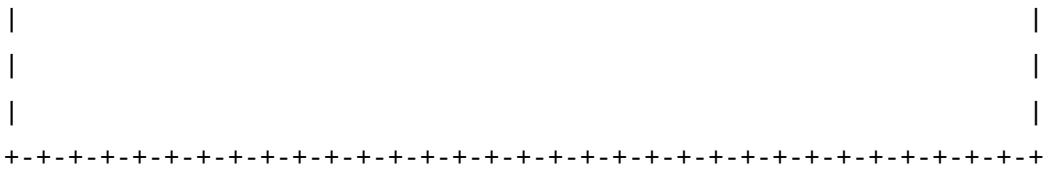
Subtype

3 for USIM-GSM-Authentication-Reject

4.6. EAP-Response/USIM-Synchronization-Failure

The format of the EAP-Response/USIM-Synchronization-Failure packet is shown below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |   Subtype     |             AUTS              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
```



The semantics of the fields is described below:

Code

2 for Response

Identifier

See [6]

Length

The length of the EAP Response packet, 20.

Type

TBD

Subtype

4 for USIM-Synchronization-Failure

AUTS

The AKA AUTS parameter, 112 bits (14 bytes).

5. Interoperability with GSM

The EAP AKA protocol is able to authenticate both UMTS and GSM users, if the subscriber's operator's network is UMTS aware. This is because the home network will be able to determine from the subscriber records whether the subscriber is equipped with a UMTS USIM or a GSM SIM. A UMTS aware home network will hence always use UMTS AKA with UMTS subscribers and GSM authentication with GSM subscribers. With GSM subscribers, the EAP AKA protocol is always used in the GSM compatible mode.

It is not possible to use a GSM AuC to authenticate UMTS subscribers. (Note that if the home network doesn't support an authentication method it should not distribute SIMs for that method.)

However, it is possible that the node actually terminating EAP and the node that stores the authentication keys (AuC) are separate, and support different authentication types. If the node terminating EAP is GSM-only but AuC is UMTS-aware, then authentication can still be achieved using the GSM compatible version of EAP AKA. This authentication will be weaker, since the GSM compatible mode does not provide for mutual authentication. Section 6.8.1.1 in [1] specifies how the GSM SRES parameter and the Kc key can be calculated on the USIM and the AuC. If a UMTS terminal does not want to accept the GSM compatible version of this protocol, then it can reject the authentication with the EAP-Response/USIM-GSM-Authentication-Reject packet.

In conclusion, the following table shows which variant of the EAP AKA protocol should be run under different conditions:

SIM	EAP node	AuC	EAP AKA mode
GSM	(any)	(any)	GSM
UMTS	(any)	GSM	(illegal)

UMTS	GSM	GSM+UMTS	GSM
UMTS	GSM+UMTS	GSM+UMTS	UMTS

6. IANA Considerations

IANA has assigned the number TBD for EAP AKA authentication.

7. Security Considerations

Implementations running the EAP AKA protocol will rely on the security of the AKA scheme, and the secrecy of the symmetric keys stored in the USIM and the AuC.

8. Intellectual Property Right Notices

On IPR related issues, Nokia and Ericsson refer to the their respective statements on patent licensing. Please see http://www.ietf.org/ietf/IPR/NOKIA and http://www.ietf.org/ietf/IPR/ERICSSON-General

Acknowledgements

The authors wish to thank Rolf Blom of Ericsson, Bernard Aboba of Microsoft and Arne Norefors of Ericsson for interesting discussions in this problem space.

Authors' Addresses

Jari Arkko
Ericsson
02420 Jorvas
Finland
Phone: +358 40 5079256
Email: jari.arkko@ericsson.com

Henry Haverinen
Nokia Mobile Phones
P.O. Box 88
33721 Tampere
Finland
Phone: +358 50 594 4899
E-mail: henry.haverinen@nokia.com

References

[1] 3GPP Technical Specification 3GPP TS 33.102 V3.6.0: "Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 1999)", 3rd Generation Partnership Project, November 2000.

[2] GSM Technical Specification GSM 03.20 (ETS 300 534): "Digital cellular telecommunication system (Phase 2); Security related network functions", European Telecommunications Standards, Institute, August 1997.

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

[4] IEEE Draft 802.11eS/D1, "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", March 2001

[5] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

[6] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[8] S. Bradner, "Key words for use in RFCs to indicate Requirement Levels", RFC 2119, March 1997.

[9] GSM Technical Specification GSM 03.03 (ETS 300 523): "Digital

cellular telecommunication system (Phase 2); Numbering, addressing and identification", European Telecommunications Standards Institute, April 1997.

[10] 3GPP Technical Specification 3GPP TS 33.105 V3.5.0: "Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements (Release 1999)", 3rdGeneration Partnership Project, October 2000