3GPP TSG WG3 S3#18
Phoenix, Arizona
23rd May – 27th May, 2001

Tdoc S3-0100200

Agenda Item: 9.3

Source: Ericsson

Title: Proposal to use a generic authentication scheme for SIP

Document for: Discussion

1 Scope and objectives

The scope for this document is to provide a concrete proposal on how the either the generic Extensible Authentication Protocol (EAP) framework or the Simple Authentication and Security Layer (SASL) can be used for SIP authentication.

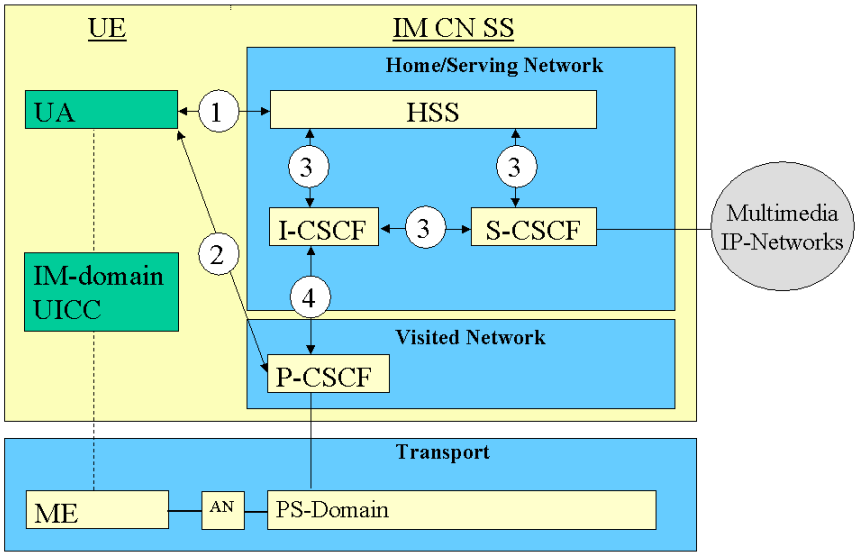
We will cover protocol details for the use of both mechanisms, and then compare them to each other and to the current working assumption which is the direct use of AKA in SIP. We conclude that the use of a generic framework will make the IP multimedia system more access-independent without additional overhead. Both EAP and SASL appear to be good candidates for the generic framework, though in terms of standardization EAP is slightly further along and has better support of AKA and DIAMETER.

In this document the following is proposed

1 The use of EAP AKA in SIP
2 The use of Diameter EAP extensions to handle EAP authentication in an access-independent way in proxies

2 Background

The Home Network performs the authentication of the IM Subscriber. The signalling protection i.e. integrity should be provided in a hop-by-hop fashion and there should be security association between the UE and the P-CSCF.



The protocol used between the UE and the P-CSCF is SIP, Session Initiation Protocol. A working assumption in SA3 has been that AKA defined in R'99 shall be reused. However, currently within IETF SIP AKA has not been defined. In SA3 #14 Nokia presented a proposal [S3-000456] on how AKA could fit into the SIP protocol by extending the protocol. That is also the current working assumption.

In order to standardize the current working assumption, it will be necessary to specify in both in IETF and 3GPP the following issues:

- Required headers for carrying AKA.
- Additional headers for carrying the keys between the home and the visited networks.
- Mechanisms to retrieve the authentication parameters to the proxy from the S-CSCF e.g. through DIAMETER.

This work has to be repeated every time modifications are made to the authentication scheme or new schemes are taken into use.

An Ericsson contribution to the Madrid stated that it would be beneficial to use a more generic authentication framework for the following reasons:

- The used protocols and protocol extensions (e.g. to SIP) could be used unchanged on other access types, promoting access independence.
- All proxy equipment can be implemented without knowledge of the details of the authentication schemes.
- Existing AAA transport attributes can be reused directly, without having to standardize special ones for UMTS.
- More general purpose extensions can be proposed to the IETF

There are several existing general authentication frameworks, the most well known being GSS_API, SASL, and EAP. An obvious question is which framework should be selected. In this contribution we have chosen to study only the EAP and SASL alternatives since GSS_API is currently not compatible with the SIP proxy or the AAA model, and its complexity exceeds that of SASL and EAP.

3 EAP SIP Extension

3.1 Introduction

EAP consists of binary request and response packets sent between the user and the home environment. Nodes passing these packets need not understand the format of the packets. The main idea in the proposed use of EAP within the IP multimedia system involves the definition of a new method for the WWW-Authenticate and Authorization fields in SIP, to provide an "eap" type in addition to the standard "pgp" type. The 3G SIP proxies and servers can then send the authentication protocol piggybacked in SIP, and can also use backend AAA protocols such as DIAMETER for fetching information from the HSS or making the authentication in the HSS.

Compared to SASL, EAP is in wider use and does not require the use of SSL/TSL in conjunction with it. There are no existing AAA extensions for SASL. There is existing work that provides both GSM and UMTS authentication within it [EAPGSM. EAPAKA]. We also note that EAP is being adopted as the basis in WLAN authentication through 802.1X, which may make it easier later to provide WLAN-UMTS interworking. One thing that is missing from EAP is the ability to negotiate the authentication mechanism. However, in the area of IM domain applications, we see it as natural that the server demands a particular authentication mechanism from a particular client. Therefore the negotiation mechanism isn't needed. At the same time, the lack of a negotiation mechanism in EAP makes its use secure against 'bidding-down' attacks.

3.2 How to use EAP within SIP

We will propose an optimized registration procedure that minimizes the number of necessary roundtrips. First, the user will send a SIP Register request to the P-CSCF and includes its identity.

REGISTER sip:… **SIP/2.0**

Authorization: **eap** *base64_eap_identity_response*

…

(It is for further study whether the EAP-Identity response is necessary here, or if the proxy could simply create one from the SIP identities.) Next, the network will determine the right home server, and ask it to provide a set of authentication vectors. The network will send the response to the user with the first EAP AKA challenge packet in the form of the SIP "407 Proxy Authentication Required" response. In the example below, we have used the AKA version of EAP, but it would be possible for the home to require also other types of authentication.

SIP/2.0 407 Proxy Authentication Required

WWW-Authenticate: **eap** *base64_eap_aka_challenge_request*

…

As a part of the EAP AKA challenge request, the user will receive AUTN and RAND, the parameters it needs to run AKA. USIM is now able to check AUTN for validity, and produce RES to authenticate itself. User will send a new register message to send the RES and complete authentication:

REGISTER sip:… **SIP/2.0**

Authorization: **eap** *base64_eap_aka_challenge_response*

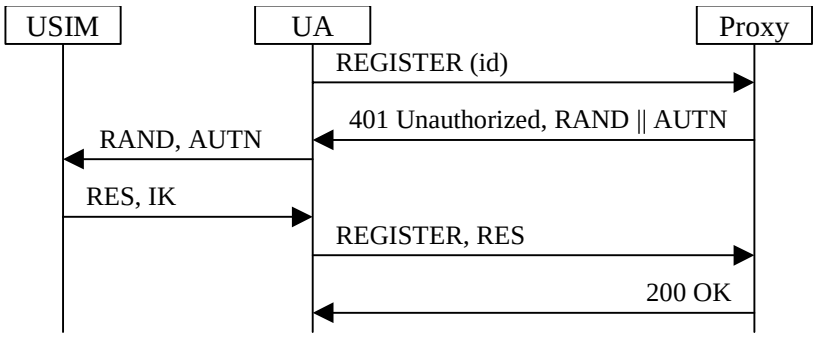
…

This completes the authentication from the user's perspective; he also now has the derived integrity key. The network still has to respond and indicate that it liked the user's result:

SIP/2.0 200 OK

WWW-Authenticate: **eap** *base64_eap_aka_success*

…



3.3 DIAMETER Extensions

The 3G SIP proxies or servers can use existing backend AAA protocols and servers for communicating authentication-related information with the HSS (see [RADIUS] and [DIAMACC]. Presently, the 3GPP is designing 3GPP-specific extension to the DIAMETER protocol to carry authentication information from home proxies to the HSS and back. These involve both new messages and new data attributes, to carry the AKA parameters. However, if existing general-purpose authentication frameworks such as EAP are used, it becomes possible to reuse existing AAA protocols in a greater extent. For instance, [DIAMACC] defines messages and

data attributes necessary to carry EAP. These can be directly reused, or if 3GPP extensions are required for other purposes, then at least the data attributes can be reused.

For DIAMETER, the following existing data attributes can be used:

- The EAP-Payload AVP can be used to carry all EAP requests between a SIP proxy and an authentication center. Typically, the first EAP message from the client contains an unsolicited EAP-Identity-Response. The second message typically contains the EAP/USIM-Challenge-Request, and the third the response to that. The final message in the SIP OK message contains the EAP-Success message.

- The NAS-Session-Key AVP (currently being discussed by the IETF AAA WG for addition to the DIAMETER protocol) can be used to carry the IK to the proxy.

The data attributes must be carried in some DIAMETER message, which could be either 3GPP specific, or one of the existing messages specifically designed for use with EAP:

- The DIAMETER message DIAMETER-EAP-REQUEST (DER) may be used to send the EAP-Payload that has been sent from the user's direction.

- The DIAMETER message DIAMETER-EAP-INDICIATION (DEI) may be used to send the normal EAP-Payload that has been sent to the user's direction.

- The DIAMETER message DIAMETER-EAP-ANSWER (DEA) may be used to send the EAP-Success or EAP-Failure payloads to the user's direction.

Of course, it isn't required to use these existing mechanisms, but the possibility at least exists. Further specification of the exact DIAMETER flows awaits the decisions regarding the placement of the authentication either to HSS or S-CSCF. Also, as of now we do not have knowledge of the kinds of inter-working scenarios UMTS-based and other types (WLAN, general Internet, …) networks will have and therefore it is hard to show exactly how the use of IETF-based standard schemes will help in them. But it seems likely though that a network design based on those schemes will be easier to evolve in these scenarios.

3.4 Effects to UMTS and IETF Standardization

In order to make this possible, the following standardization has to take place:

- SA3 has to decide to adopt this, and place the message flows to its technical specifications (but not the protocol details).

- A new value under WWW-Authentication and Authorization fields must be registered to IANA/IETF. The exact requirements on what is needed to do this are ffs, but probably include the publication of an Informational RFC.

- EAP AKA must proceed to an (Informational) RFC. (This is work in progress already, does not have to be initiated by SA3.)

Note that the second step needs to be performed regardless of what approach is chosen. There are also some additional things that need to be taken care of in any case. These include adding a mechanism to SIP to pass the IK and other data between proxies.

4 SASL SIP Extension

4.1 Introduction

The Simple Authentication and Security Layer Protocol (SASL [RFC2222]) defines a mechanism for using a variety of authentication mechanisms in any protocol supporting SASL. The main idea in the proposed use of SASL within the IP multimedia system involves the definition of a new method for the WWW-Authenticate and Authorisation fields in SIP, to provide an "SASL" type in addition to the standard "pgp" type. The 3G SIP proxies and servers can then send the authentication protocol piggybacked in SIP.

The things that point against EAP are that it is a binary protocol and that there is no description of how to use it in conjunction with http authentication. SASL describes an authentication framework for text based protocols. Work is ongoing in IETF to specify how it shall be used for http authentication

One problem with SASL is the ability to negotiate the authentication mechanism which opens up for a man in the middle attack. This can be solved by: having a underlying security protocol such as TLS, only using strong authentication schemes or by having either the server or the client demanding a particular authentication scheme. For the IM domain we see it as natural that the server demands a particular authentication mechanism from a particular client. Therefore the negotiation mechanism isn't needed and the man in the middle attack is prevented.

Two additional shortcomings with SASL is that there is currently no SASL extension for HTTP[1] and that there are no AAA extensions for SASL

4.2 How to use SASL within SIP

We will propose an optimised registration procedure that minimises the number of necessary roundtrips. First, the user will send a SIP Register request to the P-CSCF.

REGISTER sip:… **SIP/2.0**

…

It is for further study whether identity information is necessary here, or if the proxy could simply create it from the SIP identity. Next, the network will determine the right home server, and ask it to provide a set of authentication vectors. The network will send the response to the user with the first SASL AKA challenge packet in the form of the SIP "401 Unauthorized" response. Here we could have used other SASL mechanisms as well had it not been the UMTS server on the other end.

SIP/2.0 401 Unauthorized

WWW-Authenticate: **SASL** mechanism = 3GPP-AKA id = SESSION ID value= RAND|AUTN

…

The WWW-Authenticate response above contains either a sasl-challenge. The sasl-challenge is used when the server has only one sasl mechanism and it has the following structure:

```
sasl-challenge = sasl-intro sasl-mechanism sasl-sid #sasl-challenge-value
sasl-intro = "SASL" "realm" "=" realm-value
sasl-mechanism = "mechanism" "=" token
sasl-sid = "id" "=" 8*octet
sasl-challenge-value = "value" "=" token
```

The B64 format shall be used for the AUTN and RAND value.

Having received AUTN and RAND, the parameters it needs to run AKA, the client is now able check AUTN for validity, and produce RES to authenticate itself. It will send a new register message to send the RES and complete authentication:

REGISTER sip:… **SIP/2.0**

Authorisation: **SASL** mechanism =3GPP-AKA id = SESSION ID value = RES | AUTS | AUTH-REJECT.

…

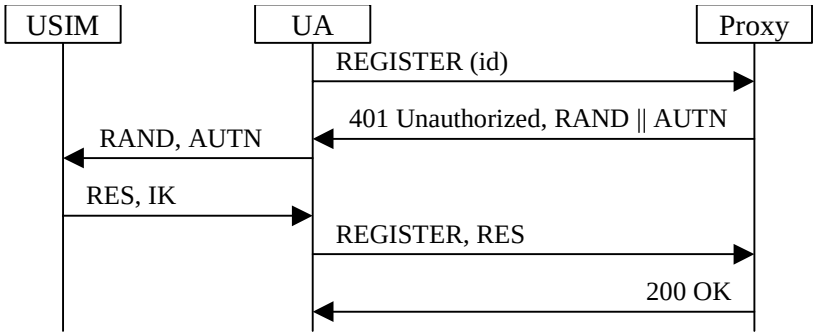
The B64 format shall be used for the RES and AUTS value. The possible value of the error-code (AUTH-REJECT) is FFS. The authorization header we just described contains a sasl-cridential. The structure of the sasl-cridential is as follows:

```
sasl-credential = sasl-intro sasl-mechanism sasl-sid #sasl-challenge-value
sasl-intro = "SASL" "realm" "=" realm-value
```

---

[1] Two competing drafts are available

```
sasl-mechanism = "mechanism" "=" token
sasl-sid = "id" "=" 8*octet
sasl-challenge-value = "value" "=" token
```



4.4 Effects to UMTS and IETF Standardisation

In order to make this possible, the following standardisation has to take place:

- SA3 has to decide to adopt this, and place the message flows to its technical specifications (but not the protocol details).
- SASL in http must proceed to an RFC. (This work is already in progress, though with two competing approaches.)
- The SASL mechanism 3GPP-AKA must be specified and registered with IANA.
- AAA extensions for SASL must be defined.

3 Evaluation

In this section we will discuss the pros and cons of the three alternatives:

- Continue with the current working assumption of direct SIP AKA support
- Adopt EAP as a generic authentication scheme in SIP
- Adopt SASL as a generic authentication scheme in SIP

We are interested in the following effects:

- Is the protocol extensible to new authentication schemes?
- Do the proxies and P-CSCF in particular have to know about the authentication scheme?
- What is the overhead of the alternative? The SIP AKA is used as a baseline for this comparison.
- What standardization must take place for SIP to use the alternative?
- Is there DIAMETER support that could perhaps be reused?

The following table shows our evaluation results:

Criteria	SIP AKA	SIP EAP	SIP SASL
Extensible to new authentication schemes?	Not SIP AKA itself, but SIP authentication is extensible. However, this extensibility is tied to the SIP protocol. This means that every time new authentication schemes are needed, SIP needs to be extended. In contrrast in the generic frameworks neither the SIP protocol specifications nor the proxies need to be modified and new authentication schemes developed for other purposes will be readily available without additional work. See also below.	Yes, multiple schemes already exist and continue to be developed.	Yes, multiple schemes already exist and continue to be developed.
Proxies have to be modified for new schemes?	As long as the authentication requests stay within SIP no, but since the authentication schemes are SIP specific, SIP can't hand them off to authentication frameworks without knowing what the schemes are.	No. SIP implementations in clients, proxies, and servers can all be programmed without specific knowledge of authentication. Generic authentication frameworks and libraries can be handed the authentication task. This 'handing-off' can happen either internally within a node or towards a network.	No. SIP implementations in clients, proxies, and servers can all be programmed without specific knowledge of authentication. Generic authentication frameworks and libraries can be handed the authentication task. This 'handing-off' can happen either internally within a node or towards a network.
Overhead?	This is the baseline against which we compare. Two roundtrips are needed, and each message needs an additional SIP header that includes the AKA parameters in base64 format, plus an indication that the method used is AKA.	An equal number of roundtrips is needed. The EAP packet consist of an 8 byte header followed by the AKA parameters themselves. The additional overhead of the header in base64 format is then 10 bytes.	An equal number of roundtrips is needed. In addition to the SIP AKA overhead, each message carries the text "mechanism = 3GPP-AKA id = SESSION ID". We can assume this is perhaps 20 bytes.
SIP standardization?	Have to define a new SIP/HTTP authentication method, which hasn't been started yet.	Have to define AKA in EAP (work already in progress). Have to define the EAP SIP/HTTP authentication method, which hasn't been started yet.	Have to define AKA in SASL, which hasn't been started yet. Also have to define the SASL SIP/HTTP authentication method. The latter work is already in progress, though with competing drafts.
Can reuse DIAMETER extensions?	No, have to be defined.	Yes	No, have to be defined.

3 Conclusions

We conclude that the use of a generic framework will make the IP multimedia system more access-independent without additional overhead. Both EAP and SASL appear to be good candidates for the generic framework, though in terms of standardization EAP is slightly further along and has better support of AKA and DIAMETER. In all alternatives including the SIP AKA alternative it is necessary to perform some standardization activities in the IETF.

References

[S3-000456] 3GPP TSG SA WG3 Security: Source Nokia; *UMTS AKA in SIP;* July 2000.

[RFC 2284] IETF RFC 2284: *Extensible Authentication Protocol (EAP);* March, 1998.

[S3-010100] 3GPP TSG SA WG3 Security, S3-010100: *Proposal on IM domain access security;* SA WG3 #17, Göteborg, 27 Feb – 2 March 2001

[DIAMACC] DIAMETER NASREQ Extension. IETF, May 2001.

[EAPGSM] H. Haverinen. EAP SIM Authentication (Version 1). IETF, April 2001.

[EAPAKA] J. Arkko, H. Haverinen. EAP AKA Authentication. IETF, May 2001.

[RADIUS] IETF RFC 2869. RADIUS Extensions. IETF, June 2000.

[RFC 2222] IETF RFC 2222: Simple Authentication and Security Layer (SASL)

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

EAP AKA Authentication May 2001

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.

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.

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]

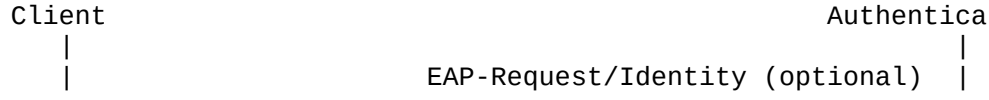
3. Protocol Overview

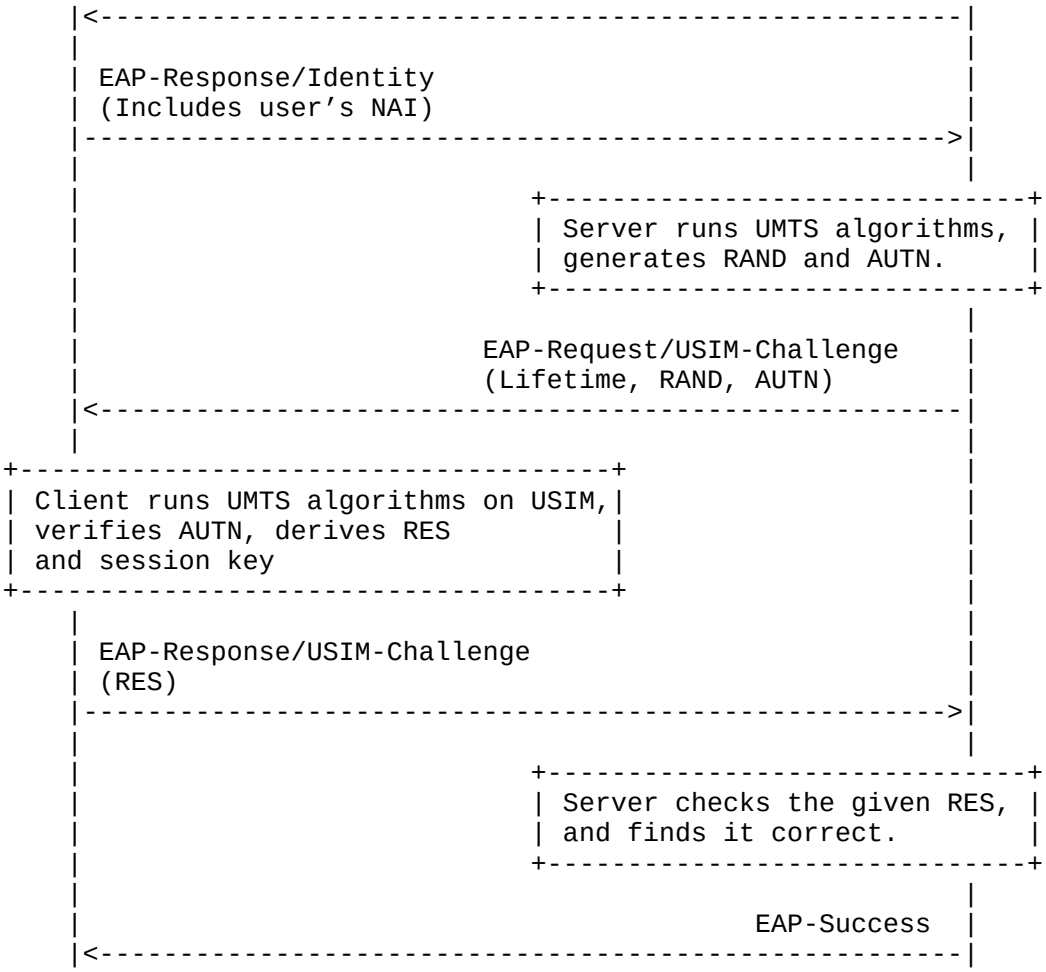
The EAP AKA uses two roundtrips to authorize the user and generate session keys. The authenticator typically communicates with the

user's AAA server using an AAA protocol. (The exact AAA communications 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.

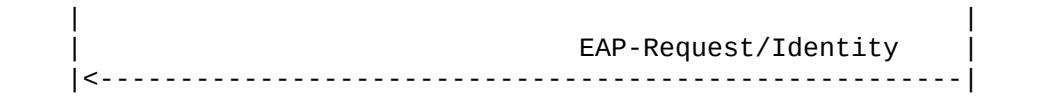


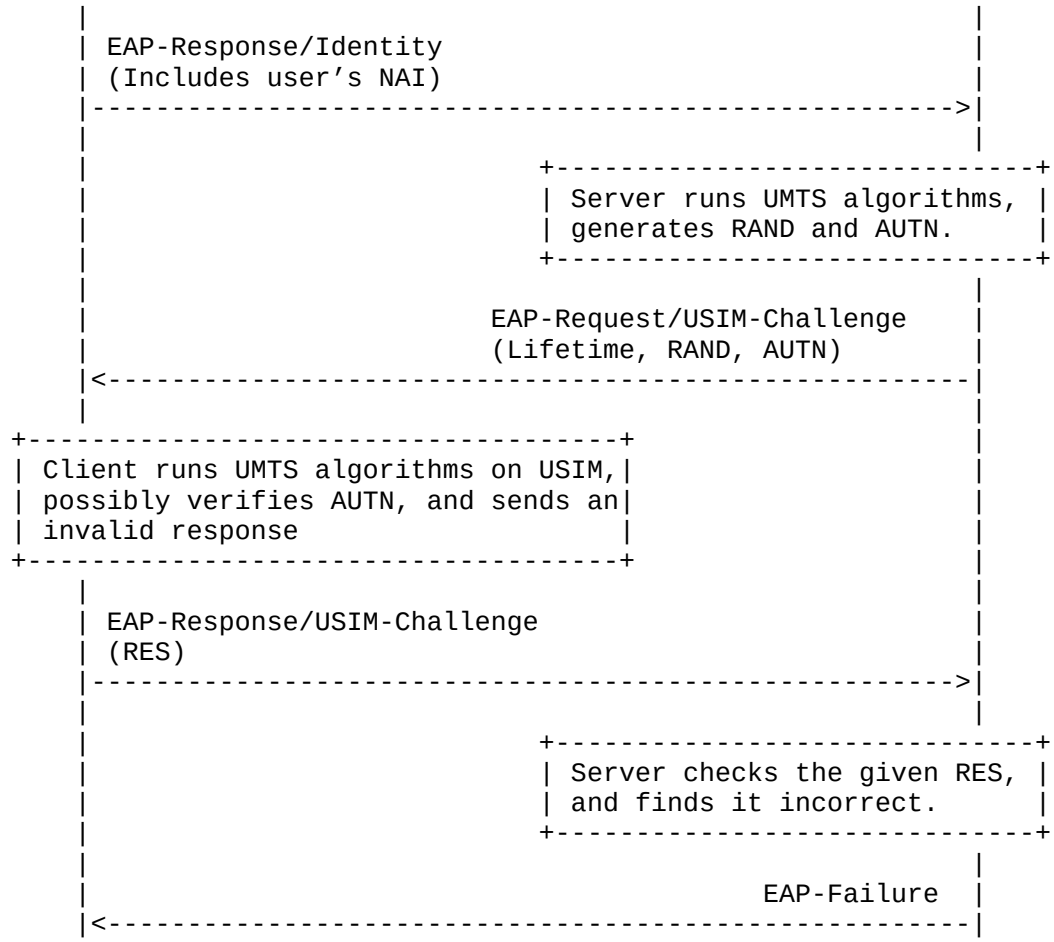


When EAP AKA is run in the GSM compatible mode, the message flow is otherwise identical to the message flow below except that the AUTN parameter is not included in EAP-Request/USIM-Challenge packet.

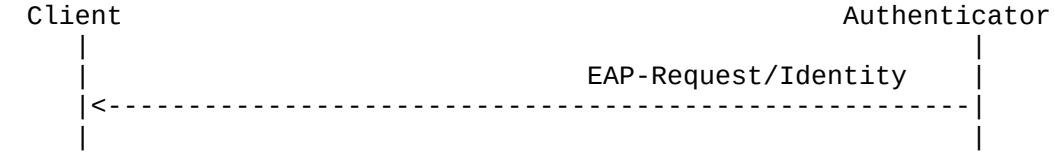
An optional lifetime may be associated to the challenge message. This specifies the server side's limit on how long the ciphering and integrity keys generated as a part of the authentication process can be used. (The use of such keys is outside the scope of this document.)

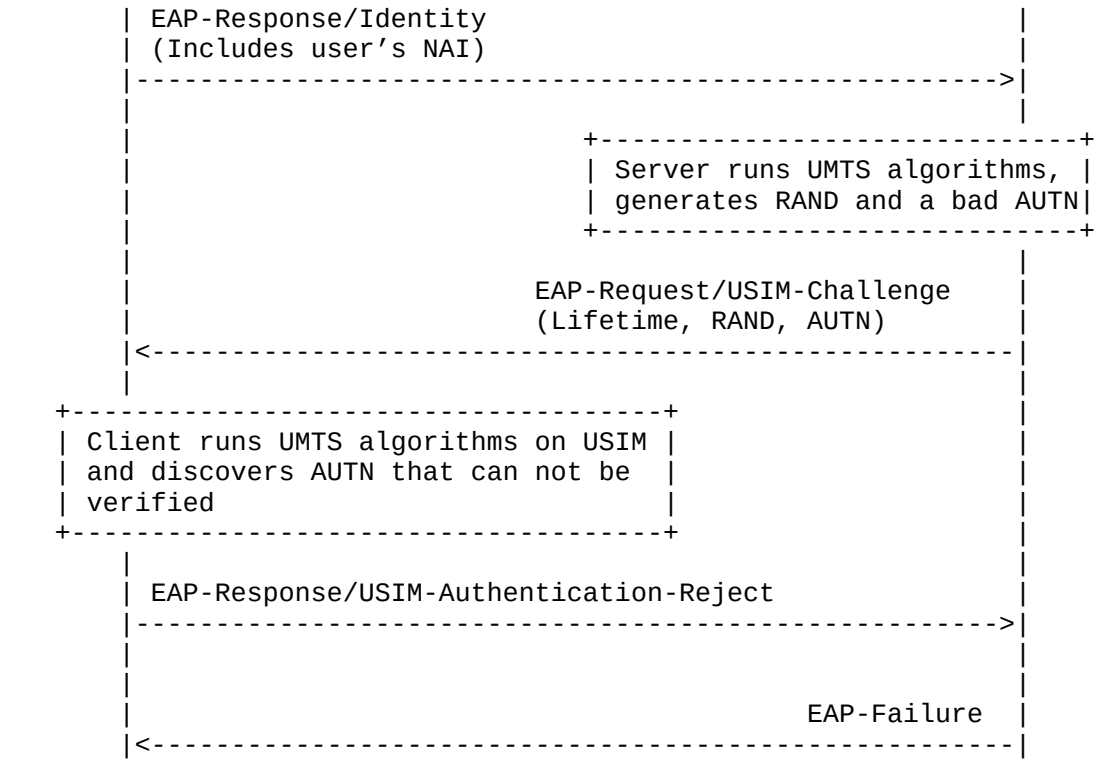
The second message flow shows how the Authenticator rejects the Client due to failed authentication. The same flow is also used in the GSM compatible mode, except that the AUTN parameter is not included in the EAP-Request/USIM-Challenge packet.



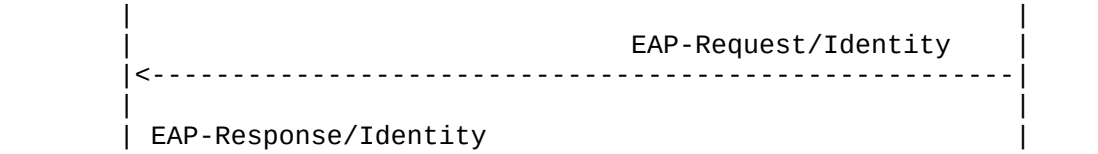


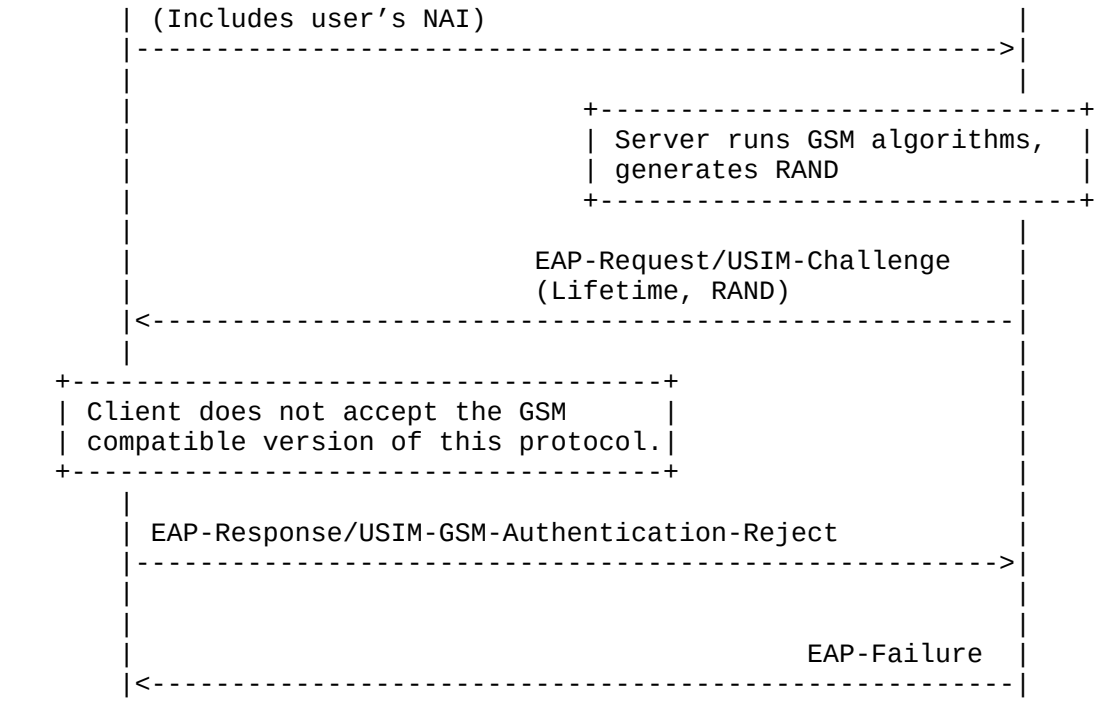
The next message flow shows the client rejecting the AUTN of the Authenticator. This flow is not used in the GSM compatible mode.



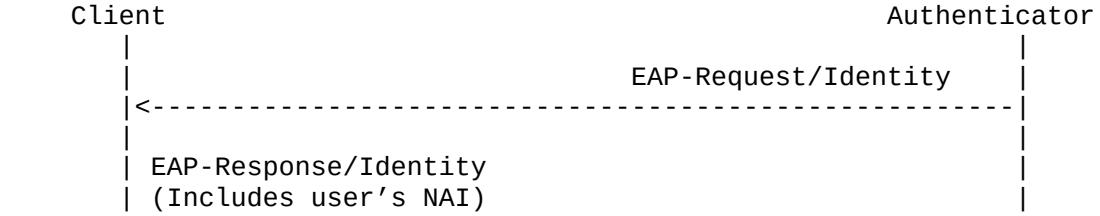


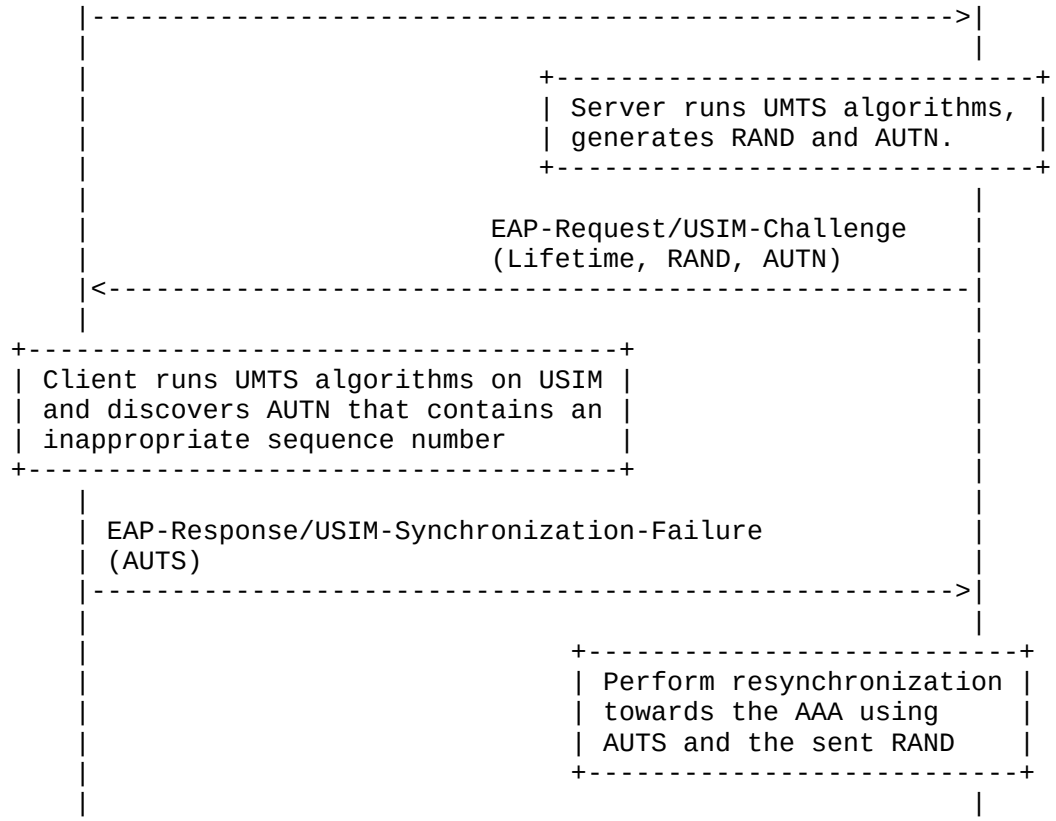
Networks that are not UMTS aware use the GSM compatible version of this protocol even for UMTS subscribers. In this case, the AUTN parameter is not included in the EAP-Request/USIM-Challenge packet. If a UMTS capable client does not want to accept the use of the GSM compatible mode, the client can reject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





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].

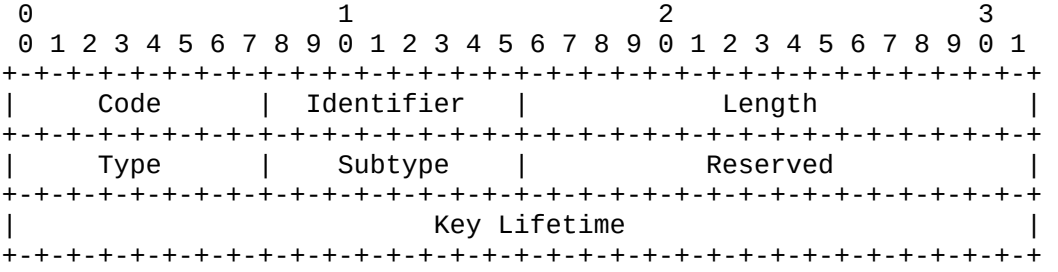
The AAA network routes AAA requests to the correct AAA server using the realm part of the NAI. Because cellular roaming can be used with EAP AKA, the AAA request can be routed to an AAA server in the visited network instead of the server indicated in the NAI realm.

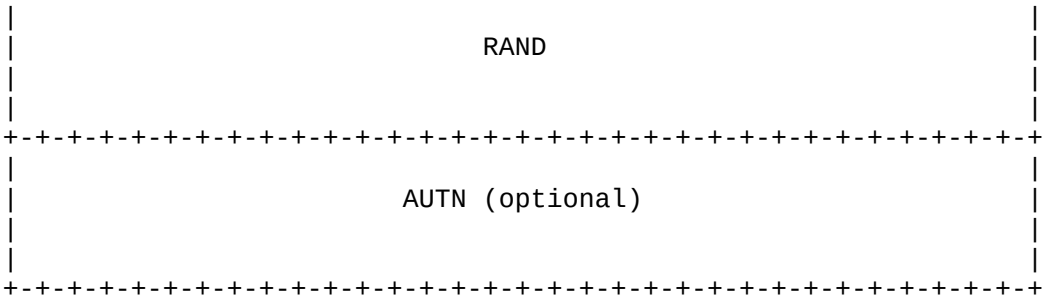
The operators need to agree on this special AAA routing in advance. It is recommended that operators should reserve the realm portion of NAI used with EAP AKA to UMTS and GSM subscribers only, so that exactly the same realm is not used with other authentication methods. This convention makes it easy 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

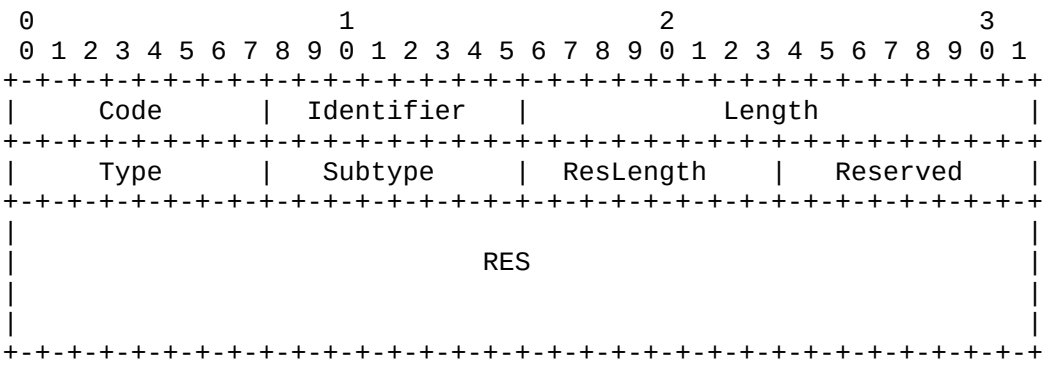
The AKA RAND parameter, 16 bytes (128 bits).

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.

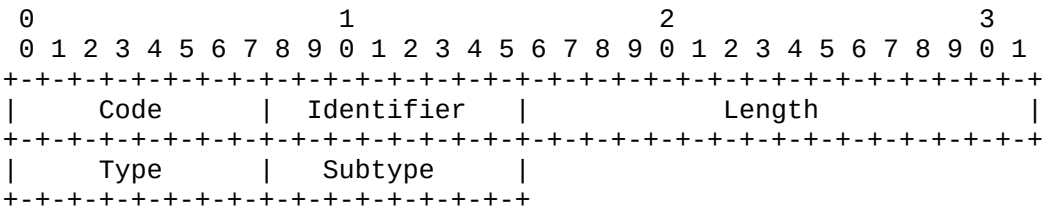
RES

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

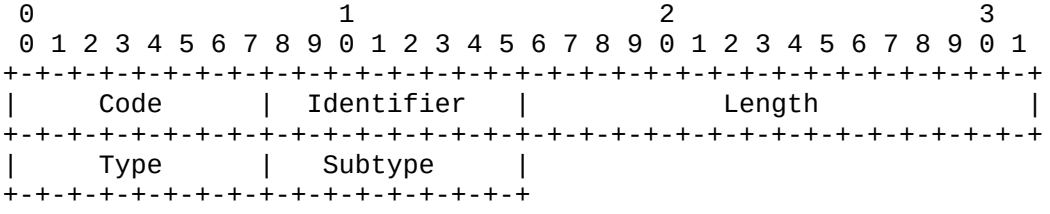
TBD

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.



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

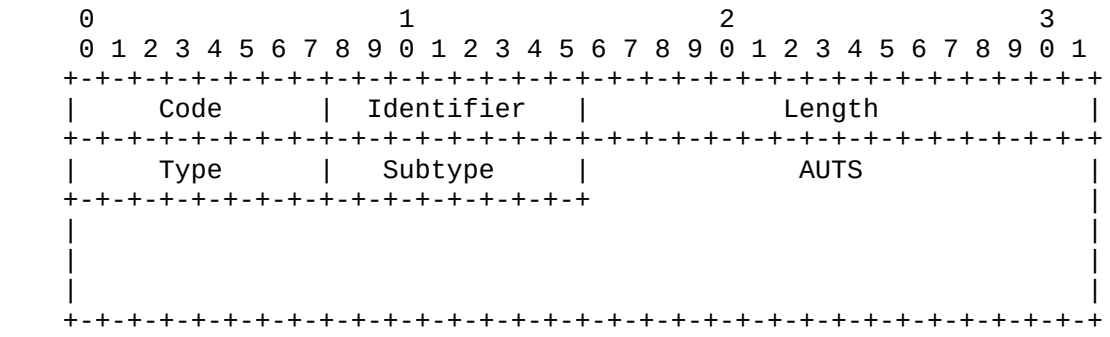
TBD

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.



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