3GPP TSG WG3 S3#18 Tdoc S3-0100263
Phoenix, Arizona
21st May – 24th May, 2001

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.

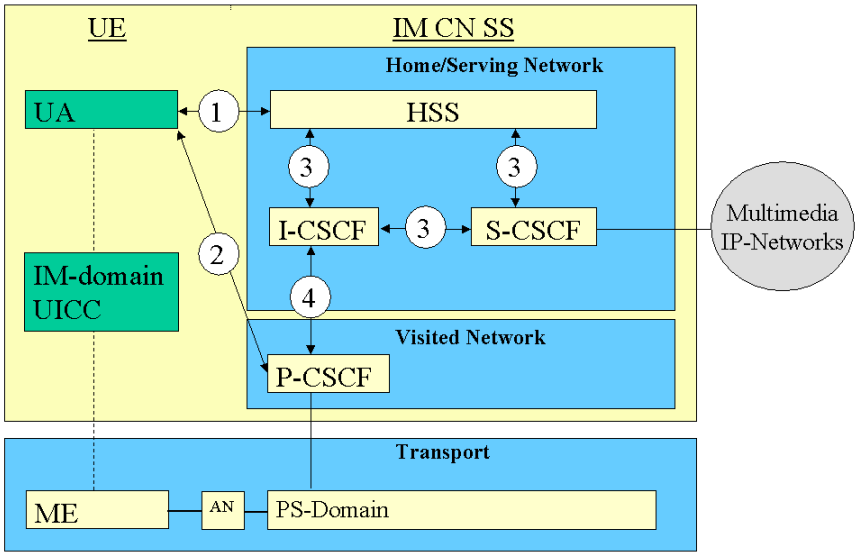
We will cover protocol details for the use of both mechanisms, and then compare them to each other and to the current working assumption which is the direct use of AKA in SIP. We conclude that the use of a generic framework will make the IP multimedia system more access-independent without additional 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~~I-CSCF/S-CSCF

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~~ S-CSCF from the HSS~~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~~nodes 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~~to the S-CSCF.

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~~ P-CSCF 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.

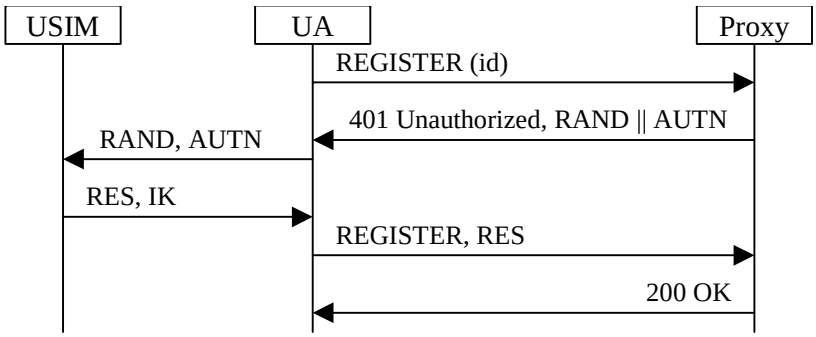
SIP/2.0 407 Proxy Authentication Required
WWW-Authenticate: **eap** *base64_eap_aka_challenge_request*
…

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~~I-CSCF and S-CSCF 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~~S-CSCF 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~~S-CSCF 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~~S-CSCF.

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~~P-CSCF and the I-CSCF, for instance.

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~~nodes 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~~ P-CSCF 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.

…

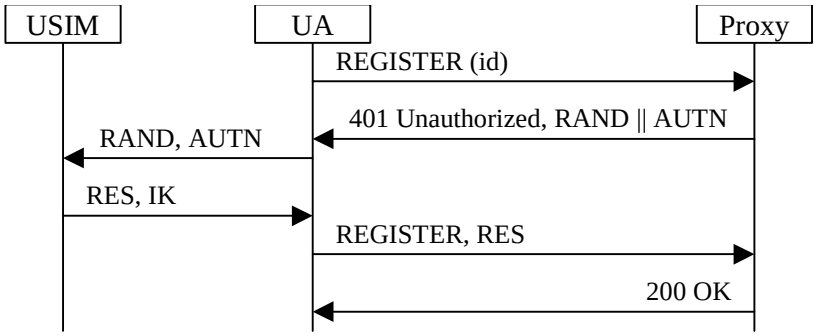
The B64 format shall be used for the RES and AUTS value. The possible value of the error-code (AUTH-REJECT) is FFS. The authorization header we just described contains a sasl-cridential. The structure of the sasl-cridential is as follows:

```
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 (see below for this) 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. Example schemes include the following: - Public-key based authentication through EAP TLS [RFC 2716] - GSM authentication through EAP SIM [EAPGSM] - Any authentication supported by GSS_API through EAP GSS [EAPGSS], including Kerberos and secure authentication method negotiation [SPNEGO]	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. In a 3GPP context, this means that the P-CSCF does not have to be modified, but the S-CSCF may have to.	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?~~Standardized 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. The main advantages are the ability to use existing, other authentication schemes than AKA, the ability to more easily change the used authentication scheme, and the ability to reuse AAA protocols for carrying authentication information.

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)

[RFC 2716] IETF RFC 2716: PPP EAP TLS Authentication Protocol

[EAPGSS] B. Aboba. EAP GSS Authentication Method. Draft-ietf-pppext-eapgss-03.txt, IETF,

[SPNEGO] IETF RFC 2478. Simple and Protected GSS_API Negotiation Mechanism.