3GPP TSG SA WG3 Security **S3z020021**

January 31 – February 1, 2002

Antwerp, Belgium

Agenda Item: 5.1

Source: Ericsson

Title: IETF #52 status report

Document for: Discussion

1. Scope and objectives

The scope of the document is to discuss the outcome from the IETF #52 meeting related to:

- Overall SIP standardization
- Extensible authentication
- Security Mode Setup
- HTTP Digest
- Key transfer

2 Summary

IETF has gotten very strict on SIP modifications and extensions, only the SIP WG can extend it, and only as a standards track RFC.

The Bis version of the SIP RFC is being produced. Current information we have from this process is that a mandatory lower layer security will have to be specified, and that may be TLS. HTTP Basic is also removed

According to [N1-020070] IETF has proposed that 3GPP could define a new body to transport 3GPP specific information in SIP. The advantages with this proposal is that 3GPP gains some more freedom and some independence from IETF. It will work also through a standard SIP proxy since it will be treated as an apaque body and simply forwarded. The major disadvantage is that the SIP message will increase in size and an INVITE containing an SDP body will become a multipart body so more headers will be added. To some extent SIP compression will be able to compress this part efficiently. 3GPP has to define such a body which could e.g. be based on XML. This is currently under study in CN1.

A SIP security design team has been formed, tasked to produce a full requirements document as well as a "next generation" SIP security plan. It is somewhat unclear whether the design team will have an effect to what Bis RFC contains. Members from Cisco, Ericsson, Neustar, Trusecure, Rtfm, and Columbia University are included.

EAP AKA received a number of technical comments, could go forward but the IETF EAP extension organization is unclear and a new WG may be founded. Overall the comments from IETF were positive. Recently, the IETF ADs have asked us if the process should be made faster by doing a more specific solution instead rather than a generic solution, though it is unclear if 3GPP specific extensions would be allowed.

Known problems and shortcomings related to the utilisation of HTTP Digest in SIP will be fixed.

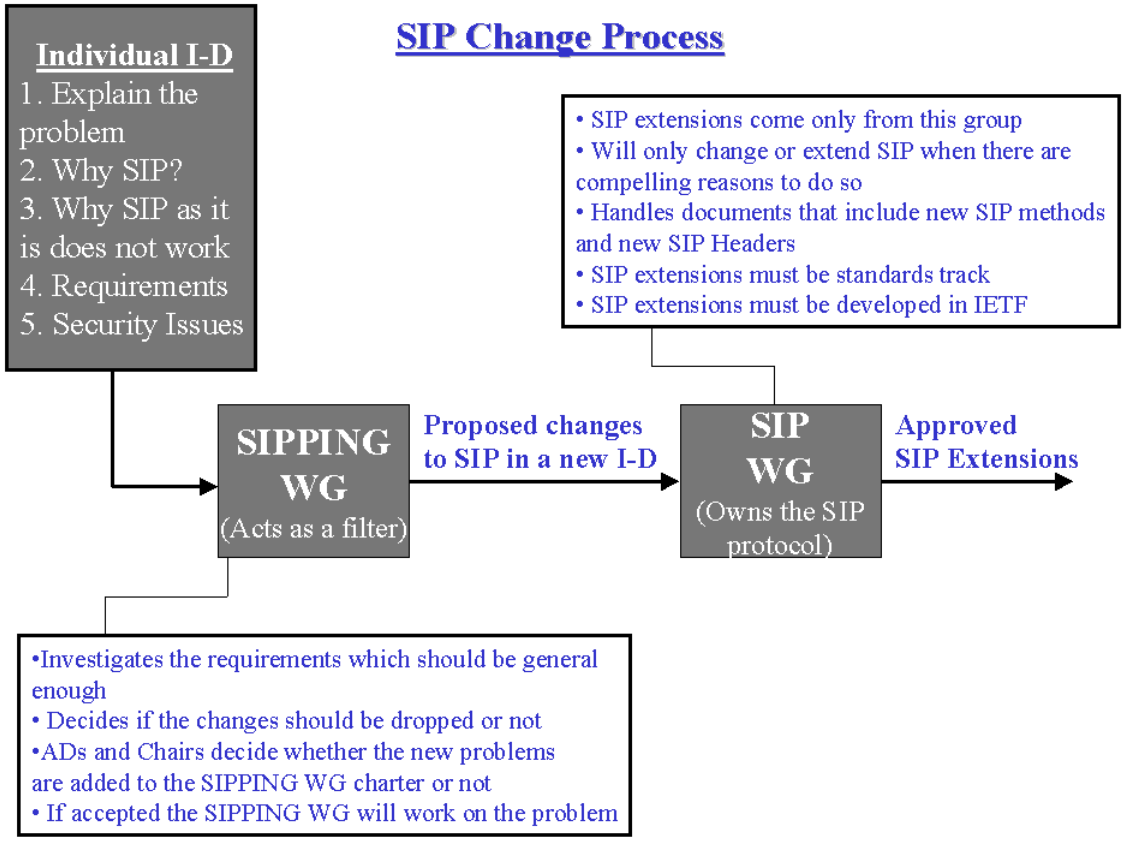
IETF recommended key transfer to take place through extensions of HTTP EAP (not EAP) rather than inventing new general purpose SIP headers for the purpose. The IETF ideal solution to transport session keys would have been a full AAA roaming infrastructure between visited and home networks, but they agreed that building such an infrastructure just for this purpose would be quite expensive.

3GPP requirements were discussed and there were some comments stating that the current draft, cf. [3], is too implementation oriented and that solutions are mentioned rather than the requirement itself.

3 Security issues of interest

3.1 Overall SIP Process

A new sip change process has been defined in IETF, cf. [7]. The reason for defining such a change process is due to the immense interest in SIP, which has increased the number of proposals, how to modify and extend SIP. The working procedure has been agreed between the Transport ADs and the SIP and SIPPING chairs. The flow for the SIP Change process is given below:



3.2 SIP Bis RFC Security

The Bis version of the SIP RFC is being produced. A serious look at the security parts in Bis is being taken, in an effort to guarantee that the IESG will pass the standard. Current information we have from this process is that no major new developments will be done, except for the following:

- A mandatory lower layer security must be selected. The current model is that TLS (not IPSec) will be mandated. Discussions around this are currently in progress. If TLS stays, 3GPP will still be able to use (and needs to for scalability etc reasons) SEGs and IPsec, but vendors may have to additionally implement TLS as well to claim RFC compliance.

- HTTP Basic will be removed, Digest stays.

- Current Bis editor opinion is that any Digest enhancements will be published separately and will not go to the Bis RFC.

3.3 EAP

1. SIP WG

It seems that IETF SIP group in general supports the work done so far in relation to EAP and the 3GPP requirements. However some comments were received:

- Some people felt that statelessness would have to be a requirement, i.e. that the EAP methods shall be stateless. It isn't clear if this is the case for SIP nodes themselves, or for the AAA behind them.

- A mandatory-to-implement EAP method (such as MD5) would have to be specified in the HTTP EAP RFC.

The HTTP EAP draft is not officially included in the SIP charter yet. But IETF SIP and SIPPING chairs encouraged the authors to continue the work, and to separate the extensible authentication requirements from the draft-garcia-sipping-3gpp-reqs-02.txt and to get them through as a small separate draft. They expected this to happen easily and without a new IETF meeting. (But see item 3 below.)

2. PPPEXT WG

The draft [2] was discussed and in particular the proposed solution with unsolicited identity response was not agreed as being optimal. The group accepted that the identity should be sent in the first access request and outside EAP. Another issue was related to two different drafts that at a first glance look similar: EAP AKA for GSM and UMTS [1] and improved GSM authentication [9]. It was commented by IETF that these two drafts could be merged. Finally it was explained that while similar, the drafts are protocol-wise different and fulfill different roles, and IETF appears to agree to have separate drafts.

A standard track status was asked for but the group did not respond nor decide anything on this issue. It was also discussed whether a new group for EAP issues should be defined and if it might be good to wait for new EAP methods until RFC 2284 bis is published. AD Allisson Mankin proposed that 3GPP should send a letter to IETF stating that 3GPP wants EAP AKA to be standardised. Allison believes that IETF EAP-related work needs some time to get organised and the proposed way on how to encapsulate EAP needs some more serious technical review, cf. below:

WWW-Authenticate
Auth-method: EAP
EAP Method: AKA

3. IETF Directors

Since the IETF meeting, we have also initiated a discussion with the IETF AD Alison Mankin on how to proceed with EAP issues, both in SIP and in the PPPEXT WGs.

Alison Mankin brought up the issue of generality vs. specificity and commented that in order to approve the SIP EAP approach, an extensive review and thinking should take place in order to verify that the approach does not cause any unforeseen problems in the future. She also brought up the possibility of defining AKA as an algorithm in Digest as opposed to bringing in the full generality of EAP as a possible means to get the process done sooner. We are going to have a conference with the ADs on these issues this week.

A particular issue in this matter if a AKA specific Digest RFC will be acceptable to the IETF. Alison says yes, though we have previously understood otherwise.

3.4 Security Mode Setup

The discussion on [3] took place in the SIP 3GPP Ad Hoc meeting and not in the SIP WG. There where discussions around the usefulness of such a mechanism. But it was finally concluded that a requirement does exist, and it should be defined such that it is possible to securely negotiate the algorithms to be used.

It is still open if such a mechanism should be included in the SIP bis draft or to be kept in a separate draft. It is also still open if the existing SIP headers like e.g. Support header can be used for this or not. If it is possible to re-use the existing headers (as suggested by Jonathan Rosenberg), some new rules on how they are used need to be defined in order to make the negotiation secure.

3.5 HTTP Digest and related items

HTTP Basic will be removed from the SIP bis and it was concluded that HTTP Digest need to be enhanced.

A number of proposals have emerged to provide better integrity protection in HTTP Digest [4, 5, 6]. HTTP Digest is also known to have other shortcomings, e.g. lack of some parameters in Authentication-Info headers and inability to provide proxy-to-server authentication. IETF mandated James Undery from Ubiquity to drive the work together with a team, which also included people from Nortel and Ericsson. The outcome from the group is expected to be a new HTTP Digest draft, which solves the known problems.

References

[1] draft-arkko-pppext-eap-aka-01.txt

[2] draft-torvinen-http-eap-01.txt

[3] draft-arkko-sip-sec-agree-00.txt

[4] draft-undery-sip-digest-00.txt

[5] draft-sen-sipping-onehop-digest-00.txt

[6] draft-rosenberg-sip-http-pnonce-00.txt

[7] draft-tsvarea-sipchange-00.txt

[8] [N1-020070]

[9] draft-haverinen-pppext-eap-sim-02.txt