3GPP TSG SA WG3 Security **S3z020009**

January 31 – February 1, 2002

Antwerp, Belgium

Agenda Item: ~~TBD~~5.2

Source: Ericsson

Title: Results of a conference call with IETF ADs and SIP WG chairs regarding IMS security

Document for: Discussion

1. Scope and objectives

As an earlier Ericsson contribution reported [1], we had a reasonably good discussion of various things in the last IETF meeting, and expected to continue forward as planned. We have since then, however, been involved in discussions with various IETF Area Directors and experts regarding the SIP security area [2]. Our recent IETF co-ordination meeting ~~meeting last Friday~~ that took place January 25, 2002 brought up their opinions clearly and as a conclusion they recommended us to change our plans on some parts.

If these recommendations are adopted in SA3, there is an impact to our stage two requirements in 33.203. The main effects are in CN1's stage three specifications, however, and the stage two implications are perhaps not that severe. CN4 specifications may also be affected. But SA3 needs to understand the upcoming solutions since this affects our current working assumptions.

On a positive note, the IETF ADs and WG chairs are now behind the new approach and it seemed to be the general feeling that this plan can be completed in time. Such support is necessary to make progress in IETF.

The main results are as follows:

1. We need to break away some agreed-upon requirements from draft-garcia-sipping-3gpp-reqs-03.txt and submit them as small independent drafts.

2. We need to provide AKA in SIP through an extension of Digest, not through EAP.

3. Key transport can not be provided as an additional feature of digest or EAP, as earlier suggested by CN1. An application layer security scheme must be provided.

Beyond this list we noted that HTTP Digest is being enhanced by the SIP WG to provide good integrity protection. We also couldn't cover algorithm negotiation issues and have to get back to those later.

2 Requirements Document Split

The motivation for splitting the requirements is that where there seems to be consensus, a small requirement draft can simply be endorsed and the process becomes faster this way.

The requirements we are breaking apart will be the following:

- AKA authentication in SIP

- Secure algorithm agreement

- Key transport

3 Authentication via AKA

We discussed the main requirements from the point of view of 3GPP networks, and concluded that the highest priority issue is AKA use rather than extensibility. Therefore, the question is how to provide this, through EAP or through some other means.

It was finally recommended by the IETF ADs that a new algorithm value in Digest would be the best solution due to the following observations:

- Alison Mankin (one of the IETF ADs) said that the EAP approach can not be completed by June. This is due to (a) re-organisation of the IETF's PPPEXT and possibly future EAPEXT group, and (b) due to its general approach, the EAP solution would require substantially more review and process than an algorithm extension to Digest.

- Bernard Aboba noted that extensible protocols suffer from interoperability problems as the peers might implement different extensions. The IETF would like to constrain the spread of new authentication types.

- The IETF view is that special SIM-card and other authentication types may not be the final, desired end-state for application layer protocols. The two truly fundamental types of authentication appear to be certificates and tickets. Therefore, while the IETF recognises the short-term need and wants to fulfil it, they do not feel that we should do more than the absolutely necessary part.

We were assured that it would not be an issue to standardise a 3GPP specific extension like this (as we had previously understood).

We may get some IANA space or similar solution to handle possible future upgrades to AKA such that those don't necessarily have to involve the SIP WG. Major revisions to change the number of messages etc. could not however be accommodated in this manner. There also isn't a possibility to use other, already existing authentication types supported by a more general approach such as EAP.

The effects of this are mainly in the CN1 specifications. CN4 is also relying on EAP in order to download authentication parameters from HSS to S-CSCF at the Cx interface. (However, we are presently uncertain if there is or needs to be technical references to EAP or its packet formats in the Cx specifications, since at least some authentication methods in the Diameter multimedia extension are transferred using authentication headers as opaque text.) It should be investigated to what extent specifications and working assumptions in CN4 should be changed.

4 Key Transport

It became clear in the meeting that it is not recommended to make bundled key transport features into either Digest AKA or SIP EAP, or any other such mechanism. It will also not be recommended to specify a standardised mechanism that relies on underlying security of which the application using the keys is not aware.

We should specify the key transport as an individual function, with its own headers or bodies used for transporting the keys.

The reliance to lower-layer security schemes in the transport of the keys is also problematic. Due to the importance of the session keys for the security of the system, the ADs recommended that the applications should be aware of where they are receiving keys. While the 3GPP approach with SEGs is acceptable in the 3GPP case, a standardised key transport mechanism is likely to find other users as well, and needs to prepare for different network cases. A separate gateway solution is unlikely to provide information to the application layer from which specific source the keys came from – it can at most guarantee that the keys came from one of the sources trusted by the gateway. Secondly, in a multi-hop situation (such as the one in 3GPP networks), even information provided from an underlying security mechanism may not be very helpful. Therefore, the recommendation was that an application layer mechanism be used to protect key transport. One such mechanism is S/MIME, though also other possibilities such as XML Digital Signatures exist.

5 Conclusions

Ericsson hopes the SA3 considers the new information presented above and makes decisions regarding how to proceed with TS 33.203. In particular, we need to decide if the above proposals satisfy our requirements, whether there are any security issues that this brings up, and what guidance should we give to CN1 and CN4.

6 References

[1] “IETF #52 Status Report”. Ericsson contribution to the SA3 meeting in Antwerp, January 2002.

[2] “Results from the recent IETF coordination meeting”. Stephen Hayes’ e-mail to SA3 (forwarded).