3GPP TSG SA WG3 Security — S3#17bis **S3z010029**

23-26 April, 2001

Madrid, Spain

Source:	**Nokia**
Title:	**Open issues in IMS security**
Document for:	**Discussion / Decision**
Agenda Item:	**tbd**

This contribution deals with the main open issues in the work item "Access security to IMS". Those items were marked as "ffs" in the S3 position statement S3-010100.

The open issues are:

1) The authentication is performed in the home network.
It is ffs whether it is performed in the HSS or the S-CSCF.

2) It is ffs whether confidentiality of SIP messages is required on all hops.

3) The exact mechanisms for integrity and confidentiality are ffs.

This contribution is divided into two parts. The first part deals with the open issue 1) while the second part deals with issues 2) and 3).

The location of the authentication comparison

As decided by S3 earlier, the authentication vectors are generated in the HSS and the decisive comparison between the parameter RES (transmitted from the UE) and the parameter XRES in the authentication vector is done in the home network also in the roaming case.

This leaves basically three options for the element that performs the authentication comparison: HSS or S-CSCF or I-CSCF. The last one can be excluded from the list since it may change during the authentication process.

Siemens has already provided a good analysis of pros and cons of the two remaining alternatives. We add here a few arguments which seem to shift the balance a bit thus leading us to a different conclusion.

We briefly list the pros and cons (of doing the comparison in S-CSCF) from Siemens' contribution:

Pros:

- Stateless paradigm for HSS can be preserved (from UMTS and GSM):
- HSS becomes more vulnerable to DoS attacks:
- HSS can send a batch of authentication vectors to the S-CSCF:

Cons:

- Home network more vulnerable to DoS attacks:
- S-CSCF temporarily needs to store authentication related information:

The explanation of all these points can be found in the referred contribution.

We briefly discuss these pros and cons and then add a few more.

The pro and con about DoS attacks more or less balance each other: the HSS is anyhow vulnerable since it has to generate all the authentication vectors, the batch of vectors in S-CSCF gives some leeway but, on the other hand, S-CSCF becomes another target. Altogether, some protection measures against DoS attacks should exist in the visited network already.

Also, the first pro and the last con more or less balance each other since they are about locating the same comparison functionality in to two different elements.

The additional relevant pros and cons are listed below:

More Pros:

The signalling flow for authentication in the REGISTER case is simpler: this means the delay during the registration is shorter.

The authentication functionality is not divided into several home network elements: this means the solution is better future-proof for potential architectural evolutions in later releases of IMS.

More Cons:

The signalling flow for authentication in the INVITE case is more complex: there is an additional HSS query in the signalling flow. This clearly adds delay. However, the major part of delay results from the fact that INVITE is authenticated in the first place by home network; whether it is done in S-CSCF or in HSS plays a minor role.

We now analyze these new pros and cons.

At first sight it may seem that the first pro and the con balance each other. However, as the INVITEs are integrity protected between UE and P-CSCF there is no big need to authenticate the INVITEs by the home network. The refreshing of keys can as well be done during re-registrations. On the other hand, registrations must be authenticated because integrity protection is not available yet.

As a conclusion, the additional points listed here seem to turn the balance into the direction of performing authentication comparison in the HSS.

Protection of SIP signaling between UE and P-CSCF

We begin with the discussion of the exact mechanism for integrity protection.

The main alternatives are

- use of IPSEC in the IP layer to protect the upper layer communications
- protection of SIP signaling directly by a suitable mechanism

We analyze pros and cons for the first alternative.

Pros:

The mechanism is already specified: Indeed, the ESP functionality seems to be enough for this purpose which reduces the implementation requirements on the terminal.

Security associations may be derived from AKA generated keys

Cons:

The protection is tied into IP address and not to directly to SIP identities: this is problematic for two reasons in case there are several SIP users for the same device:

- the distinction between the users has to be done by e.g. separate SPIs
- it has to be checked in the receiving end that the used SA in the IPSEC really corresponds to the correct SIP identity

The cons seem to cause serious complications. It does not help if the device has several IP addresses. Still it is a severe constraint if the IP layer both in the UE and the P-CSCF has to be tied into the SIP layer this way.

The main disadvantage of a SIP level mechanism is that there are no suitable mechanisms specified in SIP. The solution by PGP does not work well. However, there are standard mechanisms available that can be used to protect SIP signaling in our case. An example of such a mechanism is S-MIME.

Since, there are serious problems in the IPSEC solution it seems better to take the other route and adapt an existing IETF mechanism, e.g. S-MIME, to protect SIP.

As regards confidentiality protection, the same mechanism can be used. However, it should be carefully studied whether it is enough to require this only as an option, since the confidentiality is anyhow protected, for instance, in the radio interface.