3GPP TSG SA WG3 Security — S3#21bis (aSIP ad-Hoc) **S3z020016**

January 31st– February 1st, 2002

Antwerp, Belgium

Agenda Item:	6.1
Source:	Ericsson
Title:	On integrity protecting SIP-signalling in IMS
Document for:	Discussion and decision

1. Scope and objectives

The scope for this document is to discuss and highlight some issues and concerns related to integrity protection of SIP signalling i.e. SIP-level and IPSec.

It is proposed that SA3 should adopt SIP-level protection as a working assumption.

2 Background

As decided during our ad-hoc meeting on aSIP last September, TS 33.203 considers two options to provide integrity protection to SIP signalling at the first hop between the UE and the P-CSCF; Annex B includes mechanisms for the IPSec-based solution while Annex C specifies mechanisms for the SIP-level solution. At the same time, it was decided to monitor the progress of the work in IETF making it possible to take a decision to include SIP-level protection for Rel-5 or not.

Several contributions have been already presented and discussed proposing one alternative or the other and also comparing pros and cons of each one. This contribution tries to bring the latest status of each alternative, further elaborate in pros and cons and finally conclude in the selection of the most optimal alternative that fulfils our requirements.

3 Discussion

3.1 IPSec-Based Solution

The integrity protection mechanism for the IPSec-based solution proposed in Annex B is based in the assumption that IPSec can be applied in order to protect SIP signalling at the underlying IP layer.

The claimed main advantages of this solution can be summarized in the following bullet points …

1. It is a fast solution. Only standardisation work is to define IPSec profiles done by SA3.
2. Minimised interaction with IETF and the SIP workgroup
3. IPSec is already implemented in IMS nodes
4. IPSec SAs can be derived from the AKA

However, there have been several contributions outlining some of the disadvantages of this approach which may lead to re-evaluate the advantages presented above …

- Using IPSec together with a SIP client in the MT or TE requires binding SIP-signalling with IP-parameters in a way, which is not specified today.

This violation raises some security concerns if there are several users using the same device. For example a couple of SIP clients share the same IP address with individual IMS identities may not be distinguished successfully by the IMS core network.

From a system protocol layer this approach does not look very pretty. The security solution will not be self contained and several layers co-operation is needed. In particular, the following is needed:

- Security association and policy state must be duplicated at both layers
- Software and hardware for implementing the facilities must be provided in two places, the IP and the SIP layers, as opposed to simply providing a SIP proxy application, for instance, that contains all security features and can run on top of any operating system.
- There must exist an API that allows dynamic modification of policy and security association databases from the application to the IP layer. No such standard API exists today, and it is not guaranteed that all products have such an API at all. Note that the API must be general enough to ensure, for instance, that traffic from an incorrect port enters the SIP proxy because the security policies couldn't be specified at fine enough detail.

- It has already been identified that e.g. some special handling on port numbers might be needed to make IPSec to fulfil 3GPP requirements on SIP (i.e. handling of protection to originating and terminating SIP signalling and special handling of error messages). This means that of-the-shelf IP-stacks in a MT and the TE can't be used.
- It is not so clear how IPSec will affect efficiency of UDP/IP header compression.
- It is not possible to extend the protection to the home network using the IPSec-based approach, thus restricting which business models and services the operator can offer in the future. End-to-middle protection can only be done at SIP layer.

3.2 SIP-level protection

The integrity protection mechanism for the SIP-level solution proposed in Annex C is based in an adaptation of the existing SIP authentication/integrity-protection framework called HTTP Digest which is used to satisfy the requirement for UE-to-Proxy CSCF SIP integrity protection.

This proposal can not make use as such of HTTP-digest, as described in [RFC2617] and as used in [SIPbis05]. Most of the required adaptations to the http authentication framework are specified in "draft-sen-sipping-onehop-digest-00.txt". This and other similar I-Ds trying to solve the shortcomings of HTTP-digest were presented at IETF#52 meeting. IETF created a team (driven by James Undery from Ubiquity and with the participation of people from Nortel and Ericsson) which is expected to provide a new HTTP Digest draft, which solves the known problems including the lack of integrity protection. This team will deliver a proposal for enhanced HTTP Digest to the SIP WG mailing list in brief.

Based on the determination IETF is showing it would be then safe to say that a SIP-level integrity solution will be in place in the near future. This solution will not only fulfil our 3GPP requirements on integrity protection, it will also solve other limitations in HTTP-digest.

Being this the case, this solution will be present in standard SIP implementations and it sounds reasonable that our architecture adopts such a solution now. That will minimize the number of integrity mechanisims supported due to backwards compatibility reasons (if the IPSec-based solution is selected today, terminals will end-up supporting both solutions when http-digest enhancements reach RFC status at IETF).

Some other arguments why Ericsson believes that this solution is also the most optimal in order to fulfil 3GPP requirements are listed below:

- Represents a clean architectural model since it would not break the layering structure (the number of states that have to be kept at different layers is minimised and only a single port number for all SIP messages is required whereas IPSec needs two).
- Represents a future proof solution in the sense that it does not put any restrictions on future business models as IPSec does (flexible upgrade from hop-by-hop security architecture to end-to-middle architecture is possible without any change to the MT).
- Represents a backward compatible solution (i.e. only one solution has to be built into the terminal for SIP-signalling protection).

- The proposed solution for SIP-level protection can be used by other applications towards other services in the service network.

4 Conclusions

This contribution clearly shows that IETF is commited to provide SIP signalling with integrity protection in a time frame that fits with our Release 5. It is also shown that if this approach also represents a more optimal solution than the IPSec-based solution from architectural, backward compatibility and future proof point of view.

Ericsson seeks support from SA3 to have the SIP-level protection mechanism currently defined in Annex C of TS 33.203 as the working assumption to provide SIP with integrity protection (content of Annex C should be then moved to chapter 6 in the main body of the specification).