3GPP TSG SA WG3 Security — S3#20 **S3-010408**

16 - 19 October, 2001

Sydney, Australia

3GPP TSG SA WG3 aSIP ad hoc **Version 0.1**
Nice, France
14th September 2001

Source: **SA WG3 Secretary (M Pope)**

Title: **Draft report of the meeting - version 0.1**

Document for: **Information**

---

1 Opening of the meeting (09:00 Friday)

The Chairman of the ad-hoc meeting, Mr. V. Niemi, opened the meeting and welcomed delegates to Sophia Antipolis.

2 Approval of the agenda and objectives of the meeting

TD S3z010071 Draft agenda for SA WG3 meeting #19bis (IMS security). The draft agenda and objectives were presented by the Chairman, V. Niemi. The objectives were discussed and it was noted that the integrity protection would still need to be discussed in SA WG3 where more views could be taken into account in any decision-making. It was reported that the SA WG3 Chairman had agreed that a LS could be produced to CN WG1. This was added under a new agenda item 6.3 "Other". It was agreed that the primary objectives would be considered first and other documents considered if there is enough time left.

Objectives:

1 The primary objective is to make progress on integrity protection for SIP signalling. Currently IPSec and SIP-level protection is under consideration. The goal is to agree on working assumptions and provide with guidelines for future work.

2 A secondary objective is also to understand the current situation in IETF and identify issues that are related to IMS and that may affect future work.

3 Allocation of documents to agenda items

The available documents were allocated to their appropriate agenda items.

4 Liaisons from other groups

The LSs which had been provided to the SA WG3 #20 meeting (Sydney) and which were relevant to these discussions were briefly considered in order to check for potential impacts on the discussions. It was agreed that the LSs should be considered in the Sydney meeting, and only replied to if an urgent response is considered necessary, and after SA WG3 email agreement if possible.

TD S3z0100104 Reply LS on “Using a generic authentication scheme for SIP” (CN WG1). This should be considered by delegates for treatment at SA WG3 #20.

TD S3z0100105 LS to SA3 on Signalling for user authentication (CN WG4). A response should be prepared for SA WG3 #20.

TD S3z0100106 Liaison Statement on "IMS security and UE functionality split" (SA WG1). This should be considered by delegates for treatment at SA WG3 #20.

TD S3z0100107 LS response to SA3 on “Using a generic authentication scheme for SIP” (CN WG4). Noted for discussion at SA WG3 #20.

TD S3z0100108 LS from SA WG2: Response to LS S3-010403 on the use of Network Domain Security for protection of SIP signalling messages from SA WG3. (SA WG2). The confusion from SA WG2 was considered in need of clarification, which may be returned to under agenda item 6.2, if there is time at the meeting or otherwise in S3#20 in Sydney. This was then noted.

TD S3z0100109 LS from SA WG2: Security aspects for IMS related to Authentication (SA WG2). This suggests that multiple Public Identities implies the possibility of multiple service profiles, which may be served by different S-CSCFs. The issues raised by the LS should be considered by delegates for treatment at SA WG3 #20.

TD S3z0100110 Liaison Statement on "Flows related to Authenticated Registrations and Re-Registrations" (CN WG1). Noted for discussion at SA WG3 #20.

TD S3z0100111 Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem (CN WG1). Suggestion of a CLIR-like mechanism in IMS. Noted for discussion at SA WG3 #20.

TD S3z0100112 Response to LS "On the use of Network Domain Security for protection of SIP signalling messages“ (N1-011041 or S3-010403) (CN WG1). This was considered relevant to discussions under agenda item 6.2 and may be discussed if time allows in order to provide feedback before CN WG1's next meeting (2-4 October).

TD S3z0100113 Response to Liaison Statement on "Progressing the work in SA3 and CN1 on the IP Multimedia core network subsystem" (CN WG1). Noted for discussion at SA WG3 #20.

TD S3z0100126 LS from T WG3 on IMS identifiers and ISIM or TSIM. It was thought that contribution on the ISIM issue is needed at SA WG3 #20 before there would be any input to such a meeting. Therefore the proposal of late October for a joint meeting was not appropriate, and the need for such a meeting would be clear after discussion at SA WG3 #20.

5 IETF

5.1 Report from the IETF meeting in August (London)

P. Howard provided a verbal report of the IETF meeting. a written report will be provided to the SA WG3 #20 meeting.

5.2 3GPP related IETF drafts

TD S3z010128 This was presented by J. Arkko and discussed. The need for input to the IETF to include the 3GPP security requirements was highlighted. It was agreed that effort should be made by SA WG3 members in order to ensure that security architecture for 3GPP can use the IETF specifications. All requirements should be covered by one contribution to the IETF. It was recognised that there was no guarantee of acceptance of the requirements in the IETF, but that we should try to have them accepted at least. Input to the editors of the 3GPP requirements Internet draft was needed by 21 September in order to meet the tight schedule for contribution.

TD S3z010093 IMS requirements on SIP for IETF. Sections 6.20 onwards were presented by J. Arkko for discussion and some comments were provided to the draft. Comments were requested by 21 September to allow the editor to input the requirements to the IETF. J. Arkko agreed to send an e-mail to the SA WG3 list to ask for consideration of this requirements draft and to provide comments to him.

6 SIP signalling protection

6.1 Integrity

TD S3z010097 IPsec for Integrity protection between UE and P-CSCF. This was presented by Siemens and provided their assessment of the need to find a solution for integrity protection of SIP messages for Rel-5 3GPP specifications. Two alternatives to provide integrity protection for SIP signalling exist: application layer mechanisms that provide integrity within SIP messages, and IPsec that protects SIP messages through standard security mechanisms at the IP layer. The contribution further elaborated on the open issues identified in the context of considering IPsec and considers CMS providing SIP integrity protection at the application layer. Discussions ensued, and it was agreed to look at the companion contribution **TD S3z010098**.

TD S3z010098 was briefly introduced by Siemens and describes a proposal for SA mechanism assuming sufficient security is provided by IPSec.

TD S3z010102 On integrity protecting SIP-signalling in IMS. This was provided by Ericsson, Nokia and Nortel Networks and was briefly introduced by Ericsson. It discussed the issues and concerns to integrity protection of SIP signalling: SIP-level and IPSec. The paper concludes that although there is a time and resource problem on the specification of SIP-level protection, the contributing companies would like to use this in order to benefit from a single solution implementated in terminals. It was suggested that double number of ports will not be needed for error messages as all could be on the same port.

TD S3z010099 Requested changes to TS 33.203 v050. This was briefly presented by Siemens.

TD S3z010103 Digest-Based SIP Message Integrity Protection for IMS. This was presented by Ericsson, as the author was unable to attend the meeting. This should be considered by delegates for further elaboration at SA WG3 #20. It was agreed that "checking points" should be defined within SA WG3, where the progress of the work in the IETF is monitored in order that a decision can be made on whether the SIP-level protection can be included in time for Rel-5. Both integrity solutions would be included in the draft specification as annexes and one would be removed for the freezing of the specification for Rel-5 (the best available solution being kept).

Note: The specification is targeted to be provided to TSG SA #14 for information in December 2001. It was noted that December version may still contain two alternative annexes for integrity protection.

6.2 Confidentiality

There was no time for this.

6.3 Other

TD S3z010092 Proposal to do some Network initiated deregistration using the SIP-SUBSCRIBE method - a similar simple mech could be used for authenticated re-registration. It was decided that Siemens should provide this to a CN WG1 collegue to take to CN WG1. Gunther will check this with Mike Walker and send an e-mail and a proposed LS to the SA WG3 list.

7 Review of output documents

7.1 For SA WG3 meeting #20, 16-19 October 2001

It was agreed that "checking points" should be defined within SA WG3, where the progress of the work in the IETF is monitored in order that a decision can be made on whether the SIP-level protection can be included in time for Rel-5. Both integrity solutions would be included in the draft specification as annexes and one would be removed for the freezing of the specification for Rel-5 (the best available solution being kept).

8 AoB

A 3-minute silence was observed at 12.00 in consideration of the victims of the USA attacks of 11 September.

9 Closing of the meeting (17:00)

100, 101, 118 no time to deal with these.