25 - 28 February 2002

Bristol, UK

3GPP TSG SA WG3 Security #21bis — MAPSEC/NDS ad-hocs   **version 0.0.1rm**

31 January, 2002

Antwerp, Belgium

Source: **SA WG3 Secretary**

Title: Draft Report of MAPSEC and NDS/IP ad-hoc

Document for: **Information**

1   Opening of the meeting (9:00)

The meeting was opened by V. Niemi, SA WG3 Vice Chairman, and outlined the schedule for the ad-hoc meetings.

Olivier Paridaens welcomed delegates to Antwerp, Belgium, on behalf of Alcatel, and provided domestic arrangements for the ad-hoc meetings.

2   Approval of the agenda

TD S3z020002 Draft agenda for MAPSEC and NDS/IP ad-hoc meetings. The agenda was reviewed, agenda item 6.7 "Release 6 issues" and was then approved.

3   Allocation of the input documents

TD S3-020008 and TD S3-020016 for the SA WG3 meeting #22 (Bristol), were allocated to MAP/NDS agenda item 5.1.

4   Report from SA#14

The relevant part of the report from SA #14 (section 7.3.3) was reviewed, where separate CRs for the Release 5 version of MAP Security was requested. Also it was noted that TSG CN had reported that the Ze interface specification work in CN would not be complete by March 2002.

5   MAPSEC issues (handled until no later than 13:00)

5.1   Relevant LSs

TD S3-020008 LS on MAPsec error handling (response to S3z010121). This was presented by Siemens. It was noted that CN believe the messages protected are consistent with flows given in 33.200CR007. The problem reported on DoS attack scenarios had already been identified and considered by SA WG3, and protection against this had been considered too expensive for the gain achieved (similar attacks will still exist if this is protected against). The stable draft of TS 33.200 was available after the SA#14 meeting (noted as version 1.0.0).

TD S3-020016 Liaison statement on Protocol Specification of the Ze interface. This was presented by Vodafone and requested time during the SA WG3#22 meeting (Bristol) for discussion with CN WG4

experts on the Ze interface. It was, unfortunately, too late for the proposal for SA WG3 experts to attend the CN WG4 meeting, but it was agreed that this would be useful and some time during the meeting should be allocated (host needed contacting to determine the best slot for this). A response LS to CN WG4, responding to the LS in TD S3-020008 and TD S3-020016 was provided in TD S3z020028. This was modified slightly and re-provided in TD S3z020038 which was approved. **(Note that this carries a footnote explaining the status of the LS, which needs final approval on the SA WG3 e-mail list)**.

5.2 Status of 33.200 Rel. 5

TD S3z020023 Latest version TS 33.200 Rel-5. The MAP Rapporteur provided this for information and shows the proposed Release 5 version of MAP Security with change bars from the Release 4 version. The current version was noted. See the discussion on structuring the CR(s) under agenda item 5.3.

5.3 How to structure CRs proposed to SA#15

TD S3z020023 Latest version TS 33.200 Rel-5. The MAP Rapporteur provided this for information and shows the proposed Release 5 version of MAP Security with change bars from the Release 4 version. This was the proposal for a single CR to TSG SA for approval and production of Release 5. It was argued that if several separate CRs were produced, then there was a need for all CRs to be approved, as they were mainly relying on each other. As TSG SA had requested a set of functionally separate CRs to produce Release 5, this possibility was investigated. It was concluded that the changes could be split into around 7-8 parts, but that they would not be really separate, and the process was rather artificial. e.g. KAC affects Ze and Zd interfaces, and these changes would all need to be approved or rejected together. After some discussion it was agreed that a single CR was the only practical way forward, as if any parts were not approved, then none of the changes should be included as the document would then be incomplete. **A cover document will be created by the MAP Security Rapporteur, explaining the reason for a single CR and the dependencies of the changes, for inclusion with the CR to TSG SA Plenary**.

5.4 Ze interface

TD S3z020013 Proposed additions to 33.200 about COPS usage in Ze interface for Local Security Association and Policy Distribution. This was introduced by Nokia and proposed an additional section 8.2 concerning Local Security Association and Policy Distribution in the Ze interface, using the COPS protocol. The exact COPS message content would need to be developed by CN WG4. The detail of the proposal was presented by Nokia and some issues were discussed:

Dependencies upon IETF work. It was suggested that COPS extension may be required to be done in the IETF. It was suggested that 3GPP could produce the COPS specification for MAP security and input it to the IETF for information.

It was agreed that this contribution should be re-submitted to the joint session with CN WG4 experts at the SA WG3#22 meeting (Bristol).

TD S3z020024 Secure connection between KAC and NE. This was introduced by Alcatel and discussed the need for a mandatory protected connection between the KAC and NEs. The proposed changes were approved and the MAPsec Rapporteur was asked to include it in the Rel-5 changes CR. Some text was recognised as needed for clause 8, in order to mandate the protection of trigger messages. It was also suggested that "protection in this context did not imply encryption, in the case of physical proximity protection of the elements, however, the Introduction to the Specification states that the techniques .are based upon cryptographic techniques, so both these sections were also in need of modification to clarify the situation in line with the changes to section 8. It was generally agreed that the protection of the internal interface is optional, and each operator may decide how to protect his own internal network. It was finally agreed that the issue needed more consideration and discussion than was available at the ad-hoc, and an e-mail discussion, based on a proposed text from the Rapporteur would take place the following week in order to finalise the text for the SA WG3 meeting #22 (Bristol).

> NOTE: Changes are considered appropriate for Rel-5 only, not reflected back into Rel-4.

5.5 MAPSEC DoI

D. Castellanos (Ericsson) provided a verbal progress report on progress. There is to be a submission after a presentation in December - work ongoing after this meeting and an updated version is likely to be submitted to the IETF for comments, and then it will be provided to the SA WG3 meeting #22 (Bristol).

5.6 Other technical issues

The Chairman raised the issue of the "dialog portion", as there are some MAPsec items which do not contain this dialog portion. Protection of the dialog portion would lead to two security headers in the MAP message. Also, adding such messages for protection will require an analysis of the method of protection for them. This could give problems for CN WG4 for inclusion in the protected messages list.

These issues were recognised as being post Rel-5 issues. It was concluded that these issues could be discussed with CN WG4 in the joint session in Bristol. Nokia were asked to provide a contribution discussing these issues to the Bristol meeting, after discussion with CN WG4 experts.

6 NDS/IP issues (handled until no later than 15:30)

6.1 Relevant LSs

There were no contributions under this agenda item.

6.2 Status of 33.210

TD S3z020005 Draft TS 33.210 v 1.0.1. This was briefly introduced by the Rapporteur, he reported that IPsec input was still outstanding. The IP version for the SEG-SEG interface may need specification in order to avoid interoperability problems. It was agreed to remove the editors note, acknowledging that this is an issue which needs resolution. **Delegates were asked to consider this issue and provide contribution to try to resolve the issue**.

Annex C: The SCTP protocol may be used as an alternative to ~~GTP~~TCP, but protection of this presents additional challenges. The IETF is aware of this and a draft RFC is available which proposes a solution to this problem. It was suggested that this could be included as information in the text (as it is unlikely that full material will be available for the Bristol meeting) as notes on the transfer of DIAMETER using SCTP. A proposal was provided in TD S3z020015.

TD S3z020015 On Use of IPSec for SCTP. This was introduced by Ericsson, and suggested some text to cover SCTP to transfer DIAMETER messages over the Cx interface, referring to the draft RFC. This proposal was agreed and the Rapporteur was asked to add the agreements reached at this ad-hoc for the SA WG3 meeting #22 (Bristol).

TD S3z020012 Comments to 33.210 v1.0.0: IP network layer security. This was introduced by Siemens and each proposed changed was considered. the comments and agreed modifications to the proposals were noted by the Rapporteur, who agreed to update the draft 33.210 to include this information and distribute it for the SA WG3 meeting #22 (Bristol).

NOTE to Rapporteur: (Geir): The final change to Annex C was discussed. The proposed changed were not agreed and the text re-instated as before. It was, however, agreed to delete the words: "such as Mm, Mk, Mg and Sr" .

6.3 AES issues

6.4 Zb/Zc merging

TD S3z020025 SA mode in Zb interface. This was introduced by Alcatel and pointed out some contradictions in the document in specifying the use of tunnel mode towards a SEG, whereas the possibility to use transport mode is also allowed in some situations (between NEs in the operators own network). The contradiction pointed out in the contribution was recognised by the group, however, no

agreement on whether to mandate tunnel mode only instead of generalising with the use of the SA terminology, as proposed in the contribution, could be reached in the limited time available. **It was therefore agreed that this should be the subject of contribution to the SA WG3 meeting #22 (Bristol) for a decision and resolution of the contradiction**.

6.5 Relation to 33.203

6.6 Other technical issues

6.7 Release 6 issues

TD S3z020022 A proposal for evolution of Network Domain Security for Release 6 – Introduction of an authentication framework. This was provided for information and proposes an enhancement to a WI. The document was noted and delegates asked to review this for contribution to the SA WG3 meeting #22 (Bristol).

7 Review of output documents

Output Liaison: S3z020038: LS to CN WG4 on joint session on Ze interface. To: CN WG4.

8 AOB

9 Closing of the meeting (no later than 16:00)