3GPP TSG SA WG3 Security — S3#13 **DRAFT Report Version 0.0.2**

MAP Security Ad-hoc meeting 23 May, 2000

Yokohama, Japan

Source:	**Vice-Chairman 3GPP TSG-SA WG3**
Title:	**Draft AD-HOC Meeting Report**
Document for:	**Approval**
Agenda Item:	**3**

1 Opening of the meeting

Mr. M. Markovici acted as chairman for this meeting.

Dr. Hirotaka Nakno (NTT DoCoMo) welcomed delegates to Japan, and extended his appreciation to the group for their contribution to the Release 2000 work under the short timescales set for this. e also provided a general overview of the NTT DoCoMo research departments' work.

2 Objectives of meeting

The Chairman gave the objectives for the meeting, which were to agree on the requirements for release 2000 MAP Security and related work, in order to provide agreed input to the joint meeting with CN planned for June 2000.

3 Approval of the agenda

The agenda, provided in TD S3-000340 was approved.

4 Registration and assignment of input documents

The documents available for the ad-hoc meeting, included as part of SA WG3 documents, were allocated to their agenda items.

5 Work Items in preparation for the joint CN/S3 meeting in 13-14 June, 2000

5.1 Plan for joint CN/S3 work items

TD S3-000318: Proposal for the Release 2000 Features, Building Blocks and Work Tasks Version 1.0. This was introduced by Mr. P Howard and provides the details of the Security work that needs to be considered by SA WG3.

TD S3-000313 and TD S3-000314: Draft R00 Project Plan version 0.0.4 (with and without revision marks). The proposals from SA WG2 need to be discussed in SA WG3 and the proposed work items and their timescales checked. The MAP security ad-hoc looked at section 3.1.1.4 - Network Security - Minimal Solution and section 3.1.1.5 - Network Security - Full solution. Both have timescales for June 2000 for completion of SA WG3 work. The use of IPSec for the minimal solution and the need for SA WG5 involvement was questioned (the solutions are thought to be moving to a MAP-based solution, rather than a TMN-based solution for Layer 2). The document should be updated by the ad-hoc group and passed to SA WG3 for acceptance

ACTION #AH/1: All to contribute to update the draft Project Plan for input to the SA WG3 meeting.

5.2 Layer 3 (e.g., GTP, MAP Security)

TD S3-000312: Independence of confidentiality and integrity in MAP Layer 3 and other layer 3 issues. This Siemens AG contribution proposes to provide different modes of protection, a mode with integrity protection, but no confidentiality protection, and one with integrity and confidentiality protection. (This would allow two networks, where one network does not allow encryption, to have at least integrity protection). Some open issues were also identified by this contribution: the requirements for and definition of a time-variant parameter, and the definition of a security association for Layer 3.

The encryption of the integrity data could lead to some problems, as usually integrity is checked before decryption. This needs to be further investigated for impacts.

It was decided that the MAP security work should be held in a working document ready for introduction into the Release 2000 document as CR(s) once version 4.x.y is under change control.

Mr. R. Lubarsky (T-Mobil) agreed to act as editor of the MAP security working document, which will initially consist of 33.102, V 3.4.0 modified by the proposal of TD S3-000312. This will be discussed via e-mail and updated for presentation to the joint meeting with CN in June 2000.

ACTION #AH/2: Mr. R. Lubarsky to act as editor for the working document on MAP Security for Release 2000. To be produced by 2 June 2000.

TD S3-000329: Use IPSec to secure GTP messages (Motorola). This proposes the use of IPSec to secure GTP messages in TS 29.060 v3.4.0 (CN WG4 document). This adds some Cause Values and descriptions to the document. The need for AH as well as ESP was discussed. It was concluded that the need for AH needs further study. Some other modifications to the proposed Cause Values were considered necessary, e.g. KAC session key expiry is covered by no agreement on Security Association.

The proposal did not include details on how IPSec will be used to secure GTP, and this would be needed in order to ensure that the use of IPSec is adequate for this. Motorola agreed to revise this contribution, taking comments into account, and present it to the next meeting. e-mail correspondence should be used for additional ideas and discussion on this subject.

For the joint meeting with CN, in June 2000, SA WG3 can only say that the use of IPSec is needs more discussion on the detailed implementation within SA WG3. An agreed position was to be drafted during the SA WG3 meeting, if possible, otherwise to be agreed by e-mail after the meeting. Mr. P. Howard agreed to draft a document for discussion.

ACTION #AH/3: Mr. P. Howard to draft a discussion document on the use of IPSec to secure GTP messages for the Joint meeting with CN in June 2000. To be completed by 2 June 2000.

TD S3-000339: MAP Security Layer 3 open items. Some discussion on the use of Protection Mode 0 and Mode 1 took place. It was noted that protection mode cannot be dynamically changed on a message by message basis, as this would be negotiated and set-up at the start of a call. The structure proposed by CN WG4 increases the security header length significantly. The reason for the chosen structure was not known. It was finally agreed that a liaison to CN WG4 on the results of the discussion on Security Mode 0 would be provided and transmitted to CN WG4. Mr. D. Castellanos agreed to produce a note to CN WG4.

ACTION #AH/4: Mr. D. Castellanos to produce a note to CN WG4. on MAP Security Layer 3 open issues.

Discussion over the length of the TVP (32 bits initially proposed) and the content of the TVP resulted in the decision to further investigate the possibilities via e-mail. Mr. P. Howard undertook to contribute on and manage this discussion.

ACTION #AH/5: Mr. P. Howard to manage discussion group on Protection Modes and TVP definition.

5.3 Key Management (e.g. IKE)

TD S3-000331: Using IKE for Layer 1 of MAP Security. This contribution points out that IKE is a suitable mechanism for Key exchange in Layer 1. It was reported that a newer version of the referenced RFC for IKE was available, which had some significant changes in mandatory/advisory options. It was generally agreed that use of IKE seemed to be a reasonable working assumption, and that other groups should be asked to comment on this proposal (i.e. SA WG2 and relevant CN WGs). Investigation of the Security Associations requirements for Layer 3 and the mechanisms available in IKE needs to be made and reported back before a decision on the use of IKE can be made by SA WG3. Mr. R. Lubarsky agreed to manage an e-mail discussion group on this and interested delegates should contact him.

ACTION #AH/6: Mr. R. Lubarsky to manage discussion group on use of IKE for Layer 1, including any Liaison Statements to other groups which are needed. Draft liaison(s) to be completed by 24 May 2000 for discussion in SA WG3.

In order for CN to include the MAP security requirements in Release 2000, they have requested stable requirements from SA WG3 by the June TSG CN Plenary. It was agreed that IKE would be investigated as the preferred system (Mr. R. Lubarsky undertook to do this).

TD S3-000328: Use of IPSec IKE for Layer 2 key distribution. In this contribution, Motorola propose that IKE could be the preferred solution for Layer 1 network to network key distribution. It was pointed out that the Key Management will need to cope with non-IP networks for some time, and that the GSM solution cannot be abandoned for Release 2000.

The contribution also suggests the use of the 6-message "main mode" which affords increased identity confidentiality, which had not been addressed before by SA WG3. The need for identity confidentiality on these interfaces needs to be considered.

The following questions were raised by the contribution:

1 Can we have a IP based security mechanism for Layer 2?

2 Do we need it?

Further discussion around this was needed, and SA WG2 and CN WGs should be asked whether all Release 2000 Network Elements are assumed to be IP-aware or not. If so, then the IKE solution could be used for Layer 2, and Layer 1 could be left as a network operators choice. (CN WGs can be asked during the joint meeting in June 2000).

ACTION #AH/7: Mr. V. Niemi to write a liaison to SA WG2 on the assumptions of Network Elements being IP-aware.

5.4 Identification of SA WG3 CRs and LS to other groups that need to be discussed and approved at the SA WG3 plenary

This was not completed due to lack of time.

6 Close of meeting

The Chairman thanked the hosts for the meeting arrangements and delegates for their co-operation and hard work and closed the meeting.

Annex A: List of action points at the meeting

ACTION #AH/1: **All to contribute to update the draft Project Plan for input to the SA WG3 meeting.**

ACTION #AH/2: **Mr. R. Lubarsky to act as editor for the working document on MAP Security for Release 2000. To be produced by 2 June 2000.**

ACTION #AH/3: **Mr. P. Howard to draft a discussion document on the use of IPSec to secure GTP messages for the Joint meeting with CN in June 2000. To be completed by 2 June 2000.**

ACTION #AH/4: **Mr. D. Castellanos to produce a note to CN WG4. on MAP Security Layer 3 open issues.**

ACTION #AH/5: **Mr. P. Howard to manage discussion group on Protection Modes and TVP definition.**

ACTION #AH/6: **Mr. R. Lubarsky to manage discussion group on use of IKE for Layer 1, including any Liaison Statements to other groups which are needed. Draft liaison(s) to be completed by 24 June 2000 for discussion in SA WG3.**

ACTION #AH/7: **Mr. V. Niemi to write a liaison to SA WG2 on the assumptions of Network Elements being IP-aware.**

Annex B: List of documents to the meeting

Annex C: List of attendees