3GPP TSG SA WG3 Security — S3#20 **S3-010407**

16 - 19 October, 2001

Sydney, Australia

3GPP TSG SA WG3 Security — MAP Security ad-hoc **version 0.2**

13 September, 2001

Sophia Antipolis, France

Source: Secretary SA WG3 (M Pope)

Title: Draft report of the MAP Security ad-hoc meeting version 0.2

Document for: Information

1 Opening of the meeting

Due to the terrorist events which occurred on 11 September 2001, and the consequential disruption in flights, some delegates were unable to travel to the meeting. It was therefore agreed that all approved CRs at this meeting would be provided to the delegates who had registered for the meeting, in order to provide them with a chance to veto any CRs before presentation to TSG SA plenary for approval. It was agreed that the voting period would need to be short - and end of Monday 17 September was set as a deadline - the approved CRs to be sent out after this meeting (in the evening). Mr. Pope would then collect together the approved CRs for input to TSG SA #13.

2 Approval of the agenda

TD S3z010070 Draft agenda for SA WG3 meeting #19bis (MAP security). The draft agenda was approved.

3 Allocation of the input documents

Documents were allocated to appropriate agenda items.

4 Release 4 issues

4.1 Proposed CRs to 33.200

NOTE: It was agreed that all approved CRs at this meeting would be provided to the delegates who registered for the meeting for a chance to veto any CRs before presentation to TSG SA plenary for approval. It was agreed that the acceptance period would need to be short - and end of Monday 17th September was set as a deadline - the agreed CRs to be sent out after this meeting (in the evening). Mr. Pope would then collect together the approved CRs for input to TSG SA #13.

TD S3z010088 Proposed CR to 33.200-400: MAPsec Message Flow including extra SPD table. This Porposed CR, to add a new Annex of information flows and include required Security Policy Database (SPD) and Security Association Database (SAD) descriptions (based on the agreements on **TD S3z010084**), was discussed. A revised version was produced in **TD S3z0100120** (see below).

TD S3z0116 Mandate MAPsec vs Protected Message Table. This was provided by Hutchinson 3G UK, but a representative was not able to travel to this meeting. The contribution was discussed and was seen to be a complexity issue rather than a security issue. It was argued that the updating of the tables and distribution of Policy information could be done in a robust way by use of the KAC (for Rel-5), and for Rel-4 there were still other automation problems. It was agreed that the CR provided in **TD S3z0100120** would be the preferred solution. **TD S3z010120** was then agreed. **The above explanation will be added to the e-mail for acceptance procedure.**

An LS to CN WG4 was produced in **TD S3z0100121** to advise on the handling of errors returned by the MAPsec procedures. which was agreed (see AI 6 below) (to be sent for consideration as for CRs).

TD S3z010086 CR - discussed and modified with respect to discussion documents, and replaced by **TD S3z0100122** which was agreed.

TD S3z010095 CR - discussed - covered in part by TD122 - revised in **TD S3z0100123** (including the first part of **TD S3z010081**) and was agreed.

TD S3z010081 The sequencing of SA was transferred into **TD S3z0100123**. Further modifications were made to align with other agreed CRs (SPD parts) The remainder was modified and provided in **TD S3z010124** which was agreed.

TD S3z010073 CR agreed.

TD S3z010074 CR agreed.

TD S3z010078 CR Withdrawn. Considered useful and not harmful in Rel-4.

TD S3z010079 CR Withdrawn. Considered useful and not harmful in Rel-4.

TD S3z010080 CR Withdrawn - Covered by S3z010120.

TD S3z010090 Introduced by Siemens. Proposed that MAPsec Encryption Mode be based on counter mode described in NIST 800-XX. It was reported that this draft had been removed from the internet site, probably for additional changes (unknown by the group). It was also noted that ISO/IEC 10116 was also not stable, and was targeted for completion in 2003. After some discussion over the use of algorithm specs, it was decided to postpone this issue to SA WG3#20 meeting where the status of the algorithms could be reviewed. **The majority of those present at the ad-hoc meeting were in favour of using the NIST standard.** The CR could not be agreed as the NIST standard had not been finalised.

TD S3z010091 CR agreed.

TD S3z010094 CR updated in **TD S3z010125** agreed.

4.2 Message flows

TD S3z010084 Overview on MAP Security procedures. This was introduced by Ericsson. The main objective of this document was to define the mechanisms and flows for the protection of MAP signalling within 3GPP Rel-4. It also highlighted some open issues for discussion during S3#19. During the presentation it was noted that in 1c) "higher protocol" should be replaced by "MAP user". It was also noted that 4a) should read "MAPsec message" in place of "MAPsec traffic". It was also suggested that 4b) should be devided to clarify the option of choosing protection mode 0.

It was agreed that an LS should be provided to CN WG4 in order to check that the proposed mechanisms are acceptable in terms of impact on the MAP stage 3 specification. This was included in the LS in **TD S3z010121** (see agenda item 6).

The related CRs were provided in **TD S3z010087**, **TD S3z010088**

TD S3z010085 MAP security threats and policy requirements. This was presented by Siemens and discusses the use of cut-off dates for introduction of security features into the field. TSG SA#10 had asked SA WG3 to include a warning about the use of MAP security into their specifications. The inclusion of was provided in a proposed CR in **TD S3z010086**.

The fallback to unprotected mode had been noted as in need of contribution at SA WG3#18.

Common use of Protection levels for incoming/outgoing messages between operators. Proposed that an operator should use the same level of protection for all interconnected operators, at least for received traffic.

Use of a table to determine whether a signal requires protection or not to improve efficiency by allowing unprotected messages to be handled without all the security profile look-ups.

Protection groups and protection profiles: proposal to only allow the use of protection groups provided in the standard, and not allowing operators to define other groups. It also proposed to make protection profiles bi-directional for simplicity.

The related CRs were provided in **TD S3z010088**

4.3 Policy requirements 82

TD S3z010082 MAP security threats and policy requirements (Postponed S3-010354). This was covered by **TD S3z010085**.

4.4 Other Rel. 4 issues

5 Release 5 issues

5.1 Status of 33.800

TD S3z010096 MAPSEC Version 03 and Status This was presented by J. Arkko. After some discussion it was considered that the October meeting should be used to review the latest draft, and contributions were requested on this in order that comments can be provided to IETF, in order that they can finalise the document. Port numbers were considered in need of study. The attached DOI draft was noted.

TD S3z010072 Draft of 33.800 with MAPsec Rel5 material (Postponed S3-010302). There was no time to discuss this document, and the author was not available, so it was postponed to SA WG3#20.

5.2 MAPSEC DoI

TD S3z010075 The MAP Security Domain of Interpretation for ISAKMP (Postponed S3-010333 and postponed S3-010215).

TD S3z010076 Presentation on MAPSEC DOI Version -02 (Postponed S3-010335 and postponed S3-010221).

TD S3z010077 Comments on MAPsec DOI –02 Internet Draft (Postponed S3-010338 and postponed S3-010254).

5.3 Key management

TD S3z010083 Local Security Association Distribution (Postponed S3-010368).

5.4 Other Rel. 5 issues

6 Review of output documents

TD S3z010121 LS to CN WG4 on MAPsec error handling. This was agreed, and **TD S3z010120** was attached for transmission to CN WG4.

7 CRs were agreed for transmission to the list of registered delegates for checking.

7 AOB

8 Closing of the meeting

72, 83, 114, 115, 117 postponed.