3GPP TSG SA WG3 Security — S3#22 **S3-020004**

25 - 28 February 2002

Bristol, UK

3GPP TSG SA WG3 #21bis aSIP ad hoc **Tdoc** **version 0.0.1**
Antwerp, Belgium
31st January – 1st February 2002

Source: **SA WG3 Secretary**

Title: **Draft report of the meeting**

Document for: **Information**

1 Opening of the meeting (January 31st at latest 16:00)

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

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

2 Approval of the agenda and objectives of the meeting

TD S3z020001 Proposed agenda and objectives for aSIP ad-hoc meeting. This was presented by the Chairman. A new Agenda Item 4b: "Incoming LSs" was added and with this, the agenda was then approved.

Meeting objectives:

- The primary objective was to make progress on TS33.203v100 and prepare the specification for approval at SA#15.
- The secondary objective was to make progress on SIP signalling protection and discuss the two different options currently kept in the Annex of TS33.203v100.
- The third objective was to progress the discussion on ISIM taking into account the output from SA#14.

The objectives were agreed.

3 Allocation of documents to agenda items

Documents were allocated to their respective agenda items.

TD S3-020006, TD S3-020007, TD S3-020029, TD S3-020030 and TD S3-020031 for the SA WG3 meeting #22 (Bristol) were allocated in addition to those specifically provided to this meeting.

4 SA#14 report and status report of TS33.203v100

The parts of the draft report of SA#14 were considered for ISIM and IETF dependency issues.

TD S3z020032 aSIP-Access Security for IP-Based Services. This was presented by K. Boman, and provided the aims and expectations from the ad-hoc meeting, and the open issues remaining in TS 33.203.

The open issues still left at the end of the ad-hoc meeting would need to be seriously considered and contributed to for the SA WG3 meeting #22 (Bristol) in order to stabilise the document for approval at SA#15.

K. Boman was thanked for the presentation of his views on the way forward.

4b Incoming LSs

TD S3-020007 Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem. This was introduced by Lucent. There was nothing that could be done by the ad-hoc meeting, and so the LS was noted and would be further considered at the SA WG3 meeting.

TD S3-020029 Reply Liaison Statement on Prevention of Identity Spoofing in IMS. This was introduced by Hutchinson 3G UK. The solution 1 was not considered a good solution to the group, and after some discussion on the way forward, it was agreed to consider the Ericsson contribution in TD S3z020014 which provided a potential procedure:

TD S3z020014 On the use of KSI-IMS. this was introduced by Ericsson and proposed that the P-CSCF allocates and stores a new identifier each time the S-CSCF triggers an IMS-AKA procedure during the registration procedure. For clarification of the procedures, the draft of 33.203, provided in TD S3z020018 was used (in particular, section 7.3.1.1). It was suggested that the Public Identity may be needed so that the P-CSCF knows the destination SA. There was some discussion on the Mobile Terminated case, and further investigation on the impact of the availability of the Public Address/IMPU. The KSI-IMS solution described here could not be agreed upon at the ad-hoc meeting, and it was agreed that further investigation on protection against such attacks needs to be done. It was recognised that whether to send back the KSI or the IMPU was still an open issue.

TD S3z020026 LS S5-020003 (S1-011241) Packet Switched Streaming Service. This was introduced by Hutchinson 3G UK, and provided a scenario where the SA keys can outlive their intended lifetime, providing an opportunity for key compromise. **<RETURN?>**

It was agreed that a LS would be created for CN WG1 informing them that solution 2 was more acceptable to SA WG3 ad-hoc than solution 1. A. Escott agreed to produce this LS for e-mail approval on the SA WG3 list. (TD S3z020041). Schedule: Distribution to e-mail list for comment Monday 4 February. Comments following Monday 11 February - Revised version available Tuesday 12 February, for final e-mail approval Friday 15 February.

TD S3-020030 Liaison Statement (from CN WG1) on transportation of SIP session keys from S-CSCF to P-CSCF. This was presented by Vodafone. For the second point, it was agreed that a maximum of 3 re-authentication attempts was acceptable. For the final point, Ericsson contribution section 4 of TD S3z020009 was introduced:

> TD S3z020009 Results of a conference call with IETF ADs and SIP WG chairs regarding IMS security. Section 4: Key Transport. This was introduced by Ericsson and discussed. It recommended that an application layer mechanism be used to protect key transport (e.g. S/MIME or XML Digital Signatures). It was generally accepted that the IETF had rejected the use of EAP for AKA, which implies that SA WG3 need to find another mechanism if the IETF protocols are to be used. Hop-by-hop protection was still considered the method used in SA WG3.

It was agreed that a LS to CN WG1 was needed to confirm the maximum of 3 re-authentication attempts, corresponding to the action in their LS, which P. Howard agreed to draft this, for SA WG3 e-mail approval (TD S3z020039). Schedule: Distribution to e-mail list for comment Monday 4 February. Comments following Monday 11 February - Revised version available Tuesday 12 February, for final e-mail approval Friday 15 February.

TD S3-020031 Liaison Statement on "Prefix allocation for IPv6 stateless address auto-configuration". This was introduced by the Chairman, and delegates were asked to read this through to analyse potential impacts on security with an aim to closing the open issue on privacy at the SA WG3 meeting #22 (Bristol). The LS was then noted.

TD S3z020033 Liaison Statement on ISIM for support of IMS. This was introduced by Vodafone, along with the attached presentation slides. SA WG3 were asked to confirm the requirement of up to 4 simultaneously active applications. It was considered that the security implications may come about if an application is temporarily closed in order to activate a parallel IMS subscription application, which is considered equivalent as removal of the (U)SIM. It was agreed that for multiple subscriptions, each would need independent data and applications. It was agreed to list the security issues identified in a response LS to T WG3 including pointing out that no compelling security reason implies the ruling out of Case 1a. **C. Blanchard agreed to create a draft LS for consideration at the SA WG3 meeting #22 (Bristol) in TD S3-020033.**

TD S3-020010 LS (from RAN WG2) on START value calculation. Ericsson had provided a draft response to this in TD S3z020035.

TD S3z020035 [draft] Response to the LS from RAN2 on START value calculation (response to S3-020010). It was agreed that this response would be discussed and approved over e-mail on the SA WG3 list, led by D. Castellanos. Schedule: Distribution to e-mail list for comment Monday 4 February. Comments following Monday 11 February - Revised version available Tuesday 12 February, for final e-mail approval Friday 15 February.

5 IETF

5.1 Report from the IETF meeting in December (Salt Lake City)

TD S3z020021 IETF #52 status report. This was introduced by Ericsson. The IETF has proposed that 3GPP define a new body to transport 3GPP-specific information which would bring greater independence from the IETF work. This would result in a larger SIP messages. The Bis version of RFC SIP is being produced and a serious look at the security parts in Bis is being taken in order to ensure that the IESG passes the standard. The report was then noted.

5.2 3GPP related IETF drafts

TD S3z020034 Correspondence from CN Chairman. This is the report of the IETF#52 meeting from the TSG CN Chairman and was introduced by Ericsson. An RFC number is expected to be allocated on 7 March for SIP Bis, which will allow TSG CN to add the references into their specifications at the Plenary for Rel-5 specification finalisation. EAP for AKA was not considered by the IETF as stable enough and other, simpler mechanisms (e.g. HTTP Digest) could be used. This letter was then noted.

TD S3z020009 Results of a conference call with IETF ADs and SIP WG chairs regarding IMS security. This was presented by Ericsson. SA WG3 were asked to consider the information provided and to make decisions regarding progressing 33.203, in particular to decide if the suggested protocols satisfy the security requirements and any issues this raises, in order to provide early guidance to CN WG1 and CN WG4. Ericsson proposed the use of HTTP Digest for AKA, as recommended by the IETF. Also, the proposal from the IETF meeting #52, that 3GPP define a new body was recommended as a good way forward by Ericsson, which could solve the Key transport issue. It was reported that CN WG1 are currently working on the development of a new body, and this should be available for June 2002. The development of this new body, for transport, was considered a CN WG1 issue.

It was concluded that the removal of EAP from the requirements in 33.203 would remove the implication for development of Stage 3 EAP work. It was agreed to recommend this course of action to SA WG3 meeting #22 (Bristol) and also to recommend to CN WG1 to follow the IETF recommendations for AKA transport using HTTP Digest. It was decided to draft an LS to CN WG1 and CN WG4 informing them of the changes agreed in the ad-hoc for approval by e-mail on the SA WG3 list. D. Castellanos (Ericsson) agreed to draft this LS (TD S3z020040). Schedule: Distribution to e-mail list for comment Monday 4 February. Comments following Monday 11 February - Revised version available Tuesday 12 February, for final e-mail approval Friday 15 February.

End to end security between S-CSCF and P-CSCF: It was considered that this is not required, as the security will be provided by NDS/IP in the 3GPP context.

6 SIP signalling protection

6.1 Integrity

TD S3z020008 Reflection attacks in IMS. This was introduced by Vodafone and proposed to add a direction bit to the integrity check to provide robust and future-proof protection against reflection attacks.

TD S3z020030 Anti-Replay Protection for the SIP-level Security Solution. This was introduced by Nortel Networks and proposed adjustments to the behaviour of the IMS UE and P-CSCF to accomplish anti-replay protection at the SIP-level. (Comments from Siemens to this contribution were provided in TD S3z020037 and proposed enhancement, taking later agreements in the IETF meeting into account, was included TD S3z020042).

TD S3z020042 Updates from IETF to SIP-Level Solution for IMS Integrity. This was introduced by Nortel Networks and updates the information given in TD S3z020030 to "*reflect the agreements reached since IETF#52 among those parties that seek to enhance HTTP Digest such that it is a viable solution mechanism for SIP message integrity in the IMS*".

It was commented that replay protection mechanism which does not introduce extra messages / round trips in the call set-up would be desirable, and such a mechanism should be investigated.

TD S3z020037 Comments and questions on the revised anti-replay protection scheme for the SIP level integrity solution in TD S3z020030. This was introduced by Siemens and outlined the required clarifications and open issues, and questioning some of the points in TD S3z020030.

Nortel Networks agreed that some of the issues raised had not been considered by the IETF editing group, and undertook to take the comments into account and try to bring a finalised version to the SA WG3 meeting #22 (Bristol). It was hoped that the draft RFC would be publicly available by then (i.e. it is expected to be submitted to IETF in advance of their next meeting) and that some form of Profiling could be done for 3GPP requirements. All delegates were asked to make an effort to ensure early availability of the RFC.

TD S3z020011 Unprotected re-registration during SA lifetime. This was introduced by Nokia and discussed whether or not unprotected re-registration should be permitted. Vodafone had provided a contribution which conflicted with this proposal in section 7 of TD S3z020006 which was considered.

> TD S3z020006, section 7: This was introduced by Vodafone and suggests that the network should clear the registration if the integrity check repeatedly fails at the P-CSCF (in the case of a lost SM8). Recovery can be achieved only by treating the registration as a new registration and performing authentication.

It was generally concluded that there may be a need to allow unprotected re-registrations, but that protection against associated attacks requires further examination. Suitable policies for handling re-registration requests from both P-CSCF and UE needs to be put in place.

Delegates were asked to continue this discussion over e-mail in order to come to a generally acceptable solution for the SA WG3 meeting #22 (Bristol). **A. Escott was asked to lead this discussion based upon the contributions in this ad-hoc on the subject**.

TD S3z020016 On integrity protecting SIP-signalling in IMS: See discussion below.

TD S3z020010 Primary choice between IPsec and SIPsec: See discussion below.

TD S3z020036 Integrity protection for SIP messages in the IMS at network or application layer? See discussion below.

> Discussions on moving SIP security into the main body of 33.203 and leaving the IPSec solution in the Annex for a fall-back solution took place. The progress of the SIP security draft was questioned, as there did not seem to be any visible progress (indeed it had been withdrawn into a editing group in the IETF with a reported target for completion of the draft SIP Bis in February 2002, in order to meet the submission deadline for the IETF. As there were differences of opinion on this from different companies, **it was decided to leave this decision until the SA WG3 meeting #22 (Bristol) in order to base the decision on the SA WG3 "preferred solution" upon progress on the two drafts made by that time.**

TD S3z020017 Requirements on SA_ID. This was postponed to the SA WG3 meeting #22 (Bristol). Delegates were asked to consider this in the meantime and comment on e-mail if necessary.

TD S3z020029 Set-up Procedures for the SIP-level Security Solution. This was postponed to the SA WG3 meeting #22 (Bristol). Delegates were asked to consider this in the meantime and comment on e-mail if necessary, in particular on the proposed use of elements for the SA.

6.2 Confidentiality

TD S3z020018 Editorial changes to TS33.203v100.

TD S3z020019 The need for confidentiality protection for the first/last hop. This was introduced by Ericsson and discusses the provision of confidentiality for the first and last hop for the Rel-5 timeframe. It proposes a working assumption that SIP signalling is only integrity protected for Rel-5 and provided a roadmap for SA WG3 to follow. It also proposed that the Security Mode set-up procedure should still take encryption into account, utilising NULL encryption for Rel-5. The assumption for the use of S/MIME in Rel-6 was questioned. It was decided that such discussions need to take place at a later date and any assumptions made by SA WG3 at this time would not include the use of a S/MIME solution. It was concluded that confidentiality is not needed for SIP signalling between the UE and P-CSCF for Rel-5, since the USer Plane is not confidentiality protected. This will be sought for future Releases.

TD S3z020020 SIP layer confidentiality between UA and P-CSCF. This was covered by discussions on TD S3z020019 and was noted.

7 ISIM

A Liaison Statement from T WG3 was provided in TD S3z020033 which was dealt with under agenda item 4.

8 Further contributions to TS33.203v100

TD S3z020004 Pseudo-CR to 33.203 v1.0.0: Incorporation of Integration Guidelines for R5 into TS33.203. This was postponed to the SA WG3 meeting #22 (Bristol). Delegates were asked to consider the usefulness of the inclusion of integration guidelines material in 33.203, for Rel-5.

TD S3z020006 Proposed changes to 33.203. (Section 7 of this contribution was considered under agenda item 6.1 with TD S3z020011). This was postponed to the SA WG3 meeting #22 (Bristol). Delegates were asked to consider this in the meantime and comment on e-mail if necessary.

TD S3z020007 Maximum number of requested authentication vectors. This was introduced by Vodafone and discusses the maximum number of Authentication Vectors that can be requested and stored. It discussed the issue and suggested some preliminary maximum values. The meeting did not feel that this required specification, but if CN WG4 requested this for any technical reason then this would be considered and decided upon in SA WG3 and then communicated to CN WG4.

TD S3z020027 Need for section 7.3.3. This was postponed to the SA WG3 meeting #22 (Bristol) due to lack of time.

TD S3z020031 Network Handling of Untrusted IMS Clients. This was briefly introduced by Nortel Networks and recommends SA WG3 to consider the threats posed by untrusted IMS clients and discuss the mitigation solutions to standardise. Delegates were asked to consider these issues and what, if anything, can be done for Rel-5 in the time frame.

9 AOB

There were no contributions under this agenda item.

10 Closing of the meeting (February 1st at 16:00)

Documents not dealt with at the meeting, due to lack of time. Postponed to Bristol meeting:

TD S3z020006 Proposed changes to 33.203. (Section 7 of this contribution was considered under agenda item 6.1 with TD S3z020011).

TD S3z020017 Requirements on SA_ID.

TD S3z020029 Set-up Procedures for the SIP-level Security Solution.

TD S3z020004 Pseudo-CR to 33.203 v1.0.0: Incorporation of Integration Guidelines for R5 into TS33.203.

TD S3z020006 Proposed changes to 33.203.

TD S3z020027 Need for section 7.3.3 (in 33.203).

<CHECK FOR ANY OTHERS NOT FULLY DEALT WITH>

The Chairman thanked Alcatel for providing the arrangements for the ad-hoc meetings, thanked delegates for their co-operation and work during the meetings and closed the meeting.