3GPP TSG SA WG3 Security — S3#22 **S3-020002**

25 - 28 February 2002

Bristol, UK

3GPP TSG SA WG3 Security — S3#21 **version 0.0.5**

27-30 November 2001

Sophia Antipolis, France

Source: **Secretary 3GPP TSG-SA WG3**

Title: **Draft Report of meeting #21**

Document for: **Comment**

Contents

1 Opening of the meeting

Michael Walker, SA WG3 Chairman opened the meeting and welcomed delegates to Sophia Antipolis, France. Due to other commitments of the Chairman, the meeting was Chaired by M. Walker from 27-28 November, and by the Vice Chairman, V. Niemi from 29-30 November.

2 Meeting objectives and approval of the agenda

The objectives and priorities for the meeting were outlined by the Chairman:

To complete all necessary work for the December 2001 TSG SA meeting #14:

- To complete IMS Security Architecture document TS 33.203, to be presented to TSG SA#14 for information;
- To complete the NDS/IP security document TS 33.210, to be presented to TSG SA#14 for information
- To agree CRs to Rel-4 of MAP security TS 33.200 and to stabilise the Rel-5 version to be presented to TSG SA#14 as a document showing the expected content of Rel-5 for information (CRs to be created for approval at TSG SA#15).

Therefore the priorities were to start the meeting with the approval of the report from SA WG3#20, then to extract the relevant LSs on the above Specifications and deal with these first (sections 7.1 to 7.3).

TD S3-010562 Draft Agenda for meeting #21. The draft agenda was introduced by the Chairman and approved. (Note, some additional agenda items were included later, as documents were found to need a separate item, this is reflected in the section numbering of this report).

3 Assignment of input documents

The available documents were assigned to their respective agenda items, taking into account the urgent items to be dealt with early in the meeting.

4 Reports from 3GPP SA3 meetings

4.1 S3#20, 16-19 October 2001, Sydney

TD S3-010563 Draft report of meeting #20. The report was reviewed and minor changes were made to the report and the actions in the report reviewed. The final version will be placed on the FTP server as version 1.0.0.

4.2 Joint meeting with T3, 26 November 2001, Sophia Antipolis

V. Niemi, the Chairman of the joint session with T WG3, provided a verbal report in advance of the written report being made available (still in need of editing). He introduced the output LS from the joint session, which needed speedy transmission to the groups meeting the same week in Cancun. This was provided in TD S3-010642 "Draft Response LS on IMS identifiers and ISIM and USIM". It was stressed that this was a result of the joint session, and had not been discussed fully by SA WG3. This was discussed and modified in TD S3-010647 which was approved and distributed during the meeting.

5 Reports and liaisons from other groups

5.1 3GPP SA3 lawful interception sub-group

TD S3-010613 Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #5/01 on lawful interception Aspen, Colorado 30 October – 1 November 2001. This was presented by B. Wilhelm and outlined the important issues and **reported that the LI group no longer had a Chairman** due to the current Chairman resigning at the last meeting and asked **companies to consider providing candidates** for this important position.

TD S3-010609 3GPP TS 33.108 (Version 0.2.1). This was provided for information and noted. Delegates were asked to check the draft TS and provide comments and contribution to the LI group.

TD S3-010612 Proposed CR to 33.107: Source of PDP context initiation (Rel-5). This CR was approved. Note: It was discovered after the meeting that this CR had already been approved at meeting#20, TD S3-010518 (corresponding to the Rel-4 CR in TD S3-010517).

TD S3-010610 Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-5). This was withdrawn by LI group pending production of corresponding Rel-4 and Release 1999 CRs.

TD S3-010611 Revised Work Item Description (revision of SP-000309). This Rel-4 WI was approved.

TD S3-010614 Overview of differences and gaps of Lawful Interception between legacy telecommunication and multimedia call scenarios (presentation). This was presented by B. Wilhelm. It provided a good overview of the differences between legacy systems and multimedia systems and current problems with intercepting in multimedia scenarios. These issues were brought to the attention of SA WG3 in order to consider that changes may be required to meet lawful interception requirements in the future. Delegates were invited to study the issues and consider directions to provide solutions. The presentation was then noted.

5.2 3GPP SA plenary

There had been no meeting of TSG SA since the last SA WG3 meeting.

5.3 3GPP working groups

TD S3-010573 Liaison Statement on Security of Rel5 IP Transport in UTRAN. This was presented by Nokia and asked SA WG3 to confirm the working assumption of RAN WG3 that the Rel-5 IP UTRAN transport networks can be seen as closed environments. A contribution related to this was provided by Nokia in TD S3-010618 "*Proposed Changes to 33.210 about the scope*" which was considered. It implied that the Rel-5 IP UTRAN was not a closed environment and that SA WG3 will work on providing the necessary security. It was suggested that as the protection of the Iu interface had been out of the scope for Rel-5 until now, that there was not time to include IP UTRAN protection for Rel-5 at this late date. The proposal in TD S3-010618 was discussed and comments included in an updated version provided in TD S3-010656 which was agreed. Nokia agreed to draft a LS in response to RAN WG3 was provided in TD S3-010657 which was updated in TD S3-010662 and was approved (transmitted immediately for RAN WG3 consideration at their meeting the same week).

TD S3-010564 Liaison Statement on AMR-WB and Legal Interception. This LS was intended for the LI group and was **forwarded to the LI group for handling at their next meeting**.

TD S3-010565 LS to GSM-A TWG/SERG “regarding User Profile”. This was presented by the Chairman and discussed to check the security requirements on the GUP draft. It was agreed that more information on the GUP should be sought:

Action 21/1: Colin Blanchard to contact the editor of the GUP draft to determine the background and the rationale for the requirements in the security section (section 6)

Action 21/2: ~~Steward~~ Stuart Ward to invite Paul ~~Henry~~ Amery to give SA WG3 a briefing on GUP work.

TD S3-010568 LS on Message size limitation for f9 algorithm. It was clarified that SA WG3 had specified the upper limit of bits for f9 processing after consultation with RAN WG3/RAN WG2 on the maximum message size. There is no reason for this limitation from a cryptographic point of view. It had been verified by SAGE that removing this limit did not adversely affect the cryptographic aspects of f9.

The SAGE representative, Per Christoffersson, confirmed that removal of the upper limit of the number of bits had been checked in ETSI SAGE and there was no problem found.

The CR to 33.105 (TD S3-010187) was endorsed by ETSI SAGE earlier and the ETSI SAGE Chairman had sent a message to SA WG3 Secretary and the SAGE Representative, stating that there was no foreseen problem with this CR. The LS was noted and a response LS confirming this was provided in TD S3-010682 "LS to RAN WG2: Response to S3-010568 confirming changes requested". This LS reviewed and approved.

TD S3-010680 (replacement of TD S3-010601) Proposed CR to 35.201: Correct the maximum input message length for f8 and f9 (Rel-99). This CR was updated in TD S3-010689 and was approved.

TD S3-010681 (replacement of TD S3-010602)Proposed CR to 35.201: Correct the maximum input message length for f8 and f9 (Rel-4). This CR was updated in TD S3-010690 and was approved.

TD S3-010571 LS from T WG2: VASP MMS Connectivity. This was presented by the Chairman and requested guidance and information about the existence for plans for end-to-end encryption of traffic between terminals and external applications or encryption of links between MMS relay/Server and a VASP or Gateway. The reply would depend on the type of traffic, and if NDS/IP traffic, then this may be covered by the NDS/IP security but other traffic types could not be guaranteed to be secured by the normal 3GPP operator-operator security, which is based on a known trust model. Lawful interception issues were also identified with the introduction of external application providers using encryption for protection. The LI group were asked to consider this and the LS was forwarded to them for their next meeting (Berthold Wilhelm to take this to the meeting). A reply LS with the requested guidance from SA WG3 was provided in TD S3-010683 which was updated editorially in TD S3-010698 which was approved.

TD S3-010572 LS from RAN WG3: WID: AMR-WB Speech Service – Core Network Aspects. This was presented by Vodafone, and was provided for information to SA WG3. The LS was noted.

TD S3-010574 LS to CN WG5: Comments on TS 29.198. This had been approved by e-mail after meeting#20 and sent to CN WG5 and was noted. A response was received in TD S3-010661 which was introduced by the Chairman. CN WG5 informed SA WG3 that they intend to enhance the encryption algorithm data type, to include more recent encryption algorithms. CN WG5 asked SA WG3 to review and approve the proposed updates in the attached CR. The CR was reviewed and it was considered that a note should be added after the data type definition table stating that the P_DES_56 and ~~P_DES_128~~ R_DES_128 algorithms are no longer considered adequate for use. Other problems were also recognised, and it was considered that the should be updated to include the requirements intended by SA WG3 in their original LS. A response LS was produced in TD S3-010685 informing CN WG5 that the CR is not acceptable to SA WG3 as it is incomplete and does not fully reflect the requirements intended in SA WG3 LS to them. Companies who are in the list of supporting companies for the related WI were requested to ensure that this is progressed before the next SA WG3 meeting, by communicating with CN WG5 colleagues. C. Blanchard and B. Owen agreed to brief the CN WG5 delegates from their companies. This LS was updated in TD S3-010696 and was approved.

P. Howard agreed to set up an e-mail discussion on this in order to produce a proposal for a CR to 29.198 for CN WG5. The discussion should take TD S3-010506 from meeting #20 as background material. It was agreed that the e-mail discussion closed on 18 January 2002, final comments on the output proposed CR by 25 January 2002.

Action 21/3: P. Howard to set up an e-mail discussion on this in order to produce a proposal for a CR to 29.198 for CN WG5.

TD S3-010575 LS from SA WG2 on Enhanced user privacy for location services. This was presented by Nokia and asked SA Wg3 to study the Enhanced user privacy for location services Draft and provide comments and feedback to SA WG1 and SA WG2. It was agreed that this would need some time to study and an e-mail discussion group should be set up.

Action 21/4: ~~Steward~~ Stuart Ward to start off an e-mail discussion on Location Services Privacy and report back to SA WG3 meeting #22.

TD S3-010587 Liaison Statement from SA WG1 on 3GPP Generic User Profile Stage 1. This was presented by the Chairman and was noted.

TD S3-010590 Liaison Statement from SA WG1 on Revised Push Service Stage 1. This was presented by the Chairman and asked SA WG3 to review the attached updates to the draft specification and provide comments and updates to the security parts. It was proposed that the stage 1 should be concentrated on before looking at the stage 2 requirements to ensure that the basis is correct for the requirements. A response LS to SA WG1 and SA WG2 was provided in TD S3-010686 which was updated in TD S3-010700 and approved.

TD S3-010591 Reply from SA WG1 to LS SA WG2 on “Privacy Override Indicator”. This was presented by Nokia and asks SA WG3 to consider the potential security aspects if Privacy Override is applied between countries. It was decided to forwarded this LS to the LI group as it is also applicable to Lawful Interception. From the Emergency Services viewpoint, further discussion in the e-mail debate run by ~~Steward~~ Stuart Ward in the action 21/4 above (re: TD S3-010575). A response LS was provided to inform SA WG1 that the issue required further discussion was provided in TD S3-010687 which was updated in TD S3-010697 and was approved.

TD S3-010592 Liaison Statement from SA WG1 on DRM. This was presented by the Chairman and informs SA WG3 that SA WG1 are working on DRM and would like to work with SA WG2, SA WG3 and SA WG4 on DRM requirements. The LS was noted.

TD S3-010594 Answer to LS on requirements on Multimedia Broadcast/Multicast Service. This was presented by the Chairman and was copied to SA WG3 for information. It was commented that the use of ciphering and integrity protection on broadcast messages would need consideration by SA WG3. The draft of TS 22.146 was considered in the previous meeting in TD S3-010418 where it was noted.

Action 21/5: A. Escott agreed to check the draft TS 22.146 and determine if any input is needed and report back to the next SA WG3 meeting.

The LS was then noted.

TD S3-010598 Mail received from TSG CN Chairman on IETF Dependencies table. This was presented by Ericsson and informed 3GPP members of a table to track 3GPP dependencies on IETF documents. The table was attached and briefly checked. Item 32 was marked as "Nice to have" which was taken to mean that the Rel-5 work could continue without the finalised document. Delegates were asked to review the document and contact Stephen Hayes (TSG CN Chairman) with any errors or omissions. The contribution was then noted.

5.4 Others (e.g. ETSI SAGE, ETSI MSG, GSMA, TIA TR-45)

SAGE: Per Christoffersson reported no developments in ETSI SAGE for 3GPP related work since the previous meeting.

GSMA: C Brookson the Chairman of the GSMA SG gave a verbal report. The SG is discussing items including security for GPRS, Wireless LANs and M-Commerce. It was noted that the GSMA SG had supported the encryption indicator for 3GPP (see TD S3-010597).

COMP128 now exists in three forms:

- COMP128-1 is the original version, subject to the well-known attacks;
- COMP128-2 is the variant introduced which overcomes the problems of COMP128-1;
- COMP128-3 is the variant that produces a 64-bit key. No known infrastructure issues now exist for the support of a 64-bit key.

It is hoped that COMP128-4 will be introduced sometime next year, and it will be similar to 3GPP MILENAGE.

A5/3: TD S3-010677 Approval of A5/3 formally by SA WG3. 3GPP coordination committee and 3GPP and GSMA lawyers had come to agreement and the design of A5/3 can now go ahead. SA WG3 were asked to approve the development of A5/3 and record it in the minutes of the meeting to allow the development to be formally carried out. It was clarified that KASUMI would be a wrapper of the A5/3 algorithm, so A5/3 is a variant based on KASUMI. **SA WG3 formally approved the development of A5/3 by ETSI SAGE.**

It was noted that A5/3 should be an open process, should be based on KASUMI with as little change as possible, and the intention was that it should support GPRS and EDGE.

The expected timescale was reported as 6 months from start of development, which is set for February 2002.

TD S3-010597 Cipher indicators and selection options in UMTS. This was presented by C. Brookson and provided the GSMA view on rejection of non-ciphered connections as default operation. This was in line with the SA WG3 approved CR in TD S3-010679, and the document was noted.

SCP: TD S3-010569 Liaison Statement on Technical Solution for Prepaid Cards Using Smart Cards with Real-Time Clock. SCP asked GSMA SCAG for views on charging capabilities in UICC. This was provided to SA WG3 for information, discussed briefly and noted.

TD S3-010621 Response to liaison from IP Cablecom on LI. **This was intended for the LI group for information and was forwarded to them for their next meeting**.

AHAG: G Rose gave a verbal report on developments of relevance to SA WG3 in AHAG. It had been decided to create a new 3GPP2 S-WG4. AHAG have decided to keep 3GPP2 S-WG4~~2~~ in the loop but not to hand over the control of the Joint Control documents between AHAG and SA WG3.

Joint meetings with AHAG were hoped for and the next S-WG4 meeting is being held in Newport, CA and cannot be moved to the location of the AHAG/SA WG3 meeting in Victoria. Low attendance from AHAG is therefore expected at the joint meeting.

6 Technical specifications and reports

6.1 Security architecture (TS 33.102)

No specific contributions were received on this agenda item (see CR to 33.102 under agenda item 7.5)

6.2 f8 and f9 specification (TS 35.201)

No specific contributions were received on this agenda item (see CRs to 35.201 under agenda item 5.3)

6.3 MAP security Rel-4 (TS 33.200)

TD S3-010658 (revision of TD S3-010606) Proposed CR to 33.200: Removing the Sending PLMN-Id from Security Header (Rel-4). This was presented by Hutchison 3G UK, and had been postponed from meeting#20 (TD S3-010471). This CR was approved. A LS to CN WG4 was produced to inform them of this in TD S3-010671 which was approved.

~~TD S3-010643 Use of Push vs Pull Mechanisms in local SA distribution. This was presented by Alcatel and elaborates on the pros and cons of each possible approach for Push/Pull mechanisms, to show that the best solution is to adopt a default Push mechanism, supplemented by extensions for exceptional cases.~~ ~~**The proposal was adopted as a SA WG3 working assumption**.~~

~~TD S3-010637 SA distribution mechanism for the Ze interface. This was presented by Siemens and proposed an "extended" push model for MAPsec SA distribution.~~

~~**General requirements related to SA distribution over Ze:** The general requirements given in the document were generally agreed by SA WG3. These requirements should be transmitted to TSG CN, with the remark that the security protocols have already been developed (assuming it is IP-based). It was agreed to include these requirements in the specification and attach the specification to the LS. TheLS was provided in TD S3-010672 which was reviewed and clarified in TD S3-010692 which was approved.~~

~~**NOTE: If the updated MAPsec Rel-5 draft is available in time, then M Pope to input to TSG CN#14 to support this LS.**~~

~~**Proposed SA distribution procedures: 'Extended' Push mechanism:** There was some concern on the performance aspects of SA distribution using the mechanism. This was outside the scope of security requirements, and should be considered by other groups. It was agreed that the mechanism would be included in the MAPsec document and other groups could comment on the performance aspects if necessary.~~

~~TD S3-010648 Comments on TS 33.200 R5 v0.1.0. This was provided by Alcatel. It was noted that the comments had been written to an earlier version of the draft and some had already been addressed in the present version. The changes were reviewed and explained and the relevant modifications should be included in the MAPsec document by the rapporteur.~~

~~It was clarified that the Rapporteur will provide an updated document for presentation to TSG SA#14 to provide information of the expected content of Rel-5, and official Rel-5 CR(s) would be approved in time for TSG SA#15 (March 2002).~~ ~~**MOVED TO 7.1**~~

TD S3-010635 Protection Profiles Version Identification. This was presented by Siemens Atea and proposes the addition of a new identifier for Protection Profiles. The addition of a PPVI was proposed to allow Protection Groups (PGs) to be changed in different Releases in an Application Context way. Each Release may require different PGs to be added, which would be difficult without this identifier. Clarification on the meaning of MAP-NE versions was requested and the author agreed to do this in an associated proposed CR, for further discussion. This proposed CR was provided in TD S3-010688. It was noted that this proposed a Rel-4 (Category F) change to add the new Identifier. This was modified slightly to PPRI and provided in TD S3-010691 which was approved.

SHA-256: It was reported that this is only Draft at present and only has 96 bits. The IETF Rapporteur clarified that the SHA-256 is defined in the same internet draft as AES encryption, but that SHA-1 would also be acceptable. It was also clarified that this is only used for HMAC and SHA-256 has no advantage over SHA-1. The meeting agreed that SHA-1 should be chosen. The Rapporteur agreed to update the document according to agreements made here (including any agreement on TD S3-010635 proposal for PPVI) and submit the draft to the IETF.

TD S3-010607 Proposed CR to 33.200: Completing the specification of a MAPsec SA (Rel-4). This was presented by Hutchinson 3G UK, was modified in TD S3-010693 to clarify the "consequences if not approved" and the CR was approved.

7 Work items

7.1 MAP security Rel-5 (draft TR 33.800, MAPsec DoI)

TD S3-010608 Update on changes to MAPsec Release 5. This was presented by the MAPsec Rapporteur (Hutchinson 3G) and described the changes made to the Rel-5 specification. It was commented that the text under section 7 was redundant and that some MAP DoI specifications had been lost in the editing. This will be corrected by the Rapporteur. The contributions on MAP Security were then dealt with and the Rapporteur agreed to update the specification with agreed changes.

TD S3-010615 draft-arkko-map-doi-04: The MAP Security Domain of Interpretation for ISAKMP. This was presented by the IETF liaison Rapporteur (Ericsson). SHA-256 had been chosen for the AES encryption and SA WG3 were asked to confirm the acceptance of this. The contribution from Siemens in TD S3-010635 also needed decision for input to the MAP DoI (see below). The Port number needed to be fixed at some time, it was reported that receiving port numbers did not appear to present any problems.

~~TD S3-010635 Protection Profiles Version Identification. This was presented by Siemens Atea and proposes the addition of a new identifier for Protection Profiles. The addition of a PPVI was proposed to allow Protection Groups (PGs) to be changed in different Releases in an Application Context way. Each Release may require different PGs to be added, which would be difficult without this identifier. Clarification on the meaning of MAP-NE versions was requested and the author agreed to do this in an associated proposed CR, for further discussion. This proposed CR was provided in TD S3-010688. It was noted that this proposed a Rel-4 (Category F) change to add the new Identifier. This was modified slightly to PPRI and provided in TD S3-010691 which was approved.~~

~~SHA-256: It was reported that this is only Draft at present and only has 96 bits. The IETF Rapporteur clarified that the SHA-256 is defined in the same internet draft as AES encryption, but that SHA-1 would also be acceptable. It was also clarified that this is only used for HMAC and SHA-256 has no advantage over SHA-1. The meeting agreed that SHA-1 should be chosen. The Rapporteur agreed to update the document according to agreements made here (including any agreement on TD S3-010635 proposal for PPVI) and submit the draft to the IETF. **MOVED TO 6.3**~~

TD S3-010695 Mapping of Ze-interface information onto the Zd-Interface. This was presented by Siemens Atea and proposes text to be included in TS 33.200 Rel-5. An error was noted in the added text to section 5.6.1, which should read: "The KAC shall **not** use the Key Length Attribute of the SA for IKE phase 2 as this information is implicitly available for the Partner KAC via the used TransFormID".

This contribution was agreed and the rapporteur agreed to try to include this information under section 7 of TS 33.200 Rel-5.

TD S3-010643 Use of Push vs Pull Mechanisms in local SA distribution. This was presented by Alcatel and elaborates on the pros and cons of each possible approach for Push/Pull mechanisms, to show that the best solution is to adopt a default Push mechanism, supplemented by extensions for exceptional cases. **The proposal was adopted as a SA WG3 working assumption**.

TD S3-010637 SA distribution mechanism for the Ze interface. This was presented by Siemens and proposed an "extended" push model for MAPsec SA distribution.

General requirements related to SA distribution over Ze: The general requirements given in the document were generally agreed by SA WG3. These requirements should be transmitted to TSG CN, with the remark that the security protocols have already been developed (assuming it is IP-based). It was agreed to include these requirements in the specification and attach the specification to the LS. TheLS was provided in TD S3-010672 which was reviewed and clarified in TD S3-010692 which was approved.

NOTE: If the updated MAPsec Rel-5 draft is available in time, then M Pope to input to TSG CN#14 to support this LS.

Proposed SA distribution procedures: ‘Extended’ Push mechanism: There was some concern on the performance aspects of SA distribution using the mechanism. This was outside the scope of security requirements, and should be considered by other groups. It was agreed that the mechanism would be included in the MAPsec document and other groups could comment on the performance aspects if necessary.

TD S3-010648 Comments on TS 33.200 R5 v0.1.0. This was provided by Alcatel. It was noted that the comments had been written to an earlier version of the draft and some had already been addressed in the present version. The changes were reviewed and explained and the relevant modifications should be included in the MAPsec document by the rapporteur.

It was clarified that the Rapporteur will provide an updated document for presentation to TSG SA#14 to provide information of the expected content of Rel-5, and official Rel-5 CR(s) would be approved in time for TSG SA#15 (March 2002).

7.2 IP network layer security (draft TS 33.210)

TD S3-010582 NDS/IP suggestions. This was presented by the Telenor and provides comments based on the report of SA WG3 meeting#20 report and the current draft of 33.210. The suggestions were discussed as follows:

1) To keep TS 33.210 NDS/IP as a framework for use of IPsec in the UMTS core network. It was proposed that this should be designed as a building block but in such a way that SA WG3 can keep control of the security. A~~n inf~~ normative annex on the use of the security protocol could be added in order to keep the control over the protocol within SA WG3. GTP-C was identified as a protocol which should be moved in this way. SA3 decided to keep profiling information about the protocols to be protected by NDS/IP in normative annexes in TS 33.210.

2) Support for GTP-U and GTP Release 97/98 ? Contribution TD S3-010617 "*Proposed changes to 33.210 about protecting GTP-U*" related to this and was discussed. It was recognised that there is no requirement for SA WG3 to protect GTP-U and the proposal adds a recommendation to protect GTP-U over public hops (as an operator option). After some discussion over the implications of this to the NDS/IP draft, the changes proposed in this contribution were not accepted. It was suggested that the protection of GTP-Rel97/98 should be purely informative (as this could not be mandated and the protection would need to extend to GTP-U for these systems as the GTP-C is not discernable). The use of NDS/IP for GTP-U protection was considered possible and it was decided to return to this. This was raised again under the review of the updated draft TD S3-010670 where the protection of GTP-U using NDS/IP was mentioned as possible and left as outside the scope of the specification in a note.

3) Clause 5.3.1: ~~Potential protection of~~ IP payload compression ~~which~~ is currently disallowed. There was a suggestion to allow IP payload compression again and SA WG3 accepted to remove clause 5.3.1 and thereby in effect allow IP payload compression.~~This suggestion was withdrawn by the author.~~

4) SEG discovery function: This was for Rel-6 and should be included in the Rel-6 update.

5) Minor Clarification on IKE: This was accepted.

6) This was for Rel-6 and was postponed.

TD S3-010616 Proposed Changes to 33.210 about the ESP Algorithms. This was presented by Nokia and proposed addition of text for the support of ESP authentication transforms (new section 5.3.5). It was reported that there was a contribution from Ericsson proposing not to use AES-MAC and whether SHA-1 should be the only transform used. It was pointed out that AES is mandatory for encryption. It was agreed that the support of AES-MAC would be considered when it is available. Therefore SHA-1 will be supported and support of AES-MAC would become the subject of an editors’ note. It was agreed that the statements provided should be limited to those that are supported and not to comment on the reletive strength of other transforms. **The NDS/IP rapporteur undertook to update the document taking these agreements into account**.

TD S3-010619 Resubmitted S3-010489: Proposed changes to 33.210 about defining the BG element. This was presented by Nokia. The Border Gateway was also subject of a contribution from Ericsson in TD S3-010627, section 2.3 which was considered. Ericsson proposed that as BG applies only to PLMNs supporting GPRS, that it is not needed to mention it in this part of the document and that BG and SEG should be defined as two separate logical entities. Ericsson also suggested that SA WG3 review the meaning of "*adequate security*" in the BG context in order to clarify this.

It was proposed that the definitions of BG in 5.6.2 are removed and the relationship between BG and SEG are included in an informative annex by further contribution. **The NDS/IP Rapporteur agreed to try to add something into the GTP annex of the NDS/IP draft**. These contributions (TD S3-010619 and section 2.3 of TD S3-010627) were then noted.

TD S3-010626 On Definition of Za/Zb/Zc Interfaces. This was presented by Ericsson and proposed that the new SEG entity introduced by NDS/IP implied that new interfaces were introduced (interfaces Za, Zb and Zc). It proposes Za is mandatory and Zb and Zc optional, as they may not be required in some implementations. There was some discussion over the formulation of the implementation of Zb and Zc interfaces in order to allow operators to be able to specify their requirements to manufacturers and in the use of IKE over the Zb interface for maintenance of SAs where IPSec is supported. It was suggested that the Zb and Zc interfaces should be mandatory for implementation and optional for use by the operator. An exception was identified when the NEs are physically co-located, where securing this with IPsec would be unnecessary. It was concluded that as the SEG is a NE, then there was no real need for defining distinct Zb and Zc interfaces (between NE and SEG and NE-NE respectively).

It was agreed that the Zb and Zc interfaces should be merged into a single interfaces (the NDS/IP Rapporteur agreed to attempt to do this), and that the implementation of the Za and "merged" interface should be mandatory, while use would be optional (depending on the implementation of IPSec in the NEs).The contribution was updated to reflect these decisions in TD S3-010659 which was re-presented by Ericsson (Note, the "merged" interface was called "Zb" and "Zc" was removed), some modifications were suggested and agreed and the NDS/IP Rapporteur agreed to include the finally agreed text in the NDS/IP draft.

TD S3-010628 On Protection of IMS using NDS-IP. This was presented by Ericsson and proposed changes necessary to introduce how NDS-IP procedures shall be applied in order to protect the IMS CN SS into TS 33.210 and introduces sections 7.1 and 7.2 of the draft. The Rapporteur reminded the group that the content of this section had already been agreed to be inserted as an annex, rather than in the main part of the document. It was clarified that the points in the table X were Reference Points (as defined by TS 23.002), which should be made clear in the draft. It was decided that the list in the table should be removed and replaced by a reference to the list in TS 23.002. It was also agreed that the specification should state that all messages are protected except those specifically identified. The document was updated with these agreements in TD S3-010660 for use by the NDS/IP Rapporteur. Some minor modifications were noted by the NDS/IP Rapporteur for inclusion in the NDS/IP draft.

TD S3-010649 Comments on TS 33.210 v0.6.0. This was presented by Alcatel and suggested changes to clarify various parts of the draft. Some proposals were already covered in other discussions and the NDS/IP Rapporteur agreed to revisit these during implementation of agreed changes to the draft.

It was agreed that the rapporteur should update the presented draft TS 33.210 v0.7.0. The updated version should then go through an e-mail approval procedure similar to that suggested in TD S3-010644. It was **explicitly noted** that all the GTP and IMS specific material is open for discussion.

This means that TS 33.210 v0.8.0 will be submitted to the e-mail exploder for discussion no later than 5 December 2001. The discussion closes on 12 December 2001 and a new version will be made available on the e-mail exploder shortly thereafter. After the e-mail approval closes, provided that an agreement has been reached, the final version of the TS will be forwarded “for information” to the TAG SA#14 plenary.

7.3 IP multimedia subsystem security (draft TS 33.203)

TD S3-010644 Presentation on TS 33.203. This was presented by K. Boman (Ericsson), the Rapporteur for this work as an introduction to the work done on TS 33.203. It was agreed that Visibility and Configurability and the editors' note in section 5.3, Network Topology Hiding should be removed from the TS, as suggested in the presentation (see slide 4). It was also agreed that the issue of Network-initiated re-authentication (section 11.4.1.5, see slide 5) should be solved by a LS on this for TS 24.229 (K. Boman to produce). Due to lack of contribution for Rel-5, it was agreed to delete IP-address anonymity from the document if no input is received at this meeting (pending handling of an LS to this meeting - TD S3-010588). The status of IETF documents are included in TD S3-010598 and will be taken into account for the discussion on stability for the TS. It was recognised that the availability of the draft for TSG SA plenary (for information) was a very short time before the meeting started, and the **Rapporteur was asked that the document be sent to Mr. Pope on the Friday 14 December at the latest**. The timing for stability dependent upon the IETF specifications should be raised by the SA WG3 Chairman at the TSG SA plenary.

It was verified later in the meeting which of the issues given in the presentation had been covered by contributions and discussions, so that the stability of the draft for information to TSG SA#14 could be assessed. Not addressed: UE functional split, Hiding mechanisms (contributions under these agenda items had not been dealt with at the time of this review). It was concluded that the specification was suitably stable for sending to TSG SA for information in December 2001.

TD S3-010566 Reply Liaison Statement On the use of Network Domain Security for protection of SIP signalling messages. This was provided to SA WG3 for information and was noted.

TD S3-010570 This had been dealt with at the joint T WG3 session and was noted.

TD S3-010577 This was briefly introduced by Ericsson and had been copied to SA WG3 for information, as SA WG3 had already responded on this issue. The LS was then noted.

TD S3-010576 LS on IMS identifiers and ISIM and USIM. This had been dealt with at the joint T WG3 session and the response LS from this session (see TD S3-010647). It was recognised that further discussion would be necessary in SA WG3 itself, to consider the issues not relevant to the joint session. This was allocated under a new agenda item 7.10 *"UE functionality split"*.

TD S3-010578 Response to the LS S2-012896 from SA3 on Security Aspects related to the IMS Authentication. It was decided that this could be revisited when the requirements for Rel-6 are elaborated and the LS was noted.

TD S3-010579 Draft TS 33.203 version 0.7.0: Access security for IP-based services (Rel-5). This was provided for information supporting the presentation given in TD S3-010644, and not for particular review at the meeting. The TS was therefore noted.

TD S3-010588 LS from SA WG1: RE: Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem. This was copied to SA WG3 and the response was reviewed. It was agreed that this is not a Rel-5 issue and the LS was noted.

TD S3-010589 Response to: Liaison Statement on Usage of Private ID. This was provided for information and was briefly reviewed and noted.

TD S3-010569 Liaison Statement from SCP on Technical Solution for Prepaid Cards Using Smart Cards with Real-Time Clock. This was provided for information and was noted

TD S3-010593 LS from SA WG1: Presence Service requirements. This was reviewed to ascertain any impact on IMS security. It was decided that this is a separate WI and although it may have an impact on IMS, was not directly related to it. A separate Agenda item was created to deal with this: *7.11 "Presence".*

TD S3-010599 Definition of UICC. This had been briefly discussed at the joint T WG3 session and it was decided that SA WG3 should verify the definition of UICC and the alignment with the T WG3 request. This was considered a Rel-5 impact and was noted. (CRs for Release 1999 and Rel-4 were approved in SA WG3 meeting #20).

TD S3-010629 P-CSCF resides in the home network. This was presented by Ericsson and proposed an update to 33.203 to align with SA WG2 text on the position of the P-CSCF. The contribution was discussed and it was recognised that some editorial modifications would be needed. The principles were agreed to be included in draft TS 33.203.

TD S3-010630 P-CSCF initiated authentication. This was presented by Ericsson and discussed P-CSCF initiated authentication in relation to the SA WG2 Stage 2 documents. It proposes that this functionality is not well-developed at this time and that it is not included in the Rel-5 timeframe and that the editors' note related to this in 33.203 is removed. It was proposed that an LS should be sent to

SA WG2 in order to confirm that there would be no impact due to charging events, etc. before finally deciding to remove this functionality from Rel-5. **SA WG3 therefore agreed a working assumption that P-CSCF triggered re-authentication can be removed from Rel-5, pending confirmation from SA WG2**. The LS to SA WG2 was provided in TD S3-010654 which was presented by P. Howard which was approved and distributed during the meeting.

TD S3-010631 Lifetime of SA between UE and P-CSCF. This was presented by Ericsson and discussed the need for a separate timer to control the SA lifetime between UE and P-CSCF. It proposed that there should be no need for an additional SA lifetime timer in UE or P-CSCF and that the decision to initiate authentication can be done internally in the initiating entity and TS 33.203 should be updated to reflect this. The trigger to delete the SA in the P-CSCF was questioned. It was clarified that this should be standard SIP behaviour for complete registration cancellation (to be verified that this exists). The proposal was accepted in principle, and it needs to be added to the specification that the P-CSCF deletes the SA with the UE when the SA expires in the S-CSCF.

TD S3-010632 Implicit registration of IMS User Public Identities, IMPU(s). This was presented by Ericsson and discussed the implications of the SA WG2 agreement (in S2-012997) that the service Profile can perform implicit registrations of IMS User Public IDs (IMPUs). TS 33.203 should reflect the need for the S-CSCF to receive all IMPU(s) that are implicitly registered. It was suggested that a similar contribution to the information is provided to the P-CSCF (to be discussed in TD S3-010633). It was agreed that an LS to CN WG2 should be provided to inform them of the implications of this change. The proposal was provisionally accepted pending discussions of TD S3-010633 (later discussion of TD S3-010633 did not change the status of this). The LS to CN WG2 was provided in TD S3-010655 which was presented by K. Boman, modified slightly in TD S3-010668 which was approved and distributed during the meeting.

TD S3-010636 SIP application required to check IP address. This was presented by Siemens and proposed some text to be added to TS 33.203 regarding the processing if incoming messages. It was clarified that by use of IPSec, ESP tunnel-mode would be needed (Siemens needed to verify that this was the intention). The proposal was provisionally accepted, pending discussion of TD S3-010633 (later discussion of TD S3-010633 did not change the status of this). The implication that IPSec is being used and another mechanism would need to be provided for this in the annex of the mechanism at the SIP layer.

TD S3-010603 EAP extension drafts – new versions. This was presented by Nokia, and detailed the latest changes to the IETF drafts for EAP extensions. The Public Key authentication was considered unacceptable security for the wider range of applications that the internet drafts will be used for. It was agreed that the IETF should be informed of the needs of 3GPP in order to use these internet drafts for UMTS security at the SIP layer.

It was reported that the drafts should be accepted in the December meeting of the IETF. SA WG3 should be able to take the relevant parts of the drafts even before the complete IETF specifications are completed. If any draft is not accepted, then the next opportunity would be the March 2002 meeting of IETF. 6 companies represented at the meeting indicated that there will be representation from their companies at the next IETF meeting in December.

It was clarified that the drafts go to the PPP and the SIP/SIPing working groups of the IETF.

TD S3-010620 Extensible Authentication Protocol (EAP) progress in IETF. This was presented by Nokia and detailed the work on extensions to EAP that is progressing in the IETF.

The Key distribution as part of the authentication procedure was questioned, it was clarified that this is a technique to combine 2 (Kc) keys in order to produce a stronger authentication and generate longer keys - there was some reservation on the strength obtained from this technique. G. Rose agreed to analyse the draft to determine the validity of the approach.

Action 21/6: G. Rose to ~~eveluate~~evaluate the EAP/SIM authentication technique to determine it's validity for increased authentication strength.

SA WG3 delegates were asked to analyse the EAP/SIM work and documentation and provide comments to the next meeting - the IETF draft was provided for this purpose in TD S3-010663. Nokia were thanked for bringing this information to the attention of SA WG3.

TD S3-010604 Security Mechanism Agreement for SIP Connections. This was presented by the IETF liaison rapporteur for SA WG3 (Ericsson). The relationship with draft TS 33.203 was questioned, in particular whether the SA WG3 specifications will conform to the IETF standards. It was clarified that all the mechanisms use the option tag, which is a fully qualified domain name and this will allow anyone to negotiate their required security mechanisms (i.e. 3GPP systems can add the required mechanisms). Error cases are for further study in the IETF. Delegates were asked to provide comments to the rapporteur for progression of the document.

TD S3-010605 draft-garcia-sipping-3gpp-reqs-02: 3GPP requirements on SIP. This was presented by the IETF liaison rapporteur for SA WG3 (Ericsson). Delegates were asked to provide comments to the rapporteur for progression of the document.

It was requested that the IETF members are made aware that these documents are so far still drafts.

TD S3-010634 SIP Message Integrity Protection Work in IETF. This was presented by Nortel and detailed the internet draft that Nortel Networks have provided for submission to the IETF following a request from SA WG3 meeting#20. The draft was submitted to SA WG3 in advance and presented, detailing the issues, for discussion. It was commented that the replay mechanism given in this draft would need enhancement to be suitable and complete for use in the 3GPP specifications. Siemens saw a problem with the single counter replay protection scheme and provided an input explaining this in TD S3-010664 "*Problems with the replay protection scheme in the SIP level integrity solution in Annex C of TS 33.203, v070*". The scenario explained the call loss problem and Nortel agreed to take this into consideration and provide a more robust solution to overcome the problem.

P. Howard also agreed to provide input on synchronisation problems he had identified in the draft.

TD S3-010633 The “Fraudulent User” Attack Against the IMS. This was presented by Ericsson and described an attack scenario identified in current specifications. It was clarified that any authentication needs to be done with the Private ID, and cannot be done using a Public ID. The solutions provided in the contribution were discussed. **Delegates were invited to consider this attack scenario and possible solutions and contribute to the next meeting**. In addition, it was agreed to produce a LS to CN WG1 to outline the problem with implicitly registered Public IDs and some potential solutions being considered by SA WG3, which was provided in TD S3-010667 which was modified to clarify the problem, and provided in TD S3-010673. A draft version of this was displayed for discussion. It was decided to check the LSs related to this from other groups before deciding on the approval of this LS, as follows:

> TD S3-010567 Reply to Liaison Statement on Usage of Private ID. This was presented by Siemens and gave the CN WG4 questions on provision of the Public IDs in the P-CSCF. The LS was noted.

The final version of TD S3-010673 was elaborated in a drafting group, and was presented by G. Horn. The LS was approved.

TD S3-010665 LS to CN WG1: IMS Security. This was discussed and modified editorially and updated in TD S3-010669 which was approved and distributed during the meeting.

TD S3-010627 On defining NDS/IP traffic. This was presented by Ericsson, noting that section 2.3 on BG had been dealt with in conjunction with TD S3-010619 under agenda item 7.2. The proposed changes were accepted and the NDS/IP Rapporteur was asked to include them in the draft. The updated draft was provided in TD S3-010670 for review and was briefly introduced by the Rapporteur to provide an overview of the updates agreed and included in the draft and other issues that should be considered. This will be circulated by e-mail for final comment before forwarding to the TSG SA#14 for information. It was noted that Sections 6 and 7 will become Annexes B and C in the version distributed for e-mail. The updated draft was agreed for information to TSG SA#14 except for section 6.2, section 6.3 and section 7 which were left open are subject to change on the e-mail discussion.

TD S3-010684 Discussion on EAP unsolicited response packets. This was presented by Qualcomm and discusses the view from a Qualcomm IETF delegate. It was recognised that there could be a problem and this and it needs further consideration. Ericsson and Nokia agreed to check the implications on time scales for 3GPP work. Qualcomm were thanked for inputting this and the contribution was then noted.

A proposal to hold an interim ad-hoc meeting on IMS was considered to progress the work in this area in time for finalisation for Rel-5. was agreed: 31 January - 1 February 2002.

7.4 Security aspects of network configuration hiding

TD S3-010653 Mechanism to Hide Network Configuration. This was presented by Alcatel and discussed possible solutions for hiding network configuration. It was suggested that the required changes and extension to SIP implied here, that CN WG1 should be informed before taking action in order to get their analysis too. It was stated that the length of the header would grow as encryption is overlaid due to the MAC additions, it was clarified that the length grows as you pass more and more nodes in any case, which reduces this problem. Also the normal cases would be peer-peer direct roaming and would not cause multiple encryption to occur. TD S3-010586 which was also considered.

TD S3-010586 (Pseudo) CR to 33.203: Network Hiding Mechanism. This was presented by AT&T Wireless and proposed a modification to 33.203 for network hiding. It was agreed to use this contribution as a basis for further elaboration, in order to have some indication in the draft to be presented to TSG SA for information. An editors note with the outstanding issues to be solved should be added, this list of issues was prepared by a drafting group and provided in TD S3-010701 which was modified slightly and provided in TD S3-010702 which was agreed for inclusion in the NDS/IP draft.

7.5 Visibility and configurability of security

TD S3-010581 Proposed CR to 33.102: Configurability of cipher use (Rel-5). This was presented by Telia and had been submitted to meeting#20 and discussed over e-mail between meetings. The CR was updated in TD S3-010674, which was modified slightly in TD S3-010679 and approved. It was decided to send it to CN WG1 for comment on any impact to their specifications (copied to T WG2), and a LS was provided in TD S3-010675 which was approved.

7.6 Guide to 3G security (TR 33.900)

There were no contributions under this agenda item.

7.7 GERAN security

There were no contributions under this agenda item.

7.8 MExE security

There were no contributions under this agenda item.

7.9 OSA security

The contribution concerning OSA security was dealt with in TD S3-010661 under agenda item 5.3.

7.10 UE functionality split

TD S3-010576 The ISIM issues were dealt with in the joint session with T WG3, and this meeting considered the other issues included in the attachment. The LS was then noted.

TD S3-010595 Liaison Statement on UE functionality split. This was considered and there were concerns over the meaning of much of the document, as to whether there will be any termination of call control on the TE. The document does state that the call control is on the MT, and much discussion ensued as to whether this disallowed the TE access to the network directly. The majority of delegates expressing a view assumed that the call control is wholly contained in the MT, and the functions in the TE shall have no impact on the IMS security (i.e. the TE does not access the ISIM). The MT must be GERAN, UTRAN or GSM. It was agreed to produce a LS response to SA WG1 which was provided in TD S3-010703 which was approved.

7.11 Presence Service

TD S3-010593 Presence Service requirements. This was presented by the Chairman and requests SA WG3 to update their specifications in order to include security requirements for the Presence service. There was some concern expressed over this Stage 1 had been approved for Rel-5, when the service had not been considered before in SA WG3. It was agreed to start a security analysis on this service and an e-mail discussion would be set-up to study this, by D. Castellanos. A reply LS to SA WG1 was produced to inform them of this study group was provided in TD S3-010699 which was approved.

Nokia requested that SA WG3 should start work on the Stage 2 security aspects in advance of the decision on whether the feature is Rel-5 or Rel-6 (to be decided by TSG SA). Delegates were encouraged to contribute on this work in order to complete the work in good time.

Action 21/7: D. Castellanos to set up an e-mail discussion on Presence service, with support from Nokia, Telenor and Vodafone.

~~TD S3-010576 The ISIM issues were dealt with in the joint session with T WG3, and this meeting considered the other issues included in the attachment. The LS was then noted.~~

~~TD S3-010595 Liaison Statement on UE functionality split. This was considered and there were concerns over the meaning of much of the document, as to whether there will be any termination of call control on the TE. The document does state that the call control is on the MT, and much discussion ensued as to whether this disallowed the TE access to the network directly. The majority of delegates expressing a view assumed that the call control is wholly contained in the MT, and the functions in the TE shall have no impact on the IMS security (i.e. the TE does not access the ISIM). The MT must be GERAN, UTRAN or GSM. It was agreed to produce a LS response to SA WG1 which was provided in TD S3-010703 which was approved.~~ ~~**MOVED TO 7.10**~~

8 Proposed work items

8.1 Support for subscriber certificates

TD S3-010623 Proposed Work Item description: Support for subscriber certificates. This was presented by Nokia. There were various comments on the timescales and whether this should be done by CRs to 33.102 or by creating a new specification. It was decided to leave this until further development of the work and leave a note in the WI sheet stating that a new TS may be used if needed instead of CRs. The WI description sheet was updated in TD S3-010704 and was approved.

TD S3-010600 General Purpose Authenticator via Mobile Phone. This was provided for information and was noted.

TD S3-010622 Using PKI to provide network domain security. This was presented by Nokia and was noted.

9 Review and update of work programme

M. Pope and P. Howard agreed to update the Work Program (Project Plan for SA WG3) after the meeting and send to Rapporteurs for comment. The updated project plan would then be included in the version sent to TSG SA#14.

10 Future meeting dates and venues

Ad-hocs to progress the work for Rel-5 were agreed as follows:

NDS/IP ad-hoc 31 Jan 2002, Antwerp, Belgium.

MAPsec ad-hoc 31 Jan 2002, Antwerp, Belgium.

IMS security (aSIP) 1.5 days afternoon 31 Jan - 1 Feb 2002 (16.00 finish), Antwerp, Belgium.
(M Pope to make the invitation in conjunction with Olivier Paradiens, Alcatel).

G. Horn reported a potential problem in availability of Hotel rooms during the Munich meeting in October 2002. He agreed to check availability on the intended week and surrounding weeks and make a suggestion on the e-mail if a change is found desirable.

Meeting	Date	Location	Host
NDS/IP ad-hoc (Rel-5)	31 Jan ~~2001~~2002	Antwerp, Belgium	Alcatel
MAPsec ad-hoc (Rel-5)	31 Jan ~~2001~~2002	Antwerp, Belgium	Alcatel
IMS security (aSIP) ad-hoc	31 Jan (pm) - 01 Feb ~~2001~~2002	Antwerp, Belgium	Alcatel
S3#22	~~26~~ 25 - 28 Feb ~~- 1 March~~ 2002	Bristol, UK	Orange
S3#23 + AHAG	14 - 17 May 2002	Victoria, Canada	AT&T Wireless
S3#24	9 - 12 July 2002	Helsinki, Finland (TBC)	Nokia
S3#25	15 - 18 October 2002	Munich, Germany (TBC)	Siemens (TBC)

11 Any other business

There were no items discussed under this agenda item.

12 Close of meeting

The Chairman (V. Niemi was Chairman for the second half of the meeting) thanked the delegates for their hard work and good co-operation during the meeting and the host, ETSI, for the meeting venue and closed the meeting.

Annex A: List of attendees at the SA WG3#20 meeting and Voting List

A.1 List of attendees

Name	Company	e-mail	3GPP ORG	
Mr. Nigel Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	GB	ETSI
Mr. Colin Blanchard	BT Group Plc	colin.blanchard@bt.com	GB	ETSI
Mr. Marc Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	BE	ETSI
Mr. Krister Boman	ERICSSON L.M.	krister.boman@emw.ericsson.se	SE	ETSI
Mr. Charles Brookson	DTI	cbrookson@iee.org	GB	ETSI
Mr. Daniel Brown	Motorola Inc.	adb002@email.mot.com	US	T1
Mr. Steve Canning	CESG	steve.canning@CESG.GSI.GOV.UK	GB	ETSI
Mr. David Castellanos	ERICSSON L.M.	david.castellanos-zamon@ece.ericsson.se	SE	ETSI
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp	JP	ARIB
Mr. Per Christoffersson	TELIA AB	per.e.christoffersson@telia.se	SE	ETSI
Mr. Stephen Dutnall	AT&T Wireless Services, Inc.	steve.dutnall@northstream.se	US	T1
Dr. Adrian Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	GB	ETSI
Mr. Jean-Bernard Fischer	OBERTHUR CARD SYSTEMS S.A.	jb.fischer@oberthurcs.com	FR	ETSI
Ms. Tao Haukka	NOKIA Corporation	tao.haukka@nokia.com	FI	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	DE	ETSI
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vodafone.com	GB	ETSI
Mr. Rafal Jaczynski	POLKOMTEL S.A.	rafal.jaczynski@polkomtel.com.pl	PL	ETSI
Mr. Geir Koien	TELENOR AS	geir-myrdahl.koien@telenor.com	NO	ETSI
Mrs. Tiina Koskinen	NOKIA Corporation	tiina.s.koskinen@nokia.com	FI	ETSI
Mr. Alexander Leadbeater	BT Group Plc	alex.leadbeater@bt.com	GB	ETSI
Mr. Tomi Mikkonen	SSH Communications Security	tomi.mikkonen@ssh.com	FI	ETSI
Mr. Sebastien Nguyen Ngoc	France Telecom	sebastien.nguyenngoc@rd.francetelecom.com	FR	ETSI
Mr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	FI	ETSI
Mr. Petri Nyberg	SONERA Corporation	petri.nyberg@sonera.com	FI	ETSI
Mr. Bradley Owen	Lucent Technologies N. S. UK	bvowen@lucent.com	GB	ETSI
Mr. Olivier Paridaens	ALCATEL S.A.	Olivier.Paridaens@ALCATEL.BE	FR	ETSI
Miss Mireille Pauliac	GEMPLUS Card International	mireille.pauliac@gemplus.com	FR	ETSI
Mrs. Beatrice Peirani	GEMPLUS Card International	beatrice.peirani@gemplus.com	FR	ETSI
Mr. Maurice Pope	ETSI Secretariat	maurice.pope@etsi.fr	FR	ETSI
Mr. Greg Rose	QUALCOMM EUROPE S.A.R.L.	ggr@qualcomm.com	FR	ETSI
Mr. Teruharu Serada	NEC Corporation	serada@aj.jp.nec.com	JP	ARIB
Mr. Benno Tietz	MANNESMANN Mobilfunk GmbH	benno.tietz@d2vodafone.de	DE	ETSI
Mr. Lee Valerius	NORTEL NETWORKS (EUROPE)		GB	ETSI
Prof. Michael Walker	VODAFONE Group Plc	mike.walker@vodafone.com	GB	ETSI
Mr. Stuart Ward	ORANGE PCS LTD	stuart.ward@orange.co.uk	GB	ETSI
Ms. Monica Wifvesson	ERICSSON L.M.	Monica.Wifvesson@ecs.ericsson.se	SE	ETSI
Mr. Berthold Wilhelm	~~Brand Communications Ltd~~BMWi	berthold.wilhelm@regtp.de	GB	ETSI

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #19, #20 and #21, the following companies are eligible to vote at SA WG3 meeting #22:

Company	Country	Status	Partner Org
ALCATEL S.A.	FR	3GPPMEMBER	ETSI
AT&T Wireless Services, Inc.	US	3GPPMEMBER	T1
BUNDESMINISTERIUM FUR WIRTSCHAFT	DE	3GPPMEMBER	ETSI
~~Brand Communications Ltd~~BMWi	~~GB~~DE	3GPPMEMBER	ETSI
BT Group Plc	GB	3GPPMEMBER	ETSI
Communications-Electronics Security Group	GB	3GPPMEMBER	ETSI
Cingular Wireless LLC	US	3GPPMEMBER	T1
DTI - Department of Trade and Industry	GB	3GPPMEMBER	ETSI
Telefon AB LM Ericsson	SE	3GPPMEMBER	ETSI
France Telecom	FR	3GPPMEMBER	ETSI
GEMPLUS Card International	FR	3GPPMEMBER	ETSI
Hutchison 3G UK Limited	GB	3GPPMEMBER	ETSI
KPN - Koninklijke PTT Nederland NV	NL	3GPPMEMBER	ETSI
Lucent Technologies	US	3GPPMEMBER	T1
Lucent Technologies Network Systems UK	GB	3GPPMEMBER	ETSI
MANNESMANN Mobilfunk GmbH	DE	3GPPMEMBER	ETSI
Mitsubishi Electric Co.	JP	3GPPMEMBER	ARIB
Motorola Inc.	US	3GPPMEMBER	T1
MOTOROLA Ltd	GB	3GPPMEMBER	ETSI
NEC Corporation	JP	3GPPMEMBER	ARIB
NOKIA Corporation	FI	3GPPMEMBER	ETSI
NORTEL NETWORKS (EUROPE)	GB	3GPPMEMBER	ETSI
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
OBERTHUR CARD SYSTEMS S.A.	FR	3GPPMEMBER	ETSI
ORANGE PCS LTD	GB	3GPPMEMBER	ETSI
POLKOMTEL S.A.	PL	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
SAMSUNG Electronics Research Institute	GB	3GPPMEMBER	ETSI
SIEMENS AG	DE	3GPPMEMBER	ETSI
SIEMENS ATEA NV	BE	3GPPMEMBER	ETSI
SONERA Corporation	FI	3GPPMEMBER	ETSI
SSH Communications Security Corp	FI	3GPPMEMBER	ETSI
Telenor AS	NO	3GPPMEMBER	ETSI
TELIA AB	SE	3GPPMEMBER	ETSI
VODAFONE Group Plc	GB	3GPPMEMBER	ETSI

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by
S3-010562	Draft Agenda for meeting #21	Chairman	2	Approval	
S3-010563	Draft report of meeting #20	Secretary	3	Approval	
S3-010564	Liaison Statement on AMR-WB and Legal Interception	CN WG4	5.3	Information	
S3-010565	LS to GSM-A TWG/SERG "regarding User Profile"	3GPP Joint ad-hoc on Generic User Profile (GUP)	5.3	Information	
S3-010566	Reply Liaison Statement On the use of Network Domain Security for protection of SIP signalling messages	CN WG4	7.3	Action	
S3-010567	Reply to Liaison Statement on Usage of Private ID	CN WG4	5.3	Information	
S3-010568	LS on Message size limitation for f9 algorithm	RAN WG2	5.3	Action	
S3-010569	Liaison Statement on Technical Solution for Prepaid Cards Using Smart Cards with Real-Time Clock	ETSI EP SCP	7.3	Information	
S3-010570	Liaison Statement on IMS identifiers and ISIM	T WG3	6 / 7.3	Discussion	
S3-010571	VASP MMS Connectivity	T WG2	5.3	Discussion / Guidance	
S3-010572	LS from RAN WG3: WID: AMR-WB Speech Service – Core Network Aspects	RAN WG3	5.3	Information	
S3-010573	Liaison Statement on Security of Rel5 IP Transport in UTRAN	RAN WG3	5.3	Action	
S3-010574	LS to CN WG5: Comments on TS 29.198	SA WG3	- / 5.3	Information	
S3-010575	LS on Enhanced user privacy for location services	SA WG2	5.3	Action	
S3-010576	LS on IMS identifiers and ISIM and USIM	SA WG2	7 / 7.10	Action	
S3-010577	Reply to Liaison Statement on Usage of Private ID	SA WG2	7.3	Information	
S3-010578	Response to the LS S2-012896 from SA3 on Security Aspects related to the IMS Authentication	SA WG2	7.3	Action	
S3-010579	Draft TS 33.203 version 0.7.0: Access security for IP-based services (Rel-5)	Rapporteur			
S3-010580	ISIM Application	Gemplus	8	Discussion	
S3-010581	Proposed CR to 33.102: Configurability of cipher use (Rel-5)	Telia		Approval	S3-010674
S3-010582	NDS/IP suggestions	Telenor		Discussion	S3-010670
S3-010583	Update information on 33.210-060	Geir M Køien, rapporteur		Presentation / Discussion	
S3-010584	T3 ISIM working assumptions	Jeremy Norris (Vodafone Ltd) USIM rapporteur	6	Discussion	
S3-010585	LS from CN WG1 on IMS identifiers: Response to: LS (S2-013067) on IMS identifiers and ISIM and USIM	CN WG1	7	Discussion	
S3-010586	(Pseudo) CR to 33.203: Network Hiding Mechanism	AT&T Wireless		Approval	
S3-010587	Liaison Statement on 3GPP Generic User Profile Stage 1	SA WG1	5.3	Information	
S3-010588	RE: Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem	SA WG1	7.3	Information	
S3-010589	Response to: Liaison Statement on Usage of Private ID	SA WG1	7.3	Information	
S3-010590	Liaison Statement on Revised Push Service Stage 1	SA WG1	5.3	Discussion	
S3-010591	Reply to LS on "Privacy Override Indicator"	SA WG1	5.3	Action	
S3-010592	Liaison Statement on DRM	SA WG1	5.3	Action	
S3-010593	Presence Service requirements	SA WG1	7.3	Action	
S3-010594	Answer to LS on requirements on Multimedia Broadcast/Multicast Service	SA WG1	5.3	Information	
S3-010595	Liaison Statement on UE functionality split	SA WG1	7 / 7.10	Action	
S3-010596	RE: LS on IMS identifiers and ISIM and USIM (S2 Tdoc S2-013067)	T WG2	7	Information	
S3-010597	Cipher indicators and selection options in UMTS	GSM Association SG		Information	
S3-010598	Mail received from TSG CN Chairman on IETF Dependancies table	Secretary SA WG3 (TSG CN Chairman)		Review / Comment	
S3-010599	Definition of the UICC	SA WG1	7	Action	
S3-010600	General Purpose Authenticator via Mobile Phone	Orange		Discussion	

TD number	Title	Source	Agenda	Document for	Replaced by
S3-010601	Proposed CR to 35.201: Correct the maximum input message length for f8 and f9 (Rel-99)	Siemens Atea		Approval	S3-010680
S3-010602	Proposed CR to 35.201: Correct the maximum input message length for f8 and f9 (Rel-4)	Siemens Atea		Approval	S3-010681
S3-010603	EAP extension drafts – new versions	Ericsson, Nokia		Information	
S3-010604	Security Mechanism Agreement for SIP Connections	Ericsson, Nokia, Nortel Networks		Information	
S3-010605	draft-garcia-sipping-3gpp-reqs-02: 3GPP requirements on SIP	Ericsson		Discussion	
S3-010606	Proposed CR to 33.200: Removing the Sending PLMN-Id from Security Header (Rel-4)	Hutchison 3G UK		Approval	S3-010658
S3-010607	Proposed CR to 33.200: Completing the specification of a MAPsec SA (Rel-4)	Hutchison 3G UK		Approval	S3-010693
S3-010608	Update on changes to MAPsec Release 5	Hutchison 3G UK		Information	
S3-010609	3GPP TS 33.108 (Version 0.2.1)	SA WG3-LI	5.1	Approval	
S3-010610	Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-5). WITHDRAWN as Rel99,Rel4 CRs not available	SA WG3-LI	5.1	Approval	
S3-010611	Revised Work Item Description (revision of SP-000309)	SA WG3-LI		Approval	
S3-010612	Proposed CR to 33.107: Source of PDP context initiation (Rel-5)	SA WG3-LI		Approval	
S3-010613	Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #5/01 on lawful interception Aspen, Colorado 30 October – 1 November 2001	SA WG3-LI		Information	
S3-010614	Overview of differences and gaps of Lawful Interception between legacy telecommunication and multimedia call scenarios	SA WG3-LI		Presentation	
S3-010615	draft-arkko-map-doi-04: The MAP Security Domain of Interpretation for ISAKMP	Jari Arkko (Ericsson)		Discussion	
S3-010616	Proposed Changes to 33.210 about the ESP Algorithms	Nokia		Discussion / Decision	
S3-010617	Proposed changes to 33.210 about protecting GTP-U	Nokia		Discusion	
S3-010618	Proposed Changes to 33.210 about the scope	Nokia	5.3	Discussion / Decision	
S3-010619	Resubmitted S3-010489: Proposed changes to 33.210 about defining the BG element	Nokia		Discussion	
S3-010620	Extensible Authentication Protocol (EAP) progress in IETF	Nokia		Presentation	
S3-010621	Response to liaison from IPCablecom on LI	ETSI EP TIPHON		Action	
S3-010622	Using PKI to provide network domain security	Telenor, Nokia		Discussion	
S3-010623	Proposed Work Item description: Support for subscriber certificates	Nokia		Approval	S3-010704
S3-010624	Parameters stored on a UICC card for IMS services	Ericsson	8	Discussion	
S3-010625	Use of a R99 or REL-4 USIM application on a UICC card for IMS services	Ericsson	8	Discussion	
S3-010626	On Definition of Za/Zb/Zc Interfaces	Ericsson	7.2	Discussion / Decision	S3-010659
S3-010627	On defining NDS/IP traffic	Ericsson	7.2	Discussion / Decision	
S3-010628	On Protection of IMS using NDS-IP	Ericsson	7.2	Discussion / Decision	S3-010660
S3-010629	P-CSCF resides in the home network	Ericsson	7.3	Discussion / Decision	
S3-010630	P-CSCF initiated authentication	Ericsson	7.3	Discussion / Decision	
S3-010631	Lifetime of SA between UE and P-CSCF	Ericsson	7.3	Discussion / Decision	
S3-010632	Implicit registration of IMS User Public Identities, IMPU(s)	Ericsson	7.3	Discussion / Decision	
S3-010633	The “Fraudulent User” Attack Against the IMS	Dynamicsoft, Ericsson	7.3	Discussion / Decision	
S3-010634	SIP Message Integrity Protection Work in IETF	Nortel Networks	7.3	Discussion	
S3-010635	Protection Profiles Version Identification	Siemens Atea	6.3	Discussion / Decision	
S3-010636	SIP application required to check IP address	Siemans	7.3	Discussion / Decision	
S3-010637	SA distribution mechanism for the Ze interface	Siemans	7.1	Discussion / Decision	
S3-010638	Work Item Description: Support for subscriber certificates	Nokia	8.1	Approval	
S3-010639	Draft agenda for joint SA WG3/T WG3 session	Chairman	3	Approval	
S3-010640	aSIP-Access Security for IP-Based Services	Ericsson	5	Presentation	
S3-010641	On the use of R99/Rel-4 USIMs for IMS access	Vodafone	8	Discussion	

TD number	Title	Source	Agenda	Document for	Replaced by
S3-010642	Draft Response LS on IMS identifiers and ISIM and USIM	Joint Session / V. Niemi	4.2	Approval	S3-010647
S3-010643	Use of Push vs Pull Mechanisms in local SA distribution	Siemens / Alcatel	8.1	Discussion	
S3-010644	Presentation on TS 33.203	K. Boman, Rapporteur	7.3	Presentation	
S3-010645	WITHDRAWN - Reallocated : Reserved IMS doc	Alcatel	7.3		S3-010650
S3-010646	WITHDRAWN - Reallocated : Reserved IMS doc	Alcatel	7.3		S3-010651
S3-010647	Response LS on IMS identifiers and ISIM and USIM	SA WG3	4.2	Approval	
S3-010648	Comments on TS 33.200 R5 v0.1.0	Alcatel	6.3	Discussion	
S3-010649	Comments on TS 33.210 v0.6.0	Alcatel	7.2	Discussion	
S3-010650	Comments on draft-arkko-pppext-eap-aka-00	Alcatel		Discussion	
S3-010651	Comments on draft-arkko-pppext-eap-aka-01	Alcatel		Discussion	
S3-010652	Comments on draft-torvinen-http-eap-01	Alcatel		Discussion	
S3-010653	Mechanism to Hide Network Configuration	Alcatel	7.5	Discussion	
S3-010654	LS to SA WG1 on P-CSCF triggered re-authentication	SA WG3	7.3	Approval	
S3-010655	LS to CN WG2: Implicitly registered IMPU(s)	SA WG3	7.3	Approval	S3-010668
S3-010656	Changes to 33.210 about the scope	SA WG3	5.3	Approval	
S3-010657	Draft Response LS on Security of Rel5 IP Transport in UTRAN	SA WG3	5.3	Approval	S3-010662
S3-010658	Proposed CR to 33.200: Removing the Sending PLMN-Id from Security Header (Rel-4)	Hutchison 3G UK	6.3	Approval	
S3-010659	On Definition of Za/Zb/Zc Interfaces (revised S3-010626)	Ericsson	7.2	Discussion / Decision	
S3-010660	On Protection of IMS using NDS-IP (revised S3-010628)	Ericsson	7.2	Information	
S3-010661	Liaison Statement on the Support of Up to Date Encryption Algorithms in the OSA Framework	CN WG5	5.3	Action	
S3-010662	Response LS on Security of Rel5 IP Transport in UTRAN	SA WG3	5.3	Approval	
S3-010663	IETF draft EAP/SIM	G Rose	7.3	Information	
S3-010664	Problems with the replay protection scheme in the SIP level integrity solution in Annex C of TS 33.203, v070	Siemens	7.3	Discussion	
S3-010665	Proposed LS to CN WG1: IMS Security	Ericsson	7.3	Approval	S3-010669
S3-010666	WITHDRAWN				
S3-010667	LS to CN1: Identity spoofing attacks in the IMS	SA WG3	7.3	Approval	S3-010673
S3-010668	LS to CN WG2: Implicitly registered IMPU(s) (revision of S3-010655)	SA WG3	7.3	Approval	
S3-010669	LS to CN WG1: IMS Security	SA WG3	7.3	Approval	
S3-010670	33.210 draft NDS/IP document (revised S3-010582)	Rapporteur	7.3	Review	
S3-010671	LS to CN WG4 on approved CR	Hutchinson	6.3	Approval	
S3-010672	LS to TSG CN on General requirements for SA distribution over Ze interface	Marc Blommaert	6.3	Approval	S3-010692
S3-010673	LS to CN1: Identity spoofing attacks in the IMS	SA WG3	7.3	Approval	
S3-010674	CR to 33.102: Configurability of cipher use (Rel-5) (revision of S3-010581)	Telia	7.5	Approval	S3-010679
S3-010675	LS to CN WG1: Configurability of cipher use (CR in S3-010675 for info)	Telia	7.5	Approval	
S3-010676	LS to N1 / T2 for comment on Connection set-up procedures	P Howard/Per	7.5	Approval	<not provided>
S3-010677	Approval of A5/3 formally by SA3	GSMA SG Chairman		Decision	
S3-010678	WITHDRAWN - Allocated in error				
S3-010679	CR to 33.102: Configurability of cipher use (Rel-5) (revision of S3-010674)	Telia	7.5	Approval	
S3-010680	Proposed CR to 35.201: Correct the maximum input message length for f8 and f9 (Rel-99)	Siemens Atea		Approval	S3-010689
S3-010681	Proposed CR to 35.201: Correct the maximum input message length for f8 and f9 (Rel-4)	Siemens Atea		Approval	S3-010690
S3-010682	LS to RAN2: Response to S3-010568 confirming changes requested	Marc Blommaert		Approval	
S3-010683	Response to LS T2-010905 (S3-010571) on VASP MMS connectivity	SA WG3		Approval	S3-010698

TD number	Title	Source	Agenda	Document for	Replaced by
S3-010684	Discussion on EAP unsolicited response packets	Qualcomm Europe S.A.R.L.		Discussion	
S3-010685	Response LS to CN WG5: Re S3-010661	Olivier P/Drafting group		Approval	S3-010696
S3-010686	LS to SA WG1, SA WG2: Response to: Liaison Statement on Revised Push Service Stage 1	SA WG3		Approval	S3-010700
S3-010687	Reply LS to SA WG1 on “Privacy Override Indicator”	SA WG3		Approval	S3-010697
S3-010688	CR to 33.200: Protection Profile Variant Identifier (Rel-4)	Siemens Atea		Approval	S3-010691
S3-010689	CR to 35.201: Correct the maximum input message length for f8 and f9 (Rel-99)	SA WG3		Approval	
S3-010690	CR to 35.201: Correct the maximum input message length for f8 and f9 (Rel-4)	SA WG3		Approval	
S3-010691	CR to 33.200: Protection Profile Revision Identifier (Rel-4)	Siemens Atea		Approval	
S3-010692	LS to TSG CN on General requirements for SA distribution over Ze interface	SA WG3	6.3	Approval	
S3-010693	Proposed CR to 33.200: Completing the specification of a MAPsec SA (Rel-4)	Hutchison 3G UK		Approval	
S3-010694	Provisional work plan for the design of the SAGE GSM A5/3 Task Force (SAGE GSM A5/3 TF)	SA WG3 Secretary		Information	
S3-010695	Mapping of Ze-interface information onto the Zd-Interface	Siemens Atea	7.1	Discussion	
S3-010696	Response LS to CN WG5: Re S3-010661	Olivier P/Drafting group		Approval	
S3-010697	Reply LS to SA WG1 on “Privacy Override Indicator”	SA WG3		Approval	
S3-010698	Response to LS T2-010905 (S3-010571) on VASP MMS connectivity	SA WG3		Approval	
S3-010699	LS to SA WG1 (CC S2, SA): Security and privacy requirements of presence	SA WG3		Approval	
S3-010700	LS to SA WG1, SA WG2: Response to: Liaison Statement on Revised Push Service Stage 1	SA WG3		Approval	
S3-010701	(pseudo) CR to 33.203: Network Hiding Mechanism	AT&T Wireless / Alcatel		Approval	S3-010702
S3-010702	(pseudo) CR to 33.203: Network Hiding Mechanism	AT&T Wireless / Alcatel		Approval	
S3-010703	LS response to SA WG1 (S1-011321): UE Functionality Split	G Horn drafting group		Approval	
S3-010704	Proposed Work Item description: Support for subscriber certificates	Nokia		Approval	

Annex C: Status of specifications under SA WG3 responsibility

NOTE: If the Editors are still not accurate - please provide the secretary with an update in order to update the main specifications database.

Specification			Title	Editor	Rel
TR	01.31	7.0.1	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	WRIGHT, Tim	R98
TR	01.31	8.0.0	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	WRIGHT, Tim	R99
TR	01.33	7.0.0	Lawful Interception requirements for GSM	MCKIBBEN, Bernie	R98
TR	01.33	8.0.0	Lawful Interception requirements for GSM	MCKIBBEN, Bernie	R99
TS	01.61	6.0.1	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	WALKER, Michael	R97
TS	01.61	7.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	WALKER, Michael	R98
TS	01.61	8.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	WALKER, Michael	R99
TS	02.09	3.1.0	Security Aspects	CHRISTOFFERSSON, Per	Ph1
TS	02.09	4.5.1	Security Aspects	CHRISTOFFERSSON, Per	Ph2
TS	02.09	5.2.1	Security Aspects	CHRISTOFFERSSON, Per	R96
TS	02.09	6.1.1	Security Aspects	CHRISTOFFERSSON, Per	R97
TS	02.09	7.1.1	Security Aspects	CHRISTOFFERSSON, Per	R98
TS	02.09	8.0.1	Security Aspects	CHRISTOFFERSSON, Per	R99
TS	02.31	7.1.1	Fraud Information Gathering System (FIGS) Service description; Stage 1	WRIGHT, Tim	R98
TS	02.31	8.0.1	Fraud Information Gathering System (FIGS) Service description; Stage 1	WRIGHT, Tim	R99
TS	02.32	7.1.1	Immediate Service Termination (IST); Service description; Stage 1	WRIGHT, Tim	R98
TS	02.32	8.0.1	Immediate Service Termination (IST); Service description; Stage 1	WRIGHT, Tim	R99
TS	02.33	7.3.0	Lawful Interception; Stage 1	MCKIBBEN, Bernie	R98
TS	02.33	8.0.1	Lawful Interception; Stage 1	MCKIBBEN, Bernie	R99
TS	03.20	3.3.2	Security-related Network Functions	NGUYEN NGOC, Sebastien	Ph1
TS	03.20	3.0.0	Security-related Network Functions	NGUYEN NGOC, Sebastien	Ph1-EXT
TS	03.20	4.4.1	Security-related Network Functions	NGUYEN NGOC, Sebastien	Ph2
TS	03.20	5.2.1	Security-related Network Functions	NGUYEN NGOC, Sebastien	R96
TS	03.20	6.1.0	Security-related Network Functions	NGUYEN NGOC, Sebastien	R97
TS	03.20	7.2.0	Security-related Network Functions	NGUYEN NGOC, Sebastien	R98
TS	03.20	8.1.0	Security-related Network Functions	NGUYEN NGOC, Sebastien	R99
TS	03.31	7.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 2	WRIGHT, Tim	R98
TS	03.31	8.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 2	WRIGHT, Tim	R99
TS	03.33	7.2.0	Lawful Interception; Stage 2	MCKIBBEN, Bernie	R98
TS	03.33	8.1.0	Lawful Interception; Stage 2	MCKIBBEN, Bernie	R99
TS	03.35	7.0.1	Immediate Service Termination (IST); Stage 2	WRIGHT, Tim	R98
TS	03.35	8.1.0	Immediate Service Termination (IST); Stage 2	WRIGHT, Tim	R99
TS	21.133	3.1.0	Security threats and requirements	CHRISTOFFERSSON, Per	R99
TS	21.133	4.0.0	Security threats and requirements	CHRISTOFFERSSON, Per	Rel-4

TS	22.022	3.1.0	Personalisation of Mobile Equipment (ME); Mobile functionality specification	NGUYEN NGOC, Sebastien	R99
TS	22.022	4.0.0	Personalisation of Mobile Equipment (ME); Mobile functionality specification	NGUYEN NGOC, Sebastien	Rel-4
TS	33.102	3.9.0	3G security; Security architecture	BLOMMAERT, Marc	R99
TS	33.102	4.2.0	3G security; Security architecture	BLOMMAERT, Marc	Rel-4
TS	33.103	3.7.0	3G security; Integration guidelines	BLANCHARD, Colin	R99
TS	33.103	4.2.0	3G security; Integration guidelines	BLANCHARD, Colin	Rel-4
TS	33.105	3.8.0	Cryptographic Algorithm requirements	CHIKAZAWA, Takeshi	R99
TS	33.105	4.1.0	Cryptographic Algorithm requirements	CHIKAZAWA, Takeshi	Rel-4
TS	33.106	3.1.0	Lawful interception requirements	WILHELM, Berthold	R99
TS	33.106	4.0.0	Lawful interception requirements	WILHELM, Berthold	Rel-4
TS	33.106	5.0.0	Lawful interception requirements	WILHELM, Berthold	Rel-5
TS	33.107	3.3.0	3G security; Lawful interception architecture and functions	WILHELM, Berthold	R99
TS	33.107	4.1.0	3G security; Lawful interception architecture and functions	WILHELM, Berthold	Rel-4
TS	33.107	5.0.0	3G security; Lawful interception architecture and functions	WILHELM, Berthold	Rel-5
TS	33.108	none	Lawful Interception; Handover Interface for Lawful Interception~~between core network and law agency equipment~~	~~WILHELM, Berthold~~Ron Ryan	Rel-5
TS	33.120	3.0.0	Security Objectives and Principles	WRIGHT, Tim	R99
TS	33.120	4.0.0	Security Objectives and Principles	WRIGHT, Tim	Rel-4
TS	33.200	4.1.0	Network Domain Security - MAP	ESCOTT, Adrian~~KOIEN, Geir~~	Rel-4
TS	33.201	none	Access domain security	POPE, Maurice	Rel-5
TS	33.203	0.4.0	Access Security for IP based services	BOMAN, Krister	Rel-5
TS	33.210	none	Network Domain Security - IP	KOIEN, Geir~~VACANT,~~	Rel-5
TR	33.800	0.3.5	Principles for Network Domain Security	ESCOTT, Adrian~~VACANT,~~	Rel-4
TR	33.800	none	Principles for Network Domain Security	ESCOTT, Adrian~~VACANT,~~	Rel-5
TR	33.900	0.4.1	Guide to 3G security	BROOKSON, Charles	Rel-5
TR	33.901	3.0.0	Criteria for cryptographic Algorithm design process	BLOM, Rolf	R99
TR	33.901	4.0.0	Criteria for cryptographic Algorithm design process	BLOM, Rolf	Rel-4
TR	33.902	3.1.0	Formal Analysis of the 3G Authentication Protocol	HORN, Guenther	R99
TR	33.902	4.0.0	Formal Analysis of the 3G Authentication Protocol	HORN, Guenther	Rel-4
TR	33.903	none	Access Security for IP based services	VACANT,	Rel-4
TR	33.903	none	Access Security for IP based services	VACANT,	Rel-5
TR	33.904	none	Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms	VACANT,	Rel-4
TR	33.908	3.0.0	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	WALKER, Michael	R99
TR	33.908	4.0.0	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	WALKER, Michael	Rel-4
TR	33.909	4.0.1	3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions	WALKER, Michael	Rel-4
TS	35.201	3.1.2	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	WALKER, Michael	R99
TS	35.201	4.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	WALKER, Michael	Rel-4
TS	35.202	3.1.2	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	WALKER, Michael	R99
TS	35.202	4.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	WALKER, Michael	Rel-4
TS	35.203	3.1.2	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	WALKER, Michael	R99

TS	35.203	4.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	WALKER, Michael	Rel-4
TS	35.204	3.1.2	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	WALKER, Michael	R99
TS	35.204	4.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	WALKER, Michael	Rel-4
TR	35.205	4.0.0	3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General	WALKER, Michael	Rel-4
TS	35.206	4.0.0	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification	WALKER, Michael	Rel-4
TS	35.207	4.0.0	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' test data	WALKER, Michael	Rel-4
TS	35.208	4.0.0	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	WALKER, Michael	Rel-4
TR	35.909	4.0.0	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	WALKER, Michael	Rel-4
TR	41.031	4.0.1	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	WRIGHT, Tim	Rel-4
TR	41.033	4.0.1	Lawful Interception requirements for GSM	MCKIBBEN, Bernie	Rel-4
TS	41.061	4.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	WALKER, Michael	Rel-4
TS	42.009	4.0.0	Security Aspects	CHRISTOFFERSSON, Per	Rel-4
TS	42.031	4.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 1	WRIGHT, Tim	Rel-4
TS	42.032	4.0.0	Immediate Service Termination (IST); Service description; Stage 1	WRIGHT, Tim	Rel-4
TS	42.033	4.0.0	Lawful Interception; Stage 1	MCKIBBEN, Bernie	Rel-4
TS	43.020	4.0.0	Security-related network functions	GILBERT, Henri	Rel-4
TS	43.031	4.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 2	WRIGHT, Tim	Rel-4
TS	43.033	4.0.0	Lawful Interception; Stage 2	MCKIBBEN, Bernie	Rel-4
TS	43.035	4.0.0	Immediate Service Termination (IST); Stage 2	WRIGHT, Tim	Rel-4

Annex D: List of CRs to specifications under SA WG3 responsibility agreed at this meeting

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WG status
33.200	017		Rel-4	Removing the Sending PLMN-Id from Security Header	F	4.1.0	S3-21	S3-010658	agreed
33.200	018		Rel-4	Protection Profile Revision Identifier	F	4.1.0	S3-21	S3-010691	agreed
33.200	019		Rel-4	Completing the specification of a MAPsec SA	F	4.1.0	S3-21	S3-010693	agreed
33.102	162		Rel-5	Configurability of cipher use	A	4.2.0	S3-21	S3-010679	agreed
35.201	001		R99	Correct the maximum input message length for f8 and f9	F	3.1.2	S3-21	S3-010689	agreed
35.201	002		Rel-4	Correct the maximum input message length for f8 and f9	A	4.0.0	S3-21	S3-010690	agreed

Note: The following CR was approved at this meeting (S3-010612), but had already been created and approved at meeting#20:

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WG status
33.107	016		Rel-5	Source of PDP context initiation	A	5.0.0	S3-20 / S3-21	S3-010518 / S3-010612	Agreed S3#20 / Agreed S3#21

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	Source TD	Comment/Status
S3-010564	Liaison Statement on AMR-WB and Legal Interception	N4-011199	For LI group. Forwarded to LI group for action.
S3-010565	LS to GSM-A TWG/SERG "regarding User Profile"	UP-010046	More information on the GUP should be sought. Actions 21/1 and 21/2.
S3-010566	Reply Liaison Statement On the use of Network Domain Security for protection of SIP signalling messages	N4-011205	Noted
S3-010567	Reply to Liaison Statement on Usage of Private ID	N4-011206	Noted
S3-010568	LS on Message size limitation for f9 algorithm	R2-012400	Removal of upper limit checked OK by SAGE. Noted.
S3-010569	Liaison Statement on Technical Solution for Prepaid Cards Using Smart Cards with Real-Time Clock	SCP-010291	Noted
S3-010570	Liaison Statement on IMS identifiers and ISIM	T3-010721	Dealt with at Joint session T3. Noted.
S3-010571	VASP MMS Connectivity	T2-010905	Response LS in S3-010698
S3-010572	LS from RAN WG3: WID: AMR-WB Speech Service – Core Network Aspects	R3-013037	Noted
S3-010573	Liaison Statement on Security of Rel5 IP Transport in UTRAN	R3-013064	Urgent Response requested. Response in S3-010662
S3-010575	LS on Enhanced user privacy for location services	S2-013063	Response LS in S3-010662
S3-010576	LS on IMS identifiers and ISIM and USIM	S2-013067	Dealt with at Joint session T3. Noted.
S3-010577	Reply to Liaison Statement on Usage of Private ID	S2-013069	Noted
S3-010578	Response to the LS S2-012896 from SA3 on Security Aspects related to the IMS Authentication	S2-013079	Noted
~~S3-010583~~	~~Update information on 33.210-060~~	~~S3-010429~~	~~33.200v060 attached. Presented by NDS/IP rapporteur. Noted.~~
S3-010585	LS from CN WG1 on IMS identifiers: Response to: LS (S2-013067) on IMS identifiers and ISIM and USIM	N1-011768	Dealt with at Joint session T3 and noted at SA WG3 meeting. Noted.
S3-010587	Liaison Statement on 3GPP Generic User Profile Stage 1	S1-011176	Noted
S3-010588	RE: Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem	S1-011190	Noted
S3-010589	Response to: Liaison Statement on Usage of Private ID	S1-011191	Noted
S3-010590	Liaison Statement on Revised Push Service Stage 1	S1-011252	Response LS in S3-010700.
S3-010591	Reply to LS on "Privacy Override Indicator"	S1-011286	Response LS in S3-010697.
S3-010592	Liaison Statement on DRM	S1-011300	Noted
S3-010593	Presence Service requirements	S1-011301	Response LS in S3-010699.
S3-010594	Answer to LS on requirements on Multimedia Broadcast/Multicast Service	S1-011310	Noted. Action 21/5 resulted.
S3-010595	Liaison Statement on UE functionality split	S1-011321	Dealt with at Joint session T3. Noted
S3-010596	RE: LS on IMS identifiers and ISIM and USIM (S2 Tdoc S2-013067)	~~T2~~T3-010730	Dealt with at Joint session T3. Noted
S3-010597	Cipher indicators and selection options in UMTS	SG Doc 113/01	Noted
S3-010599	Definition of the UICC	T3-010716	Dealt with at Joint session T3. Noted
S3-010621	Response to liaison from IPCablecom on LI	24td154r2	Forwarded to LI group
S3-010661	Liaison Statement on the Support of Up to Date Encryption Algorithms in the OSA Framework	N5-011159	Response LS in S3-010696

E.2 Liaisons from the meeting

TD number	Title	Comment/Status	TO	CC
S3-010647	Response LS on IMS identifiers and ISIM and USIM	Approved	**T3, SA2, SA1, CN1, T2**	**EP SCP**
S3-010654	LS to SA WG1 on P-CSCF triggered re-authentication	Approved	**SA2**	**SA5, CN1**

TD number	Title	Comment/Status	TO	CC
S3-010662	Response LS on Security of Rel5 IP Transport in UTRAN	Approved	**RAN3**	
S3-010668	LS to CN WG2: Implicitly registered IMPU(s) (revision of S3-010655)	Approved	**CN4**	
S3-010669	LS to CN WG1: IMS Security	Approved	**CN1**	
S3-010671	LS to CN WG4 on approved CR	Approved	**CN4**	
S3-010673	LS to CN1: Identity spoofing attacks in the IMS	Approved	**CN1, SA2**	
S3-010675	LS to CN WG1: Configurability of cipher use (CR in S3-010675 for info)	Approved	**CN1**	**T2**
S3-010682	LS to RAN2: Response to S3-010568 confirming changes requested	Approved	**RAN2**	
S3-010692	LS to TSG CN on General requirements for SA distribution over Ze interface	Approved	**TSG CN, CN4**	
S3-010696	Response LS to CN WG5: Re S3-010661	Approved	**CN5**	
S3-010697	Reply LS to SA WG1 on "Privacy Override Indicator"	Approved	**SA1, SA2**	
S3-010698	Response to LS T2-010905 (S3-010571) on VASP MMS connectivity	Approved	**T2**	**CN5**
S3-010699	LS to SA WG1 (CC S2, SA): Security and privacy requirements of presence	Approved	**SA1**	**SA2, SA**
S3-010700	LS to SA WG1, SA WG2: Response to: Liaison Statement on Revised Push Service Stage 1	Approved	**SA1, SA2**	
S3-010703	LS response to SA WG1 (S1-011321): UE Functionality Split	Approved	**SA1, SA2**	

Annex F: List of Actions from the meeting

Action 21/1: **Colin Blanchard to contact the editor of the GUP draft to determine the background and the rationale for the requirements in the security section (section 6)**

Action 21/2: **~~Steward~~ Stuart Ward to invite Paul Henry to give SA WG3 a briefing on GUP work.**

Action 21/3: **P. Howard to set up an e-mail discussion on this in order to produce a proposal for a CR to 29.198 for CN WG5.**

Action 21/4: **~~Steward~~ Stuart Ward to start off an e-mail discussion on Location Services Privacy and report back to SA WG3 meeting #22.**

Action 21/5: **A. Escott agreed to check the draft TS 22.146 and determine if any input is needed and report back to the next SA WG3 meeting.**

Action 21/6: **G. Rose to eveluate the EAP/SIM authentication technique to determine it's validity for increased authentication strength.**

Action 21/7: **D. Castellanos to set up an e-mail discussion on Presence service, with support from Nokia, Telenor and Vodafone.**