3GPP TSG SA WG3 Security — S3#21

27 - 30 November, 2001

Sophia Antipolis, France

3GPP TSG SA WG3 Security — S3#20   **Draft Report - version 1.0.0**

16-19 October, 2001

Sydney, Australia

Source:	**Secretary SA WG3 (Maurice Pope, MCC)**
Title:	**Report of SA WG3 meeting #20**
Status:	**Approved**

Front view   **Night View**   **Harbour view**

The Sydney Opera House

Contents

1   Opening of the meeting

The meeting was chaired by the vice Chairman, Mr. V. Niemi, who opened the meeting, welcoming delegates to Sydney. Mr G. Rose wecomed delegates to Sydney on behalf of the hosts, Qualcomm Europe. He provided the domestic arrangments for the meeting and for the social event (a starlight Harbour Cruise).

2   Meeting objectives and approval of the agenda

IPR Declaration: The Chairman reminded delegates of the 3GPP IPR policy and their obligation to declare essential IPRs to their respective Partner Organisations (SDOs).

TD S3-010405 The Chairman introduced the draft agenda. It was noted that the close of the meeting should be 19 October. A new item was added "7.11: PKI". The agenda, with these changes, was then approved.

The objectives were outlined as:

- Production of TSs 33.203, 33.210 and 33.200 Rel-5 to be provided to TSG SA#14, for information, in December 2001.

- Preparation of the action plan on IETF

- Progress the normal business of SA WG3 (Liaisons from other groups, etc.).

Adrian Escott reported that he could confirm that he could become Editor for TS 33.200 and TR 33.800. He was thanked for taking on this task.

Geir Koien is the editor for 33.210 and Krister Boman for TS 33.203.

3   Assignment of input documents

The available documents were assigned to their respective agenda items.

4   Approval of reports from 3GPP SA3 meetings

4.1   S3#19, 4-6 July, Newbury

TD S3-010406 Draft report of SA WG3 meeting #19. The report of the last meeting was reviewed and approved.

4.2   S3 MAPSEC ad hoc, 13 September, Sophia Antipolis

TD S3-010407 Draft report of MAP Sec ad-hoc meeting, 13 September 2001. The report was presented by the Chairman and reviewed.

E-mail "Veto" of CRs: It was reported that one CR had received comments, and that this had been updated to remove the unagreed parts from the CR before presentation to TSG SA where it was approved. There was a request for a formal approach for e-mail approval in SA WG3. Mr. Pope was asked to look for existing guidelines on this.

    Action: M Pope to find e-mail approval guidelines for 3GPP (if there are any).

The outstanding documents from the meeting were included in contributions to this meeting. The report was then approved.

4.3   S3 IMS ad hoc, 14 September, Sophia Antipolis

TD S3-010408 Draft report of IMS Sec ad-hoc meeting, 14 September 2001. The report was presented by the Chairman and reviewed. Under agenda item 6.3, the liaison that was produced did not seem to be available - it was decided to find the final LS that was sent to CN WG1 for discussion in the meeting. This was allocated to TD S3-010511 for discussion at this meeting under agenda item 7.3. The outstanding documents from the meeting were included in contributions to this meeting. The report was then approved.

5   Reports and liaisons from other groups

5.1   3GPP SA3 lawful interception sub-group

TD S3-010477 Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #3/01 on lawful interception. This is the written report which was provided verbally at the previous SA WG3 meeting and was provided for information and noted.

TD S3-010488 Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #4/01 on lawful interception. This was provided for information and presented by B. Wilhelm. Output documents from the meeting were presented to SA WG3 for information or approval as appropriate.

The report was noted.

TD S3-010487 Proposed CR to 33.107: Alignment of TS 33.107 for Release 5 to previous Releases (Rel-5). This was updated in TD S3-010513 and was approved.

TD S3-010478 Proposed CR to 33.107: Correct the MO-SMS and MT-SMS events (R99). This was updated in TD S3-010514 and was approved.

TD S3-010479 Proposed CR to 33.107: Correct the MO-SMS and MT-SMS events (Rel-4). This was updated in TD S3-010515 and was approved.

TD S3-010480 Proposed CR to 33.107: Correct the MO-SMS and MT-SMS events (Rel-5). This was updated in TD S3-010516 and was approved.

TD S3-010481 Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-4). SA WG3-LI group were asked to clarify if this change is really a technical correction (Category F) as the "Consequences if not approved" field stated "Missing functionality", which implies a Category "C" CR, which is not allowed for Release 4. The question should also be asked why, if this is Category "F", it is not reflected also in Release 1999. The CR was therefore postponed for a response.

TD S3-010482 Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-5). This was postponed for consideration by the LI group as for TD S3-010481.

TD S3-010483 Proposed CR to 33.107: Source of PDP context initiation (Rel-4). This was updated in TD S3-010517 and was approved.

TD S3-010484 Proposed CR to 33.107: Source of PDP context initiation (Rel-5). This was updated in TD S3-010518 and was approved.

TD S3-010485 Proposed CR to 33.107: Start of secondary interception of an active PDP context (Rel-4). This CR was approved.

TD S3-010486 Proposed CR to 33.107: Start of secondary interception of an active PDP context (Rel-5). This CR was approved.

TD S3-010500 Work Item Description: 3GPP Handover Interface for Lawful Interception. It was proposed that the LI group include the H/O interface work in the overall LI Work Item. The LI group was therefore asked to reconsider this WID and it was noted.

TD S3-010501 Draft 33.108 version 0.1.0. This was provided for information and was noted. It was reported that the target was to complete this for the SA WG3 November meeting, in order to present it to TSG SA for information in December 2001. Delegates were asked to review the current draft and contribute as necessary to the LI group.

5.2   3GPP SA plenary

TD S3-010521 Draft report of TSG SA meeting #13: version 0.0.5. The parts relevant to SA WG3 were presented by the Chairman.

NIST workshop: G. Rose reported on the workshop, where there was discussion on the contents of the draft FIPS on AES Modes of Operation, and it was generally agreed that counter-mode should be included. The group wished to release all 3 documents simultaneously, which may mean a delay to the release of the FIPS corresponding to NIST 800-xy. They did expect the draft to be available by end 2001, with an update later to include examples. It was concluded that it was safe to assume availability of AES and Modes of Operation FIPS for reference by 33.200 when needed.

TSG RAN WGs requested information on the IP Transport security and the SA WG3 Chairman had agreed that information on status would be provided to the relevant RAN WGs.

Digital Rights Management: A new WI was approved in TSG SA document TD SP-010577, which was shown on-screen for information (not provided as a TD to the SA WG3 meeting). Some work on security aspects in SA WG3 was implied by this WI. There was some discussion over whether 3GPP should be providing such services as part of the basic system, and different opinions on the whole DRM issue were provided (not reported in detail here). This discussion lead to the continuation of the handling of TD S3-010419 (see agenda item 5.3).

The report was then noted.

5.3   3GPP working groups   431,446R

TD S3-010410 Reply from CN WG1 LS on "Using a generic authentication scheme for SIP". This was presented by K. Boman. After some discussion, K. Boman agreed to produce a response to CN WG1 on references to specific SIP messages, which was provided in TD S3-010519 which was approved.

TD S3-010411 Liaison Statement from CN WG4 on 3GPP User Profiles. The User Profiles meeting took place, but SA WG3 did not feel it was necessary to attend at this early stage. The LS was noted.

TD S3-010412 LS to SA WG3 on Signalling for user authentication. This was related to a number of LSs which SA WG3 had sent to CN WG4 and contributions to the meeting as follows:

> TD S3-010503 Proposed response to LS S3z010105 from CN WG4 on signalling for user authentication. This was presented by Siemens and argued that, while it would be feasible for SA WG3 to define the security procedures for this case, it would introduce considerable complexity. It therefore asks SA WG2 to reconsider their approach and, if ever possible, base Release 5 of IMS on the assumption that only one S-CSCF is assigned to one Private ID at any one time. There was some discussion and clarification to the LS, which was updated in TD S3-010522. This proposal was modified slightly and provided in TD S3-010540 which was approved.

TD S3-010432 LS response to SA3 on "Using a generic authentication scheme for SIP". This was presented by Ericsson and reported the conclusions on the analysis of the use of EAP and Diameter NASREQ in the Cx interface. The LS was noted.

TD S3-010439 Liaison Statement on "Flows related to Authenticated Registrations and Re-Registrations". This was presented by Lucent. SA WG3 agreed and noted that optimisations or changes to the flows should not be made that make the I-CSCF either transaction stateful or call stateful. The LS was then noted.

TD S3-010440 Reply LS on rejection of 2G AKA by 3G ME with USIM in UTRAN. This was presented by Ericsson and reported that CN WG1 confirm that TS 24.008 now takes account of the SA WG3 requirement that should a 3G ME with USIM being served by a UTRAN be asked to do a 2G AKA, the 3G ME shall fail that authentication attempt by the network and allow the network to repeat the AKA. Should the second AKA attempt again fail, the 3G ME should consider that cell barred for a period of time. This was in agreement with the request of SA WG3. Concerning the suggestion from T WG3 and the response from CN WG1, it was agreed that a response should be sent to T WG3 and CN WG1 to clarify the security reasons for the mechanism, which was provided in TD S3-010523 which was approved.

TD S3-010441 Liaison Statement from CN WG1on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem. This was presented by Lucent and requests information from SA WG1. The LS was noted. It was reported that there was a table included in TS 33.203 with open issues including this issue.

TD S3-010442 Response from CN WG1 to LS "On the use of Network Domain Security for protection of SIP signalling messages" (N1-011041 or S3-010403). This was presented by the Chairman and discussed. It was felt that the LS sent to CN WG1 had created some confusion and clarification on the assumptions made by SA WG3 on confidentiality protection between the UE and the P-CSCF were needed. It was agreed to revisit this LS and the related LS from SA WG2 in TD S3-010433, under agenda item 7.3.

TD S3-010443 Response to Liaison Statement on "Progressing the work in SA3 and CN1 on the IP Multimedia core network subsystem". This was presented by Lucent and responded to questions posed by SA WG3 in TD S3-010404. The LS was noted.

TD S3-010452 Liaison Statement from CN WG1 on Usage of Private ID. This was presented by Ericsson and asks SA WG3:

1) To verify whether it is acceptable to transport the private user identifier in the optional (from the SIP perspective) Authentication header value of the REGISTER message instead of the mandatory (from the SIP perspective) From header value. This will effectively mandate the Authorization header in 3GPP-IMS UEs.

2) Does SA3 foresee any additional security issues with the proposed approach?

3) To respond regarding whether there is an impact to the date when the specification/documentation containing the Authentication Protocol and header details including the transport of the Private User ID would be available for Rel-5 if the approach contained in N1-011355 was adopted by CN1.

It was agreed to include the responses to these questions, and the basic problems identified in this proposal, in an LS to the addressed groups, in TD S3-010524: this was updated in TD S3-010539 which was approved.

TD S3-010453 LS from TSG CN on the WID: AMR-WB Speech Service - Core Network Aspects. This was presented by Vodafone and informed SA WG3 of a new WI approved by TSG CN. The need for study of Lawful Interception by SA WG3 was identified by TSG CN. It was agreed that the LI group should study this and the LS was forwarded to them (to be sent by M. Pope to the LI group e-mail list and presented by B. Wilhelm at their meeting next week). Concerning voice group calls, delegates were asked to check if there were any other potential security aspects not identified by TSG CN and contribute to SA WG3 meeting #21. The LS was then noted by SA WG3.

TD S3-010413 LS from RAN WG2 on Guidance Needed Concerning Security Mode Reconfiguration. This was presented by the Chairman and asked SA WG3 "*Is it possible that the ciphering algorithm or/and the integrity protection algorithm is changed while the security key set is kept unchanged during the security mode reconfiguration?*". It was recognised that a mechanism needs to be included in the SA WG3 specifications, but this is not a problem at present, as there is only a single algorithm. No solution could be agreed upon quickly in the meeting and it was agreed to draft a response with the current situation to RAN WG2. This was provided in TD S3-010525 which was updated in TD S3-010555 and approved.

TD S3-010414 Reply from SA WG1 to LS on New feature for SAT originated SMS. This was presented by Motorola for information and was noted.

TD S3-010415 Liaison Statement from SA WG1 on "IMS security and UE functionality split". This was presented by Motorola. This was covered after consideration of related contributions under agenda item 7.3 (see also related LS in TD S3-010548).

TD S3-010416 IP Based Multimedia Services Framework Report. This was presented by Motorola on behalf of SPC for information and was noted. It was agreed that the content of relevant sections should be reviewed by SA WG3 delegates to comment to the next SA WG3 meeting. The LI group were asked to look at the Lawful Interception parts (M. Pope to forward this document to the LI group e-mail list).

TD S3-010420 LS on Cell ID in SIP messages. This reports that it is expected that Cx interface should provide the ability for the HSS to control whether the S-CSCF is allowed to (or prohibited from) supplying the cell identification to other nodes and asks whether these levels of control will satisfy privacy (and other) requirements. Replies had been received in the following document:

> TD S3-010417 Reply from SA WG1 to SA WG2 LS on Cell ID in SIP messages. SA WG1 reported that they asked whether these levels of control will satisfy privacy (and other) requirements. It was recognised that this requires further study in SA WG3.

A response to these LSs was drafted in TD S3-010526 which was approved.

TD S3-010418 LS from SA WG1 on Multimedia Broadcast/Multicast Service (MBMS). This was provided for information and a response from GERAN was available in TD S3-010431. The LS was noted.

TD S3-010431 Liaison statement on requirements on Multimedia Broadcast/Multicast Service. Delegates were asked to look at the comments from TSG GERAN and the document as a whole and was noted.

TD S3-010419 LS from SA WG1 on "Digital Rights Management". This was introduced by Nokia. It was noted that TSG SA had approved a WI on DRM and that there will be some impact on the work of

SA WG3. This document, along with TD S3-010436 were postponed to after the consideration of the draft report of the TSG SA Plenary (agenda item 5.2). It was recognised that there seemed to be confusion by SA WG2, and they need to consider both the illegal downloading of content, and the illegal copying or modification of content, which may have been legally downloaded. P. Howard agreed to draft a response LS to SA WG1, which was provided in TD S3-010532 and was approved.

TD S3-010424 MMS digital rights management. This was provided by T WG2 for information to SA WG3 and was noted.

TD S3-010436 LS from SA WG4 on Digital Rights Management (DRM) requirements for PSS Rel-5. This was introduced by Ericsson and asked for a reduction in the scope of DRM for Rel-5. This was provided by SA WG4 for information to SA WG3 and was noted.

TD S3-010421 LS from SA WG5 in reply to SA WG2 Liaison "WI on the End-to-End QoS Architecture for Release 5" (S2-011098). This was copied to SA WG3 for information. Section 7.6 (Security Management) was considered and delegates were asked to review this section and comment to the next SA WG3 meeting if necessary. The LS was then noted.

TD S3-010422 Reply from SA WG5 to LS on basic and advanced services examples (S1-010271 / S5-010302). This was copied to SA WG3 for information and was noted.

TD S3-010423 Use of the phrase "X interface". This reply from SA WG5 to an LS to them and clarified that SA WG5 are obliged to use the term "X-interface" in their ITU related work and that there should be no confusion with the 3GPP Security X-interfaces. The LS was then noted.

TD S3-010425 Transmission of user identity from a GGSN to MMS Relay/Server. This was provided by T WG2 for information and presented by Nokia. The LS was noted.

TD S3-010428 LS from SA WG1 on stage 1 for Extended Streaming Service. This was presented by Ericsson and informed the 3GPP WGs of their new WI on Extended Streaming Services and asked for input to a Streaming ad-hoc meeting. The LS was noted and delegates were asked to review the document and input comments to their SA WG1 colleagues.

TD S3-010437 Reply to LS on stage 1 for Extended Streaming Service. This was provided for information and was noted.

TD S3-010448 Liaison Statement from T WG2 on Extended Streaming Service. This was provided for information and was noted.

TD S3-010434 LS from SA WG2 on Security aspects of the 3GPP push service. SA WG2 asked SA WG3 to provide advice on the security aspects of the different Push architectures which are under consideration. In particular the mechanisms by which a subscriber can (a) avoid being pushed unwanted content and (b) avoid automatic connection by the mobile to Push servers that are not in the (home/subscriber's preferred) operator's domain. An attached document, TR 23.974 version 0.2.0, was reviewed for security aspects. It was recognised that this would require a more detailed review and a separate session would be needed. P. Howard agreed to check the timing of a response for this and report back to the meeting. It was agreed that delegates should try to provide good contribution to the next meeting concerning Push architectures, otherwise it may be necessary to form a drafting group on this subject. The document embedded in TD S3-010434 should be used as a basis.

TD S3-010438 LS from SA WG5 on "Access Point Name" usage. This was provided by SA WG5 and requested all TSG SA and TSG CN WGs to take any necessary action to ensure that there are no contradictions or potential ambiguities between their TSs and TS 32.215. The document was provided in TD S3-010527 for this purpose. **Delegates were asked to review this after the meeting and provide any identified ambiguities or contradictions to the next meeting**.

TD S3-010444 LS from T WG2 to SyncML Requesting DevMan Update. This was provided to SA WG3 for information and was noted.

TD S3-010447 LS from T WG2: Response to SA5 on Multiple Aspects of Device Management. This was provided to SA WG3 for information and was noted.

TD S3-010446 LS from T WG2 to SA WG3 cc SA WG5, SA WG1, T WG3 on Security Needs for Terminal Applications. This was discussed and it was considered that more information was needed and the SyncML specification and 3GPP documents referring to it were needed. D. Castellanos agreed to send an e-mail to obtain this information and the discussion was postponed until an answer was received. The following URL for DEVMAN specifications was provided after the meeting: http://www.syncml.org

Any delegate with material for discussion should also send it to the e-mail list.

TD S3-010445 LS from T WG2: Response to T2-010617 (LS from SA WG2 on Cell ID in SIP messages). This was copied to SA WG3 for information and was noted.

TD S3-010449 Liaison statement from T WG2 in response to LS S3-010226 regarding revision of MExE security analysis activity WID proposed in S3-010228. The T WG2 MExE group provided SA WG3 with the proposed WID on Generic User Profile which is linked to device management (attached to the LS). The Security Aspects part of this WID states *"Access to the 3GPP Generic User Profile data shall be performed in a secure and authenticated manner, and the integrity of user profile information shall be assured"*. Ericsson provided a related contribution: TD S3-010530, which they introduced. This included a presentation from T WG2, intended as a starting point of discussions on this matter at SA WG3. It should be also considered as the starting point of co-operation with T WGs in order to agree on the best way to accomplish the related work. This was presented by Ericsson. There was some discussion on the role of SA WG3 in MExE Security issues raised in the presentation, and it was agreed that delegates should consider this and contribute to the next SA WG3 meeting on proposals for SA WG3 role in the security work. The documents were then noted.

TD S3-010451 Liaison Statement from T WG3 on IMS identifiers and ISIM or TSIM (response to LS from SA WG3 in TD S3-010400). T WG3 reported their understanding that the private and public identifiers for the IP Multimedia Subsystem are independent of the USIM and should be stored in the ISIM instead of USIM and asked for this to be clarified. It was decided that T WG3 should be informed that these are different logical entities, and it is recognised, that for Rel-5, it will be best to include ISIM as part of the USIM application, rather than physically separated. Concerning the request for an ad-hoc meeting, it was not possible to do so in October, but may be possible on 26 November, pre-pended to the next SA WG3 meeting. A reply LS stating that the only feasible way to implement ISIM would be to physically group them for Rel-5, and physically separated entities required further study of the security issues and the potential duplication of functionality that would be required. The concept of "application" used in the LS to T WG3 (TD S3-010400) also needed to be clarified, as it may be different from the understanding of the term in T WG3. G. Rose agreed to draft a liaison, which was provided in TD S3-010531 which was updated in TD S3-010548 and revised again to include SA WG1 in the "TO" list, in TD S3-010554 which was approved.

TD S3-010454 PKCS#15 support for MExE in the USIM. This was provided by T WG2 for information and was presented by Vodafone. The LS was noted.

5.4   ETSI SAGE

Per Christofferssen provided a verbal report on the work of ETSI SAGE. There was disagreement between the GSMA and 3GPP on the funding and distribution/ownership of the A5/3 algorithm. This was noted.

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

GSMA: Charles Brookson could not attend the meeting, but provided information on the e-mail list, an extract of which was provided in TD S3-010533. This was presented by the Chairman. It was reported that GSMA document SG07 (availability restricted to GSMA Members) had been updated to include GPRS Fraud threats. Threats on forwarding services had been analysed and some information will be added to 33.900. User Identification (UCI) was also being considered for inclusion in 33.900. The document was noted.

TIA TR-45: Greg Rose provided an informal report on the 3GPP2/AHAG discussions. A new 3GPP2 TSG S-WG4 has been created for security issues (F. Quick Chairman, M. Marcovici Vice Chairman). The Joint Control agreement document responsibility may be desirable to be transferred to the new WG4, but this had not yet been decided between AHAG and S-WG4. This was noted.

6   Technical specifications and reports

6.1   Security architecture (TS 33.102)

TD S3-010455 Proposed CR to 33.102 (R99): Annex F.2 (changing list parameters) modification. This was presented by Siemens. This CR was agreed.

TD S3-010456 Proposed CR to 33.102 (Rel-4): Annex F.2 (changing list parameters) modification. This CR was agreed.

TD S3-010457 Proposed CR to 33.102 (R99): SQNMS retrieval in AuC during resynchronisation. This was presented by Siemens. This CR was agreed.

TD S3-010458 Proposed CR to 33.102 (Rel-4): SQNMS retrieval in AuC during resynchronisation. This CR was agreed.

TD S3-010459 Proposed CR to 33.102 (R99): Sequence Number Management Corrections. This was presented by Siemens. The C.2 addition should be in italic font. The CR was modified editorially for the cover sheet and provided in TD S3-010534 which was agreed.

TD S3-010460 Proposed CR to 33.102 (Rel-4): Sequence Number Management Corrections. This modified editorially for the cover sheet (as for TD S3-010459) and provided in TD S3-010535 which was agreed.

TD S3-010474 Proposed CR to 33.103 v 3.9.0: Alignments with 25.331. This was presented by Nokia. The CR intended to align with RAN WG4 interpretation of the THRESHOLD use - RAN WG4 had included "> *THRESHOLD*" in their specifications, whereas "$\geq$ *THRESHOLD*" had been intended by SA WG3. This change needed further consideration, as it affects more areas of the specifications than indicated in the CR. It was decided to postpone this CR to the next meeting after analysis of all the consequences of this change is done.

TD S3-010475 Proposed CR to 33.103 v 4.2.0: Alignments with 25.331. It was decided to postpone this CR as for TD S3-010474.

TD S3-010476 Security concern with HFN reset procedure. This was presented by Qualcomm and discusses some vulnerabilities with the RLC Reset procedure, which was introduced in Release 1999 TS 25.322 with a CR approved at TSG RAN#10 in December 2000. It proposed that RAN WG2 should take a second look at the problem discussed in their e-mail exchange, which led to this change, and solve it differently, by using methods that do not compromise security. During discussion, it was clarified that some of the problems were already present before the change, but changes such as this without consultation with SA WG3 should be avoided. It was agreed that a LS should be sent to RAN WG2 showing the examples of potential problems, requesting consultation on changes that are made to security sensitive mechanisms and informing them that the HFN is used in security mechanisms. This was provided in TD S3-010537 which was updated in TD S3-010556 and approved. Possible changes to specifications to overcome these problems should be considered by delegates to determine if any changes should be made to RAN specifications (significant threats would need to be identified in order to propose CRs to Release 1999 specifications).

6.2   Guide to 3G security (TR 33.900)

TD S3-010430 33.900 - Guide to 3G Security version 0.4.1. The document was reviewed and some discussion over what the content of the document should be ensued. The inclusion of as many identified threats as possible against only those for which solutions are available in the architecture. It was agreed that more threat descriptions should be included to identify potential problems to Operators. The editors were asked to update the document to include more general descriptions of threats for the next SA WG3 meeting (November 2001). All delegates were asked to contact Colin Blanchard or Charles Brookson to help with this update.

7   Work items

7.1   MAP security (TS 33.200, draft TR 33.800)

TD S3-010450 Siemens Comments to MAP-doI v3 <draft-arkko-map-doi-03>. This was introduced by Siemens. It was noted and there was a response to these comments from Ericsson in TD S3-010508 which was taken for discussion.

TD S3-010508 Reply to comments on MAPSec-DOI. This was presented by Ericsson with the aim of getting agreement on final comments to MAPSec DOI for submission to the IETF. Each comment/response was reviewed and discussed. The comments were taken into account in the updated version (MAP-doi-04-pa1.txt) included in TD S3-010508. Further comments to the draft were invited before the IETF editor forwards the document to the IETF. Absolute time versus duration was discussed, and A. Escott was asked to add the to 33.800 as a placeholder. 2 weeks (2nd September) for comments was agreed - comments should be sent to the editor.

TD S3-010462 MAPsec counter mode of operation. This was presented by Siemens and provides the status of the alternative documents for proposes to use the counter mode of operation as described in NIST 800-XXX that will be stable end of this year instead of the counter mode of operation as drafted in SC 27 N 2711 (Enhancement of ISO/IEC 10116) that is intended to become a new standard in 2003. It was proposed that the FIPS standard is referred to until the end of 2001, and a proposal to take MAC from the same source.

It was proposed to take the Siemens proposal, but to add an editors note, warning that the algorithm chosen may change if it not available in time (end 2001).

It was agreed, after some debate, that a reference would be made to (NIST) FIPS-800-XXX (July 2001) in the specification, to be modified to the final version when it is available, or replaced by the text of the draft if the final version is incompatible with the requirements.

A proposed CR to 33.200 was also provided in this contribution. The CR was given a separate document number in TD S3-010538 and was approved: The strategy was agreed as **to include a reference to a draft NIST document, which may not be available after their document is published. A CR to update the reference if the final counter mode is compatible with requirements will be made, or the relevant text of the draft NIST standard will be included in 33.200.**

TD S3-010464 NIST Special Publication 800-XX: Recommendation for Block Cipher Modes of Operation. This was provided for information in the above discussions and was noted.

TD S3-010467 Proposed CR to 33.200 v 4.1.0: The Soft Lifetime for the MAPSec SA. This was presented by Nokia. The concept of the second timer "soft lifetime" was accepted, but it was thought that this could be calculated as a function of the "hard lifetime" and removed from the SA. It was proposed that this was also needed in Rel-4, where the use of manual key management makes the SA changeover guarding procedure more critical. It was decided to set up an evening drafting group to try to provide a solution and required CRs. TD S3-010467 was then postponed pending the results of this drafting group. The drafting group provided TD S3-010549 " Proposed CR to 33.200 v 4.1.0: The Soft Lifetime for the MAPsec SA (revised after drafting session)" which was reviewed and revised in TD S3-010560 which was approved.

TD S3-010528 (Replacement of TD S3-010426) Proposed Updates to Structures of SADB and SPD on MAPSec. This proposed solution would have implied problems which do not exist with the current solution and the proposal was not agreed.

TD S3-010471 Proposed CR to 33.200 v4.1.0: Use of 'Original component identifier' during MAPsec processing. This was presented by Siemens and was approved.

TD S3-010472 Proposed CR to 33.200 v4.1.0: Protection Profiles correction. This was presented by Siemens and was updated to include the reason for removing the editors note and provided in TD S3-010541 which was approved.

TD S3-010473 Proposed CR to 33.200 v4.1.0: Policy configuration clarification. This was presented by Siemens and the consequences if not approved part was updated and provided in TD S3-010542 which was approved.

TD S3-010492 Flexibility of MAP Protection Profiles. This was presented by Hutchison 3G UK, and proposes that a weakness of the non-flexible protection profiles is that it would require un update to the standard in order to patch any problems found in the future and suggests a solution for inclusion in TS 33.200 and asks SA WG3 to make some decisions on the following suggested principles:

- It must be possible to increase the level of protection on messages independently of defining new standard protection groups.

- Proprietary protection profiles must be implemented.

- The split between standard and proprietary PPI.

It was clarified that if a security breach is discovered, then there will be no way of protecting against it if the vulnerable messages are not in the standardised Protection Profiles.

There were mixed opinions on the inclusion of either a "Proprietary" PP or a "Full Protection" PP. More information on the working of the Proprietary PP mechanism was needed. It was agreed that the issue should be considered by delegates and contribution on the topic for the next meeting are invited. The associated CR in TD S3-010493 was then postponed pending further discussion.

TD S3-010498 Some potential changes for MAPSec. This was presented by Hutchison 3G UK, and contained several suggestions for changes to TS 33.200. It requested that SA WG3 make a decision on each of the possible changes, in order that the relevant CRs can be prepared.

Checking the Sending PLMN-Id from the security header

Proposal to remove the Sending PLMN-Id from the security header, as it is purely redundant information and to alter the message flow to plug a security weakness. This was agreed in principle and a CR should be provided to the next meeting.

Protection Mode 0 Security Headers

Proposal to remove TVP, NE-Id and Prop from the security header of Protection Mode 0 messages. This was agreed in principle as this is not a security feature.

SA Identifiers

Proposal of adding destination PLMN-Id and SPI to the SA and that the sending PLMN-Id is included in the SA for completeness. This was in need of further consideration. Hutchison 3G UK were asked to send a message to the list as a reminder and to start an e-mail discussion on this.

Alignment of TS 29.002 and TS 33.200

TS 29.002 uses Prop and NE-Id as optional, whereas TS 33.200 specifies them as mandatory. A CR to 29.002 is required to correct this. Hutchison 3G UK agreed to write a LS to CN WG4 informing them of the problem, but during the drafting of this it was realised that a formal LS was not required as this information could be done verbally, so that any CN WG4 CRs on this could be conditionally approved at TSG CN Plenary pending approval of the corresponding SA WG3 CRs in TSG SA Plenary. The allocated document for the LS, TD S3-010543 was therefore withdrawn.

Hutchison 3G UK were asked to provide relevant CRs and contribution to the next SA WG3 meeting resulting from the above agreements and e-mail discussions.

TD S3-010507 Resubmission of TD S3-010368: Local Security Association Distribution. This was presented by Alcatel and discusses the generic architecture as currently described in TR 33.800 and suggests possible protocols to achieve intra-domain SA management:

Security Policy in NEs

Proposes that the NE needs some minimal policy information (to be distributed from the KAC). It was agreed that the NE has no decision making on this. The KAC controls the policy information and provides necessary information to the NEs.

Pull Mechanism

Suggests that this is not practical and that consequently, the architecture should allow for both push and pull mechanisms. It was considered that a push mechanism is needed for the Policy database and a pull mechanism for the SA database. The difference between the push mechanism for revoking SAs and the use of a push mechanism for distribution of SAs was questioned. There could be an implementation difference due to the different frequency of their expected usage, but the standardisation differences are small. The issue was considered too involved to make a decision at this meeting, although the availability of both push and pull mechanisms in both databases seemed useful. Further analysis should be done before making decisions on this. It was considered that the usual case for both databases should be push, and in exception cases pull. **It was decided that an e-mail discussion should be made to try to agree on a mechanism, and contribution, on detailed mechanisms and analysis of them, should be made to the next meeting.**

SA Lifetime Supervision

Proposes that although the KAC may have negotiated two SAs, only one should be valid at a given time. For outbound traffic, the NE should always use the SA which expires the sooner. For inbound traffic, the NE should use the SA indicated in the received MAP message. **This was covered by other contributions.**

Management Protocol over IPsec

Proposal that rather than a new protocol, existing policy protocols, such as COPS, may be considered.

New IKE Phase 2

In the solution proposed above, IKE Phase 1 is used to set up a secure communication channel between the KAC and the NE. A new DoI is specified in which the KAC sends the SA information together with the related policy to the NE.

Secure Multicast

Notes that security multicast solutions being developed within the IETF are not ready yet and should be expected in a timeframe of one year at the earliest.

The use of IPsec is covered by NDS-IP document (33.210) and this should be discussed in the context of NDS-IP.

TD S3-010510 TS 33.800 version 0.4.0: Principles for Network Domain Security; MAP application layer security. This was provided for information and was noted.

TD S3-010528 Proposed Updates to Structures of SADB and SPD on MAPSec. This was presented by Huawei Technologies and proposed that PPI should be moved from the Security Association Database (SAD) to the Security Policy Database (SPD) and SPI should be a mandated parameter in the SAD. A proposed CR was provided in the attachment to this document. Problems were found with the negotiation of SAs and resulting synchronisation of the Security Policies if the PPI is moved into the SPD. The speed argument was not considered relevant, as the PPI is not needed until step 6, and by then the SA is known. Due to lack of support, the proposal was rejected.

7.2   IP network layer security (draft TS 33.210)

TD S3-010489 Proposed changes to 33.210 about defining the BG element. This was presented by Nokia and proposed clarifications to the text concerning Border Gateway (BG) definition. The document was discussed briefly, (concerning the text for BG) and was noted (to be discussed further).

TD S3-010490 Proposed changes to 33.210 about GGSN – P-CSCF interface (Go). This was presented by Nokia and proposed that the interface between GGSN and P-CSCF (the Go interface) is protected by the network domain security as already assumed in TS 33.203 v0.6.0. It was considered that this needed further study and was not accepted for inclusion in the TS at present. The proposal was noted.

TD S3-010496 Proposed changes to 33.210 about protecting GTP-U. This was presented by Nokia and proposed clarifications to the text concerning GTP-U protection. This was discussed briefly, and will be updated and resubmitted to the next meeting. The contribution was then noted.

TD S3-010429 and TD S3-010529 were postponed to next meeting:

7.3   IP multimedia subsystem security (draft TS 33.203)

TD S3-010545 aSIP-Access Security for IP-Based Services. These slides were presented by K. Boman (Ericsson) and provided a status and time plan for the completion of TS 33.203. Some discussion over the timescales and procedure for updating and finalising the IETF documents ensued. S3z010128 was consulted, but didn't provide useful guidance on the problem of providing agreed solutions to IETF. A long discussion resulted in no progress and it was decided to continue with the update of 33.203 in order to have a set of agreed solutions and to return to this problem later. **There was no time in this meeting to continue with this so it was deferred to off-line discussions and contribution at the next meeting**.

SA WG3 delegates were asked to provide updates to 33.203 and in particular, to provide input to remove the FFS and editors' notes in order to help finalise the document. Contributions should be provided using "pseudo-CRs" wherever possible, to ease the identification, discussion and incorporation of the changes in the document.

K. Boman was thanked for the presentation.

TD S3-010529 Update Proposal on Security Domain

Responses to LS from SA WG3 in TD S3-010403.

TD S3-010442 Response from CN WG1 to LS "On the use of Network Domain Security for protection of SIP signalling messages" (N1-011041 or S3-010403). This was presented by the Chairman.

CN WG1 had discussed the potential solutions included in S3-010403 and believes that, if SIP

protection is going to be based on NDS/IP mechanisms (i.e. not between the UE and the P-CSCF but rather within the network in a hop-by-hop fashion), then it is preferred to specify a solution that:

- *can be applied on both Iu-ps and Gn/Gp interfaces, and*

- *cause minimum or no impact on UMTS architecture and protocols.*

In this context, CN WG1 would be interested to know if SA WG3 has investigated any solutions inline with the above preferences. For instance, has SA WG3 investigated the limitations of option 2 in S3-010403? Has SA WG3 considered any potential extensions to IPsec (on Iu-ps and Gn/Gp) as alternative solutions? Such extensions wouldn't have an impact on the UMTS architecture or protocols.

TD S3-010433 LS from SA WG2: Response to LS S3-010403 on the use of Network Domain Security for protection of SIP signalling messages from SA WG3.

Alternative 2 (protect all GTP-U messages) *is inefficient since only a small percentage of the GTP-U messages are IMS SIP messages.*

Solutions 3 (to introduce GTP-IC) *and 4* (to extend GTP-C) *assume that RAN has knowledge of which IP packets carry SIP signalling. Currently RAN is not aware of contents of IP packets.*

SA WG2 would like to understand what requirements are being addressed here? It is SA WG2's understanding that the protection of SIP messages between the UE and P-CSCF is covered with Access Security (integrity protection) and the security between different CSCFs is covered via NDS. SA WG2 has difficulty understanding the security requirements to GTP-U related to IMS.

Action: *SA WG2 would like to understand what security issue is being addressed here that is not already covered via SIP application level security and network domain security.*

SA WG3 Discussion and conclusions:

TD S3-010470 IMS access domain security and NDS. This was presented by Siemens and aimed to clarify the current discussion related to the protection of IMS signalling between UE and P-CSCF, and proposes **not** to use Rel-5 network domain security means to secure this specific signalling, since end-to-end protection between UE and P-CSCF will already be provided by the IMS itself.

In figure 1, the Zc interface between SGSN and GGSN and between GGSN and P-CSCF in the UMTS CN seemed to be the cause of confusion in CN WG1, as it implied that this was part of NDS Security.

Siemens did not see any additional benefits from a security point of view, over the protection already provided by the IMS, that justifies the additional effort of any of the solutions 2 to 4, particularly as SIP signalling messages are only a very small part of GTP-U traffic, and may cause unacceptable delays in real-time traffic. Therefore Siemens proposed to agree within SA3 on the working assumption that no PS core network domain security means are required for protecting IMS access network signalling (signalling between UE and P-CSCF)

TD S3-010546 Confidentiality of SIP signalling between UE and P-CSCF. This was presented by Hutchinson 3G and proposed that aSIP security (i.e. IMS access network security) should be independent from NDS and that no reliance on NDS should be assumed. TS 33.203 should reflect this viewpoint. The principles were agreed and a Liaison to SA WG2, CN WG1 (CC CN WG4) was provided in TD S3-010547 which was modified and provided in TD S3-010557 and approved.

TD S3-010468 ISIM/USIM independence. This was presented by Telia and highlights incorrect and inconsistent definitions of UICC in specifications. Telia were asked to produce CR to TS 21.133 to align and correct these definitions by referring to the 3GPP Vocabulary (TR 21.905). This CR was provided in TD S3-010552 "CR to 21.133 - Definition of UICC": This was modified slightly and provided in TD S3-010558 and the CR was approved. A corresponding Rel-4 CR was provided in TD S3-010559 and approved.

The USIM/ISIM issue was covered by the LS approved in TD S3-010548.

TD S3-010469 ISIM/USIM independence. This was covered by other contributions and discussions.

TD S3-010491 <draft-garcia-sipping-3gpp-reqs-00.txt>. This was provided for information and contained the draft 3GPP requirements now forwarded to the IETF. The document was noted.

TD S3-010494 On access independence and authentication. This was presented by Ericsson and proposed that IMS AKA shall be one option for the operators to authenticate the IM subscribers. TS 33.203 shall not exclude other IETF mechanisms e.g. already existent in SIP like HTTP Digest. If the operators policy states that IMS AKA should be used, then TS 33.203 needs to provide the appropriate requirements for this. It was clarified that the Rel-5 was still AKA-based and could not provide all the features provided in this contributions. For Access Independence, it was noted that the IMS-AKA can also be used for other accesses. It was questioned whether this provides an advantage if introduced into Rel-5, when it will only be used for Rel-6, as Access Independence is not being worked on for Rel-5 in other WGs. There was no consensus to include this in Rel-5 and it should be considered further for Rel-6, or in the next SA WG3 meeting if Ericsson wish to further discuss the introduction of this in Rel-5.

TD S3-010435 LS from SA WG2: Security aspects for IMS related to Authentication. (postponed from the ad-hoc meeting). This was presented by Siemens and answered some questions that SA WG2 had received, and requested the following from SA WG3:

> *Subscribers may have different service profiles just as requested by SA WG1. SA WG2 assumes that each Public ID belongs to a single service profile, but a single service profile may have several Public IDs. Furthermore, different service profiles may be assigned to different S-CSCFs even when these service profiles have the same Private ID. However these service profiles shall have a different set of Public IDs. SA WG2 kindly asks SA WG3 to respond if this work assumption significantly increases the SA WG3 work load such that the Release 5 IMS security standardisation can not be completed on time.*

Ericsson and Siemens provided contributions on this in TD S3-010495 and TD S3-010544 and a proposed response LS was provided by Siemens in TD S3-010550.

TD S3-010495 On registering several public identities in IM CN SS. This was presented by Ericsson and discussed different requirements needed and different alternatives on how to register several public identities in IM CN SS. Ericsson proposed that the UE and the P-CSCF shall establish just one SA through which all the SIP signalling between the UE and the P-CSCF is carried, and that further discussions are needed to decide on the needed optimisations. Ericsson assumed that the optimisations in sections 3.3.1 and 3.3.2 of this contribution could be used in combination or separately. It was clarified that in 3.3.2, the mechanism would update the SA on each new Public ID registration, and not set up new SAs for each Public identity. The proposal to have only one SA between the user and P-CSCF was agreed.

TD S3-010544 Security Association Management in the IMS. This was presented by Siemens and discussed the problems of complexity in introducing the functionality as in SA WG2's working assumption and suggests that resolution of the problems could cause a significant delay to Rel-5 IMS security work. Siemens conclude that SA WG3 should propose to SA WG2 to reconsider their approach to allow different S-CSCFs to be assigned for registrations with different public IDs of one user at a time, at least for Rel-5. This was discussed at length, and it was noted that this showed one set of assumptions, which showed the resulting complexity, and other sets of assumptions and solutions need to be considered before asking SA WG2 to reconsider their architecture assumptions.

TD S3-010550 (Replacement of TD S3-010502) Response to LS S2-012456 from SA2 on Security aspects for IMS related to Authentication. This was presented by Siemens. TD S3-010544 and TD S3-010495 were intended as attachments. The LS concludes that given the high workload of SA WG3 and the significant amount of IMS security work which still has to be done to complete Rel'5 there is indeed a possibility that the additional specification work required by SA WG2's working assumption may negatively affect SA WG3's ability to complete IMS security in time. It was decided that the LS should not include the attachments, and the LS was updated and provided in TD S3-010551 which was approved.

TD S3-010497 EAP Extensions - status report. This was provided by Ericsson and Nokia and was presented by Ericsson. It briefly describes the current status of IETF standardization efforts related to the use of Extensible Authentication Protocol (EAP) and UMTS Authentication and Key Agreement (AKA) for SIP authentication. Some comments were made and discussed, and the report was noted.

TD S3-010504 Requested changes to TS 33.203 v060 concerning security mode set-up. This was provided by Siemens and was discussed, it was agreed that this should be discussed over the e-mail list over the next two weeks, along with any other issues which arise. K. Boman was asked to update

the document taking comments into account after 2 November 2001. Delegates were requested to provide pseudo-CRs to the draft in time for the next SA WG3 meeting in order to finalise the document.

It was agreed that an editors note should be added in section 7.1, stating that the support of different mechanisms is for further study.

TD S3-010509 Integrity Protection: Mechanism for SIP-level solution. This was provided by Nortel Networks, Ericsson and Nokia and was presented by Nortel Networks. It proposed text for inclusion in TS 33.203, section C.2 Integrity mechanisms describing a SIP-level solution for message integrity protection in the 3GPP IMS involving the use of the HTTP Digest security framework.

The proposal was reviewed and discussed. It was agreed that an editors note should be added that further details will be provided on the replay protection mechanism. A description of the security-mode set up headers and message flows was requested for inclusion in the section, and an editors note to include this information later, should be added.

Proposals were invited for an equivalent of Annex D for the SIP-level solution (as Annex E) which should also be discussed in the 2 week e-mail period, and can be included if there are no problems found.

It was agreed to include this contribution in the draft 33.203.

TD S3-010511 The LS was agreed by e-mail and sent to CN WG1 and SA WG2. The working assumption of SA WG3 that authentication is only required for registration and re-registration was endorsed.

SA WG3 also endorsed the need for network initiated re-registrations for security reasons.

Note: This liaison statement, approved by e-mail after the IMS Security ad-hoc meeting, was TD S3z010129.

TD S3-010520 Requested changes to TS 33.203 v060 concerning network initiated authenticated re-registrations. This was presented by Siemens. Ericsson asked for more time to consider this change and it was agreed to return to this at the next meeting, and it was decided to put the proposed changes into an editors note. The updated document was provided in TD S3-010553 and K. Boman was asked to include this in TS 33.203.

TD S3-010415 Liaison Statement on "IMS security and UE functionality split". The response to this was covered in the liaison approved in TD S3-010554

7.4   GERAN security

There were no contributions on this agenda item. Related LSs were discussed under agenda item 5.3.

7.5   Security aspects of UE functionality split

This topic was covered under agenda items 5.3 and 7.3.

7.6   Security aspects of network configuration hiding

There were no contributions under this agenda item.

7.7   Visibility and configurability of security   466

TD S3-010465 Proposed CR to 33.102: Configurability and visibility. This was presented by Telia and proposed a procedure (for Rel-5) to allow user control of accepting or rejecting unciphered calls. The default configuration of the ME is to reject unciphered calls and to prompt the user whether he wishes to start receiving unciphered connections. When the next ciphered connection is made, the ME switches back to the default "reject" mode. It was proposed that this functionality should be mandatory for implementation but optional for use - such that "sensitive" users would be able to switch on the mechanism. It was also suggested that the USIM should have some control over the default configuration, in order to allow operator control. It was proposed that the CR is sent to other groups in order to provide a basis for comments, and listing the issues that have been identified by SA WG3. It was thought that sending a CR with a mechanism which is not agreed by SA WG3 could provide the wrong signal to other WGs. No agreement could be reached on the mechanism and contributions

were requested, particularly from companies who support the visibility and configurability WI in order to find an acceptable mechanism, for contribution to SA WG3 meeting #21.

TD S3-010466 This was not considered as the CR in TD S3-010465 was not accepted.

7.8 MExE security

There were no contributions on this agenda item. Related LSs were discussed under agenda item 5.3.

7.9 OSA security

TD S3-010506 Resubmission of TD S3-010317: Review of OSA Security - some issues for SA WG3 to consider. This was presented by BT. Issues for SA WG3 to consider were listed in the document:

- **Key Management** - Should SA WG3 standardise the key management reusing the mechanisms developed for Network Domain Security (IP) ?
  Not possible for Rel-4, unlikely to be done in time for Rel-5. Earliest likely mechanism would be Rel-6.

- **Challenge Mechanism** - The challenge mechanism used will be in accordance with the IETF PPP Authentication Protocols - Challenge Handshake Authentication Protocol RFC 1994, August1996 [4]. Is this acceptable to SA WG3 or do we want to suggest that we use a challenge response based on 3GPP AKA with sequence numbers, etc. ?
  Not possible for Rel-4, something may be possible for Rel-5, the RFC seemed acceptable to SA WG3.

- **Authentication mechanism requested by the client** - Should SA WG3 provide any guidelines on the choice of operator specific authentication ?
  No specific reason to do this was identified.

- **Algorithm definitions** - Should SA WG3 provide details of other algorithms that could be used?
  DES-56 and RSA-512 are not considered adequately secure. It was noted that the Mode of Operation was missing from the description. **P. Howard agreed to draft a proposal with comments on inconsistencies in the document concerning cryptographic algorithms, for e-mail approval after the meeting**. **1 week after sending of the proposal for comments**. This was provided by e-mail after the meeting in TD S3-010561 which was modified and approved by e-mail in TD S3-010574 (input to meeting #21 for information).

Delegates were asked to review the document and provide comment and contribution to the next meeting.

7.10 FIGS/IST

There were no contributions on this agenda item.

7.11 PKI

TD S3-010499 USIM functionalities to support PKI architectures. This was provided by Gemplus and Oberthur Card Systems and presented by Oberthur Card Systems. It was noted that Nokia had taken an action to create a WI proposal, but had not managed to create it for this meeting. Delegates were asked to consider this after the meeting and Nokia were asked to provide the WI description for the work. The document was then noted.

8 Review and update of work programme

M. Pope to send the Work Programme to SA WG3 for comments via e-mail after the meeting. **All are encouraged to update the SA WG3 Work Items to show accurate information**.

9   Future meeting dates and venues

Meeting	Date	Location	Host
Joint with T WG3, SA WG1 (ISIM issues) **TBC**	26 November 2001	Sophia Antipolis, France	ETSI
S3#21	27 - 30 November 2001	Sophia Antipolis, France	ETSI
S3#22	26 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)

10   Any other business

There was no other business.

11   Close of meeting

The Chairman thanked the host, Qualcomm, for the meeting arrangements and the delegates for their hard work and closed the meeting.

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

Name	Company	e-mail	3GPP	ORG
Mr. Nigel Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	GB	ETSI
Dr. Stephen Billington	Hutchison 3G UK Limited	stephen.billington@hutchison3g.com	GB	ETSI
Mr. Colin Blanchard	BT	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. David Castellanos	ERICSSON L.M.	david.castellanos-zamon@ece.ericsson.se	SE	ETSI
Ms. Lily Chen	Motorola Inc.	lchen1@email.mot.com	US	T1
Mr. Per Christoffersson	TELIA AB	per.e.christoffersson@telia.se	SE	ETSI
Dr. Adrian Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	GB	ETSI
Mr. John B Fenn	SAMSUNG Electronics	johnbfenn@aol.com	GB	ETSI
Mr. Louis Finkelstein	Motorola Inc.	louisf@labs.mot.com	US	T1
Mr. Jean-Bernard FISCHER	OBERTHUR CARD SYSTEMS S.A.	jb.fischer@oberthurcs.com	FR	ETSI
Miss Jessica Gunnarsson	TELIA AB	jessica.l.gunnarsson@telia.se	SE	ETSI
Mr. Philip Hawkes	QUALCOMM EUROPE S.A.R.L.	phawkes@qualcomm.com	FR	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
Miss Dave Kennerley	MOTOROLA Ltd	david.kennerley@motorola.com	GB	ETSI
Mrs. Tiina Koskinen	NOKIA Corporation	tiina.s.koskinen@nokia.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
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. Hugh Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	US	T1
Mr. Al Thomas	Cingular Wireless LLC	al.thomas@cingular.com	US	T1
Mr. Benno Tietz	MANNESMANN Mobilfunk GmbH	benno.tietz@d2vodafone.de	DE	ETSI
Mr. Vesa Torvinen	ERICSSON L.M.	vesa.torvinen@lmf.ericsson.se	SE	ETSI
Mr. Lee Valerius	NORTEL NETWORKS (EUROPE)	valerius@nortelnetworks.com	GB	ETSI
Mr. Berthold Wilhelm	BMWi	berthold.wilhelm@regtp.de	DE	ETSI

A.1   SA WG3 Voting list

Based on the attendees lists for meetings #18, #19 and #20, the following companies are eligible to vote at SA WG3 meeting #21:

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
BT	GB	3GPPMEMBER	ETSI
Cingular Wireless LLC	US	3GPPMEMBER	T1
Deutsche Telekom AG	DE	3GPPMEMBER	ETSI
DTI - Department of Trade and Industry	GB	3GPPMEMBER	ETSI
Telefon AB LM Ericsson	SE	3GPPMEMBER	ETSI
France Telecom	FR	3GPPMEMBER	ETSI
Hutchison 3G UK Limited	GB	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
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
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
S3-010405	Draft agenda for SA WG3 meeting #20	Chairman	2	Approval	
S3-010406	Draft report of SA WG3 meeting #19	Secretary	4.1	Approval	
S3-010407	Draft report of MAP Sec ad-hoc meeting, 13 September 2001	Secretary	4.2	Approval	
S3-010408	Draft report of IMS Sec ad-hoc meeting, 14 September 2001	Secretary	4.3	Approval	
S3-010409	Re: The availability of Motorolas GPRS test capability	Motorola PCS	10	Information	
S3-010410	Reply LS on "Using a generic authentication scheme for SIP"	CN WG1	5.3	Discussion / Action	
S3-010411	Liaison Statement on 3GPP User Profiles	CN WG4	5.3	Information	
S3-010412	LS to SA3 on Signalling for user authentication	CN WG4	5.3	Discussion / Action	
S3-010413	LS on Guidance Needed Concerning Security Mode Reconfiguration	RAN WG2	5.3	Discussion / Action	
S3-010414	Reply to LS on New feature for SAT originated SMS	SA WG1	5.3	Information	
S3-010415	Liaison Statement on "IMS security and UE functionality split"	SA WG1	5.3	Discussion / Action	
S3-010416	IP Based Multimedia Services Framework Report		5.3	Information	
S3-010417	Reply to SA2 LS on Cell ID in SIP messages	SA WG1	5.3	Discussion / Action	
S3-010418	LS on Multimedia Broadcast/Multicast Service (MBMS)	SA WG1	5.3	Information	
S3-010419	LS on "Digital Rights Management"	SA WG1	5.3	Discussion / Action	
S3-010420	LS on Cell ID in SIP messages	SA WG2	5.3	Discussion / Action	
S3-010421	LS in reply to SA2 Liaison "WI on the End-to-End QoS Architecture for Release 5" (S2-011098)	SA WG5	5.3	Information	
S3-010422	Reply to LS on basic and advanced services examples (S1-010271/ S5-010302)	SA WG5	5.3	Information	
S3-010423	Use of the phrase "X interface"	SA WG5	5.3	Information	
S3-010424	MMS digital rights management	T WG2	5.3	Information	
S3-010425	Transmission of user identity from a GGSN to MMS Relay/Server	T WG2	5.3	Information	
S3-010426	Proposed Updates to Structures of SADB and SPD on MAPSec	Huawei Technologies CO., LTD/CWTS	7.1	Discussion / Decision	S3-010528
S3-010427	Update Proposal on Security Domain	Huawei Technologies CO., LTD/CWTS	7.1	Discussion / Decision	S3-010529
S3-010428	LS on stage 1 for Extended Streaming Service	SA WG1	5.3	Discussion	
S3-010429	Update information on 33.210-060	Geir M Køien, rapporteur	7.2	Presentation / Discussion	
S3-010430	33.900 - Guide to 3G Security	C Brookson, Rapporteur	6.2		
S3-010431	Liaison statement on requirements on Multimedia Broadcast/Multicast Service	TSG GERAN	5.3	Information	
S3-010432	LS response to SA3 on "Using a generic authentication scheme for SIP"	CN WG4	5.3	Discussion	
S3-010433	LS from SA WG2: Response to LS S3-010403 on the use of Network Domain Security for protection of SIP signalling messages from SA WG3.	SA WG2	5.3	Discussion	
S3-010434	LS on Security aspects of the 3GPP push service	SA WG2	5.3	Discussion	
S3-010435	LS from SA WG2: Security aspects for IMS related to Authentication	SA WG2	5.3	Discussion	

TD number	Title	Source	Agenda	Document for	Replaced by
S3-010436	LS on Digital Rights Management (DRM) requirements for PSS Rel-5	SA WG4	5.3	Information	
S3-010437	Reply to LS on stage 1 for Extended Streaming Service	SA WG4	5.3	Information	
S3-010438	LS on "Access Point Name" usage	SA WG5	5.3	Information	
S3-010439	Liaison Statement on "Flows related to Authenticated Registrations and Re-Registrations"	CN WG1	5.3	Information	
S3-010440	Reply LS on rejection of 2G AKA by 3G ME with USIM in UTRAN	CN WG1	5.3	Information	
S3-010441	Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem	CN WG1	5.3	Information	
S3-010442	Response to LS "On the use of Network Domain Security for protection of SIP signalling messages" (N1-011041 or S3-010403)	CN WG1	5.3	Discussion / Response	
S3-010443	Response to Liaison Statement on "Progressing the work in SA3 and CN1 on the IP Multimedia core network subsystem"	CN WG1	5.3	Information	
S3-010444	LS from T WG2 to SyncML Requesting DevMan Update	T WG2	5.3	Information	
S3-010445	LS from T WG2: Response to T2-010617 (LS from SA WG2 on Cell ID in SIP messages)	T WG2	5.3	Information	
S3-010446	LS from T WG2 to S3 cc S5, S1, T3 on Security Needs for Terminal Applications	T WG2	5.3	Action	
S3-010447	LS from T WG2: Response to SA5 on Multiple Aspects of Device Management	T WG2	5.3	Information	
S3-010448	Liaison Statement from T WG2 on Extended Streaming Service	T WG2	5.3	Information	
S3-010449	Liaison statement in response to LS S3-010226 regarding revision of MExE security analysis activity WID proposed in S3-010228	T WG2	5.3	Action	
S3-010450	Siemens Comments to MAP-doI v3 <draft-arkko-map-doi-03>	Siemens	7.1	Discussion	
S3-010451	Liaison Statement on IMS identifiers and ISIM or TSIM	T WG3	5.3	Discussion	
S3-010452	Liaison Statement on Usage of Private ID	CN WG1	5.3	Discussion	
S3-010453	LS on the WID: AMR-WB Speech Service - Core Network Aspects	TSG CN	5.3	Discussion	
S3-010454	PKCS#15 support for MExE in the USIM	T WG2	5.3	Discussion	
S3-010455	Proposed CR to 33.102 (R99): Annex F.2 (changing list parameters) modification	Siemens Atea	6.1	Approval	
S3-010456	Proposed CR to 33.102 (Rel-4): Annex F.2 (changing list parameters) modification	Siemens Atea	6.1	Approval	
S3-010457	Proposed CR to 33.102 (R99): SQNMS retrieval in AuC during resynchronisation.	Siemens Atea	6.1	Approval	
S3-010458	Proposed CR to 33.102 (Rel-4): SQNMS retrieval in AuC during resynchronisation.	Siemens Atea	6.1	Approval	
S3-010459	Proposed CR to 33.102 (R99): Sequence Number Management Corrections	Siemens Atea	6.1	Approval	
S3-010460	Proposed CR to 33.102 (Rel-4): Sequence Number Management Corrections	Siemens Atea	6.1	Approval	
S3-010461	3GPP TS 33.203 v 0.6.0: Access security for IP-based services (Rel-5)	Rapporteur	7.3	Discussion / Update	
S3-010462	MAPsec counter mode of operation	Siemens Atea	7.1	Discussion / Decision	
S3-010463	3GPP TR 33.900 V0.4.1: A Guide to 3rd Generation Security	Rapporteur	6.2	Discussion / Update	
S3-010464	NIST Special Publication 800-XX: Recommendation for Block Cipher Modes of Operation		7.1	Information	

TD number	Title	Source	Agenda	Document for	Replaced by
S3-010465	Proposed CR to 33.102: Configurability and visibility	Telia	7.7	Approval	
S3-010466	Proposed LS to T WG2, CN WG1 (cc: T WG3) on proposed CR to TS 33.102 on security visibility and configurability	Telia	7.7	Approval	
S3-010467	Proposed CR to 33.200 v 4.1.0: The Soft Lifetime for the MAPsec SA	Nokia	7.1	Approval	
S3-010468	ISIM/USIM independence	Telia	7.3	Information	
S3-010469	ISIM/USIM independence	Telia	7.3	Decision	
S3-010470	IMS access domain security and NDS	Siemens, Ericsson	7.3	Discussion / Decision	
S3-010471	Proposed CR to 33.200 v4.1.0: Use of 'Original component identifier' during MAPsec processing	Siemens	7.1	Approval	
S3-010472	Proposed CR to 33.200 v4.1.0: Protection Profiles correction	Siemens Atea	7.1	Approval	S3-0105341
S3-010473	Proposed CR to 33.200 v4.1.0: Policy configuration clarification	Siemens Atea	7.1	Approval	S3-0105342
S3-010474	Proposed CR to 33.103 v 3.9.0: Alignments with 25.331	Nokia	6.1	Approval	
S3-010475	Proposed CR to 33.103 v 4.2.0: Alignments with 25.331	Nokia	6.1	Approval	
S3-010476	Security concern with HFN reset procedure	Qualcomm Europe S.A.R.L.	6.1	Discussion / Decision	
S3-010477	Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #3/01 on lawful interception	SA WG3-LI	5.1	Information	
S3-010478	Proposed CR to 33.107: Correct the MO-SMS and MT-SMS events (R99)	SA WG3-LI	5.1	Approval	S3-010514
S3-010479	Proposed CR to 33.107: Correct the MO-SMS and MT-SMS events (Rel-4)	SA WG3-LI	5.1	Approval	S3-010515
S3-010480	Proposed CR to 33.107: Correct the MO-SMS and MT-SMS events (Rel-5)	SA WG3-LI	5.1	Approval	S3-010516
S3-010481	Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-4)	SA WG3-LI	5.1	Approval	
S3-010482	Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-5)	SA WG3-LI	5.1	Approval	
S3-010483	Proposed CR to 33.107: Source of PDP context initiation (Rel-4)	SA WG3-LI	5.1	Approval	S3-010517
S3-010484	Proposed CR to 33.107: Source of PDP context initiation (Rel-)	SA WG3-LI	5.1	Approval	S3-010518
S3-010485	Proposed CR to 33.107: Start of secondary interception of an active PDP context (Rel-4)	SA WG3-LI	5.1	Approval	
S3-010486	Proposed CR to 33.107: Start of secondary interception of an active PDP context (Rel-5)	SA WG3-LI	5.1	Approval	
S3-010487	Proposed CR to 33.107: Alignment of TS 33.107 for Release 5 to previous Releases (Rel-5)	SA WG3-LI	5.1	Approval	S3-010513
S3-010488	Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #4/01 on lawful interception	SA WG3-LI Chairman	5.1	Information	
S3-010489	Proposed changes to 33.210 about defining the BG element	Nokia	7.2	Discussion	
S3-010490	Proposed changes to 33.210 about GGSN – P-CSCF interface (Go)	Nokia	7.2	Discussion	
S3-010491	<draft-garcia-sipping-3gpp-reqs-00.txt>	Ericsson	7.3	Information	
S3-010492	Flexibility of MAP Protection Profiles	Hutchison 3G UK	7.1	Discussion / Decision	
S3-010493	Proposed CR to 33.200: Flexible Protection Profiles for MAP (Rel-4)	Hutchison 3G UK	7.1	Approval	
S3-010494	On access independence and authentication	Ericsson	7.3	Discussion	
S3-010495	On registering several public identities in IM CN SS	Ericsson	7.3	Discussion	

TD number	Title	Source	Agenda	Document for	Replaced by
S3-010496	Proposed changes to 33.210 about protecting GTP-U	Nokia	7.2	Discussion	
S3-010497	EAP Extensions - status report	Ericsson, Nokia	7.3	Information	
S3-010498	Some potential changes for MAPsec	Hutchison 3G UK	7.1	Discussion / Decision	
S3-010499	USIM functionalities to support PKI architectures	Gemplus, Oberthur Card Systems	7.11	Discussion	
S3-010500	Work Item Description: 3GPP Handover Interface for Lawful Interception	SA WG3-LI	5.1	Information	
S3-010501	Draft 33.108 version 0.1.0	SA WG3-LI	5.1	Information	
S3-010502	Proposed response on LS S3z0100109 from SA2 on the usage of public user identifiers and the assignment of S-CSCFs	Siemens	5.3	Discussion / Decision	S3-010550
S3-010503	Proposed response to LS S3z010105 from CN4 on signalling for user authentication	Siemens	5.3	Discussion / Decision	S3-010522
S3-010504	Requested changes to TS 33.203 v060 concerning security mode set-up	Siemens	7.3	Discussion / Decision	
S3-010505	OSA spec 29.198-03 version 4.2.0				
S3-010506	Resubmission of TD S3-010317: Review of OSA Security - some issues for SA3 to consider	BT	7.9	Discussion / Decision	
S3-010507	Resubmission of TD S3-010368: Local Security Association Distribution	Alcatel	7.1	Discussion / Decision	
S3-010508	Reply to comments on MAPSec-DOI		7.1		
S3-010509	Integrity Protection: Mechanism for SIP-level solution	Nortel Networks, Ericsson, Nokia	7.3	Discussion / Decision	
S3-010510	Resubmission of TD S3z010072: Draft of 33.800 with MAPsec Rel5 material	NDS Rapporteur	7.1		
S3-010511	LS sent to CN WG1 from SA WG3 after e-mail approval.	IMS ad-hoc	7.3	Information	
S3-010512	Resubmission of TD S3z010118: Confidentiality of SIP signalling between UE and P-CSCF	Hutchison 3G UK	7.3	Discussion / Decision	S3-010536
S3-010513	Proposed CR to 33.107: Alignment of TS 33.107 for Release 5 to previous Releases (Rel-5)	SA WG3-LI	5.1	Approval	
S3-010514	Proposed CR to 33.107: Correct the MO-SMS and MT-SMS events (R99)	SA WG3-LI	5.1	Approval	
S3-010515	Proposed CR to 33.107: Correct the MO-SMS and MT-SMS events (Rel-4)	SA WG3-LI	5.1	Approval	
S3-010516	Proposed CR to 33.107: Correct the MO-SMS and MT-SMS events (Rel-5)	SA WG3-LI	5.1	Approval	
S3-010517	Proposed CR to 33.107: Source of PDP context initiation (Rel-4)	SA WG3-LI	5.1	Approval	
S3-010518	Proposed CR to 33.107: Source of PDP context initiation (Rel-)	SA WG3-LI	5.1	Approval	
S3-010519	Response to LS from CN1 (N1-011052) on using a generic authentication scheme for SIP	SA WG3	5.3	Approval	
S3-010520	Requested changes to TS 33.203 v060 concerning network intitiated authenticated re-registrations	Siemens	7.3	Discussion / Decision	
S3-010521	Draft report of TSG SA meeting #13: version 0.0.5	Secretary	5.2	Information	
S3-010522	Response to LS S3z010105 from CN4 on signalling for user authentication	Siemens	5.3	Discussion / Decision	S3-010540
S3-010523	Reply LS on the rejection of 2G AKA by 3G ME with USIM in UTRAN	SA WG3	5.3	Approval	
S3-010524	Response to LS from CN1 (N1-011430/S3-010452) Liaison Statement on Usage of Private ID	SA WG3	5.3	Approval	S3-010539

TD number	Title	Source	Agenda	Document for	Replaced by
S3-010525	Response to LS from RAN2 (R2-011763) on Guidance Needed Concerning Security Mode Reconfiguration	SA WG3	5.3	Approval	S3-010555
S3-010526	Response to SA2 LS on Cell ID in SIP messages (S3-010420)	SA WG3	5.6/7.1	Approval	
S3-010527	32.215 version 4.0.0	SA WG5	5.3	Review	
S3-010528	Proposed Updates to Structures of SADB and SPD on MAPSec	Huawei Technologies CO., LTD/CWTS	7.1	Discussion / Decision	
S3-010529	Update Proposal on Security Domain	Huawei Technologies CO., LTD/CWTS	7.2	Discussion / Decision	
S3-010530	Application Level Security Framework for Terminals	Ericsson	5.1	Information	
S3-010531	Reply to S3-010451: LS to T WG3 on USIM/ISIM functional independence issues	G. Rose	5.3	Approval	
S3-010532	Reply to S3-010419 - LS to SA WG1 on DRM issues	P. Howard	5.3		
S3-010533	Extract of e-mail from C Brookson on GSMA and 33.900	Secretary	5.5	Information	
S3-010534	Rev of CR in S3-010459			Approval	
S3-010535	Rev of CR in S3-010460			Approval	
S3-010536	WITHDRAWN - Duplicated				S3-010546
S3-010537	LS to RAN WG2 on HFN Reset and THRESHOLD	SA WG3	6.1	Approval	S3-010556
S3-010538	CR012 to 33.200: MEA encryption algorithm update	SA WG3	7.1	Approval	
S3-010539	Response to LS from CN1 (N1-011430/S3-010452) Liaison Statement on Usage of Private ID	SA WG3	5.3	Approval	
S3-010540	Response to LS from CN4 on signalling for user authentication	SA WG3	5.3	Approval	
S3-010541	CR to 33.200 v4.1.0: Protection Profiles correction	SA WG3	7.1	Approval	
S3-010542	CR to 33.200 v4.1.0: Policy configuration clarification	SA WG3	7.1	Approval	
S3-010543	WITHDRAWN				
S3-010544	Security Association Management in the IMS	Siemens	7.3	Discussion / Decision	
S3-010545	aSIP-Access Security for IP-Based Services	Ericsson		Presentation	
S3-010546	Confidentiality of SIP signalling between UE and P-CSCF	Hutchison 3G UK	7.3		
S3-010547	Response to LS S2-012311, LS N1-011332 on the use of Network Domain Security for protection of SIP signalling messages.	SA WG3	7.3	Approval	S3-010557
S3-010548	Reply to S3-010451: LS to T WG3 on USIM/ISIM functional independence issues	SA WG3	5.3	Approval	
S3-010549	Proposed CR to 33.200 v 4.1.0: The Soft Lifetime for the MAPsec SA (revised after drafting session)	Drafting Group	7.1	Approval	S3-010560
S3-010550	Response to LS S2-012456 from SA2 on Security aspects for IMS related to Authentication	Siemens	5.3	Discussion / Decision	S3-010551
S3-010551	Response to LS S2-012456 from SA2 on Security aspects for IMS related to Authentication	Siemens	6.3	Discussion / Decision	
S3-010552	CR to 21.133: Definition of UICC	Telia	7.3	Approval	S3-010558
S3-010553	Revision of S3-010520				
S3-010554	Reply to S3-010451: LS to T WG3 and SA WG1 on USIM/ISIM functional independence issues	SA WG3	5.3	Approval	

TD number	Title	Source	Agenda	Document for	Replaced by
S3-010555	Response to LS from RAN2 (R2-011763) on Security Mode Reconfiguration	SA WG3	5.3	Approval	
S3-010556	LS to RAN WG2 on HFN Reset and THRESHOLD	SA WG3	6.1	Approval	
S3-010557	Response to LS S2-012311, LS N1-011332 on the use of Network Domain Security for protection of SIP signalling messages.	SA WG3	7.3	Approval	
S3-010558	CR to 21.133: Definition of UICC (R99)	SA WG3	7.3	Approval	
S3-010559	CR to 21.133: Definition of UICC (Rel-4)	SA WG3	7.3	Approval	
S3-010560	Proposed CR to 33.200 v 4.1.0: The Soft Lifetime for the MAPsec SA (revised after drafting session)	SA WG3	7.1	Approval	
S3-010561	LS to CN WG5 : Comments on inconsistencies concerning cryptographic algorithms	SA WG3 (P. Howard)	_	e-mail Approval	S3-010574 (meeting#21 for info)

Annex C: Status of specifications under SA WG3 responsibility

NOTE: The Editors are not all accurate - please provide the secretary with an update with the correct Editors.

	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	7.0.0	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	Vinck, Bart	R99
TS	33.102	4.2.0	3G security; Security architecture	Vinck, Bart	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; Interface between core network and law agency equipment	Wilhelm, Berthold	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	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	Rel-5
TR	33.800	0.3.5	Principles for Network Domain Security	Escott, Adrian	Rel-4
TR	33.800	none	Principles for Network Domain Security	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
21.133	002		R99	Definition of UICC	F	3.1.0	S3-20	S3-010558	agreed
21.133	003		Rel-4	Definition of UICC	A	4.0.0	S3-20	S3-010559	agreed
33.102	156		R99	Annex F.2 (changing list parameters) modification	F	3.9.0	S3-20	S3-010455	agreed
33.102	157		Rel-4	Annex F.2 (changing list parameters) modification	A	4.2.0	S3-20	S3-010456	agreed
33.102	158		R99	Sequence Number Management Corrections	F	3.9.0	S3-20	S3-010534	agreed
33.102	159		Rel-4	Sequence Number Management Corrections	A	4.2.0	S3-20	S3-010535	agreed
33.102	160		R99	SQNMS retrieval in AuC during resynchronisation.	F	3.9.0	S3-20	S3-010457	agreed
33.102	161		Rel-4	SQNMS retrieval in AuC during resynchronisation.	A	3.9.0	S3-20	S3-010458	agreed
33.107	009		Rel-4	Start of secondary interception of an active PDP context	F	4.1.0	S3-20	S3-010485	agreed
33.107	010		Rel-5	Start of secondary interception of an active PDP context	A	5.0.0	S3-20	S3-010486	agreed
33.107	011		Rel-5	Alignment of TS 33.107 for Release 5 Network Architecture	C	5.0.0	S3-20	S3-010513	agreed
33.107	012		R99	Correct the MO-SMS and MT-SMS events	F	3.3.0	S3-20	S3-010514	agreed
33.107	013		Rel-4	Correct the MO-SMS and MT-SMS events	A	4.1.0	S3-20	S3-010515	agreed
33.107	014		Rel-5	Correct the MO-SMS and MT-SMS events	A	5.0.0	S3-20	S3-010516	agreed
33.107	015		Rel-4	Source of PDP context initiation	F	4.1.0	S3-20	S3-010517	agreed
33.107	016		Rel-5	Source of PDP context initiation	A	5.0.0	S3-20	S3-010518	agreed
33.200	012		Rel-4	MEA encryption algorithm update	F	4.1.0	S3-20	S3-010538	agreed
33.200	013		Rel-4	Use of 'Original component identifier' during MAPsec processing	F	4.1.0	S3-20	S3-010471	agreed
33.200	014		Rel-4	Protection Profiles correction	F	4.1.0	S3-20	S3-010541	agreed
33.200	015		Rel-4	Policy configuration clarification	F	4.1.0	S3-20	S3-010542	agreed
33.200	016		Rel-4	The Soft Expiry Time for the MAPsec SA	F	4.1.0	S3-20	S3-010560	agreed

Annex E: List of Liaisons

E.1   Liaisons to the meeting

TD number	Title	Source TD	Comment/Status
S3-010410	Reply LS on "Using a generic authentication scheme for SIP"	N1-011052	Response in TD S3-010519 (approved)
S3-010411	Liaison Statement on 3GPP User Profiles	N4-010917	Noted
S3-010412	LS to SA3 on Signalling for user authentication	N4-010969	Response in TD S3-010540 (approved)
S3-010413	LS on Guidance Needed Concerning Security Mode Reconfiguration	R2-011763	Response in TD S3-010525 (approved)
S3-010414	Reply to LS on New feature for SAT originated SMS	S1-010773	Noted
S3-010415	Liaison Statement on "IMS security and UE functionality split"	S1-010863	Covered after consideration of related contributions (TD S3-010548)
S3-010416	IP Based Multimedia Services Framework Report	S1-010869	Forwarded to LI group for consideration of LI parts. Relevant sections should also be reviewed by SA WG3 delegates
S3-010417	Reply to SA2 LS on Cell ID in SIP messages	S1-010872	Noted. Requires further study in SA WG3
S3-010418	LS on Multimedia Broadcast/Multicast Service (MBMS)	S1-010876	Noted
S3-010419	LS on "Digital Rights Management"	S1-010877	Response in TD S3-010532 (approved)
S3-010420	LS on Cell ID in SIP messages	S2-011697	Noted. See also TD S3-010417.
S3-010421	LS in reply to SA2 Liaison "WI on the End-to-End QoS Architecture for Release 5" (S2-011098)	S5-010412	Noted
S3-010422	Reply to LS on basic and advanced services examples (S1-010271/ S5-010302)	S5-010413	Noted
S3-010423	Use of the phrase "X interface"	S5-010416	Noted
S3-010424	MMS digital rights management	T2-010634	Noted
S3-010425	Transmission of user identity from a GGSN to MMS Relay/Server	T2-010606	Noted
S3-010428	LS on stage 1 for Extended Streaming Service	S1-010837	Noted. Should be reviewed by SA WG3 delegates and comments input to SA WG1 via SA WG1 colleagues.
S3-010431	Liaison statement on requirements on Multimedia Broadcast/Multicast Service	GP-011913	Noted
S3-010432	LS response to SA3 on "Using a generic authentication scheme for SIP"	N4-010968	Noted
S3-010433	LS from SA WG2: Response to LS S3-010403 on the use of Network Domain Security for protection of SIP signalling messages from SA WG3.	S2-012311	Discussed and noted.
S3-010434	LS on Security aspects of the 3GPP push service	S2-012423	Noted. Delegates to provide contribution to the next meeting concerning Push architectures using document embedded in this LS as a basis

TD number	Title	Source TD	Comment/Status
S3-010435	LS from SA WG2: Security aspects for IMS related to Authentication	S2-012456	Response in TD S3-010551 (approved)
S3-010436	LS on Digital Rights Management (DRM) requirements for PSS Rel-5	S4-010534	Noted
S3-010437	Reply to LS on stage 1 for Extended Streaming Service	S4-010535	Noted
S3-010438	LS on "Access Point Name" usage	S5-010555	Noted. Delegates to review TS 32.215 and provide comments to the next meeting
S3-010439	Liaison Statement on "Flows related to Authenticated Registrations and Re-Registrations"	N1-011250	Noted
S3-010440	Reply LS on rejection of 2G AKA by 3G ME with USIM in UTRAN	N1-011264	Response in TD S3-010523 (approved)
S3-010441	Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem	N1-011313	Noted
S3-010442	Response to LS "On the use of Network Domain Security for protection of SIP signalling messages" (N1-011041 or S3-010403)	N1-011332	Discussed and noted.
S3-010443	Response to Liaison Statement on "Progressing the work in SA3 and CN1 on the IP Multimedia core network subsystem"	N1-011344	Noted
S3-010444	LS from T WG2 to SyncML Requesting DevMan Update	T2-010722	Noted
S3-010445	LS from T WG2: Response to T2-010617 (LS from SA WG2 on Cell ID in SIP messages)	T2-010823	Noted
S3-010446	LS from T WG2 to S3 cc S5, S1, T3 on Security Needs for Terminal Applications	T2-010831	Noted. Further study needed on SyncML: Any delegate with material for discussion should also send it to the SA WG3 e-mail list
S3-010447	LS from T WG2: Response to SA5 on Multiple Aspects of Device Management	T2-010856	Noted
S3-010448	Liaison Statement from T WG2 on Extended Streaming Service	T2-010859	Noted
S3-010449	Liaison statement in response to LS S3-010226 regarding revision of MExE security analysis activity WID proposed in S3-010228	T2-010690	Noted. See also TD S3-010530
S3-010451	Liaison Statement on IMS identifiers and ISIM or TSIM	T3-010613	Response in TD S3-010554 (approved)
S3-010452	Liaison Statement on Usage of Private ID	N1-011430	Response in TD S3-010539 (approved)
S3-010453	LS on the WID: AMR-WB Speech Service - Core Network Aspects	NP-010540	Forwarded to LI group.
S3-010454	PKCS#15 support for MExE in the USIM	T2-010692	Noted

E.2 Liaisons from the meeting

TD number	Title	Comment/Status	TO	CC
S3-010416	IP Based Multimedia Services Framework Report	Forwarded to LI group for consideration of LI text. 16/10/2001	**LI**	
S3-010453	LS on the WID: AMR-WB Speech Service - Core Network Aspects	Forwarded to LI group 16/10/2001	**LI**	
S3-010519	Response to LS from CN1 (N1-011052) on using a generic authentication scheme for SIP	Approved. Sent to CN1 17/10/2001	**CN1**	
S3-010523	Reply LS on the rejection of 2G AKA by 3G ME with USIM in UTRAN	Approved. Sent to CN1 17/10/2001	**CN1**	**SA1, T2, T3, GSMA-SG**
S3-010526	Response to SA2 LS on Cell ID in SIP messages	Approved.	**SA1, SA2**	**CN1, CN4, T2, R2, GERAN2**
S3-010532	Initial comments on digital rights management	Approved. TD419, 424, 436 and SP-010577 attached	**SA1, SA4, T2**	**SA2**
S3-010539	Response to LS from CN1 (N1-011430/S3-010452) Liaison Statement on Usage of Private ID	Approved. Sent to CN1 17/10/2001	**CN1**	**CN4, SA1, SA2, SA5**
S3-010540	Response to LS from CN4 on signalling for user authentication	Approved. Sent to CN1 17/10/2001	**CN4**	**SA2, CN1**
S3-010554	Reply to T3-010613 and S1-010863: LS to T WG3 and SA WG1 on USIM/ISIM functional independence issues	Approved.	**T3, S1**	**EP SCP, T2, SA2**
S3-010551	Response to LS S2-012456 from SA2 on Security aspects for IMS related to Authentication	Approved.	**SA2**	**CN1, CN4**
S3-010555	Response to LS from RAN2 (R2-011763) on Security Mode Reconfiguration	Approved.	**RAN2**	
S3-010556	LS to RAN WG2 on HFN Reset and THRESHOLD	Approved. TD474, 476 attached	**RAN2**	
S3-010557	Response to LS S2-012311, LS N1-011332 on the use of Network Domain Security for protection of SIP signalling messages.	Approved.	**SA2, CN1**	**CN4**