3GPP TSG SA WG3 Security — S3#19 **S3-010301**

3 - 6 July, 2001

Newbury, UK

3GPP TSG SA WG3 Security — S3#18

21-24 May, 2001

Phoenix, USA

Source: **Secretary, SA WG3 (Maurice Pope, MCC)**

Title: **Draft Report of Meeting #18**

Version: **0.0.3**

The hiking pioneers at 100°F: South Mountain

1 Opening of the meeting

The Chairman, Prof. Michael Walker welcomed delegates to the 18th meeting of SA WG3. Mr. Dan Brown, Motorola Inc., welcomed delegates to Phoenix, and provided the domestic arrangements and wished SA WG3 a successful meeting.

2 Meeting objectives and approval of the agenda

The Chairman provided the objectives for the meeting:

- Election of SA WG3 Chairman and 2 Vice Chairmen (Tuesday a.m.)
- Completion of Rel-4 NDS documents for presentation to TSG SA for approval in June 2001 (and for information by e-mail after this meeting)
- Completion of the GERAN Integrity Protection for approval in the June 2001 TSG meeting
- UE Split to be completed
- Network Security to be progressed
- IMS Security to be progressed, as it needs to be provided to TSG SA in June 2001 for information - the ad-hoc IMS meeting had discussed the positioning of the authentication checking and SA WG2 were asked for advice from an architecture viewpoint. Ericsson had since withdrawn their proposals
- Changes for Release 1999 in order to align and corrections to UTRAN - SIM access specifications

The agenda, provided in TD S3-010140, was updated to include some extra items: 8.2, 8.3 and 9.9 was updated to the title "UE Split". The agenda was then approved.

3 Assignment of input documents

The available documents were assigned to their appropriate agenda items.

4 Approval of reports from 3GPP SA3 meetings

4.1 S3#17, 27 February – 1 March, Gothenburg

TD S3-010141 Draft report of meeting #17 version 0.0.4: This was modified editorially and approved. The updated version 1.0.0 will made available on the ftp server.

4.2 S3#17bis, 23-27 April, Madrid

TD S3-010143 Draft report of NDS ad-hoc, April 23-24 April 2001: This report was approved. The approved version will made available on the ftp server.

TD S3-010144 Draft report of aSIP ad-hoc, April 25 2001: This report was approved. The approved version will made available on the ftp server.

TD S3-010145 Draft report of SA WG3/SAWG1 IMS joint session, April 26 2001: This report was approved with minor changes. The approved version will made available on the ftp server.

TD S3-010146 Draft report of SA WG3/GERAN joint meeting, April 27 2001: This report was approved with minor changes. The approved version will made available on the ftp server.

4.3 Joint S3/T3 meeting, 3 May, Munich

TD S3-010224 Report of the TSG-T3 Ad Hoc Meeting #37 (Joint with TSG-S3): This report was presented by N. Barnes, Motorola, and the conclusions were taken into account in the discussion of other relevant topics during the meeting. The report was then noted.

5 Reports and liaisons from other groups

5.1 3GPP SA3 lawful interception sub-group

TD S3-010229 Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #2/01 on lawful interception. The SA WG3 – LI Chairman presented the report of the Clearwater meeting, the agreed output of which were summarised in Annex C of the report. The report was noted and Bernie McKibben, having earlier announced his resignation, was thanked by SA WG3 for all his hard work in the LI group, and wished him success in his future work.

5.2 3GPP SA plenary

TD S3-010213 Report to SA3 on SA#11. This was presented by the SA WG3 Chairman, and had been distributed by e-mail before the meeting. The main points were the importance of distribution of Security algorithm documents very quickly after approval in order to reduce criticism of the algorithms, as the evaluation reports usually provide answers to the alleged "threats" that may be reported. The Liaison of SA WG3 to other groups was also criticised in the SA Plenary, with no specific examples of problems, but it was noted that the LS procedure needed to be improved. Mr. Pope agreed to try to improve the MCC side of the liaison process, as some LSs that SA WG3 had approved in previous meetings had taken a long time to be delivered to the relevant groups. The report was then noted.

5.3 3GPP WGs

5.3.1 SA

TD S3-010159 LS from SA WG1 regarding User Profile: The contribution on User Profiles from Ericsson, which was presented at the SA WG1 ad-hoc meeting was provided in TD S3-010172, and was noted. TD S3-010159 was considered and discussed, but SA WG3 did not identify any specific security contribution that could be made to the user profile description. The liaison was noted, and a response to SA WG1 and SA WG4 was included in TD S3-010225, replaced by TD S3-010281 "Reply LS on streaming and user profile" which was again updated in TD S3-010293 and approved.

TD S3-010160 Reply LS from SA WG2 for "IM User Identities": The LS was considered, but there was some confusion over the meaning of the LS, and delegates were asked to consider it overnight and contact their SA WG2 collegues. This was returned to under agenda item 9.3.

TD S3-010161 Proposed Liaison to S3 on use of Diameter. SA WG2 had considered the adoption of the IETF AAA architecture as the architecture to be used for Authentication and Authorization in the IP Multimedia CN subsystem, and asked SA WG3 for their reaction. This had been handled at the April 2001 ad-hoc meeting, ~~and~~ which concluded that SA WG3 did not favour this approach. The LS was then noted.

TD S3-010168 LS from SA WG5 in reply to T WG2 LS on MExE and User Equipment Management (T2-000756): This was copied to SA WG3 for information, and noted. The MExE Rapporteur was asked to provide a LS back to SA WG5, informing them that SA WG3 will consider this as part of the MExE Security work. This was provided in TD S3-010226 and an updated WI description was provided in TD S3-010227. This was modified in TD S3-010288 to add SA WG5 as a secondary responsible group which was approved. The WI description sheet was attached for information to TD S3-010226.

TD S3-010142 Response to LS (S1-010144) from T3 chairman on the Elaboration of KEY IDENTIFICATION EVENT: This LS was noted as the LS from T WG3 in TD S3-010166 " Response to LS (S3-010128) on the Elaboration of KEY IDENTIFICATION EVENT (T3-010323)" reported no security work was required at this stage.

TD S3-010156 LS from SA WG1 on basic and advanced services examples (S1-010271): This LS was noted. SA WG3 will inform SA WG1 if any security definition is needed for these services when they have been agreed and further elaborated by SA WG1.

TD S3-010157 LS from SA WG1 on Extended Streaming Service (S1-010501): This was provided to SA WG3 for information, and a response from SA WG4 had been provided in TD S3-010174. A response LS was drafted by P. Howard in TD S3-010293 to inform SA WG1 that SA WG3 have a WI on end-to-end encryption, and asking whether SA WG3 should also produce a WI on Digital Rights Management to support this work (see above).

TD S3-010267 Response LS to S1 LS Regarding User Profiles. A joint meeting was suggested, an invitation provided in TD S3-010278. A LS to SA WG1 had been produced, informing SA WG1 that there were no security impacts identified, included in TD S3-010225, which was updated to include this in TD S3-010281 (later updated further in TD S3-010293).

5.3.2 CN

TD S3-010151 LS from CN WG1 on Re-transmission of authentication requests: This included a CR to 24.008. SA WG3 had submitted and had approved CR134 on this at SA#11. A response to inform CN WG1 of this was drafted in TD S3-010230 which was approved.

TD S3-010152 LS from SA WG2 / CN WG1 Joint SIP Adhoc on "Security for IM SIP session Signalling": This requests SA WG3 to send representatives to CN WG1 to present the SIP signalling status and to discuss the identified issues. CN WG1 also offered to provide input to SA WG3, which was welcomed by SA WG3. Gü~~u~~nther Horn agreed to draft a reply LS to deal with the questions to be elaborated at the meeting, in TD S3-010231, which was updated in TD S3-010291 and approved.

TD S3-010234 Liaison Statement from CN WG1 on THRESHOLD check at RRC connection establishment: A corresponding LS from RAN WG2 in TD S3-010153 is covered under agenda item 5.3.4. A reply was sent in TD S3-010273 (see agenda item 9.1).

5.3.3 T

TD S3-010162 Reply LS from T WG3 to T WG1 on authentication test algorithm to be implemented in test USIMs. This was copied to SA WG3 for information and was noted.

TD S3-010163 LS from T WG3 on Rejection of 2G Authentication and Key Agreement by 3G ME with USIM in UTRAN: SA WG3 considered this liaison and agreed that this should be made a clear requirement. The situation would only arise due to incorrect implementation of the standards. It is a requirement that issuers of 3G USIMs support 3G authentication in their Authentication Centres. A reply LS was drafted to T WG3, TSG T and TSG SA on this in TD S3-010232, which was approved (copied to the GSMA-SG for information).

TD S3-010164 LS from T WG3 for "IM Subsystem Address Storage on USIM": This was a response to SA WG2, and was provided to SA WG3 for information, and was noted.

TD S3-010166 Response from T WG3 to LS (S3-010128) on the Elaboration of KEY IDENTIFICATION EVENT: No activity was considered necessary by T WG3 at the moment in SA WG3, and they will inform SA WG3 when action is needed.The LS was therefore noted.

TD S3-010167 LS from T WG3 to T WG1 on authentication test algorithm to be implemented in test USIM. SA WG3 noted that using f1 = f1* was acceptable for a test USIM to test MEs. It was also agreed that these test USIMs could not be used for testing towards the AuC, as a real USIM would be needed for this. The LS was then noted (see also TD S3-010193).

TD S3-010193 Response from T WG1 to T WG3 LS on authentication test algorithm in test USIM: This was covered in the discussion of TD S3-010167. A response LS was produced to inform T WG1 and T WG3 that the proposals were acceptable in order to prevent delay of the work, if the test USIMs are used only for testing of MEs, and to inform them that this would not test that f1 and f1* are different for real USIMs in TD S3-010233, which was approved.

TD S3-010194 LS from T WG3 on New feature for SAT originated SMS. This was copied to SA WG3 for information, and was noted. SA WG3 will consdier this further after SA WG1 provide firm service requirements for such a feature.

TD S3-010253 T WG2 Reply to T WG3 LS on New feature for SAT originated SMS. This LS was a response to the T WG3 LS in TD S3-010194 (see above) and was copied to SA WG3 for information and was noted.

5.3.4 RAN

TD S3-010153 LS from RAN WG2 on THRESHOLD check at RRC connection establishment. This was presented by Ericsson, and a corresponding CR was provided in TD S3-010196 (see agenda item 9.1). A corresponding LS from CN WG1 was provided in TD S3-010234. A draft reply LS was provided in TD S3-010237. This LS was updated to remove "Draft" in S3-010273 and approved. This was sent immediately to the RAN WG2 Chairman with the approved CRs in TD S3-010271 and TD S3-010272 attached (see agenda item 9.1), in the hope that they would be able to receive it during their meeting the same week.

TD S3-010154 LS from RAN WG2 on Wrap around of the calculated START value: This was presented by Ericsson, and Ericsson proposed to keep the START at its maximum value (option 1), rather than wrapping it around (option 2), in order to better limit the possibility of ~~repeqting~~ repeating of the Key string. After some discussion, and consideration of corresponding CRs in TD S3-010195 (see agenda item 9.1), Option 1 was chosen as the best method. A LS to RAN WG2 was provided in TD S3-010235, which was updated in TD S3-010268 and approved. This was sent immediately to the RAN WG2 Chairman with the approved CRs in TD S3-010269 and TD S3-010270 attached (see agenda item 9.1), in the hope that they would be able to receive it during their meeting the same week.

TD S3-010155 Response from RAN WG3 to SA WG2 and TSG GERAN to LSs related to optimised IP speech and header removal support in GERAN: This was copied to SA WG3 for information and was noted.

TD S3-010173 LS from RAN WG3 to SA WG3 on security in IP-transport based UTRAN: RAN WG3 asked SA WG3 to check the security issues for their IP transport in UTRAN Work Task, and to provide any comments. This document was noted.

5.3.5 GERAN

TD S3-010150 LS from GERAN ad-hoc #5: Revised working assumptions made at the joint TSG GERAN / SA WG3. This output from the joint GERAN/SA WG3 ad-hoc meeting had been sent to SA WG3 for further agreement. It was noted that SA WG3 would need to add a reference to GERAN TS 43.051 in TS 33.102. This CR was created in TD S3-010236, which was approved. SA WG3 did not consider the allowance of an 8-bit MAC as reasonable from a security point of view, as it would provide a false sense of security, and it would be preferable not to protect the message, than to let operators wrongly think that the messages were adequately secured. This was further discussed under agenda item 9.4.

5.4 ETSI SAGE

TD S3-010259 LS from GSMA on Development of new A5/3. This was presented by Charles Brookson, and provided information on the status in the development of A5/3. A reply was provided in TD S3-010260, which informed SAGE that SA WG3 endorsed the work plan provided in TD S3-010261. TD S3-010261 was considered and it was noted that it did not include the design of GEA3, and the reply LS was updated in TD S3-010282 to include a request for a similar work plan for GEA3. **<CHECK IF APPROVED>**

A5/3:

Mr. C. Brookson provided a verbal report on the status of A5/3: He reported that the ETSI and GSMA lawyers still had not reached agreement on the distribution and ownership of the algorithm, which is expected to be similar to the handling of the KASUMI algorithm. When agreement has been made, the 3GPP Partners will be consulted and then ETSI SAGE will be able to start the design work.

It was clarified that the algorithm will be available from 3GPP SDOs and the GSMA, so that membership of the GSMA will not be required in order to obtain the A5/3 licence, i.e. membership of one of the SDOs or GSMA will not be a pre-requisite~~necessary~~. The algorithm was expected to be ready for the end of 2001.

It was reported that the work should not take much time for ETSI SAGE, as it mainly consists of extracting only 64 bits from the output of the KASUMI kernel. Some time for public scrutiny had been included in the end of 2001 estimation for completion.

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

GSMA:

Mr. C. Brookson provided a verbal report on the activities of the GSM Association, Security work. The group meet four times a year. Operators are welcomed to join the group.

IMEI:

It was reported that the Terminal Strategies Working Group had agreed that IMEIs are to be included in terminals and that the ITU-T have shown interest in this. The IMEI may therefore become globally mandatory, i.e. all handset manufacturers will be required to include an IMEI in their equipment, in order to gain type approval.

A5/1 key length:

It was reported that tests had been done and that a 64-bit Key will work for A5/1. Many changes to the GSM specifications would be needed, however, for the use of 128-bit Key for GSM, and this was not considered practical.

Security accreditation scheme:

Audits had been performed on some SMART card manufacturers, which had produced some improvements. AuC manufacturers and GRX Network Providers were also scheduled for auditing. The scheme encourages equipment manufacturers to improve their output.

GPRS Risks and Guidelines group:

The group hold 4 meeting per year and will provide guidelines to operators on the risks and avoidance of them. Operators are welcomed to join the group.

6 Joint meeting with TIA TR-45 AHAG

6.1 Joint AKA control procedure

TD S3-010206 TR-45 / 3GPP Joint AKA Control. This was presented by TR-45 AHAG and had been approved by TR-45 in March 2001. The agreement was discussed and approved by SA WG3. The SA WG3 Chairman agreed to forward this agreement to TSG SA informing them of the status, for endorsement.

6.2 Positive authentication reporting

TD S3-010255 3GPP S3 Request for Clarification on Positive Authentication Reporting. This contribution, presented by AHAG was in response to TD S3-010131 (SA WG3 meeting #17), and confirmed that Positive Authentication Reporting is a 3GPP2 requirement for all successful Authentication and Key Agreement (AKA) procedures associated with a location update (i.e. registration). The reporting needs to include User ID, and the RAND used for the AKA procedure. It was clarified that the inclusion of an Information Element in the Location Update Information Element to include RAND would be enough to satisfy the AHAG request. SA WG3 needed to check whether the RAND would always be available for transmission. SA WG3 reported that this would be progressed when the Rel-5 work had been progressed, due to priority in SA WG3 on this work. The contribution was then noted.

6.3 Other issues

TD S3-010256 UIM Authentication Method. This~~i~~ contribution reported that TR-45 has recognized that the use of AKA in conjunction with Removable UIM (R-UIM) creates vulnerability in a form of “rogue shell” attack. The contribution proposes a possible solution and concludes that this proposal would provide adequate protection from the attack, and can be economically implemented on a R-UIM.

The contribution was considered, and it was reported that this would not be necessary for interworking between 3GPP and 3GPP2, but that if 3GPP wished to implement such a solution, it would be more efficient to implement it early, rather than later, for future interoperability. The contribution was then noted and would be considered in future SA WG3 work.

There were no other contributions for the joint session and the meeting was closed.

7 Work programme management

7.1 New work items

TD S3-010212 aSIP-Access Security for IP-Based Services - Activities and a new timeplan: These slides were presented by Ericsson and was accompanied by an updated WI description for Access security for IP-based services. The updated WI clarified that the Stage 3 is not the same as the Stage 2 document (i.e. 33.203). The timescales were reviewed and updated in TD S3-010239 which delayed the work to March 2002: This was further updated to more realistic date in TD S3-010283 and approved.

TD S3-010246 - update to WID FIGS - updates the time schedule. Ericsson reported that they did not support this WI, BT considered that there would be difficulty progressing the IMSS FIGS work, due to lack of contribution, e.g. to Immediate Service Termination (IST). The WID was **not approved**, and companies interested in the work were asked to discuss th~~y~~e future of this work off-line.

TD S3-010264 WID on Network Hiding: SA WG2 asked SA WG2 to provide recommendations and CRs on the security requirements of the new WI for SA WG2. The timescales were not included but it was reported that the work in SA WG2 was expected to be rapid (2-3 meetings) - completion date July 2001 for SA WG3 in order to forward any CRs to SA WG2 in August 2001. Updated in TD S3-010284 and approved.

TD S3-010275 Update to Network Domain Security WIs - NDS-MAP. The automated key distribution was due for completion in December 2001, which was considered an aggressive timescale. The support by T-Mobil also needed to be verified and Mr. Koien agreed to continue the rapporteurship until S3#19 meeting. The completion date was thought unrealistic and was extended to March 2002 ~~completion~~. The WID was updated and provided in TD S3-010285 which was approved. Contributions were needed in July 2001 in order to prepare the CRs to produce Rel-5.

TD S3-010276 Update to Network Domain Security WIs - IP. This was updated in TD S3-010286 and approved.

TD S3-010222 End-to-end security WI: See agenda item 9.5.

8 Release 99 and earlier

8.1 3G security architecture (TS 33.102) (2G/3G interoperation etc.)

TD S3-010179 Proposed R99 CR to 33.102: Correction to periodic local authentication: Siemens reported that TD S3-000726 had not been fully implemented in the R99 version of 33.102, but that changes approved by RAN#11 had required another update to the text to align it. This CR therefore aligned the text and covered the changes in the mis-implemented CR to 33.102. M. Pope agreed that the CR database would need to track the mistake in implementation, along with the new CR which corrected this and aligned with the RAN specifications. The CR was then approved as **Category F**.

TD S3-010180 Proposed Rel-4 CR to 33.102: Correction to periodic local authentication: This was the Rel-4 equivalent of the R99 CR in TD S3-010179 and was approved as **Category A**.

TD S3-010181 Proposed R99 CR to 33.102: Correction to COUNT-C description: Siemens introduced the CR which aligned the Stage 2 with the Stage 3. The CR was approved as **Category F**.

TD S3-010182 Proposed Rel-4 CR to 33.102: Correction to COUNT-C description: This was the Rel-4 equivalent of the R99 CR in TD S3-010181 and was approved as **Category A**.

TD S3-010183 Proposed R99 CR to 33.102: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted: Nokia introduced this CR, some modifications were made to remove the changes to section F.3 and the updated CR was provided in TD S3-010240, which was approved as **Category F**.

TD S3-010184 Proposed R99 CR to 33.102: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted: This was the Rel-4 equivalent of the R99 CR in TD S3-010183 and was modi~~o~~fied to remove the changes to section F.3 and updated in TD S3-010241 which was approved as **Category A**.

TD S3-010195 Proposed R99 and Rel-4 CRs to 33.102: Calculation and Wrap-around of START value: These CRs were introduced by Ericsson. There was a lot of discussion on the meaning of the text, and it was decided to have an off-line discussion on this to clarify the CR. See discussion of TD S3-010154, under agenda item 5.3.4). These CRs were updated in TD S3-010269 and TD S3-010270 which were approved. A corresponding LS to RAN WG2 was produced in TD S3-010268, which was approved, informing them of the decision of SA WG3, with the CRs attached (see agenda item 5.3.4).

S3-010196 Proposed R99 and Rel-4 CRs to 33.102 on THRESHOLD Check at RRC connection establishment. These CRs were presented by Ericsson. See discussion of TD S3-010153, under agenda item 5.3.4. The classification of the R99 CR was agreed as Category F, and the Rel-4 CR as Category A. The CRs were updated accordingly in TD S3-010238 and then separately in TD S3-010271 and TD S3-010272 which were approved. The CRs were attached to related LS in TD S3-010273 which was approved (see agenda item 5.3.4).

8.2 33.103 changes (Integration doc)

TD S3-010185 Proposed R99 CR to 33.103: The multiplicity of Data integrity symbols: This CR was introduced by Nokia and improved the consistency of the document. It was decided that COUNT-I_{UP} and COUNT-I_{DOWN} needed to be further checked. The CR was later checked as OK and was approved as **Category F**.

TD S3-010186 Proposed Rel-4 CR to 33.103: The multiplicity of Data integrity symbols: This was the Rel-4 equivalent of the R99 CR in TD S3-010185 and was approved as **Category A**.

8.3 33.105 Changes (Algorithms doc)

TD S3-010187 Proposed R99 CR to 33.105: Deletion of the maximum size of a RRC message: This CR was introduced by Nokia, and corrected some inconsistencies in the specification. The CR was presented as Category B, but was approved as **Category F**.

TD S3-010188 Proposed Rel-4 CR to 33.105: Deletion of the maximum size of a RRC message: This was the Rel-4 equivalent of the R99 CR in TD S3-010187 and was approved as **Category A**.

9 Work items

TD S3-010147 Status report for NDS: An additional SA WG3 plenary meeting was suggested to develop the IP Part of NDS for early delivery, between SA WG3 meeting #19 and TSG SA Meeting #13.

It was reported that the NDS ad-hoc meeting had agreed to propose a split of TS 33.200 into two documents, one dealing with NDS-MAP, and a second with NDS-IP. SA WG3 agreed to try to finalise the MAP part for approval in TSG SA#12 as Rel-4, and the IP part for Rel-5 (to be sent for information early to TSG SA). A new TS number was requested for the IP part, which was later confirmed as TS 33.210. A Rapporteur was required for TS 33.210, and delegates were asked to consider taking this responsibility during the meeting. Mr. Geir Koien agreed that he was willing to take this if nobody else volunteered. The report was then noted.

9.1 MAP security (draft TS 33.200)

TD S3-010149 Update information - TS 33.200 and TS 33.200 version 0.5.0: The update information was noted and the draft TS was considered section by section, moving on to any contributions related to each section:

> TD S3-010228 LS from CN WG4 on MAP security: CN WG4 asked SA WG3 to change the granularity of the protection profile assumption, reached at the NDS ad-hoc meeting, to the component level. CN WG4 also prepared CRs to remove the MAP Security work from their Rel-4 specifications, which they intended to present to TSG CN #12 if the issues are not resolved by SA WG3 and the NDS-MAP document not finalised in time for TSG SA #12 approval.
>
> There was a comment that the Rel-5 material in Annexes A and B should be removed and included in a TR, as it could be mis-interpreted as being a part of Rel-4 implementation. It was agreed to move Annex A to TR 33.800 which will be continued for the time being, in order to hold information moved out of the Rel-4 specification. In order to facilitate stabilisation of 33.200 for Rel-4, it was agreed that TR 33.800 will not be progressed and will be moved to Rel-5.
>
> There was discussion on the removal of Annex B, for Manual Key Management, as no agreement could be reached on the completeness of this ~~part~~Annex. It was agreed that at least some guidance was required on Manual Key Management. Contributions on Annex B were therefore requested to be provided during the meeting in order that the specification can be completed with a basic Manual Key Management system included.

For the remaining contributions on this subject, the contributions of major issues were concentrated upon.

TD S3-010189 Comments on TS 33.200 v050. This was presented by Siemens and proposes to:

> Remove all Rel5 material from the normative sections. This was agreed.
>
> Clean section 5.3 from the MAPsec DoI parts and rename it. This was agreed.
>
> Review and clean-up the Annexes, Annex B was recognised as an open issue. It was agreed to move Annexes A and C to TR 33.800.
>
> Review the MAP SA definition of annex A.3.4 and complete MAP SA definition in section 5.3.2. Contributions were requested for this at the meeting.
>
> Provide a definition for both the integrity algorithm and the encryption algorithm. Contributions were requested for this at the meeting.
>
> Evaluate MAP protection Profiles and Protection Groups. This was done by consideration of the CN WG4 recommendations in TD S3-010192.
>
> Clarify definitions: e.g. Local key distribution, UMTS network Domain, manual Interdomain SA. This was done in the editing sessions.
>
> Clarify whether the interfaces table 2 is normative or informative. This was done in the editing sessions.
>
> Include fallback to Unprotected Mode Indicator, and MAP SA handling. Contributions were requested for this at the meeting.

TD S3-010218 33.200 (MAP) v0.5.0. Comments provided by Alcatel: These comments were covered by other contributions and the proposals used in the editing sessions.

TD S3-010214 Proposed changes to 33.200v0.5.0: This was provided by Vodafone. It proposed that MAP DoI should be removed and included in a self-contained document. For the MAPsec encryption algorithm, the choice of Block or Stream cipher mode was an open issue. It was agreed that stream cipher should be chosen as it is available now, and the block cipher could be added later, when available and if required, as an option.

TD S3-010197 Use of Combined TVP/IV parameter. This was presented by Ericsson and provided the structure for IV as agreed at the NDS ad-hoc meeting. This was used in conjunction with TD S3-010190.

TD S3-010190 Structure of Initialisation Vector in MAPsec: This was presented by Siemens. It was agreed that the NE-Id numbering should be standardised, in order to ensure uniqueness of IVs, this should be considered by delegates for further contribution. The IV padding rule also requires standardisation and consideration. The possibility to reduce the length of the TVP transmitted by utilisation of the node synchronisation should also be considered. The length of the TVP had been defined as 4 bytes, but other lengths should be considered for definition.

The proposal of TD S3-010197, modified by those in TD S3-010190 were discussed and the significant points taken as a basis for the editing sessions.

TD S3-010192 Protection Profiles for MAP Security: This was presented by Siemens and assumed that single operators will have a single PLMN ID for both their GSM networks and UMTS Networks. In this ID could be used as a Network Domain ID. This was agreed as the assumption that SA WG3 would work on.

It was clarified that MAPsec applies only to MAP version 3, and not to MAPv2 or MAPv1, and therefore the Security context needs to be defined for MAPv3. The proposal of the contribution was agreed as an acceptable basis for the Protection Profiles part of 33.200, and it was noted that the Protection Profiles need to be completed.

The rapporteur for TS 33.200 agreed to take into account the following contributions in an editing session with the help of concerned parties: TD S3-010197, TD S3-010190, TD S3-010192, TD S3-010214, TD S3-010216.

Several editing sessions were held to progress the document for network aspects and algorithm aspects (to study which ISO algorithms to refer to) in parallel in order to progress faster. Interim versions of the specification were provided in TD S3-010149, TD S3-010257, TD S3-010258 and TD S3-010277. The results of both sets of sessions presented to the full SA WG3 group in TD S3-010294 and TD S3-010295 and presented to the full SA WG3 group for approval. It was noted that message flows were intended to be added and other editors notes may remain for improvement later. The document was then approved by SA WG3.

M. Pope will receive the final version from G. Koein and produce version 1.0.0 to send to TSG SA list by e-mail for information, and update again to version 2.0.0 for presentation to TSG SA for approval at TSG SA meeting #12 (June 2001).

9.2 IP network layer security (draft TS 33.210)

TD S3-010147 (NDS/IP Parts) - Rapporteur for TS 33.xxx: Geir Koien, Telenor volunteered to keep rapporteurship for this new document and this was welcomed by SA WG3. It was planned to present the TS to TSG SA for information in September, if it is to be approved and under change control in December 2001. This was considered a little over-ambitious given the other work that SA WG3 need to deal with for Rel-5 and recent slow progress of this work. Some contributions had been provided to the meeting which should help with progress. It was agreed that the final date should be updated to March 2002, and the WI descriptions for all NDS WIDs were updated and presented in TD S3-010275 and TD S3-010276 which were updated in TD S3-010285 and TD S3-010286 (see agenda item 7.1).

TD S3-010148 Introduced by the NDS Rapporteur, and relevant contributions were taken as the document was reviewed. Contributions were invited to help finalise the document in good time.

> TD S3-010203 Proposed changes to 33.xxx NDS IP Security about interfaces. This was introduced by Nokia, and proposes the addition of Mw and Mm interfaces for SIP support. Other interfaces may be affected but this required further study. This proposal was agreed.
>
> TD S3-010176 NDS architecture for IP-Based protocols. This was introduced by Motorola and proposes a centralised inter-domain SA negotiation. The proposed modifications to the draft were provided in TD S3-010178. There was some discussion over this proposal, and the claim of improved efficiency required verification. A related contribution in TD S3-010198 was also considered:
>
> > TD S3-010198 GTP security issue. This was presented by France Telecom and proposed that the protection of the signaling messages between the SGSN and GGSN is done end to end when roaming in order to guarantee the security of operators' networks for Rel-5, guarding against hackers breaking into Border Gateways and sending valid messages over the protected link between networks.
>
> The Chairman remarked that he was reluctant to change anything in the established architecture, as this would cause delays on this work, which is already delayed to March 2002, and with a lot of work to complete. It was agreed to leave this for the time being and move on to other contributions.
>
> TD S3-010191 Mandate 3DES for use of ESP with GTP-C. This proposes to use 3DES instead of AES for GTP-C confidentiality, in order to re-use existing products. It was argued that AES could be very common by the time Rel-5 is imple~~n~~mented and this proposal may lose the advantages of using it. It was considered premature to mandate the use of 3DES when AES is expected to be chosen as a replacement by the IETF. In view of the delay added to the target for the NDS/IP document, this may no longer be necessary and it was agreed that this should not be considered at the moment.
>
> TD S3-010201 Proposed changes to 33.200 about Za, Zb, Zc interfaces. This was introduced by Nokia and provided changes to the document to include the multiple SEG description to avoid a single point of failure. It was agreed that the description about multiple physical SEGs was not relevant to the stage 2 and this should not be included. Some minor modifications for the text on implementation of the Zb interface and clarifications were suggested (e.g. note 2 should remain until the document is near finalised), and the updated proposals were accepted. The overall security with the allowed implementation options should be considered during the editing of the document. It was agreed that Za (inter domain interface) is mandated and to consider the status of the Zb and Zc interfaces for further contribution.

TD S3-010204 Proposed changes to 33.xxx about protecting user plane traffic. This was presented by Nokia and mainly proposes to allow security domain operators to use NDS procedures to protect GTP-U. There was argument that the protection of the user-plane data would produce a large overhead and therefore had been forbidden. It was agreed that this should be considered at a later date in order to focus on signalling plane data protection.

TD S3-010202 Proposed changes to 33.200 about firewalls. This was presented by Nokia and proposes including some simple filtering on the input to the SEG to reject e.g. non-operator addressed traffic. This principle was accepted, although the text should be softened.

The editor was then asked to update the document off-line.

9.3 IM subsystem security (draft TS 33.203)

TD S3-010199 Integrity protection for SIP signalling. This was presented by Ericsson. The concern raised by Nokia on e.g. Multiple SIP clients on a laptop computer and the MS having the same IP address, causing packets to be~~ing~~ mixed up, was reported not to be a problem, as in the IP model, MSs need to have different IP addresses and Port numbers. The assumption that ESP would be appropriate and that security associations could be bound to port numbers needs to be studied.

It was reported that IPsec does not work well with Network Address Translators (NATs), and a solution which can cope with IPv4 should be sought in case of problems.

Cryptographic Message Syntax (CMS) was considered to be high on overhead and contains many features that are not needed by the 3GPP system. A solution to select only the required parts of CMS in order to develop a protocol with smaller overhead should also be investigated. It was noted that syntax is normally outside the SA WG3 scope, and was also a CN WG1 issue, so that the SA WG3 and the CN WG1 points should be sepa~~e~~rated for discussion in relevant groups. The contribution was then noted.

TD S3-010200 Proposal to use a generic authentication scheme for SIP. This was presented by Ericsson, and an AKA draft was attached. The contribution compares SIP AKA, SIP EAP and SIP SASL approaches for authentication and concluded that EAP and SASL were good candidates, but that all need some standardisation work to be done in the IETF.

Ericsson agreed to provide an updated contribution including the agreements reached, which would require an extension in the IETF. The stability of the RFC was questioned and it was considered that due to the increasing use (e.g. in wireless LAN networks) the RFC is likely to remain in the future.

It was recognised that the IETF would have to be informed that the proposed requirements would be used for 3GPP Security and therefore they should seriously consider the mechanism for inclusion.

The dependency of the SA WG3 specifications on the IETF documents which are under development would need to be considered, as late changes or future modification by the IETF could cause problems with the 3GPP implementations. **The Chairman agreed to take this to TSG SA as an issue for advice on how this problem should be handled in general within 3GPP**.

An updated version of TD S3-010200 containing the current assumptions agreed by SA WG3 was created by Ericsson in TD SP-010263 which was presented and agreed as an input to 33.203. A related LS in TD S3-010262 to CN WG1 and CN WG4 (and also copied to SA WG2) was presented. This was discussed and updated in TD S3-010287 and approved. The Chairman agreed to provide a LS to SA WG2 confirming the decision to terminate the authentication check in the S-CSCF. **<Secretary Note: HAS THIS BEEN PRODUCED? - WHICH TD NUMBER ?>**

TD S3-010211 33.203v0.3.0 - Access security for IP-based services (Rel-5). This provided the changes since the previous version taking into account changes agreements at the IMS ad-hoc meeting in April 2001. The document was reviewed and relevant contributions discussed when relevant:

TD S3-010205 Authentication aspects in IM. This was introduced by BT, and concludes that the ability to authenticate at any time would give the operator the same flexibility as 3G Release 1999 and that this flexibility should be available within the IM in the Rel-5 timeframe.

It was reported by AT&T that SA WG2 had discussed the re-registration on IM sessions, and had concluded that it was not a user-friendly procedure, and long session times are foreseen for IMS. It was explained that re-registration frequency would be an operator value, and the mechanisms for this were currently being discussed.

TD S3-010203 Proposed changes to 33.xxx NDS IP Security about interfaces. This was introduced by Nokia, and proposes the addition of Mw and Mm interfaces for SIP support. Other interfaces may be affected but this required further study. This was reconsidered under agenda item 9.2.

It was reported that Ericsson had withdrawn their proposals for termination of authentication in the HSS. The SA WG3 Chairman had written a letter to SA WG2 Chairman stating that he had instructed the group as follows:

> *Ericsson and Siemens to try to find a mutually acceptable solution, if no agreement is reached, then SA WG2 were asked to look for compelling architectural reason to favour one proposal over the other. If no compelling reason is found, then the SA WG3 Chairman would make a decision at S3#18 meeting.*

TD S3-010209 LS from SA WG2 on the termination of authentication in the IMS (S2-011528). This LS informed SA WG3 that SA WG2 had discussed the termination of authentication and concluded that it should terminate in the S-CSCF. Ericsson pointed out that this was not based on a compelling architectural reason, although they did not contest the decision to terminate in the S-CSCF as they had come to agreement~~net~~ with Siemens in order to progress the IMS work. Siemens agreed that some information flows were still required. The LS was then noted.

TD S3-010208 The CR in S2-011524 was noted, and a document number for the references to the IP-based access security document would be provided was provided in a response LS, in TD S3-010265 which was approved.

TD S3-010249 Liaison Statement from CN WG1on the IM Call Transfer service. This was introduced by BT and it requested~~s~~ SA WG3 to review the IM Call transfer service message flows with a view to potential fraud problems and to respond to CN WG1 by their meeting, 10 July 2001. The flows in the attachment were considered briefly, but it was considered better to receive an expla~~i~~nation of the flows from a CN WG1 expert. A LS requesting this at SA WG3 meeting #19 was produced in TD S3-010266, which was updated in TD S3-010292 and approved. **This LS will be sent to the CN WG1 Chairman**.

TD S3-010219 Integrity protection mechanism between UE and P-CSCF. This was presented by Nokia and proposes a method to provide integrity protection by a method similar to the one used in UTRAN and the message authentication code function can be defined to be the Kasumi f9. This was discussed and it was recognised that this could be used in conjunction with other contributions in order to obtain a good basis for further work. It was agreed that the whole SIP message will be protected. ***Interested parties were asked to get together and elaborate a joint proposed solution***.

TD S3-010220 Integrity protection of the IMS registration. This was presented by Nokia and reports on potential lack of integrity protection on certain registration messages and problems with performance aspects for authentication to protect these which need to be studied. After some discussion, Nokia agreed to work with Ericsson and other interested parties in order to complete the details, detail the issues and clarify the security implications for the SA WG3 meeting #19.

TD S3-010160 Proposed Reply LS for " IM User Identities " (S2-010757): This LS had been presented in the joint meeting with SA WG2 in April 2001, and was considered by SA WG3. It was clarified that the "Proposed" in the title was an editorial error, and the reply had been approved at SA WG2. It was agreed to include a response to this in TD S3-010231 which was provided by Siemens and was revised in TD S3-010291 and then approved.

TD S3-010250 Liaison Statement from CN WG1 on " Handling of ICMP messages by 3GPP SIP Implementations". This LS asked SA WG3 whether the 3GPP SIP implementation should handle the ICMP messages as recommended in RFC 2543, or be ignored by the 3GPP SIP implementation. It was agreed that it was never the intention to protect ICMP messages. A response LS was drafted in TD S3-010274 which was approved.

9.4 GERAN security

TD S3-010150 Revised working assumptions made at the joint TSG GERAN / TSG SA WG3. This provided the agreements for working assumptions that were made at the Joint ad-hoc meeting in April 2001. The proposal to use 32-bit MAC protection for messages which this would not cause additional segmentation and therefore not adversely affect the efficiency, and to use a shorter MAC length for other messages was discussed. It was recognised that the RLC/MAC Messages could not be integrity protected, and this was noted as a weakness of the GERAN compared to UTRAN, as protection had not been designed in from the beginning. Some questions were asked of SA WG3 in the document:

Q1 Can a shorter MAC-I be used for RRC messages?

A1 No

Q2 How is ciphering/integrity provided when the Controlling RAN is different from the Serving RAN node?

A2 This is open for further study (Keys need to be provided to both the Controlling and Serving RAN nodes).

Q3 What identity is used to page a MS?

A3 The MS is paged as available in the order: TMSI/PTMSI; IMSI; IMEI.

The SA WG3 Chairman agreed to provide a response LS to GERAN on the length of MAC for message protection and with the answers to the questions, which was provided in TD S3-010247. Delegates were asked to consider this overnight in order to update this Liaison if necessary before approval. The LS in TD S3-010247 was presented and approved.

9.5 End-to-end security

TD S3-010210 Hybrid sync-frame/sync-free E2E Encryption. This was provided by Lucent. The Chairman asked which companies supported the work item, and it was agreed that this should be postponed until the number of supporting companies is enough. These TDs will be input to SA WG3 meeting #19 if enough companies support the work item.

TD S3-010222 Updated Work Item Description for Network based end-to-~~-~~end~~-~~ security: This was presented by Ericsson and proposes to restrict the scope of end-to-end encryption to IP-based services. BT and Nortel had withdrawn their support, and Motorola had been added, but the status of GemPlus support was not known. There was therefore no Rapporteur for this WI. It was agreed that the required support would be needed before SA WG3 continue with this contribution. Ericsson will check if they support this work, given the withdrawal of the other companies. Support was requested to be confirmed during the meeting in order to progress this WI. **Support is requested for this WI for re-assessment at SA WG3 meeting #19.**

9.6 MExE security

There were no contributions on this agenda item ~~m~~(see also agenda item 7.1).

9.7 OSA security

Contributions for this work item were expected at SA WG3 meeting #19.

9.8 FIGS/IST

There was a proposal to extend FIGS to include the PS domain, but no progress had been made on this so far. Contributions need to be provided to SA WG3 meeting #19. It was agreed that the timescales would need to be reviewed in order to make the deadline more realistic. P. Howard provided a proposal for this update in TD S3-010246. This was presented under agenda item 7.1.

9.9 UE Split

TD S3-010158 Liaison Statement from SA WG1 on UE Functionality Split: This LS points out various scenarios where the basic security was thought to be vulnerable. It was agreed that a joint meeting should be held with SA WG1, T WG2, T WG3, SA WG2 and CN WG1 in order to discuss this, with an early version of the Report for information, as a basis for discussion. A suggested time and venue was made as 3 July 2001, in London, before the SA WG3 meeting #19. A LS to inform the groups of this proposal was provided in TD S3-010289 (approved, see agenda item 9.3).

TD S3-010207 LS from T WG2 concerning reviews of UE Functionality Split: T WG2 informed SA WG1 that they were willing to send delegates to the SA WG1 ad-hoc meeting in the week of 25 June, Dallas, USA. Although SA WG3 delegates would not be able to attend this meeting, it was thought that this could provide useful input to SA WG3 meeting #19. SA WG1 were therefore asked to provide input from this meeting to SA WG3, which would be included in TD S3-010289 (see discussion of TD S3-010158, above).

TD S3-010252 This was a duplication of TD S3-010207, above and was withdrawn.

TD S3-010165 Response from T WG3 to LS (T2-000793) on discussion document on UE functionality split over physical devices: This LS was noted. **M Walker agreed to talk to the SA WG1 Chairman** (K. Holley) to clarify that SA WG3 consider this to be a direct violation of the Security Architecture requirements, which would need a complete redesign to accommodate the proposals, in order to help prevent the WGs doing work which would not be acceptable from a security viewpoint, and thus wasting time.

TD S3-010175 UE Split over several Devices: This contribution was presented by Orange and provided some proposals for a Bridging Function to control access authentication of mul~~i~~tiple USIMs. It also raised some of the issues of the proposal. This was discussed, and the Chairman agreed to draft a LS to T WG3, SA WG1 and T WG2 to point out the security concerns and to suggest a joint meeting on 3 July 2001. This was provided in TD S3-010289.

TD S3-010280 Presented by Stewart Ward and Colin Blanchard as a personal contribution. The idea of a bridge module, which would act like a visited network, requesting AVs and authenticating the users in the same way as a Visited Network would, required some consideration. The contribution was noted, and delegates asked to contribute on this at future meetings, before SA WG3 formally endorse it for forwarding to other groups.

TD S3-010279 LS to T WG3 on Security and UE functionality split. This was introduced by the SA WG3 Chairman and discussed. It proposes a joint meeting between SA WG3, SA WG1, T WG3 and T WG2 on 3 July 2001, before SA WG3 meeting #19 in London, UK. This was updated in TD S3-010289 which was approved.

TD S3-010248 This was withdrawn as it was covered by TD S3-010289.

10 Election of S3 chair and vice chairs

The Candidates for Chairman and Vice Chairmen were as follows:

Chairman: Michael Walker (Vodafone, ETSI)

Vice Chairmen: Michael Marcovici (Lucent, T1) and Valtteri Niemi (Nokia, ETSI)

These candidates were therefore appointed to the posts, without the need for a Vote. All were congratulated and welcomed by SA WG3.

10/1 Approval of CRs and LSs from the meeting

See Annexes D and E for a full list of incoming LSs, approved outgoing LSs and approved CRs.

11 Future meeting dates and venues

Meeting	Date	Location	Host
Joint S1, S2, T3, S3 meeting	3 July 2001	London	Vodafone
S3#19	4 - 6 July 2001	London	Vodafone
S3#20	15 or 16 – 18 October 2001	Sydney, Australia	Qualcomm Int.
S3#21	3 - 5 December 2001	Sophia Antipolis, France	ETSI
S3#22	26 - 28 February 2002	Bristol, UK	Orange
S3#23 + AHAG	14 - 16 May 2002	Canada / NW USA	AT&T Wireless
S3#24	9 - 11 July 2002	Helsinki, Finland (TBC)	Nokia
S3#25	15 - 17 October 2002	Munich, Germany (TBC)	Siemens (TBC)

12 Any other business

There were no other topics raised under this agenda item.

The procedure for the approval of 33.200 Rel-4 was agreed as follows:

The Rapporteur will update the document with the agreements reached, amalgamating the two updated documents drafted in parallel sessions and send to M. Pope. Mr. Pope will update the document editorially into correct 3GPP TS format as version 1.0.0 and send to the TSG SA e-mail list for information. The document will then be updated to version 2.0.0 by Mr. Pope for submission to TSG SA#12 Plenary for approval as Rel-4 (assuming no adverse comments are received on the version 1.0.0).

13 Close of meeting

The Chairman thanked the Host, Motorola, for the excellent venue and services for the meeting, the delegates for their very hard work and good co-operation in the difficult task of finalising TS 33.200 for Rel-4, and congratulated the new Vice Chairmen, Valtteri Niemi on his appointment, Michael Marcovici on his re-appointment, and closed the meeting.

Annex A: List of attendees at the SA WG3#18 meeting

Name	Company	e-mail	3GPP ORG
Mr. Hiroshi Aono	NTT DoCoMo Inc.	aono@mml.yrp.nttdocomo.co.jp	ARIB
Mr. Jari Arkko	ERICSSON L.M.	jarkko@piuha.net	ETSI
Mr. Nigel Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	ETSI
Ms. Tao Bu	Nokia Corporation	tao.bu@nokia.com	ETSI
Dr. Stephen Billington	Hutchison 3G UK Limited	stephen.billington@hutchington3g.com	ETSI
Mr. Colin Blanchard	BT	colin.blanchard@bt.com	ETSI
Mr. Marc Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	ETSI
Mr. Krister Boman	ERICSSON L.M.	krister.boman@emw.ericsson.se	ETSI
Mr. Charles Brookson	DTI	cbrookson@iee.org	ETSI
Mr. Daniel Brown	Motorola Inc.	adb002@email.mot.com	T1
Mr. David Castellanos	ERICSSON L.M.	david.castellanos-zarrora@era.ericsson.se	ETSI
Ms. Lily Chen	T1 Standards Committee	lchen1@email.mot.com	T1
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp	ARIB
Mr. Brian K. Daly	AT&T Wireless Services, Inc.	brian.daly@attws.com	T1
Dr. Adrian Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI
Miss Jessica Gunnarsson	TELIA AB	jessica.l.gunnarsson@telia.se	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vf.vodafone.co.uk	ETSI
Miss Janette Huntington	Motorola Inc.	P28213@email.mot.com	T1
Mr. Tom Inklebarger	AT&T Wireless Services, Inc.	tominkle@home.com	T1
Mr. Geir Køien	TELENOR AS	geir-myrdahl.koien@telenor.com	ETSI
Mrs. Tiina Koskinen	NOKIA Corporation	tiina.s.koskinen@nokia.com	ETSI
Mr. Alexander Leadbeater	BT	alex.leadbeater@bt.com	ETSI
Mr. Michael Marcovici	Lucent Technologies	marcovici@lucent.com	T1
Mr. Sebastien Nguyen Ngoc	France Telecom	sebastien.nguyenngoc@francetelecom.com	ETSI
Mr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI
Mr. Petri Nyberg	SONERA Corporation	petri.nyberg@sonera.com	ETSI
Mr. Bradley Owen	Lucent Technologies N. S. UK	bvowen@lucent.com	ETSI
Mr. Olivier Paridaens	ALCATEL S.A.	olivier.paridaens@alcatel.be	ETSI
Mr. Frank Quick	QUALCOMM EUROPE S.A.R.L.	fquick@qualcomm.com	ETSI
Mr. Greg Rose	QUALCOMM EUROPE S.A.R.L.	ggr@qualcomm.com	ETSI
Mr. Dewayne Sennett	AT&T Wireless Services, Inc.	dewayne.sennett@attws.com	T1
Mr. Teruharu Serada	NEC Corporation	serada@aj.jp.nec.com	ARIB
Mr. Hugh Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	T1
Mr. Benno Tietz	MANNESMANN Mobilfunk GmbH	benno.tietz@d2vodafone.de	ETSI
Mr. Lee Valerius	NORTEL NETWORKS (EUROPE)	valerius@nortelnetworks.com	ETSI
Prof. Michael Walker	VODAFONE Group Plc	mike.walker@vf.vodafone.co.uk	ETSI
Mr. Stuart Ward	ORANGE PCS LTD	stuart.ward@orange.co.uk	ETSI
Dr. Peter Windirsch	Deutsche Telekom AG	Peter.Windirsch@t-systems.de	ETSI
Dr. Ernest Woodward	Intel Sweden AB	ernest.e.woodward@intel.com	ETSI
Tom Defray ???	PLEASE CHECK AND CORRECT/UPDATE		

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010140	Draft agenda for meeting #18	SA WG3 Chairman	2	Approval		Approved
S3-010141	Draft report of meeting #17	Secretary	4.1	Approval		Approved
S3-010142	Response to LS (S1-010144) from T3 chairman on the Elaboration of KEY IDENTIFICATION EVENT	SA WG1	5.3.1	Discussion		Noted. TD166 reports no problem.
S3-010143	Draft report of NDS ad-hoc, April 23-24 April 2001	Secretary	4.2	Information		Approved
S3-010144	Draft report of aSIP ad-hoc, April 25 2001	Secretary	4.2	Information		Approved
S3-010145	Draft report of SA WG3/SAWG1 IMS joint session, April 26 2001	Secretary	4.2	Information		Approved
S3-010146	Draft report of SA WG3/GERAN joint meeting, April 27 2001	Secretary	4.2	Information		Approved
S3-010147	Status report for NDS	NDS Rapporteur	9.1	Information and decision		Noted. Used for editing sessions
S3-010148	Update information on TS33xxx (NDS-IP) (from TS33200 v035) and 33.ndsIP v 0.5.0	NDS Rapporteur	9.2	Information and discussion		Checked and contributions provided. Spec to be updated by Rapporteur
S3-010149	Update information –TS 33.200 (NDS-MAPSec) and 33.200 v.0.5.0	NDS Rapporteur	9.1	Information and discussion		Noted. Used for editing sessions
S3-010150	Revised working assumptions made at the joint TSG GERAN / TSG SA WG3 (GAHW-01 0245)	TSG-GERAN Adhoc#5	5.3.5 / 9.4	Discussion		CR in TD236. Response in TD247
S3-010151	Re-transmission of authentication requests	CN WG1	5.3.2	Discussion		Response in TD230
S3-010152	LS on "Security for IM SIP session Signaling" (N1-010588)	CN WG1 Joint SIP ad-hoc	5.3.2	Dicussion		Response in TD291
S3-010153	LS on THRESHOLD check at RRC connection establishment (R2-010981)	RAN WG2	5.3.4 / 5.3.6	Dicussion		Corresponding CR in TD196. Corresponding response from N1 in TD234. Noted.
S3-010154	LS on Wrap around of the calculated START value (R2-010982)	RAN WG2	5.3.4	Discussion		Response in TD278
S3-010155	Response to LSs related to optimised IP speech and header removal support in GERAN (R3-010890)	RAN WG3	5.3.4	Information		Noted.
S3-010156	LS on basic and advanced services examples (S1-010271)	SA WG1	5.3.1	Information		Noted.
S3-010157	LS on Extended Streaming Service (S1-010501)	SA WG1	5.3.1	Information		Response in TD293

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010158	Liaison Statement on UE Functionality Split (S1-010575)	SA WG1	9.9	Discussion		Agreed that a JM is needed. Response LS in TD289
S3-010159	LS regarding User Profile (S1-010591)	SA WG1	5.3.1	Discussion		Noted. Response LS in TD225
S3-010160	Proposed Reply LS for " IM User Identities " (S2-010757)	SA WG2	5.3.1, 9.3	Discussion		Response in TD291
S3-010161	Proposed Liaison to S3 on use of Diameter (S2-010758)	Lucent	5.3.1	Discussion		Noted.
S3-010162	RE : LS on authentication test algorithm to be implemented in test USIMs (T3-010246)	T WG3	5.3.3	Discussion		See also S3-010167. Noted.
S3-010163	Rejection of 2G Authentication and Key Agreement by 3G ME with USIM in UTRAN (T3-010379)	T WG3	5.3.3	Discussion		Agreed. Response in TD232
S3-010164	LS for "IM Subsystem Address Storage on USIM " (T3-010193)	T WG3	5.3.3	Information		Noted.
S3-010165	Response to LS (T2-000793) on discussion document on UE functionality split over physical devices (T3-010250)	T WG3	9.9	Discussion		M Walker to talk to S1 Chairman to prevent time wasted on insecure work
S3-010166	Response to LS (S3-010128) on the Elaboration of KEY IDENTIFICATION EVENT (T3-010323)	T WG3	5.3.3	Discussion		Noted.
S3-010167	LS on authentication test algorithm to be implemented in test USIM (T3-010324)	T WG3	5.3.3	Discussion		See also S3-010162. Noted.
S3-010168	LS in reply to LS on MExE and User Equipment Management - T2-000756 (S5-010114)	SA WG5	5.3.1	Information		Noted.Response in TD293. Updated WI in TD226
S3-010169	Canidature for Vice Chairman - Valter Niemi, Nokia	Nokia	10	Information		Elected as VC
S3-010170	Canidature for Vice Chairman - Michael Marcovici, Lucent	Lucent	10	Information		Elected as VC
S3-010171	Canidate for Chairman - Michael Walker - Vodafone	Vodafone	10	Information		Elected as Chairman
S3-010172	User Profiles (S1-010435)	Ericsson LM	5.3.1	Discussion		Attachment to S3-010159. Noted
S3-010173	LS to SA WG3 on security in IP-transport based UTRAN (R3-011081)	RAN WG3	5.3.4	Approval		Noted.
S3-010174	Proposed new SA4 Work Item on Extended Streaming Service (S4-010304 attached)	SA WG4 Chairman	5.3.1	Discussion		Response in TD293
S3-010175	UE split over several devices	Orange	9.9	Discussion		Discussed. LS on security concerns produced in TD289
S3-010176	NDS architecture for IP-Based protocols	Motorola Inc.	9.2	Discussion and decision		Used to update 33.210 draft

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010177	WITHDRAWN - Change Request for “TS33.200 Network Domain Security v032”	Motorola Inc.	9.1	Discussion and decision		Withdrawn due to split of TS 33.200
S3-010178	Change Request for “TS33.xxx Network Domain Security: IP Network Layer Security”	Motorola Inc.	9.2	Discussion and decision		Used to update TS 33.210 draft
S3-010179	Proposed CR to 33.102 v3.8.0: Correction to periodic local authentication	Siemens Atea	8.1	Approval		Approved as Cat F
S3-010180	Proposed CR to 33.102 v4.0.0: Correction to periodic local authentication	Siemens Atea	8.1	Approval		Approved as Cat A
S3-010181	Proposed CR to 33.102 v3.8.0: Correction to COUNT-C description	Siemens Atea	8.1	Approval		Approved as Cat F
S3-010182	Proposed CR to 33.102 v4.0.0: Correction to COUNT-C description	Siemens Atea	8.1	Approval		Approved as Cat A
S3-010183	Proposed CR to 33.102 v3.8.0: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted.	Nokia	8.1	Approval	S3-010240	Updated in TD240
S3-010184	Proposed CR to 33.102 v4.0.0: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted.	Nokia	8.1	Approval	S3-010241	Updated in TD241
S3-010185	Proposed CR to 33.103 v3.5.0: The multiplicity of Data integrity symbols	Nokia	8.2	Approval		Approved
S3-010186	Proposed CR to 33.103 v4.0.0: The multiplicity of Data integrity symbols	Nokia	8.2	Approval		Approved
S3-010187	Proposed CR to 33.105 v3.7.0: Deletion of the maximum size of a RRC message	Nokia	8.3	Approval		Approved
S3-010188	Proposed CR to 33.105 v4.0.0: Deletion of the maximum size of a RRC message	Nokia	8.3	Approval		Approved
S3-010189	Comments on TS 33.200 v050	Siemens Atea	9.1	Discussion and decision		Discussed and used for editing sessions
S3-010190	Structure of Initialisation Vector in MAPSec	Siemnes AG	9.1	Discussion and decision		Agreed proposal.
S3-010191	Mandate 3DES for use of ESP with GTP-C	Siemnes AG	9.2	Discussion and decision		Not to be considered at present.
S3-010192	Protection Profiles for MAP Security	Siemens Atea	9.1	Discussion and decision		Agreed assumption. Used in editing session.
S3-010193	LS from T WG1: Response to LS on authentication test algorithm in test USIM (T1-010231)	T WG1	5.3.3	Discussion		Covered by TD167, response in TD233
S3-010194	LS from T WG3 on New feature for SAT originated SMS (T3-010443)	T WG3	5.3.3	Discussion		Noted.

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010195	Proposed CRs to 33.102 R99 and Rel-4: Calculation and Wrap-around of START value	Ericsson	8.1	Approval	S3-010269, S3-010270	Updated in TD269, TD270
S3-010196	Proposed CRs to 33.102 R99 and Rel-4: THRESHOLD Check at RRC connection establishment	Ericsson	8.1	Approval	S3-010238	Updated in TD238
S3-010197	Use of Combined TVP/IV parameter	Ericsson	9.1	Discussion and decision		Used in conjuntion with TD190. Used in editing session
S3-010198	GTP security issue	France Telecom	9.2	Discussion and decision		Should be considered for future development
S3-010199	Integrity protection for SIP signaling	Ericsson	9.3	Discussion and decision		Discussed and noted.
S3-010200	Proposal to use a generic authentication scheme for SIP	Ericsson	9.3	Discussion	S3-010263	Chairman to ask SA how to work with IETF
S3-010201	Proposed changes to 33.200 about Za, Zb, Zc interfaces	Nokia	9.2	Discussion and decision		Za agreed. Zb and Zc for future study.
S3-010202	Proposed changes to 33.200 about firewalls	Nokia	9.2	Discussion and decision		Accepted in principle, text should be softened.
S3-010203	Proposed changes to 33.xxx NDS IP Security about interfaces	Nokia	9.3 / 9.2	Discussion and decision		Proposal agreed.
S3-010204	Proposed changes to 33.xxx about protecting user plane traffic	Nokia	9.2	Discussion and decision		User plane protection to be considered at a later date.
S3-010205	Authentication aspects in IM	BT	9.3	Discussion and decision		Discussed and used for input to 33.203
S3-010206	TR-45 / 3GPP Joint AKA Control	TR-45/AHAG	6.1	Discussion		Approved. SA3 Chair to forward to SA for endorsement
S3-010207	LS Concerning Reviews of UE Functionality Split	T WG3	9.9	Discussion		Input requested to S3#19 in LS TD289
S3-010208	LS from SA WG2 on Security Associations for IMS functional elements (S2-011573)	SA WG2	9.3	Discussion / Decision		Provided by Motorola. Response in TD265
S3-010209	LS from SA WG2 on the termination of authentication in the IMS (S2-011528)	SA WG2	9.3	Discussion / Decision		Provided by Motorola. Noted.
S3-010210	Hybrid sync-frame/sync-free E2E Encryption	Lucent	9.5	Discussion		Postponed until enough supporting companies.
S3-010211	33.203 v 0.3.0: Access security for IP-based services (Rel-5)	Rapporteur	9.3	Discussion		Reviewed for update and other contributions discussed as appropriate.
S3-010212	WID: Access security for IP-based services		7.1		S3-010239	Updated in TD239 and then TD283
S3-010213	Report to SA3 on SA#11		5.2			Noted.
S3-010214	Proposed changes to 33.200v0.5.0	Vodafone	9.1			Discussed and used for editing sessions

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010215	The MAP Security Domain of Interpretation for ISAKMP	Ericsson	9.1			
S3-010216	Corrections to 33.200		9.1			Used for editing sessions
S3-010217	WITHDRAWN (dup of TD 210)					
S3-010218	33.200 (MAP) v0.5.0	Alcatel	9.1			Discussed and used for editing sessions
S3-010219	Integrity protection mechanism between UE and P-CSCF	Nokia	9.3			Needs further study
S3-010220	Integrity protection of the IMS registration	Nokia	9.3			Revisit at S3#19. Nokia Ericsson and interested parties to discuss and contribute.
S3-010221	Presentation on MAPSEC DOI Version -02	Ericsson	9.1			
S3-010222	Updated Work Item Description for Network based end-to end- security	Ericsson	9.5	Approval		Support requested at S3#19.
S3-010223	comments on draft-arkko-map-doi-01.txt		9.1			
S3-010224	Report of TSG-T3 Ad Hoc Meeting #37 (Joint with TSG-S3)	T WG3 Secretary	4.3	Information		Noted
S3-010225	LS to SA WG1: Reply LS on streaming and user profile	SA WG3	9.5	Approval	S3-010281	Updated in TD281
S3-010226	Response to LS S5-010114 (S3- 010168) on MExE and User Equipment Management	SA WG3	9.6	Approval		Approved.
S3-010227	Revised MExE Security Analysis Activity WID	SA WG3	7.1	Approval	S3-010288	Updated in TD288
S3-010228	LS from CN WG4 on MAP security (N4-010669)	CN WG4	9.1	Discussion		Noted. Used for editing sessions of NDS.
S3-010229	Report of LI meeting, Clearwater	SA WG3-LI Chairman	5.1			Noted
S3-010230	Reply LS on the handling of retransmitted authentication requests	SA WG3	10.1			Approved.
S3-010231	Reply to the following LSs: LS on "Security for IM SIP session Signaling" (Tdoc N1-010588, received as S3-010152) AND LS on " IM User Identities" (Tdoc S2-010757, received as S3-010160)	SA WG3	10.1		S3-010291	Updated in TD291
S3-010232	Reply to LS on rejection of 2G authentication and key agreement by 3G ME with USIM in UTRAN	SA WG3	10.1	Approval		Approved.
S3-010233	Reply LS on authentication test algorithm to be implemented in test USIM	SA WG3	10.1	Approval		Approved.
S3-010234	[DRAFT] Liaison Statement on THRESHOLD check at RRC connection establishment	CN WG1	5.3.4	Discussion		Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010235	Draft Reply LS to RAN WG2 on Wrap around of the calculated START value	SA WG3	5.3.4	Approval	S3-010278	Updated in TD278
S3-010236	CR to 33.102 : Include reference to TS 43.041 GERAN Stage 2 specification	SA WG3	10.1	Approval		Approved as Cat B
S3-010237	Draft Reply LS on THRESHOLD Check at RRC connection establishment	SA WG3		Approval	S3-010273	Updated in TD273
S3-010238	CRs to 33.102 R99 and Rel-4: THRESHOLD Check at RRC connection establishment	SA WG3	5.3.6	Approval	S3-010272, S3-010271	Updated in TD272, TD271
S3-010239	WID: Access security for IP-based services	SA WG3	7.1	Approval	S3-010283	Updated time scales in TD283
S3-010240	Proposed CR to 33.102 v3.8.0: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted.	SA WG3	8.1	Approval		Approved as Cat F
S3-010241	Proposed CR to 33.102 v4.0.0: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted.	SA WG3	8.1	Approval		Approved as Cat A
S3-010242	WITHDRAWN (not needed)					
S3-010243	WITHDRAWN (not needed)					
S3-010244	WITHDRAWN (not needed)					
S3-010245	WITHDRAWN (not needed)					
S3-010246	Revised FIGS/IST work item description	Vodafone	7.1	Approval		Approved.
S3-010247	Reply to LS on revised working assumptions made at joint GERAN/S3 meeting	SA WG3	10.1	Approval		Approved.
S3-010248	WITHDRAWN (covered by TD289)					
S3-010249	[DRAFT] Liaison Statement from CN WG1on the IM Call Transfer service	CN WG1	9.3	Discussion		Response to CN WG1 Chair in TD292
S3-010250	Liaison Statement from CN WG1 on " Handling of ICMP messages by 3GPP SIP Implementations"	CN WG1	9.3	Discussion		Response in TD274
S3-010251	WITHDRAWN (duplication of TD234)					
S3-010252	WITHDRAWN (duplication of TD207)					
S3-010253	Reply to LS on New feature for SAT originated SMS	T WG2	5.3.3	Discussion		Response to TD194. Noted.
S3-010254	Comments on MAPsec DOI –02 Internet Draft	Alcatel	-	Discussion		Postponed to S3#19
S3-010255	3GPP S3 Request for Clarification on Positive Authentication Reporting	AHAG	6.2	Discussion		Noted. To be progressed when the Rel-5 work has been progressed
S3-010256	UIM Authentication Method	AHAG	6.1	Discussion		Noted.
S3-010257	33.200 version 0.6.0	NDS Drafting group	9.1	Editing		Further edited

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010258	33.200 version 0.6.0 (as edited in morning drafting session)	NDS Drafting group	9.1	Editing		Further edited
S3-010259	LS from GSMA on Development of new A5/3	GSMA SG	5.5	Discussion		Response in TD282, including proposed update to Work Plan (TD261)
S3-010260	Reply to LS on the Development of new A5/3	SA WG3	5.5	Approval	S3-010282	Updated in TD282.
S3-010261	Provisional work plan for the design of the SAGE GSM A5/3 Task Force (SAGE GSM A5/3 TF)	KPN Research	5.5	Information		Noted. Proposed update to timescales in TD282
S3-010262	reserved for LS to CN1,N4,S2 on S3 assumptions for IMS/SIP (Ericsson)	SA WG3	10.1	Approval	S3-010287	Updated in TD287
S3-010263	Proposal to use a generic authentication scheme for SIP (rev of TD200)	Ericsson	9.3	Discussion		Agreed as input to 33.203.
S3-010264	WID Security aspects of requirements for Network Configuration Independence	AWS	7.11	Approval	S3-010284	Updated in TD284
S3-010265	Reserved for response LS to TD208	Peter H	10.1	Approval		Approved
S3-010266	Response to Liaison Statement on the IM Call Transfer Service N1-010890 (S3-010249)	SA WG3	10.1	Approval	S3-010292	Updated in TD292
S3-010267	Response LS to S1 LS Regarding User Profiles	SA WG2	5.3.1	Discussion		Joint Meeting invitation in TD278. Response LS in TD293
S3-010268	Reply LS on Wrap around of the calculated START value	SA WG3	10.1	Approval		Approved. TD269 and 270 attached
S3-010269	CR to 33.102 R99: Calculation and Wrap-around of START value	SA WG3	8.1	Approval		Approved. Attached to TD268
S3-010270	CR to 33.102 Rel-4: Calculation and Wrap-around of START value	SA WG3	8.1	Approval		Approved. Attached to TD268
S3-010271	CR to 33.102 Rel-4: THRESHOLD Check at RRC connection establishment.	SA WG3	8.1	Approval		Approved. Attached to TD273
S3-010272	CR to 33.102 R99: THRESHOLD Check at RRC connection establishment.	SA WG3	8.1	Approval		Approved. Attached to TD273
S3-010273	Reply LS on THRESHOLD Check at RRC connection establishment	SA WG3	8.1	Approval		Approved. TD271 and 272 attached.
S3-010274	Response to TD250 on ICMP protection	SA WG3	10.1	Approval		Approved.
S3-010275	Updated WIDs for NDS/MAP	NDS Rapporteur	7.1	Approval	S3-010285	Updated in TD285
S3-010276	Updated WIDs for NDS/IP	NDS Rapporteur	7.1	Approval	S3-010286	Updated in TD286
S3-010277	NDS-MAP drafting output 33.200v0.7.0	NDS Drafting group	9.1		S3-010294	updated in TD294
S3-010278	Invitation to joint meeting on User Profiles	SA WG1	5.3.1	Information		Response in TD293

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010279	LS to T WG3 on Security and UE functionality split	SA WG3	10.1	Approval	S3-010289	Updated in TD289
S3-010280	UE Split over several Devices Version 2	S. Ward, C. Blanchard	9.9	Discussion		Noted.
S3-010281	Reply LS on extended streaming service and user profiles	SA WG3	5.3.1	Approval	S3-010293	Updated in TD293
S3-010282	Reply to LS on the Development of new A5/3	SA WG3		Approval		To check if approved?
S3-010283	WID: Access security for IP-based services	SA WG3	7.1	Approval		Approved
S3-010284	WID Security aspects of requirements for Network Configuration Independence	SA WG3		Approval		Approved
S3-010285	Updated WIDs for NDS/MAP	SA WG3		Approval		Approved
S3-010286	Updated WIDs for NDS/IP	SA WG3		Approval		Approved
S3-010287	reserved for LS to CN1,N4,S2 on S3 assumptions for IMS/SIP	SA WG3	10.1	Approval		Approved
S3-010288	Revised MExE Security Analysis Activity WID	SA WG3	7.1	Approval		Approved and attached to TD226
S3-010289	LS to T WG3 on Security and UE functionality split	SA WG3	10.1	Approval		Approved
S3-010290	WITHDRAWN (not needed)					
S3-010291	Reply to the following LSs: LS on "Security for IM SIP session Signaling" (Tdoc N1-010588, received as S3-010152) AND LS on " IM User Identities" (Tdoc S2-010757, received as S3-010160)	SA WG3	10.1	Approval		Approved.
S3-010292	Response to Liaison Statement on the IM Call Transfer Service N1-010890 (S3-010249)	SA WG3	10.1	Approval		Approved. Send toi CN WG1 Chairman
S3-010293	Reply LS on extended streaming service and user profiles	SA WG3	5.3.1	Approval		Approved
S3-010294	NDS-MAP final drafting output 33.200v0.8.0 Geir draft group	NDS Drafting group1		Agreement of update		Rapporteur to update main document for SA information
S3-010295	NDS-MAP final drafting output 33.200v0.8.0 Valtteri draft group	NDS Drafting group2		Agreement of update		Rapporteur to update main document for SA information
S3-010296						
S3-010297						
S3-010298						
S3-010299						

Annex D: List of CRs to specifications under SA WG3 responsibility

Note: SA WG3 agreed CRs to be presented to TSG SA#12 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WG status	Acronym	Remarks
33.102	144		R99	Correction to periodic local authentication	F	3.8.0	S3-18	S3-010179	agreed	SEC1	
33.102	145		Rel-4	Correction to periodic local authentication	A	4.0.0	S3-18	S3-010180	Agreed	SEC1	
33.102	146		R99	Correction to COUNT-C description	F	3.8.0	S3-18	S3-010181	Agreed	SEC1	
33.102	147		Rel-4	Correction to COUNT-C description	A	4.0.0	S3-18	S3-010182	Agreed	SEC1	
33.102	148		Rel-5	Include reference to TS 43.041 GERAN Stage 2 specification	B	4.0.0	S3-18	S3-010236	Agreed	SEC1	Implement to version 4.1.0 when Rel-4 CRs are included
33.102	149		R99	Calculation and Wrap-around of START value	F	3.8.0	S3-18	S3-010269	Agreed	SEC1	
33.102	150		Rel-4	Calculation and Wrap-around of START value	A	4.0.0	S3-18	S3-010270	Agreed	SEC1	
33.102	151		R99	Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted	F	3.8.0	S3-18	S3-010240	Agreed	SEC1	
33.102	152		Rel-4	Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted	A	4.0.0	S3-18	S3-010241	Agreed	SEC1	
33.102	153		R99	THRESHOLD Check at RRC connection establishment	F	3.8.0	S3-18	S3-010272	Agreed	SEC1	
33.102	154		Rel-4	THRESHOLD Check at RRC connection establishment	A	4.0.0	S3-18	S3-010271	Agreed	SEC1	
33.103	014		R99	The multiplicity of Data integrity symbols	F	3.5.0	S3-18	S3-010185	Agreed	SEC1	
33.103	015		Rel-4	The multiplicity of Data integrity symbols	A	4.0.0	S3-18	S3-010186	Agreed	SEC1	
33.105	019		R99	Deletion of the maximum size of a RRC message	F	3.7.0	S3-18	S3-010187	Agreed	SEC1	
33.105	020		Rel-4	Deletion of the maximum size of a RRC message	A	4.0.0	S3-18	S3-010188	Agreed	SEC1	

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD Number	Title	Source	Comment
S3-010142	Response to LS (S1-010144) from T3 chairman on the Elaboration of KEY IDENTIFICATION EVENT	SA WG1	Noted. TD166 reports no problem.
S3-010150	Revised working assumptions made at the joint TSG GERAN / TSG SA WG3 (GAHW-01 0245)	TSG-GERAN Adhoc#5	CR in TD236. Response in TD247
S3-010151	Re-transmission of authentication requests	CN WG1	Response in TD230
S3-010152	LS on "Security for IM SIP session Signaling" (N1-010588)	CN WG1 Joint SIP ad-hoc	Response in TD291
S3-010153	LS on THRESHOLD check at RRC connection establishment (R2-010981)	RAN WG2	Corresponding CR in TD196. Corresponding response from N1 in TD234. Noted.
S3-010154	LS on Wrap around of the calculated START value (R2-010982)	RAN WG2	Response in TD278
S3-010155	Response to LSs related to optimised IP speech and header removal support in GERAN (R3-010890)	RAN WG3	Noted.
S3-010156	LS on basic and advanced services examples (S1-010271)	SA WG1	Noted.
S3-010157	LS on Extended Streaming Service (S1-010501)	SA WG1	Response in TD293
S3-010158	Liaison Statement on UE Functionality Split (S1-010575)	SA WG1	Agreed that a JM is needed. Response LS in TD289
S3-010159	LS regarding User Profile (S1-010591)	SA WG1	Noted. Response LS in TD225
S3-010160	Proposed Reply LS for " IM User Identities " (S2-010757)	SA WG2	Response in TD291
S3-010162	RE : LS on authentication test algorithm to be implemented in test USIMs (T3-010246)	T WG3	See also S3-010167. Noted.
S3-010163	Rejection of 2G Authentication and Key Agreement by 3G ME with USIM in UTRAN (T3-010379)	T WG3	Agreed. Response in TD232
S3-010164	LS for "IM Subsystem Address Storage on USIM " (T3-010193)	T WG3	Noted.
S3-010165	Response to LS (T2-000793) on discussion document on UE functionality split over physical devices (T3-010250)	T WG3	M Walker to talk to S1 Chairman to prevent time wasted on insecure work
S3-010166	Response to LS (S3-010128) on the Elaboration of KEY IDENTIFICATION EVENT (T3-010323)	T WG3	Noted.
S3-010167	LS on authentication test algorithm to be implemented in test USIM (T3-010324)	T WG3	See also S3-010162. Noted.
S3-010168	LS in reply to LS on MExE and User Equipment Management - T2-000756 (S5-010114)	SA WG5	Noted.Response in TD293. Updated WI in TD226
S3-010173	LS to SA WG3 on security in IP-transport based UTRAN (R3-011081)	RAN WG3	Noted.
S3-010174	Proposed new SA4 Work Item on Extended Streaming Service (S4-010304 attached)	SA WG4 Chairman	Response in TD293
S3-010193	LS from T WG1: Response to LS on authentication test algorithm in test USIM (T1-010231)	T WG1	Covered by TD167, response in TD233
S3-010194	LS from T WG3 on New feature for SAT originated SMS (T3-010443)	T WG3	Noted.

TD Number	Title	Source	Comment
S3-010208	LS from SA WG2 on Security Associations for IMS functional elements (S2-011573)	SA WG2	Provided by Motorola. Response in TD265
S3-010209	LS from SA WG2 on the termination of authentication in the IMS (S2-011528)	SA WG2	Provided by Motorola. Noted.
S3-010234	[DRAFT] Liaison Statement on THRESHOLD check at RRC connection establishment	CN WG1	Noted
S3-010249	[DRAFT] Liaison Statement from CN WG1on the IM Call Transfer service	CN WG1	Response to CN WG1 Chair in TD292
S3-010250	Liaison Statement from CN WG1 on " Handling of ICMP messages by 3GPP SIP Implementations"	CN WG1	Response in TD274
S3-010253	Reply to LS on New feature for SAT originated SMS	T WG2	Response to TD194. Noted.
S3-010255	3GPP S3 Request for Clarification on Positive Authentication Reporting	AHAG	Noted. To be progressed when the Rel-5 work has been progressed
S3-010256	UIM Authentication Method	AHAG	Noted.
S3-010259	LS from GSMA on Development of new A5/3	GSMA SG	Response in TD282, including proposed update to Work Plan (TD261)
S3-010267	Response LS to S1 LS Regarding User Profiles	SA WG2	Joint Meeting invitation in TD278. Response LS in TD293
S3-010278	Invitation to joint meeting on User Profiles	SA WG1	Response in TD293

E.2 Liaisons from the meeting

TD Number	Title	Status	To CC
S3-010226	Response to LS S5-010114 (S3- 010168) on MExE and User Equipment Management	Approved	**T WG2/MExE** SA WG5
S3-010230	Reply LS on the handling of retransmitted authentication requests	Approved	**CN WG1**
S3-010232	Reply to LS on rejection of 2G authentication and key agreement by 3G ME with USIM in UTRAN	Approved	**T WG3,** **SA WG1,** **GSMA-SG** T WG2, CN WG1
S3-010233	Reply LS on authentication test algorithm to be implemented in test USIM	Approved	**T WG1, T WG3**
S3-010247	Reply to LS on revised working assumptions made at joint GERAN/S3 meeting	Approved	**TSG GERAN**
S3-010265	Reply LS on Security Associations for IMS functional elements	Approved	**SA WG2**
S3-010268	Reply LS on Wrap around of the calculated START value	Approved e-mailed during S3#18 meeting	**RAN WG2**
S3-010273	Reply LS on THRESHOLD Check at RRC connection establishment	Approved e-mailed during S3#18 meeting	**RAN WG2,** **CN WG1**
S3-010274	Reply to LS on "Handling of ICMP messages by 3GPP SIP Implementations"	Approved	**CN WG1**
S3-010287	Using a generic authentication scheme for SIP	Approved	**CN WG1,** **CN WG4** SA WG2
S3-010289	Security and UE functionality split	Approved	**SA WG1,** **T WG2, T WG3** **TSG SA,** **TSG T,** **ETSI EP SCP**
S3-010291	Reply to LSs: "Security for IM SIP session Signaling" (Tdoc N1-010588, received as S3-010152) AND “IM User Identities” (Tdoc S2-010757, received as S3-010160)	Approved	**CN WG1,** **SA WG2**
S3-010292	Response to Liaison Statement on the IM Call Transfer Service N1-010890 (S3-010249)	Approved e-mailed during S3#18 meeting	**CN WG1** CN WG2, CN WG3, CN WG4, SA WG5
S3-010293	Reply LS on extended streaming service and user profiles	Approved	**SA WG1,** **SA WG4** SA WG2, T WG2