Technical Specification Group Services and System Aspects **TSGS#16(02)0338**

Meeting #16, Marco Island, Florida, 10-13 June 2002

**3GPP TSG SA WG3 Security** **version 0.0.4**

**14 - 17 May 2002**

**Victoria, Canada**

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

**Title:** **Draft Report of SA WG3 meeting #23**

**Document for:** **Information**

**Empress Hotel, Victoria, Canada: Venue of SA WG3 meeting #23**

## Contents

# 1 Opening of the meeting

The SA WG3 Chairman, Prof. M. Walker, opened the meeting and Mr. DeWayne Sennett welcomed delegates to Victoria, Canada on behalf of the hosts, AT&T Wireless and Rogers Wireless. The SA WG3 Chairman reported that he needed to leave the meeting on Thursday 16th due to other commitments, and Mr. V. Niemi, vice chairman, would chair the meeting for the final part.

# 2 Agreement of the agenda and meeting objectives

TD S3-020168 Draft agenda for meeting #23. The draft agenda was considered and minor modifications made to take into account some subjects in the latest set of contributions, the changes are reflected in the agenda items shown in this report. The objectives of the meeting, as stated in the agenda, were agreed.

# 3 Assignment of input documents

The available contributions were allocated to their appropriate agenda items.

# 4 Reports from 3GPP SA3 meetings

## 4.1 SA3#22, 25-28 February 2002, Bristol, UK

TD S3-020169 Draft report of SA WG3 meeting #22. This was reviewed and some minor changes made, the report was then updated in TD S3-020259 which was approved.

## 4.2 SA3#22bis, 8-9 April 2002, Fort Lauderdale, USA

TD S3-020170 Introduced by Chairman of the SA WG3 #22bis meeting, V Niemi. A comment was made on the report of item 5, and this was modified to clarify that the proposal had been made to T WG3, rather than by T WG3. The report was revised in TD S3-020261 which was approved.

## 4.3 SA3 LI #2/02, 9-11 April 2002, Orlando, USA

TD S3-020262 Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #2/02 on lawful interception. The report was introduced by B Wilhelm and was noted.

TD S3-020256 CR to 33.107: Addition of SMS type information. This was a change reflecting the features proposed in draft TS 33.108. It was thought that the request to allow SA WG3 LI to approve 33.108 for Release 5 submission to TSG SA should be considered first (TD S3-020200). This was done (see below) and the CR re-analysed. Some clarification to the description of the CR was made and the CR updated in TD S3-020263 which was approved (pending acceptance of changes in TS 33.108).

TD S3-020200 Request to expedite 33.108 v 1.0.x. The LI group asked for permission to submit TS 33.108 to TSG SA for approval as their meeting is 4-6 June 2002, and TSG SA plenary 10-13 June 2002. SA WG3 asked for time to review the updated document. This was not considered practical in the timescales available, and the SA WG3 Chairman agreed that the document would be submitted a second time for information and TSG SA would be asked to allow finalisation for September 2002. **The SA WG3 Chairman agreed to contact the TSG SA Chairman to inform him of this request.**

The LI group later complained that this delay was unnecessary, and undertook to send the TS to the SA WG3 list for e-mail approval on 20 May. It was agreed that the e-mail approval would take place and close on 31 May 12.00 (CET). If the e-mail approval is successful, the document would then be presented to TSG SA Plenary for approval.

TD S3-020257 CR to 33.107: Changes to 33.107 to support interception at a GGSN. This CR was approved.

TD S3-020258 CR to 33.107: Inclusion of Serving System IRI in TS 33.107. This was in need of a tidy-up to show the Clauses affected and summary of change (as well as the deletion of the added/deleted Annex D). This was provided in TD S3-020264 which was modified slightly again in TD S3-020310 and approved.

TD S3-020192 LS from ETSI TC SEC-LI: Future structuring of documents across the LI standardisation community. This was provided for information to inform SA WG3 of the ASN.1 agreements that had been made between ETSI TC-SEC and the SA WG3 LI group. This was noted.

# 5 Reports and liaisons from other groups

## 5.1 SA

TD S3-020171 SA3 Status Report to SA#15. This was provided for information and was noted.

TD S3-020172 Report to SA3 on SA#15. This was provided for information and was noted. It was also noted that a CR had been provided by the SA WG1 Chairman on TS 33.203 and approved removing a service requirement from the document.

### 5.1.1 SA1

TD S3-020193 Response LS from SA WG1 to SA3 on new security requirements for LCS. This was introduced by Nokia and asked SA WG3 to check the security and privacy requirements provided in the attached TS 22.071 and to provide recommendations and guidance on these issues. It was agreed to do this review as part of the LCS work (for this meeting, see agenda item 6.13).

TD S3-020194 SA1 Assumptions on IMS identities and UICCs. This was left for discussion after the SA WG2 LS in TD S3-020199 and was then noted.

### 5.1.2 SA2

TD S3-020199 LS from SA WG2 on IMS Identities for Rel 99/R4 UICC (response to S3-020167). This was introduced by Ericsson and informs SA WG3 of the assumptions for Release 1999/Rel-4 and Rel-5 MT derivation of public Identity. On reconsideration of the complexity introduced by SA WG2 on the recommendation from SA WG3, it was decided that a response allowing the transport of the IMSI would be provided as this would simplify the specifications and would have no system security impact. P. Howard provided a response LS in TD S3-020312 which was approved.

TD S3-020179 Liaison Statement Reply from SA WG2 to "Status of the Generic User Profile Work". This was introduced by Nokia and was provided for information and noted.

TD S3-020180 Liaison Statement Reply from SA WG2 to "Comments on UP-010141 and relationship of GUP to Subscription Management". This was introduced by Nokia and was provided for information and noted.

TD S3-020181 Liaison Statement from A WG2 on "Prefix allocation for IPv6 stateless address autoconfiguration". This was introduced by Ericsson and asked SA WG3 to consider the new principles adopted for IPv6 stateless address autoconfiguration and to take it into account in any ongoing work and to investigate possible impacts on specifications. The impacts on LI specifications should be considered by the LI group and the LI group was asked to consider this contribution at their next meeting. The potential impacts on IMS security also need to be investigated. TD S3-020244 and TD S3-020245 were discussed and used as part of a response for this to SA WG1.

TD S3-020195 LS back to SA1and SA3 on enhanced user privacy and new security requirements for LCS. This was postponed for discussion with SA WG1 in the joint session, and a discussion group was set up in the evening to consider this. The LS was then noted.

TD S3-020196 LS from SA WG2 on Presence Service. The review of 23.841 would be part of the WID for the Presence service (see Agenda Item 6.18).

TD S3-020198 Response to the LS on "IPv6 update of stage 3 specifications". This was provided for information and was noted.

### 5.1.3 SA5

TD S3-020182 LS reply from SA WG5 on: “3GPP System – WLAN Interworking”. This was provided for information and was noted. This should be considered with the WLAN work.

TD S3-020183 LS reply from SA WG5 on: Priority Service Feasibility Study - draft TR 22.950 v1.0.0. This was provided for information and was noted.

TD S3-020184 Reply to LS on ”IP version inter-working on the transport plane” from SA2 (S2-020291). This was provided for information and was noted. The LS was forwarded to the LI group to consider any impacts on receiving only IPv4 in the CDR.

TD S3-020185 Reply LS from SA WG5 on "support for subscriber certificates" from SA3 (S3-020163). This LS was noted.

TD S3-020186 Liaison Statement from SA WG5 on co-ordination of data definitions, identified in GUP development. This was introduced by BT and was noted.

## 5.2 CN

### 5.2.1 CN1

TD S3-020174 Liaison Statement from CN WG3 on "IPv6 update of stage 3 specifications". This was introduced by Hutchinson 3G UK and answered the questions asked by SA WG3. SA WG3 were considered responsible for the specification of any limitation on the number of SAs stored in the P-CSCF. The CRs should be checked to ensure the requirements are correctly covered (N2-020159). The LS was then noted.

### 5.2.2 CN1

TD S3-020175 Reply Liaison Statement from CN WG1 on ‘Issues with SA handling at P-CSCF’. This was contained in the reply from SA WG2 and was noted.

### 5.2.3 CN4

TD S3-020176 Liaison Statement from CN WG4 on Immediate Service Termination. This was introduced by Vodafone and asked SA WG3 to take note of their recommendations and inform CN WG4 immediately if any of the IST functionality should be removed from their specifications. CN WG4 consider IST functionality as part of the Core Network and should apply equally to GSM and UTRAN access. It was agreed to send a response LS informing them that SA WG3 agree with their recommendations which was provided in TD S3-020266 which was modified slightly in TD S3-020313 and approved.

## 5.3 RAN

TD S3-020177 Response from RAN WG2 to LS (N4-020302) on Trace and Availability of IMSI and IMEI. This was introduced by Siemens and was provided for information. The LS was noted.

TD S3-020178 LS from RAN WG2 on Group release security solution. This was introduced by Ericsson and asked SA Wg3 to inform them whether the security solution for actions at RNC Reset outlined in attached document R2-020734 is acceptable. The attached proposed solution was considered and an analysis of alternative 2 was provided by Siemens in TD S3-020206 which was presented and discussed. Qualcomm also provided comments on this mechanism in TD S3-020205 which was also presented and discussed, which concurred with the Siemens suggestion to use f9 rather than KASUMI directly. The desirability of this feature was then discussed as it may add an increased security risk for DoS attacks. There were a number of members of SA WG3 who were not content with the RNC reset concept. Other issues were also raised on key length and key refresh and a discussion group was set up to consider the implications. A response LS containing the spirit of the two contributions as an acceptable method, **if such RNC Group Release functionality is considered necessary**, was provided in TD S3-020267 which was discussed and modified again in TD S3-020287 which was approved.

## 5.4 T

### 5.4.1 T2

There were no specific contributions under this agenda item.

5.4.2 T3

There were no specific contributions under this agenda item.

### 5.5 GERAN

TD S3-020173 Response from GERAN WG2 to "Response Liaison Statement on Trace and Availability of IMSI and IMEI" (related to TD S3-020177). This was introduced by Nokia and was provided for information and noted.

### 5.6 IETF co-ordination

TD S3-020219 Digest AKA status in IETF. This was presented by Nokia and reported that AKA was progressing well in the IETF. The contribution was then noted.

TD S3-020260 Results from recent IETF coordination meeting. This was an e-mail received from S Hayes, and was introduced by Ericsson. The IETF drafts status list was noted.

### 5.7 ETSI SAGE

P. Christoffersson provided a verbal report on important issues from ETSI SAGE.

For the GSM ciphering algorithm: a new attack on A5/1 had been recently presented, which breaks the session key with statistical correlation on around 5 minutes of partly known plain text. This is not considered a critical attack at present, but shows that a replacement is desirable in the near future. A5/3 is expected to be available for 3GPP and GSMA publication for June 2002.

For the GSM authentication algorithm based on MILENAGE: one issue was whether to convert from 64 to 32 bits by adding the two 32-bit halves together or to truncate the 64 bits provided by MILENAGE. ETSI SAGE decided to leave the method as an operator option, depending on how they have implemented their (U)SIMs.

TD S3-020238 Test data for MILENAGE algorithm. It had been commented that the test data did not include all zero AMF (specifically for f1*) and ETSI SAGE provided this for information. ETSI SAGE are willing to include this if required by SA WG3 in the test data. **SA WG3 members were asked to analyse the proposal to add more test data to see if it would add any value to the test data documents and report back to the next SA WG3 meeting.**

### 5.8 GSMA SG

C. Brookson provided a verbal report on the GSMA SG work.

GSM authentication algorithm of type COMP 128 in SIM cards: A paper was produced by IBM on a potential side channel attack, details of which had been circulated by e-mail to the SA WG3 list. GSMA SG were analysing this.

GPRS implementation reports are being received and analysed by the GSMA SG.

The next GSMA SG meeting is 5-6 June, Maastricht.

EIR: this has become a large issue, in the UK there is draft legislation to make it a serious criminal offence to change IMEI in MTs. Other countries were reported to also be looking into such measures. The draft Bill was later provided for information in TD S3-020276.

### 5.9 3GPP2

M. Marcovicci agreed to act as a liaison person to report on 3GPP2 issues of interest to SA WG3.

### 5.10 TIA TR-45

**Report of Joint session with AHAG**

The AHAG Chairman C. Carroll verbally reported the issues from AHAG of interest to SA WG3. 3GPP-S WG4 is responsible for CDMA2000 security protocols. 3GPP2 AHAG have agreed to continue to develop protocol security development. AKA will remain under AHAG responsibility (and therefore the joint control responsibility) and will advise WG4 of any changes to the AKA. It was

confirmed that 3GPP2 are adopting AKA - the IS 2000 standard Rel-0 is available and Rel-A will implement AES encryption, 128 bit key, Rel-B will implement 3GPP/3GPP2 AKA.

It was also reported that the UMEI (IMEI in a smart card) is being considered in 3GPP2 for authentication based on the secret identifier on the card. There are discussions ongoing on the IMEI format (BCD/binary) for roaming between 3GPP/3GPP2 networks. It was also reported that there were some efforts ongoing to make the IMEI an ITU Recommendation in order to formalise the format used in IMT-2000 networks.

Home Control issues: This was expected for Rel-6, and contributions on this in SA WG3 were required to progress the work. The AHAG Chairman agreed to think about the mechanism to facilitate contribution on this in SA WG3.

The 3GPP2 AHAG Chairman was thanked for his report and clarifications to questions.

# 6 Technical issues

## 6.1 IP multimedia subsystem (IMS)

An evening discussion group considered the IMS inputs. A summary of the results from this was provided in TD S3-020273 which was presented by the Chairman for the discussion group, K. Boman.

**Results from the Drafting Session:**

For Release 5 only integrity protection shall be required and to make it easier to extend this in Release 6 the Null algorithm for encryption shall be included in the list from the UE.

Separate SAs are required for TCP and UDP.

The same integrity key shall be used in both directions and for TCP and UDP. In order to mitigate the reflection attack the SPIs shall be different as proposed in TD S3-020234.

The majority of the group did not see the need for a key derivation mechanism for Release 5. In order to expand a 128 bit integrity key for SHA1 the 32 first bits of the IK shall be appended to IK itself.

HMAC for MD5 and SHA1 shall be supported in Release 5.

The majority of the group supported that the SA lifetime shall be controlled at SIP layer and that at IPSec layer the SA lifetime is set to $2^{32}$-1 seconds. This shall be adopted if no alternative CR is presented challenging this proposal at this meeting. Some security concerns were raised and every participant is encouraged to investigate if there are any security weaknesses with this proposal.

Only one registration is allowed per user at a time. Hence no more than three SAs are required at the most.

The current proposal introducing the concept of suites for IPSec need to be updated such that the agreed working assumptions are reflected accurately.

An attack has been identified in TD S3-020234 and different alternatives are currently discussed. G. Horn will draft an LS to CN1 in order to conclude if the Contact can be used. Another potential solution could be to send the IP Address in SM7 by using the implementation of the SIP Sec Agree.

It was concluded that given that we should be ready on Wednesday such that an LS can be sent to CN1 a drafting session is likely to be required in order to align the agreed CRs into one ‘big’ CR which can be approved at this meeting.

Question 1: Is it possible to send information like e.g. SPI which is dynamic in a static list in SIP Sec Agree? *Yes*

Question 2: Is it possible to send the IP Address of the UE protected by the third message utilising SIP Sec Agree? *Shall be investigated further*.

Peter Howard agreed to write a LS to ETSI SAGE, which was provided in TD S3-020274 which was reviewed and updated to add the alternative key expansion proposal to append 32 '0' bits to IK, in TD S3-020315 which was approved.

TD S3-020244 The use of IPv6 addressing privacy within IMS. This was presented by Ericsson and proposed a solution for addressing the requirement when IP addresses are changed in IMS. The solution was discussed and accepted as a workable solution to be built upon. A CR covering the necessary changes for this was provided in TD S3-020245.

TD S3-020245 Proposal for CR to 33.203 (based on discussion doc S3-020244). The document was reformulated and clarified in TD S3-020268. However, TD S3-020209 deleted the modified text and re-formulated it in new clause 7.4 and this was considered before finalising the review of TD S3-020268.

> TD S3-020209 Proposed CR to 33.203-510: Update of SA handling procedures. The author was asked to revise this CR to use the "SM1, SM2" terminology in order to allow the principles of TD S3-020268 to be included consistently. A review team was set up to read the document carefully and then discuss in order to come to a final clarified text. The discussion group reported that the simplest solution was to update the text to clarify it. A. Escott presented the reasons for this to TS 33.203-510, section 7.3.3.1 and 7.3.3.2: if an attacker sends an unprotected REGISTER message, this could result in the loss of a valid SA between the valid UE and network. A revised CR to clarify the text and providing a solution to this threat was provided in TD S3-020292. This was provided in order to get agreement on the principles and it was decided to hold an e-mail discussion on the proposed changes (the CR was withdrawn from the meeting). An alternative CR was provided by Hutchison 3G UK to clean up the Security Association sections of TS 33.203 editorially in TD S3-020319 which was approved.

TD S3-020306 Draft LS to CN WG1: Secure registration of IP addresses. This was introduced by Siemens asking CN WG1 to inform SA WG3 if the approach agreed is feasible and if not to provide suggestions to provide the necessary secure binding of the UE's IP address to the SA. The LS was modified following discussions and provided in TD S3-020316 which was approved.

TD S3-020234 Justification for proposed changes to text on SIP integrity in TS 33.203 v510. This was used to aid the presentation of the CR in TD S3-020235.

TD S3-020235 Proposed CR to 33.203-510: Requested Changes for SIP integrity. This CR was presented by Siemens and resulted from the agreements made at the discussion group. It was recognised that the CR would need to be re-written as it showed the moved text from Annex B as existing text in section 6 (for clarity of the changes made), which would need to be shown in the correct format for the final CR (all new text in section 6 and deleted text in Annex B). The CR was discussed and clarifications agreed. The updated CR, taking results of agreements into account was provided in TD S3-020275 which was reviewed and updated to take additional comments into account in TD S3-020317 which was approved.

Documents covered by these agreed changes were: TD S3-020213, S3-020221, S3-020222, S3-020223, S3-020225, S3-020231, S3-020233 and S3-020241 which were then withdrawn from the discussion.

TD S3-020270 Proposed CR to 33.203: IP address as SA selector (replacement of TD S3-020240). This was presented by Nokia and discussed. There were concerns about the flexibility that this concept would leave for future developments (e.g. if an operator wishes to deploy a new Authentication Algorithm for negotiation and use within it's Home network subscribers, which would require additional "operator specific" suites to be added). It was agreed that this would simplify the mapping, but that other solutions for this should also be investigated. Delegates were asked to consider this concept and investigate other methods for later decision on the chosen method. The CR was not approved.

TD S3-020224 Proposed CR to 33.203-510: Remove Annexes that describes Extended HTTP Digest solution. This CR was approved.

TD S3-020218 Reference of HTTP Digest AKA in TS 33.203. This CR was corrected to read Category "F" in TD S3-020281 which was approved. It was noted that this adds a reference to an internet draft and would require update when the RFC is available.

TD S3-020212 Proposed CR to 33.203-510: Correcting the network behaviour in response to an incorrect AUT-S. This was updated to correct the specification number in the cover in TD S3-020282 which was later postponed for further discussion at next meeting.

TD S3-020208 Proposed CR to 33.203-510: Correction to S-CSCF behaviour on Network Authentication Failure. This was updated in TD S3-020283 which was later postponed for further discussion at next meeting.

TD S3-020210 Proposed CR to 33.203-510: Update of User Authentication Failure. This was updated in TD S3-020284 which was later postponed for further discussion at next meeting.

TD S3-020232 Proposed CR to 33.203-510: Integrity check failure in the UE. The spirit of this change was agreed to be included in the updated CR in TD S3-020275.

TD S3-020226 ISIM related issues. The CR was considered and approved. A LS was created to inform T WG3 of this change in TD S3-020285 which was modified slightly in TD S3-020314 and approved.

TD S3-020227 Proposed CR to 33.203-510: Clarifications to various issues in TS 33.203. This CR was discussed and alignment with the updated CR in TD S3-020275 was agreed. The changes were accepted in principle and were incorporated in the updated CR in TD S3-020275.

TD S3-020228 Proposed CR to 33.203-510: Removal of encryption between UE and P-CSCF as optional feature in Rel-5. The changes were accepted in principle and were incorporated in the updated CR in TD S3-020275.

TD S3-020207 Proposed CR to 33.203-510: Clean-up of section 6.1.1. This was updated in TD S3-020286 as category "D" (editorial modification), which was approved.

TD S3-020214 Usage of PF_KEY API in IPSec/ESP Parameter Handling for SIP Integrity. This was presented by SSH Communications. It was agreed that such an annex as proposed was not required for Release 5, but could be useful for Release 6 and this should be considered in future work in SA WG3. The document was then noted.

TD S3-020215 IPSec Security Indicator. This was presented by SSH Communications and proposed to add information to 33.203about a IPsec SA indicator signal for IMS connections for Release 6. It was agreed that this should be considered when Release 6 work is progressed. The document was then noted.

TD S3-020217 IETF Status Report for Security Mechanism Agreement. This was introduced by Ericsson and discussed. Ercisson were thanked for their ongoing efforts with Sipsec-agree drafting work and the document was noted.

TD S3-020243 draft-ietf-sip-sec-agree-01.txt. This internet draft was provided by Ericsson for information and was noted. SA WG3 members were encouraged to study the document.

TD S3-020211 New SAs and incomplete authentications. This was presented by Hutchinson 3G UK and described identified potential problems in order to decide whether they should be addressed by SA WG3. The attachments 3, 4 and 5 were considered and A. Escott agreed to include the highlighted changes in attachment 5 as part of the revised CR in TD S3-020292 and the CRs of attachments 3 and 4 were updated in TD S3-020293 and TD S3-020294 respectively, which were approved.

TD S3-020311 Proposed CR to 33.203-510: Security association handling in IMS when the UE changes IP address. This was presented by Siemens and added rules for SA handling when the UE changes IP address. This was modified to Cat C in TD S3-020320 which was approved.

### 6.2 Network domain security: IP layer (NDS/IP)

TD S3-020187 Proposed CR to 33.210-500: Strengthening the requirements on IV construction to prevent attacks based on predictable IV. This was presented by Qualcomm and details a protection against a potential adaptive-plaintext attack when predictable IVs are used. The CR was updated slightly in TD S3-020277 which was approved

TD S3-020188 Proposed CR to 33.210-500: Removal of reference to Internet draft draft-ietf-ipsec-sctp-03.txt. This was presented by Ericsson and proposed the removal of the reference to Internet draft "On the use of SCP with IPsec" and the text in Annex C making use of it as the RFC is unlikely to be completed. There was some concern that the removal of this would leave the protection provided by this absent and something else was needed to provide the protection. It was proposed that the relevant text of the internet draft should be included in the annex instead of the reference. **The principle of the CR was accepted** and a new CR to provide the replacement text would be needed for the next SA WG3 meeting. CN WG4 would need to be informed when the new CR is agreed in SA WG3.

TD S3-020216 Proposed WID: Network Domain Security; Authentication Framework (NDS/AF). This was presented by Nokia. It was clarified that the proposed feasibility study would start by looking at the trust models that could be used, including organisation of the CAs of operators and their inter-relationships. Nokia agreed to clarify the expected outputs of the study and return to the meeting. This was provided in TD S3-020278 which was reviewed. It was decided that this is a Feature WI. The changes were accepted and the final version produced in TD S3-020321 which was approved.

TD S3-020229 Proposed CR to 33.210-500: NDS/IP Confidentiality protection for IMS session keys. This was presented by Ericsson and was approved.

### 6.3 Network domain security: MAP layer (NDS/MAP)

There were no specific contributions under this agenda item.

### 6.4 UTRAN network access security 203 204

TD S3-020279 Proposed CR to 33.102: Encryption/Integrity algorithms ordered by preference in Security Mode command (R99). This CR was modified editorially in TD S3-020288 which was approved.

TD S3-020280 Proposed CR to 33.102: Encryption/Integrity algorithms ordered by preference in Security Mode command (R99). This CR was modified editorially in TD S3-020289 which was approved.

TD S3-020290 LS from RAN WG2 on Interpretation of UEA0. This LS was discussed and it was concluded that RAN WG2 were confused over the text for UEA0, which was a capability indicator. It was agreed that option b) was intended and a response LS stating that support of UEA0 is mandatory and that not starting ciphering is equivalent to ciphering with UEA0, was provided in TD S3-020291 which was modified in TD S3-020305 and approved.

TD S3-020203 Proposed CR to 33102-3b0: Optional use of Access Link Data Confidentiality. This CR was presented by Siemens and was approved.

TD S3-020204 Proposed CR to 33102-430: Optional use of Access Link Data Confidentiality. This CR was presented by Siemens and was approved.

TD S3-020297 Proposed CR to 33.102: Correction of USIM Toolkit (R99) (revision of TD S3-020254). This CR was approved.

TD S3-020298 Proposed CR to 33.102: Correction of USIM Toolkit (Rel-4) (revision of TD S3-020255). This CR was approved.

TD S3-020295 Proposed CR to 33.102: Clarification of seq number management (R99) (revision of TD S3-020252). This was presented by Vodafone. The formulation of the start conditions was in need of improvement. This was done off-line and the CR revised in TD S3-020308 which was approved.

TD S3-020296 Proposed CR to 33.102: Clarification of seq number management (Rel-4) (revision of TD S3-020253). The formulation of the start conditions was in need of improvement. This was done off-line and the CR revised in TD S3-020309 which was approved.

### 6.5 GERAN network access security

There were no specific contributions under this agenda item.

### 6.6 Immediate service termination (IST)

TD S3-020237 Handling of the access independent IST specifications. The advice received from the specifications manager was agreed. **The SA WG3 Chairman agreed to raise this at TSG SA for endorsement for changes to IST specification numbering.**

TD S3-020249 Application of IST feature to packet services. This was presented by Vodafone. The principles were endorsed and P. Howard was asked to create suitable CRs to cover these requirements.

### 6.7 Support for subscriber certificates 189 201

TD S3-020201 Proposed CR to 33102-430: Support for certificates. This Rel-6 CR was presented by Nokia. It was clarified that the Rel-5 version of 33.102 does not yet exist, so the CR was written to the latest Rel-4 version. There was a lengthy discussion over the document and many issues raised. It was decided not to approve the CR at this time, but to keep the document for further discussion and elaboration, without the need to create further CRs to Rel-6 to correct the proposal. V Niemi was asked to collate comments and it was decided to forward the document to SA WG2 for architectural comments and CN WG1 for information. A Liaison statement to SA WG2 and CN WG1 introduce the document was provided in TD S3-020299 which was modified and provided in TD S3-020322 which was approved. A draft CR for this was provided in TD S3-020300 and attached to the LS for information.

TD S3-020242 MAC verification service for cellular subscribers. This was presented by Nokia and some clarifications provided on the proposed mechanism. Delegates were asked to consider this further in relation to the considerations on certificates.

TD S3-020189 Role of UICC in secure PKI architectures. This was presented by GemPlus and proposed the requirements for support of a PKI infrastructure and a set of functions to achieve the requirements. After some discussion and clarification, it was decided that this contribution should be taken into account for use applications for digital signatures. The contribution was then noted.

### 6.8 Digital rights management (DRM) 220

A joint session with SA WG1 experts was held on the morning of 15 May 2002 to discuss DRM issues.

TD S3-020220 Proposed WID: DRM (Digital Right Management) Security. This was presented by Nokia. The WI Rapporteurship could be confirmed as stated, as this is a different issue to the editorship and ownership of specifications. The WID was discussed and updated in TD S3-020272 which was approved.

TD S3-020271 TS 22.xxx, Version 1.0.0: Digital Rights Management; Proposed Stage 1 (Release 6). SA WG1 presented their document (S1-020659), which contained the latest service description for DRM. The security aspects of the draft were discussed and clarified.

**AP 23/01: SA WG3 Chairman to initiate discussions with SA WG1 and SA WG2 Chairmen to debate the ownership of the DRM Work.**

### 6.9 WLAN

TD S3-020247 Some Consideration for WLAN Inter-working. This was presented by BT Group and detailed the different scenarios and charging and billing issues which will need to be considered from the security point of view. It was thought that a WID for WLAN interworking security issues would be needed and C. Blanchard agreed to create a proposal for this at the next SA WG3 meeting.

**AP 23/02: C. Blanchard to create a proposal for WLAN interworking at the next SA WG3 meeting**

### 6.10 Visibility and configurability of security

It was reported that an off-line e-mail discussion on progression of configurability work in SA WG3 did not show any resource for working on configurability (e.g. rejection of non-ciphered calls, etc.) although there was no request to remove the work item from the work plan. If any members are interested in progressing this work they were encouraged contribute to the SA WG3 meetings.

TD S3-020250 Proposed CR to 33.102: Ciphering indication (R99). This was introduced by Vodafone and clarifies the fat that the ciphering indicator is not optional. This CR was approved.

TD S3-020251 Proposed CR to 33.102: Ciphering indication (Rel-4). This CR was approved.

### 6.11 Push

TD S3-020236 Security review of Push Stage 1 specification (TS 22.174 v0.7.1). This was presented by Vodafone and provided the comments from P. Howard, no comments from other members had been received. The attached document 22.174 v071 with the comments was reviewed and discussed. The document was agreed to be sent to SA WG1 and an LS was created in TD S3-020301 with the commented TS attached, which was reviewed and found to need more time to correct the text. It was **agreed to approve this by e-mail after the meeting**. P. Howard agreed to run the e-mail approval and create a new version of the LS based on comments.

### 6.12 Priority

There were no specific contributions under this agenda item. L Valleris reported that no comments had been received over the e-mail list and comments were invited to TD S3-020084 (meeting #22, SA WG1 Priority Service feasibility study draft), particularly from companies supporting the Priority Service WI.

### 6.13 Location services (LCS)

A joint session with SA WG1 was held, where TD S3-020193 was reviewed. However SA WG1 were unable to comment on the SA WG3 statements and an LS was prepared to ask SA WG1 and SA WG2 formally about LCS issues of concern to SA WG3. These were provided in TD S3-020302 and TD S3-020303. TD S3-020302 was reviewed and it was considered in need of more consideration and **it was agreed to receive comments for a week and send for e-mail approval**. S. Schroeder agreed to run this activity.

TD S3-020303 These specifications were provided for information and noted. Members were invited to review the drafts.

### 6.14 User equipment functionality split (UEFS)

TD S3-020230 Network Handling of 'Badly Behaved' IMS Clients. This was presented by Nortel Networks and recommended that SA WG3 consider the threats posed by "badly behaved IMS clients" and how potential problems can be mitigated by recommending handling guidelines. It was proposed that these guidelines should be included as an informative annex to the UE functionality split document. There was not strong support to include this in TS 33.203 and delegates were asked to consider how such guidance can be made available to implementers for the next Release. An LS was created to SA WG1 providing the guidelines for information in TD S3-020304 which was discussed and modified in TD S3-020318 which was approved.

### 6.15 Open service architecture (OSA)

TD S3-020246 Status on OSA Security. This was presented by Alcatel and provided the current status of the ongoing discussions on OSA security. The issues and solutions were presented and the document noted. O. Paridaens agreed to monitor the outcome of the CN WG5 meeting this week with regards to these issues and report back to SA WG3.

### 6.16 Generic user profile (GUP)

TD S3-020197 Liaison Statement from SA WG2 on GUP work progress. The GUP group reported that they have completed their studies and SA WG2 recommended that WGs provide SA WG2 with input on GUP in the Rel-6 time frame and to provide comments on the attached documents to their next meeting (24-28 June 2002). B. Owen agreed to create a WID for GUP security and members were asked to send comments to B. Owen on this.

**AP 23/03: B Owen to create a WID for GUP Security. Members to send comments to him.**

### 6.17 Multimedia messaging

There were no specific contributions under this agenda item.

### 6.18 Presence

TD S3-020196 LS from SA WG2 on Presence Service. Members were asked to review the Presence stage 2 TR 23.841. A WID will be prepared by K. Boman for the Presence security work.

**AP 23/04: K. Boman to create a WID for Presence Security for distribution over e-mail. Supporting companies to in form K. Boman by e-mail. Members to review the SA WG2 draft TR 23.841.**

### 6.19 User equipment management (UEM)

A LS was reviewed at the previous meeting #22, TD S3-020013 which included presentation slides on the SyncML device management. No contribution had been made to this meeting. No response to the LS sent from the last meeting had been received. **P. Howard agreed to draft a WID for this.**

### 6.20 Multimedia Broadcast/Multicast Service (MBMS) 190, 191, 248

TD S3-020248 Report of the 3GPP MBMS Workshop. The report of the workshop was provided for information and was noted. A. Escott provided the draft stage 1 and stage 2 for MBMS in TD S3-020307 for information. MBMS-000020 "Access Security for Multicast Data" was provided to

the workshop and outlined some security work that is needed. Members were asked to review the drafts and the Workshop output and contribute to the next meeting.

### 6.21 User equipment management (UEM)

TD S3-020190 Proposed CR to 22.022: IMEI format for de-personalisation over the air - R99. This was presented by Orange France and was approved.

TD S3-020191 Proposed CR to 22.022: IMEI format for de-personalisation over the air - Rel-4. This CR was approved.

## 7 Review and update of work programme

There were no specific contributions under this agenda item.

## 8 Future meeting dates and venues

The planned meetings were as follows:

| Meeting | Date | Location | Host |
|---|---|---|---|
| S3#24 | 9 - 12 July 2002 | Helsinki, Finland | Nokia |
| S3#25 | 8 - 11 October 2002 | Munich, Germany | Siemens |
| S3#26 | 19 - 22 November 2002 | TO BE CONFIRMED | Host Required |
| | | | |
| | | | |

TSG Plenary meeting schedule

| | | | |
|---|---|---|---|
| TSG#16 | 4 –13 June | Marco Island, FL, USA | Motorola |
| TSG#17 | 3 – 12 September | Biarritz, France | Alcatel |
| TSG#18 | 3 – 12 December | USA | NA ‘Friends of 3GPP’ |
| **Meeting** | **2003** | **Location** | **Primary Host** |
| TSG#19 | EXACT DATES TO ADD March (tba) | UK | UK ‘Friends of 3GPP’ |
| TSG#20 | June (tba) | Finland | Nokia |
| TSG#21 | September (tba) | | |

## 9 Any other business

There was no other business.

## 10 Close of meeting

Mr. V. Niemi, the SA WG3 vice chairman, who chaired the meeting for the final day, thanked delegates for their hard work and fruitful co-operation in this meeting and thanked the hosts, AT&T Wireless and Rogers Wireless, for the arrangements. He then closed the meeting.

# Annex A: List of attendees at the SA WG3#23 meeting and Voting List

## A.1 List of attendees

| Name | Company | e-mail | 3GPP ORG | |
|---|---|---|---|---|
| Mr. Nigel Barnes | MOTOROLA Ltd | Nigel.Barnes@motorola.com | Member | GB |
| Mr. Colin Blanchard | BT Group Plc | colin.blanchard@bt.com | Member | GB |
| Mr. Marc Blommaert | SIEMENS ATEA NV | marc.blommaert@siemens.atea.be | Member | BE |
| Mr. Krister Boman | ERICSSON L.M. | krister.boman@erv.ericsson.se | Member | SE |
| Ms. Brye Bonner | Motorola Inc. | brye.bonner@motorola.com | Member | US |
| Mr. Charles Brookson | DTI | cbrookson@iee.org | Member | GB |
| Mr. Mauro Castagno | TELECOM ITALIA S.p.A. | mauro.castagno@tilab.com | Member | IT |
| Mr. Takeshi Chikazawa | Mitsubishi Electric Co. | chika@isl.melco.co.jp | Member | JP |
| Mr. Per Christoffersson | Telia | per.e.christoffersson@telia.se | Member | SE |
| Dr. Adrian Escott | Hutchison 3G UK Limited | adrian.escott@hutchison3G.com | Member | GB |
| Mr. Louis Finkelstein | Motorola Inc. | louisf@labs.mot.com | Member | US |
| Ms. Tao Haukka | NOKIA Corporation | tao.haukka@nokia.com | Member | FI |
| Mr. Guenther Horn | SIEMENS AG | guenther.horn@mchp.siemens.de | Member | DE |
| Mr. Peter Howard | VODAFONE Group Plc | peter.howard@vodafone.com | Member | GB |
| Mr. Kazuhiko Ishii | NTT DoCoMo Inc. | ishii@mml.yrp.nttdocomo.co.jp | Member | JP |
| Mr. Alexander Leadbeater | BT Group Plc | alex.leadbeater@bt.com | Member | GB |
| Mr. Luis Lopez Soria | Ericsson Inc. | luis.lopez-soria@ece.ericsson.se | Member | US |
| Mr. Michael Marcovici | Lucent Technologies | marcovici@lucent.com | Member | US |
| Mr. Sebastien Nguyen Ngoc | ORANGE FRANCE | sebastien.nguyenngoc@rd.francetelecom.com | Member | FR |
| Mr. Valtteri Niemi | NOKIA Corporation | valtteri.niemi@nokia.com | Member | FI |
| Mr. Petri Nyberg | SONERA Corporation | petri.nyberg@sonera.com | Member | FI |
| Mr. Bradley Owen | Lucent Technologies N. S. UK | bvowen@lucent.com | Member | GB |
| Mr. Olivier Paridaens | ALCATEL S.A. | Olivier.Paridaens@ALCATEL.BE | Member | FR |
| Miss Mireille PAULIAC | GEMPLUS Card International | mireille.pauliac@GEMPLUS.COM | Member | FR |
| Mr. Maurice Pope | ETSI Secretariat | maurice.pope@etsi.fr | Org_rep | FR |
| Mr. Greg Rose | QUALCOMM EUROPE S.A.R.L. | ggr@qualcomm.com | Member | FR |
| Ms. Stéphanie Salgado | SchlumbergerSema | salgado@montrouge.sema.slb.com | Member | FR |
| Mr. Stefan Schroeder | T-MOBILE DEUTSCHLAND | stefan.schroeder@t-mobile.de | Member | DE |
| Mr. DeWayne Sennett | AT&T Wireless Services, Inc. | dewayne.sennett@attws.com | Member | US |
| Mr. Benno Tietz | Vodafone D2 GmbH | benno.tietz@vodafone.de | Member | DE |
| Mr. Lee Valerius | Nortel Networks | valerius@nortelnetworks.com | Member | |
| Mr. Tommi Viitanen | NOKIA Corporation | tommi.viitanen@nokia.com | Member | FI |
| Ms. Monica Wifvesson | ERICSSON L.M. | monica.wifvesson@emp.ericsson.se | Member | SE |
| Mr. Berthold Wilhelm | BMWi | berthold.wilhelm@regtp.de | Member | DE |
| Mr. John Zimmer | Dansk MobilTelefon I/S | joz@sonofon.dk | Member | DK |

## A.2 SA WG3 Voting list

Based on the attendees lists for meetings #21, #22 and #23, the following companies are eligible to vote at SA WG3 meeting #24:

| 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 Group Plc | GB | 3GPPMEMBER | ETSI |
| Dansk MobilTelefon I/S | DK | 3GPPMEMBER | ETSI |
| DTI - Department of Trade and Industry | GB | 3GPPMEMBER | ETSI |
| Ericsson Incorporated | US | 3GPPMEMBER | T1 |
| Telefon AB LM Ericsson | SE | 3GPPMEMBER | ETSI |
| GEMPLUS Card International | FR | 3GPPMEMBER | ETSI |
| Hutchison 3G UK Limited | GB | 3GPPMEMBER | ETSI |
| Lucent Technologies | US | 3GPPMEMBER | T1 |
| Lucent Technologies Network Systems UK | GB | 3GPPMEMBER | ETSI |
| Mitsubishi Electric Co. | JP | 3GPPMEMBER | ARIB |
| Motorola Inc. | US | 3GPPMEMBER | T1 |
| MOTOROLA Ltd | GB | 3GPPMEMBER | ETSI |
| NOKIA Corporation | FI | 3GPPMEMBER | ETSI |
| NTT DoCoMo Inc. | JP | 3GPPMEMBER | ARIB |
| ORANGE FRANCE | FR | 3GPPMEMBER | ETSI |
| QUALCOMM EUROPE S.A.R.L. | FR | 3GPPMEMBER | ETSI |
| SchlumbergerSema - Schlumberger Systèmes S.A | FR | 3GPPMEMBER | ETSI |
| SIEMENS AG | DE | 3GPPMEMBER | ETSI |
| SIEMENS ATEA NV | BE | 3GPPMEMBER | ETSI |
| SONERA Corporation | FI | 3GPPMEMBER | ETSI |
| T-MOBILE DEUTSCHLAND | DE | 3GPPMEMBER | ETSI |
| TELECOM ITALIA S.p.A. | IT | 3GPPMEMBER | ETSI |
| Vodafone D2 GmbH | DE | 3GPPMEMBER | ETSI |
| VODAFONE Group Plc | GB | 3GPPMEMBER | ETSI |

## Annex B: List of documents

| TD number | Title | Source | Agenda | Document for | Replaced by | Status / Comment |
|---|---|---|---|---|---|---|
| S3-020168 | Draft agenda for meeting #23 | SA WG3 Chairman | 2 | Approval | | Approved with minor changes (see report for new structure) |
| S3-020169 | Draft report of SA WG3 meeting #22 | SA WG3 Secretary | 4.1 | Approval | S3-020259 | Modified in TD259 and approved |
| S3-020170 | Report of SA WG3 22bis ad-hoc meeting, Fort Lauderdale, Florida | Ad-hoc Secretary | 4.2 | Approval | S3-020261 | Modified in TD261 and approved |
| S3-020171 | SA3 Status Report to SA#15 | SA WG3 Chairman | 5.1 | Information | | Noted |
| S3-020172 | Report to SA3 on SA#15 | SA WG3 Chairman | 5.1 | Information | | Noted |
| S3-020173 | Response from GERAN WG2 to "Response Liaison Statement on Trace and Availability of IMSI and IMEI" | GERAN WG2 | 5.5 | Information | | Noted |
| S3-020174 | Reply Liaison Statement from CN WG1 on 'Issues with SA handling at P-CSCF' | CN WG1 | 5.2.1 | Action | | Noted |
| S3-020175 | Liaison Statement from CN WG3 on "IPv6 update of stage 3 specifications" | CN WG3 | 5.2.2 | Information | | Noted |
| S3-020176 | Liaison Statement from CN WG4 on Immediate Service Termination | CN WG4 | 5.2.3 | Action | | Response in S3-020266 |
| S3-020177 | Response from RAN WG2 to LS (N4-020302) on Trace and Availability of IMSI and IMEI | RAN WG2 | 5.3 | Information | | Noted |
| S3-020178 | LS from RAN WG2 on Group release security solution | RAN WG2 | 5.3 | Action | | Response in S3-020267 |
| S3-020179 | Liaison Statement Reply from SA WG2 to "Status of the Generic User Profile Work" | SA WG2 | 5.1.2 | Information | | Noted |
| S3-020180 | Liaison Statement Reply from SA WG2 to "Comments on UP-010141 and relationship of GUP to Subscription Management" | SA WG2 | 5.1.2 | Information | | Noted |
| S3-020181 | Liaison Statement from SA WG2 on "Prefix allocation for IPv6 stateless address autoconfiguration" | SA WG2 | 5.1.2 | Action | | Noted |
| S3-020182 | LS reply from SA WG5 on: "3GPP System – WLAN Interworking" | SA WG5 | 5.1.3 | Information | | Noted |
| S3-020183 | LS reply from SA WG5 on: Priority Service Feasibility Study - draft TR 22.950 v1.0.0 | SA WG5 | 5.1.3 | Information | | Noted |
| S3-020184 | Reply to LS on "IP version inter-working on the transport plane" from SA2 (S2-020291) | SA WG5 | 5.1.3 | Information | | Noted |
| S3-020185 | Reply LS from SA WG5 on "support for subscriber certificates" from SA3 (S3-020163) | SA WG5 | 5.1.3 | Information | | Noted |
| S3-020186 | Liaison Statement from SA WG5 on co-ordination of data definitions, identified in GUP development | SA WG5 | 5.1.3 | Discussion | | Noted |
| S3-020187 | Proposed CR to 33.210-500: Strengthening the requirements on IV construction to prevent attacks based on predictable IV | Qualcomm/Telenor | 6.2 | Approval | S3-020277 | Updated in TD 277 |
| S3-020188 | Proposed CR to 33.210-500: Removal of reference to Internet draft draft-ietf-ipsec-sctp-03.txt | Ericsson/Telenor | 6.2 | Approval | | Pronciple of CR proposals accepted. CR to include internet draft text into specification as an annex to be provided at next SA WG3 meeting |
| S3-020189 | Role of UICC in secure PKI architectures | Gemplus Card International, Oberthur Card Systems | 6.7 | Discussion | | Noted. To be taken into account for application work for digital signatures |
| S3-020190 | Proposed CR to 22.022: IMEI format for de-personalisation over the air - R99 | Orange France, Gemplus | 6.21 | Approval | | Approved |
| S3-020191 | Proposed CR to 22.022: IMEI format for de-personalisation over the air - Rel-4 | Orange France, Gemplus | 6.21 | Approval | | Approved |

| TD number | Title | Source | Agenda | Document for | Replaced by | Status / Comment |
|---|---|---|---|---|---|---|
| S3-020192 | LS from ETSI TC SEC-LI: Future structuring of documents across the LI standardisation community | ETSI TC SEC-LI | 4.3 | Discussion / Decision | | Noted |
| S3-020193 | Response LS from SA WG1 to SA3 on new security requirements for LCS | SA WG1 | 5.1.1 | Action | | Review of TS to be considered in joint session on LCS with Sa wg1. LSs in TDs 302 and 303 |
| S3-020194 | SA1 Assumptions on IMS identities and UICCs | SA WG1 | 5.1.1 | Information | | Noted |
| S3-020195 | LS back to SA1and SA3 on enhanced user privacy and new security requirements for LCS | SA WG2 | 5.1.2 | Information | | Noted |
| S3-020196 | LS from SA WG2 on Presence Service | SA WG2 | 5.1.2 | Action | | K. Boman to create WID for e-mail distribution |
| S3-020197 | Liaison Statement from SA WG2 on GUP work progress | SA WG2 | 5.1.2 | Action | | B Owen to create WID on GUP Security. Comments to him. |
| S3-020198 | Response to the LS on "IPv6 update of stage 3 specifications" | SA WG2 | 5.1.2 | Information | | Noted |
| S3-020199 | LS from SA WG2 on IMS Identities for Rel 99/R4 UICC (response to S3-020167) | SA WG2 | 5.1.2 | Action | | Response in TD312 |
| S3-020200 | Request to expedite 33.108 v 1.0.x | SA WG3 LI group | 4.3 | Action | | |
| S3-020201 | Proposed CR to 33102-430: Support for certificates (Rel-6) | Nokia | 6.7 | Approval | | Not approved, but to be further elaborated using this as a basis. LSs provided in TDs 299 and 300 |
| S3-020202 | Proposed CR to 33203-510: Reference of HTTP Digest AKA in TS 33.203 | Nokia | 6.1 | Approval | S3-020218 | CR References DRAFT IETF RFC |
| S3-020203 | Proposed CR to 33102-3b0: Optional use of Access Link Data Confidentiality | Siemens | 6.4 | Approval | | Approved |
| S3-020204 | Proposed CR to 33102-430: Optional use of Access Link Data Confidentiality | Siemens | 6.4 | Approval | | Approved |
| S3-020205 | Comment on R2 Group Release Security Solution | Qualcomm | 5.3 | Discussion | | Discussed with TD178: Response LS in TD267 |
| S3-020206 | Group Release Security Solution Analysis (S3-020178) | Siemens | 5.3 | Discussion | | Discussed with TD178: Response LS in TD267 |
| S3-020207 | Proposed CR to 33.203-510: Clean-up of section 6.1.1 | Hutchison 3G UK | 6.1 | Approval | S3-020286 | Updated in TD286 |
| S3-020208 | Proposed CR to 33.203-510: Correction to S-CSCF behaviour on Network Authentication Failure | Hutchison 3G UK | 6.1 | Approval | S3-020283 | Updated in TD283 |
| S3-020209 | Proposed CR to 33.203-510: Update of SA handling procedures | Hutchison 3G UK | 6.1 | Approval | S3-020292 | Changes text modified in TD268. Reformulated and incorporated with principles of TD268. |
| S3-020210 | Proposed CR to 33.203-510: Update of User Authentication Failure | Hutchison 3G UK | 6.1 | Approval | S3-020284 | Updated in TD 284 |
| S3-020211 | New SAs and incomplete authentications | Hutchison 3G UK | 6.1 | Discussion / Decision | | Att3 and att4 reproduced in TDs 293 and 294. Att5 highlights included in TD292 |
| S3-020212 | Proposed CR to 33.203-510: Correcting the network behaviour in response to an incorrect AUT-S | Hutchison 3G UK | 6.1 | Approval | S3-020282 | 33203CRxxx (incorrect spec no on contribution). Updated in TD282 |
| S3-020213 | Deriving unidirectional keys for IPSec protection of SIP messages between UA and P-CSCF | SSH Communications Security Corp | 6.1 | Discussion | | Covered by TD235/ TD275 |

| TD number | Title | Source | Agenda | Document for | Replaced by | Status / Comment |
|---|---|---|---|---|---|---|
| S3-020214 | Usage of PF_KEY API in IPSec/ESP Parameter Handling for SIP Integrity | SSH Communications Security Corp | 6.1 | Discussion | | Noted |
| S3-020215 | IPSec Security Indicator | SSH Communications Security Corp | 6.1 | Discussion | | Noted |
| S3-020216 | Proposed WID: Network Domain Security; Authentication Framework (NDS/AF) | Telenor | 6.2 | Approval | S3-020278 | Study clarified in TD 278 |
| S3-020217 | IETF Status Report for Security Mechanism Agreement | Ericsson | 6.1 | Information | | |
| S3-020218 | Reference of HTTP Digest AKA in TS 33.203 | Nokia | 6.1 | Approval | S3-020281 | Rev of S3-020202. CR References DRAFT IETF RFC. Revised in TD281 |
| S3-020219 | Digest AKA status in IETF | Nokia | 5.6 | Information | | Noted |
| S3-020220 | Proposed WID: DRM (Digital Right Management) Security | Nokia | 6.8 | Approval | S3-020272 | Discussed and updated in TD 272 |
| S3-020221 | Proposed CR to 33.203-510: Removal of 2 separate Key derivation functions | Ericsson | 6.1 | Approval | | Covered by TD235/ TD275 |
| S3-020222 | Proposed CR to 33.203-510: Handling the lifetime of an SA | Ericsson | 6.1 | Approval | | Covered by TD235/ TD275 |
| S3-020223 | The use of SHA-1 in IMS and IPSec ESP | Ericsson | 6.1 | Discussion / Decision | | Proposed CR attached (33203-510): Covered by TD235/ TD275 |
| S3-020224 | Proposed CR to 33.203-510: Remove Annexes that describes Extended HTTP Digest solution | Ericsson | 6.1 | Approval | | Approved |
| S3-020225 | Proposed CR to 33.203-510: Handling of expiry time and the lifetime of an SA | Ericsson | 6.1 | Approval | | Covered by TD235/ TD275 |
| S3-020226 | ISIM related issues | Ericsson | 6.1 | Discussion / Decision | | Proposed CR attached (33203-510) |
| S3-020227 | Proposed CR to 33.203-510: Clarifications to various issues in TS 33.203 | Ericsson | 6.1 | Approval | | Changes included in updated TD275 |
| S3-020228 | Proposed CR to 33.203-510: Removal of encryption between UE and P-CSCF as optional feature in Rel-5 | Ericsson | 6.1 | Approval | | 33203CR015. Changes included in updated TD275 |
| S3-020229 | Proposed CR to 33.210-500: NDS/IP Confidentiality protection for IMS session keys | Ericsson | 6.2 | Approval | | Approved |
| S3-020230 | Network Handling of 'Badly Behaved' IMS Clients | Nortel Networks | 6.14 | Discussion / Decision | | Could be useful as a guidelines annex to 33.203 but not supported for Rel-5.To be considered for Rel-6 |
| S3-020231 | Incoming SIP messages at the unprotected port at the UE and integrity check failures in the UE | Ericsson | 6.1 | Discussion | | Covered by TD235/ TD275 |
| S3-020232 | Proposed CR to 33.203-510: Integrity check failure in the UE | Ericsson | 6.1 | Approval | | Spirit of CR to be included in TD275 |
| S3-020233 | Proposed CR to 33.203-510: Incoming unprotected SIP messages at the UE | Ericsson | 6.1 | Approval | | Withdrawn - covered by TD235/ TD275 |
| S3-020234 | Justification for proposed changes to text on SIP integrity in TS 33.203 v510 | Siemens | 6.1 | Discussion | | Used to explain proposed CR in S3-020235 |
| S3-020235 | Proposed CR to 33.203-510: Requested Changes for SIP integrity | Siemens | 6.1 | Approval | S3-020275 | Clarified and reformatted to CR format in S3-020275 |
| S3-020236 | Security review of Push Stage 1 specification (TS 22.174 v0.7.1) | Vodafone | 6.11 | Discussion / Approval | | To be sent to SA WG1 in TD301 |
| S3-020237 | Handling of the access independent IST specifications (AP 22/7) | SA WG3 Secretary | 6.6 | Action | | Chairman to raise IST numbering at TSG SA |

| TD number | Title | Source | Agenda | Document for | Replaced by | Status / Comment |
|---|---|---|---|---|---|---|
| S3-020238 | Test data for MILENAGE algorithm | ETSI SAGE | 5.7 | Information | | SAGE asked to analyse proposal for additional test sets |
| S3-020239 | Security negotiation procedure for Ipsec | Nokia | 6.1 | Discussion / Approval | | Withdrawn |
| S3-020240 | Proposed CR to 33.203: IP address as SA selector | Nokia | 6.1 | Approval | S3-020270 | Updated in TD 270 |
| S3-020241 | Proposed CR to 33.203: Accepting unprotected messages at the P-CSCF | Nokia | 6.1 | Approval | | Included in TD275 |
| S3-020242 | MAC verification service for cellular subscribers | Nokia | 6.7 | Discussion | | Noted. Consider with certificate work. |
| S3-020243 | draft-ietf-sip-sec-agree-01.txt | Ericsson | 6.1 | Information | | Noted. Delegates asked to study the document |
| S3-020244 | The use of IPv6 addressing privacy within IMS | Ericsson | 6.1 | Discussion | | Agreed as a working solution |
| S3-020245 | Proposal for CR to 33.203 (based on discussion doc S3-020244) | Ericsson | 6.1 | Approval | S3-020268 | Reformulated and converted to CR format in TD 268 |
| S3-020246 | Status on OSA Security | Alcatel | 6.15 | Discussion | | Noted. O Paridaens to monitor outcome of CN WG5 meeting this week |
| S3-020247 | Some Consideration for WLAN Inter-working | BT Group | 6.9 | Discussion | | C Blanchard to create WID proposal for next meeting |
| S3-020248 | Report of the 3GPP MBMS Workshop | WS Secretary | 6.20 | Information | | Report noted. Stage 1 and 2 drafts provided in TD307. Contributions to next meeting requested. |
| S3-020249 | Application of IST feature to packet services | Vodafone | 6.6 | Discussion | | Agreed. P Howard to create CRs |
| S3-020250 | Proposed CR to 33.102: Ciphering indication (R99) | Vodafone | 6.10 | Approval | | Approved |
| S3-020251 | Proposed CR to 33.102: Ciphering indication (Rel-4) | Vodafone | 6.10 | Approval | | Approved |
| S3-020252 | Proposed CR to 33.102: Clarification of seq number management | Vodafone | 6.4 | Approval | S3-020295 | Revised in TD295 |
| S3-020253 | Proposed CR to 33.102: Clarification of seq number management | Vodafone | 6.4 | Approval | S3-020296 | Revised in TD296 |
| S3-020254 | Proposed CR to 33.102: Correction of USIM Toolkit | Vodafone | 6.4 | Approval | S3-020297 | Ref 16 to be updated too |
| S3-020255 | Proposed CR to 33.102: Correction of USIM Toolkit | Vodafone | 6.4 | Approval | S3-020298 | Vsn corrected on cover sheet |
| S3-020256 | CR to 33.107: Addition of SMS type information | LI group | 4.3 | Approval | S3-020263 | Updated in TD263 |
| S3-020257 | CR to 33.107: Changes to 33.107 to support interception at a GGSN | LI group | 4.3 | Approval | | Approved |
| S3-020258 | CR to 33.107: Inclusion of Serving System IRI in TS 33.107 | LI group | 4.3 | Approval | S3-020264 | Updated in TD 264 |
| S3-020259 | Approved report of meeting 23 | SA WG3 Secretary | 4.1 | Information | | Approved vsn 1.0.0 |
| S3-020260 | Results from recent IETF coordination meeting | S Hayes | 5.6 | Information | | Noted |
| S3-020261 | Approved report of meeting 22bis | V Niemi | 4.2 | Information | | Approved |
| S3-020262 | Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #2/02 on lawful interception - Orlando, Florida | SA WG3 LI group | 4.3 | Information | | Noted |
| S3-020263 | CR to 33.107: Addition of SMS type information | LI group | 4.3 | Approval | | Approved |
| S3-020264 | CR to 33.107: Inclusion of Serving System IRI in TS 33.107 | LI group | 4.3 | Approval | S3-020310 | Upodated in TD310 |

| TD number | Title | Source | Agenda | Document for | Replaced by | Status / Comment |
|---|---|---|---|---|---|---|
| S3-020265 | Report of the 3GPP MBMS Workshop (WITHDRAWN) | MBMS WS Secretary | 6.20 | Information | | WITHDRAWN (same as S3-020248) |
| S3-020266 | Response to S3-020176 (LS N4-020372 on Immediate Service Termination from CN4). | SA WG3 | 5.2.3 | Approval | | |
| S3-020267 | Reply LS on Group release security solution (Response to S3-020178) | SA WG3 | 5.3 | Approval | S3-020287 | Modified in TD287 |
| S3-020268 | CR to 33.203 (based on discussion of docs S3-020244 and S3-020245) | Ericsson | 6.1 | Approval | | Superseded by TD311 |
| S3-020269 | LS to SA WG2 / CN WG1 on change of IP address in IMS (K Boman) | SA WG3 | 6.1 | Approval | | WITHDRAWN |
| S3-020270 | Proposed CR to 33.203: IP address as SA selector | Nokia | 6.1 | Approval | | This method and other methods to be considered for parameter mapping choice. |
| S3-020271 | TS 22.xxx, Version 1.0.0: Digital Rights Management; Proposed Stage 1 (Release 6) | SA WG1 | 6.8 | Information | | presented in joint session |
| S3-020272 | Proposed WID: DRM (Digital Right Management) Security | Nokia | 6.8 | Approval | | Approved |
| S3-020273 | Notes from IMS Drafting Session | K Boman, Ericsson | 6.1 | Presentation | | Presented |
| S3-020274 | LS to SAGE: Reply LS on key expansion for HMAC-SHA-1-96 | SA WG3 | 6.1 | Approval | S3-020315 | Updated in TD315 |
| S3-020275 | Proposed CR to 33.203-510: Requested Changes for SIP integrity | Siemens et al | 6.1 | Approval | S3-020317 | Updated in TD317 |
| S3-020276 | UK Mobile Telephones reprogramming Bill | DTI | | Information | | Noted |
| S3-020277 | Proposed CR to 33.210-500: Strengthening the requirements on IV construction to prevent attacks based on predictable IV | Qualcomm/Telenor | 6.2 | Approval | | Approved |
| S3-020278 | Proposed WID: Network Domain Security; Authentication Framework (NDS/AF) | Telenor | 6.2 | Approval | S3-020321 | Final version in TD321 |
| S3-020279 | Proposed CR to 33.102: Encryption/Integrity algorithms ordered by preference in Security Mode command (R99) | Ericsson, Vodafone | 6.4 | Approval | S3-020288 | Updated in TD288 |
| S3-020280 | Proposed CR to 33.102: Encryption/Integrity algorithms ordered by preference in Security Mode command (R99) | Ericsson, Vodafone | 6.4 | Approval | S3-020289 | Updated in TD289 |
| S3-020281 | Reference of HTTP Digest AKA in TS 33.203 | Nokia | 6.1 | Approval | | Approved |
| S3-020282 | Proposed CR to 33.203-510: Correcting the network behaviour in response to an incorrect AUT-S | Hutchison 3G UK | 6.1 | Approval | | Postponed for further discussion at next meeting |
| S3-020283 | Proposed CR to 33.203-510: Correction to S-CSCF behaviour on Network Authentication Failure | Hutchison 3G UK | 6.1 | Approval | | Postponed for further discussion at next meeting |
| S3-020284 | Proposed CR to 33.203-510: Update of User Authentication Failure | Hutchison 3G UK | 6.1 | Approval | | Postponed for further discussion at next meeting |
| S3-020285 | Liaison Statement to T WG3 on ISIM parameters | SA WG3 | 6.1 | Approval | S3-020314 | Updated in TD314 |
| S3-020286 | Proposed CR to 33.203-510: Clean-up of section 6.1.1 | Hutchison 3G UK | 6.1 | Approval | | Approved |
| S3-020287 | Reply LS on Group release security solution (Response to S3-020178) | SA WG3 | 5.3 | Approval | | Approved |
| S3-020288 | Proposed CR to 33.102: Encryption/Integrity algorithms ordered by preference in Security Mode command (R99) | Ericsson, Vodafone | 6.4 | Approval | | Approved |
| S3-020289 | Proposed CR to 33.102: Encryption/Integrity algorithms ordered by preference in Security Mode command (Rel-4) | Ericsson, Vodafone | 6.4 | Approval | | Approved |
| S3-020290 | LS from RAN WG2 on Interpretation of UEA0 | RAN WG2 | 6.4 | Action | | Response in TD291 |
| S3-020291 | Reply LS on Interpretation of UEA0 (R2-020390) | SA WG3 | 6.4 | Approval | S3-020305 | Revised in TD305 |

| TD number | Title | Source | Agenda | Document for | Replaced by | Status / Comment |
|---|---|---|---|---|---|---|
| S3-020292 | Proposed CR to 33.203-510: Update of SA handling procedures | Hutchison 3G UK | 6.1 | Approval | | WITHDRAWN |
| S3-020293 | CR to 33.203-510: Integrity protection indicator (Rel-5) | Hutchison 3G UK | 6.1 | Approval | | Approved |
| S3-020294 | CR to 33.203-510: UE and P-CSCF Behaviour on an Incomplete Authentication (Rel-5) | Hutchison 3G UK | 6.1 | Approval | | Approved |
| S3-020295 | Proposed CR to 33.102: Clarification of seq number management (R99) | Vodafone | 6.4 | Approval | S3-020308 | reformulated in TD308 |
| S3-020296 | Proposed CR to 33.102: Clarification of seq number management (Rel-4) | Vodafone | 6.4 | Approval | S3-020309 | reformulated in TD309 |
| S3-020297 | Proposed CR to 33.102: Correction of USIM Toolkit (R99) | Vodafone | 6.4 | Approval | | Approved. Ref 16 also to be updated |
| S3-020298 | Proposed CR to 33.102: Correction of USIM Toolkit (Rel-4) | Vodafone | 6.4 | Approval | | Approved. |
| S3-020299 | LS to SA WG2/CN WG1 (V Niemi) | SA WG3 | 6.7 | Approval | S3-020322 | |
| S3-020300 | LS to SA WG1 (V Niemi) | SA WG3 | 6.7 | Information | | Attached to LS in TD322 |
| S3-020301 | LS to SA WG1 - Reply LS on Push Security (S1-020541) | SA WG3 | 6.11 | Approval | | To be updated and approved by e-mail after meeting (P Howard) |
| S3-020302 | Response LS to SA1 and SA2 on security and enhanced user privacy requirements for LCS (S1-020860 and S2-021466) | SA WG3 | 6.13 | Approval | | S. Schroeder to gather comments and perform e-mail approval after meeting. |
| S3-020303 | Specifications for information / review | | 6.13 | Information | | Noted. For review by interested members |
| S3-020304 | LS to SA WG1 on Network Handling of 'Badly Behaved' Software IMS Clients (reply to S1-010030) | SA WG3 | 6.13 | Approval | S3-020318 | Updated in TD318 |
| S3-020305 | Reply LS on Interpretation of UEA0 (R2-020390) | SA WG3 | 6.4 | Approval | | Approved |
| S3-020306 | Draft LS to CN WG1: Secure registration of IP addresses | Siemens | 6.1 | Approval | S3-020316 | Updated in TD316 |
| S3-020307 | A Escott MBMS Draft stage 1 and stage 2 | Hutchison 3G UK | 6.20 | Information | | Noted |
| S3-020308 | Proposed CR to 33.102: Clarification of seq number management (R99) | Vodafone | 6.4 | Approval | | Approved |
| S3-020309 | Proposed CR to 33.102: Clarification of seq number management (Rel-4) | Vodafone | 6.4 | Approval | | Approved |
| S3-020310 | CR to 33.107: Inclusion of Serving System IRI in TS 33.107 | LI group | 4.3 | Approval | | Approved |
| S3-020311 | Proposed CR to 33.203-510: Security association handling in IMS when the UE changes IP address | Siemens | 6.1 | Approval | S3-020320 | Updated in TD320 |
| S3-020312 | Reply LS to SA WG2 on IMS identities for Rel 99/R4 UICC (S2-021526) | SA WG3 | 5.1.2 | Approval | | Approved |
| S3-020313 | Response to S3-020176 (LS N4-020372 on Immediate Service Termination from CN4). | SA WG3 | 5.2.3 | Approval | | Approved |
| S3-020314 | Liaison Statement to T WG3 on ISIM parameters | SA WG3 | 6.1 | Approval | | Approved |
| S3-020315 | LS to SAGE: Reply LS on key expansion for HMAC-SHA-1-96 | SA WG3 | 6.1 | Approval | | Approved |
| S3-020316 | LS to CN WG1: Secure registration of IP addresses | SA WG3 | 6.1 | Approval | | Approved |
| S3-020317 | CR to 33.203-510: Requested Changes for SIP integrity | Siemens et al | 6.1 | Approval | | Approved |
| S3-020318 | LS to SA WG1 on Network Handling of 'Badly Behaved' Software IMS Clients (reply to S1-010030) | SA WG3 | 6.13 | Approval | | Approved |
| S3-020319 | Editorial CR to 33.203: Clean-up of 7.3 | Hutchison 3G UK | 6.1 | Approval | | Approved |

| TD number | Title | Source | Agenda | Document for | Replaced by | Status / Comment |
|---|---|---|---|---|---|---|
| S3-020320 | Proposed CR to 33.203-510: Security association handling in IMS when the UE changes IP address | Siemens | 6.1 | Approval | | Approved |
| S3-020321 | Proposed WID: Network Domain Security; Authentication Framework (NDS/AF) | Telenor | 6.2 | Approval | | Approved |
| S3-020322 | LS to SA WG2/CN WG1 (V Niemi) | SA WG3 | 6.7 | Approval | | Approved (attach TD S3-020077 and S3-020300) |

## Annex C: Status of specifications under SA WG3 responsibility

| 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 (LI); Stage 1 | MCKIBBEN, Bernie | R98 |
| TS | 02.33 | 8.0.1 | Lawful Interception (LI); Stage 1 | MCKIBBEN, Bernie | R99 |
| TS | 03.20 | 3.3.2 | Security-related Network Functions | NGUYEN NGOC, Sebastien | Ph1 |
| TS | 03.20 | 3.0.0 | Security-related Network Functions | NGUYEN NGOC, Sebastien | Ph1-EXT |
| TS | 03.20 | 4.4.1 | Security-related Network Functions | NGUYEN NGOC, Sebastien | Ph2 |
| TS | 03.20 | 5.2.1 | Security-related Network Functions | NGUYEN NGOC, Sebastien | R96 |
| TS | 03.20 | 6.1.0 | Security-related Network Functions | NGUYEN NGOC, Sebastien | R97 |
| TS | 03.20 | 7.2.0 | Security-related Network Functions | NGUYEN NGOC, Sebastien | R98 |
| TS | 03.20 | 8.1.0 | Security-related Network Functions | NGUYEN NGOC, Sebastien | R99 |
| TS | 03.31 | 7.0.0 | Fraud Information Gathering System (FIGS); Service description; Stage 2 | WRIGHT, Tim | R98 |
| TS | 03.31 | 8.0.0 | Fraud Information Gathering System (FIGS); Service description; Stage 2 | WRIGHT, Tim | R99 |
| TS | 03.33 | 7.2.0 | Lawful Interception; Stage 2 | MCKIBBEN, Bernie | R98 |
| TS | 03.33 | 8.1.0 | Lawful Interception; Stage 2 | MCKIBBEN, Bernie | R99 |
| TS | 03.35 | 7.0.1 | Immediate Service Termination (IST); Stage 2 | WRIGHT, Tim | R98 |
| TS | 03.35 | 8.1.0 | Immediate Service Termination (IST); Stage 2 | WRIGHT, Tim | R99 |
| TS | 21.133 | 3.2.0 | 3G security; Security threats and requirements | CHRISTOFFERSSON, Per | R99 |
| TS | 21.133 | 4.1.0 | 3G security; 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 | 3.11.0 | 3G security; Security architecture | BLOMMAERT, Marc | R99 |
| TS | 33.102 | 4.3.0 | 3G security; Security architecture | BLOMMAERT, Marc | Rel-4 |
| TS | 33.102 | none | 3G security; Security architecture | BLOMMAERT, Marc | Rel-5 |
| 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 | 3.5.0 | 3G security; Lawful interception architecture and functions | WILHELM, Berthold | R99 |
| TS | 33.107 | 4.3.0 | 3G security; Lawful interception architecture and functions | WILHELM, Berthold | Rel-4 |
| TS | 33.107 | 5.2.0 | 3G security; Lawful interception architecture and functions | WILHELM, Berthold | Rel-5 |
| TS | 33.108 | 1.0.0 | 3G security; Handover interface for Lawful Interception | 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 | 4.3.0 | Network Domain Security - MAP | ESCOTT, Adrian | Rel-4 |
| TS | 33.200 | 5.0.0 | Network Domain Security - MAP | ESCOTT, Adrian | Rel-5 |
| TS | 33.201 | none | Access domain security | POPE, Maurice | Rel-5 |
| TS | 33.203 | 5.1.0 | 3G security; Access security for IP-based services | BOMAN, Krister | Rel-5 |
| TS | 33.210 | 5.0.0 | 3G security; Network Domain Security (NDS); IP network layer security | 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 | ESCOTT, Adrian | 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 | 3.2.0 | Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications | WALKER, Michael | R99 |
| TS | 35.201 | 4.1.0 | Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications | WALKER, Michael | Rel-4 |
| TS | 35.201 | none | Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications | WALKER, Michael | Rel-5 |
| 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 | 35.202 | none | Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification | WALKER, Michael | Rel-5 |
| 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 | 35.203 | none | Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data | WALKER, Michael | Rel-5 |
| 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 |
| TS | 35.204 | none | Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data | WALKER, Michael | Rel-5 |
| 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 |
| TR | 35.205 | none | 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-5 |
| 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 | 35.206 | none | 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-5 |
| 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 | 35.207 | none | 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-5 |
| 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 |
| TS | 35.208 | none | 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-5 |
| 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 | 35.909 | none | 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-5 |
| TR | 41.031 | 4.0.1 | Fraud Information Gathering System (FIGS); Service requirements; Stage 0 | WRIGHT, Tim | Rel-4 |
| TR | 41.031 | none | Fraud Information Gathering System (FIGS); Service requirements; Stage 0 | WRIGHT, Tim | Rel-5 |
| TR | 41.033 | 4.0.1 | Lawful Interception requirements for GSM | MCKIBBEN, Bernie | Rel-4 |
| TR | 41.033 | none | Lawful Interception requirements for GSM | MCKIBBEN, Bernie | Rel-5 |
| 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 | 42.031 | none | Fraud Information Gathering System (FIGS); Service description; Stage 1 | WRIGHT, Tim | Rel-5 |
| TS | 42.032 | 4.0.0 | Immediate Service Termination (IST); Service description; Stage 1 | WRIGHT, Tim | Rel-4 |
| TS | 42.032 | none | Immediate Service Termination (IST); Service description; Stage 1 | WRIGHT, Tim | Rel-5 |
| TS | 42.033 | 4.0.0 | Lawful Interception; Stage 1 | MCKIBBEN, Bernie | Rel-4 |
| TS | 42.033 | none | Lawful Interception; Stage 1 | MCKIBBEN, Bernie | Rel-5 |
| 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 | 43.031 | none | Fraud Information Gathering System (FIGS); Service description; Stage 2 | WRIGHT, Tim | Rel-5 |
| TS | 43.033 | 4.0.0 | Lawful Interception; Stage 2 | MCKIBBEN, Bernie | Rel-4 |
| TS | 43.033 | none | Lawful Interception; Stage 2 | MCKIBBEN, Bernie | Rel-5 |
| TS | 43.035 | 4.1.0 | Immediate Service Termination (IST); Stage 2 | WRIGHT, Tim | Rel-4 |
| TS | 43.035 | none | Immediate Service Termination (IST); Stage 2 | WRIGHT, Tim | Rel-5 |

## 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 |
|---|---|---|---|---|---|---|---|---|---|
| 22.022 | 003 | | R99 | IMEI format for de-personalisation over the air | F | 3.1.0 | S3-23 | S3-020190 | agreed |
| 22.022 | 004 | | Rel-4 | IMEI format for de-personalisation over the air | A | 4.0.0 | S3-23 | S3-020191 | agreed |
| 33.102 | 165 | | R99 | Optional use of Access Link Data Confidentiality | F | 3.11.0 | S3-23 | S3-020203 | agreed |
| 33.102 | 166 | | Rel-4 | Optional use of Access Link Data Confidentiality | A | 4.3.0 | S3-23 | S3-020204 | agreed |
| 33.102 | 167 | | R99 | Clarification of ciphering indicator | F | 3.11.0 | S3-23 | S3-020250 | agreed |
| 33.102 | 168 | | Rel-4 | Clarification of ciphering indicator | A | 4.3.0 | S3-23 | S3-020251 | agreed |
| 33.102 | 169 | | R99 | Encryption/Integrity algorithms ordered by preference in Security Mode command | F | 3.11.0 | S3-23 | S3-020288 | agreed |
| 33.102 | 170 | | Rel-4 | Encryption/Integrity algorithms ordered by preference in Security Mode command | A | 4.3.0 | S3-23 | S3-020289 | agreed |
| 33.102 | 171 | | R99 | Correction of (U)SIM toolkit security reference | F | 3.11.0 | S3-23 | S3-020297 | agreed |
| 33.102 | 172 | | Rel-4 | Encryption/Integrity algorithms ordered by preference in Security Mode command | A | 4.3.0 | S3-23 | S3-020298 | agreed |
| 33.102 | 173 | | R99 | Clarification of sequence number management | F | 3.11.0 | S3-23 | S3-020308 | agreed |
| 33.102 | 174 | | Rel-4 | Clarification of sequence number management | A | 4.3.0 | S3-23 | S3-020309 | agreed |
| 33.107 | 023 | | Rel-5 | Changes to 33.107 to support interception at a GGSN | C | 5.2.0 | S3-23 | S3-020257 | agreed |
| 33.107 | 024 | | Rel-5 | Addition of SMS type information | B | 5.2.0 | S3-23 | S3-020263 | agreed |
| 33.107 | 025 | | Rel-5 | Inclusion of Serving System IRI in TS 33.107 | C | 5.2.0 | S3-23 | S3-020310 | agreed |
| 33.107 | 026 | | Rel-5 | Remove Annexes that describes Extended HTTP Digest solution | D | 5.2.0 | S3-23 | S3-020224 | agreed |
| 33.203 | 003 | | Rel-5 | ISIM related parameters | F | 5.1.0 | S3-23 | S3-020226 | agreed |
| 33.203 | 004 | | Rel-5 | Reference of HTTP Digest AKA in TS 33.203 | F | 5.1.0 | S3-23 | S3-020281 | agreed |
| 33.203 | 005 | | Rel-5 | Clean-up of section 6.1.1 | D | 5.1.0 | S3-23 | S3-020286 | agreed |
| 33.203 | 006 | | Rel-5 | Integrity protection indicator | F | 5.1.0 | S3-23 | S3-020293 | agreed |
| 33.203 | 007 | | Rel-5 | UE and P-CSCF Behaviour on an Incomplete Authentication | F | 5.1.0 | S3-23 | S3-020294 | agreed |
| 33.203 | 008 | | Rel-5 | Requested Changes for SIP integrity | C | 5.1.0 | S3-23 | S3-020317 | agreed |
| 33.203 | 009 | | Rel-5 | Clean-up of 7.3 | D | 5.1.0 | S3-23 | S3-020319 | agreed |
| 33.203 | 010 | | Rel-5 | Security association handling in IMS when the UE changes IP address | C | 5.1.0 | S3-23 | S3-020320 | agreed |
| 33.210 | 001 | | Rel-5 | NDS/IP Confidentiality protection for IMS session keys | F | 5.0.0 | S3-23 | S3-020229 | agreed |
| 33.210 | 002 | | Rel-5 | Strengthening the requirements on IV construction to prevent attacks based on predictable IV | F | 5.0.0 | S3-23 | S3-020277 | agreed |

# Annex E: List of Liaisons

## E.1 Liaisons to the meeting

| TD number | Title | Source TD | Comment/Status |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## E.2 Liaisons from the meeting

| TD number | Title | Comment/Status | TO | CC |
|---|---|---|---|---|
| TD S3-020287 | Reply LS on Group release security solution (Response to S3-020178) | Approved | **RAN WG2, ETSI SAGE** | |
| TD S3-020305 | Reply LS on Interpretation of UEA0 (R2-020390) | Approved | **RAN WG2** | |
| TD S3-020312 | Reply LS to SA WG2 on IMS identities for Rel 99/R4 UICC (S2-021526) | Approved | **SA WG2** | **SA WG1, CN WG1, CN WG4, T WG3** |
| TD S3-020313 | Response to S3-020176 (LS N4-020372 on Immediate Service Termination from CN4). | Approved | **CN WG4** | **TSG SA, CN WG2** |
| TD S3-020314 | Liaison Statement to T WG3 on ISIM parameters | Approved | **T WG3** | **SA WG2** |
| TD S3-020315 | LS to SAGE: Reply LS on key expansion for HMAC-SHA-1-96 | Approved | **ETSI SAGE** | |
| TD S3-020316 | LS to CN WG1: Secure registration of IP addresses | Approved | **CN WG1** | |
| TD S3-020318 | LS to SA WG1 on Network Handling of 'Badly Behaved' Software IMS Clients (reply to S1-010030) | Approved | **SA WG1** | |
| TD S3-020322 | LS to SA WG2/CN WG1 on subscriber certificates | Approved | **SA WG2, CN WG1** | **SA WG1** |

### LSs forwarded to LI Group:

| TD number | Title | Comment/Status | FROM |
|---|---|---|---|
| TD S3-020181 | Liaison Statement from A WG2 on "Prefix allocation for IPv6 stateless address autoconfiguration" | Consider impact on LI | **SA WG1** |
| TD S3-020184 | Reply to LS on "IP version inter-working on the transport plane" from SA2 (S2-020291) | Consider impact on LI | **SA WG5** |
| | | | |

## Annex F: List of Actions from the meeting

**AP 23/01:** SA WG3 Chairman to initiate discussions with SA WG1 and SA WG2 Chairmen to debate the ownership of the DRM Work.

**AP 23/02:** C. Blanchard to create a proposal for WLAN interworking at the next SA WG3 meeting

**AP 23/03:** B Owen to create a WID for GUP Security. Members to send comments to him.

**AP 23/04:** K. Boman to create a WID for Presence Security for distribution over e-mail. Supporting companies to in form K. Boman by e-mail. Members to review the SA WG2 draft TR 23.841.