3GPP TSG SA WG3 Security — S3#28 **S3-030182**
6 - 9 May 2003
Berlin, Germany

3GPP TSG SA WG3 (Security) meeting #27 **Report**

25-28 February 2003

Sophia Antipolis, France

Source:	**Secretary SA WG3**
Title:	**Report version 1.0.0**
Status:	**Approved**

ETSI Secretariat Main Building, Sophia Antipolis, France

Contents

1 Opening of the meeting

Prof. M. Walker, the Chairman of SA WG3, opened the meeting and provided the domestic arrangements for the meeting. He announced the need to elect new Chairman and Vice Chairmen at the next SA WG3 meeting. Prof. Walker also announced that he was not considering standing for re-election. A letter will be sent to the SA WG3 e-mail list indicating the procedure for candidatures.

2 Agreement of the agenda and meeting objectives

TD S3-030001 Draft Agenda for SA WG3 meeting #27. The draft agenda was reviewed and approved.

2.1 3GPP IPR Declaration

Delegates were reminded of their obligations under the IPR Policy.

3 Assignment of input documents

The available input documents were assigned to their respective agenda items. Due to the large number of documents, it was agreed that the late documents would be left until the end of the meeting and dealt with if there was time, unless they were particularly pertinent to a subject already under discussion. Delegates were asked to provide input documents in good time before the meeting in order that response contributions could also be input before the "late document" deadline.

4 Meeting reports

4.1 Approval of the report of SA3#26, Oxford, England, 19-22 November, 2002

TD S3-030002 Draft Report of SA WG3 meeting #26. Some modifications were made to the draft Report and it was then approved (note that section 5 of the report was missing from the document, but had received no comments from SA WG3, and will be re-instated in the final version). **The updated report will be put on the FTP server as version 1.0.0.**

Actions from meeting #26:

AP 26/01: Completed. EF3 will host the meeting, the meeting venue is to be advised.

AP 26/02: Completed.

AP 26/03: Completed (there was no response to the e-mail that was sent).

AP 26/04: Completed. TSG SA agreed the renumbering of FIGS specifications which will be implemented by the SA WG3 Secretary.

4.2 Report from SA#18, New Orleans, USA, 9-12 December, 2002

Algorithms UES2 and UIA2: To be discussed under agenda item 6.5.

The postponed CR on SIM access to IMS should be checked under agenda Item 6.1 for updates made to the specification at the last SA meeting.

It was noted that the NDS/AF Work Item was not tabled at TSG SA #18 and would need to be forwarded to TSG SA #19. NOTE: The WID was updated at this meeting to TD S3-030139.

AP 27/01: Secretary to input the updated NDS/AF WID into SA #19 (TD S3-030139).

4.3 Report from SA3 LI #8, Paris, France, 19-21 February, 2003

TD S3-030107 Draft Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #1/03 on Lawful Interception. The report was provided for information and was noted.

TD S3-030090 Proposed CR to 33.107: Stereo delivery to LEMF (Rel-4). This was a change to an Informative Annex A, for Release 4 and was therefore not considered an essential correction to the specification and was rejected.

TD S3-030091 Proposed CR to 33.107: Stereo delivery to LEMF (Rel-5). This was a change to an Informative Annex A, for Release 5 and was therefore not considered an essential correction to the specification and was rejected.

TD S3-030094 Proposed CR to 33.108: Coding of ASN.1 parameters of the type OCTET STRING (Rel-5). This CR was approved.

TD S3-030095 Proposed CR to 33.108: Coding of ASN.1 parameters of the type OCTET STRING (Rel-6).This CR was approved.

TD S3-030098 Proposed CR to 33.108: Changes to meet international LI Requirements (Rel-5). The change of "to" to "of" was considered incorrect. **It was decided to send this back to the LI Group to also clarify the "Other versions" of 33.108.**

TD S3-030099 Proposed CR to 33.108: Incorrect ASN.1 object tree (Rel-5). This CR was approved. **The SA WG3-LI Group were asked to provide more explanation text for CRs to aid in the Presentation to TSG SA for final approval.**

TD S3-030089 Proposed CR to 33.108: CS Section for 33.108 (Rel-6). The text from ETSI TS 101 671, modified for UMTS was proposed to replace the reference to the specification, in order to give control of the content to the 3GPP SA WG3 LI group. This CR was updated in TD S3-030110 which was approved.

TD S3-030092 Proposed CR to 33.108: Adjustments to the requirements on the delivery of the intercepted RT data over TCP (Rel-6). This CR was modified in TD S3-030111 which was approved.

TD S3-030101 Proposed CR to 33.108: Changes to meet international LI Requirements (Rel-6). The change of "to" to "of" was considered incorrect. **It was decided to send this back to the LI Group to also clarify the "Other versions" of 33.108.**

TD S3-030096 Liaison Statement (from SA WG3 LI group) on WI IMS Presence Interception. SA WG3-LI Group requested contribution regarding Lawful Interception aspects of the Presence Services for comments and appropriate action. SA WG3 questioned why SA WG1 were being asked to contribute on LI aspects, when that was the task of the LI Group. There was no other specific action on SA WG3 and so the LS was noted.

TD S3-030097 Proposed WID: Lawful Interception in the 3GPP Rel-6 architecture. This WI description was approved. **It was noted that the TSG SA Plenary approval dates should be SA#22 and not SA#26 (will be modified before presentation to TSG SA#19).**

TD S3-030100 LS (from SA WG3 LI Group) on Possible overlap of the scopes in the 3GPP TS 33.108 and DES/SEC-003020. This was noted for information.

TD S3-030093 Handling of Issues associated with S3LI CRs. The SA WG3-LI Group requested that SA WG3 did not modify their CRs before sending to TSG SA Plenary. It was argued that many of the LI Group CRs required at least editorial modifications and this request could introduce substantial delays. It was agreed that SA WG3 would continue to make minor changes where necessary, and the LI Group were encouraged to improve the quality and correctness of their CRs to SA WG3 in order to avoid this. The LS was then noted.

TD S3-030103 GTP updates for MSISDN targeted LI. This was introduced by Nortel Networks and proposed that SA WG3 should consider the highlighted problem requires a solution and send LSs to CN WG4 as necessary. A CR had been presented to CN WG4 by Nortel Networks (and was rejected by CN WG4) and was attached for information. The optionality of the parameter was questioned, if this was a requirement to perform LI. **It was agreed that SA WG3-LI Group should consider this and reply to CN WG4 on the need for this, considering the requirements in TS 33.106**.

4.4 Report from SA2/SA3 joint meeting, Milan, Italy, 24 February, 2003

TD S3-030146 TSG-SA2/SA3 Joint meeting MBMS report. This was introduced by "3". This was discussed before handling contributions under agenda item 6.21. It was noted that the working assumption from the meeting was **not** to do the protection at the Radio network, but not necessarily to do it at the application level in the IETF sense. This conclusion may have been a result of different interpretations of the "application level", and maybe "User Plane" may have been intended. In general, most (but not all) SA WG3 delegates who attended the joint meeting understood that the conclusion was only not to do the protection in the Radio Network level. *The issue where the application layer resides was further discussed and it was concluded that SA WG3 could not accept a working assumption where the "application layer" is defined as it is defined in the IETF.*

SA WG3 endorsed the decision that the encryption will neither be done at the Radio level nor in the core network, and it was agreed that the encryption should be done end-to-end between UE and BM-SC, but the method of protection was for further study. This does not rule out mechanisms which are below the "application layer in the IETF sense".

The handling of the contributions was reviewed and the report was noted.

5 Reports and liaisons from other groups

5.1 3GPP working groups

TD S3-030010 Reply LS (from SA WG5) on "New requirements about functionality to make subscription to different domains independent or linked based on operator decision". This replied to SA WG1 and was provided to SA WG3 for information. The LS was noted.

TD S3-030011 LS (from SA WG5) on bearer charging issues with use of HTTP for Rel 6. This was provided to SA WG3 for information and was noted.

TD S3-030024 Reply to LS from SA5 (from SA WG2) on bearer charging issues with use of HTTP for Rel 6. . This was provided to SA WG3 for information and was noted.

TD S3-030043 LS (from CN WG1) on updated WID for emergency call enhancements for IP & PS based calls. CN WG1 asked SA WG3 whether any Security issues have been identified or are foreseen that may impact the detailed procedures covered by CN specifications. It was thought that there could be Security implications, depending on the final service requirements, and a LS was produced in TD S3-030112 informing CN WG1 that SA WG3 would need to study the emerging Emergency Call Requirements and would comment any concerns if and when identified. The LS (TD S3-030112) was approved.

5.2 IETF

TD S3-030018 IETF/3GPP Release 6 Workshop notes. This was introduced by V. Niemi, SA WG3 Vice Chairman, who attended the IETF/3GPP Joint workshop as a representative of SA WG3. The conclusions of the workshop were not binding on 3GPP or IETF, but the recommendations were provided for discussion in 3GPP in order to discuss the application of them in the SA WG3 work. The report was briefly introduced, delegates were asked to read more thoroughly themselves for background information. The document was then noted.

TD S3-030017 3GPP/IETF Release 6 Workshop Major Conclusions. This was introduced by V. Niemi, SA WG3 Vice Chairman, and had been provided by the 3GPP co-ordinator for IETF, S. Hayes. The recommendations were presented and discussed in order to gain a general understanding of them.

AP 27/02: V Niemi to consult S. Hayes on possible follow-up to the Joint 3GPP/IETF Workshop conclusions.

WLAN Interworking: It was explained that the IETF urgency for verification of the IEEE Security techniques is not as urgent as the 3GPP due to deadlines. Therefore 3GPP were recommended to review the techniques before finalising standardisation of their use. There were many questions on the implications and scope of reviews of the various security techniques and mechanisms and what they should be reviewed against (e.g. review against which Security requirements). It was considered that further clarification was needed in order to facilitate completion of the IETF work for Release 6. It was agreed that S. Hayes should be asked to obtain this clarification and list of the reviews that are requested from SA WG3. The SA WG3 Chairman agreed to contact S. Hayes on this matter.

AP 27/03: M. Walker to contact S. Hayes to obtain a list of actions requested from SA WG3 for WLAN Interworking in order to ensure completion of 3GPP work for Release 6.

V. Niemi was thanked for representing SA WG3 in San Francisco and providing the presentations to and notes from the Workshop.

5.3 ETSI SAGE

P. Christoffersson provided a verbal report of the ETSI SAGE activities since the last meeting.

There had not been a SAGE meeting for a long time. Following the request from SA WG3 to provide back-up algorithms for f8;/f9 there had been some activity in the group. Contributions on this is included in this meeting and if funding is agreed then work can begin in March 2003.

The Plaintext redundancy study work had not progressed as the search is continuing to find experts interested in working on this.

P. Christoffersson was thanked for his report.

5.4 GSMA SG

C Brookson provided a verbal report of the GSMA activities since the last meeting.

Security issues raised in handsets.

NDS - some guidelines on operator advice to GPRS customers to protect themselves against potential fraudulent usage of their subscriptions.

Handset violation causing congestion on networks. Different legislation in different countries causing some discussion.

TCAM (RTTE Directives) Committee considering to make mandatory testing of IMEI Security. There are some practical problems with this as the complete securing of IMEI needs some consideration. SA WG3 may wish to make a statement on this issue. An ad-hoc group to discuss this was organised during the meeting by C. Brookson for interested members. The following report was provided by C. Brookson after the meeting:

A discussion was held on the evening of the 26th February on the recent developments of Fraud and IMEI Security. Members had before them the background, contained within an ETSI OCG 19 document presented as Tdoc 132. Charles Brookson (who was involved as ETSI OCG and also GSM Association Security Chairman, and who was hoping to attend TCAM) gave a presentation to set the scene. He described:

That various groups involved were

- *ETSI with the OCG Group (document available).*
- *GSM Association (who ran the SEIR and CEIR, which black listed the IMEI on a country and world-wide respectively) with the Security Group SG and the Terminal Group TWG who at present provided funding to administer the IMEI.*
- *ITU who were looking at making the use of the IMEI a recommendation.*
- *Manufacturers body EICTRA.*
- *JEM Joint Expert Meeting were producing a draft agreement to use the IMEI in standard format in many other mobility standards worldwide.*

TCAM, which is the Standing Committee of Directive 1999/5/EC (R&TTE Directive), was looking at the IMEI as a result of a previous meeting. Another meeting was due on the 12th March, and he would be describing some of the issues.

It was suggested that SA3 could be involved in defining the possible way forward, recognising that this debate had been going on for over 12 years. SA3 recognised that

- *There is no single secure solution,*
- *Technology improvement will occur to secure the IMEI, so one definition is not appropriate,*
- *IMEI security must be economic to manufacture, but uneconomic to break,*
- *That it is not technically possible to manufacture a commercially viable product with an unbreakable IMEI,*
- *that 3GPP could help by looking at the issues that might help to come to a world-wide solution,*
- *Various solutions are preferable (one should not break one, and so break all).*

The resulting discussion within SA3 covered the areas of

- *the possible ways of proving the IMEI security (by testing any claim),*
- *ways of changing the IMEI, recent methods have included the insertion of an extra processor in the mobile (PIC chip), which for example leaves the IMEI intact, but changes it when it is sent to the network,*
- *looking at other possible means of meeting the objectives of preventing the theft of mobiles which might not include the IMEI,*
- *looking at future solutions and challenges, such as software defined radios,*
- *existing proposals that had already been proposed within the GSMA,*

- *that the IMEI was originally introduced for type approval purposes, and therefore the integrity was not then an issue. The use of the IMEI to black list stolen mobiles had created a financial incentive to change it, which is why we had this issue,*
- *that there were many other uses of the IMEI. A 1999 paper addressing these issues would be re-circulated (this was originally used in the change requests to make the IMEI unchangeable in the 3GPP specifications for GSM and 3GPP).*

3GPP SA3 decided that it should study these areas as an email discussion to come to a conclusion of the way forward. Charles Brookson was asked to feed back other initiatives from the other groups, and to attempt to co-ordinate them and keep everyone informed and involved.

A presentation on GPRS over-billing attacks was provided to members present at the meeting and was noted. A proprietary solution had been developed and tested, but the possibility of a standardised protection from this may be considered by Members.

GPRS ad-hoc:

An ad hoc was held to look at some of the issues concerned with GPRS and fire walls, and methods to resolve over billing. It was decided that:

1) Those people who were interested in trying to find a solution should participate in an ad-hoc email discussion (indicating their willingness to participate by sending an email to eric.gauthier@orange.ch or cbrookson@iee.org).
2) That the objective would be to come up with a proposal to modify the standards to try to overcome the issues raised, working with the Industry.
3) Once solutions are identified consensus should be reached, and changes to the standards proposed to SA WG3.

C. Brookson was thanked for his report.

5.5 3GPP2

M. Marcovici provided a verbal report. 3GPP2 Security algorithms have been published. MBMS Framework in progress, IMS Security as an adaptation of the 3GPP IMS Security work is in progress. WLAN Security negotiations ongoing.

5.6 TIA TR-45

TR-45 AHAG has moved their 3GPP work to the 3GPP SG and are meeting 3-4 times per year. A joint meeting between 3GPP and 3GPP2 SGs is planned in San Francisco in July 2003.

5.7 Other Groups

There were no specific contributions under this agenda item.

6 Work areas

6.1 IP multimedia subsystem (IMS)

TD S3-030008 Requirement to Allow Access to IMS by Means of SIM in 3G UEs. This was introduced by T-Mobile. The technical impact of this had been discussed at the previous meeting of SA WG3 and the document was noted until further decision by TSG SA and TSG CN.

TD S3-030009 SA WG2 response to “Response to IETF LS on Interoperability Issues and SIP in IMS”. This was introduced by Ericsson and asked SA WG3 to take into account the inputs in the LS for the proposed way forward on interoperability issues and SIP in IMS. A response to IETF had been sent in TD SP-020842 from SA#18 meeting. The LS was therefore noted.

TD S3-030013 LS from TSG SA: Additional Release 5 work needed for Policy Control and Subscription Control of Media. This was introduced by Ericsson and was a request for SA WG3 (and other addressed groups) to investigate the issues and provide appropriate Rel-5 CRs to TSG SA#19 to complete open issues as a result of approval of a new solution at TSG CN#18 on Policy Control and Subscription Control of Media. The related TSG SA CR to 23.228 was provided for information in TD S3-030115 and a group met to discuss this and provide a LS reply to TSG SA was provided in TD S3-030116 which was approved.

TD S3-030023 LS (from SA WG2) on Multiple IMS registrations. This was introduced by Nokia and asked SA WG3 for feedback on the security implications of extending the relationship of Public User Identities and Private User Identities as described in the attachment to the LS. A response was requested during the meeting as SA WG2 were meeting in the same week as SA WG3. It was discussed and generally thought that as long as each subscription is a separate Private entity, there was no implication on the system, as each separate subscription would be identified for billing procedures. An ad-hoc group was set up to consider these issues more closely and provide a LS back to SA WG2 on the subject, which was provided in TD S3-030117 which was approved and sent immediately to SA WG2 who were meeting at the same time.

TD S3-030032 Proposed CR to 33.203: Malicious UE bypassing the P-CSCF (Rel-5). This was introduced by Nokia. A related proposal from Siemens was provided in TD S3-030057 (and related CR proposal in TD S3-030058) which was considered in relation to this proposal (see below). This was discussed and it was decided to make a new CR based upon this CR and the Nokia contribution in TD S3-030058 which was provided in TD S3-030119 which was reviewed and approved.

TD S3-030057 Means to counter IMS P-CSCF bypassing. This was introduced by Siemens and discussed 3 scenarios for IMS P-CSCF bypassing and concludes that the treat can be countered by appropriate FW functionality in Home and Visited IMS domains.

The following recommendations for measures to counter the attack scenarios described in this contribution (details to be found in the scenario discussions of section 2) are proposed to be incorporated into TS33.203:

- *Access to S-CSCF entities must be restricted to the core network entities that are required for IMS operation, only. It shall be ensured that no UE is able to directly send IP packets to IMS-entities other than the required ones, ie. assigned P-CSCF, or HTTP servers.*
- *Impersonation of IMS core network entities at IP level (IP spoofing), especially impersonation of P-CSCFs by UEs shall be prevented.*
- *It is desirable to have a general protection mechanism against UEs spoofing (source) IP addresses in any access network providing access to IMS services*.

A related CR to add an informative Annex to TS 33.203 was provided in TD S3-030058.

TD S3-030058 Proposed CR to 33.203: Malicious UE bypassing the P-CSCF (Rel-5). This was discussed and it was decided to make a new CR based upon this CR and the Nokia contribution in TD S3-030032. The joint CR was provided in TD S3-030119 and approved.

Trust Domain: Ericsson discussed the text in section 4.4 of 24.229 version 5.3.0: The statement that "*ASs provided by third-party service providers are outside the trust domain*" should be taken into account in the CR produced. Ericsson agreed to help with the drafting of the joint CR.

TD S3-030105 Openness of Rel6 IMS network: security methods required. This was introduced by Nokia and provided further considerations on the IMS security issue above, related to Rel-6. As this is not related to the immediate Rel-5 problem, Nokia were asked to develop this for input to a future discussion on Rel-6 security issues. The contribution was then noted.

TD S3-030042 LS (from CN WG4) on clarification on the requirement for UE re-authentication initiated by HSS. This was introduced by Orange France and asked SA WG3 to give clear guidance with regards to the requirement for the UE re-authentication triggered by the HSS via the Cx interface. It was agreed that there is no requirement from SA WG3 for triggering of re-authentication from the HSS. A reply liaison statement was provided in TD S3-030120 which was reviewed and updated in TD S3-030159 and approved.

TD S3-030047 Proposed CR to 33.203: Remove error message as unprotected response (Rel-5). This was introduced by Nokia and proposes the removal of the accepting error messages on the unprotected port as error messages could be protected in any established SA, and unprotected error messages are covered by "*responses to unprotected REGISTER messages*". There was some discussion on the need for this change, as removal of redundancy was not an essential correction, whereas the removal of the incorrect statement would depend on the consequences: Incompatible implementations or serious security threat. **There was no support for this change and the CR was rejected.**

TD S3-030048 Proposed CR to 33.203: Correction of the Port 2 definition for SA establishment (Rel-5). This was introduced by Nokia. The change proposed to the main body was not thought to be an essential correction as it was already stated that the Proxy can send on any port. The proposals for Annex H were subjected to an off-line discussion to produce a full clarification. The CR was updated and provided in TD S3-030121 which was reviewed and **the change to Bullet "7." was agreed in principle**. It was decided to update this over e-mail. Discussion deadline 5 March 2003, approval 7 March 2003. The approved document was later allocated to TD S3-030170.

TD S3-030049 Proposed CR to 33.203: Add protected port into Via header (Rel-5). This was introduced by Nokia and adds the protected port number to the Via header to allow response from P-CSCF. The CR was revised in TD S3-030123 which was reviewed and updated editorially in TD S3-030158 and approved.

TD S3-030052 Proposed CR to 33.203: Ensuring the deletion of unwanted SAs (Rel-5). This was introduced by "3" and adds the deletion of unwanted SAs from an incomplete authentication process to prevent 3 SA pairs being held in P-CSCF following unsuccessful authentications. This CR was updated to clarify the text in TD S3-030124 which was approved.

TD S3-030055 Proposed CR to 33.203: Clarification of the use of ISIM and USIM for IMS access (Rel-5). This CR was approved and a Liaison Statement to SA WG1, SA WG2, CN WG1 and T WG3 was produced to inform them of this change in TD S3-030125 which was updated in TD S3-030160 and approved.

TD S3-030106 Impacts due to the use of SIM for IMS access. This was introduced by GemPlus and discusses the threats and proposed solutions for allowing IMS access with SIM in Rel-5. It concludes that the issues and threats should be reported by SA WG3 to TSG SA and recommends the rejection of IMS access using SIM in Rel-5. It was clarified that the use of SIM for IMS Access in release 5 is an item for study after TSG SA meeting #18 and this contribution was considered an input to the study. GemPlus agreed to produce a LS based on this contribution and taking other Members views into account in TD S3-030126 which was updated in TD S3-030161 and approved.

6.2 Network domain security: MAP layer (NDS/MAP)

There were no specific contributions under this agenda item.

6.3 Network domain security: IP layer (NDS/IP)

TD S3-030034 Proposed CR to 33.210: Za-interface and roaming agreements (Rel-5). This was introduced by Siemens and clarifies that roaming agreements are not always needed for the Za interface. The CR was updated in TD S3-030127 which was approved.

TD S3-030035 Proposed CR to 33.210: Za-interface and roaming agreements (Rel-6). This was revised in TD S3-030128 which was approved.

TD S3-030075 Proposed CR to 33.210: Clarification to the re-keying aspects of network domain security (Rel-5). This was introduced by Lucent Technologies. The second paragraph of the changes was considered adequate for this CR and Lucent agreed to revise the CR and produce a Rel-6 version. These were provided in TD S3-030129 and TD S3-030130 which were updated in TD S3-030162 and TD S3-030163 and were approved.

6.4 Network domain security: Authentication framework (NDS/AF)

TD S3-030082 NDS/AF TS TOC proposal. The attached table of contents for the draft NDS/AF TS was introduced by Nokia. The document contained proposals for content to populate the sections. Further proposals for inclusion were provided in a companion document TD S3-030083. It was recognised that some sections may need re-naming or moving when content is agreed for them. The Rapporteur was thanked for this document, which was noted. Delegates were asked to contribute to the draft TS.

TD S3-030083 Introduction and requirements for manual cross-certification within NDS/AF. This was introduced by Nokia on behalf of Nokia, Siemens, SSH and T-Mobile and proposes content for sections 4 and 5 of the NDS/AF Draft TS. The principles were accepted as input to the TS and the rapporteur was asked to add this text. The contribution was then noted.

TD S3-030104 Profiling of IKE and Certificates for use within NDS/AF (Late document from Siemens, SSH, T-mobile and Nokia). This was briefly introduced by Siemens and delegates were asked to provide comments to the author 14 days before the next SA WG3 meeting.

TD S3-030108 Guidelines for selecting between a bridge CA and a direct cross certification model for NDS/AF (Late document). The principles were accepted in TD S3-030083, so this contribution was noted.

TD S3-030139 Updated WID: Network Domain Security; Authentication Framework (NDS/AF). This WI description was approved.

TD S3-030150 Draft TS ab.cde NDS/AF version 0.1.0. Updated at this meeting, the draft was provided for information and noted. The SA WG3 Secretary agreed to request a TS number for this document after the WID is agreed at TSG SA.

6.5 UTRAN network access security

TD S3-030016 LS to 3GPP TSG SA3 regarding use of the “AMF” field to switch between multiple authentication algorithms. This was received from GSMA SG#45 and asked SA WG3 to continue standardisation work on this feature and provided a draft document to use as a starting point as an attachment.

TD S3-030065 "AMF" field to switch between multiple authentication algorithms. This was introduced by Siemens and discussed the proposal to standardise the usage of the AMF-field (as available in TD S3-030016) to switch between multiple authentication algorithms, as this is the most interesting but also the most critical use of the proposal. The analysis shows that the use of the AMF for authentication-algorithm switching will lead to authentication problems in certain scenarios. Siemens suggested that this analysis should be forwarded to GSMA SG before SA WG3 begins working on this feature. It was noted that the addition of backup algorithms would not necessarily remove the threat of algorithm compromise and also that different key sets should be used for different algorithms. A response LS to TD S3-030016 with the analysis in TD S3-030065 was provided in TD S3-030134 which was approved.

TD S3-030085 Requirements list for UEA2 and UIA2. This was introduced by Vodafone and provided a list of draft requirements for new encryption and integrity algorithms. Some modifications to the proposal were suggested and included in an LS to ETSI SAGE in TD S3-030135 which was approved.

Manufacturers were asked to provide guidelines on implementation complexity so that SA WG3 can finalise parameters, e.g. the requirements on gate count and clock speed, at the next SA WG3 meeting.

TD S3-030086 Provisional work plan for the design of the 3GPP confidentiality and integrity algorithms UEA2 and UIA2. This was introduced by P. Christoffersson on behalf of ETSI SAGE. It was agreed that this should be forwarded to TSG SA for approval and a LS to TSG SA was provided in TD S3-030136 which was approved.

TD S3-030087 Security issue with multiple PDP Contexts in GPRS. This was introduced by Vodafone and discussed a problem with multiple PDP contexts in GPRS. Vodafone proposed that SA WG3 endorse the concept of enabling the network to deny the establishment of new PDP Contexts depending on there being others currently active. Solutions have been discussed in CN WG4 (TD N4-030172) which was submitted to this meeting for information in TD S3-030137 (noted). After some discussion, no full endorsement of this proposal was achieved, and further study was considered necessary before agreeing on the type of solution to apply. A Liaison Statement to CN WG4, attaching this contribution, in order to receive more information on the potential solutions being investigated by CN WG4 was provided in TD S3-030138 which was updated in TD S3-030164 and was approved.

6.6 GERAN network access security

TD S3-030038 LS from TSG GERAN: Use of Kc in the Uplink TDOA location method. This was introduced by True Position and asked SA WG3 to analyse the security impacts when using the Kc in Uplink TDOA location. The attached slide presentation was also presented by True Position. There was some concern over routinely transmitting the Kc to 10 to 20 LMUs, more study on the possible security risk against the gain in performance received was considered necessary before SA WG3 could agree to doing this. It was agreed that a Liaison Statement would be drafted to TSG GERAN on this to inform them that SA WG3 wish to study the implications more and requesting more information, if available. The LS was provided in TD S3-030133 which was reviewed and updated in TD S3-030152 and approved.

TD S3-030109 Updated GERAN A/Gb mode security enhancements WID. This WI description was approved.

TD S3-030113 GERAN A/Gb mode security enhancements. This was introduced by Vodafone and due to lack of time, was presented for information. Members were asked to consider this and comment to the Author. The document was then noted.

6.7 Immediate service termination (IST)

TD S3-030012 Reply LS (from SA WG5) on Indication of call termination as a result of IST operation. This was introduced by Siemens and asked SA WG3 to clarify the requirements on including support for the IST operation in charging specifications concerning the applicable Release and welcome further comments related to the e-mail discussion on IST for PS services. A response from SA WG1 was available in TD S3-030021. It was decided that an e-mail discussion should be held and a response LS advising on the Releases will be provided. Discussion until 7 March 2003, approval date for circulated LS 14 March 2003. TD S3-030153 was allocated for the approved LS.

TD S3-030021 Response LS (from SA WG1) on Indication of call termination as a result of IST operation. This was introduced by Lucent Technologies. SA WG1 inform SA WG5 that the ODB for the PS Domain is defined from Release 4. The LS was noted and used in the handling of the original LS in TD S3-030012.

6.8 Fraud information gathering system (FIGS)

There were no specific contributions under this agenda item.

6.9 Support for subscriber certificates

TD S3-030036 Alternative proposals for subscriber certificate bootstrapping. This was introduced by Alcatel and proposed several solutions for subscriber certificate bootstrapping for discussion. Documents related to this were TD S3-030050 and TD S3-030051 which were then considered. It was agreed that this alternative proposals would need study to determine the full impact and delegates were asked to do this and contribute to the next SA WG3 meeting. The editor of the TS on bootstrapping and support for Subscriber Certificates was asked to include the proposal in the draft TS.

TD S3-030050 Bootstrapping of application security from 3G AKA and support for subscriber certificates. This was introduced by Siemens on behalf of Siemens and Nokia. Several proposals were made and suggestions for bootstrapping which need consideration by SA WG3. The principles were agreed, but it was agreed that other groups need to be consulted (e.g. SA WG2 and CN WG4) on these ideas. The editor of the TS on bootstrapping and support for Subscriber Certificates was asked to include the proposal in the draft TS.

TD S3-030051 Draft TS Table of Contents for “Bootstrapping and Support for Subscriber Certificates”. This was introduced by Siemens on behalf of Siemens and Nokia. There was some discussion on whether a TR should be produced in the first instance, rather than a TS. It was considered that a TS would be needed and that it may slow down the production of the TS if it is produced as a TR first. It was concluded that this should be used as a basic structure for the TS and proposals in TD S3-030036 and TD S3-030050 should be included for further discussion. Further contributions were requested on this draft TS. **Tao Haukka (Nokia) agreed to be the editor for this TS.**

TD S3-030037 Consideration of CA generating public/private key pairs. This was introduced by Alcatel and proposed that SA WG3 address the issue of where the short-lived public/private key pairs should be generated and how it can be securely stored on the Smart Card. **Alcatel were asked to provide text based on this contribution to the editor of the TS on bootstrapping and support for Subscriber Certificates for inclusion in the draft TS**.

TD S3-030071 Parameters in subscriber certificate and subscriber profile supporting operator control and service differentiation. This was briefly introduced by Nokia, in support of the proposal in TD S3-030073. This proposed that there should be a control class for each certificate usage type. It was clarified that the visited network case would not apply to the first phase of the work, but could be extended in this way for a future phase. **Nokia agreed to make further discussion of this an e-mail discussion item and input to the next meeting**.

TD S3-030072 NAF-BSF (D interface) protocol. This was briefly introduced by Nokia, in support of the proposal in TD S3-030073. This concludes that there are no DIAMETER applications currently suitable for the D interface, but two DIAMETER applications can be considered for modification, or a new DIAMETER application could be defined. **Nokia agreed to make further discussion of this an e-mail discussion item and input to the next meeting**. It was agreed to forward this contribution in a liaison statement to CN WG4, informing them of the e-mail discussion and that SA WG3 were considering these issues. The Liaison Statement was provided in TD S3-030131 which was approved.

TD S3-030073 Protocol B: Subscriber Certificate Enrolment based on Bootstrapping. This was briefly introduced by Nokia to provide an overview of the contribution. It proposed that this requirements information be inserted in the TS (TD S3-030050) and the Nokia preferred solution (solution#1) PKCS#10 with HTTP Digest authentication, be incorporated in an Annex. It was agreed that the requirement part could be included for further discussion and the solution should be discussed with the Alcatel contribution (TD S3-030037) and incorporated together in an Annex of the TS.

6.10 Digital rights management (DRM)

There were no specific contributions under this agenda item.

6.11 WLAN inter-working

The contributions in the form of "Pseudo-CRs" to the draft TS were considered individually, recognising that the agreements made here would require co-ordination of the changes between the authors of changes to the same areas.

TD S3-030077 Pseudo-CR to 33.234: Editorial changes to WLAN. This was introduced by the TS Editor. It was agreed that the 4th bullet on the Network Elements change should be WLAN (card) **integrated**. The changes were agreed and the editor was asked to include this in the draft TS.

TD S3-030045 Pseudo CR to 33.234: Change to the security requirement related to the storage of all long-term security credentials used for subscriber and network authentication. This was introduced by GemPlus. There was some question over the term "UICC" as there should be no impact on existing (Rel-4) SIMs. It was clarified that the UICC does not imply SIM. Therefore this change implied changes to requirements, not agreed in 3GPP. Therefore the Pseudo-CR was rejected.

TD S3-030151 Pseudo-CR to 33.234: Change to the security requirement related to the storage of all long-term security credentials used for subscriber and network authentication. This CR was presented as a replacement to the CR proposed in TD S3-030045 (see above). The CR removed the points of contention in the previous version and was reviewed and approved.

TD S3-030039 Security requirements for WLAN. This was introduced by Orange France. The changes were a result of an e-mail discussion launched by Orange France, and no response was received on the changes proposed in the document. Therefore the changes were reviewed and agreed to be added to the draft TS.

TD S3-030078 Pseudo-CR to 33.234: Update of Security Requirements. This was introduced by Ericsson. Bullet 2 should be changed to remove "*tamper-resistant memory, such as UICC*" and read "*UICC or SIM Card*". Bullet 3 of 4.2.1 should be re-worded in the same terminology as the (modified) second bullet for clarity. For changes to 4.2.2, the "shall" changes will be reverted to "should". "3G" will be added before "WLAN". Changes to 4.2.3 : Bullets 1 and 2 were re-instated and modified. The third bullet will be changed from "must" to "shall" and "adequately" will be deleted. Other changes were also made and the editor will include the agreed text of bullet 3.

TD S3-030079 3G-WLAN Threat Analysis. This was introduced by Ericsson. This was agreed to be added to the draft TS.

TD S3-030080 WLAN Link Layer Security Requirements. This was introduced by the TS Editor (contribution from Ericsson). It was proposed to put the questions and issues raised in this contribution as Editors' Notes in the draft TS. There were many issues identified over the availability of 802.11i in time for Rel-6, and solutions may need to be found to use other solutions. A Liaison Statement to IEEE 802.11i was provided in TD S3-030140 which was updated in TD S3-030166 and approved. Another Liaison Statement to SA WG2 was provided in TD S3-030141 which was updated in TD S3-030167 and approved.

AP 27/04: J. Puthenkulam to lead an e-mail discussion on IEEE 802.11i requirements from the 3GPP Security point of view.

TD S3-030029 Security Requirements for 3G-WLAN Interworking. This was introduced by Intel on behalf of Intel and Cisco. For this part of the agenda item, only the General requirements change proposals were considered: (See below for remainder of document).

TD S3-030041 Provision of indication to the USIM that the authentication procedure is executed in the 3G-WLAN access context. This was introduced by Telenor and proposed to investigate the policy control problem outlined in the contribution further. Members were asked to study this off line and provide comments to the author, and to contribute to the next SA WG3 meeting. The document was then noted.

TD S3-030006 LS from SA WG1: Having a Single USIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link. This was introduced by Toshiba. A presentation was provided to describe the scenarios. Toshiba were thanked for the presentation. A related LS from T WG2 was provided in TD S3-030027. A response LS was provided in TD S3-030145.

TD S3-030027 LS from T WG2: Response to LS S1-022388. "Having a Single (U)SIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link". This was introduced by Nokia. Discussion concerning this input and TD S3-030006 resulted in a reply Liaison Statement provided in TD S3-030145 which was modified in TD S3-030165 and was approved.

TD S3-030088 Security Issues of Having a Single (U)SIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link. This was a **late contribution** related to the discussions in TD S3-030006 and so was briefly presented and noted.

TD S3-030031 WLAN-UE Functionality Split : Request for Work Item. This was a **late contribution** related to the discussions in TD S3-030006 and so was briefly presented and noted.

TD S3-030143 LS from T WG3: Response to LS S1-022388: “Having a Single USIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link”. This was a **late contribution** (due to a problem with distribution of the LSs within MCC) and was provided for information to SA WG3. The LS was briefly presented and noted.

TD S3-030081 WLAN – Certificate-Based Protection of IMSI for EAP-SIM/AKA. This was introduced by Ericsson and proposes 3 levels of protection for IMSI and suggested that SA WG3 adopt the mechanism described as an optional mechanism to further enhance identity privacy support. It was agreed that for the present, level 1 and level 2 protection was considered to fulfil the requirements, and further level 3 protection would be reconsidered if stronger requirements are identified and agreed as necessary.

TD S3-030029 Security Requirements for 3G-WLAN Interworking. This was introduced by Intel on behalf of Intel and Cisco (note that the first part of the document was presented here). There was some discussion on the proposals for addition and it was clarified that all users would have UICC in the security work required by the service scenarios from SA WG1 and some of the proposals were outside of the scope of this. The statements about >128 bit key *entropy* were also questioned and should be verified. It was considered that the reference to RFC 2284bis should not be considered until the document is stable. **It was agreed that this should be added as an editors note and considered when the document final content is clearer.**

It was requested whether IEEE could provide a draft of the 802.11i specification (and any other relevant specifications) to 3GPP for evaluation and comment. This request was included in the Liaison Statement in TD S3-030140.

TD S3-030030 PKI Deployment Models for PEAP. This was introduced by Intel on behalf of Intel and Cisco. It was provided for information and members were asked to consider the content of this and comment. The contribution was then noted.

TD S3-030033 Identity protection using P-TMSI for 3GPP/WLAN interworking. There was nobody from Thomson to present this document, which was for information, so it was noted.

TD S3-030046 Handling invalid temporary identifiers. This was introduced by Nokia and discussed 3 possible alternative methods to handle invalid temporary identifiers. **It was agreed that in the case the IMSI is sent in clear the user may be prompted, this decision is UE-specific and outside the scope of the security standard.**

TD S3-030144 LS from T WG3: Request for Information Regarding WLAN Interworking Impacts to UICC applications. This was a **late contribution** (due to a problem with distribution of the LSs within MCC) and was postponed to the next meeting.

TD S3-030102 EAP support in smart cards and security requirements in WLAN authentication. This was a **late contribution** for information and was briefly presented by SchlumbergerSema. It had been presented in SA WG2, and considered to be a security-related issue. Due to lack of time, the contribution was noted at this time and the author was asked to continue any discussion on e-mail for further contribution to SA WG3 meetings.

TD S3-030114 LS (from SA WG2) on WLAN/3GPP Simultaneous Access. Due to lack of time it was necessary to discuss this over e-mail and create a reply LS. P. Howard agreed to lead the e-mail discussion. Deadline for discussion: 21 March 2003, Deadline for approval of Reply LS: 28 March 2003. TD S3-030169 was allocated for the approved LS reply.

6.12 Visibility and configurability of security

There were no specific contributions under this agenda item.

6.13 Push

There were no specific contributions under this agenda item.

6.14 Priority

There were no specific contributions under this agenda item.

6.15 Location services (LCS)

There were no specific contributions under this agenda item.

6.16 User equipment functionality split (UEFS)

There were no specific contributions under this agenda item.

6.17 Open service architecture (OSA)

There were no specific contributions under this agenda item.

6.18 Generic user profile (GUP)

TD S3-030014 Proposed WID update: 3GPP Generic User Profile Security. This was introduced by Lucent Technologies. The dates were updated in TD S3-030154 which was approved.

TD S3-030020 LS (from SA WG1) on T2 proposal for GUP requirements- UE Data access and Backwards Compatibility. **An e-mail discussion and review group was set up to provide a response LS. Deadline for discussion: 21 March 2003. Deadline for approval: 28 March 2003**. Brad Owen will lead this e-mail discussion group and produce the LS, which was allocated to TD S3-030155.

6.19 Presence

TD S3-030059 Draft TS 33.abc: Presence Service; Security. Version 0.3.0. This was reviewed and noted.

TD S3-030005 LS (from SA WG2) on management and regulatory requirements for Presence service. SA WG2 asked SA WG3 if there are any service-specific regulatory and lawful interception related requirements specific to the presence service. It was agreed to forward this LS to the SA WG3-LI Group for consideration. **The LI Group were asked to respond to SA WG2 on this issue.**

TD S3-030025 LS (from SA WG5) on management and regulatory requirements for Presence service. This was copied to SA WG3 for information and was noted.

TD S3-030022 LS (from SA WG2) on use of HTTP between UE and AS in the IMS. This was introduced by Siemens and asked SA WG3 to study security mechanisms for an HTTP based reference point between the UE and Application Server (AS). Contributions proposing responses to the questions posed in the LS were provided in TD S3-030056, TD S3-030060,TD S3-030069 and TD S3-030084 which were presented and discussed together. After discussion on the topic, a response to the LS was provided in TD S3-030148. **Due to lack of time at the meeting, it was agreed that this would be discussed over the e-mail list and approved by e-mail. Deadline for discussion: 14 March 2003. Approval by 21 March 2003. The LS was updated after e-mail discussions in TD S3-030171 and approved.**

TD S3-030056 Security solution for IMS-related HTTP services. This was introduced by Siemens and discussed solutions for security of IMS-related HTTP Services. This formed part of the general discussion and agreements for IMS-related HTTP services security.

TD S3-030060 HTTP authentication. This was introduced by Nokia and introduced 4 authentication methods and an analysis for HTTP security. It summarised that the short-life subscriber certificate seems to be the preferred and cleanest approach to authenticate client in transport layer, dependent upon certain factors being satisfied. Nokia suggest that SA WG3 form a decision of the alternatives so as to proceed the work.

TD S3-030069 The use of HTTP in Presence/IMS. This was introduced by Ericsson and outlined a working assumption of SA WG2, proposed that SA WG3 adopt this. Ericsson also identified threats with HTTP security. A Pseudo-CR was attached which provided a detailed text proposal. It was reported that TLS has been omitted until now as SA WG2 had not decided upon the architecture. It was agreed to add the Pseudo-CR text to the draft TS.

TD S3-030084 How to mitigate the Interleaving attack and reduce the trust in the Authenticator. This was introduced by Ericsson and discussed how the HTTP security threat provided in TD S3-030069 can be resolved. It suggests adding text to the Draft TS as a placeholder. It was confirmed that the described problem was valid. The proposal to include the solutions in the Presence TR should wait further study of the mechanism to be chosen and analysis of the applicable solutions for that mechanism.

SA WG3 agreed on these principles as a working assumption: *TLS will be taken as a priority mechanism, but this would be further studied along with other mechanisms. Tunnelling should be investigated for use, and MITM type attacks would need to be analysed and eliminated. The authentication method should use the AKA architecture if possible.*

A Liaison Statement to ETSI SAGE was produced in TD S3-030147 informing them of the current status of the Key Derivation function discussions and the potential functions which may be chosen, in order to ask if such functions can be provided in the future if requested by SA WG3. The LS in TD S3-030147 was left for e-mail approval due to lack of time. **Deadline for discussion: 14 March 2003, Approval 21 March 2003**.

TD S3-030007 LS from SA WG2: Proposed Confidentiality for IMS. A discussion paper was provided in TD S3-030070 which answered some questions, so this was consulted. A response LS to SA WG2 was provided in TD S3-030149 which was updated in TD S3-030168 and was approved.

TD S3-030070 Confidentiality in Presence. This was introduced by Ericsson and provided potential solutions to the confidentiality problems with the Presence feature when connecting through (Pre Rel-6) NEs. A Pseudo-CR to implement the alternative solutions as also attached. It was remarked that a Rel-5 P-CSCF cannot be accessed over a WLAN, and therefore only GERAN and UTRAN access should be possible in Rel-5. It was agreed that this should be studied more to determine whether there is a real problem and the best solutions if so. It was also agreed that the requirements on Po and Pw interfaces would be added as editors notes in the draft TS.

TD S3-030068 End-to-end authentication of Presence subscriptions in Pw. This was introduced by Ericsson and introduces potential new requirements for end-to-end authentication of Presence subscription requests. Ericsson proposed SA WG3 study further the current working assumption to re-use IMS authentication for Presence in the Pw interface (i.e. Watcher application) and suggests it would be enough to mandate only authentication of all subscription requests. After some discussion, it was agreed that end-to-end should be removed, and 2 requirements were not accepted. With these changes, the editor was asked to include the proposal in the draft TS.

6.20 User equipment management (UEM)

There were no specific contributions under this agenda item.

6.21 Multimedia broadcast/multicast service (MBMS)

The report of the joint meeting with SA WG2 on MBMS was provided in TD S3-030146 which is reported under agenda item 4.4.

TD S3-030028 Draft TS 33.246 v0.0.3: Security of Multimedia Broadcast/Multicast Service. This was introduced by the rapporteur for the MBMS draft TS and contained the changes agreed at the previous meeting of SA WG3. The changes were reviewed and noted. The document was used as a basis for discussion of further contributions.

TD S3-030066 Comments to MBMS security requirements. This was introduced by Siemens. In 4.1.1.2 it was decided to add an editors note stating that the need for authentication during content delivery was for further study. In 4.1.2 the comment was added as an editors note. In 4.1.5 it was agreed that the requirement does not apply when the content provider is part of the same network. When outside of the network, national laws and regulations on privacy cover this requirement. The text should be changed to reflect this. It was agreed to add an editors note to R1a and to make the text of 5.2 an editors note, as it is for further study.

TD S3-030064 MBMS: Key Encryption Keys requirements. It was agreed to postpone this contribution and the author will submit a new contribution, based on agreements made at this meeting, to the next SA WG3 meeting.

TD S3-030061 Comparison of MBMS security scenarios. This was introduced by Ericsson. This had been presented to the joint meeting on MBMS and proposed distributing the MBMS security functionality between fewer nodes, move it away from the radio layers and moving it towards the upper layers (application layer). The contribution was in line with earlier decisions in SA WG3, and the contribution was noted.

TD S3-030062 UE considerations when evaluating MBMS security at application layer vs. network layer. This was introduced by Ericsson. The contribution was in line with earlier decisions in SA WG3, and the contribution was noted.

TD S3-030074 MBMS: Reuse of RAN/GERAN ciphering functions. This was introduced by Siemens. The contribution highlights the need to involve TSG RAN groups in an analysis of impacts if it is decided to use UE-BM-SC ciphering to avoid double ciphering employed on a point-to-point / point-to-multipoint bearer. It was agreed to send this issue to RAN WG2 asking their view on the complexity of introducing a selective encryption mechanism. **Siemens will provide a LS to RAN WG2 for e-mail discussion by 7 March 2003, approval by 14 March 2003**. TD S3-030156 was allocated for the approved LS.

TD S3-030076 MBMS security issues. This was introduced by Nokia. The text in section 2.1 concerning sessions should be discussed at a future meeting. The contribution was generally in line with earlier decisions in SA WG3, and the contribution was noted.

TD S3-030040 MBMS Security Framework and Pseudo-CR to 33.246. This was presented by Qualcomm and outlines some security goals for MBMS from the market view and describes the Key sets and example architecture for key distribution. It was questioned whether existing UICC could be used for this scheme. It was clarified that this mechanism could be applied without involvement of UICC, e.g. if secure storage in the ME is available, or running as an application on the UICC. An attack where a rogue terminal replaces SK_RAND with SK and sends on was raised. This would need further study. Qualcomm were thanked for the presentation which was noted.

TD S3-030053 Some consideration about MBMS re-keying across various reference points. This was provided as a background doc to TD S3-030054 and was noted and delegates were asked to read this off line for more detail.

TD S3-030054 Text proposal for MBMS re-keying based on LKH principles. This was introduced by Samsung Electronics. The main point in section 5.2 was discussed and it was agreed to add this text to the draft TS adding an editors note that LHK mechanism is only one possible solution.

TD S3-030063 Key distribution at Application Layer for MBMS. This was introduced by Ericsson and is updated from the contribution to the previous SA WG3 meeting with message flows modified in section 5. The Ericsson preferred solution is with either HTTP or RTSP, Digest AKA and MIKEY. **It was agreed to produce a LS to SA WG4 for comments by 7 March 2003 and approval by 14 March 2003.** A. Escott agreed to write a draft LS and send to the e-mail list for approval.

TD S3-030122 PayTV model. This was a late contribution, and was briefly presented by Oberthur on behalf of Gemplus and Oberthur. Delegates were asked to consider the scheme described for consideration at future meetings. The contribution was then noted.

6.22 Guide to 3G security (TR 33.900)

There were no specific contributions under this agenda item.

7 Review and update of work programme

Due to lack of time this agenda item could not be dealt with at the meeting. SA WG3 delegates, and in particular Work Item rapporteurs were asked to provide any updates to the Secretary on Work Items, using TD S3-030044 as a basis for comments. **The SA WG3 Secretary requires this information by Wednesday 5 March 2003.**

8 Future meeting dates and venues

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#28	06 - 09 May 2003	Berlin	European 'Friends of 3GPP'
S3#29	15-18 July 2003	San Francisco	3GPP2
S3#30	7-10 October 2003	Europe (TBD)	European 'Friends of 3GPP'

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#9	20 - 22 May 2003	Vienna	European 'Friends of 3GPP'
SA3 LI-#10	23 - 25 September 2003	US	TBA
SA3 LI-#11	18-20 November 2003	London	DTI

TSGs RAN/CN/T and SA Plenary meeting schedule

TSG RAN/CN/T #18	3 – 6 December	New Orleans USA	NA 'Friends of 3GPP'
TSG SA #18	9 – 12 December	New Orleans USA	NA 'Friends of 3GPP'
Meeting	**2003**	**Location**	**Primary Host**
TSG RAN/CN/T #19	11-14 March (tba)	UK	European 'Friends of 3GPP'
TSG SA #19	17-20 March	UK	European 'Friends of 3GPP'
TSG RAN/CN/T #20	3-6 June	Hämeenlinna, FIN	Nokia
TSG SA #20	9-12 June	Hämeenlinna, FIN	Nokia
TSG RAN/CN/T #21	16-19 September	Germany	
TSG SA #21	22-25 September	Germany	
TSG RAN/CN/T #22	9-12 December	US	
TSG SA #22	15-18 December	US	
Meeting	**2004 DRAFT TBD**	**Location**	**Primary Host**
TSG#23	March 9-12 & 15-18	China	
TSG#24	June 1-4 & 7-10	Korea	
TSG#25	7-10 & 13-16 September	USA	
TSG#26	7-10 & 13-16 December	To Be Decided	

9 Any other business

There were no specific contributions under this agenda item.

Frequency of SA WG3 meetings and deadline for submission of documents:

Due to the problem of lack of time at the recent SA WG3 meetings, some documents had been left for e-mail discussion, or postponed for re-submission and discussion at the following meeting. It was questioned whether SA WG3 need to meet more often, or whether a new system should be introduced in order to control the deadline for submission of documents in good time for delegates to consult within their companies and provide response contributions which can still meet the "late document" deadline. V. Niemi agreed to start an e-mail discussion on this topic.

AP 27/05: V. Niemi to lead an e-mail discussion on meeting frequency and document submission deadlines.

It was noted that the positions for Chairmanship and 2 Vice-Chairmanships were expiring and candidatures were invited. An e-mail will be sent to the e-mail list, by MCC, explaining the requirements and details on how to apply for these positions. If there are more candidates than available positions, then a Vote will be held at the next meeting to elect the Chairman and Vice Chairmen. Results of elections will be subject to PCG endorsement.

10 Close of meeting

The Chairman, M. Walker handed the chairmanship over to the Vice Chairman, V. Niemi on the third day of the meeting. V. Niemi thanked the delegates present for their hard work at the meeting and the Host, ETSI, for the accommodation and meeting facilities. He then closed the meeting.

Annex A: List of attendees at the SA WG3#26 meeting and Voting List

A.1 List of attendees

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Jorge Abellan Sevilla	SchlumbergerSema	jorge.abellan@slb.com		+33 1 46 00 59 33	+33 1 46 00 59 31	FR	ETSI
Mr. Palekar Ashwin	MICROSOFT EUROPE SARL	ashwinp@microsoft.com		+1 425 7035144	+1 425 7067329	FR	ETSI
Mr. Nigel Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	+44 7785 31 86 31	+44 1 256 790 169	+44 1 256 790 190	GB	ETSI
Mr. Colin Blanchard	BT Group Plc	colin.blanchard@bt.com	+44 7711 191835	+44 1473 605353	+44 1473 623910	GB	ETSI
Mr. Marc Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.com		+32 14 25 34 11	+32 14 25 33 39	BE	ETSI
Mr. Krister Boman	ERICSSON L.M.	krister.boman@erv.ericsson.se		+46 31 747 4055	+46 31 7470 5050	SE	ETSI
Mr. Charles Brookson	DTI	mail@zeata.demon.co.uk	+44 7956 567 102	+44 20 7215 3691	+44 20 7931 7194	GB	ETSI
Mr. Holger Butscheidt	BMWi	Holger.Butscheidt@RegTP.de		+49 6131 18 2224	+49 6131 18 5613	DE	ETSI
Mr. Mauro Castagno	TELECOM ITALIA S.p.A.	mauro.castagno@tilab.com		+39 0112285203	+39 0112287056	IT	ETSI
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp		+81 467 41 2181	+81 467 41 2185	JP	ARIB
Mr. Per Christoffersson	TeliaSonera AB	per.e.christoffersson@telia.se		+46 705 925100		SE	ETSI
Mr. Ashishkumar ramdas Dhawane	C-DOT	ashish@cdotb.ernet.in		+91 80 2282168	+91 80 2282168	IN	ETSI
Mr. Kevin England	mmO2 plc	kevin.england@o2.com		+447710016799		GB	ETSI
Dr. Adrian Escott	3	adrian.escott@three.co.uk		+44 7866 600924	+44 1628 766012	GB	ETSI
Mr. John B Fenn	SAMSUNG Electronics	johnbfenn@aol.com				GB	ETSI
Mr. Louis Finkelstein	MOTOROLA JAPAN LTD	louisf@labs.mot.com		+1 847 576 4441	+1 847 538 4593	JP	ARIB
Mr. Jean-Bernard Fischer	OBERTHUR CARD SYSTEMS S.A.	jb.fischer@oberthurcs.com		+33 141 38 18 93	+33 141 38 48 23	FR	ETSI
Dr. Eric Gauthier	GSM Association	eric.gauthier@orange.ch		+41 21 216 53 08	+41 21 216 18 88	IE	OTHER
Mr. Robert Gross	TruePosition Inc.	rlgross@trueposition.com		+1 610 680 1119	+1 610 680 1199	US	ETSI
Mr. Mark Gullett	HEWLETT-PACKARD France	mark.gullett@hp.com		+17194815723	+17194815724	FR	ETSI
Dr. Thomas Hardjono	VeriSign Switzerland SA	thardjono@verisign.com	+1-781-883-2636	+1-781-245-6996	+1-781-729-9559	CH	ETSI
Ms. Tao Haukka	Nokia Korea	tao.haukka@nokia.com		+358 40 5170079		KR	TTA
Mr. Philip Hawkes	QUALCOMM EUROPE S.A.R.L.	phawkes@qualcomm.com		+61-2-9817-4188	+61-2-9817-5199	FR	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@siemens.com		+49 8963 641494	+49 8963 648000	DE	ETSI
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vodafone.com	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB	ETSI
Mr. Yu Inamura	NTT DoCoMo Inc.	jane@mml.yrp.nttdocomo.co.jp		+81-468-40-3809	+81-468-40-3364	JP	ARIB
Mr. Geir Koien	TELENOR AS	geir-myrdahl.koien@telenor.com		+47 90752914	+47 37 04 52 84	NO	ETSI
Mr. Alex Leadbeater	BT Group Plc	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. Michael Marcovici	Lucent Technologies	marcovici@lucent.com		+1 630 979 4062	+1 630 224 9955	DE	ETSI
Mr. Sebastien Nguyen Ngoc	ORANGE FRANCE	sebastien.nguyenngoc@rd.francetelecom.com		+33 1 45 29 47 31	+33 1 45 29 65 19	FR	ETSI
Mr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com		+358 50 4837 327	+358 9 437 66850	FI	ETSI
Mr. Petri Nyberg	TeliaSonera AB	petri.nyberg@sonera.com		+358 204066824	+358 2040 0 3168	SE	ETSI

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Anand Palanigounder	Nortel Networks	anand@nortelnetworks.com		+1 972 684 4772	+1 972 685 3123	US	T1
Miss Mireille PAULIAC	GEMPLUS Card International	mireille.pauliac@GEMPLUS.COM		+33(0)442365441	+33(0)442365792	FR	ETSI
Mr. Maurice Pope	ETSI Secretariat	maurice.pope@etsi.org	+33 (0)6 07 59 08 49	+33 4 92 94 42 59	+33 4 92 38 52 59	FR	ETSI
Mr. Jose Puthenkulam	INTEL CORPORATION SARL	jose.p.puthenkulam@intel.com		+1 503 264 6121	+1 503 264 8154	FR	ETSI
Mr. Sanjay Razdan	C-DOT	sanjay@cdotb.ernet.in		+91 80 2282168	+91 80 2282168	IN	ETSI
Mr. Rhys Robinson	TruePosition Inc.	rrobinson@TruePosition.com	+1 610-209-0832	+1 610-680-2119	+1 610-680-1199	US	ETSI
Mr. Stefan Schroeder	T-MOBILE DEUTSCHLAND	STEFAN.SCHROEDER@T-MOBILE.DE		+49 228 936 3312	+49 228 936 3309	DE	ETSI
Mr. Ramachandran Subramanian	QUALCOMM EUROPE S.A.R.L.	rsubrama@qualcomm.com		+1 858 651 2350	+1 858 651 2880	FR	ETSI
Mr. Benno Tietz	Vodafone D2 GmbH	benno.tietz@vodafone.com		+49 211 533 2168	+49 211 533 1649	DE	ETSI
Mr. Vesa Torvinen	ERICSSON L.M.	vesa.torvinen@lmf.ericsson.se	+358 407230822	+358407230822	+35892993838	SE	ETSI
Ms. Annelies Van Moffaert	ALCATEL S.A.	annelies.van_moffaert@alcatel.be		+32 3 240 83 58	+32 3 240 48 88	FR	ETSI
Mr. Tommi Viitanen	Nokia Telecommunications Inc.	tommi.viitanen@nokia.com		+358405131090	+358718074383	US	T1
Prof. Michael Walker	VODAFONE Group Plc	mike.walker@vodafone.com	+44 77 85 277 687	+44 1635 673 886	+44 1634 234939	GB	ETSI
Ms. Monica Wifvesson	ERICSSON L.M.	monica.wifvesson@emp.ericsson.se		+46 46 193634	+46 46 231650	SE	ETSI
Mr. Berthold Wilhelm	BMWi	berthold.wilhelm@regtp.de		+49 681 9330 562	+49 681 9330 725	DE	ETSI
Dr. Raziq Yaqub	Toshiba Corporation	ryaqub@tari.toshiba.com	+1-908-319-8422	+1 973 829 2103	+1-973-829-5601	JP	ARIB
Mr. Yanmin Zhu	SAMSUNG Electronics	zym@samsung.co.kr		+861068427711	+861068481898	GB	ETSI

48 attendees

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #25, #26 and #27, the following companies are eligible to vote at SA WG3 meeting #28:

Company	Country	Status	Partner Org
3	GB	3GPPMEMBER	ETSI
ALCATEL S.A.	FR	3GPPMEMBER	ETSI
AT&T Corp.	US	3GPPMEMBER	T1
AT&T Wireless Services, Inc.	US	3GPPMEMBER	T1
BT Group Plc	GB	3GPPMEMBER	ETSI
BUNDESMINISTERIUM FUR WIRTSCHAFT	DE	3GPPMEMBER	ETSI
Centre for Development of Telematics	IN	3GPPMEMBER	ETSI
Cisco Systems France	FR	3GPPMEMBER	ETSI
Communications-Electronics Security Group	GB	3GPPMEMBER	ETSI
DTI - Department of Trade and Industry	GB	3GPPMEMBER	ETSI
Ericsson Incorporated	US	3GPPMEMBER	T1
GEMPLUS Card International	FR	3GPPMEMBER	ETSI
HEWLETT-PACKARD France	FR	3GPPMEMBER	ETSI
INTEL CORPORATION SARL	FR	3GPPMEMBER	ETSI
Lucent Technologies	US	3GPPMEMBER	T1
Lucent Technologies Network Systems UK	GB	3GPPMEMBER	ETSI
Lucent Technologies Networks System GmbH	DE	3GPPMEMBER	ETSI
MICROSOFT EUROPE SARL	FR	3GPPMEMBER	ETSI
Mitsubishi Electric Co.	JP	3GPPMEMBER	ARIB
mmO2 plc	GB	3GPPMEMBER	ETSI
Motorola Inc.	US	3GPPMEMBER	T1
MOTOROLA JAPAN LTD	JP	3GPPMEMBER	ARIB
MOTOROLA Ltd	GB	3GPPMEMBER	ETSI
NOKIA Corporation	FI	3GPPMEMBER	ETSI
NOKIA KOREA	KR	3GPPMEMBER	TTA
Nokia Telecommunications Inc.	US	3GPPMEMBER	T1
NORTEL NETWORKS (EUROPE)	GB	3GPPMEMBER	ETSI
Nortel Networks (USA)	US	3GPPMEMBER	T1
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
OBERTHUR CARD SYSTEMS S.A.	FR	3GPPMEMBER	ETSI
ORANGE FRANCE	FR	3GPPMEMBER	ETSI
ORANGE PCS LTD	GB	3GPPMEMBER	ETSI
POLKOMTEL S.A.	PL	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
Research In Motion Limited	CA	3GPPMEMBER	ETSI
Samsung Electronics Ind. Co., Ltd.	KR	3GPPMEMBER	TTA
SAMSUNG Electronics Research Institute	GB	3GPPMEMBER	ETSI
SchlumbergerSema - Schlumberger Systèmes S.A	FR	3GPPMEMBER	ETSI
SIEMENS AG	DE	3GPPMEMBER	ETSI
SIEMENS ATEA NV	BE	3GPPMEMBER	ETSI
SSH Communications Security Corp	FI	3GPPMEMBER	ETSI
T-MOBILE DEUTSCHLAND	DE	3GPPMEMBER	ETSI
TELECOM ITALIA S.p.A.	IT	3GPPMEMBER	ETSI

Company	Country	Status	Partner Org
Telefon AB LM Ericsson	SE	3GPPMEMBER	ETSI
Telenor AS	NO	3GPPMEMBER	ETSI
TeliaSonera AB	SE	3GPPMEMBER	ETSI
Toshiba Corporation, Digital Media Network Company	JP	3GPPMEMBER	ARIB
TruePosition Inc.	US	3GPPMEMBER	ETSI
VeriSign Switzerland SA	CH	3GPPMEMBER	ETSI
Vodafone D2 GmbH	DE	3GPPMEMBER	ETSI
VODAFONE Group Plc	GB	3GPPMEMBER	ETSI

51 Individual Member Companies

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030001	Draft Agenda for SA WG3 meeting #27	SA WG3 Chairman	2	Approval		Approved
S3-030002	Draft Report of SA WG3 meeting #26	SA WG3 Secretary	4.1	Approval		Modified and approved -> version 1.0.0
S3-030003	Extract from Draft Report of meeting #18 - version 0.0.4 (revision marked)	SA WG3 Secretary	4.2	Information		Noted
S3-030004	LS on ECSD and Ciphering	TSG GERAN	6.6	Action		Reply in S3-030015
S3-030005	LS (from SA WG2) on management and regulatory requirements for Presence service	SA WG2	6.19	Action		Forwarded to S3-LI Group
S3-030006	LS from SA WG1: Having a Single USIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link	SA WG1	6.11	Action		Reply LS in S3-030145
S3-030007	LS from SA WG2: Proposed Confidentiality for IMS	SA WG2	6.19	Action		Response in S3-030168
S3-030008	Requirement to Allow Access to IMS by Means of SIM in 3G UEs	SA WG2	6.1	Action		Noted. SA decision awaited
S3-030009	SA WG2 response to “Response to IETF LS on Interoperability Issues and SIP in IMS”	SA WG2	6.1	Action		Noted
S3-030010	Reply LS (from SA WG5) on ‘New requirements about functionality to make subscription to different domains independent or linked based on operator decision’	SA WG5	5.1	Information		Noted
S3-030011	LS (from SA WG5) on bearer charging issues with use of HTTP for Rel 6	SA WG5	5.1	Information		Noted
S3-030012	Reply LS (from SA WG5) on Indication of call termination as a result of IST operation	SA WG5	6.7	Action		Further e-mail discussion required. Response LS in S3-020153
S3-030013	LS from TSG SA: Additional Release 5 work needed for Policy Control and Subscription Control of Media	TSG SA	6.1	Action		Related CR in S3-030115 - Response LS in S3-030116
S3-030014	Proposed WID update: 3GPP Generic User Profile Security	Lucent Technologies	6.18	Approval	S3-030154	Revised in S3-030154
S3-030015	LS on "A5/3 ciphering modes for ECSD" (response to LS to SA3 (GP-023402) on "ECSD and Ciphering")	SA WG3 (e-mail)	6.6	Approval		Approved by e-mail 29 Jan 2003
S3-030016	LS to 3GPP TSG SA3 regarding use of the “AMF” field to switch between multiple authentication algorithms	GSMA SG#45	6.5	Information		Response LS in S3-030134
S3-030017	3GPP/IETF Release 6 Workshop Major Conclusions	Stephen Hayes IETF Coordinator	5.2	Information		V Niemi to consult S. Hayes on follow-up to the Workshop conclusions
S3-030018	IETF/3GPP Release 6 Workshop notes	V Niemi (SA WG3 Vice Chairman)	5.2	Discussion		Noted
S3-030019	LS from TSG GERAN: Use of Kc in the Uplink TDOA location method	TSG GERAN		Action	S3-030038	WITHDRAWN - Updated in S3-030038 with Slides
S3-030020	LS (from SA WG1) on T2 proposal for GUP requirements- UE Data access and Backwards Compatibility	SA WG1	6.18	Action		e-mail group to discuss and provide response LS in S3-030155
S3-030021	Response LS (from SA WG1) on Indication of call termination as a result of IST operation	SA WG1	6.7	Information		Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030022	LS (from SA WG2) on use of HTTP between UE and AS in the IMS	SA WG2	6.19	Action		Response LS in S3-030148
S3-030023	LS (from SA WG2) on Multiple IMS registrations	SA WG2	6.1	Action		Response in S3-030117
S3-030024	Reply to LS from SA5 (from SA WG2) on bearer charging issues with use of HTTP for Rel 6	SA WG2	5.1	Information		Noted
S3-030025	LS (from SA WG5) on management and regulatory requirements for Presence service	SA WG5	6.19	Information		Noted
S3-030026	LS from T WG2: Response to LS S1-022388. "Having a Single (U)SIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link"	T WG2		Action	S3-030027	WITHDRAWN - Revised version provided in S3-030027
S3-030027	LS from T WG2: Response to LS S1-022388. "Having a Single (U)SIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link"	T WG2	6.11	Action		Guidance requested from SA WG3. Response in S3-030145
S3-030028	Draft TS 33.246 v0.0.3: Security of Multimedia Broadcast/Multicast Service	Rapporteur	6.21	Discussion		Reviewed and noted. Used as basis for further contributions
S3-030029	Security Requirements for 3G-WLAN Interworking	Intel, Cisco	6.11	Discussion / Decision		Discussed. Some material added draft TS and some as a basis for LS to IEEE
S3-030030	PKI Deployment Models for PEAP	Intel, Cisco	6.11	Discussion		Presented for information. Noted
S3-030031	WLAN-UE Functionality Split : Request for Work Item	Intel, Toshiba	6.11	Discussion		Late contribution. Briefly presented. Noted
S3-030032	Proposed CR to 33.203: Malicious UE bypassing the P-CSCF (Rel-5)	Nokia	6.1	Approval	S3-030119	(Document renumbered after first ditribution as S3-020032). Revised with S3-030058 in S3-030119
S3-030033	Identity protection using P-TMSI for 3GPP/WLAN interworking	Thomson	6.11	Discussion		Noted (not presented)
S3-030034	Proposed CR to 33.210: Za-interface and roaming agreements (Rel-5)	Siemens	6.3	Approval	S3-030127	Revised in S3-030127
S3-030035	Proposed CR to 33.210: Za-interface and roaming agreements (Rel-6)	Siemens	6.3	Approval	S3-030128	Revised in S3-030128
S3-030036	Alternative proposals for subscriber certificate bootstrapping	Alcatel	6.9	Discussion		Text to be included in TS (S3-030050)
S3-030037	Consideration of CA generating public/private key pairs	Alcatel	6.9	Discussion		Alcatel to provide text for inclusion in draft TS (S3-030050)
S3-030038	LS from TSG GERAN: Use of Kc in the Uplink TDOA location method	TSG GERAN	6.6	Action		LS to GERAN in S3-030133
S3-030039	Security requirements for WLAN	Orange France	6.11	Discussion / Decision		Changes agreed to add to draft TS
S3-030040	MBMS Security Framework and Pseudo-CR to 33.246	Qualcomm	6.21	Presentation		Presented and noted
S3-030041	Provision of indication to the USIM that the authentication procedure is executed in the 3G-WLAN access context	Telenor	6.11	Discussion / Decision		Members asked to study and contribute. Noted
S3-030042	LS (from CN WG4) on clarification on the requirement for UE re-authentication initiated by HSS	CN WG4	6.1	Action		Response LS in S3-030120

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030043	LS (from CN WG1) on updated WID for emergency call enhancements for IP & PS based calls	CN WG1	5.1	Action		Response LS in S3-030112
S3-030044	3GPP Work Plan	SA WG3 Secretary	7	Action		Delegates/Rapporteurs to provide updates to secretary
S3-030045	Pseudo CR to 33.234: Change to the security requirement related to the storage of all long-term security credentials used for subcriber and network authentication	GemPlus	6.11	Discussion / Approval		Not agreed. Changes requirements on SIM and USIM
S3-030046	Handling invalid temporary identifiers	Nokia	6.11	Decision		Agreed that IMSI in clear should be prompted depending on UE. Not standardised
S3-030047	Proposed CR to 33.203: Remove error message as unprotected response (Rel-5)	Nokia	6.1	Approval		Rejected
S3-030048	Proposed CR to 33.203: Correction of the Port 2 definition for SA establishment (Rel-5)	Nokia	6.1	Approval	S3-030121	Annex H changes for off-line discussion to produce S3-030121
S3-030049	Proposed CR to 33.203: Add protected port into Via header (Rel-5)	Nokia	6.1	Approval	S3-030123	Revised in S3-030123
S3-030050	Bootstrapping of application security from 3G AKA and support for subscriber certificates	Nokia, Siemens	6.9	Discussion / Decision		T Haukka agreed to be Editor - to add text agreed at meeting
S3-030051	Draft TS Table of Contents for “Bootstrapping and Support for Subscriber Certificates”	Nokia, Siemens	6.9	Discussion / Decision		Text to be included in TS (S3-030050)
S3-030052	Proposed CR to 33.203: Ensuring the deletion of unwanted SAs (Rel-5)	3	6.1	Approval	S3-030124	Revised in S3-030124
S3-030053	Some consideration about MBMS re-keying across various reference points	Samsung Electronics	6.21	Discussion / Decision		Background for S3-030054 - Noted
S3-030054	Text proposal for MBMS re-keying based on LKH principles	Samsung Electronics	6.21	Discussion / Decision		5.2 added to draft TS as editors note possible solution
S3-030055	Proposed CR to 33.203: Clarification of the use of ISIM and USIM for IMS access (Rel-5)	Ericsson	6.1	Approval		Approved. LS in S3-030125
S3-030056	Security solution for IMS-related HTTP services	Siemens	6.19	Discussion / Decision		Discussed. LS to be provided for e-mail approval
S3-030057	Means to counter IMS P-CSCF bypassing	Siemens	6.1	Discussion / Decision		Discussed. CRs in S3-030032 and S3-030058 revised into single CR
S3-030058	Proposed CR to 33.203: Malicious UE bypassing the P-CSCF (Rel-5)	Siemens	6.1	Discussion / Decision		Revised with S3-030032 in S3-030119
S3-030059	Draft TS 33.abc: Presence Service; Security. Version 0.3.0	Rapporteur	6.19	Discussion		Presented and noted. For update with comments
S3-030060	HTTP authentication	Nokia	6.19	Discussion / Decision		Discussed. LS to be provided for e-mail approval
S3-030061	Comparison of MBMS security scenarios	Ericsson	6.21	Discussion		In line with SA3 decisions - Noted
S3-030062	UE considerations when evaluating MBMS security at application layer vs. network layer	Ericsson	6.21	Discussion		In line with SA3 decisions - Noted
S3-030063	Key distribution at Application Layer for MBMS	Ericsson	6.21	Discussion		LS to be agreed by e-mail by 14 March 2003

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030064	MBMS: Key Encryption Keys requirements	Siemens	6.21	Discussion / Decision		Postponed. Author to input into next meeting
S3-030065	"AMF" field to switch between multiple authentication algorithms	Siemens	6.5	Discussion / Decision		Attached to LS in S3-030134
S3-030066	Comments to MBMS security requirements – Siemens	Siemens	6.21	Discussion		Editors notes to be added to draft TS
S3-030067	Impacts due to the use of SIM for IMS access	GEMPLUS Card International, OBERTHUR Card Systems	6.1	Discussion / Approval	S3-030106	Revised in S3-030106 to add companies and editorial changes
S3-030068	End-to-end authentication of Presence subscriptions in Pw	Ericsson	6.19	Discussion / Decision		Agreed with modifications. Editor to add to draft TS
S3-030069	The use of HTTP in Presence/IMS	Ericsson	6.19	Discussion / Decision		Discussed. LS to be provided for e-mail approval
S3-030070	Confidentiality in Presence	Ericsson	6.19	Discussion / Decision		Need to study Rel-5 access problems further. Proposals added to TS as editors note
S3-030071	Parameters in subscriber certificate and subscriber profile supporting operator control and service differentiation	Nokia	6.9	Discussion		Noted as basis to proposal in S3-030073. E-mail discussion to be led by Nokia
S3-030072	NAF-BSF (D interface) protocol	Nokia	6.9	Discussion		Noted as basis to proposal in S3-030073. E-mail discussion to be led by Nokia. LS to CN4 in S3-030131
S3-030073	Protocol B: Subscriber Certificate Enrollment based on Bootstrapping	Nokia	6.9	Discussion / Decision		Requirements to be included in TS (S3-030050) and Solution#1 discussed with Alcatel solution and included in an Annex.
S3-030074	MBMS: Reuse of RAN/GERAN ciphering functions	Siemens	6.21	Discussion / Decision		Forwarded to RAN WG4. LS by e-mail inS3-030156
S3-030075	Proposed CR to 33.210: Clarification to the re-keying aspects of network domain security (Rel-5)	Lucent Technologies	6.3	Approval	S3-030129	Revised in S3-030129
S3-030076	MBMS security issues	Nokia	6.21	Discussion / Decision		In line with SA3 decisions - Noted
S3-030077	Pseudo-CR to 33.234: Editorial changes to WLAN	Ericsson	6.11	Approval		Editor to add to draft TS
S3-030078	Pseudo-CR to 33.234: Update of Security Requirements	Ericsson	6.11	Approval		Mods made to proposed changes
S3-030079	3G-WLAN Threat Analysis	Ericsson	6.11	Discussion / Approval		Agreed
S3-030080	WLAN Link Layer Security Requirements	Ericsson	6.11	Discussion / Approval		Editors notes added and LS to IEEE in S3-030140
S3-030081	WLAN – Certificate-Based Protection of IMSI for EAP-SIM/AKA	Ericsson	6.11	Discussion / Decision		Level 3 protection not considered necessary at present.
S3-030082	NDS/AF TS TOC proposal	Nokia, Siemens, SSH, T-Mobile	6.4	Discussion / Approval		Noted. Members asked to provide input to the TS

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030083	Introduction and requirements for manual cross-certification within NDS/AF	Nokia, Siemens, SSH, T-Mobile	6.4	Discussion / Decision		Principles accepted. Noted
S3-030084	How to mitigate the Interleaving attack and reduce the trust in the Authenticator	Ericsson	6.19	Discussion / Decision		LS to be agreed by e-mail by 21 March 2003 in S3-030148
S3-030085	Requirements list for UEA2 and UIA2	Vodafone	6.5	Approval		Updated proposal in LS to SAGE in S3-030135
S3-030086	Provisional work plan for the design of the 3GPP confidentiality and integrity algorithms UEA2 and UIA2	Vodafone / SAGE Chairman	6.5	Approval		Agreed - forwarded to TSG SA in S3-030136
S3-030087	Security issue with multiple PDP Contexts in GPRS	Vodafone	6.5	Discussion / Decision		More information required - LS in S3-030164
S3-030088	Security Issues of Having a Single (U)SIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link	Toshiba America Research Inc.	6.11	Discussion		Late contribution. Briefly presented. Noted
S3-030089	Proposed CR to 33.108: CS Section for 33.108 (Rel-6)	SA WG3-LI Group	4.3	Approval	S3-030110	Modified in S3-030110
S3-030090	Proposed CR to 33.107: Stereo delivery to LEMF (Rel-4)	SA WG3-LI Group	4.3	Approval		Rejected
S3-030091	Proposed CR to 33.107: Stereo delivery to LEMF (Rel-5)	SA WG3-LI Group	4.3	Approval		Rejected
S3-030092	Proposed CR to 33.108: Adjustments to the requirements on the delivery of the intercepted RT data over TCP (Rel-6)	SA WG3-LI Group	4.3	Approval	S3-030111	Modified in S3-030111
S3-030093	Handling of Issues associated with S3LI CRs	SA WG3-LI Group	4.3	Discussion / Action		SA WG3 would continue to make minor changes where necessary, and the LI Group were encouraged to improve the quality and correctness of their CRs
S3-030094	Proposed CR to 33.108: Coding of ASN.1 parameters of the type OCTET STRING (Rel-5)	SA WG3-LI Group	4.3	Approval		Approved
S3-030095	Proposed CR to 33.108: Coding of ASN.1 parameters of the type OCTET STRING (Rel-6)	SA WG3-LI Group	4.3	Approval		Approved
S3-030096	Liaison Statement (from SA WG3 LI group) on WI IMS Presence Interception	SA WG3-LI Group	4.3	Action		Noted - unsure about request for S1 to comment on LI aspects of Presence
S3-030097	Proposed WID: Lawful Interception in the 3GPP Rel-6 architecture	SA WG3-LI Group	4.3	Approval		Approved. SA Plenary dates #22, not #26
S3-030098	Proposed CR to 33.108: Changes to meet international LI Requirements (Rel-5)	SA WG3-LI Group	4.3	Approval		RETURN LI GROUP TO CLARIFY
S3-030099	Proposed CR to 33.108: Incorrect ASN.1 object tree (Rel-5)	SA WG3-LI Group	4.3	Approval		Approved
S3-030100	LS (from SA WG3 LI Group) on Possible overlap of the scopes in the 3GPP TS 33.108 and DES/SEC-003020	SA WG3-LI Group	4.3	Information		Noted
S3-030101	Proposed CR to 33.108: Changes to meet international LI Requirements (Rel-6)	SA WG3-LI Group	4.3	Approval		RETURN LI GROUP TO CLARIFY
S3-030102	EAP support in smartcards and security requirements in WLAN authentication	SchlumbergerSema	6.11	Discussion / Approval		Late contribution. Briefly presented

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030103	GTP updates for MSISDN targeted LI	Nortel Networks	4.3	Discussion / Approval		Late contribution. Agreed to forward to LI group for consideration
S3-030104	Profiling of IKE and Certificates for use within NDS/AF	Nokia, Siemens, SSH, T-Mobile	6.4	Information		Late contribution. Delegates asked to provide comment to M Blommaert 2 weeks before next meeting
S3-030105	Openness of Rel6 IMS network: security methods required	Nokia	6.1	Discussion		Late contribution.
S3-030106	Impacts due to the use of SIM for IMS access	Gemplus, Oberthur, SchlumbergerSema	6.1	Discussion / Approval		Agreed principles. LS in S3-030126
S3-030107	Draft Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #1/03 on Lawful Interception	SA WG3-LI Group	4.3	Information		Late contribution. Noted
S3-030108	Guidelines for selecting between a bridge CA and a direct cross certification model for NDS/AF	SSH, Siemens, Nokia	6.4	Discussion		Late contribution. Noted
S3-030109	Revised GERAN A/Gb mode security enhancements WID	Vodafone	6.6	Approval		Approved
S3-030110	Proposed CR to 33.108: CS Section for 33.108 (Rel-6)	SA WG3-LI Group	4.3	Approval		Approved
S3-030111	Proposed CR to 33.108: Adjustments to the requirements on the delivery of the intercepted RT data over TCP (Rel-6)	SA WG3-LI Group	4.3	Approval		Approved
S3-030112	Reply to LS (N1-030271/S3-030043) on updated WID for emergency call enhancements for IP & PS based calls	SA WG3	5.1	Approval		Approved
S3-030113	GERAN A/Gb mode security enhancements	Vodafone	6.6	Information		Late contribution. Noted members to comment to author
S3-030114	LS (from SA WG2) on WLAN/3GPP Simultaneous Access	SA WG2	6.11	Action		Late contribution. E-mail discussion for response in S3-030169
S3-030115	CR to 23.228: Handling of SDP manipulation issue in stage-2 specifications	TSG SA	6.1	Information		For Info with S3-030013. Noted
S3-030116	SA3 response on the "Additional Release 5 work needed for Policy Control and Subscription Control of Media"	SA WG3	6.1	Approval		Approved
S3-030117	Response to LS (S2-030374) on Multiple IMS registrations	SA WG3	6.1	Approval		Approved (sent to SA WG2 immediately)
S3-030118	LS (from GSMA SG) to 3GPP TSG SA3 regarding synchronisation of GGSNs and Gi firewalls	GSMA SG	6.5	Action		Late contribution
S3-030119	CR produced from S3-030032 and S3-030058	Nokia, Siemens	6.1	Approval		Approved
S3-030120	Response LS to S3-030042: Reply LS on clarification on the requirement for UE re-authentication initiated by HSS	SA WG3	6.1	Approval	S3-030159	Updated in S3-030159
S3-030121	Proposed CR to 33.203: Correction of the Port 2 definition for SA establishment (Rel-5)	Nokia	6.1	Approval	S3-030170	For e-mail approval bt 5 March 2003 (Tao) - Approved version in S3-030170
S3-030122	PayTV model	Gemplus, Oberthur	6.21	Discussion		Late contribution. Briefly presented and noted. Delegates to consider off-line

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030123	Proposed CR to 33.203: Add protected port into Via header (Rel-5)	Nokia	6.1	Approval	S3-030158	Updated in s3-030158
S3-030124	Proposed CR to 33.203: Ensuring the deletion of unwanted SAs (Rel-5)	3	6.1	Approval		Approved
S3-030125	LS to SA1, SA2, CN1, T3: Ericsson	SA WG3	6.1	Approval	S3-030160	Updated in S3-030160
S3-030126	LS on “Requirement to allow IMS access by means of SIM”	SA WG3	6.1	Approval	S3-030161	Updated in S3-030161
S3-030127	Proposed CR to 33.210: Za-interface and roaming agreements (Rel-5)	Siemens	6.3	Approval		Approved
S3-030128	Proposed CR to 33.210: Za-interface and roaming agreements (Rel-6)	Siemens	6.3	Approval		Approved
S3-030129	Proposed CR to 33.210: Clarification to the re-keying aspects of network domain security (Rel-5)	Lucent Technologies	6.3	Approval	S3-020162	Updated in S3-030162
S3-030130	Proposed CR to 33.210: Clarification to the re-keying aspects of network domain security (Rel-6)	Lucent Technologies	6.3	Approval	S3-020163	Updated in S3-030163
S3-030131	LS on "Support for subscriber certificates"	SA WG3	6.9	Approval		Approved
S3-030132	OCG#19 Document 21: Proofing of products against crime	C Brookson		Information		Noted
S3-030133	Reply LS on security issues regarding Uplink TDOA location method	SA WG3	6.6	Approval	S3-030152	Updated in S3-030152
S3-030134	Reply LS on “the use of the “AMF” field to switch between multiple authentication algorithms”	SA WG3	6.5	Approval		Approved
S3-030135	LS to ETSI SAGE on Requirements list for UEA2 and UIA2	SA WG3	6.5	Approval		Approved
S3-030136	LS to TSG SA: Funding for UEA2/UIA2 - Per	SA WG3	6.5	Approval		Approved
S3-030137	N4-030172: CR to 29.060 Controlling the creation of multiple PDP Contexts	Vodafone	6.5	Information		Noted for information
S3-030138	LS to CN WG4 - LS on security issues regarding multiple PDP contexts in GPRS	SA WG3	6.5	Approval	S3-030164	Updated in S3-030164
S3-030139	Updated WID: Network Domain Security; Authentication Framework (NDS/AF)	Nokia	6.4	Approval		Approved
S3-030140	Draft LS on interworking between 3GPP and IEEE 802.11 systems	SA WG3	6.11	Approval	S3-030166	Updated in S3-030166
S3-030141	LS to SA WG2 on 802.11i issues - Krister	SA WG3	6.11	Approval	S3-030167	Updated in S3-030167
S3-030142	Terminal Security: Requirements for a Secure Identity (v4) - A draft discussion document	C Brookson		Information		Late contribution. Noted
S3-030143	LS from T WG3: Response to LS S1-022388: “Having a Single USIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link”	T WG3	6.11	Information		Late contribution. Noted
S3-030144	LS from T WG3: Request for Information Regarding WLAN Interworking Impacts to UICC applications	T WG3	6.11	Action		Late contribution. Postponed
S3-030145	LS to SA WG1, T WG2: Study of UE Functionality Split Security Issues for Release 6	SA WG3	6.11	Approval	S3-030165	Updated in S3-030165
S3-030146	TSG-SA2/SA3 Joint meeting MBMS REPORT	SA WG2	4.4	Information		Working assumption not agreed, encryption will not be done at radio level was endorsed. Report reviewed and noted.

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030147	LS to SAGE on key derivation for IMS-based application services	SA WG3	6.19	Approval		Approved
S3-030148	Response to LS (S2-030445) on use of HTTP between UE and AS in the IMS	SA WG3	6.19	E-mail Approval		Approval by 21/03/2003
S3-030149	SA3 response on the “Proposed Confidentiality for IMS”	SA WG3	6.19	Approval	S3-030168	Updated in S3-030168
S3-030150	Draft TS ab.cde NDS/AF version 0.1.0	Rapporteur	6.4	Information		Noted
S3-030151	Pseudo-CR to 33.234: Change to the security requirement related to the storage of all long-term security credentials used for subcriber and network authentication	GemPlus		Approval		Approved to add to draft TS
S3-030152	Reply LS on security issues regarding Uplink TDOA location method	SA WG3	6.6	Approval		Approved
S3-030153	Reply LS on Indication of call termination as a result of IST operation (Marc)	SA WG3	6.7	E-mail Approval		Approval by 14/03/2003
S3-030154	Proposed WID update: 3GPP Generic User Profile Security	Lucent Technologies	6.18	Approval		Approved
S3-030155	Response LS to S3-030020 (Brad Owen)	SA WG3	6.18			Approval by 28/03/2003
S3-030156	LS to RAN WG2: MBMS: Reuse of RAN/GERAN ciphering functions (Marc)	SA WG3	6.21	E-mail Approval		Approval by 14/03/2003
S3-030157	LS to SA WG4 MBMS (Adrian)	SA WG3	6.21	E-mail Approval		Approval by 14/03/2004
S3-030158	Proposed CR to 33.203: Add protected port into Via header (Rel-5)	Nokia	6.1	Approval		Approved
S3-030159	Response LS to S3-030042: Reply LS on clarification on the requirement for UE re-authentication initiated by HSS	SA WG3	6.1	Approval		Approved
S3-030160	LS to SA1, SA2, CN1, T3: Ericsson	SA WG3	6.1	Approval		Approved
S3-030161	LS on “Requirement to allow IMS access by means of SIM”	SA WG3	6.1	Approval		Approved
S3-030162	Proposed CR to 33.210: Clarification to the re-keying aspects of network domain security (Rel-5)	Lucent Technologies	6.3	Approval		Approved
S3-030163	Proposed CR to 33.210: Clarification to the re-keying aspects of network domain security (Rel-6)	Lucent Technologies	6.3	Approval		Approved
S3-030164	LS to CN WG4 - LS on security issues regarding multiple PDP contexts in GPRS	SA WG3	6.5	Approval		Approved
S3-030165	LS to SA WG1, T WG2: Study of UE Functionality Split Security Issues for Release 6	SA WG3	6.11	Approval		Approved
S3-030166	Draft LS on interworking between 3GPP and IEEE 802.11 systems	SA WG3	6.11	Approval		Approved
S3-030167	LS to SA WG2 on 802.11i issues - Krister	SA WG3	6.11	Approval		Approved
S3-030168	SA3 response on the “Proposed Confidentiality for IMS”	SA WG3	6.19	Approval		Approved
S3-030169	LS on WLAN/3GPP simultaneous access (P. Howard)	SA WG3	6.11	E-mail Approval		Approval by 28/03/2004
S3-030170	Proposed CR to 33.203: Correction of the Port 2 definition for SA establishment (Rel-5)	Nokia	6.1	Approval		Approved 7 March 2003 by e-mail
S3-030171	Response to LS (S2-030445) on use of HTTP between UE and AS in the IMS	SA WG3	6.19	E-mail Approval		Approved 21 March 2003 by e-mail

Annex C: Status of specifications under SA WG3 responsibility

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
Release 1999 GSM Specifications and Reports							
TR	01.31	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	8.0.0	R99	S3	WRIGHT, Tim	
TR	01.33	Lawful Interception requirements for GSM	8.0.0	R99	S3	MCKIBBEN, Bernie	
TS	01.61	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	8.0.0	R99	S3	WALKER, Michael	
TS	02.09	Security aspects	8.0.1	R99	S3	CHRISTOFFERSSON, Per	
TS	02.33	Lawful Interception (LI); Stage 1	8.0.1	R99	S3	MCKIBBEN, Bernie	
TS	03.20	Security-related Network Functions	8.1.0	R99	S3	NGUYEN NGOC, Sebastien	
TS	03.33	Lawful Interception; Stage 2	8.1.0	R99	S3	MCKIBBEN, Bernie	
Release 1999 3GPP Specifications and Reports							
TS	21.133	3G security; Security threats and requirements	3.2.0	R99	S3	CHRISTOFFERSSON, Per	
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	3.2.1	R99	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	3.0.0	R99	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	3.0.0	R99	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards).
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	3.0.0	R99	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031.
TS	23.035	Immediate Service Termination (IST); Stage 2	3.1.0	R99	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards).
TS	33.102	3G security; Security architecture	3.13.0	R99	S3	BLOMMAERT, Marc	
TS	33.103	3G security; Integration guidelines	3.7.0	R99	S3	BLANCHARD, Colin	
TS	33.105	Cryptographic Algorithm requirements	3.8.0	R99	S3	CHIKAZAWA, Takeshi	
TS	33.106	Lawful interception requirements	3.1.0	R99	S3	WILHELM, Berthold	
TS	33.107	3G security; Lawful interception architecture and functions	3.5.0	R99	S3	WILHELM, Berthold	
TS	33.120	Security Objectives and Principles	3.0.0	R99	S3	WRIGHT, Tim	
TR	33.901	Criteria for cryptographic Algorithm design process	3.0.0	R99	S3	BLOM, Rolf	
TR	33.902	Formal Analysis of the 3G Authentication Protocol	3.1.0	R99	S3	HORN, Guenther	
TR	33.908	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	3.0.0	R99	S3	WALKER, Michael	TSG#7: S3-000105=NP-000049
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	3.2.0	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
Release 4 3GPP Specifications and Reports							
TS	21.133	3G security; Security threats and requirements	4.1.0	Rel-4	S3	CHRISTOFFERSSON, Per	
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	4.1.0	Rel-4	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards).
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031.
TS	23.035	Immediate Service Termination (IST); Stage 2	4.1.0	Rel-4	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards).
TS	33.102	3G security; Security architecture	4.5.0	Rel-4	S3	BLOMMAERT, Marc	
TS	33.103	3G security; Integration guidelines	4.2.0	Rel-4	S3	BLANCHARD, Colin	
TS	33.105	Cryptographic Algorithm requirements	4.1.0	Rel-4	S3	CHIKAZAWA, Takeshi	
TS	33.106	Lawful interception requirements	4.0.0	Rel-4	S3	WILHELM, Berthold	
TS	33.107	3G security; Lawful interception architecture and functions	4.3.0	Rel-4	S3	WILHELM, Berthold	
TS	33.120	Security Objectives and Principles	4.0.0	Rel-4	S3	WRIGHT, Tim	
TS	33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	4.3.0	Rel-4	S3	ESCOTT, Adrian	2001-05-24: title grows MAP; see 33.210 for IP equivalent.
TR	33.901	Criteria for cryptographic Algorithm design process	4.0.0	Rel-4	S3	BLOM, Rolf	
TR	33.902	Formal Analysis of the 3G Authentication Protocol	4.0.0	Rel-4	S3	HORN, Guenther	
TR	33.903	Access Security for IP based services	none	Rel-4	S3	VACANT,	
TR	33.908	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	4.0.0	Rel-4	S3	WALKER, Michael	TSG#7: S3-000105=NP-000049
TR	33.909	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	4.0.1	Rel-4	S3	WALKER, Michael	TSG#7: Is a reference in 33.908. Was withdrawn, but reinstated at TSG#10.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	4.1.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.205	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	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE. 2002-06: clarified that deliverable is TS not TR.
TS	35.206	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	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TS	35.207	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	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TS	35.208	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	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TR	35.909	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	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	4.0.1	Rel-4	S3	WRIGHT, Tim	
TR	41.033	Lawful Interception requirements for GSM	4.0.1	Rel-4	S3	MCKIBBEN, Bernie	
TS	41.061	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	4.0.0	Rel-4	S3	WALKER, Michael	
TS	42.009	Security Aspects	4.0.0	Rel-4	S3	CHRISTOFFERSSON, Per	
TS	42.033	Lawful Interception; Stage 1	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
TS	43.020	Security-related network functions	4.0.0	Rel-4	S3	GILBERT, Henri	
TS	43.033	Lawful Interception; Stage 2	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
Release 5 3GPP Specifications and Reports							
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	5.0.0	Rel-5	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards).
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031.
TS	23.035	Immediate Service Termination (IST); Stage 2	5.1.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards).

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
TS	33.102	3G security; Security architecture	5.1.0	Rel-5	S3	BLOMMAERT, Marc	
TS	33.106	Lawful interception requirements	5.1.0	Rel-5	S3	WILHELM, Berthold	
TS	33.107	3G security; Lawful interception architecture and functions	5.5.0	Rel-5	S3	WILHELM, Berthold	
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	5.2.0	Rel-5	S3	WILHELM, Berthold	2001-12-04 Title changed from "Lawful Interception; Interface between core network and law agency equipment" (Berthold.Wilhelm@RegTP.de).
TS	33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	5.1.0	Rel-5	S3	ESCOTT, Adrian	2001-05-24: title grows MAP; see 33.210 for IP equivalent.
TS	33.201	Access domain security	none	Rel-5	S3	POPE, Maurice	
TS	33.203	3G security; Access security for IP-based services	5.4.0	Rel-5	S3	BOMAN, Krister	
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	5.2.0	Rel-5	S3	KOIEN, Geir	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210).
TR	33.900	Guide to 3G security	0.4.1	Rel-5	S3	BROOKSON, Charles	
TR	33.903	Access Security for IP based services	none	Rel-5	S3	VACANT,	
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.205	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	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE. 2002-06: clarified that deliverable is TS not TR.
TS	35.206	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	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE
TS	35.207	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	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE
TS	35.208	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	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE
TR	35.909	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	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	5.0.0	Rel-5	S3	WRIGHT, Tim	
TR	41.033	Lawful Interception requirements for GSM	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	
TS	42.033	Lawful Interception; Stage 1	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	
TS	43.020	Security-related network functions	5.0.0	Rel-5	S3	GILBERT, Henri	
TS	43.033	Lawful Interception; Stage 2	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	
Release 6 3GPP Specifications and Reports							
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	6.0.0	Rel-6	S3	WILHELM, Berthold	2001-12-04 Title changed from "Lawful Interception; Interface between core network and law agency equipment" (Berthold.Wilhelm@RegTP.de).
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	6.0.0	Rel-6	S3	KOIEN, Geir	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210).
TR	33.810	3G Security; Network Domain Security / Authentication Framework (NDS/AF); Feasibility Study to support NDS/IP evolution	6.0.0	Rel-6	S3	N, A	2002-07-22: was formerly 33.910.
TS	55.205	Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8	6.0.0	Rel-6	S3	WALKER, Michael	Not subject to export control.
TS	55.216	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 1: A5/3 and GEA3 specification	6.1.0	Rel-6	S3	N, A	
TS	55.217	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data	6.1.0	Rel-6	S3	N, A	
TS	55.218	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 3: Design and conformance test data	6.1.0	Rel-6	S3	N, A	
TR	55.919	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report	6.1.0	Rel-6	S3	N, A	

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

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WG status
33.108	007	-	Rel-5	Coding of ASN.1 parameters of the type OCTET STRING	F	5.2.0	S3-27	S3-030094	agreed
33.108	008	-	Rel-6	Coding of ASN.1 parameters of the type OCTET STRING	A	6.0.0	S3-27	S3-030095	agreed
33.108	009	-	Rel-6	CS Section for 33.108	B	6.0.0	S3-27	S3-030110	agreed
33.108	010	-	Rel-6	Adjustments to the requirements on the delivery of the intercepted RT data over TCP	F	6.0.0	S3-27	S3-030111	agreed
33.108	011	-	Rel-5	Incorrect ASN.1 object tree	F	5.2.0	S3-27	S3-030099	agreed
33.108	012	-	Rel-6	Incorrect ASN.1 object tree	A	6.0.0	S3-27	S3-030099	agreed
33.108	013	-	Rel-5	Correction to implementation of CR 005	F	5.2.0	S3-27	(Note 1)	
33.108	014	-	Rel-6	Correction to implementation of CR 005	A	6.0.0	S3-27	(Note 1)	
33.203	035	-	Rel-5	Clarification of the use of ISIM and USIM for IMS access	F	5.4.0	S3-27	S3-030055	agreed
33.203	036	-	Rel-5	Malicious UE bypassing the P-CSCF	F	5.4.0	S3-27	S3-030119	agreed
33.203	036	1	Rel-5	Malicious UE bypassing the P-CSCF	F	5.4.0		(Note 2)	-
33.203	037	-	Rel-5	Ensuring the deletion of unwanted SA's	F	5.4.0	S3-27	S3-030124	agreed
33.203	038	-	Rel-5	Add protected port into Via header	F	5.4.0	S3-27	S3-030158	agreed
33.203	039	-	Rel-5	Correction of the Port 2 definition for SA establishment	F	5.4.0	S3-27	S3-030170	agreed
33.210	005	-	Rel-5	Za-interface and roaming agreements	F	5.2.0	S3-27	S3-030127	agreed
33.210	006	-	Rel-6	Za-interface and roaming agreements	A	6.0.0	S3-27	S3-030128	agreed
33.210	007	-	Rel-5	Clarification to the re-keying aspects of network domain security	F	5.2.0	S3-27	S3-030162	agreed
33.210	008	-	Rel-6	Clarification to the re-keying aspects of network domain security	A	6.0.0	S3-27	S3-030163	agreed

NOTE 1: 33.108 CR013 and CR014 were produced by the SA WG3 Secretary to implement a change, which had been omitted in the previous CR implementation.

NOTE 2: 33203 CR036 was revised in TSG SA Plenary due to a cover page error.

Secretary's Note: ALL THE ABOVE CRs (except 33.203 CR036, of which the revision 1 was approved) WERE APPROVED BY TSG SA#19.

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	Source TD	Comment/Status
S3-030004	LS on ECSD and Ciphering	GP-023402	Reply in S3-030015
S3-030005	LS (from SA WG2) on management and regulatory requirements for Presence service	S2-023627	Forwarded to S3-LI Group
S3-030006	LS from SA WG1: Having a Single USIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link	S1-022388	Reply LS in S3-030145
S3-030007	LS from SA WG2: Proposed Confidentiality for IMS	S2-023676	Response in S3-030168
S3-030008	Requirement to Allow Access to IMS by Means of SIM in 3G UEs	S2-023677	Noted. SA decision awaited
S3-030009	SA WG2 response to “Response to IETF LS on Interoperability Issues and SIP in IMS”	S2-023678rev3	Noted
S3-030010	Reply LS (from SA WG5) on ‘New requirements about functionality to make subscription to different domains independent or linked based on operator decision’	S5-024584	Noted
S3-030011	LS (from SA WG5) on bearer charging issues with use of HTTP for Rel 6	S5-024585	Noted
S3-030012	Reply LS (from SA WG5) on Indication of call termination as a result of IST operation	S5-024607	Further e-mail discussion required. Response LS in S3-020153
S3-030013	LS from TSG SA: Additional Release 5 work needed for Policy Control and Subscription Control of Media	SP-020839	Related CR in S3-030115 - Response LS in S3-030116
S3-030016	LS to 3GPP TSG SA3 regarding use of the “AMF” field to switch between multiple authentication algorithms	SG Doc 014/03	Response LS in S3-030134
S3-030020	LS (from SA WG1) on T2 proposal for GUP requirements- UE Data access and Backwards Compatibility	S1-030218	e-mail group to discuss and provide response LS in S3-030155
S3-030021	Response LS (from SA WG1) on Indication of call termination as a result of IST operation	S1-030240	Noted
S3-030022	LS (from SA WG2) on use of HTTP between UE and AS in the IMS	S2-030445	Response LS in S3-030148
S3-030023	LS (from SA WG2) on Multiple IMS registrations	S2-030446	Response in S3-030117
S3-030024	Reply to LS from SA5 (from SA WG2) on bearer charging issues with use of HTTP for Rel 6	S2-030450	Noted
S3-030025	LS (from SA WG5) on management and regulatory requirements for Presence service	S5-032021	Noted
S3-030027	LS from T WG2: Response to LS S1-022388. "Having a Single (U)SIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link"	T2-030190	Guidance requested from SA WG3. Response in S3-030145
S3-030042	LS (from CN WG4) on clarification on the requirement for UE re-authentication initiated by HSS	N4-030249	Response LS in S3-030120
S3-030043	LS (from CN WG1) on updated WID for emergency call enhancements for IP & PS based calls	N1-030271	Response LS in S3-030112
S3-030093	Handling of Issues associated with S3LI CRs	S3LI03_024r1	SA WG3 would continue to make minor changes where necessary, and the LI Group were encouraged to improve the quality and correctness of their CRs
S3-030096	Liaison Statement (from SA WG3 LI group) on WI IMS Presence Interception	S3LI03_024r1	Noted - unsure about request for S1 to comment on LI aspects of Presence
S3-030100	LS (from SA WG3 LI Group) on Possible overlap of the scopes in the 3GPP TS 33.108 and DES/SEC-003020	S3LI03_029r1	Noted
S3-030114	LS (from SA WG2) on WLAN/3GPP Simultaneous Access	S2-030279	Late contribution. E-mail discussion for response in S3-030169
S3-030118	LS (from GSMA SG) to 3GPP TSG SA3 regarding synchronisation of GGSNs and Gi firewalls	SG043_03	Late contribution. Postponed
S3-030143	LS from T WG3: Response to LS S1-022388: “Having a Single USIM to Authenticate Multiple Devices Simultaneously Using Local Wireless Link”	T3-030112	Late contribution. Noted
S3-030144	LS from T WG3: Request for Information Regarding WLAN Interworking Impacts to UICC applications	T3-030116	Late contribution. Postponed

E.2 Liaisons from the meeting

TD number	Title	Comment/Status	TO	CC
S3-030015	LS on "A5/3 ciphering modes for ECSD" (response to LS to SA3 (GP-023402) on "ECSD and Ciphering")	Approved by e-mail 29 Jan 2003	**TSG GERAN**	
S3-030112	Reply to LS (N1-030271/S3-030043) on updated WID for emergency call enhancements for IP & PS based calls	Approved	**CN WG1**	
S3-030116	SA3 response on the "Additional Release 5 work needed for Policy Control and Subscription Control of Media"	Approved	**TSG SA, SA WG1, SA WG2, SA WG4, TSG CN, CN WG1, CN WG4**	
S3-030117	Response to LS (S2-030374) on Multiple IMS registrations	Approved (sent to SA WG2 immediately)	**SA WG2**	**SA WG1**
S3-030131	LS on "Support for subscriber certificates"	Approved	**CN WG4**	
S3-030134	Reply LS on "the use of the "AMF" field to switch between multiple authentication algorithms"	Approved	**GSMA Security Group**	
S3-030135	LS to ETSI SAGE on Requirements list for UEA2 and UIA2	Approved	**ETSI SAGE**	
S3-030136	LS to TSG SA: Funding for UEA2/UIA2 - Per	Approved	**TSG SA**	
S3-030147	LS to SAGE on key derivation for IMS-based application services	Approved	**ETSI SAGE**	
S3-030152	Reply LS on security issues regarding Uplink TDOA location method	Approved	**TSG GERAN**	
S3-030159	Response LS to S3-030042: Reply LS on clarification on the requirement for UE re-authentication initiated by HSS	Approved	**CN WG1, CN WG4**	**SA WG2**
S3-030160	LS to SA1, SA2, CN1, T3: Ericsson	Approved	**SA WG1, SA WG2, CN WG1, T WG3**	
S3-030161	LS on "Requirement to allow IMS access by means of SIM"	Approved	**TSG SA, SA WG1, SA WG2 , T WG3, CN WG1, CN WG4**	
S3-030164	LS to CN WG4 - LS on security issues regarding multiple PDP contexts in GPRS	Approved	**CN WG4, SA WG2**	
S3-030165	LS to SA WG1, T WG2: Study of UE Functionality Split Security Issues for Release 6	Approved	**SA WG1**	**T WG2, T WG3, GSMA Security Group**
S3-030166	Draft LS on interworking between 3GPP and IEEE 802.11 systems	Approved	**IEEE 802.11 task group i**	**SA WG2**
S3-030167	LS to SA WG2 on 802.11i issues - Krister	Approved	**SA WG2**	
S3-030168	SA3 response on the "Proposed Confidentiality for IMS"	Approved	**SA WG2**	

E.3 Liaisons to be approved by e-mail

TD number	Title	Comment/Status	TO	CC
S3-030153	Reply LS on Indication of call termination as a result of IST operation (Marc)	E-mail Approval by 28/03/2004	**SA WG5**	**SA WG1**
S3-030155	Response LS to S3-030020 (Brad Owen)	E-mail Approval by 28/03/2004	**SA WG1**	**SA WG2, T WG2**
S3-030156	LS to RAN WG2: MBMS: Reuse of RAN/GERAN ciphering functions (Marc)	E-mail Approval by 14/03/2003	**RAN WG2, GERAN WG2**	**CN WG1**
S3-030157	LS to SA WG4 MBMS (Adrian)	E-mail Approval by 14/03/2003	**SA WG4**	**SA WG1, SA WG2**
S3-030169	LS on WLAN/3GPP simultaneous access (P. Howard)	E-mail Approval by 28/03/2004	**SA WG2**	**SA WG1**
S3-030171	Response to LS (S2-030445) on use of HTTP between UE and AS in the IMS	E-mail Approval by 21/03/2004	**SA WG2**	

Annex F: Actions from the meeting

AP 27/01: Secretary to input NDS/AF WID into SA #19 (TD S3-030139).

AP 27/02: V Niemi to consult S. Hayes on possible follow-up to the Joint 3GPP/IETF Workshop conclusions.

AP 27/03: M. Walker to contact S. Hayes to obtain a list of actions requested from SA WG3 for WLAN Interworking in order to ensure completion of 3GPP work for Release 6.

AP 27/04: J. Puthenkulam to lead an e-mail discussion on IEEE 802.11i requirements from the 3GPP Security point of view.

AP 27/05: V. Niemi to lead an e-mail discussion on meeting frequency and document submission deadlines.