Source:	**Secretary of 3GPP SA WG3**	
Title:	**Draft Report of meeting #28**	**Version 1.0.0**
Document Status:	**Approved**	

Berlin Dom

Contents

1 Opening of the meeting (Tuesday, 6 May, 09:00)

The Vice Chairman, V. Niemi, opened the meeting and welcomed delegates on behalf of the "*European Friends of 3GPP*".

2 Agreement of the agenda and meeting objectives

TD S3-030172 Draft Agenda for SA WG3 meeting #28. The agenda was reviewed. The Chairman reminded the delegates that Release 5 is functionally frozen and the main objectives for this meeting was the progressing of Release 6 work and essential corrections only to earlier Releases.

2.1 3GPP IPR Declaration

Delegates were reminded of their responsibilities as Members of 3GPP to declare any essential IPRs in the 3GPP work.

3 Assignment of input documents

The documents available at the meeting were assigned to their respective agenda items.

4 Meeting reports

4.1 Approval of the report of SA3#27, Sophia Antipolis, France, 25-28 February, 2003

TD S3-030182 Draft Report of SA WG3 meeting #27 version 0.0.5 (with revision marks). This was reviewed and it was noted that a comment on the wording for section 4.4 from Ericsson had not been fully included. **The SA WG3 Secretary agreed to include the agreed text in the final version of the report**. With this change, the report was then approved. The updated version 1.0.0 will be put on the FTP server.

Action Points from the meeting:

AP 27/01: *Secretary to input NDS/AF WID into SA #19 (TD S3-030139).* Completed, NDS/AF WID was approved at TSG SA#19.

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

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.* Completed.

AP 27/04: *J. Puthenkulam to lead an e-mail discussion on IEEE 802.11i requirements from the 3GPP Security point of view.* Completed. An input document was provided to this meeting for presentation.

AP 27/05: *V. Niemi to lead an e-mail discussion on meeting frequency and document submission deadlines.* Completed. A successful e-mail discussion was held. It was summarised that some working methods proposals were received, to increase meeting frequency, to have longer meetings, to use parallel sessions, to use ad-hoc meetings and to have more e-mail discussions.

It was proposed that

- a meeting should be held in November in order to progress and finalise work for the TSG December Plenaries.
- the October and (new) November meetings should be 4.5 days (Start Monday afternoon and finish Friday afternoon).
- Parallel sessions should not be used as this causes difficulties with smaller delegations in the meeting, who need to attend more than one session. Evening sessions should continue to be used.
- Possible 2-day ad-hoc meeting in 3-4 September 2003 (Host required): The need for this and topics to be decided in July meeting.

- e-mail discussions should continue in order to improve efficiency of contributions at meetings. The deadline for document submission worked well this time, as it had been moved to the Wednesday before the meeting due to bank holidays in Europe. It was suggested to move to 1 week before the meeting (e.g. for meetings starting on a Tuesday, 17.00 Tuesday the week before). For ad-hocs, 2 working days before the meeting was considered adequate. Tele-conferences should be explored for discussion of individual topics.

4.2 Report from SA#19, Birmingham, UK, 17-20 March, 2003

TD S3-030267 Extract from Draft Report of TSG SA meeting #19. This was provided by the SA WG3 Secretary for information and was noted.

The presentation from the SA WG3 Chairman to TSG SA#19 was provided for information in TD S3-030269 and was also noted.

5 Reports and liaisons from other groups

5.1 3GPP working groups

TD S3-030173 LS on proposed deletion of security-related work items in TSG-CN. This was introduced by Vodafone and proposes the deletion of the Ze interface as no progress has been made on the protocols in CN WG4 and there was no support for this in TSG CN. Also the FS on network impacts of enhanced HE control of Security work had had no progress in CN WG4 and there was no support for the WI in TSG CN. SA WG3 were asked to inform CN WG4 if these items are required and if so, to encourage companies to provide contributions to CN WG4 to progress the work.

The Ze interface was needed for MAPsec Automatic Key Management and was removed from Rel-5 as CN WG4 could not finish their work in time. The continued need for this in Rel-6 was questioned and supporting companies for this were asked to investigate their continued support for Automatic Key Management and, if so, to encourage contribution to the CN WG4 work.

It was agreed that the Positive Authentication Reporting was not required for Rel-6.

A response LS was provided in TD S3-030270 which was approved.

TD S3-030178 Reply LS (from SA WG2) on updated WID for emergency call enhancements for IP & PS based calls. This was introduced by Ericsson and provides replies from CN WG1 to their questions to SA WG2. There were no actions on SA WG3 and the LS was noted.

TD S3-030191 Response (from SA WG2) to LS on security issues regarding multiple PDP contexts in GPRS. This was introduced by Vodafone and asks SA WG3 to clarify the nature of the Security threats associated with PDP contexts. It was agreed to set up a drafting session in the evening in order to discuss these issues and provide a proposed LS reply in TD S3-030271 which was reviewed and revised in TD S3-030303 which was approved.

TD S3-030194 Template for Study on 3GPP work which is related to work in OMA. This was introduced by the SA WG3 Chairman and asked SA WG3 members to complete a table of work items where there is overlap and / or dependences between 3GPP and OMA. It was agreed that the Rapporteur for each item should consider the overlap with OMA and hold an off-line meeting to fill in the table and add to a reply LS to the TSG T Vice-Chairman. The Reply LS was provided in TD S3-030272 which was reviewed and updated in TD S3-030304 and approved.

TD S3-030215 Acceptance of CRs: S3-030098 (S3LI03_026) and S3-03030101 (S3-LI03030). (This contained re-submitted CRs from SA WG3 meeting #27). This was introduced by the SA WG3 LI Group representative (B. Wilhelm). It was clarified that the text "Handover interface port 2" refers to HI2, and not "port 2" as it could be mis-read. It was considered that the LI group had considered the questions asked by SA WG3 and the CRs were verified as correct and unambiguous. The CRs were then approved.

Siemens proposed that in future, LI Group CRs are approved over the SA WG3 e-mail list within the 2 weeks following their meetings. In this way there is time for reaction and would save time in case of problems with the LI CRs, where they can be corrected and then approved by SA WG3.

It was agreed that CRs from SA WG3 LI Group will be approved by e-mail following their meetings from now on.

TD S3-030216 LS (from SA WG1) on Privacy and Security Requirements within GSM/UMTS Devices. This was introduced by Vodafone and asked SA WG3 to study the security implications for a secure privacy domain for User Equipment and provide details to SA WG1. The attached LS to SA WG1 from SERG was also considered. It was thought that further input from SA WG1 on Privacy and GUP would be needed before any work can start in SA WG3. It was noted that SA WG1 were considering the requirements for these services. It was agreed to produce a response LS explaining this which was provided in TD S3-030273 which was approved.

5.2 IETF

There were no specific contributions under this agenda item.

5.3 ETSI SAGE

TD S3-030218 SOBER-128 for use as UMTS Encryption/Integrity Algorithm. This was provided by Qualcomm Europe for information. Qualcomm kindly offered the SOBER-128 algorithm for use as a UMTS Encryption/Integrity algorithm. The contribution was noted.

TD S3-030266 Proposed CR to 33.206: Addition of missing line to Rijndael S-box listing (Rel-5). This was introduced by Vodafone and corrects the Rijndael block cipher in order to avoid any confusion among implementers. It was noticed that the specification is 35.206, rather than 33.206. The document was updated to the correct specification number in TD S3-030274 which was approved.

5.4 GSMA SG

A verbal report on activities of GSMA SG was provided by C. Brookson. There had been no GSMA SG meetings since SA WG3 meeting #27. The next SG meeting will be 21 - 22 May 2003.

There had been some changes to the management of the GSMA. There was now a Board of CEOs from the operators in overall charge, and the day to day management was the job of the Executive Management Committee (EMC). On of the first roles of the EMC was to look at the organisation and roles of the working groups, and this is still in progress.

Since the last SA WG3 meeting there had been progress on the subject of IMEI security. A TCAM meeting (12 March 2003) was held which included a proposed directive on Crime Prevention of mobile phones. The proposal is to put the testing of the security of the IMEI in the R&TTE directive (see http://europa.eu.int/comm/enterprise/rtte/). The outcome was that this would be looked at further at TCAM 14 (in June 2003), and it was proposed that before this time (late May) all the interested parties would meet to discuss proposals and solutions in a session organised by TCAM.

5.5 3GPP2

A verbal report on activities of 3GPP2 was provided by M. Marcovici. 3GPP2 TSG-S WG4 (3GPP2 security) meets approximately 10 times per year. Currently all the security algorithms and procedures for 3GPP2 have been approved and published. The documents can be downloaded from the 3GPP2 Server (http://www.3gpp2.org/). The specification documents are:

(a) S.S0053 - Common Cryptographic Algorithms,

(b) S.S0054 - Interface Specification for Common Cryptographic Algorithms,

(c) S.S0055 - Enhanced Cryptographic Algorithms and

(d) S.S0078 - Common Security Algorithms.

The Broadcast/ Multicast Security Framework (S.P0083) has basically been completed and is in the process of being approved by the other technical groups. IMS Security Framework Draft (S.P0086 V0.2) has been completed and is based on 3GPP TS 33.203 (with modifications). 3GPP2 Packet Data Security Framework has been completed (S.P0082). Work is commencing on WLAN - 3GPP2 interworking specifications. 3GPP2 TSG-S WG4 agreed to meet jointly with 3GPP SA WG3 on July 17th. The 3GPP SA3 meeting will be sponsored by 3GPP2 members. Tentative subject for the joint meetings are: 3GPP2 IMS security framework, WLAN interworking - security framework, BCMCS security framework, use of UAK in 3GPP2 and use of TLS and/or IPSec in securing SIP.

It was reported that the date and times for the joint session between SA WG3 and 3GPP2 in San Francisco would be announced soon on the e-mail list. Some discussion on the subjects to be raised at the joint session ensued. It was agreed that the joint session should include IMS, WLAN and MBMS and, in particular, should include any questions to other groups that are for clarification on these items.

5.6 TIA TR-45

There were no specific contributions under this agenda item.

5.7 Other Groups

TD S3-030268 LS (from OMA) on DRM Content Format Statement. This was introduced by "**3**". The LS asks for action and responses from questions to SA WG4 and was copied to SA WG3 for information. This was thought to be useful as background for the MBMS discussions under agenda item 7.21. The LS was then noted.

6 WG Chairman and Vice Chairman elections

The following candidatures were received for the Chairman position and the two Vice Chairman positions:

TD S3-030183 Nomination for 3GPP TSG-SA WG3 Chairman position (nomination of V. Niemi, Nokia Corporation).

TD S3-030195 Nomination for 3GPP TSG-SA WG3 Vice Chairman position (nomination of P. Howard, Vodafone Group PLC).

TD S3-030204 Nomination for 3GPP TSG-SA WG3 Vice Chairman position (nomination of M. Marcovici, Lucent Technologies).

The SA WG3 Chairman reported the candidatures received to the group and asked if there were any additional candidates for these posts. No further candidatures were received and so the Chairman and two Vice Chairmen were therefore elected to the positions.

The current Chairman, Prof. Michael Walker, was thanked by the SA WG3 group for his Chairmanship of SA WG3 over the past 4 years and for SMG 10 before. The group presented him with parting gifts of Garden Centre vouchers and a commemorative dinner plate!

Prof. Walker thanked all the delegates who had contributed over the years with hard work and co-operation at and between the meetings, making his task as chairman an enjoyable experience.

Summary:

Chairman SA WG3: Dr. Valtteri Niemi, Nokia Corporation

Vice Chairman: Mr. Michael Marcovici, Lucent Technologies

Vice Chairman: Mr. Peter Howard, Vodafone Group PLC

7 Work areas

7.1 IP multimedia subsystem (IMS)

TD S3-030175 Response (from SA WG2) to LS on clarification on the requirement for UE re-authentication initiated by HSS. This was introduced by Ericsson and reports to CN WG4 the requirements for UE re-authentication initiated by the HSS. A response to CN WG4 had already been sent from the previous SA WG3 meeting. The LS was then noted.

TD S3-030190 LS Response (from SA WG2) on Use of ISIM and USIM for IMS access. This was introduced by Ericsson and informed SA WG3 that the SA WG2 specifications are in line with SA WG3 requirements. The LS was then noted.

TD S3-030199 Clarification of USIM-based access to IMS. This was introduced by T-Mobile and proposed clarifying the use of ISIM for IMS access with a Rel-5 UICC. There was some objection on this as it is was considered to be a SA WG1 requirement that needs clarifying and not a security issue. No agreement could be reached at the meeting and it was considered necessary to Ask SA WG1 for their interpretation of the requirements to ensure that all specifications are consistent before approving anything. It was considered that if Interpretation 3 is correct, SA WG3 would need to approve the changes. If Interpretation 2 is correct then SA WG1 and T WG3 may have to make changes to their specifications. It was clarified that only the SA WG3 specification implements interpretation 2 and others WGs seem to implement interpretation 3.

It was agreed that a LS should be sent to TSG SA, SA WG1, SA WG2 and T WG3 explaining the problem and asking for clarification on the ISIM/USIM issue, and requesting a decision to align all the specifications around the decision. The LS was provided in TD S3-030275 which was approved.

TD S3-030200 Proposed CR to TS 33.203: Clarification on USIM-based access to IMS (Rel-5). This CR was related to the discussions under TD S3-030199. The CR was updated editorially and revised in TD S3-030276 which was **conditionally approved** depending on the decision at TSG SA on the LS in TD S3-030275.

TD S3-030207 Proposed CR to 33.203: Annex H: Alignment of Authentication algorithm handling with RFC3329 (Rel-5). This CR was presented by Siemens and was approved.

TD S3-030228 Proposed CR to 33.203: Removing Cx-put and response procedure in failure cases (Rel-5). This CR was presented by Nokia. It was commented that the authentication pending flag would not become reset in the HSS and this should be further analysed before accepting the CR. It was requested that the procedure should be analysed to see if there is only a waste of some resources, or whether there is a security threat, as it seemed that the Stage 3 has been implemented differently than envisaged by SA WG3 with a 3-state flag. Nokia agreed to check the implementation with the experts in CN WG4 and re-present the CR with a more comprehensive description of the mechanism. The CR was therefore **rejected** (Nokia could bring this CR back for approval at the next meeting).

TD S3-030229 Proposed CR to 33.203: UA behaviour in Network authentication failures (Rel-5). This CR was presented by Nokia. It was argued that a solution to the problem had been found in the stage 3. Nokia was asked to investigate the issue with CN WG1 colleagues and re-submit a CR at the next meeting, if appropriate.

TD S3-030235 Openness of Rel6 IMS network: security methods required. This was presented by Nokia for discussion. It was clarified that the change was equivalent for the change made for Rel-5 on the network bypassing solution, but applicable to Rel-6. The difference being that in Rel-6 is proposed to be allowed to receive traffic from an I-CSCF, whereas in Rel-5 the IMS traffic must come from the P-CSCF (opening up of IMS access). It was agreed that an e-mail discussion should be held and an LS could be presented to the July 2003 meeting containing an agreed position of SA WG3.

AP 28/01: T. Viitanen to lead an e-mail discussion on Openness of Rel-6 IMS Network.

TD S3-030258 Proposed CR to 33.203: SA set-up procedure (Rel-5). This was presented by Lucent technologies and describes a potential problem with the SA set-up procedure. A proposed solution was provided in an attached CR. There was a potential problem with conflict with the RFC 3261, section 18.2.2, as the inbound and outbound ports should be the same, was identified. This needs verification. It was agreed that an e-mail discussion should be held and a good solution found for the problem.

AP 28/02: B. Owen to lead an e-mail discussion on SA set-up procedure in Rel-5.

AP 28/03: SA set-up procedure in Rel-5 problem to be reported to TSG SA by SA WG3 Chairman.

TD S3-030260 Network Authentication Failure in 33.203. This was introduced by Qualcomm Europe and presents a possible DoS attack due to I-CSCF clearing registration information on network authentication failure. This was considered to be a low-level attack scenario as the attacker has to use as much effort as the victim to perform the attack. Further study was thought necessary to determine what information is concerned in the proposal. The contribution was then noted.

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

There were no specific contributions under this agenda item.

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

TD S3-030263 Proposed CR to 33.210: Use of IPsec ESP with encryption on the Za-interface (Rel-5). This was introduced by Siemens and was approved.

TD S3-030264 Proposed CR to 33.210: Use of IPsec ESP with encryption on the Za-interface (Rel-6). This CR was approved.

TD S3-030243 NDS/IP and SIGTRAN security. This was introduced by Ericsson and discussed the SIGTRAN protocols and potential impacts on 3G security and TS 33.210. The contribution concluded that SIGTRAN may have an impact on the trust model of TS 33.210 and may require the definition of new Z-interfaces. SA WG3 were recommended to study further the impacts of SIGTRAN on TS 33.210. It was noted that there is no true Za interface as transport mode is used and not tunnelling (the interfaces are more like the Zb interface, except that they are not internal interfaces). It was also mentioned that no key management had been defined for this. It was agreed that an e-mail discussion should be held, using this contribution as a starting point. Mr. B. Sahlin agreed to lead the discussion.

AP 28/04: B. Sahlin to lead e-mail discussion based on TD S3-030243 on impacts of SIGTRAN on TS 33.210 for input to SA WG3 meeting #29.

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

TD S3-030201 Draft TS: NDS/AF TS ab.cde Version 0.2.0. The Rapporteur (T. Viitanen) presented the changes made to the draft TS following agreements at the previous SA WG3 meeting. The Draft TS was noted.

TD S3-030211 Profiling of IKE and Certificates for use within NDS/AF. This was introduced by Siemens on behalf of the contributors (Nokia, Siemens, SSH, T-Mobile, Verisign). It was noted that the "Motivation" statements were included in the drafting stage of the TS, but would be removed before final submission for approval to TSG SA. An editors note was added to remind the Rapporteur to remove these paragraphs later. This Pseudo-CR was then approved for inclusion in the draft TS.

TD S3-030233 Pseudo CR to NDS/AF: NDS/AF Trust Model (Rel-6). This was introduced by SSH on behalf of the contributors (Nokia, Siemens, SSH, T-Mobile, Verisign). This Pseudo-CR was approved for inclusion in the draft TS, with some redundant parts from A.3 not included.

TD S3-030234 Pseudo CR to NDS/AF: NDS/AF Repositories (Rel-6). This was introduced by T-Mobile on behalf of the contributors (Nokia, Siemens, SSH, T-Mobile, Verisign). This Pseudo-CR was approved for inclusion in the draft TS.

TD S3-030240 Pseudo CR to NDS/AF: NDS/AF Lifecycle Management (Rel-6). This was introduced by SSH on behalf of the contributors (Nokia, Siemens, SSH, T-Mobile, Verisign). It was noted that the CMPv2 needs to be an RFC before it can be referenced in the specification. It was reported that this is expected to happen soon. This Pseudo-CR was approved for inclusion in the draft TS with the addition of the draft status of the internet draft. It was agreed to add this draft to the list of IETF dependencies document.

TD S3-030295 Draft TS: NDS/AF TS ab.cde Version 0.3.0. This new version (0.3.0), updated with agreements at the meeting was provided by the Rapporteur (T) for information and as a basis further Pseudo-CRs. The Draft TS was noted.

7.5 UTRAN network access security

TD S3-030192 LS (from SA WG2) on unciphered IMEISV transfer. This was introduced by Siemens and asked SA WG3 to evaluate and potential issues caused by the transfer of the unciphered IMEI Software Version. Siemens had produced a discussion document based on draft TS 23.195, which was used to provide an insight into the mechanism used to send the IMEISV (TD S3-030225). This was considered with this LS.

TD S3-030225 Unciphered IMEISV transfer (Early UE). This was introduced by Siemens and discusses the issues raised in the LS from SA WG2 (TD S3-030192). There were some potential ambiguities in the transmission of IMEI in the specifications, and it was suggested that Manufacturers in CN WG1 should be asked whether they have implementations of "/REQ-B/" in the contribution.

It was considered an increased risk to user privacy to provide the IMEISV in clear at every location update and could open up potential Man-In-The-Middle attacks. It was recognised that the IMSI is sent in clear occasionally in the current standards, and allowing the same level of exposure of the IMEISV may be an acceptable compromise. It may also be helpful in the future to send the IMEI along with the IMSI between NEs in order to reduce the frequency of requests for it from the UE. A response LS was provided in TD S3-030277 which was reviewed and revised in TD S3-030294 which was approved. A Escott agreed to lead a discussion on the Man In The Middle attack problem.

AP 28/05: A. Escott to lead e-mail discussion on "potential Man-In-The-Middle threat providing IMEISV in clear", related to TD S3-030225, for contribution to SA WG3 meeting #29.

TD S3-030217 Proposed CR to 33.102: Handling of START values stored on a ME for use with a SIM (Rel-5). This was introduced by Siemens on behalf of the contributors (Siemens, Nokia, Vodafone). This CR was approved. It was decided that this should be sent to relevant WGs to inform them of this clarification for R99+ ME START value handling. An LS was provided for this in TD S3-030278 which was updated to include "Release 5" in the title in TD S3-030296 which was approved.

7.6 GERAN network access security

TD S3-030227 Key length parameter within A5/3 and GEA3 specifications. This was introduced by Siemens and discusses the value of the parameter KLEN, which is currently fixed to 64-bit. Using the same algorithm-id with different key lengths in future may lead to complicated solutions to accommodate that flexibility. Siemens proposed to write a CR against TS 55.216 in order to avoid confusion for present and future protocol implementations. The contribution from Ericsson in TD S3-030244 was related to this contribution and was also considered.

TD S3-030244 Enhanced Security for A/Gb. This was introduced by Ericsson and discussed the key length for A/Gb. Ericsson concluded that it should be possible to increase the key length to support any range from 64 bit to 128 bit keys. The easiest way forward is to assume that only the use of USIMs can be granted the increased security level over BSS accesses including the use of a Release 99+ version of the HLR/AuC, the SGSN and the ME. Ericsson expressed a slight preference for the ciphering alternative, as it would not change the AKA protocol. However the final decision should be based on the preference from SA WG3 considering feedback from other 3GPP groups. Ericsson proposed that the principles discussed in this contribution are agreed as a working assumption for increasing the security for Gb. It was thought that other groups should be consulted (particularly CN WG1) before making changes to the algorithm specification.

SA WG3 agreed as a working assumption that there was a need only for 64-bit key algorithm (GEA3) and a 128-bit algorithm (GEA4), rather than a variable bit-length.

SA WG3 agreed as a working assumption that increased key-length will only be possible with the use of the USIM. The use of SIM for secure negotiation should be subject to future contribution.

It was recognised that an attacker could try to reduce the security strength by reducing the negotiation. The following assumptions were considered necessary aims to counteract the attack:

- The signalling flow should be kept intact. i.e. it should be a three-way handshake;
- Both the SGSN and UE should be able to verify that secure negotiation was possible to use;
- The solution should allow the use of legacy UEs and SGSNs.

It was agreed to send a LS to CN WG1 outlining the proposal to create a new Algorithm definition "GEA4" with 128-bit key length. This was provided in TD S3-030279 which was revised in TD S3-030308 and approved.

7.7 Immediate service termination (IST)

There were no specific contributions under this agenda item.

7.8 Fraud information gathering system (FIGS)

There were no specific contributions under this agenda item.

7.9 Support for subscriber certificates

TD S3-030203 Draft TS ab.cde version 0.1.0: Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description. This was introduced by the Rapporteur (T. Haukka, Nokia). The draft integrated the agreements reached at SA WG3 meeting #27. The draft TS was noted.

TD S3-030220 Pseudo CR to "SSC": Further information related to the storage of the public/private key pairs present in the User Equipment (Rel-6). This was introduced by Gemplus. There was some discussion over the validity of mandating the use of UICC for storage of long-term key pairs. It was concluded that this is necessary as the keys are pre-loaded from the Home Network. The Pseudo CR was updated to include clarifications made in TD S3-030280 which was approved for inclusion in the draft TS.

TD S3-030221 Pseudo CR to "SSC": Further information related to the UE's public/private key pair associated to the requested subscriber certificate (Rel-6). This was introduced by Gemplus. There was a comment that the potential business case of a UICC supporting subscriber certificates without having to re-issue UICCs should not be ruled out. There was no support to mandate that keys shall be generated on the UICC. **Only the note on on-board key generation was accepted:**
"*NOTE: On board key generation is already defined in the WIM specification [WIM] issued by Open Mobile Alliance (OMA) group.*" will be added to the draft TS.

TD S3-030222 Pseudo CR to "SSC": Requirements on UE's public/private key pair associated to requested subscriber certificate (Rel-6). This was introduced by Gemplus. This was rejected as it mandated the storage of Keys on the UICC. Further discussion on this should be done via e-mail.

TD S3-030230 Pseudo-CR to "SSC": HTTP Digest AKA as protocol A (Rel-6). This was introduced by Nokia. It was noted that 4.2.3.1 mentions reference points in CS-domain which contradicts 4.2.3.2, where HTTP Digest is used. It was agreed to add an editors note in section 4.2.3.1 stating "*The applicability of CS domain is ffs*". It was also agreed that the text "*(XRES is used)*" should be removed from the new figure 3. It was agreed to delete the word "response" from step 4 "*response RES*". It was agreed to remove the mention of key agreement procedure from 4.3 and between the steps 7 and 8 of section 4.3.1. With these changes, the Pseudo-CR was approved for inclusion in the draft TS.

TD S3-030231 Pseudo-CR to "SSC": Development to the draft TS contents (Rel-6). This was introduced by Nokia. It was agreed that 4.1.2 would read "*Authentication shall be based on AKA protocol*". It was agreed to move the final bullet from 4.2.2.2 and move it into 4.2.2.1 and also to add an editors note that key generation for NAF is ffs. With these changes, the Pseudo-CR was approved for inclusion in the draft TS.

TD S3-030232 Pseudo-CR to "SSC": Development to the annex of the draft TS (Rel-6). This was introduced by Nokia. It was clarified that the mandate for PKCS#10 is for legacy reasons, as this is being used extensively and is being specified by OMA. This Pseudo-CR was approved for inclusion in the draft TS.

TD S3-030239 Notes for the use of CMPv2 as the subscriber certificate enrolment protocol (Protocol B). This was introduced by SSH and discussed the arguments given in TD S3-030073 from meeting #27. The contribution concludes that despite the apparent disadvantages of the full CMPv2 as defined, an appropriate profiling for 3GPP use can provide advantages and proposes to re-evaluate the use of CMPv2 as the Protocol B. SSH reported that CMPv2 has passed the WG last call and should be an RFC in a few months time. SSH were asked to provide suggestions for profiling CMPv2 for 3GPP use and provide contributions on this at the next SA WG3 meeting.

AP 28/06: SSH to provide suggestions for profiling CMPv2 for 3GPP use and provide contributions on this at the next SA WG3 meeting.

TD S3-030241 BSF-HSS (C interface) Bootstrapping protocol. This was introduced by Nokia and discussed DIAMETER based implementation of the C interface. The study shows that the Bootstrapping C interface is possible to implement by direct reuse of 3GPP Diameter IMS Cx interface specification. Nokia proposed that this should be adopted as the preferred solution and studied further by SA WG3.

SA WG3 agreed a working assumption to adopt the use of DIAMETER based implementation of the C interface for further study.

TD S3-030242 NAF-BSF (D interface) protocol. This was introduced by Nokia and discussed DIAMETER based implementation of the D interface. The study shows that the D interface is possible to implement by re-using the 3GPP IMS Diameter Cx interface specification. Nokia proposed that this should be adopted as the preferred solution and studied further by SA WG3. It was noted that the use of NAF in the Visited Network is for study in future versions of the specification and Home Network only is envisaged for the first version of the specification.

SA WG3 agreed a working assumption to adopt the use of DIAMETER based implementation of the D interface for further study.

It was concluded that the Cx application could be used for the C interface and possibly also for the D interface. A LS to CN WG4 was provided to ask them to study these proposals and provide feedback in TD S3-030283 which was revised in TD S3-030305 and was approved.

The contribution (TD S3-030242) was corrected editorially, in TD S3-030282, for attachment to the LS.

TD S3-030253 Pseudo CR to "SSC": Bootstrapping of application security using AKA (Rel-6). This was introduced by Alcatel. Alcatel argued that the draft TS is not about subscriber certificates, but a application-independent bootstrapping mechanism which can be used for the subscriber certificates application and proposes to delete "subscriber certificates" from the title and scope of the TS. It was suggested that the document should consist of the generic bootstrapping mechanism and each identified application could be described in informative annexes. It was agreed to continue with the TS structure as it is for the moment and make a decision on the need for a separation of the bootstrapping and applications when the content is more mature and the application-independent mechanism can be identified. An e-mail discussion on the best structure for this work was set up to help get general agreement on the structure for the next meeting. A. Van Moffaert agreed to lead this e-mail discussion.

AP 28/07: A. Van Moffaert to lead an e-mail discussion on structure and scope of the draft TS on bootstrapping of application security.

TD S3-030254 Location of key pair generation. This was introduced by Alcatel and raised the issue of where the public/private key pair being certified is generated. Possibilities are generation by the UE or outside the UE (e.g. in the Network) with consequences on the choice of certificate request/response protocol and necessary security measures. It was reported that the CMPv2 allows the generation of Key pairs in the network, but there is an associated security reduction compared to UE generation. SA WG3 delegates were asked to discuss this further via e-mail and provide contributions to the next SA WG3 meeting.

7.10 Digital rights management (DRM)

There were no specific contributions under this agenda item.

7.11 WLAN inter-working (TS 33.234)

TD S3-030262 Draft TS 33.234 v0.4.0: Wireless Local Area Network (WLAN) Interworking Security; (Release 6). This was presented by the Rapporteur (C. Blanchard, BT Group PLC) and included the changes agreed at SA WG3 meeting #27. The Draft TS was noted.

TD S3-030176 LS (from SA WG2) on Clarification of Scenario 2 and Scenario 3 architectural characteristics and stable and non-stable parts of TS 23.234. This LS was introduced by Nokia. SA WG2 asked SA WG3 to proceed with the WLAN 3GPP Security aspects based on the Scenario clarifications. It was noted from information from the WLAN ad-hoc group that Scenario 3 is now less stable. The LS was then noted.

TD S3-030177 LS (from SA WG2) on Incorporation of re-authentication into TS 33.234. This LS was introduced by Nokia. SA WG2 asked SA WG3 to consider re-authentication for inclusion in the draft TS 33.234 and to inform SA WG2 if and when they can remove this from their draft TS 23.234. It was agreed to include this in draft TS 33.234 as an editorial note, for further elaboration by Pseudo-CRs when the usefulness of re-authentication has been studied. A response LS to SA WG2 to inform them of this was provided in TD S3-030284 which was reviewed and revised in TD S3-030297 and approved.

TD S3-030189 LS (from SA WG2) on impacts on the UE of UE-Initiated Tunnelling. This LS was introduced by Orange France and asks SA WG3 to evaluate the impacts on the UE of the UE-Initiated tunnels; to check what tunnel security options (if any) impact the UE and which WLAN UEs could not support them; and to comment on any security issue around the specific case of UE-initiated tunnels terminated in the Packet Data Gateway. A related contribution had been provided by Nokia in TD S3-030236 which was also considered. A response LS was provided in TD S3-030285 which was approved.

TD S3-030236 UE-Initiated Tunnelling with L2TP/IPSec. This was introduced by Nokia and discusses the SA WG2 work on UE-Initiated Tunnelling. Nokia proposed that SA WG3 uses L2TP/IPSec for a secure VPN solution for UE-initiated tunnelling in 3GPP-WLAN interworking scenario 3 and takes under further investigation the related design details. Ericsson considered it too be premature for SA WG3 to agree on any particular solutions as SA WG2 are still discussing scenarios and have time scale problems. It was reported that SA WG2 may remove Scenario 3 from their specification, or delay their completion until September 2003. It was decided to postpone decision on this work until the SA WG2 situation was known.

TD S3-030237 Pseudo CR to 33.234: Transport of Authentication Signalling in 3G-WLAN (Rel-6). The reference to 29.234 could not be verified as it was not available. It was considered unnecessary to reference the Stage 3 specification and so this was removed from the proposed changes. The other changes in this Pseudo-CR were approved for inclusion in the draft TS.

TD S3-030252 Pseudo CR to 33.234: Editorial changes to 33.234 (Rel-6). This was introduced by Ericsson and editorially cleaned up some parts of the draft TS. In 4.2.4 it was agreed to keep "*authentication and authorisation*". It was also agreed that the first paragraph of 4.2.2 will be reinstated. With these changes, the Pseudo-CR was approved for inclusion in the draft TS.

TD S3-030259 Pseudo CR to WLAN: Editorial changes to section 6.1 - AKA (Rel-6). This was introduced by Ericsson. This Pseudo-CR was approved for inclusion in the draft TS.

TD S3-030202 Pseudo CR to TS 33.234: Clarification of WLAN UE terminology. This was introduced by T-Mobile. This Pseudo-CR was approved for inclusion in the draft TS. It was agreed to add an editors note that the WLAN UE is a form of radio coverage.

TD S3-030261 WLAN – Implications of the trust relation between the Cellular Operator and the WLAN Access Provider. This was introduced by Ericsson and considered the relationship between the Cellular Operator and the WLAN Access Provider and concludes with a table containing two trust levels based on the analysis. Ericsson proposed incorporating the table in Annex B of the draft TS and to inform SA WG1 and SA WG2 of the implications of the trust relationship. As this document was provided after the deadline (*"Late Document"*) and there were some concerns over the analysis results, it was agreed to discuss this further over e-mail for conclusion at the next meeting. D. Mariblanca agreed to lead the e-mail discussion on this.

AP 28/08: D. Mariblanca to lead an e-mail discussion on Implications of the trust relation between the Cellular Operator and the WLAN Access Provider based on TD S3-030261 for conclusion at the next meeting.

TD S3-030251 SIM access via 'SIM Access Profile' and Bluetooth link. This was introduced by Ericsson and discusses aspects of SIM access via SIM AP and Bluetooth. Ericsson proposed to send an LS to the Bluetooth Architecture Review Board (BARB) and the CAR groups asking them to start work on a new version of the SIM Access Profile, including a list of requirements from SA WG3. Ericsson also proposed to remove some requirements on a Bluetooth link from draft TS 33.234. It was decided to postpone this discussion to agenda item 7.16 when it was agreed to take account of the principles of the contribution in the feasibility study work item in TD S3-030289.

With regards to the attached Pseudo-CR, this was considered and it was agreed to reject the change but add an editors note that the security for Bluetooth was for further study.

TD S3-030255 IEEE 802.11i Requirements. This was introduced by Intel and resulted from a request from SA WG3 meeting #27 for Intel to provide a report on the requirements of IEEE 802.11i, related to PEAP. IEEE 802.11i are working on an EAP method with 256-bit key length (128-bit minimum key length) and have requested inclusion of their supported method to the IETF. Member companies who support the 3GPP-WLAN Work Item were asked to try to ensure the IETF completes the requirements for IEEE 802.11i. Intel were thanked for providing the report which was then noted.

TD S3-030213 LS from T WG3: Request for Information Regarding WLAN Interworking Impacts to UICC applications. This was introduced by SchlumbergerSema and asked SA WG3 (and other WGs) whether there is a need for T WG3 to start a work item to support the WLAN interworking efforts and to provide guidance on the focus of the WI. A response from SA WG1 was provided in TD S3-030187 and TD S3-030206. A related contribution suggesting a response was also provided in TD S3-030198. These contributions were considered and a response LS produced (see below).

> TD S3-030187 Reply LS (from SA WG1) on 'Request for Information Regarding WLAN Interworking. This was introduced by SchlumbergerSema and reported that SA WG1 see a need for T WG3 work on WLAN Interworking and asks SA WG3 and T WG3 to make efforts to find a standardised solution for a secured WLAN authentication based on (U)SIM. This was noted and used in discussion of TD S3-030213.
>
> TD S3-030206 LS from SA WG2: RE: Request for Information Regarding WLAN Interworking Impacts to UICC applications. This was introduced by SchlumbergerSema and reported that SA WG2 believe that a work item on the UICC may be welcome at this time and suggested that T WG3 liaise actively with the other WGs during the work on WLAN Interworking impacts to UICC. SA WG3 noted this liaison. This was noted and used in discussion of TD S3-030213.
>
> TD S3-030198 EAP support in smart cards and security requirements in WLAN authentication. This was introduced by SchlumbergerSema and proposed responding to SA WG2 (Copied to SA WG1) that:
> *SA WG3 has found that relevant authentication security improvements are provided by "EAP support in smart cards". These enhancements may be taken into account by the standardisation activities undertaken in SA WG2 and SA WG3 in order to promote any further study by other groups. Moreover, this liaison shall ask T WG3 to start the corresponding actions to enable these security enhancements in the ME-(U)SIM interface.*
> and also proposes that EAP support in smart cards shall be referenced in TS 33.234 and to add a new section 6.1.3 "EAP support in smart cards".

There was some discussion over the need for SIM access and a new "WLAN-Specific Card". SIM Access was included for backward compatibility reasons and enhancements of the smart cards would be using AKA. A Draft response LS was drafted in TD S3-030287 which was modified in TD S3-030306 and approved.

TD S3-030188 LS reply (from SA WG1) on WLAN/3GPP Simultaneous Access. This was introduced by Nokia and provided replies to questions asked in TD S3-030169 which was approved by e-mail after the previous meeting. This was noted for use in future discussions.

TD S3-030205 LS from SA WG2: Security in WLAN and 3G interworking. This was introduced by BT Group and confirmed that SA WG2 requirements impact mutual authentication, support of peer-to-peer session key exchange and re-keying techniques. SA WG2 asked SA WG3 to confirm that WPA defined encryption meets the security requirements for WLAN interworking and to comment on the security implications of RADIUS to Diameter interworking. It was debated whether or not an evaluation of WLAN security should be done by SA WG3 and concluded that this should not be done systematically, as this could also be done for many other technologies, without any real justification. It was recognised that SA Wg3 still need to study and develop the trust model, and this would impact on other decisions. It was also recognised that there are charging issues which would impact the trust model for different Scenarios. A late contribution had been received related to the second question from SA WG2 in TD S3-030265 which was also considered. A response to SA WG2 was provided in TD S3-030288 (attaching TD S3-030265) which was updated in TD S3-030299 and approved.

TD S3-030265 Co-Existence of RADIUS and Diameter. This was introduced by Ericsson and presented the differences between Diameter and RADIUS protocols, discussed the use of these protocols in WLAN inter-working in 3GPP in an interoperable manner. The contribution also discussed the security-related impacts of this, as well as the status of, e.g. EAP support in both of these protocols in IETF. Ericsson recommended considering the adoption of Diameter – RADIUS compatibility mode; to take a stand on whether IPsec is required in those cases where RADIUS is used; to adopt the use of RFC 2869bis and corresponding Diameter counterpart as the standard for running EAP over AAA protocols and reported that the participation of SA WG3 Member companies in the standardisation of EAP keying framework and key transport is highly desirable. **The recommendations of this contribution were endorsed by SA WG3** and Member companies were asked to help ensure EAP keying framework and key transport standardisation could progress quickly.

7.12 Visibility and configurability of security

There were no specific contributions under this agenda item.

7.13 Push

There were no specific contributions under this agenda item.

7.14 Priority

There were no specific contributions under this agenda item.

7.15 Location services (LCS)

TD S3-030196 Kc security for the U-TDOA LCS method. This was presented by TruePosition. A LS from GERAN had been presented at SA WG3 meeting #27 in TD S3-030038. The response from SA WG3 to GERAN (TD S3-030152) advised that the encryption of Kc was advisable as it is distributed to many more NEs than at present and that physical security of the equipment using the Kc was also necessary. The presentation provided here proposed encryption technique for Kc protection and physical security measures for protection of Kc when used for U-TDOA. The proposed mechanism was considered a good starting point, but SA WG3 did not feel ready to decide on the final mechanism until more information is received from TSG GERAN on the need to distribute Kc and the efficiency gains from the proposed techniques. TruePosition were asked to report this position to GERAN and ask them to provide their reply to the SA WG3 LS in TD S3-030152 with detailed information. SA WG3 members were asked to provide comments to TruePosition on the proposed mechanism over e-mail.

7.16 User equipment functionality split (UEFS)

TD S3-030281 Work Item Description for U(SIM) Re-use Security Requirements For Multiple Network Interfaces. This was introduced by Toshiba on behalf of the contributors (Toshiba, Intel, T-Mobile, Nokia). It was considered that the objectives should include the text under "Security Aspects" and the intention to do a thorough threat analysis. There were also concerns about the timing of this feasibility study, as when completed, it may be necessary to start producing CRs to specifications.

It was requested that this work should be de-coupled from the WLAN work, in order not to introduce any delay into the WLAN draft TS progress. It was also requested that the WLAN draft TS requirements should take priority over any conflicting requirements in the Feasibility Study TR.

It was agreed that this WI should not delay the WLAN work.

The contributors were asked to revise the timescales in order to have a document available for September 2003 with an aim for approval in December 2003. The title required clarification and other modifications were also requested. The WID was revised and provided in TD S3-030289 which was revised again in TD S3-030307 and approved.

It was agreed that the contribution in TD S3-030251 will be considered for the development of the TR.

7.17 Open service architecture (OSA)

There were no specific contributions under this agenda item.

7.18 Generic user profile (GUP)

TD S3-030179 Liaison Statement (from SA WG2) on GUP Interworking with Device Management. This was introduced by Vodafone and was noted.

7.19 Presence

TD S3-030214 Draft TR ab.cde version 0.4.0: Presence service: Security (Rel-6). This was introduced by the Rapporteur (K. Boman, Ericsson) and included agreements made at SA WG3 meeting #27. The draft was noted and used as a basis for further contributions.

TD S3-030180 Reply LS (from SA WG2) on management and regulatory requirements for Presence service. This was introduced by Ericsson and was copied to SA WG3 for information. The LS was noted.

TD S3-030193 LS (from SA WG2) on enhancements of the Mt reference point. This was introduced by Ericsson and to asked SA WG3 to provide feedback to SA WG2 on whether using a proxy/gateway on the Mt reference point would cause any major negative impact in providing security mechanisms for the communication on the Mt reference point. It was commented that the answer to the question was dependant on the functions that the Proxy/Gateway will perform and whether TLS can be run and terminated in the Proxy/Gateway. There were some contributions related to this which were then considered to see if a response could be given. A response LS was provided after discussion of other Presence issues (below) in TD S3-030291 which was revised in TD S3-030300 which was approved.

TD S3-030210 Response (from SA WG2) to LS (S2-030445) on use of HTTP between UE and AS in the IMS. This was introduced by Siemens and asks SA WG3 to take into account the conclusions of SA WG2 that:

- dependencies on work that is not certain to meet the Release 6 deadline should be avoided;
- usage of Mt does not require the user to be IMS registered; and
- the possibility to have multiple Application Servers at the same time should be taken into account.

It was recognised that the second bullet would need more study in SA WG3. The LS was then noted.

TD S3-030219 LS from ETSI SAGE: Initial response on key derivation for IMS-based application services. This was introduced by the ETSI SAGE representative and provided comments about the feasibility of deriving several symmetric keys DKi, to secure links between the UE and various end-points, from the cipher key CK, as requested by SA WG3 in an LS provided in TD S3-030147 at the previous meeting. SAGE reported that they are willing to define a mechanism if SA WG3 provide a well-defined cryptographic problem, as abstract from the context as possible. SA WG3 need to study this in order to define the problem precisely. P. Christoffersen agreed to inform ETSI SAGE of the discussions in the meeting.

TD S3-030224 Security protocols for the use of HTTP at the Mt reference point in the IMS. This was introduced by Siemens and proposed protocols to provide mutual authentication, confidentiality and integrity over the Mt reference point. It was agreed at the previous meeting that TLS should be used for confidentiality and integrity (i.e. HTTPS). Siemens also proposed using TLS for Server Authentication but this was in need of further study in SA WG3.

TD S3-030223 Key management for the use of http at the Mt reference point in the IMS. This was introduced by Siemens and proposes a solution how to establish a shared secret between the UE and the AS, based on the IMS registration. Siemens proposed that the principles in the contribution are adopted as a working assumption in SA WG3.

> There was a concern that forcing a registration could cause a flooding of the user with Presence services, which may not be what is wanted.
>
> It was commented that the proposed solution seems quite complicated and places many new requirements upon equipment.
>
> It was noted that Siemens believed the Key Synchronisation not to be a large problem, as re-registrations are not expected to be frequent.

Some comments and discussion ensued, it was decided to have a general summing up discussion after the other 2 proposals from Ericsson and Nokia had been presented and discussed (see below).

TD S3-030245 HTTP Security in Mt interface. This was introduced by Ericsson and discussed security solutions for IMS/Presence Mt interface. The proposed solution is able to provide access security to several Application Servers as proposed by SA WG2. The solution is also independent of IMS registration. The dependency of AKAv2 specification work with IETF is not seen as a big risk, since AKAv2 is not a new protocol but an extension to an existing one.

Some comments and discussion ensued, it was decided to have a general summing up discussion after the other proposal from Nokia had been presented and discussed (see below).

TD S3-030256 Analysis of HTTP authentication. This was introduced by Nokia and analysis 3 approaches to authentication and concluded by proposing to use a TLS approach with server-only authentication, then using HTTP Digest with a bootstrapped key or HTTP AKA with password derived from the bootstrapped key for client authentication. The Authentication Proxy can either retrieve the bootstrapped key from the Bootstrapping Function (BSF) or, preferably, directly from the HSS.

General discussion of TD S3-030223, TD S3-030245 and TD S3-030256:

It was decided to collect together the objections to each proposal and utilise this list as a basis for an e-mail discussion in order to find the best approach:

Siemens Proposal: Authentication using TLS and HTTP (HTTPS).

Objections:

1 Restricted to IMS users only
2 At least 1 IMS registration is needed for every profile prior to contacting the Application Server
3 Complexity: 3rd Party Registration, Key Management, Update at each (Re-)Authentication, Key Synchronisation
4 S-CSCF impacted
5 UE requires non-volatile memory / storage of normally deleted secret data
6 Key derivation done in terminal (not UE)
7 Keys transported over SIP which it is not designed to do
8 Terminal needs TLS connection with many Network End-Points

Ericsson Proposal: Authentication using AKAv2.

Objections:

1 RFC is still under development in IETF
2 New Cx-like interface is needed
3 Number of elements having an interface to HSS
4 Complexity: Heavy consumption of AVs
5 Effects on SQN handling
6 Server Authentication is done twice
7 Detail of Proxy Functionality missing

Nokia Proposal: Authentication using TLS and Bootstrapping Function for HTTP AKA.

Objections:

1 Dependency on BSF specification
2 Subset of objections to Ericsson proposal

Siemens, Ericsson and Nokia were asked to confer together and try to provide detailed proposals at the next SA WG3 meeting.

It was agreed to include information on these contributions to CN WG4 in the LS in TD S3-030283. Another LS to SA WG1 and SA WG2 was provided in TD S3-030290. The wording was discussed and modified for clarity of the questions to ask the WGs in TD S3-030301 which was approved.

An LS to CN WG2 and SA WG2 on Keying for ISC and use of nonce in the Siemens proposal was provided in TD S3-030292 and was modified slightly in TD S3-030302 and approved.

TD S3-030246 Watcher Authentication. This was introduced by Ericsson and proposed that SA WG3 choose the use of HTTP Digest as the solution for Watcher Authentication. **The Rapporteur was asked to add information on the use of manual delivery of Passwords to the draft TR.**

TD S3-030247 Presence / IMS Confidentiality. This was introduced by Ericsson and proposed a solution for the confidentiality protection solution in the Peu and Pw interfaces. SA WG3 were asked to make a decision on the issue, and to accept the accompanied Pseudo-CR to [Presence-Security] as a working assumption. It was clarified that the negotiation procedure is from Sip-Sec-Agree. This Pseudo-CR was approved for inclusion in the draft TR.

7.20 User equipment management (UEM)

TD S3-030181 Reply LS (from SA WG5) on OMA Device Management Requirements document. This was copied to SA WG3 for information and was noted. SA WG3 may need to review the OMA work when SA WG5 have decided what work they will give to and take from OMA.

7.21 Multimedia broadcast/multicast service (MBMS)

TD S3-030185 Draft TS 33.246 V0.1.0: Security of Multimedia Broadcast/Multicast Service (Rel-6). This was introduced by the Rapporteur (A. Escott, '***3***') and included agreements made at SA WG3 meeting #27. The draft was noted and used as a basis for further contributions.

TD S3-030197 MBMS re-keying: point-to-point and LKH. This was introduced by Qualcomm Europe and considers the relationship between point-to-point and LKH MBMS re-keying proposals received at SA WG3 meeting #27. Qualcomm concluded that the LKH proposal was worth further study for a later phase of the standard, but proposed that SA WG3 adopt the point-to-point Broadcast Access Key (BAK) scheme for Release 6 and consider enhancements like LKH functionality, if required, in later Releases. It was noted that study on recovery, in case a user does not receive a broadcast key and needs to request it from the network, is still required. Qualcomm reported that 3GPP2 are about to choose the point-to-point BAK scheme (comment period ends mid-May 2003) and harmonisation with the 3GPP2 scheme would be a great advantage. Qualcomm added that the BAK scheme was considered superior by 3GPP2 for the usage cases of MBMS and offers flexibility with the hierarchical Key structure. This was considered in discussions of other contributions about LKH.

TD S3-030238 Levels of MBMS key hierarchy. This was introduced by Nokia and presents the results of an analysis of 3 proposals and their reasoning, to conclude how valid they are in the MBMS context. Nokia propose that re-keying is not done in the case that a user leaves the service or a key compromise occurs and that a 3-level key hierarchy is used. It was suggested that the assumptions made on charging in this contribution, although appearing reasonable, were out of the scope of SA WG3 and should be confirmed by SA WG1 before making a decision on the choice of mechanisms. It was agreed to discuss and approve an LS to SA WG1 over e-mail. **T. Viitanen agreed to create the draft LS by 16 May, comments by 23 May and approval by 30 May 2003. (a document number will be given when the document is approved)**

TD S3-030249 Key generation and distribution in MBMS. This was introduced by Ericsson and proposes that TEK generation and distribution to UE are performed by the BM-SC. This was related to a companion contribution in TD S3-030248 which was considered at the same time.

SA WG3 agreed that TEK generation and distribution to UE are performed by the BM-SC.

TD S3-030248 Authentication in MBMS. This was introduced by Ericsson and discusses the different authentication methods and proposes a new Authentication procedure based on AKA supported between the BM-SC and the UE. It was considered that the Bootstrapping function and the visited case need to be analysed before deciding on the AKA proposal.

Ericsson also proposed to send an LS to SA WG2 and CN WG4 asking whether SA WG2 agree with the analysis; whether SA WG2 agree that the MBMS Architecture could follow a similar approach to the IMS Architecture and to ask CN WG4 whether they see any problems with using the Cx interface between HSS and BM-SC. It was agreed to send in an LS to CN WG4 regarding the use of the Cx interface and this was added to the LS in TD S3-030283. An LS to SA WG2 was drafted in TD S3-030293 concerning the agreed parts of the contribution. The LS was reviewed and some comments received on the clarity of the assumptions made by SA WG3 and the responsibility of SA WG2 to answer some of the questions. It was not possible to reach agreement at the meeting, so it was decided to start an e-mail discussion taking into account any responses from SA WG2 and SA WG4 meetings. M Wivfesson agreed to lead this e-mail discussion.

AP 28/09: M Wivfesson to lead an e-mail discussion based on SA WG2 and SA WG4 responses to MBMS and DRM issues based on TD S3-030293 to create a new proposed LS to these groups.

TD S3-030257 PayTV model. This was introduced by Gemplus and describes and proposes the PayTV model as a solution for MBMS data protection and to incorporate it in the draft TS 33.246. There were some questions over the problems with Broadcast Key compromise. It was clarified that the model is good for Broadcast services. The applicability for the MBMS service would need further analysis of the risks and recovery possibilities.

TD S3-030226 MBMS: Key Encryption Keys requirements. This was introduced by Siemens and proposed the following new requirements for the MBMS Keys:

1) shall not allow the BM-SC to infer any information about used UE-keys at radio level (i.e. if they would be derived from it).
2) shall be MBMS-service specific.
3) shall be unique per BM-SC.

4) remains valid until the MBMS user leaves the MBMS-service.

The new requirement 1 was agreed, the other were left for further discussion pending other decisions on Key issues.

TD S3-030184 Reply (from TSG GERAN) to LS on double ciphering for MBMS multicast data. This was introduced by Vodafone. TSG GERAN informed SA WG3 that in *A/Gb mode*, ciphering is completed at the LLC layer, with each LLC PDU indicating if ciphering is used and in *Iu mode* it is possible to switch on or off ciphering on a Radio Bearer basis. The LS was noted and the Rapporteur was asked to include this confirmation as an editors note in the draft TS.

TD S3-030250 Status of SRTP and MIKEY in IETF. This was introduced by Ericsson and describes the standardization status of the Secure RTP (SRTP) protocol and Multimedia Internet KEYing (MIKEY) protocol in the IETF. These protocols were regarded as strong candidates for security and key management protocols, respectively, for MBMS. It was reported that the RFCs are expected to be available in time for Release 6 (i.e. issued in 2003). Ericsson were thanked for this information and were asked to continue monitoring and reporting any significant change in the status of this work. The contribution was noted.

TD S3-030286 Further consideration of LKH for MBMS re-keying. (Late document). This was introduced by Samsung Electronics and offered some clarification and some further consideration about MBMS LKH for MBMS re-keying and proposed that SA WG3 should continue studying applying the LKH principles for MBMB re-keying and also the feasibility of the proposed simplified LKH mechanism for MBMS re-keying. It was noted that LKH has some support within SA WG3 and will continue to be studied. Contributions on MBMS re-keying were requested from SA WG3 members.

7.22 Guide to 3G security (TR 33.900)

There were no specific contributions under this agenda item. Contributions were invited for this document in order to update the Rel-4 version to (maybe Rel-5 and) Rel-6.

8 Review and update of work programme

Although there were no contributions under this agenda item, the SA WG3 Secretary undertook to send an extract of the SA WG3 items to Rapporteurs who should review and correct the data for completion of the input to TSG SA in June 2003.

9 Future meeting dates and venues

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#29	15-18 July 2003	San Francisco	3GPP2
Possible S3-Ad-Hoc	3-4 September 2003	TBD	Host required
S3#30	6 (13.00) - 10 October 2003	Europe (TBD)	European 'Friends of 3GPP'
S3#31	18-21 November 2003	London co-located with S3-LI (TBC)	DTI (TBC)

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

Meeting	2003	Location	Primary Host
TSG RAN/CN/T #20	3-6 June	Hämeenlinna, Finland	Nokia
TSG SA #20	9-12 June	Hämeenlinna, Finland	Nokia
TSG RAN/CN/T #21	16-19 September	Berlin, Germany	European Friends of 3GPP
TSG SA #21	22-25 September	Berlin, Germany	European Friends of 3GPP
TSG RAN/CN/T #22	9-12 December	Hawaii, USA	NA Friends of 3GPP
TSG SA #22	15-18 December	Hawaii, USA	NA Friends of 3GPP
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	

Invitations to the next meeting should be transmitted the week after this meeting. M Pope to contact hosts.

10 Any other business

There was no other business.

11 Close (Friday, 9 May, 16:00)

The Chairman, V. Niemi, thanked delegates for their hard work during the meeting and the Hosts for the facilities. He then closed the meeting.

Annex A: List of attendees at the SA WG3#28 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. 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 31 344 6055	+46 31 7470 5050	SE	ETSI
Mr. Robert Brewer	TruePosition Inc.	rbrewer@trueposition.com		+1 610 680 1162	+1 610 680 1199	US	ETSI
Mr. Charles Brookson	DTI	etsi@zeata.plus.com	+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@telecomitalia.it		+39 0112285203	+39 0112287056	IT	ETSI
Mr. Sharat Chander	AT&T Wireless Services, Inc.	sharat.chander@attws.com	+1 435 894 7756	+1 425 580 6596	+1 425 580 6811	US	T1
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.christoffersson@teliasonera.com		+46 705 925100		SE	ETSI
Mr. Kevin England	mmO2 plc	kevin.england@o2.com	+447710016799	+447710016799		GB	ETSI
Dr. Adrian Escott	3	adrian.escott@three.co.uk		+44 7782 325254	+44 1628 766012	GB	ETSI
Mr. John B Fenn	SAMSUNG Electronics	johnbfenn@aol.com	+44 78 02 339070	+44 1784 428 600	+44 1784 428 629	GB	ETSI
Mr. Louis Finkelstein	MOTOROLA JAPAN LTD	mailto:louis.finkelstein@motorola.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
Mr. Philip Ginzboorg	NOKIA Corporation	philip.ginzboorg@nokia.com		+358 5 0483 6224	+358 9 4376 6852	FI	ETSI
Mr. Robert Gross	TruePosition Inc.	rlgross@trueposition.com		+1 610 680 1119	+1 610 680 1199	US	ETSI
Ms. Tao Haukka	Nokia Korea	tao.haukka@nokia.com		+358 40 5170079		KR	TTA
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. Tero Kivinen	SSH Communications Security	kivinen@ssh.com		+358 20 500 7452	+358 20 500 7021	FI	ETSI
Mr. Pekka Laitinen	NOKIA Corporation	pekka.laitinen@nokia.com		+358 5 0483 7438	+358 7 1803 6852	FI	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	US	T1
Mr. David Mariblanca	ERICSSON L.M.	david.mariblanca-nieves@ece.ericsson.se		+34646004736	+34913392538	SE	ETSI
Mr. Sebastien Nguyen Ngoc	ORANGE FRANCE	sebastien.nguyenngoc@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@teliasonera.com		+358 204066824	+358 2040 0 3168	SE	ETSI
Mr. Bradley Owen	Lucent Technologies N. S. UK	bvowen@lucent.com		+44 1793 736245	+44 1793 897414	GB	ETSI
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 4 42365441	+33 4 42365792	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. Greg Rose	QUALCOMM EUROPE S.A.R.L.	ggr@qualcomm.com	+61 2 8701 4052	+61 2 9817 4188	+61 2 9817 5199	FR	ETSI
Mr. Bengt Sahlin	ERICSSON L.M.	bengt.sahlin@lmf.ericsson.se		+358 40 778 4580	+358 9 299 3401	SE	ETSI
Mr. Ville Salmensuu	SSH Communications Security	ville.salmensuu@ssh.com	+358 40 569 1977	+358 20 500 7496	+358 20 500 7041	FI	ETSI
Mr. Stefan Schroeder	T-MOBILE DEUTSCHLAND	stefan.schroeder@t-mobile.de		+49 228 9363 3312	+49 228 9363 3309	DE	ETSI
Mr. James Semple	QUALCOMM EUROPE S.A.R.L.	c_jsemple@qualcomm.com		+44 7880791303		FR	ETSI
Mr. Benno Tietz	Vodafone D2 GmbH	benno.tietz@vodafone.com		+49 211 533 2168	+49 211 533 1649	DE	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

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
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. Zhu Yamin	Samsung	zym@samsung.co.kr		+86 10 6842 7711		JP	ARIB

45 attendees

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #26, #27 and #28, the following companies are eligible to vote at SA WG3 meeting #29:

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
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 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 (USA)	US	3GPPMEMBER	T1
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
OBERTHUR CARD SYSTEMS S.A.	FR	3GPPMEMBER	ETSI
ORANGE FRANCE	FR	3GPPMEMBER	ETSI
POLKOMTEL S.A.	PL	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	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
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

46 Individual Member Companies

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030172	Draft Agenda for SA WG3 meeting #28	SA WG3 Chairman	2	Approval		Approved
S3-030173	LS on proposed deletion of security-related work items in TSG-CN	TSG CN	5.1	Discussion		Reply in S3-030270
S3-030174	WITHDRAWN - LS (from SA WG2) on WLAN/3GPP Simultaneous Access	SA WG2	7.11	Action		WITHDRAWN - Dealt with at S3#27 - S3-030114
S3-030175	Response (from SA WG2) to LS on clarification on the requirement for UE re-authentication initiated by HSS	SA WG2	7.1	Discussion		Noted
S3-030176	LS (from SA WG2) on Clarification of Scenario 2 and Scenario 3 architectural characteristics and stable and non-stable parts of TS 23.234	SA WG2	7.11	Action		Scenario 3 less stable now. Noted
S3-030177	LS (from SA WG2) on Incorporation of re-authentication into TS 33.234	SA WG2	7.11	Action		Added as editorial note. Reply in S3-030297
S3-030178	Reply LS (from SA WG2) on updated WID for emergency call enhancements for IP & PS based calls	SA WG2	5.1	Information		Noted
S3-030179	Liaison Statement (from SA WG2) on GUP Interworking with Device Management	SA WG2	7.18	Information		Noted
S3-030180	Reply LS (from SA WG2) on management and regulatory requirements for Presence service	SA WG2	7.19	Information		Noted
S3-030181	Reply LS (from SA WG5) on OMA Device Management Requirements document	SA WG5	7.20	Information		Noted
S3-030182	Draft Report of SA WG3 meeting #27 version 0.0.5 (with revision marks)	SA WG3 Secretary	4.1	Approval		Approved with update to section 4.4 to be included by secretary
S3-030183	Nomination for 3GPP TSG-SA WG3 Chairman position	Nokia Networks	6	Information		Nomination of V. Niemi. - Elected Chairman
S3-030184	Reply (from TSG GERAN) to LS on double ciphering for MBMS multicast data	TSG GERAN	7.21	Information		Noted. Confirmation to be added to draft TS
S3-030185	Draft TS 33.246 V0.1.0: Security of Multimedia Broadcast/Multicast Service (Rel-6)	Editor	7.21	Discussion		Noted. Used as a basis for further contributions
S3-030186	LS (from SA WG1) on Privacy and Security Requirements within GSM/UMTS Devices	SA WG1	5.1	Action	S3-030216	Replaced by S3-030216 including missing attachment
S3-030187	Reply LS (from SA WG1) on 'Request for Information Regarding WLAN Interworking Impacts to UICC applications'	SA WG1	7.11	Action		Response to LS in S3-030216. Noted and used in discussion of S3-030213.
S3-030188	LS reply (from SA WG1) on WLAN/3GPP Simultaneous Access	SA WG1	7.11	Information		Noted for use in further discussions
S3-030189	LS (from SA WG2) on impacts on the UE of UE-Initiated Tunnelling	SA WG2	7.11	Action		Considered with S3-030236. Response LS in S3-030298
S3-030190	LS Response (from SA WG2) on Use of ISIM and USIM for IMS access	SA WG2	7.1	Information		Noted
S3-030191	Response (from SA WG2) to LS on security issues regarding multiple PDP contexts in GPRS	SA WG2	5.1	Action		Drafting group provided Reply in S3-030303
S3-030192	LS (from SA WG2) on unciphered IMEISV transfer	SA WG2	7.5	Action		Related contribution in S3-030225. Response LS to S2 in S3-030294

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030193	LS (from SA WG2) on enhancements of the Mt reference point	SA WG2	7.19	Action		Need to know more about functions in the Proxy/Gateway. Other contributions considered and LS in S3-030300
S3-030194	Template for Study on 3GPP work which is related to work in OMA	TSG T Vice Chair (K. Holley)	5.1	Action	S3-030272	Rapporteurs to meet and provide a response LS in S3-030304
S3-030195	Nomination for 3GPP TSG-SA WG3 Vice Chairman position	Vodafone	6	Information		Nomination of P. Howard. - Elected VC.
S3-030196	Kc security for the U-TDOA LCS method	TruePosition	7.15	Discussion		Presented.
S3-030197	MBMS re-keying: point-to-point and LKH	Qualcomm Europe	7.21	Discussion		Used for discussion of other LKH contributions
S3-030198	EAP support in smartcards and security requirements in WLAN authentication	SchlumbergerSema	7.11	Discussion / Approval		Related to LS in S3-030213. Response LS in S3-030306
S3-030199	Clarification of USIM-based access to IMS	T-Mobile, Vodafone	7.1	Discussion		LS to SA and other WGs in S3-030275
S3-030200	Proposed CR to TS 33.203: Clarification on USIM-based access to IMS (Rel-5)	T-Mobile, Vodafone	7.1	Approval	S3-030276	Related to S3-030199. Revised in S3-030276
S3-030201	Draft TS: NDS/AF TS ab.cde Version 0.2.0	Nokia, Siemens, SSH, T-Mobile, Verisign	7.1	Discussion		Noted. Updated version provided in S3-030295
S3-030202	Pseudo CR to TS 33.234: Clarification of WLAN UE terminology	T-Mobile	7.11	Approval		Approved for inclusion in Draft TS
S3-030203	Draft TS ab.cde version 0.1.0: Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description	Nokia	7.9	Discussion		Noted
S3-030204	Nomination for 3GPP TSG-SA WG3 Vice Chairman position	Lucent Technologies	6	Information		Nomination of M. Marcovici. - Elected VC
S3-030205	LS from SA WG2: Security in WLAN and 3G interworking	SA WG2	7.11	Action		Response in S3-030299
S3-030206	LS from SA WG2: RE: Request for Information Regarding WLAN Interworking Impacts to UICC applications	SA WG2	7.11	Action		Response to LS in S3-030216. Noted and used in discussion of S3-030213.
S3-030207	Proposed CR to 33.203: Annex H: Alignment of Authentication algorithm handling with RFC3329 (Rel-5)	Siemens	7.1	Approval		Approved
S3-030208	WITHDRAWN Proposed CR to 33.210: Use of IPsec ESP with encryption on the Za-interface (Rel-5)	Siemens	7.3	Approval	S3-030263	WITHDRAWN - updated in S3-030263
S3-030209	WITHDRAWN Proposed CR to 33.210: Use of IPsec ESP with encryption on the Za-interface (Rel-6)	Siemens	7.3	Approval	S3-030264	WITHDRAWN - updated in S3-030264
S3-030210	Response (from SA WG2) to LS (S2-030445) on use of HTTP between UE and AS in the IMS	SA WG2	7.19	Action		second bullet needs further study. Noted
S3-030211	Profiling of IKE and Certificates for use within NDS/AF	Nokia, Siemens, SSH, T-Mobile, Verisign	7.4	Discussion / Decision		Approved for inclusion in draft TS
S3-030212	WITHDRAWN Work Item Description for U(SIM) Re-use Security Requirements For Multiple Network Interfaces	Toshiba, Intel, T-Mobile, Nokia	7.16	Discussion / Decision	S3-030281	Revised in S3-030281

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030213	LS from T WG3: Request for Information Regarding WLAN Interworking Impacts to UICC applications	T WG3	7.11	Action		Postponed S3-030144 from meeting #27. LS provided in S3-030306
S3-030214	Draft TR ab.cde version 0.4.0: Presense service: Security (Rel-6)	Rapporteur	7.19	Information		Noted. Used as a basis for further contributions
S3-030215	Acceptance of CRs: S3-030098 (S3LI03_026) and S3-03030101 (S3-LI03030)	SA WG3 LI Group	5.1	Approval		Contains re-submitted CRs from S3#27. CRs approved. It was agreed that CRs from SA WG3 LI Group will be approved by e-mail following their meetings from now on.
S3-030216	LS (from SA WG1) on Privacy and Security Requirements within GSM/UMTS Devices	SA WG1	5.1	Action		Response LS asking for input in S3-030273
S3-030217	Proposed CR to 33.102: Handling of START values stored on a ME for use with a SIM (Rel-5)	Siemens, Nokia, Vodafone	7.5	Approval		Approved. LS to impacted groups in S3-030296
S3-030218	SOBER-128 for use as UMTS Encryption/Integrity Algorithm	QUALCOMM Europe	5.3	Discussion		Noted
S3-030219	LS from ETSI SAGE: Initial response on key derivation for IMS-based application services	ETSI SAGE	7.19	Action		P. Christoffersen to inform SAGE of discussions
S3-030220	Pseudo CR to "SSC": Further information related to the storage of the public/private key pairs present in the User Equipment (Rel-6)	GemPlus	7.9	Approval	S3-030280	Revised in S3-030280
S3-030221	Pseudo CR to "SSC": Further information related to the UE's public/private key pair associated to the requested subscriber certificate (Rel-6)	GemPlus	7.9	Approval		note on on-board key generation was accepted. Other changes rejected
S3-030222	Pseudo CR to "SSC": Requirements on UE's public/private key pair associated to requested subscriber certificate (Rel-6)	GemPlus	7.9	Approval		Rejected. E-mail discussion on UICC storage of keys required
S3-030223	Key management for the use of http at the Mt reference point in the IMS	Siemens	7.19	Discussion / Decision		Ericsson, Siemens and Nokia discussion to develop proposals
S3-030224	Security protocols for the use of HTTP at the Mt reference point in the IMS	Siemens	7.19	Discussion / Decision		Further study on TLS usage needed
S3-030225	Unciphered IMEISV transfer (Early UE)	Siemens	7.5	Discussion / Decision		Used for discussion of S3-030192. Response LS to S2 in S3-030294
S3-030226	MBMS: Key Encryption Keys requirements	Siemens	7.21	Discussion / Decision		Requirement 1 agreed. Others pending Key discussions
S3-030227	Key length parameter within A5/3 and GEA3 specifications	Siemens	7.6	Discussion / Decision		Working assumption: Need only 64-bit and 128-bit key lengths. GEA4 proposed new alg. Related LS to CN1 in S3-030308
S3-030228	Proposed CR to 33.203: Removing Cx-put and response procedure in failure cases (Rel-5)	Nokia	7.1	Approval		Rejected. Nokia to investigate mechanism implemented in Stage 3
S3-030229	Proposed CR to 33.203: UA behavior in Network authentication failures (Rel-5)	Nokia	7.1	Approval		Nokia to check with CN1 colleagues and re-submit if appropriate

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030230	Pseudo-CR to "SSC": HTTP Digest AKA as protocol A (Rel-6)	Nokia	7.9	Approval		Approved with numerous modifications for inclusion in draft TS
S3-030231	Pseudo-CR to "SSC": Development to the draft TS contents (Rel-6)	Nokia	7.9	Approval		Approved with modifications for inclusion in draft TS
S3-030232	Pseudo-CR to "SSC": Development to the annex of the draft TS (Rel-6)	Nokia	7.9	Approval		Approved for inclusion in draft TS
S3-030233	Pseudo CR to NDS/AF: NDS/AF Trust Model (Rel-6)	Nokia, Siemens, SSH, T-Mobile, Verisign	7.4	Approval		Approved 'most text' for inclusion in draft TS (some parts of A.3 are redundant)
S3-030234	Pseudo CR to NDS/AF: NDS/AF Repositories (Rel-6)	Nokia, Siemens, SSH, T-Mobile, Verisign	7.4	Approval		Approved for inclusion in draft TS
S3-030235	Openness of Rel6 IMS network: security methods required	Nokia	7.1	Discussion		T Viitanen to lead e-mail discussion for new LS at next meeting
S3-030236	UE-Initiated Tunneling with L2TP/IPSec	Nokia	7.11	Discussion / Decision		See also S3-030189. SA2 work status unstable. Wait until more known
S3-030237	Pseudo CR to 33.234: Transport of Authentication Signalling in 3G-WLAN (Rel-6)	Nokia	7.11	Approval		Ref to 29.234 removed. Other changes agreed for inclusion in draft TS
S3-030238	Levels of MBMS key hierarchy	Nokia	7.21	Discussion / Decision		T. Viitanen - draft LS by 16 May, comments by 23 May, approval by 30 May
S3-030239	Notes for the use of CMPv2 as the subscriber certificate enrollment protocol (Protocol B)	SSH Communications Security	7.9	Discussion / Decision		SSH to provide suggestions for profiling CMPv2 for 3GPP
S3-030240	Pseudo CR to NDS/AF: NDS/AF Lifecycle Management (Rel-6)	Nokia, Siemens, SSH, T-Mobile, Verisign	7.4	Approval		Approved for inclusion in draft TS. Draft IETF doc to be added to dependencies list
S3-030241	BSF-HSS (C interface) Bootstrapping protocol	Nokia	7.9	Discussion / Decision		Agreed as working assumption. Attached to LS to CN4 ion S3-030305
S3-030242	NAF-BSF (D interface) protocol	Nokia	7.9	Discussion / Decision		Agreed as working assumption. Updated in S3-030282 for attachment to LS to CN4 in S3-030305
S3-030243	NDS/IP and SIGTRAN security	Ericsson	7.3	Discussion		E-mail discussion to study impacts on 33.210 (B. Sahlin)
S3-030244	Enhanced Security for A/Gb	Ericsson	7.6	Discussion / Decision		Working assumption: Need only 64-bit and 128-bit key lengths. GEA4 proposed new alg. Related LS to CN1 in S3-030308
S3-030245	HTTP Security in Mt interface	Ericsson	7.19	Discussion / Decision		Ericsson, Siemens and Nokia discussion to develop proposals

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030246	Watcher Authentication	Ericsson	7.19	Discussion / Decision		Editors note on manual password distribution to be added to draft TR
S3-030247	Presence / IMS Confidentiality	Ericsson	7.19	Discussion / Decision		Pseudo-CR approved for inclusion in draft TR
S3-030248	Authentication in MBMS	Ericsson	7.21	Discussion / Decision		LS to CN4 in S3-030305
S3-030249	Key generation and distribution in MBMS	Ericsson	7.21	Discussion / Decision		Considered with S3-030248. LS in S3-030305
S3-030250	Status of SRTP and MIKEY in IETF	Ericsson	7.21	Information		Noted. Protocols expected in time for Release 6
S3-030251	SIM access via 'SIM Access Profile' and Bluetooth link	Ericsson	7.11	Discussion		Postponed to 7.16 discussions. Attached Pseudo CR rejected, editors note added. To be considered for FS in S3-030307
S3-030252	Pseudo CR to 33.234: Editorial changes to 33.234 (Rel-6)	Ericsson	7.11	Approval		Approved for inclusion in Draft TS with some modifications
S3-030253	Pseudo CR to "SSC": Bootstrapping of application security using AKA (Rel-6)	Alcatel	7.9	Approval		A Van Moffaert to lead e-mail discussion on structure of draft TS
S3-030254	Location of key pair generation	Alcatel	7.9	Discussion		Further discussion over e-mail and contribution to next meeting
S3-030255	IEEE 802.11i Requirements	Intel	7.11	Discussion		Members to try to ensure IETF complete IEEE 802.11i needs. Report noted.
S3-030256	Analysis of HTTP authentication	Nokia	7.19	Discussion / Decision		Ericsson, Siemens and Nokia discussion to develop proposals
S3-030257	PayTV model	Gemplus, Oberthur	7.21	Discussion / Approval		Risks of global key compromise needs more study
S3-030258	Proposed CR to 33.203: SA set-up procedure (Rel-5)	Lucent Technologies	7.1	Approval		B Owen to lead e-mail discussion for approval of CR at next meeting
S3-030259	Pseudo CR to WLAN: Editorial changes to section 6.1 - AKA (Rel-6)	Ericsson	7.11	Approval		Approved for inclusion in Draft TS
S3-030260	Network Authentication Failure in 33.203	Qualcomm Europe	7.1	Discussion / Decision		LATE DOCUMENT. Not considered serious DoS attack. Noted.
S3-030261	WLAN – Implications of the trust relation between the Cellular Operator and the WLAN Access Provider	Ericsson	7.11	Discussion / Decision		LATE DOCUMENT. E-mail discussion based on this document (D. Mariblanca to lead)
S3-030262	Draft TS 33.234 v0.4.0: Wireless Local Area Network (WLAN) Interworking Security; (Release 6)	Rapporteur	7.11	Information		LATE DOCUMENT. Noted
S3-030263	Proposed CR to 33.210: Use of IPsec ESP with encryption on the Za-interface (Rel-5)	Siemens	7.3	Approval		Approved
S3-030264	Proposed CR to 33.210: Use of IPsec ESP with encryption on the Za-interface (Rel-6)	Siemens	7.3	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030265	Co-Existence of RADIUS and Diameter	Ericsson	7.11	Discussion		LATE DOCUMENT. Recommendations endorsed. Added to LS in S3-030299
S3-030266	Proposed CR to 33.206: Addition of missing line to Rijndael S-box listing (Rel-5)	Vodafone / SAGE chairman	5.3	Approval	S3-030274	LATE DOCUMENT. Revised in S3-030274 as spec number is 35.206
S3-030267	Extract from Draft Report of TSG SA meeting #19	SA WG3 Secretary	4.2	Information		LATE DOCUMENT. Noted
S3-030268	LS (from OMA) on DRM Content Format Statement	OMA	5.7	Information		LATE DOCUMENT. Noted. Background for MBMS
S3-030269	SA3 Status Report to SA#19	SA WG3 Secretary	4.2	Information		LATE DOCUMENT. Noted
S3-030270	Reply LS on proposed deletion of security-related work items in TSG-CN	SA WG3	5.1	Approval		Approved
S3-030271	Security issues regarding multiple PDP contexts in GPRS	SA WG3	5.1	Approval	S3-030303	Revised in S3-030303
S3-030272	Response LS on Template for Study on 3GPP work which is related to work in OMA	SA WG3	5.1	Approval	S3-030304	Revised in S3-030304
S3-030273	LS on Privacy and Security Requirements within GSM/UMTS Devices	SA WG3	5.1	Approval		Approved
S3-030274	Proposed CR to 35.206: Addition of missing line to Rijndael S-box listing (Rel-5)	SA WG3	5.3	Approval		LATE DOCUMENT: Approved
S3-030275	LS to TSG SA on clarification of USIM-based access to IMS	SA WG3	7.1	Approval		Approved. CR in S3-030276
S3-030276	Proposed CR to TS 33.203: Clarification on USIM-based access to IMS (Rel-5)	T-Mobile, Vodafone	7.1	Approval		CONDITIONALLY APPROVED (depends on SA decision on S3-030275)
S3-030277	Reply LS on unciphered IMEISV transfer	SA WG3	7.5	Approval	S3-030294	Revised in S3-030294
S3-030278	LS on 'Handling of START values stored on a ME for use with a SIM'	SA WG3	7.5	Approval	S3-030296	Attach CR in S3-030217. Revised in S3-030296
S3-030279	LS to CN1 on increasing the key length for GEA3	K Boman	7.6	Approval	S3-030308	Revised in S3-030308
S3-030280	Pseudo CR to "SSC": Further information related to the storage of the public/private key pairs present in the User Equipment (Rel-6)	GemPlus	7.9	Approval		Approved
S3-030281	Work Item Description of a feasibility studying for U(SIM) Re-use Security Requirements For Multiple Network Interfaces	Toshiba, Intel, T-Mobile, Nokia	7.16	Discussion / Decision	S3-030289	Revised in S3-030289
S3-030282	NAF-BSF (D interface) protocol	Nokia	7.9	Discussion / Decision		Typos corrected for LS in S3-030305
S3-030283	LS to CN4: Adopting Cx as basis protocol for several interfaces: NAF-BSF (D interface) and BSF-HSS (C interface), the interface between Authentication Proxy and HSS, and the interface between HSS and BM-SC for MBMS	SA WG3	7.9	Approval	S3-030305	Attach S3-030241 and S3-030282. Revised in S3-030305
S3-030284	Reply LS to SA WG2 on re-authentication in TS 33.234	SA WG3	7.11	Approval	S3-030297	revised in S3-030297
S3-030285	Draft LS on impacts on the UE of UE-Initiated Tunnelling	SA WG3	7.11	Approval	S3-030298	Draft removed in S3-030298

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030286	Further consideration of LKH for MBMS re-keying	Samsung Electronics	7.21	Discussion		LATE DOCUMENT. LKH continue to be studied. Contributions requested
S3-030287	Reply LS on 'Request for Information Regarding WLAN Interworking Impacts to UICC applications'	SA WG3	7.11	Approval	S3-030306	Revised in S3-030306
S3-030288	Response LS to SA WG2 on WLAN interworking	SA WG3	7.11	Approval	S3-030299	Revised in S3-030299
S3-030289	Work Item Description for Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces	Toshiba, Intel, T-Mobile, Nokia	7.16	Discussion / Decision	S3-030307	S3-030251 to be considered in this work. Revised in S3-030307
S3-030290	LS to SA WG1 and SA WG2 on Presence server authentication considerations	SA WG3	7.19	Approval	S3-030301	Revised in S3-030301
S3-030291	Response to SA2 for their LS on enhancements of the Mt reference point	SA WG3	7.19	Approval	S3-030300	Revised in S3-030300
S3-030292	LS on Keying in ISC and use of Nonce	SA WG3	7.19	Approval	S3-030302	Revised in S3-030302
S3-030293	LS to SA WG2 on DRM content multicasted via MBMS	SA WG3	7.21	Approval		Not agreed. M Wivfesson to lead e-mail discussion
S3-030294	Reply LS on unciphered IMEISV transfer	SA WG3	7.5	Approval		Approved. MITM threat to be studied by SA WG3 (A Escott)
S3-030295	Draft TS: NDS/AF TS ab.cde Version 0.3.0	Rapporteur	7.1	Information		Updated with agreements at meeting. Noted
S3-030296	LS on 'Handling of START values stored on a ME for use with a SIM'	SA WG3	7.5	Approval		Approved. Attach CR in S3-030217
S3-030297	Reply LS to SA WG2 on re-authentication in TS 33.234	SA WG3	7.11	Approval		Approved
S3-030298	Draft LS on impacts on the UE of UE-Initiated Tunnelling	SA WG3	7.11	Approval		Approved
S3-030299	Response LS to SA WG2 on WLAN interworking	SA WG3	7.11	Approval		Approved
S3-030300	Response to SA2 for their LS on enhancements of the Mt reference point	SA WG3	7.19	Approval		Approved
S3-030301	LS to SA WG1 and SA WG2 on Presence server authentication considerations	SA WG3	7.19	Approval		Approved
S3-030302	LS on Keying in ISC and use of Nonce	SA WG3	7.19	Approval		Approved
S3-030303	LS to SA WG2: Security issues regarding multiple PDP contexts in GPRS	SA WG3	5.1	Approval		Approved
S3-030304	Response LS on Template for Study on 3GPP work which is related to work in OMA	SA WG3	5.1	Approval		Approved
S3-030305	Adopting Cx-based protocols for several interfaces: NAF-BSF (D interface) and BSF-HSS (C interface), the interface between Authentication Proxy and HSS, and the interface between HSS and BM-SC for MBMS	SA WG3	7.9	Approval		Approved
S3-030306	Reply LS on 'Request for Information Regarding WLAN Interworking Impacts to UICC applications'	SA WG3	7.11	Approval		Approved
S3-030307	Work Item Description for Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces	Toshiba, Intel, T-Mobile, Nokia	7.16	Discussion / Decision		Approved
S3-030308	LS to CN1 on increasing the key length for GEA3	SA WG3	7.6	Approval		Approved

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)	5.3.0	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	5.5.0	Rel-5	S3	BOMAN, Krister	
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	5.3.0	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)	6.1.0	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	6.1.0	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	015	1	Rel-5	Changes to meet international LI Requirements	F	5.3.0	S3-28	S3-030215	SEC1-LI
33.108	016	1	Rel-6	Changes to meet international LI Requirements	A	6.1.0	S3-28	S3-030215	SEC1-LI
33.203	040	-	Rel-5	Annex H: Alignment of Authentication algorithm handling with RFC3329	F	5.5.0	S3-28	S3-030207	IMS-ASEC
33.203	041	-	Rel-5	Clarification on USIM-based access to IMS	F	5.5.0	S3-28	S3-030276	IMS-ASEC
33.102	179	-	Rel-5	Handling of START values stored on a ME for use with a SIM	F	5.1.0	S3-28	S3-030217	SEC1
33.210	009	-	Rel-5	Use of IPsec ESP with encryption on the Za-interface	F	5.3.0	S3-28	S3-030263	SEC-NDS-IP
33.210	010	-	Rel-6	Use of IPsec ESP with encryption on the Za-interface	A	6.1.0	S3-28	S3-030264	SEC-NDS-IP
35.206	001	-	Rel-5	Addition of missing line to Rijndael S-box listing	F	5.0.0	S3-28	S3-030274	SEC1-CSALG01, SEC1-PSALG01

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	Source TD	Comment/Status
S3-030173	LS on proposed deletion of security-related work items in TSG-CN	NP-030139	Reply in S3-030270
S3-030174	WITHDRAWN - LS (from SA WG2) on WLAN/3GPP Simultaneous Access	S2-030279r1	WITHDRAWN - Dealt with at S3#27 - S3-030114
S3-030175	Response (from SA WG2) to LS on clarification on the requirement for UE re-authentication initiated by HSS	S2-030905	Noted
S3-030176	LS (from SA WG2) on Clarification of Scenario 2 and Scenario 3 architectural characteristics and stable and non-stable parts of TS 23.234	S2-030994	Scenario 3 less stable now. Noted
S3-030177	LS (from SA WG2) on Incorporation of re-authentication into TS 33.234	S2-030995	Added as editorial note. Reply in S3-030297
S3-030178	Reply LS (from SA WG2) on updated WID for emergency call enhancements for IP & PS based calls	S2-030997	Noted
S3-030179	Liaison Statement (from SA WG2) on GUP Interworking with Device Management	S2-031006	Noted
S3-030180	Reply LS (from SA WG2) on management and regulatory requirements for Presence service	S2-031027	Noted
S3-030181	Reply LS (from SA WG5) on OMA Device Management Requirements document	S5-032133	Noted
S3-030184	Reply (from TSG GERAN) to LS on double ciphering for MBMS multicast data	GP-030914	Noted. Confirmation to be added to draft TS
S3-030187	Reply LS (from SA WG1) on 'Request for Information Regarding WLAN Interworking Impacts to UICC applications'	S1-030546	Response to LS in S3-030216. Noted and used in discussion of S3-030213.
S3-030188	LS reply (from SA WG1) on WLAN/3GPP Simultaneous Access	S1-030547	Noted for use in further discussions
S3-030189	LS (from SA WG2) on impacts on the UE of UE-Initiated Tunnelling	S2-031569	Considered with S3-030236. Response LS in S3-030298
S3-030190	LS Response (from SA WG2) on Use of ISIM and USIM for IMS access	S2-031581	Noted
S3-030191	Response (from SA WG2) to LS on security issues regarding multiple PDP contexts in GPRS	S2-031589	Drafting group provided Reply in S3-030303
S3-030192	LS (from SA WG2) on unciphered IMEISV transfer	S2-031565	Related contribution in S3-030225. Response LS to S2 in S3-030294
S3-030193	LS (from SA WG2) on enhancements of the Mt reference point	S2-031593	Need to know more about functions in the Proxy/Gateway. Other contributions considered and LS in S3-030300
S3-030205	LS from SA WG2: Security in WLAN and 3G interworking	S2-031510	Response in S3-030299
S3-030206	LS from SA WG2: RE: Request for Information Regarding WLAN Interworking Impacts to UICC applications	S2-031607	Response to LS in S3-030216. Noted and used in discussion of S3-030213.
S3-030210	Response (from SA WG2) to LS (S2-030445) on use of HTTP between UE and AS in the IMS	S2-031583	second bullet needs further study. Noted
S3-030213	LS from T WG3: Request for Information Regarding WLAN Interworking Impacts to UICC applications	T3-030116	Postponed S3-030144 from meeting #27. LS provided in S3-030306
S3-030216	LS (from SA WG1) on Privacy and Security Requirements within GSM/UMTS Devices	S1-030559	Response LS asking for input in S3-030273
S3-030219	LS from ETSI SAGE: Initial response on key derivation for IMS-based application services	SAGE (03) 01	P. Christoffersen to inform SAGE of discussions
S3-030268	LS (from OMA) on DRM Content Format Statement		LATE DOCUMENT. Noted. Background for MBMS

E.2 Liaisons from the meeting

TD number	Title	Comment/Status	TO	CC
S3-030270	Reply LS on proposed deletion of security-related work items in TSG-CN	approved	**CN WG4**	**TSG SA, TSG CN**
S3-030273	LS on Privacy and Security Requirements within GSM/UMTS Devices	approved	**SA WG1**	**GSMA SerG LBS**
S3-030275	LS to TSG SA on clarification of USIM-based access to IMS	approved	**TSG SA, SA WG1, SA WG2, T WG3**	
S3-030294	Reply LS on unciphered IMEISV transfer	approved	**SA WG2, CN WG1**	
S3-030296	LS on 'Handling of START values stored on a ME for use with a SIM'	approved	**TSG GERAN, CN WG1, T WG3, RAN WG2**	
S3-030297	Reply LS to SA WG2 on re-authentication in TS 33.234	approved	**SA WG2**	
S3-030298	Draft LS on impacts on the UE of UE-Initiated Tunnelling	approved	**SA WG2**	**CN WG1, T WG2**
S3-030299	Response LS to SA WG2 on WLAN interworking	approved	**SA WG2**	
S3-030300	Response to SA2 for their LS on enhancements of the Mt reference point	approved	**SA WG2**	
S3-030301	LS to SA WG1 and SA WG2 on Presence server authentication considerations	approved	**SA WG1, SA WG2**	
S3-030302	LS on Keying in ISC and use of Nonce	approved	**CN WG1, SA WG2**	
S3-030303	LS to SA WG2: Security issues regarding multiple PDP contexts in GPRS	approved	**SA WG2**	**CN WG4**
S3-030304	Response LS on Template for Study on 3GPP work which is related to work in OMA	approved	**TSG T Vice Chair (K. Holley)**	
S3-030305	Adopting Cx-based protocols for several interfaces: NAF-BSF (D interface) and BSF-HSS (C interface), the interface between Authentication Proxy and HSS, and the interface between HSS and BM-SC for MBMS	approved	**CN WG4**	
S3-030306	Reply LS on 'Request for Information Regarding WLAN Interworking Impacts to UICC applications'	approved	**T WG3, SA WG1**	**SA WG2, ETSI EP SCP**
S3-030308	LS to CN1 on increasing the key length for GEA3	approved	**CN WG1**	**TSG GERAN**

Annex F: Actions from the meeting

AP 28/01: T. Viitanen to lead an e-mail discussion on Openness of Rel-6 IMS Network.

AP 28/02: B. Owen to lead an e-mail discussion on SA set-up procedure in Rel-5.

AP 28/03: SA set-up procedure in Rel-5 problem to be reported to TSG SA by SA WG3 Chairman.

AP 28/04: B. Sahlin to lead e-mail discussion based on TD S3-030243 on impacts of SIGTRAN on TS 33.210 for input to SA WG3 meeting #29.

AP 28/05: A. Escott to lead e-mail discussion on "potential Man-In-The-Middle threat providing IMEISV in clear", related to TD S3-030225, for contribution to SA WG3 meeting #29.

AP 28/06: SSH to provide suggestions for profiling CMPv2 for 3GPP use and provide contributions on this at the next SA WG3 meeting.

AP 28/07: A. Van Moffaert to lead an e-mail discussion on structure and scope of the draft TS on bootstrapping of application security.

AP 28/08: D. Mariblanca to lead an e-mail discussion on Implications of the trust relation between the Cellular Operator and the WLAN Access Provider based on TD S3-030261 for conclusion at the next meeting.

AP 28/09: M Wivfesson to lead an e-mail discussion based on SA WG2 and SA WG4 responses to MBMS and DRM issues based on TD S3-030293 to create a new proposed LS to these groups.