3GPP TSG SA WG3 Security — S3#32 **S3-040002**
09 - 13 February 2004
Edinburgh, Scotland, UK

3GPP TSG SA WG3 (Security) meeting #31 Report

18-21 November 2003, Munich, Germany

Source: Secretary of SA WG3 (M. Pope, MCC)

Title: Draft report of SA WG3 meeting #31

Status: Approved at SA WG3 meeting #32

River Isar from Volksbad, Munich, Germany

Contents

1 Opening of the meeting

The SA WG3 Chairman, Mr. V. Niemi, opened the meeting and Welcomed delegates to Munich on behalf of the European Friends of 3GPP (EF3). The meeting was hosted in the Siemens Conference Centre. G. Horn, Siemens welcomed delegates to the Conference Centre and informed them of the domestic arrangements for the meeting.

2 Agreement of the agenda and meeting objectives

TD TD S3-030655: Draft agenda for SA WG3 meeting #31. Draft Agenda for SA WG3 meeting #31. This was introduced by the SA WG3 Chairman.

Objectives:

Technical items in Agenda Item 6 will be taken in reverse order, i.e. starting with 6.22, 6.21, 6.20, etc. It was also agreed that GAA should be taken before Presence for practical reasons (i.e. 6.9 followed by 6.18). The priority for the meeting was to get all draft TSs and TRs in form ready for presentation to TSG SA for information in the December TSG Plenary.

The agenda was then approved.

2.1 3GPP IPR Declaration

The Chairman made the following call for IPRs, and asked ETSI members to check the latest version of ETSI's policy available on the web server:

> The attention of the members of this Technical Specification Group is drawn to the fact **that 3GPP Individual Members have the obligation** under the IPR Policies of their respective Organizational Partners to **inform their respective** Organizational Partners **of Essential IPRs they become aware of**.
>
> The members take note that they are hereby invited:
>
> - to investigate in their company whether their company does own IPRs which are, or are likely to become Essential in respect of the work of the Technical Specification Group.
>
> - to notify the Director-General, or the Chairman of their **respective** Organizational Partners, of all potential IPRs that their company may own, by means of the IPR Statement and the Licensing declaration forms (e.g. see the ETSI IPR forms http://webapp.etsi.org/Ipr/).

3 Assignment of input documents

The available documents were allocated to their relevant agenda items.

4 Meeting reports

4.1 Approval of the report of SA3#30, Povoa de Varzim, 6-10 October, 2003

TD S3-030656: Draft Report of SA WG3 meeting #30. The draft report was reviewed on-line and comments provided.

Actions from the meeting:

AP 30/01: Eric Gauthier (Orange, Switzerland) to lead an e-mail discussion on GPRS over-billing. Discussion started. Proposal that GPRS over-billing issues can be overcome when GPRS contexts are initiated by the network (pushed). SA WG2 are considering this proposal. Another Proposal to look at the problem in a general way and other scenarios were requested from Members and the possible (maybe partial) standardisation of the Firewall interfaces is being considered. For Firewall companies, their advice is being asked and they can either become 3GPP Members or Eric will act as a proxy between their views and bringing them to SA WG3 for consideration. **Information on this will be sent to the SA WG3 e-mail list.** SA WG2 work results need to be considered before deciding on the final way forward. It was agreed to hold an evening session on this issue lead by E. Gauthier. This was then completed.

AP 31/01: B. Sahlin to send IETF firewall-standardisation information to the e-mail list.

AP 30/02: M. Blommaert to check with authors of TD S3-030499 whether the quote on SIM is their understanding or an editorial error in the LS.
It was reported that this was an editorial error in Release 1999 which had already been corrected in Rel-5. Completed.

AP 30/03: M. Pauliac to run an e-mail discussion on the SSC Informative Annex on Key Pair Storage. 2 weeks for comments, 1 further week to check the implementation in the draft TS to be used for any Pseudo-CRs at the next meeting.
Completed. Document provided to this meeting.

AP 30/04: B. Wilhelm to ask LI group to investigate the LI impacts of the tunnelling solution for WLAN interworking.
Ongoing. e-mail discussion initiated. Discussion expected in the parallel LI meeting in London.

AP 31/02: B. Owen to contact SA WG3 LI group for results of LI impact of tunnelling solution for WLAN during the meeting.

AP 30/05: B Owen to respond to LSs on GUP from meeting #29, informing the senders that there are still open issues in SA WG3.
Completed. e-mail sent to contact persons.

AP 30/06: J. Abellan to draft an LS reply to TD S3-030511 for e-mail approval. Drafting by 14 October, Comments by 20 October and Approval 23 October 2003.
Completed.

AP 30/07: Rapporteurs of SA WG3 Work Items to provide the SA WG3 Secretary with updates to the Work Plan by 24 October 2003.
Completed. Rapporteurs were asked to make more effort to provide updates to the Work Plan.

The updated report was then approved and will be placed on the FTP server as version 1.0.0.

Secretary's note: The Attendees list and Voting list will be updated and verified before placing version 1.0.0 on the FTP server.

TD S3-030657: Draft Report of Joint SA WG3 / CN WG1 session 7 October 2003. The draft report was reviewed on-line and was endorsed without change.

5 Reports and Liaisons from other groups

5.1 3GPP working groups

TD S3-030671: LS on security of the Diameter protocol for the Gq interface. This was introduced by France Telecom and asked SA WG3 to give guidance on the following security issues with the Diameter protocol:

- *requirement of end-to-end security if the third party AF is located within an un-trusted domain;*
- *use of the Diameter CMS Security Application draft for end-to-end security and availability of the RFC in the Release 6 timeframe.*

A related LS had been sent to SA WG2 in S3-030444 and it was agreed to provide a new LS to CN WG3, copied to SA WG2 attaching the LS and adding the clarification that if NDS/IP is used, then there cannot be any un-trusted proxies in the link in order to preserve security. It was also noted that the IETF document is not in the Rel-6 dependency list. This LS was drafted in TD S3-030765 and reviewed. It was modified slightly in TD S3-030810 and approved.

TD S3-030680: LS (from SA WG1) on Privacy and Security Requirements within GSM/UMTS Devices. This was introduced by Vodafone and asked SA WG3 to investigate how unauthorised access shall be prevented to user and network operator confidential information in GSM and UMTS devices and that SA WG1 would also welcome SA WG3's recommendations for any new Stage 1 requirements that are identified during the investigation. SA WG3 considered that the solutions should be done in other bodies than 3GPP (e.g. JAVA community), whereas the need to provide some high-level requirements should be investigated and decided by SA WG1. An LS response was drafted in TD S3-030766 which was modified slightly in TD S3-030809 and approved.

TD S3-030687: CR to 33.108: CS Section for 33.108 – User data packet transfer (Rel-6). This was for discussion and finalisation in the parallel LI Group meeting and will be provided to SA WG3 for e-mail approval when agreed by the LI Group. The CR was noted at this time.

TD S3-030688: CR to 33.108: CS Section for 33.108 – LI Management Operation (Rel-6). This was for discussion and finalisation in the parallel LI Group meeting and will be provided to SA WG3 for e-mail approval when agreed by the LI Group. The CR was noted at this time.

5.2 IETF

There were no specific contributions under this agenda item.

5.3 ETSI SAGE

Per Christoffersson reported on issues raised within SAGE:

SAGE had an action on the suitability of reducing the Randomness of RAND from 128 to 80 bits in order to use the special-RAND was discussed and investigated by SAGE and it was concluded that this was acceptable. It was further reported that the conclusions allowed a reduction down to 64 bits as a minimum for RAND.

A5/3 - CC, EDGE and GEA3 variations. Difference is bit-pattern. Shall stay with same inputs for A5/4 or produce 3 new inputs? - SAGE require more time to investigate and SAGE therefore asked for a delay of another meeting before submission to SA WG3.

5.4 GSMA SG

GSMA SG report and LS:

TD S3-030682: LS (from GSMA SG) on solutions to solve the A5/2 issue. This LS was introduced by Louis Finkelstein, Motorola (on behalf of Charles Brookson) and requested operators and manufacturers to comment on the impact of the various solutions to solve the A5/2 issue. The solutions include removing A5/2 from the handsets, offering A5/1 (and maybe A5/3) to a wider group of operators, increase the number of authentications, allowing the users to select which algorithm their handset support, the special RAND solution, solutions that require changes to both the mobile and visited and home networks. The GSMA SG invited comments from Operators, GSMA and Manufacturers on the following:

- Removal of A5/2 from the handset;
- Wider availability of A5/1;
- Increase in the number of authentications;
- User configurability of the handset;
- Infrastructure impact;
- Updates to BTSs, BSCs and MSCs;
- Network timing.

It was reported that the GSMA had already started a survey amongst Operators and will collate the results.

Delegates were asked to take this LS back to their companies for internal discussion and comment, and to respond to the GSMA SG via David Maxwell dmaxwell@gsm.org. The LS was noted by SA WG3.

Eric Gauthier then gave a report of the GSMA SG activities. On the IMEI he indicated that IMEI integrity is now a priority work item for the GSMA board. GSMA SG is finalising a document that defines handset security requirement with the input from TWG and EICTA. GSMA will then send this document to manufacturers. In addition, a RFI was sent out to various organisations to request information on a service called Wireless Response Emergency Service. This service is similar to the CERT service but specialised from mobile operators and equipment manufacturers. Regarding the LS "Effects of Service 27/38 on 2G/3G Interworking and Emergency Call" that GSMA SG received from SA WG3: GSMA SG gave guidance based on SA WG3 views that there might be security risks. GSMA SG realizes that there may be other considerations (legal, licence, etc.) so GSMA SG passed the LS on to other GSMA Groups (e.g. SERG).

Tuesday evening session on GPRS Over-billing:

During the Tuesday evening session on GPRS Over-billing (GOB) chaired by Eric Gauthier, the participants brainstormed on different similar attack scenarios. No other scenarios were identified although the GOB scenario could be used for different purposes (such as scanning the customer terminal). There are two current solutions to GOB: one based on a GTP-aware firewall and the other based on synchronisation between the GGSN and the Gi firewall. It was agreed that the first solution could not be standardised by 3GPP. However the second one should be considered. An example of synchronisation protocol between the GGSN and the Gi firewall is RADIUS. Although, 5 out of 6 of the manufacturers present said their GGSN supported the RADIUS protocol, other alternatives should also be considered such as other IETF standards (e.g. a recent Midcom proposal) and protocols standardised by SA WG2 (e.g. recent proposal to synchronise the GGSN and the application server). Furthermore, the GOB scenario should also be considered in a WLAN interworking environment. Finally it was agreed that standardisation and/or guidelines to operators should be considered to solve this issue.

TD S3-030694: MMS Security Considerations Version 1.0.0. This was introduced by the MMS Representative (A. Bergmann). The purpose of the task was to study the security related issues of MMS and to produce input to SA WG3, the GSMA SG and OMA, in order to motivate work on countermeasures. It was also a part of the task to suggest countermeasures and security requirements, where applicable. The document therefore analysed threats and countermeasures. Mr. Bergmann was thanked for the presentation of the document and delegates were asked to consider the content in their companies and work. Companies were asked to look into possibility of the provision of human resources for the work on MMS and to try to organise a MMS Workshop in January/February 2004 on the organisation and content of the standardisation work across the different involved bodies.

The document was then noted. It was decided to run an e-mail discussion to plan the work for standardisation across the different involved bodies and what will be standardised. A. Bergmann agreed to chair this discussion and potentially arrange the MMS Workshop in January/February 2004.

AP 31/03: A. Bergmann to run an e-mail discussion on the MMS standardisation work and to organise a Workshop in January/February 2004 across the involved bodies if necessary.

5.5 3GPP2

There were no specific contributions under this agenda item.

5.6 OMA

There were no specific contributions under this agenda item.

5.7 Other groups

TD S3-030718: Presentation Slides: Liberty Alliance Project - Setting the Standard for Federated Network Identity. An updated version in TD S3-030764 was presented by Nokia and provided an overview of the Liberty Alliance Project. The presentation was provided for information and was noted.

TD S3-030719: Presentation Slides: Potential synergies between Liberty and 3GPP. This was presented by Nokia and provided potential synergies between Liberty and 3GPP. The presentation was provided for information and was noted.

Delegates were encouraged to contact the presenter off-line for more information or specific questions.

TD S3-030757: T1P1.5 Lawful Intercept. This was provided by T1P1.5 and detailed the comments to a Ballot on an LI document. It was considered that the LI Group should check this document and in particular the adverse comments that are made about TS 33.108. SA WG3 LI Group were asked to report back to SA WG3 any issues raised by this document and comments. The document was noted at this time.

6 Work areas

NOTE: TSs and TRs agreed here for presentation to TSG SA #22: Any comments need to be sent to the editors by 30 November 2003. The editors are to send them to M. Pope for editorial clean-up and presentation to TSG SA by 5 December 2003.

6.1 IP multimedia subsystem (IMS)

TD S3-030712: Proposed CR to 33.203: Ensuring the correct RAND is used in synchronization failures (Rel-5). This was introduced by **3** on behalf of **3**, Nokia, Vodafone and Ericsson. The CR was updated to clarify the text in TD S3-030768 and was approved.

TD S3-030713: Proposed CR to 33.203: Ensuring the correct RAND is used in synchronization failures (Rel-6). The CR was updated to clarify the text in TD S3-030769 and was approved.

TD S3-030726: Proposed CR to 33.203: Network behaviour of accepting initial requests (Rel-5). This was introduced by Nokia. There was some reservation over the scope of the proposal, as some appeared to be in the domain of CN WG1. It was agreed to work on this off-line to create a new version. This was provided in TD S3-030770 with a Rel-6 "mirror" CR provided in TD S3-030771 which were both approved.

TD S3-030670: LS (from CN WG1) on Introducing the Privacy Mechanism in Stage 2. This was introduced by Lucent Technologies and was produced in response to the LS from SA WG3 in TD S3-030649. CN WG1 asked SA WG3 to revise the CR to make the appropriate references to RFCs. A CR approved at the previous meeting (TD S3-030648) was considered for modification in line with this LS and the one from SA WG1 in TD S3-030675 (see below).

TD S3-030675: Response (from SA WG2) for Introducing the Privacy Mechanism in Stage 2. This was introduced by Ericsson and asked SA WG3 to include a reference to TS 23.228 in section 5.3. It was agreed to do this and provide an updated version of the CR in TD S3-030648 from the previous meeting in TD S3-030772 which was approved.

TD S3-030798: This was introduced by **3** and proposed corrections to already approved CRs where a reference had been missed in the original CRs in TD S3-030601 and TD S3-030602. The updated CRs were provided in TD S3-030799 and TD S3-030800. This proposal was agreed and the CRs in TD S3-030799 and TD S3-030800 were approved to replace the CRs in TD S3-030601 and TD S3-030602.

TD S3-030725: Proposed CR to 33.203: Removing anti-replay requirement from Confidentiality clause (Rel-6). It was noted that the cover sheet showed the changes to be for Rel-5, although the editorial change was really for Rel-6. This CR was corrected for presentation to TSG SA in TD S3-030812 which was approved.

TD S3-030727: NDS and Openness of IMS. This was introduced by Nokia and proposed that SA WG3 endorse the following conclusions:

1. SA WG3 should decide the levels of security listed in section 3 of the contribution, and the security requirements associated with them, for Rel-6..
2. The NDS/IP TS 33.210 is proposed to cover the first level security in the informative annex.
3. TLS is proposed to resolve the second level of security for interworking scenario with non-IMS as the baseline for further development.

It was decided that these proposals should be discussed over e-mail for contribution and decision at the next meeting. T. Haukka agreed to run the e-mail discussion on this.

AP 31/04: T Haukka to run an e-mail discussion on TD S3-030727. Comments by 23 December 2003, conclusions to e-mail list 15 January 2004.

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

There were no specific contributions under this agenda item.

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

There were no specific contributions under this agenda item.

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

TD S3-030661: TS 33.310 V0.6.0: Network Domain Security; Authentication Framework (Rel-6). The updated draft TS was noted.

TD S3-030705: Pseudo-CR to 33.310: Removing outdated editor's notes. This editorial Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-030677: Pseudo-CR to 33.310: Clarification of SEG certificate profiling. This was introduced by Siemens on behalf of Nokia, Siemens, T-Mobile and Vodafone. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-030691: Pseudo-CR to 33.310: Removal of unnecessary restriction on serial number. This was introduced by Siemens on behalf of Siemens, Nokia, SSH and T-mobile. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-030706: Pseudo-CR to 33.310: Recommendation to SEG certificate and IKE profiling. This was introduced by Nokia on behalf of Nokia, Siemens and Vodafone. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-030707: Pseudo-CR to 33.310: Local repository access clarification. This was introduced by Nokia on behalf of Nokia, Siemens, T-Mobile and Vodafone. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

The Rapporteur was asked to update draft TS 33.310 with the agreed changes and distribute it to M. Pope for presentation to TSG SA #22 for information.

6.5 UTRAN network access security

TD S3-030754: Enhancements to GSM/UMTS AKA. This was introduced by Ericsson and proposed a key separation mechanism for use as a stronger mechanism to guard against A5/2 attacks. It was clarified that this was a more long-term solution for consideration post-Rel-6. Contributions were invited on this over the e-mail list.

TD S3-030753: CR's on "Handling of key sets at inter-system change". This was introduced by Ericsson and proposed to withdraw documents TD S3-030625 and TD S3-030626 (CRs to 33.102: Handling of key sets at inter-system change, originally proposed by Ericsson and approved by SA WG3) and that these documents are not forwarded to the next TSG SA plenary in December 2003 because other WGs have not agreed equivalent changes and a complete package of CRs should be approved at the same time. It was decided to wait until the outcome of the stage 3 work is known and then re-develop alignment CRs for the stage 2. **These CRs were therefore postponed and will not be presented to TSG SA for approval.**

TD S3-030672: LS to SA3 on Clarification on use of Re-attempt Information element in Authentication Failure Report service. This was introduced by the SA WG3 Chairman. CN WG4 asked SA WG3:

Question 1: What is the purpose of the 'Re-attempt' parameter to be included in Authentication Failure Report Service? Particularly, how the HLR utilize this information.
Question 2: What is a situation where 'Re-attempt' parameter is set in VLR and SGSN.

It was agreed to have an e-mail discussion on this lead by C. Blanchard.

AP 31/05: C. Blanchard to lead an e-mail discussion on the questions from CN WG4 in TD S3-030672. Discussion and comment deadline 17 December 2003. Draft response created by 24 December 2003. Approved response by 5 January 2004.

6.6 GERAN network access security

TD S3-030668: Reply LS (from CN WG1)on Special-RAND mechanism. A proposed response to this LS from France telecom was provided in TD S3-030693, section 4, which was considered. The proposed replies were agreed and included in a response LS in TD S3-030802 which was approved.

TD S3-030669: LS on Special-RAND mechanism. This was introduced by Siemens. This was provided by CN WG4 for information and was in-line with SA WG3 activities. The LS was noted.

TD S3-030693: More elements on the Special RAND mechanism. Section 4 of this contribution was used as a response to TD S3-030668. This was introduced by Orange and suggested that SA WG3 endorse the principle of limiting the standardisation work for special RAND to special RAND format and UE behaviour, as the HLR/AuC internal procedure is out of the scope of 3GPP. **SA WG3 agreed as a principle that the main focus of the SA WG3 special RAND work was for the special RAND format and the UE behaviour. The internal HLR/AuC behaviour will not be standardised by SA WG3.** It was recognised that this decision may need to be reviewed in the light of any issues that come to the attention of SA WG3 in the future. It was also noted that the Emergency call issues need to be studied for any possible impact of the special RAND work.

Orange also proposed that additional information over the use of the mechanism is included into some GSMA document as recommendation to operators. This was considered to be the responsibility of the GSMA and Orange were invited to contact the GSMA on this matter.

TD S3-030698: Proposed CR to 43.020: Introducing the special RAND mechanism (Rel-6). This was introduced by Orange on behalf of Orange and Vodafone and proposes the changes needed to introduce the special RAND mechanism into TS 43.020. It was recognised that there were other changes needed to the affected sections and it was considered bad practice to approve these changes now and then further change the specification in the near future (including a statement about the bit-ordering assumptions in the document). As this was a Rel-6 change, the CR was endorsed as a basis for further elaboration for final approval at the next meeting. **S. Fouquet agreed to co-ordinate inputs to these sections and provide an updated CR for the next meeting**.

TD S3-030761: Proposed CR to 33.102: Introducing the special RAND mechanism (Rel-6). This was introduced by Vodafone on behalf of Orange and Vodafone and proposed the introduction of equivalent mechanism as for TD S3-030698 into 33.102. It was agreed that this could await approval until when the CR to 43.020 is finalised and updated if necessary for the next meeting.

6.7 Immediate service termination (IST)

There were no specific contributions under this agenda item.

6.8 Fraud information gathering system (FIGS)

There were no specific contributions under this agenda item.

6.9 GAA and support for subscriber certificates

TD S3-030662: TS 33.220 V0.1.1: Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (Rel-6). This was introduced by the Rapporteur and included changes agreed by SA WG3. The document was noted and used for updates with Pseudo CRs below. Completeness estimate: 45%

TD S3-030728: Pseudo-CR to 33.220: Bootstrapping procedure: merging of last two messages. This was introduced by Nokia. This Pseudo-CR was approved for inclusion by the editor in the draft TS.

TD S3-030743: Key separation in a Generic Bootstrapping Architecture. This was introduced by Siemens and proposes some changes to the draft TS and a Pseudo-CR was attached to implement the proposed changes. A parameter n is proposed for use to generate keys based upon parts of the DNS name of the NAF, allowing differentiation from the full DNS name to up to the rightmost 7 parts of the DNS name. It was clarified that AKA is always run once to derive Kc and then once again to provide the differentiable Key and that only one key is distributed to an individual NAF. The change in section 4.2.2.1 was changed to read: "The BSF can restrict the applicability of the key material to a defined set of NAFs by using a suitable key derivation procedure." The use of "NAF_Id" was agreed to be changed to "NAF_Id_n". The Pseudo-CR was updated with agreed changes and updated in TD S3-030793 which was agreed for inclusion in the draft TS. **P. Christoffersson agreed to ask SAGE to advise SA WG3 on suitable algorithm(s) for this mechanism, taking into account the AKA-EAP and AKA-SIM key derivation functions.**

TD S3-030704: Pseudo-CR to 33.220: Transaction Identifier independence for different NAFs or NAF groups. This was introduced by Huawei Technologies Co., Ltd. After some discussion it was thought that other issues on synchronisation and lifetime need to be finalised and then this issue can be correctly dealt with. The Pseudo-CR was therefore rejected at this time and the issue should be revisited when the other issues are stabilised. New contributions were invited on this.

TD S3-030729: UE triggered unsolicited push from BSF to NAFs. This was introduced by Nokia and discussed and proposed a possibility for UE to trigger BSF to do an unsolicited push of transaction identifier (TID), NAF specific shared secret (Ks_naf), and optional subscriber profile information (TID, Ks_naf, and the profile are later referred as “bootstrapping information”) to one or more NAFs in order to simplify procedures during shared secret usage over Ua interface. Overhead issues were raised and it was considered that some evaluation of this was needed. The attached Pseudo-CR was therefore rejected at this time and the issue should be revisited when the overhead issue is stabilised. New contributions were invited on this.

TD S3-030742: Application specific user profiles in GBA. This was introduced by Nortel Networks and proposed that the requirements with respect to transferring application-specific user/subscriber profiles from HSS to BSF (and BSF to NAF) be removed from the GBA. A Pseudo-CR implementing this was attached to the contribution. The Pseudo-CR was modified to re-insert the requirements on the Z-interfaces and to add editors notes and was updated in TD S3-030794 which was agreed for inclusion by the editor in the draft TS.

TD S3-030663: TS 33.221 V0.1.1: Generic Authentication Architecture (GAA); Support for Subscriber Certificates (Rel-6). This was introduced by the Rapporteur and contained the changes agreed by SA WG3. The draft TS was noted and used for further Pseudo-CRs.

TD S3-030667: "Updated Annex C to 33.109: Key pair storage". This was introduced by the Rapporteur and proposed to add a new informative annex to the draft TS. This was agreed.

TD S3-030683: Pseudo-CR to 33.221: Results of risk analysis in the “Key Pair Storage” informative annex. This was introduced by Gemplus on behalf of Gemplus, Giesecke & Devrient, Oberthur, Schlumberger. It was commented that the informative annex should not mandate functionality and that the operator should be allowed the choice of storage of the Private keys. The Pseudo-CR was revised in line with comments in TD S3-030795 which was agreed for inclusion by the editor in the draft TS.

TD S3-030686: Pseudo-CR to 33.221: on clarifications on Certificate enrolment using pre-certified keys. This was introduced by Schlumberger on behalf of Schlumberger, OCS and Gemplus. The proposal for "4.1 (really 4.3) was removed and a better position will be sought for the text. The CR was updated off-line to include comments received and re-presented in TD S3-030796 and the Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-030684: Pseudo-CR to 33.221: on enrolment of keys in a UICC application. This was introduced by Schlumberger on behalf of Schlumberger, OCS and Gemplus. It was agreed that the occurrences of UICC should be replaced with WIM where appropriate and a note added stating that other applications may act like the WIM and be done in the same way. The CR was updated off-line to include comments received and re-presented in TD S3-030797 and the Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-030685: Pseudo-CR to 33.221: on on-board key generation in a UICC. This was introduced by Schlumberger on behalf of Schlumberger, OCS and Gemplus. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-030730: Subscriber Certificate Enrolment Protocol. This was introduced by Nokia and discussed Subscriber Certificate Enrolment Protocol solutions. Nokia concluded that the enrolment of subscriber certificates as specified in the contribution has several synergies with the OMA based enrolment:

- 3GPP specifications are in line with OMA specifications.
- The OMA PKI portal may be also used in subscriber certificate enrolment provided that PKI portal is able to do GBA base authentication, i.e. it assumes the role of a NAF.
- Code from OMA based enrolment may be reused on the UE for doing the subscriber certificate enrolment.

Nokia proposed that SA WG3 endorse the subscriber certificate enrolment procedures described in the contribution (section 2.3) as the working assumption for TS SSC. A Pseudo-CR implementing the proposals was attached to the contribution. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-030664: TR 33.919 V0.1.0: Generic Authentication Architecture; System Description (Rel-6). This was introduced by the Rapporteur and was noted. The TR will be used for further Pseudo-CRs to update it.

TD S3-030716: Pseudo CR to GAA TR 33.919. This was introduced by Alcatel. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

The updated draft TR will be forwarded to TSG SA #22 for information.

TD S3-030722: User authentication process decision. This was introduced by Ericsson and suggested a general approach to be considered by applications regarding the user authentication in order to make the application decision flexible. After some discussion on the proposal, it was agreed to add an editors note and incorporate it into the updated draft TS. This Pseudo-CR was then agreed for inclusion by the editor in the draft TS.

TD S3-030665: 3GPP TS 33.222 V0.1.1: Generic Authentication Architecture (GAA); Access to Network Application Functions using HTTPS (Rel-6). This was introduced by the Rapporteur and included agreed changes and was noted. The draft TS was used for Pseudo-CRs.

TD S3-030717: Organization of Presence TS and HTTPS TS. This was introduced by Ericsson on behalf of Ericsson and Nokia and asked SA WG3 to endorse the following proposals:

1. The Presence Technical Specification shall be completed for release 6. It shall describe on stage 2 level how the Presence Service can be accessed securely using HTTP over TLS.
2. In release 6, the HTTPS TS shall describe secure access using HTTP over TLS for other services than Presence. Potential services to describe are conferencing, messaging, push, etc.. To avoid duplicate work in release 6, the HTTPS TS shall reference the Presence TS when appropriate.
3. For future releases, the two Technical Specifications could be restructured when needed.

These proposals were endorsed by SA WG3 for Release 6 and onwards.

TD S3-030721 and TD S3-030732 were on the same issue and were presented in turn and considered together:

TD S3-030721: Challenges in using shared-secret TLS with NAFs. This was introduced by Ericsson and proposed that SA WG3 adopts the following working assumptions related to the potential use of shared-secret TLS with NAFs:

- Shared-secret TLS is seen as an optimisation for TLS. Both the client and the NAF must also have full TLS implementation in addition to shared-secret TLS.
- The minimum implementation should include the normal TLS. Shared-secret TLS can only be optional for implementations.
- The solution should include a capability for negotiating between different TLS models. In particular, the NAF should be able to inform UE that it is able to use shared-secret TLS.
- Negotiation of TLS related security parameters needs to be further specified.

TD S3-030732: Using shared key TLS with NAFs. This was introduced by Nokia and described a way of using shared-key TLS between UE and NAF. The contribution proposed a way to use GBA based shared secret within GAA. Nokia proposed to make a decision to give a priority for the GBA supported shared-key TLS over the other possible solution and if the shared-key TLS is endorsed as the working assumption, then Nokia further proposed to add this work into dependency list of IETF as done for Rel-5 work.

In summary, Nokia proposed giving priority to shared-key TLS, whereas Ericsson proposed that this should be considered as an optional-for-implementation ad-on until there is more maturity in the IETF drafts.

It was agreed that this issue should be left open until IETF status progress can be assessed and try to make a decision at the next SA WG3 meeting. **Delegates were asked to study this issue and contribute to the next meeting**.

TD S3-030720 TD S3-030731 and TD S3-030744 were on the same issue and were presented in turn and considered together:

TD S3-030720: Comparison of authentication proxy solutions. This was provided by Ericsson and recommended that SA WG3 would keep the working assumption that the Presence Ut interface would benefit for having an authentication proxy. The working assumption should be that this proxy is of type "reverse proxy". Ericsson recommended clarification of forwarding proxy issues listed in the contribution.

TD S3-030731: Proxy and various HTTP services. This was introduced by Nokia and proposed to endorse the TD S3-030555 (Using shared key TLS with GAA NAFs) solution as working assumption.

TD S3-030744: Role of Authentication Proxy (AP-NAF) – Discussion and Pseudo-CRs to TSs on GAA/HTTPS and Presence Security. This was introduced by Siemens and proposed to include the following requirement in section 5.1 (Use of authentication proxy / requirements and principles) of TS 33.222 v011 (GAA/HTTPS) and in section 5.4.1 of TS 33.141 v020 (Presence Security):

"The use of an authentication proxy should be such that there is no need to manage the authentication proxy configuration in the UE.

Note: *This requirement implies that the authentication proxy should be a reverse proxy in the following sense: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers - in addition to web pages on disk or generated dynamically by CGI - making these pages look like they originated at the reverse proxy."*

In summary the Ericsson and Siemens proposals were in line and the Nokia proposal could accept it if the shared-key TLS is chosen rather than the reverse-proxy solution. It was clarified that there would still be a need for configuration with shared-key TLS as for the reverse-proxy solution. It was agreed that the text proposed by Siemens would be acceptable, and an editors note would be added as follows:

Editors' note: The above requirements may be revisited after the following issues are fully studied:
- *feasibility of shared-key TLS;*
- *terminal configurability*

Nokia proposed in addition in TD S3-030731 to consider the "special cookie" discussion where the UE inserts its own ID into the HTTP message and the proxy checks that the user is authorised. G. Horn and K. Boman agreed to consider this and comment to T. Haukka before 20 December 2003.

AP 31/06: G. Horn and K. Boman to consider section 3 of TD S3-030731 and comment to T. Haukka before 20 December 2003.

TD S3-030745: Technical solutions for access to application servers via Authentication Proxy and HTTPS - Pseudo-CRs to TSs on GAA/HTTPS and Presence Security. This was introduced by Siemens and proposed to include an informative annex in both the HTTPS and Presence draft TSs, as it is currently unclear whether both TSs will be completed within the Release 6 timeframe. If both TSs are completed in time, SA WG3 may decide later that all material on authentication proxies is to be contained in TS 33.222, and that TS 33.141 only is to make reference to TS 33.222. It was decided that this could be used as a starting point for further update in the future and so the changes were accepted to be included in the draft TSs. An editors' note was added as follows:

Editors' note: The text in this informative annex may need to be revisited if changes in the main body of the text are made.

TD S3-030746: Transfer of an asserted User Identity and Location of Access Control – Discussion and Pseudo-CRs to TSs on GAA/HTTPS and Presence Security. This was introduced by Siemens and proposed to include the following requirements in TS 33.222, section 5.1, and in TS 33.141, section 5.1.4:

- *Implementation of check of asserted user identity in the AS is optional.*
- *Activation of transfer of asserted user identity shall be configurable in the AP on a per AS base.*

It was agreed to add "asserted" as shown above.

Section 2 of the contribution was left for off-line discussion.

AP 31/07: T. Haukka and K. Boman to provide any comments on section 2 of TD S3-030746 to G. Horn.

TD S3-030749: Pseudo-CR to GAA/HTTPS doc: Initial text for the TS. This was introduced by Siemens. **It was agreed that editors' notes should be added about the initiation of the bootstrapping procedure being described in the GBA TS in section 4.2 and Annex Z. It was also agreed to add an editors note to Annex Z on the issue of co-location of BSF and NAF having an impact on implementation being ffs.** This Pseudo-CR was then agreed for inclusion by the editor in the draft TS.

Draft TS 33.222 was not considered complete enough at this time for forwarding to TSG SA #22 for information.

The Rapporteurs were asked to update draft TS 33.220 and draft TS 33.221 with the agreed changes and distribute it to M. Pope for presentation to TSG SA #22 for information.

6.10 WLAN interworking

TD S3-030689: Draft TS 33.234 V0.7.0 Wireless Local Area Network (WLAN) Interworking Security. This was introduced by the Rapporteur and included the changes agreed at the previous meeting. The draft TS was noted.

TD S3-030715: Pseudo-CR to 33.234: Clarification to re-authentication procedures. This was introduced by Nokia. This Pseudo-CR was approved for inclusion by the editor in the draft TS.

TD S3-030734: Pseudo-CR to 33.234: Re-authentication identities generation. This was introduced by Ericsson. This Pseudo-CR was approved for inclusion by the editor in the draft TS. Note: This implied the removal of the editors' note in section 7.15.

TD S3-030735: Pseudo-CR to 33.234: Editorial changes and informative annex in TS 33.234. This was introduced by Ericsson. This Pseudo-CR was approved for inclusion by the editor in the draft TS.

TD S3-030740: Pseudo-CR to 33.234: Only one active USIM application. This was introduced by Ericsson. There was some concerns over the correctness of this requirement and the author agreed to check and return with information. After checking it was found that the changes were no longer valid and the Pseudo-CR was withdrawn.

TD S3-030737: Split WLAN-UE: SIM Access Profile protocol in Bluetooth forum. This was introduced by Ericsson and proposed that SA3 discuss each proposal presented in this paper and takes a decision in order to progress the work in Bluetooth forum and also proposed that SA WG3 send an LS with the requirements in this paper to the Bluetooth Architecture Review Board (BARB) and the CAR groups, asking them to develop a new version of the SIM Access Profile for a split WLAN UE in work item WLAN Inter-working in 3GPP. It was agreed to send a LS to Bluetooth with the requirements identified and agreed after discussion of other contributions. An LS to Bluetooth groups was provided in TD S3-030780 and was reviewed and approved.

TD S3-030738: Split WLAN UE: Termination of EAP-AKA/SIM protocol. This was introduced by Ericsson and analysed different scenarios of Bluetooth security and the SIM Access Profile. The main issue from this analysis seemed to be the case when EAP-SIM protocol terminates in the Laptop and the threat exists that an attacker in the Laptop can get hold of the RAND and Kc, and distribute these publicly. Ericsson suggested that SA WG3 should consider whether this is seen as a major threat. Ericsson proposed that SA WG3 should take a decision on whether EAP-AKA and EAP-SIM shall terminate in the Laptop or the 3GPP UE. It was agreed to attach this contribution to the LS in TD S3-030780.

TD S3-030747: Pseudo-CR to TS 33.234 on Requirements on UE split. This was introduced by Siemens and proposed to include a related requirement into TS 33.234. A threat scenario was given to motivate the proposal. Revision-marked text to implement the proposal was included in the contribution. It was clarified that the threat described applied to offering service using the USIM keys and not a separate key set for a WLAN application. The proposed changes were discussed and agreed to be included with a change to make the note into an editors note, including the text "at least the Master Keys are computed". The editor was asked to make this change in the implementation.

TD S3-030739: Split WLAN-UE: Integrity protection on local interface. This was introduced by Ericsson and proposed that SA WG3 decide whether integrity protection will be required on the local interface between a Laptop and a UE. Ericsson did not see the need to add integrity protection on the local interface between the Laptop and the 3GPP UE and proposed to delete the requirement on integrity protection in TS 33.234. If SA WG3 kept the requirement, then Ericsson proposed that Bluetooth are informed of the requirement. It was agreed that modification of EAP parameters will cause EAP to fail. It was therefore agreed to remove this requirement from the draft TS.

AP 31/08: C. Blanchard was asked to check the changes made to the figures in TS 33.234 are reflected in the SA WG2 specification where they were originally copied from.

TD S3-030733: Implications of the A5/2 Attack for 3GPP WLAN Access. This was introduced by Ericsson on behalf of Ericsson and TeliaSonera and propose to insert their analysis and recommendations on the A5/2 attack scenarios for WLAN access in an Informative Annex C.3 of TS 33.234. The threat was clarified that is the A5/2 GSM keys can be recovered, then the EAP/SIM can be exploited for WLAN terminal impersonation towards the 3GPP network. There was a comment that the issue of recovering the keys by attacking the WLAN system and exploiting the GSM network should be examined and the scope of the analysis should be increased. Contributions were invited on this. It was agreed to include an informative annex to provide this attack scenario and countermeasures.

TD S3-030676: LS (from SA WG2) on Tunnel Establishment and Security Association. This was introduced by France Telecom. SA WG2 requested SA WG3 to evaluate the SA WG2 assumption that it is possible to separate the tunnel establishment and tunnel data handling into separate nodes, noting that these nodes are both in 3G networks, and not linked over the public internet. SA WG3 were requested to provide feedback to SA WG2. TD S3-030741 was related to this and was also considered for the reply LS.

TD S3-030741: End-to-end tunnelling: Security Considerations on resolution gateways. This was introduced by Nortel Networks on behalf of Nortel Networks, Siemens AG and Nokia and proposed that SA WG3 should communicate the conclusions of the contribution to SA WG2. A comment to this contribution was provided in TD S3-030763 which was considered.

> TD S3-030763: Comments on S3-030741: Security Considerations on resolution gateways. This was introduced by Huawei Technologies Co., Ltd. and provided comments on the proposals in TD S3-030741. There was some discussion and some comments were not fully supported. Others were agreed.

It was agreed that a response LS to SA WG2 should be developed taking into account the two contributions and discussions in the meeting on them. The LS was provided in TD S3-030789 which was reviewed and updated in TD S3-030808 and approved.

TD S3-030748: Security procedures for the set up of UE-initiated tunnels in scenario 3. This was introduced by Siemens and proposed that SA WG3 endorse the accompanying CR which implements three types of changes:

- Changes to headlines of existing sections and introduction of new subsections to make room for the specification of the security for scenario 3 in TS 33.234. These affect sections 4, 5, and 6.1.1 through 6.1.4 of TS 33.234.
- Changes agreed at SA3#30 regarding the use of IPsec ESP for data protection in the tunnel. These affect sections 6.2, 6.3, and 6.6 (new) of TS 33.234.
- The working assumption on tunnel set up procedures proposed in section 2 of this contribution. These affect sections 6.1.5 (new), 6.5 (new) and Annex X (new) of TS 33.234.

The attached Pseudo-CR to 33.234 was then considered and some additions made to the editors notes in section 6.1.5. The updated Pseudo-CR was provided in TD S3-030790 which was agreed for inclusion by the editor in the draft TS.

AP 31/09: D. Mariblanca to lead an e-mail discussion on the editors note about the use of public key signatures to authenticate the PDG in section 6.1.5 of the Pseudo-CR in TD S3-030790.

TD S3-030736: Security of EAP or SSID based network advertisements. This was introduced by Ericsson and concludes that neither EAP or link-layer mechanisms support the cryptographic protection of network-selection related advertisements today. Only a limited support for the protection of the chosen network is available. Ericsson suggested that this vulnerability is recognised as a current limitation and that means outside the protocols are used to mitigate its effects. Ericsson proposed sending a LS to SA WG2 informing them of this. It was reported that there is no requirement currently to cipher or protect this. An LS to SA WG2 was provided in TD S3-030791 which was updated in TD S3-030807 and was approved.

TD S3-030783: LS (from LI Group) on 3GPP WLAN interworking Lawful Interception Requirements. The SA WG3 LI Group asked SA WG3 to take the SA WG3 LI Groups' comments on WLAN interworking interception requirements of receiving unencrypted traffic in the roaming case into account when progressing work on 3GPP WLAN interworking security. There was a problem identified by SA WG3 LI Group in the roaming case as there may be an end-to-end tunnel from the roaming UE to the home network. It was commented that the Visited Network Operator is not involved in the set-up of the security tunnel. It was also commented that the Visited Network is involved in the set-up of Scenario 3, which may have an impact. The SA WG3 LI Group were asked to consider this. Delegates were asked to talk to SA WG3 LI Delegates in their companies to clarify the SA WG3 work and to clarify any issues.

TD S3-030762: Security Analysis on the SA WG2 resolution architecture. Huawei Technologies Co., Ltd. also provided a version containing revision marks from the originally submitted contribution, for easier appreciation of the changes made in TD S3-030788, however, as the original and revised documents were received after the document submission deadline, it was postponed due to lack of time. Huawei Technologies Co., Ltd. were invited to re-submit the contribution to the next meeting, if still relevant.

The Rapporteur was asked to update draft TS 33.234 with the agreed changes and distribute it to M. Pope for presentation to TSG SA #22 for information.

6.11 Visibility and configurability of security

There were no specific contributions under this agenda item.

6.12 Push

There were no specific contributions under this agenda item.

6.13 Priority

There were no specific contributions under this agenda item.

6.14 Location services (LCS)

There were no specific contributions under this agenda item.

6.15 Feasibility Study on (U)SIM Security Reuse by Peripheral Devices

TD S3-030666: Technical Report on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6). This was introduced by the Rapporteur on behalf of Toshiba, Intel, T-Mobile, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel and Gemplus and included changes agreed at the last meeting and during telephone conference calls and e-mail discussions. The TR was presented to SA WG3 for approval for presentation to TSG SA Plenary for information.

It was agreed that this was a feasibility study and therefore the title of section 6 should be "Potential requirements". It was also agreed that the title should be changed to "Feasibility Study on (U)SIM security re-use by peripheral devices on local interfaces". Comments on the requirements of section 6.1.1 were also made as the intension and expected scenarios for the potential requirements was unclear. It was clarified that the scenarios were as discussed over the conference calls and the TR outlined what would be needed for re-use of some UICC functions for Bluetooth access.

It was agreed that the scope should state that the FS would be used as a basis to future CRs to 33.234 as and when any of the proposals were developed by SA WG3. It was stated that it is not currently intended to develop this FS further into a 3GPP TS.

The rapporteur updated the document with the comments and provided the document again in TD S3-030779. The new version was reviewed and some minor changes made and the final version (without revision marks) was provided in TD S3-030792 which was **approved for presentation to TSG SA #22 for information.**

6.16 Open service architecture (OSA)

There were no specific contributions under this agenda item.

6.17 Generic user profile (GUP)

TD S3-030759: LS (from SA WG1) on clarified requirements on synchronization for GUP. This was introduced by Ericsson and informed T WG1 about the synchronisation requirements in GUP. this was provided to SA WG3 for information and was noted. It was reported that Nokia had a proposal in line with this at the previous meeting in TD S3-030581 and delegates were asked to consider this for comments at the next meeting.

6.18 Presence

TD S3-030695: Draft TS 33.141 V0.2.0 Presence Service; Security. This was introduced by the Rapporteur and was reported as needing much more text and was about 10-15% complete. The draft TS was noted.

TD S3-030673: The requirement and feasibility of IMS watcher authentication. This was introduced by Nokia. CN WG1 asked SA WG3 to take their analysis of IMS watcher authentication requirements. The LS was noted.

TD S3-030674: Reply LS on "The requirement and feasibility of IMS watcher authentication". This was introduced by Nokia. SA WG2 informed SA WG3 that they did not have an opinion on the need for IMS watcher authentication as they considered this to be in SA WG3 competence. The LS was noted.

TD S3-030681: Reply (from SA WG1) on the requirement and feasibility of IMS watcher authentication. This was introduced by Nokia. SA WG1 informed SA WG3 that they did not any detailed requirement on the need for IMS watcher authentication as they considered that SA WG3 could find a suitable solution with the support of CN WG1 and SA WG2. SA WG1 requested a similar level of security for both IMS and non-IMS watchers. It was considered that the non-IMS watcher security should be made as good as the IMS watcher security. It was agreed that the "optionality" of password based authentication means optional for implementation. The LS was noted.

6.19 User equipment management (UEM)

There were no specific contributions under this agenda item.

6.20 Multimedia broadcast/multicast service (MBMS)

TD S3-030660: LS Response on potential USIM impact of the MBMS security framework. This LS had been approved over e-mail after SA3#30 and transmitted. The LS was noted.

TD S3-030678: Reply (from SA WG1) to LS on potential USIM impact of the MBMS security framework S1-031104; T3-030697). This was introduced by **3** and encouraged T WG3 to continue this work and informed them that SA WG1 will notify T WG3 with any further requirements as they are developed. The LS was noted.

TD S3-030756: Liaison (from Download+DRM group OMA) to 3GPP SA WG4 and SA WG3 on issues on DRM for PSS and MBMS streams. This was introduced by Ericsson. OMA DLDRM suggested that SA WG3 and SA WG4 consider the attached OMA DCF specification for the development of their specifications, specifically for the specification of the streaming mechanism for protected 3GPP PSS media. The related LS in TD S3-030758 was considered with this LS.

TD S3-030758: Liaison (from Download+DRM group OMA) to 3GPP SA WG4 and SA WG3 on issues on DRM for PSS and MBMS streams. This was introduced by Ericsson and informed SA WG4 and SA WG3 about:

- a recommendation for the choice of a stream cipher for continuous PSS media;
- Considerations on stream integrity protection for continuous PSS media;
- the DRM information to be conveyed to a terminal;
- a request from OMA DLDRM to provide a version of TS 26.244 that can be normatively referenced, by January 2004;
- a request to SA4 to include signalling of DRM support for PSS clients into the 3GPP PSS UAProf vocabulary;
- a request to SA3 for information on the requirements and solutions for protection of MBMS streams.

OMA DLDRM requested SA WG3 to note the information contained in the LS, and to reply in case there are questions or comments. OMA DLDRM would welcome a reply from SA WG3 on the requirements and solutions for protection of MBMS streams.

Following discussions and LS was produced to OMA in TD S3-030805 (see below).

TD S3-030750: Considerations on selective encryption and integrity protection for DRM protected PSS media streams. This was introduced by Ericsson, using presentation slides in TD S3-030776. Ericsson proposed:

- not to use selective encryption;
- to use integrity protection for DRM protected streams;
- that SRTP could be used for protection of PSS and MBMS streams.

More background was provided in section 2 of TD S3-030750. Details of the file format and input streaming was provided in the attachments.

It was commented that OMA DRM had not received a public review, and the proposed transform of SRTP had also not been reviewed by the IETF security experts.

It was agreed that as a principle, the 3GPP solution and OMA DRM solutions should be as closely aligned as possible.

There is an optional integrity protection in the requirements for MBMS, as there may be groups / receivers which can be fully trusted. It was noted that this was not covered by the OMA work.

The discussions resulted in the LS provided in TD S3-030777 (see below).

TD S3-030752: DRM usage for MBMS security. This was introduced by Nokia and presented principles by which Nokia proposed that the SA WG3 work on MBMS security can be aligned with the ongoing co-operation between OMA DRM group and SA WG4 group for PSS.

It was concluded after some discussion that the encryption proposals should be studied by ETSI SAGE in order to verify it's suitability. A LS to OMA should be provided informing them that AS counter mode is acceptable and selective encryption is being further studied by SA WG3. The LS was drafted in TD S3-030777 which was reviewed and updated in TD S3-030805 which was approved.

TD S3-030714: Draft TS 33.246 V0.2.2: Security of Multimedia Broadcast/Multicast Service. This was introduced by the Rapporteur and included changes agreed in discussions. The draft TS was noted.

Docs from S3#30

TD S3-030522: Differentiation of MBMS traffic protection mechanisms. This was introduced by Samsung Electronics and proposed changes to the section 5.3 *Protection of the transmitted traffic* of the draft TS to include the protection method details in the service announcement. It was considered that SA WG2 should be consulted on this proposal. An LS was provided in TD S3-030778 (see below).

TD S3-030523: MBMS service activation and Initial TEK distribution. This was introduced by Samsung Electronics and proposed changes to the section 5.2 *Key management and distribution* of the draft TS such that the network shall indicate the “Joining Availability Time” in the service announcement. It was considered that SA WG4 should also be consulted on this proposal. This was added to the LS in TD S3-030778, which was also sent to SA WG4 and copied to SA WG1 for information (see below).

TD S3-030778 LS to SA WG2, SA WG4, copied to SA WG1 on protection method indication in service announcement and Joining Availability Time. This LS was provided in response to contributions TD S3-030522 and TD S3-030523 (which were postponed from SA WG3 meeting #30). The LS was reviewed and updated in TD S3-030806 which was approved.

TD S3-030700: MBMS (re-)keying models. This was introduced by Siemens and proposed to adopt following working assumptions:

- *If only a UE-based solution will be developed then the point-to-point (re)-keying solution shall be as efficient as possible in viewpoint of consumed radio resources'. For a UE-based solution the adoption of DRM methods should be considered as they are specifically designed to run in a UE-based environment. In particular the OMA DRMDL solution should be considered for MBMS download, while for MBMS streaming more study is needed.*
  This working assumption was endorsed by SA WG3. It was noted that the point-to-multipoint also needs to be as efficient as possible and that the solution should be **ME-based**, rather than **UE-based**.
- *If a UICC-based solution will be developed then the design of a UICC-based solution shall take care that the security is as high as possible but the solution shall at the same time be cost-efficient. In particular there has to be a way to recover from the situation where secrets from within one single UICC are revealed by an attacker.*
  This working assumption was endorsed by SA WG3. It was noted that the cost-efficiency requirement holds for all potential solutions. It was commented that the impact on the breaking of a single UICC needs to be analysed to determine the recovery actions required.

Following requirement for a UICC-based solution (to be incorporated in TS 33.246) was proposed:

- *The point-to-point key delivery procedures for the 'generate KEK'-step shall give assurance to the BM-SC where the KEK has been stored. The UE shall not be able to simulate or replay any assurance indication during that procedure.*
  The requirement that the BM-SC should know where the KEK has been stored was agreed in principle by SA WG3. Note that the definition of "generate KEK" needs review and clarification before inclusion in the draft TS.

TD S3-030690: 3GPP Over the Air (OTA) procedures applied to BAK Distribution and MBMS Subscription management. This was introduced by Schlumberger on behalf of Schlumberger, Qualcomm, Gemplus and OCS. The contribution concludes that OTA mechanisms are the existing 3GPP standard way for point-to-point communication between the UICC and the network and provide all the functionality required for efficient, secure MBMS key management and proposed to reuse these existing 3GPP mechanisms for BAK distribution and MBMS management operations instead of reinventing new ones.

It was clarified that OTA is an interface between the home network and the OTA Gateway and that keys would be distributed from the BN-SC. It was noted that new interfaces would be needed for this.

TD S3-030699: MBMS UICC open issues. This was introduced by Siemens and concluded that without significant progress on the open issues highlighted in the contribution, a decision in this meeting in favour of a UICC-based solution within Rel-6 should not be made. Also the requirements on UICC-based solutions should be verified on completeness and stability before going further in that direction. Siemens clarified that many of the open issues included could be removed by the contributions present at the meeting. Comments were taken on the issues highlighted:

1-1. The requirement for acceptable on-time deliveries of UICC-keys to late MBMS-entrants are unknown. Stringent time settings could be a problem for OTA. It was commented that this should not be a problem in Rel-6 under normal operating conditions. Requirements were lacking on this issue.

1-2. No solutions (i.e. selected protocols) are yet available for connection OTA-servers to MBMS-server that reside in the VN. This was considered a general issue even for non-UICC solutions.

1-3. The use of OTA needs to be supplemented by a terminal mechanism that requests key updates. This was considered a general issue even for non-UICC solutions.

1-4. No estimations of the moderate free memory amount of existing pre Rel-6 UICC in the field is available. It was recognised that this needs further clarification ("probably" is not a sufficient definition of free-memory requirements). It was commented that the majority of current pre-Rel-6 UICCs do not have this available memory space (1 kbyte).

2-1. No solution for key deletion to the UICC is provided. The deletion of BAK to prevent access by stolen terminals was considered necessary and was considered an open issue.

2-2. No solution to bootstrap the MIKEY-run (the KEK-generation) is provided. This issue needs further consideration.

2-3. No detailed estimation of the complexity of terminating MIKEY at the UICC is available. This issue needs further consideration.

TD S3-030767: Impacts on the 3GPP network with a UICC based and a non-UICC based solution in MBMS. This was introduced by Ericsson and proposed that SA WG3 send a LS to SA WG2 and OMA asking whether a new interface between the BM-SC and OTA provisioning server can be standardized. Ericsson also proposed that SA WG3 should send a LS to various groups, such as SA WG2, OMA and T WG3, to comment on the issues mentioned in section 3 of the contribution and the architecture with a UICC based solution. It was commented that a proprietary OTA could be used to provide MBMS service on pre-Rel-6 UICCs (Java enabled).

TD S3-030697: MBMS Usage and Quality of Service based on BAK Distribution. This was introduced by Qualcomm on behalf of Gemplus, Oberthur, QUALCOMM Europe and SchlumbergerSema. The content of this contribution was based on SA WG1 requirements, some of which were no longer valid. It was noted that the application would need to be relied upon in this system. The document was then noted.

TD S3-030701: MBMS: Replaying of RAND values. This was introduced by Siemens and proposed to add the following requirement to the MBMS specification:

R5f: A UICC, realizing the function of providing session keys for decrypting the streaming data at the UE, shall only give session keys back to the UE if the input values used for obtaining the session keys were fresh (have not been replayed) and came from a trusted source.

Solutions for this requirement may be elaborated and its feasibility be decided at SA WG3 meeting #32 (Siemens withdrew the second proposal as it was obsolete due to previous agreements).

SA WG3 agreed that this requirement was needed if the UICC-based solution is chosen.

Contributions TD S3-030703 , TD S3-030751 , TD S3-030709 and TD S3-030723 were each introduced by their authors and then a general discussion was held.

TD S3-030703: Evaluation of re-keying methods. This was introduced by Huawei Technologies Co., Ltd. and proposed accepting the improved combined re-keying method or the simple PTP re-keying method:

1. If the combined re-keying method is accepted, it was proposed to adopt the improvement described in TD S3-030520 from SA WG3 meeting #30.
2 If the simple PTP re-keying method is accepted, it was proposed to add the figure and bullets proposed in TD S3-030521 from SA WG3 meeting #30 to the draft TS.

TD S3-030751: Further updates on Combined model for MBMS security. This was introduced by Nokia and proposed that the following are adopted as working assumptions in SA WG3:

1) Combined model adopted as a compromise between Simple and Two-tiered model;

2) ME based solution chosen as a solution for Rel-6;

3) GBA usage considered as a basis for authentication between UE and BM-SC;

4) In later releases, BM-SC shall be able to distinguish between different solutions used by the UE.

TD S3-030709: Composite MBMS Key Distribution. This was introduced by Samsung Electronics and proposed that SA WG3 adopt this composite method for MBMS key distribution, and especially, to select the proposed solution 2 for MBMS key distribution.

TD S3-030723: Migration of MIKEY in MBMS key management. This was introduced by Ericsson and proposed that before making a decision on key management solution SA WG3 should take a standpoint on the trust model that is applied in MBMS. That is, whether ME is trusted or not. Ericsson also proposed to adopt MIKEY as key management protocol for MBMS. MIKEY can support both ME and UICC based methods. Ericsson believed that MIKEY also provides smooth migration path to UICC based method.

Discussion of contributions TD S3-030703 , TD S3-030751 , TD S3-030709 and TD S3-030723:

Ericsson reiterated that they believed SA WG3 should make a decision taking into account the availability of a whole solution and the key management and traffic protection are linked together.

SA WG3 also needs to decide whether an ME or UICC based solution will be used.

It was proposed to try to have a combined solution taking ideas from the contributions.

It was also proposed that a migration would be needed and UICC based solution should be included for Rel-6 as it is easier to determine the UICC technology in the field than the variety of ME capabilities that will be available. Support of the UICC solution in Rel-6 would facilitate a migration path.

Ericsson commented that the cost against security strength of any mechanism also needs to be kept in mind and suggested that the MIKEY solution could be used for early deployment of a ME based solution which would include a migration path to UICC based solution if additional security was considered necessary by operators at a future time.

3 suggested a compromise to standardise both then ME and UICC based solutions for Rel-6 and allow the Market to decide on the choice. It was clarified that the UICC based solution would need to be mandated for implementation in Rel-6 networks. Ericsson suggested that the flows in figure 3 of their contribution could satisfy such a compromise solution.

Decisions: After some discussion SA WG3 agreed on the following:

It will be possible to run the whole MBMS security with ME only, but will also be possible to run key management using the UICC. A migratory path between the two solutions is needed and the solutions will be developed to allow this. Deviations between the two solutions would only be made for the benefit of the whole system (this implies the use of a 2-tiered system). The difference between the two solutions for delivering the low-level keys would be visible only inside the UE and secondly, the BMSC would know which solution is implemented in the UE side. A Rel-6 compliant UE will support both UICC based and ME based solutions and the Operator will have control over the choice of method used for MBMS services.

Telecom Italia expressed strong reservations to this compromise.

For the ME part, GBA and MIKEY (with possible 3GPP-specific enhancements, e.g. for the support of encrypted keys) will be used as a basis for the standardised solution. This does not rule out DRM based solutions, e.g. DOWNLOAD.

TD S3-030696: Adding Integrity to Counting Idle Mode terminals in MBMS. This was introduced by Qualcomm Europe and describes a concern is that a malicious UE may force a network operator to broadcast MBMS content when there are insufficient MBMS subscribers to warrant the broadcast. Therefore an attack on network resources may be launched. Qualcomm Europe proposed to add integrity to the registration procedure to prevent this attack on network resources. There was some discussion on the methods considered in RAN for counting / deciding which delivery method to use. It was reported that RAN WGs were considering connect and starting with point-to-point, then point-to-multipoint before opening up to full broadcast depending on the number of connects active. It was also reported that GERAN WGs had not yet decided on a method. It was decided that this issue should be studied by SA WG3 and contributions were invited on this subject if Members think this should be developed.

TD S3-030708: MBMS Traffic Encryption Key gradually Changing and Updating for streaming service. This was introduced by Samsung Electronics and proposed to adopt the described TEK gradually changing and updating for MBMS key management. A text proposal was provided in the contribution to implement the proposal. The idea was considered interesting, but puts an additional requirement upon the algorithm, which has already been decided upon. The cryptographic strength of this proposal would also need to be investigated. Further contribution was invited based on analysis of the issues around this.

TD S3-030710: Differentiation of MBMS traffic protection mechanisms. This was provided by Samsung Electronics at meeting #30 and had already been handled.

TD S3-030711: MBMS service activation and Initial TEK distribution. This was provided by Samsung Electronics at meeting #30 and had already been handled.

TD S3-030755: Some MBMS data flows. This was introduced by **3** and proposed some data flows to help complete the draft TS. 3 pointed out that some of the proposed changes may be controversial and delegates should study the impact of the proposals. There was some concern on the number of keys used and it was clarified that the proposal was for 2 keys for each multicast service. The Pseudo-CR was reviewed and updated in TD S3-030801 which was agreed for inclusion by the editor in the draft TS.

The Rapporteur was asked to update draft TS 33.246 with the agreed changes and distribute it to M. Pope for presentation to TSG SA #22 for information.

6.21 Key Management of group keys for Voice Group Call Services

TD S3-030658: SMG10 meeting report (extract on ASCI). This was introduced by BT Group and described the Voice Group Call Service concepts as provided in SMG 10 meeting in October 1998. The document was provided for information and was noted.

TD S3-030659: Use of the same algorithms for encryption of VGCS-calls as for normal GSM-speech calls (i.e. A5/0-A5/7). This was introduced by BT Group and makes some recommendations based on discussions previously held about Group Call Keys:

1) SA WG3 reconsider the use of a two key hierarchy;
2) SA WG3 should consider the use of additional inputs to the ciphering algorithm e.g. TETRA combines the cipher key with the Carrier Number (CN) and Base station Colour Code (CC) and Location Area identifier (LA) to prevent attacks on the encryption process by replaying cipher text to eliminate the key stream;
3) A distinguishing direction id may need to be added as an input to the ciphering algorithm.

It was clarified that the choice of ciphering algorithm was the subject of other contributions. It was commented that to obtain plaintext by the XOR technique was not a trivial task.

These recommendations had been captured in TD S3-030692 and therefore the contribution was noted.

TD S3-030692: Securing VGCS calls. This was introduced by Siemens on behalf of Siemens and Vodafone and proposed a different concept to secure GSM Voice Group Calls which has some similarities to TETRA. Some discussion on the scenarios and proposals ensued. BT Group reported that there were many services other than simple voice calls envisaged for this service and the security requirements for some are higher than simple telephone conversation protection (e.g. emergency Rail telemetry monitoring service) and key stream repeat could be a serious threat to the system.

The contribution proposed changes to the working assumptions:

C) On call set-up the GCR selects one group key and sends it to the BSS and the group key number to the UE which fetches the corresponding key from the USIM.
Comment: Changes required as the Group Key will not leave the UICC and GCR.
Proposed new text: On call set-up the GCR selects one group key, generates a temporary key with a RAND and sends the temporary key~~it~~ to the BSS and the group key number and RAND to the UE. The UE then asks the UICC to generate a temporary key based on the group key number and broadcasted information (RAND). ~~which fetches the corresponding key from the USIM.~~

D) Principle D was deleted as proposed. It was noted that Group Key Management would need further study.

E) Proposed to delete the note and to add following text: Any requirement for modification of the input parameters to A5 shall be achieved using a separate Key Modification Function (KMF). How this function is realized is currently under study.

F) Principle F was deleted as proposed.

G) Principle G was deleted as proposed.

H) Porposed to make the use of OTA for updating VGCS group keys to the UICC optional for the operator. This proposal was approved.

I) Principle was proposed for further study.

The paper concluded with the following proposals:

1) To agree that REQ-1 and REQ-2 need to be realized. **AGREED.** Depends on GERAN WG2 reply.
2) To discuss and decide if SA WG3 wants a solution for realizing REQ-3 and REQ-4 as this enhances VGCS call channel security above dedicated channel security. **Pending: Contribution invited.**
3) To wait for agreeing a solution for realizing REQ-3 and REQ-4 as inputs from GERAN 2 are needed to evaluate complexity and feasibility. **AGREED.**
4) To adopt the two-step approach and rationales from section 3 as a working assumption. **AGREED.**
5) To inform ETSI EP RT (GSM-R) on the progress of the discussions. **AGREED.** An LS was provided in TD S3-030773 which was revised in TD S3-030803 and approved.
6) To ask T WG3 to realize the needed functions on the USIM. **AGREED.** An LS was provided in TD S3-030774 which was revised in TD S3-030804 and approved.
7) To ask SAGE to select suitable key derivation/modification functions for both ME and UICC after deciding the input and output parameters. Minimal length of RAND should be requested.
P. Christoffersson to take early warning message to SAGE .
8) To decide whether all VGCS network interfaces and key derivation/modification functions shall already be able to support 128-bit cipher keys although no A5 cipher algorithm are yet in the field that support 128-bit keys. At least the key modification/derivation functions should be able to handle 128-bit keys for the input and output parameters. **AGREED.**
9) To inform GERAN WG2 about the above decisions (bullet point 2 and 8) and ask them for commenting a) if potential problems with CGI at handover can be expected and b) to select the right mechanism for broadcasting a RAND, GLOBAL_COUNT to generate the short term key from.
AGREED (also to check correctness of text changes in C) for channel use). See the LS in TD S3-030774.

TD S3-030760: Response LS (from SA WG1) on support of GSM SIM files (and services) on the USIM, and USIM changes for key management of Voice Group Call Services. This was introduced by Motorola and asked SA WG3 to continue work developing key management for ASCI / VGCS. It was noted that work is ongoing on this in SA WG3 and the LS was noted.

6.22 Guide to 3G security (TR 33.900)

There were no specific contributions under this agenda item.

7 Review and update of work programme

Due to lack of time to deal with this during the meeting, Rapporteurs and editors were given the action to provide the secretary with updates to the Work Plan for their respective Work Items. The Secretary, M. Pope undertook to send the current status in the work plan of SA WG3 Work Items on 24 November for update and return by 27 November 2003. **This was considered an important task, as TSG SA are expected to use the Work Plan status for determining the Rel-6 freeze date at TSG SA meeting #22 in December 2003.**

AP 31/10: M. Pope to send SA WG3 Work Plan status details to the mailing list on 24 November 2003. Rapporteurs and Editors to provide feedback to M. Pope by 27 November 2003 in order to have an accurate SA WG3 status in the work plan presented to TSG SA #22.

8 Future meeting dates and venues

There had been a discussion on the e-mail list following Qualcomms' announcement that they could only host the February 2004 meeting the week after planned at SA WG3 meeting #30.

More discussion was held over the meeting dates and venues. the 2-6 February overlapped with OMA meeting, 9-13 February with 3GPP2 and 16-20 February with a SA WG2 meeting. The results are shown in the table below.

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#32	09-13 February 2004	Edinburgh, UK	EF3
S3#33	11-14 May 2004	Beijing, China	Samsung
S3#34	06-09 July 2004 (TBC)	USA (TBC)	"NA Friends of 3GPP" (TBC)
S3#35	5-8 October 2004	Host required (Sophia?)	Host required (ETSI/EF3?)
S3#36	23-26 November 2004	Shenzhen, China	HuaWei Technologies
S3#37	February 2005	Australia (TBC)	Qualcomm (TBC)

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#12	27-29 January 2004	USA (TBA)	FBI (TBA)
SA3 LI-#13	14-16 April 2004	Europe (TBA)	TBA
SA3 LI-#14	20-22 July 2004	Combined with ETSI TC LI (Location TBA)	TBA
SA3 LI-#15	12-14 October 2004	USA (TBA)	TBA

TSGs RAN/CN/T and SA Plenary meeting schedule

Meeting	**2003**	**Location**	**Primary Host**
TSG RAN/CN/T #22	9-12 December 2003	Hawaii, USA	NA Friends of 3GPP
TSG SA #22	15-18 December 2003	Hawaii, USA	NA Friends of 3GPP
Meeting	**2004 DRAFT TBD**	**Location**	**Primary Host**
TSGs#23	March 9-12 & 15-18 2004	Phoenix, USA	
TSGs#24	June 1-4 & 7-10 2004	Korea	
TSGs#25	7-10 & 13-16 September 2004	USA	
TSGs#26	7-10 & 13-16 December 2004	To Be Decided	

9 Any other business

The following CRs from the LI group were received to avoid the need for e-mail approval:

TD S3-030787: Proposed CR to 33.108: Alignment of Lawful Interception identifiers length to ETSI TS 101 671 (Rel-6). This CR was approved.

TD S3-030786: Proposed CR to 33.106: References (Rel-6). There was a problem with the change to section 6 as it appeared to be incomplete. Also the base version number used was questioned. The CR was **not approved** and **the LI Group were asked to repair this over e-mail in time for TSG SA approval if possible**. The updated CR was provided in TD S3-030811.

TD S3-030785: Proposed CR to 33.108: Reporting TEL URL (Rel-6). This CR was approved. M. Pope agreed to ensure the final change section is indicated in the CR for TSG SA.

TD S3-030784: Proposed CR to 33.107: Reporting TEL URL (Rel-6). This CR was approved.

TD S3-030782: Proposed CR to 33.108: CS Section for 33.108 – LI Management Operation (Rel-6). This CR was approved. It was noted that only the content of figure B.1 has changed, not the title and M. Pope agreed to correct this before presentation to TSG SA for approval.

> Secretary's note: There were significant modifications necessary, so this CR was updated in TD S3-030813 for presentation to TSG SA.

TD S3-030781: Proposed CR to 33.108: CS Section for 33.108 – User data packet transfer (Rel-6). This CR was approved. It was noted that only the presentation of changes in sections B.2 was not clear and M. Pope agreed to correct this before presentation to TSG SA for approval.

> Secretary's note: There were significant modifications necessary, so this CR was updated in TD S3-030814 for presentation to TSG SA.

Close of meeting

The Chairman, V. Niemi, thanked delegates for their hard work during the meeting and the Hosts EF3 for the facilities at Siemens Conference Centre, Munich. He then closed the meeting.

It was agreed that the SA WG3 Chairman would produce a work plan for the handling of agenda items and time limits for the presentation of documents before the next meeting depending on the available contributions after the **document deadline which will be 2 February 2004 16.00 CET**.

It was agreed that contributions in direct response to input documents received could be accepted until a **second deadline of 4 February 2004, 16.00 CET**.

Annex A: List of attendees at the SA WG3#30 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
Dr. Selim Aissi	Intel Corporation S.A.	selim.aissi@intel.com		+01-503 264-3349	+01-503 264-1578	BE	ETSI
Mr. Hiroshi Aono	NTT DoCoMo Inc.	aono@mml.yrp.nttdocomo.co.jp		+81 468 40 3509	+81 468 40 3788	JP	ARIB
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 nv/sa	marc.blommaert@siemens.com		+32 14 25 34 11	+32 14 25 33 39	BE	ETSI
Mr. Krister Boman	ERICSSON LM	krister.boman@ericsson.com	+46 70 246 9095	+46 31 747 4055		SE	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 Christofferson	TeliaSonera AB	per.christoffersson@teliasonera.com		+46 705 925100		SE	ETSI
Mr. Kevin England	mmO2 plc	kevin.england@o2.com	+447710016799	+447710016799		GB	ETSI
Mr. Hubert Ertl	GIESECKE & DEVRIENT GmbH	hubert.ertl@de.gi-de.com	+49 172 8691159	+49 89 4119 2796	+49 89 4119 2921	DE	ETSI
Dr. Adrian Escott	3	adrian.escott@three.co.uk		+44 7782 325254	+44 1628 766012	GB	ETSI
Mr. Louis Finkelstein	MOTOROLA JAPAN LTD	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
Miss Sylvie Fouquet	ORANGE SA	sylvie.fouquet@francetelecom.com		+33 145 29 49 19	+33 145 29 65 19	FR	ETSI
Dr. Eric Gauthier	ORANGE SA	eric.gauthier@orange.ch		+41 21 216 53 08	+41 21 216 56 00	FR	ETSI
Ms. Tao Haukka	NOKIA Corporation	tao.haukka@nokia.com		+358 40 5170079		FI	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@siemens.com		+49 8963 641494	+49 8963 648000	DE	ETSI
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vodafone.com	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB	ETSI
Ms. Yingxin Huang	HuaWei Technologies Co., Ltd	huangyx@huawei.com		+86-10-82882752	+86-10-82882940	CN	CCSA
Mr. Robert Jaksa	HUAWEI TECHNOLOGIES Co. Ltd.	rjaksa@futurewei.com		+1 972 509 5599	+1 972 509 0309	CN	ETSI
Mr. Bradley Kenyon	HEWLETT-PACKARD France	brad.kenyon@hp.com		+1 402 384 7265	+1 402 384 7030	FR	ETSI
Mr. Pekka Laitinen	NOKIA Corporation	pekka.laitinen@nokia.com		+358 5 0483 7438	+358 7 1803 6852	FI	ETSI
Mr. Bernd Lamparter	NEC EUROPE LTD	bernd.lamparter@netlab.nec.de		+49 6221 905 11 50	+49 6221 905 11 55	GB	ETSI
Mr. Alex Leadbeater	BT Group Plc	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. David Mariblanca	ERICSSON LM	david.mariblanca@ericsson.com		+34 646004736	+34 913392538	SE	ETSI
Dr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com		+358504837327	+358718036850	FI	ETSI
Mr. Petri Nyberg	TeliaSonera AB	petri.nyberg@teliasonera.com		+358 204066824	+358 2040 0 3168	SE	ETSI
Mr. Nobuyuki Oguri	NTT DoCoMo Inc.	oguri@mmd.yrp.nttdocomo.co.jp		+81 46 840 3873	+81 46 840 3726	JP	ARIB
Mr. Bradley Owen	Lucent Technologies N. S. UK	bvowen@lucent.com		+44 1793 897312	+44 1793 897414	GB	ETSI
Mr. Anand Palanigounder	NORTEL NETWORKS (EUROPE)	anand@nortelnetworks.com		+1 972 684 4772	+1 972 685 3123	GB	ETSI
Miss Mireille Pauliac	GEMPLUS S.A.	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. Anand Prasad	NTT DoCoMo	prasad@docomolab-euro.com		+49-89-56824112	+49-89-56824300	JP	ETSI
Mr. Bengt Sahlin	ERICSSON LM	Bengt.Sahlin@ericsson.com		+358 40 778 4580	+358 9 299 3401	SE	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		+447880791303		FR	ETSI
Mr. Benno Tietz	Vodafone D2 GmbH	benno.tietz@vodafone.com		+49 211 533 2168	+49 211 533 1649	DE	ETSI

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Ms. Chikako Tsukada	NTT DoCoMo Inc.	tsukadac@nttdocomo.co.jp		+81 468403873	+81 468403726	JP	ARIB
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. Willy Verbestel	RIM	wverbestel@rim.net	+1 760 580 4585	+1 760 737 8428	+1 760 294 2125	CA	ETSI
Mr. Tommi Viitanen	Nokia Telecommunications Inc.	tommi.viitanen@nokia.com		+358405131090	+358718075300	US	T1
Ms. Monica Wifvesson	ERICSSON LM	monica.wifvesson@ericsson.com		+46 46 193634	+46 46 231650	SE	ETSI
Mr. Zhu yanmin	SAMSUNG Electronics	yanmin.zhu@samsung.com		+86-10-68427711	+86-10-68481891	GB	ETSI
Dr. Raziq Yaqub	Toshiba Corporation	ryaqub@tari.toshiba.com	+1-908-319-8422	+1 973 829 2103	+1-973-829-5601	JP	ARIB

46 Attendees

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #29, #30 and #31, the following companies are eligible to vote at SA WG3 meeting #32:

Company	Country	Status	Partner Org
3	GB	3GPPMEMBER	ETSI
ALCATEL S.A.	FR	3GPPMEMBER	ETSI
AT&T Wireless Services, Inc.	US	3GPPMEMBER	T1
BMWi	DE	3GPPMEMBER	ETSI
BT Group Plc	GB	3GPPMEMBER	ETSI
China Mobile Com. Corporation	CN	3GPPMEMBER	CCSA
DTI	GB	3GPPMEMBER	ETSI
ERICSSON LM	SE	3GPPMEMBER	ETSI
GEMPLUS S.A.	FR	3GPPMEMBER	ETSI
GIESECKE & DEVRIENT GmbH	DE	3GPPMEMBER	ETSI
HEWLETT-PACKARD France	FR	3GPPMEMBER	ETSI
HUAWEI TECHNOLOGIES Co. Ltd.	CN	3GPPMEMBER	ETSI
HuaWei Technologies Co., Ltd	CN	3GPPMEMBER	CCSA
Intel Corporation S.A.	BE	3GPPMEMBER	ETSI
Lucent Technologies	US	3GPPMEMBER	T1
Lucent Technologies N. S. UK	GB	3GPPMEMBER	ETSI
Mitsubishi Electric Co.	JP	3GPPMEMBER	ARIB
mmO2 plc	GB	3GPPMEMBER	ETSI
MOTOROLA JAPAN LTD	JP	3GPPMEMBER	ARIB
MOTOROLA Ltd	GB	3GPPMEMBER	ETSI
NEC EUROPE LTD	GB	3GPPMEMBER	ETSI
NOKIA Corporation	FI	3GPPMEMBER	ETSI
Nokia Korea	KR	3GPPMEMBER	TTA
Nokia Telecommunications Inc.	US	3GPPMEMBER	T1
NORTEL NETWORKS (EUROPE)	GB	3GPPMEMBER	ETSI
NTT DoCoMo	JP	3GPPMEMBER	ETSI
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
OBERTHUR CARD SYSTEMS S.A.	FR	3GPPMEMBER	ETSI
ORANGE SA	FR	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
RIM	CA	3GPPMEMBER	ETSI
SAMSUNG Electronics	GB	3GPPMEMBER	ETSI
Samsung Electronics Co., Ltd	KR	3GPPMEMBER	TTA
SchlumbergerSema	FR	3GPPMEMBER	ETSI
SIEMENS AG	DE	3GPPMEMBER	ETSI
Siemens nv/sa	BE	3GPPMEMBER	ETSI
T-MOBILE DEUTSCHLAND	DE	3GPPMEMBER	ETSI
TELECOM ITALIA S.p.A.	IT	3GPPMEMBER	ETSI
TELENOR AS	NO	3GPPMEMBER	ETSI
TeliaSonera AB	SE	3GPPMEMBER	ETSI
Toshiba Corporation	JP	3GPPMEMBER	ARIB
Vodafone D2 GmbH	DE	3GPPMEMBER	ETSI
VODAFONE Group Plc	GB	3GPPMEMBER	ETSI

43 Voting Members

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030655	Draft agenda for SA WG3 meeting #31	SA WG3 Chairman	2	Approval		Approved
S3-030656	Draft Report of SA WG3 meeting #30	SA WG3 Secretary	4.1	Approval		Modified and approved. To be put on FTP server as v1.0.0
S3-030657	Draft Report of Joint SA WG3 / CN WG1 session 7 October 2003	SA WG3 Secretary	4.1	Approval		Approved. To be put on FTP server as v1.0.0
S3-030658	SMG10 meeting report (extract on ASCI)	BT Group	6.21	Information		Noted
S3-030659	Use of the same algorithms for encryption of VGCS-calls as for normal GSM-speech calls (i.e. A5/0-A5/7)	BT Group	6.21	Discussion / Decision		Recommendations captured in S3-030692. Noted
S3-030660	LS Response on potential USIM impact of the MBMS security framework	SA WG3	6.20	Information		Approved over e-mail after SA3#30. Noted at this meeting
S3-030661	TS 33.310 V0.6.0: Network Domain Security; Authentication Framework (Rel-6)	Rapporteur	6.4	Information		Noted and used for updates.
S3-030662	TS 33.220 V0.1.1: Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (Rel-6)	Rapporteur	6.9	Information		Noted and used for updates.
S3-030663	TS 33.221 V0.1.1: Generic Authentication Architecture (GAA); Support for Subscriber Certificates (Rel-6)	Rapporteur	6.9	Information		Noted and used for updates.
S3-030664	TR 33.919 V0.1.0: Generic Authentication Architecture; System Description (Rel-6)	Rapporteur	6.9	Information		Noted and used for updates.
S3-030665	3GPP TS 33.222 V0.1.1: Generic Authentication Architecture (GAA); Access to Network Application Functions using HTTPS (Rel-6)	Rapporteur	6.9	Information		Allocated as TS 33.222. Noted
S3-030666	Technical Report on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6)	Toshiba, Intel, T-Mobile, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel, Gemplus	6.15	Approval	S3-030779	Updated with comments in S3-030779
S3-030667	Updated Annex C to 33.109: Key pair storage	Rapporteur	6.9	Information		Updated after e-mail discussion on S3-030561. Agreed to add new Annex C
S3-030668	Reply LS (from CN WG1) on Special-RAND mechanism	CN WG1	6.6	Action		Response LS in S3-030802
S3-030669	LS (from CN WG4) on Special-RAND mechanism	CN WG4	6.6	Information		Noted
S3-030670	LS (from CN WG1) on Introducing the Privacy Mechanism in Stage 2	CN WG1	6.1	Action		CR updated in line with this LS in S3-030772
S3-030671	LS (from CN WG3) on security of the Diameter protocol for the Gq interface	CN WG3	5.1	Action		Response LS in S3-030765
S3-030672	LS to SA3 on Clarification on use of Re-attempt Information element in Authentication Failure Report service	CN WG4	6.5	Action		C Blanchard to lead e-mail discussion and provide response by 5 Jan 2004
S3-030673	The requirement and feasibility of IMS watcher authentication	CN WG1	6.18	Action		Noted
S3-030674	Reply LS (from SA WG2) on "The requirement and feasibility of IMS watcher authentication"	SA WG2	6.18	Information		Noted
S3-030675	Response (from SA WG2) for Introducing the Privacy Mechanism in Stage 2	SA WG2	6.1	Action		CR updated in line with this LS in S3-030772
S3-030676	LS (from SA WG2) on Tunnel Establishment and Security Association	SA WG2	6.10	Action		Reply LS to SA2 in S3-030789
S3-030677	Pseudo-CR to 33.310: Clarification of SEG certificate profiling	Nokia, Siemens, T-Mobile, Vodafone	6.4	Approval		agreed for inclusion in draft TS
S3-030678	Reply (from SA WG1) to LS on potential USIM impact of the MBMS security framework S1-031104; T3-030697)	SA WG1	6.20	Information		Noted
S3-030679	LS (from SA WG1) on clarified requirements on synchronization for GUP	SA WG1	6.17	Information	S3-030759	Wrong CR attached - replaced by S3-030759

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030680	LS (from SA WG1) on Privacy and Security Requirements within GSM/UMTS Devices	SA WG1	5.1	Action		Response LS in S3-030766
S3-030681	Reply (from SA WG1) on the requirement and feasibility of IMS watcher authentication	SA WG1	6.18	Information		Noted
S3-030682	LS (from GSMA SG) on request for information on impact on equipment of solutions	GSMA Security Group working Party	5.4	Action		Delegates asked to discuss questions in companies and comment to GSMA. Noted.
S3-030683	Pseudo-CR to 33.221: Results of risk analysis in the "Key Pair Storage" informative annex	Gemplus, Giesecke&Devrient, Oberthur, Schlumberger	6.9	Approval	S3-030795	Revised in S3-030795
S3-030684	Pseudo-CR to 33.221: on enrollment of keys in a UICC application	Schlumberger, OCS, Gemplus	6.9	Approval	S3-030797	Revised in S3-030797
S3-030685	Pseudo-CR to 33.221: on on-board key generation in a UICC.	Schlumberger, OCS, Gemplus	6.9	Approval		Agreed for inclusion in the draft TS
S3-030686	Pseudo-CR to 33.221: on clarifications on Certificate enrollement using pre-certified keys	Schlumberger, OCS, Gemplus	6.9	Approval	S3-030796	Revised in S3-030796
S3-030687	CR to 33.108: CS Section for 33.108 – User data packet transfer (Rel-6)	SA WG3 LI Group	5.1	Approval		Under discussion in LI group. Will be provided for e-mail if agreed. Noted
S3-030688	CR to 33.108: CS Section for 33.108 – LI Management Operation (Rel-6)	SA WG3 LI Group	5.1	Approval		Under discussion in LI group. Will be provided for e-mail if agreed. Noted
S3-030689	Draft TS 33.234 V0.7.0 Wireless Local Area Network (WLAN) Interworking Security	Rapporteur	6.10	Information		Noted. Used for further updates from Pseudo-CRs
S3-030690	3GPP Over the Air (OTA) procedures applied to BAK Distribution and MBMS Subscription management	Schlumberger, QUALCOMM, GEMPLUS, OCS	6.20	Discussion / Decision		Noted. Issues need to be clarified
S3-030691	Pseudo-CR to 33.310: Removal of unnecessary restriction on serial number	Siemens, Nokia, SSH, T-mobile	6.4	Approval		agreed for inclusion in draft TS
S3-030692	Securing VGCS calls	Siemens, Vodafone	6.21	Discussion / Decision		Principles discussed and some agreed. Resulting LSs in S3-030773 and S3-030774
S3-030693	More elements on the Special RAND mechanism	Orange	6.6	Discussion / Decision		Section 4 used for LS in S3-030802. Special RAND proposal endorsed. Orange may contact GSMA about their issue
S3-030694	MMS Security Considerations Version 1.0.0	MMS Representative (A Bergmann)	5.4			Noted. A Bergmann to arrange workshop if enough resources provided
S3-030695	Draft TS 33.141 V0.2.0 Presence Service; Security	Rapporteur	6.18	Information		Noted. Estimated 10-15% complete
S3-030696	Adding Integrity to Counting Idle Mode terminals in MBMS	Qualcomm Europe	6.20	Discussion / Decision		Contribution invited if need seen for protection against this
S3-030697	MBMS Usage and Quality of Service based on BAK Distribution	Gemplus, Oberthur, QUALCOMM Europe, SchlumbergerSema	6.20	Discussion		Noted
S3-030698	Proposed CR to 43.020: Introducing the special RAND mechanism (Rel-6)	Orange, Vodafone	6.6	Approval		Related CR in S3-030761. Additional changes to be sent to S Fouquet for input to next meeting
S3-030699	MBMS UICC open issues	Siemens	6.20	Discussion / Decision		Comments recorded on each issue
S3-030700	MBMS (re-)keying models	Siemens	6.20	Discussion / Decision		Working assumptions and requirement agreed in principle

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030701	MBMS: Replaying of RAND values	Siemens	6.20	Discussion / Decision		Req needed if UICC-based solution chosen
S3-030702	Security Analysis on the SA2 resolution architecture	Huawei Technologies Co., Ltd.	6.10	Discussion	S3-030762	Revised in S3-030762
S3-030703	Evaluation of re-keying methods	Huawei Technologies Co., Ltd.	6.20	Discussion / Decision		Discussed with S3-030751, S3-030709 and S3-030723. Common decisions reached
S3-030704	Pseudo-CR to 33.220: Transaction Identifier independence for different NAFs or NAF groups	Huawei Technologies Co., Ltd.	6.9	Approval		rejected as synchronisation issues need solving before this can be agreed
S3-030705	Pseudo-CR to 33.310: Removing outdated editor's notes	Nokia, Siemens, T-Mobile, Vodafone	6.4	Approval		agreed for inclusion in draft TS
S3-030706	Pseudo-CR to 33.310: Recommendation to SEG certificate and IKE profiling	Nokia, Siemens, Vodafone	6.4	Approval		agreed for inclusion in draft TS
S3-030707	Pseudo-CR to 33.310: Local repository access clarification	Nokia, Siemens, T-Mobile, Vodafone	6.4	Approval		agreed for inclusion in draft TS
S3-030708	MBMS Traffic Encryption Key gradually Changing and Updating for streaming service	Samsung Electronics	6.20	Discussion / Decision		Further analysis of impacts needed
S3-030709	Composite MBMS Key Distribution	Samsung Electronics	6.20	Discussion / Decision		Discussed with S3-030703, S3-030751 and S3-030723. Common decisions reached
S3-030710	Differentiation of MBMS traffic protection mechanisms	Samsung Electronics	6.20	Discussion / Decision		Handled at meeting #30
S3-030711	MBMS service activation and Initial TEK distribution	Samsung Electronics	6.20	Discussion / Decision		Handled at meeting #30
S3-030712	Proposed CR to 33.203: Ensuring the correct RAND is used in synchronization failures (Rel-5)	3, Nokia, Vodafone, Ericsson	6.1	Approval	S3-030768	Revised in S3-030768
S3-030713	Proposed CR to 33.203: Ensuring the correct RAND is used in synchronization failures (Rel-6)	3, Nokia, Vodafone, Ericsson	6.1	Approval	S3-030769	Revised in S3-030769
S3-030714	Draft TS 33.246 V0.2.2: Security of Multimedia Broadcast/Multicast Service	Rapporteur	6.20	Information		noted
S3-030715	Pseudo-CR to 33.234: Clarification to reauthentication procedures	Nokia	6.10	Approval		Agreed for inclusion in the draft TS
S3-030716	Pseudo CR to GAA TR 33.919	Alcatel	6.9	Discussion / Decision		Agreed for inclusion in the draft TS
S3-030717	Organization of Presence TS and HTTPS TS	Ericsson, Nokia	6.9 / 6.18	Discussion / Decision		Proposals endorsed
S3-030718	Presentation Slides: Liberty Alliance Project - Setting the Standard for Federated Network Identity	Nokia	5.7	Information	S3-030764	revised version in S3-030764
S3-030719	Presentation Slides: Potential synergies between Liberty and 3GPP	Nokia	5.7	Information		Noted
S3-030720	Comparison of authentication proxy solutions	Ericsson	6.9 / 6.18	Discussion / Decision		Text from S3-030744 with editors note agreed
S3-030721	Challenges in using shared-secret TLS with NAFs	Ericsson	6.9 / 6.18	Discussion / Decision		No decision - delegates asked to study and contribute
S3-030722	User authentication process decision	Ericsson	6.9	Discussion / Decision		Agreed to add to draft TS. Additional editors note to be included in draft TS
S3-030723	Migration of MIKEY in MBMS key management	Ericsson	6.20	Discussion / Decision		Discussed with S3-030703, S3-030751 and S3-030709. Common decisions reached
S3-030724	Impacts on the 3GPP network with a UICC based and a non-UICC based solution in MBMS	Ericsson	6.20	Discussion / Decision	S3-030767	Revised in S3-030767
S3-030725	Proposed CR to 33.203: Removing anti-replay requirement from Confidentiality clause (Rel-6)	Ericsson	6.1	Approval	S3-030812	Corrected to Rel-6 CR in S3-030812

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030726	Proposed CR to 33.203: Network behaviour of accepting initial requests (Rel-5)	Nokia	6.1	Approval		Revised in S3-030770, mirror CR in S3-030771
S3-030727	NDS and Openness of IMS	Nokia	6.1	Discussion		To be discussed over e-mail - results by 15 Jan 2004
S3-030728	Pseudo-CR to 33.220: Bootstrapping procedure: merging of last two messages	Nokia	6.9	Approval		agreed for inclusion in draft TS
S3-030729	UE triggered unsolicited push from BSF to NAFs	Nokia	6.9	Discussion / Decision		Not agreed. Overhead issues to be investigated
S3-030730	Subscriber Certificate Enrollment Protocol	Nokia	6.9	Discussion / Decision		Agreed for inclusion in the draft TS
S3-030731	Proxy and various HTTP services	Nokia	6.9	Discussion / Decision		Text from S3-030744 with editors note agreed
S3-030732	Using shared key TLS with NAFs	Nokia	6.9	Discussion / Decision		No decision - delegates asked to study and contribute
S3-030733	Implications of the A5/2 Attack for 3GPP WLAN Access	Ericsson, TeliaSonera	6.10	Discussion / Decision		Agreed to add informative annex. Contributions on further scope of this invited
S3-030734	Pseudo-CR to 33.234: Re-authentication identities generation	Ericsson	6.10	Approval		Agreed for inclusion in draft TS
S3-030735	Pseudo-CR to 33.234: Editorial changes and informative annex in TS 33.234	Ericsson	6.10	Approval		Agreed for inclusion in draft TS
S3-030736	Security of EAP or SSID based network advertisements	Ericsson	6.10	Discussion		LS to SA2 in S3-030791
S3-030737	Split WLAN-UE: SIM Access Profile protocol in Bluetooth forum	Ericsson	6.10	Discussion / Decision		LS to be created
S3-030738	Split WLAN UE: Termination of EAP-AKA/SIM protocol	Ericsson	6.10	Discussion / Decision		Attached to LS in S3-030780
S3-030739	Split WLAN-UE: Integrity protection on local interface	Ericsson	6.10	Discussion / Decision		Agreed to remove requirement
S3-030740	Pseudo-CR to 33.234: Only one active USIM application	Ericsson	6.10	Approval		Withdrawn as redundant
S3-030741	End-to-end tunneling: Security Considerations on resolution gateways	Nortel Networks, Siemens AG, Nokia	6.10	Discussion / Decision		Comments against this in S3-030763. Discussed with other contributions and reply LS to SA2 in S3-030789
S3-030742	Application specific user profiles in GBA	Nortel Networks	6.9	Discussion / Decision		Pseudo CR updated in S3-030794
S3-030743	Key separation in a Generic Bootstrapping Architecture	Siemens	6.9	Discussion / Decision		Pseudo CR updated in S3-030793
S3-030744	Role of Authentication Proxy (AP-NAF) – Discussion and Pseudo-CRs to TSs on GAA/HTTPS and Presence Security	Siemens	6.9 / 6.18	Discussion / Decision		Text from S3-030744 with editors note agreed
S3-030745	Technical solutions for access to application servers via Authentication Proxy and HTTPS - Pseudo-CRs to TSs on GAA/HTTPS and Presence Security	Siemens	6.9 / 6.18	Discussion / Decision		Agreed to add to TSs with editors note added
S3-030746	Transfer of an asserted User Identity and Location of Access Control – Discussion and Pseudo-CRs to TSs on GAA/HTTPS and Presence Security	Siemens	6.9 / 6.18	Discussion / Decision		Agreed with "asserted" added.
S3-030747	Pseudo-CR to TS 33.234 on Requirements on UE split	Siemens	6.10	Discussion / Decision		Agreed changes, editors note to be updated
S3-030748	Security procedures for the set up of UE-initiated tunnels in scenario 3	Siemens	6.10	Discussion / Decision		Agreed to add updated Pseudo-CR in S3-030790
S3-030749	Pseudo-CR to GAA/HTTPS doc: Initial text for the TS	Siemens	6.9	Discussion / Decision		Agreed and 2 editors notes added
S3-030750	Considerations on selective encryption and integrity protection for DRM protected PSS media streams	Ericsson	6.20	Discussion		Presentation slides provided in S3-030776. LS in S3-030777

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030751	Further updates on Combined model for MBMS security	Nokia	6.20	Discussion / Decision		Discussed with S3-030703, S3-030709 and S3-030723. Common decisions reached
S3-030752	DRM usage for MBMS security	Nokia	6.20	Discussion / Decision		LS in S3-030777
S3-030753	CR's on "Handling of key sets at inter-system change"	Ericsson	6.5 / 6.6	Discussion / Decision		CRs in S3-030625 and S3-030626 were postponed
S3-030754	Enhancements to GSM/UMTS AKA	Ericsson	6.5 / 6.6	Discussion		long-term solution. Comments over e-mail requested
S3-030755	Some MBMS data flows	**3**	6.20	Discussion / Approval		attached P-CR updated in S3-030801
S3-030756	Liaison (from Download+DRM group OMA) to 3GPP SA WG4 and SA WG3 on issues on DRM for PSS and MBMS streams	Download+DRM group OMA	6.20	Discussion		LATE_DOC. Related LS in S3-030758 also considered.
S3-030757	T1P1.5 Lawful Intercept	T1P1.5 Chair	5.7	Information		LATE_DOC. LI Group to handle. Noted.
S3-030758	Liaison (from Download+DRM group OMA) to 3GPP SA WG4 and SA WG3 on issues on DRM for PSS and MBMS streams	Download+DRM group OMA	6.20	Action		LATE_DOC. Related LS in S3-030756 also considered.
S3-030759	LS (from SA WG1) on clarified requirements on synchronization for GUP	SA WG1	6.17	Information		LATE_DOC Noted
S3-030760	Response LS (from SA WG1) on support of GSM SIM files (and services) on the USIM, and USIM changes for key management of Voice Group Call Services	SA WG1	6.21	Action		LATE_DOC. Work ongoing in S3. Noted
S3-030761	Proposed CR to 33.102: Introducing the special RAND mechanism (Rel-6)	Orange, Vodafone	6.6	Approval		LATE_DOC. Related CR in S3-030698. Update if needed after 43.020 is updated at next meeting
S3-030762	Security Analysis on the SA2 resolution architecture	Huawei Technologies Co., Ltd.	6.10		S3-030788	LATE_DOC New version with rev marks in S3-030788
S3-030763	Comments on S3-030741: Security Considerations on resolution gateways	Huawei Technologies Co., Ltd.	6.10	Discussion / Decision	S3-030789	LATE_DOC Discussed with other contributions and reply LS to SA2 in S3-030789
S3-030764	Presentation Slides: Liberty Alliance Project - Setting the Standard for Federated Network Identity	Nokia	5.7	Information		Noted
S3-030765	Response LS to S3-030671 on security of the Diameter protocol for the Gq interface	SA WG3	5.1	Approval	S3-030810	Revised in S3-030810
S3-030766	Response LS to S3-030680: Reply LS on privacy and security requirements in GSM/UMTS devices	SA WG3	5.1	Approval	S3-030809	Revised in S3-030809
S3-030767	Impacts on the 3GPP network with a UICC based and a non-UICC based solution in MBMS	Ericsson	6.20	Discussion / Decision		Discussed and noted
S3-030768	Proposed CR to 33.203: Ensuring the correct RAND is used in synchronization failures (Rel-5)	3, Nokia, Vodafone, Ericsson	6.1	Approval		Approved
S3-030769	Proposed CR to 33.203: Ensuring the correct RAND is used in synchronization failures (Rel-6)	3, Nokia, Vodafone, Ericsson	6.1	Approval		Approved
S3-030770	Proposed CR to 33.203: Network behaviour of accepting initial requests (Rel-5)	Nokia	6.1	Approval		Approved
S3-030771	Proposed CR to 33.203: Network behaviour of accepting initial requests (Rel-6)	Nokia	6.1	Approval		Approved
S3-030772	Proposed CR to 33.203: Introducing the SIP Privacy mechanism in Stage 2 specifications (Rel-5)	Krister	7.1	Approval		Includes comments from CN1 and SA2. Approved
S3-030773	LS to T3 cc GSM-R on Status of VGCS work in SA3	SA WG3	6.21	Approval	S3-030803	Revised in S3-030803
S3-030774	LS to GERAN 2 on 'Ciphering for Voice Group Call Services'	SA WG3	6.21	Approval	S3-030804	Revised in S3-030804

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030775	Proposed order of handling MBMS documents	**3**	6.20	Information		Noted
S3-030776	Considerations on selective encryption and integrity protection for DRM protected PSS and MBMS media streams	Ericsson	6.20	Information		Presentation used for S3-030750. Discussed & Noted
S3-030777	LS on Protection of MBMS and DRM Streaming Services	SA WG3	6.20	Approval	S3-030805	Revised in S3-030805
S3-030778	LS to SA2 and SA4 (CC SA1) on service announcement and UE joining procedure	SA WG3	6.20	Approval	S3-030806	Revised in S3-030806
S3-030779	TR 33.8xy: Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6)	Toshiba, Intel, T-Mobile, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel, Gemplus	6.15	Approval	S3-030792	Minor changes made and revisions removed. Revised in S3-030792
S3-030780	LS to Bluetooth groups: SIM Access Profile in split WLAN-UE	SA WG3	6.10	Approval		Approved
S3-030781	Proposed CR to 33.108: CS Section for 33.108 – User data packet transfer (Rel-6)	SA WG3 LI Group		Approval	S3-030814	Approved and later updated in S3-030814 by MCC
S3-030782	Proposed CR to 33.108: CS Section for 33.108 – LI Management Operation (Rel-6)	SA WG3 LI Group		Approval	S3-030813	Approved and later updated in S3-030813 by MCC
S3-030783	LS (from LI Group) on 3GPP WLAN interworking Lawful Interception Requirements	SA WG3 LI Group	6.10	Action		Delegates to talk to LI colleagues to clarify issues
S3-030784	Proposed CR to 33.107: Reporting TEL URL (Rel-6)	SA WG3 LI Group		Approval		Approved
S3-030785	Proposed CR to 33.108: Reporting TEL URL (Rel-6)	SA WG3 LI Group		Approval		Approved
S3-030786	Proposed CR to 33.106: References (Rel-6)	SA WG3 LI Group		Approval	S3-030811	Change in section 6 is corrupted. LI to repair over e-mail. New version in S3-030811
S3-030787	Proposed CR to 33.108: Alignment of Lawful Interception identifiers length to ETSI TS 101 671 (Rel-6)	SA WG3 LI Group		Approval		Approved
S3-030788	Security Analysis on the SA2 resolution architecture (with and without revision marks)	Huawei Technologies Co., Ltd.	6.10	Discussion		LATE_DOC Not dealt with. Author can submit to next meeting if still relevant
S3-030789	Reply LS to SA WG2 on Tunnel Establishment and Security Association	SA WG3	6.10	Approval	S3-030808	Revised in S3-030808
S3-030790	Pseudo-CR to 33.234: Security procedures for UE-initiated tunneling	Ericsson	6.10	Approval		Agreed for inclusion in draft TS
S3-030791	LS to SA WG2 on Security of EAP or SSID based network advertisements	SA WG3	6.10	Approval	S3-030807	Revised in S3-030807
S3-030792	TR 33.8xy: Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6)	Toshiba, Intel, T-Mobile, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel, Gemplus	6.15	Approval		Approved for presentation to TSG SA for information
S3-030793	Pseudo-CR to 33.220: Key separation	Siemens	6.9	Approval		Approved. P Christofferson to ask SAGE to advise on Algs
S3-030794	Pseudo-CR to 33.220: Removal of application spefic user profile requirements from GBA	Nortel Networks	6.9	Approval		Approved for inclusion in the draft TS
S3-030795	Pseudo-CR to 33.221: Results of risk analysis in the “Key Pair Storage” informative annex	Gemplus, Giesecke&Devrient, Oberthur, Schlumberger	6.9	Approval		Approved for inclusion in the draft TS
S3-030796	Pseudo-CR to 33.221: on clarifications on Certificate enrollement using pre-certified keys	Schlumberger, OCS, Gemplus	6.9	Approval		Agreed for inclusion in the draft TS
S3-030797	Pseudo-CR to 33.221: on enrollment of keys in a UICC application	Schlumberger, OCS, Gemplus	6.9	Approval		Agreed for inclusion in the draft TS
S3-030798	Proposed correction to IMS CRs	**3**	6.1	Approval		LATE_DOC. Agreed

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030799	Proposed CR to 33.203: Correcting the text on sending an authentication response (Rel-5) Replacing S3-030601	**3**	6.1	Approval		LATE_DOC. Approved
S3-030800	Proposed CR to 33.203: Correcting the text on sending an authentication response (Rel-6) Replacing S3-030602	**3**	6.1	Approval		LATE_DOC. Approved
S3-030801	Pseudo-CR to MBMS draft TS: Key management	SA WG3	6.20	Approval		Agreed for inclusion in draft TS
S3-030802	Reply LS to CN1 on special-RAND	SA WG3	6.6	Approval		Approved
S3-030803	LS to T3 cc GSM-R on Status of VGCS work in SA3	SA WG3	6.21	Approval		Approved
S3-030804	LS to GERAN 2 on ‘Ciphering for Voice Group Call Services’	SA WG3	6.21	Approval		Approved
S3-030805	LS on Protection of MBMS and DRM Streaming Services	SA WG3	6.20	Approval		Approved
S3-030806	LS to SA2 and SA4 (CC SA1) on service announcement and UE joining procedure	SA WG3	6.20	Approval		Approved
S3-030807	LS to SA WG2 on Security of EAP or SSID based network advertisements	SA WG3	6.10	Approval		Approved
S3-030808	Reply LS to SA WG2 on Tunnel Establishment and Security Association	SA WG3	6.10	Approval		Approved
S3-030809	Response LS to S3-030680: Reply LS on privacy and security requirements in GSM/UMTS devices	SA WG3	5.1	Approval		Approved
S3-030810	Response LS to S3-030671 on security of the Diameter protocol for the Gq interface	SA WG3	5.1	Approval		Approved
S3-030811	Proposed CR to 33.106: References (Rel-6)	SA WG3 LI Group		Approval		e-mail check ongoing
S3-030812	Proposed CR to 33.203: Removing anti-replay requirement from Confidentiality clause (Rel-6)	Ericsson	6.1	Approval		Approved
S3-030813	Proposed CR to 33.108: CS Section for 33.108 – User data packet transfer (Rel-6)	SA WG3 LI Group		Approval		Approved
S3-030814	Proposed CR to 33.108: CS Section for 33.108 – LI Management Operation (Rel-6)	SA WG3 LI Group		Approval		Approved

* Documents in blue font were created after the close of the meeting.

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
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	

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
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
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

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
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).
TS	33.102	3G security; Security architecture	5.3.0	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	5.6.0	Rel-5	S3	WILHELM, Berthold	
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	5.5.0	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	5.7.0	Rel-5	S3	BOMAN, Krister	
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	5.5.0	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

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	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	5.1.0	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
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	33.102	3G security; Security architecture	6.0.0	Rel-6	S3	BLOMMAERT, Marc	Created by CRs @TSG SA#21
TS	33.107	3G security; Lawful interception architecture and functions	6.0.0	Rel-6	S3	WILHELM, Berthold	Created by CRs @TSG SA#21
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	6.3.0	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	33.203	3G security; Access security for IP-based services	6.0.0	Rel-6	S3	BOMAN, Krister	Created by CRs @TSG SA#21
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	6.3.0	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	6.2.0	Rel-6	S3	N, A	

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
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	WI
33.106	006	-	Rel-6	Correction to lawful interception references (currently on e-mail approval)	F	5.1.0	S3-31	S3-030811	SEC1-LI
33.107	035	-	Rel-6	Reporting TEL URL	F	6.0.0	S3-31	S3-030784	SEC1-LI
33.108	030	-	Rel-6	CS Section for 33.108 – LI Management Operation (editorially corrected by MCC)	F	6.3.0	S3-31	S3-030813	SEC1-LI
33.108	031	-	Rel-6	CS Section for 33.108 – User data packet transfer (editorially corrected by MCC)	F	6.3.0	S3-31	S3-030814	SEC1-LI
33.108	032	-	Rel-6	Reporting TEL URL	B	6.3.0	S3-31	S3-030785	SEC1-LI
33.108	033	-	Rel-6	Alignment of Lawful Interception identifiers length to ETSI TS 101 671	F	6.3.0	S3-31	S3-030787	SEC1-LI
33.203	047	1	Rel-5	Correcting the text on sending an authentication response	F	5.7.0	S3-31	S3-030799	IMS-ASEC
33.203	048	1	Rel-6	Correcting the text on sending an authentication response	A	6.0.0	S3-31	S3-030800	IMS-ASEC
33.203	058	1	Rel-5	Introducing the SIP Privacy mechanism in Stage 2 specifications	F	5.7.0	S3-31	S3-030772	IMS-ASEC
33.203	059	-	Rel-6	Removing anti-replay requirement from Confidentiality clause (corrected to Rel-6 by MCC)	D	6.0.0	S3-31	S3-030812	IMS-ASEC
33.203	060	-	Rel-5	Ensuring the correct RAND is used in synchronization failures	F	5.7.0	S3-31	S3-030768	IMS-ASEC
33.203	061	-	Rel-6	Ensuring the correct RAND is used in synchronization failures	A	6.0.0	S3-31	S3-030769	IMS-ASEC
33.203	062	-	Rel-5	Network behaviour when a new REGISTER is challenged during an on going authentication	F	5.7.0	S3-31	S3-030770	IMS-ASEC
33.203	063	-	Rel-6	Network behaviour when a new REGISTER is challenged during an on going authentication	A	6.0.0	S3-31	S3-030771	IMS-ASEC

D.1 List of CRs to specifications under SA WG3 responsibility agreed at meeting #30

Some CRs agreed at meeting #30 were modified or postponed at meeting #31. The following list shows the new status of CRs from meeting #30.

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WI
33.102	183	-	Rel-5	Handling of key sets at inter-system change (Postponed at meeting #31 - Not for TSG SA#22)	F	5.3.0	S3-30	S3-030625	SEC1-NDS, IMS-ASEC
33.102	184	-	Rel-6	Handling of key sets at inter-system change (Postponed at meeting #31 - Not for TSG SA#22)	A	6.0.0	S3-30	S3-030626	SEC1-NDS, IMS-ASEC
33.107	034	-	Rel-6	MSISDN/IMEI clarification for GPRS interception	F	6.0.0	S3-30	S3-030607	SEC1-LI
33.108	027	-	Rel-5	Correction to Annex G on TCP based transport	F	5.5.0	S3-30	S3-030532	SEC1-LI
33.108	028	-	Rel-6	Correction to Annex G on TCP based transport	A	6.3.0	S3-30	S3-030608	SEC1-LI
33.108	029	-	Rel-6	LI Reporting of Dialed Digits	B	6.3.0	S3-30	S3-030606	SEC1-LI
33.203	047	-	Rel-5	Correcting the text on sending an authentication response (Revised at meeting #31)	F	5.7.0	S3-30	S3-030601	IMS-ASEC
33.203	048	-	Rel-6	Correcting the text on sending an authentication response (Revised at meeting #31)	A	6.0.0	S3-30	S3-030602	IMS-ASEC
33.203	049	-	Rel-5	SA procedures	F	5.7.0	S3-30	S3-030609	IMS-ASEC
33.203	050	-	Rel-6	SA procedures	A	6.0.0	S3-30	S3-030611	IMS-ASEC
33.203	051	-	Rel-5	SA parameters and management	F	5.7.0	S3-30	S3-030610	IMS-ASEC
33.203	052	-	Rel-6	SA parameters and management	A	6.0.0	S3-30	S3-030612	IMS-ASEC
33.203	053	-	Rel-5	Reject or discard of messages	F	5.7.0	S3-30	S3-030614	IMS-ASEC
33.203	054	-	Rel-6	Reject or discard of messages	A	6.0.0	S3-30	S3-030615	IMS-ASEC
33.203	055	-	Rel-5	Correcting the SA handling procedures	F	5.7.0	S3-30	S3-030619	IMS-ASEC
33.203	056	-	Rel-6	Correcting the SA handling procedures	A	6.0.0	S3-30	S3-030620	IMS-ASEC
33.203	057	-	Rel-6	Terminology alignment	F	6.0.0	S3-30	S3-030613	IMS-ASEC
33.203	058	-	Rel-5	Introducing the SIP Privacy mechanism in Stage 2 specifications (Revised at meeting #31)	F	5.7.0	S3-30	S3-030648	IMS-ASEC
55.205	001	-	Rel-6	Correction of reference	D	6.0.0	S3-30	S3-030489	SEC1-CSALGO1

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	Source TD	Comment/Status
S3-030668	Reply LS (from CN WG1) on Special-RAND mechanism	N1-031612	Response LS in S3-030802
S3-030669	LS (from CN WG4) on Special-RAND mechanism	N4-031289	Noted
S3-030670	LS (from CN WG1) on Introducing the Privacy Mechanism in Stage 2	N1-031728	CR updated in line with this LS in S3-030772
S3-030671	LS (from CN WG3) on security of the Diameter protocol for the Gq interface	N3-030830	Response LS in S3-030765
S3-030672	LS to SA3 on Clarification on use of Re-attempt Information element in Authentication Failure Report service	N4-031152	C Blanchard to lead e-mail discussion and provide response by 5 Jan 2004
S3-030673	The requirement and feasibility of IMS watcher authentication	N1-031724	Noted
S3-030674	Reply LS (from SA WG2) on "The requirement and feasibility of IMS watcher authentication"	S2-033803	Noted
S3-030675	Response (from SA WG2) for Introducing the Privacy Mechanism in Stage 2	S2-033804	CR updated in line with this LS in S3-030772
S3-030676	LS (from SA WG2) on Tunnel Establishment and Security Association	S2-033813	Reply LS to SA2 in S3-030789
S3-030678	Reply (from SA WG1) to LS on potential USIM impact of the MBMS security framework S1-031104; T3-030697)	S1-031334	Noted
S3-030680	LS (from SA WG1) on Privacy and Security Requirements within GSM/UMTS Devices	S1-031312	Response LS in S3-030766
S3-030681	Reply (from SA WG1) on the requirement and feasibility of IMS watcher authentication	S1-031210	Noted
S3-030682	LS (from GSMA SG) on request for information on impact on equipment of solutions	-	Delegates asked to discuss questions in companies and comment to GSMA. Noted.
S3-030756	Liaison (from Download+DRM group OMA) to 3GPP SA WG4 and SA WG3 on issues on DRM for PSS and MBMS streams	OMA-BAC-DLDRM-2003-0264	LATE_DOC. Related LS in S3-030758 also considered.
S3-030757	T1P1.5 Lawful Intercept	-	LATE_DOC. LI Group to handle. Noted.
S3-030758	Liaison (from Download+DRM group OMA) to 3GPP SA WG4 and SA WG3 on issues on DRM for PSS and MBMS streams	OMA-BAC-DLDRM-2003-0221R3	LATE_DOC. Related LS in S3-030756 also considered.
S3-030759	LS (from SA WG1) on clarified requirements on synchronization for GUP	S1-031278	LATE_DOC Noted
S3-030760	Response LS (from SA WG1) on support of GSM SIM files (and services) on the USIM, and USIM changes for key management of Voice Group Call Services	S1-031208	LATE_DOC. Work ongoing in S3. Noted
S3-030783	LS (from LI Group) on 3GPP WLAN interworking Lawful Interception Requirements	S3LI03_124r1	Delegates to talk to LI colleagues to clarify issues

E.2 Liaisons from the meeting

TD number	Title	Comment/Status	TO	CC
S3-030780	LS to Bluetooth groups: SIM Access Profile in split WLAN-UE	Approved	**Bluetooth Architecture Review Board (BARB), Bluetooth CAR group, Bluetooth Security Expert Group**	
S3-030802	Reply LS to CN1 on special-RAND	Approved	**CN WG1**	**GERAN WG2**
S3-030803	LS to T3 cc GSM-R on Status of VGCS work in SA3	Approved	**T WG3**	**ETSI EP RT, GERAN WG2, ETSI EP SCP**
S3-030804	LS to GERAN 2 on 'Ciphering for Voice Group Call Services'	Approved	**GERAN WG2**	**ETSI EP RT, T WG3**
S3-030805	LS on Protection of MBMS and DRM Streaming Services	Approved	**SA WG4, OMA DLDRM, ETSI SAGE**	**SA WG1**
S3-030806	LS to SA2 and SA4 (CC SA1) on service announcement and UE joining procedure	Approved	**SA WG1, SA WG2, SA WG4**	**-**
S3-030807	LS to SA WG2 on Security of EAP or SSID based network advertisements	Approved	**SA WG2**	**-**
S3-030808	Reply LS to SA WG2 on Tunnel Establishment and Security Association	Approved	**SA WG2**	**-**
S3-030809	Response LS to S3-030680: Reply LS on privacy and security requirements in GSM/UMTS devices	Approved	**SA WG1**	**GSMA SeRG**
S3-030810	Response LS to S3-030671 on security of the Diameter protocol for the Gq interface	Approved	**CN WG3**	**SA WG2**

Annex F: Actions from the meeting

AP 31/01: **B. Sahlin to send IETF firewall-standardisation information to the e-mail list.**

AP 31/02: **B. Owen to contact SA WG3 LI group for results of LI impact of tunnelling solution for WLAN during the meeting.**

AP 31/03: **A. Bergmann to run an e-mail discussion on the MMS standardisation work and to organise a Workshop in January/February 2004 across the involved bodies if necessary.**

AP 31/04: **T Haukka to run an e-mail discussion on TD S3-030727. Comments by 23 December 2003, conclusions to e-mail list 15 January 2004.**

AP 31/05: **C. Blanchard to lead an e-mail discussion on the questions from CN WG4 in TD S3-030672. Discussion and comment deadline 17 December 2003. Draft response created by 24 December 2003. Approved response by 5 January 2004.**

AP 31/06: **G. Horn and K. Boman to consider section 3 of TD S3-030731 and comment to T. Haukka before 20 December 2003.**

AP 31/07: **T. Haukka and K. Boman to provide any comments on section 2 of TD S3-030746 to G. Horn.**

AP 31/08: **C. Blanchard was asked to check the changes made to the figures in TS 33.234 are reflected in the SA WG2 specification where they were originally copied from.**

AP 31/09: **D. Mariblanca to lead an e-mail discussion on the editors notes in section 6.1.5 of the Pseudo-CR in TD S3-030790.**

AP 31/010: **M. Pope to send SA WG3 Work Plan status details to the mailing list on 24 November 2003. Rapporteurs and Editors to provide feedback to M. Pope by 27 November 2003 in order to have an accurate SA WG3 status in the work plan presented to TSG SA #22.**