3GPP TSG SA WG3 Security — S3#31 **S3-030656**
18 - 21 November 2003
Munich, Germany

3GPP TSG SA WG3 (Security) meeting #30 **Draft Report**

6-10 October 2003

Povoa de Varzim, Portugal

Source:	**Secretary of SA WG3 (M. Pope)**
Title:	**Draft Report of SA3#30 - version 0.0.5 (revision marked)**
Document for:	**Comment**
Status:	**Draft version 0.0.5 with revision marks**

Fisherman Statue, Povoa de Varzim, Portugal

Contents

1 Opening of the meeting

The SA WG3 Chairman, Mr. V. Niemi, opened the meeting and Welcomed delegates to Portugal on behalf of the European Friends of 3GPP (EF3).

2 Agreement of the agenda and meeting objectives

TD S3-030495 Revised Draft Agenda for SA WG3 meeting #30. This was introduced by the SA WG3 Chairman.

Priorities:

1 Progress of IMS Security issues. See results from joint meeting with CN WG1 on IMS.
2 Progress specifications for Rel-6 in order to send to TSG SA Plenary for Information or Approval in December 2003.

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. Conclusions from the 6 October joint IMS session with CN1

TS S3-030483: Draft agenda for joint SA3-CN1 session on IMS security. The draft agenda for the joint meeting was reviewed and the SA WG3 Chairman provided a verbal report of the handling of agenda items. Resulting output documents to SA WG3 for approval and discussion were added under agenda item 7.1 of this meeting.

For the Stage 2 of Privacy, it had been agreed that the work is under SA WG3 responsibility, but there may already exist the necessary Stage 2 work in TS 22.229. SA WG3 agreed to consider the Stage 2 requirements and to check whether everything is covered, along with a LS to SA WG2 to check on the suitability of the Stage 2 privacy work. The output for this can be found in TD S3-030600. The proposed LS in TD S3-030579 had not been dealt with in the joint session and was decided to handle it while CN WG1 experts were available.

TS S3-030579: Proposed LS (to SA WG1): The requirement and feasibility of IMS watcher authentication. This was introduced by Nokia and asked SA WG1 to evaluate the need for IMS watcher authentication, based on some flaws identified by SA WG3 in the proposed system. There was a discussion on the requirements for IMS watcher authentication and there were different opinions on the expected Presence service requirements and scope of the services which may be provided using Presence. CN WG1 delegates were against the idea adding an authentication mechanism on top of IMS Authentication. There was some argument that this mechanism could be used for e.g. a *NetMeeting*-like service for, e.g. corporate IMS

systems, to give users control over access to their personal data (e.g. by distributing passwords, etc.). It was agreed that any agreed LS on Presence should be copied to CN WG1. The LS was revised in TD S3-030654 and approved.

5 Meeting reports

5.1 Approval of the report of SA3#29, San Francisco, USA, 15-18 July, 2003

TS S3-030592: Documents approved by e-mail after SA WG3 meeting #29. These documents were approved by e-mail after the last meeting. This was noted and delegates were asked to check if any approved documents were missing and inform the SA WG3 Secretary.

TS S3-030481: Draft report of TSG SA meeting #29. The draft report was reviewed and approved. The SA WG3 Secretary will accept the revision marks and add it to the 3GPP FTP server as version 1.0.0.

November meeting: This could not be hosted co-located with the LI group by the DTI, so it had been arranged to hold it at Siemens Conference Centre, Munich, hosted by the European Friends of 3GPP (EF3).

February 2004 meeting: The host was still not confirmed. M. Pope agreed to check if ETSI could host this as a backup.

May 2004 meeting: It was reported that this could be based in Jeju Island, South Korea, which is difficult to travel to and delegates were asked to consider the acceptability of this venue.

Actions from the meeting:

AP 29/01: M Pope to get a new TS number for use to provide the draft A5/4 and GEA4 document. The MCC specifications manager asked for details of the number of documents to be allocated numbers and their Titles, Rapporteurs, Releases, WIDs, etc. M Pope will obtain the necessary information and inform the SA WG3 Members of the allocated numbers over e-mail. Considered Completed.

AP 29/02: M Blommaert and P Howard to chair e-mail discussions on Early release IMEISV transfer and produce CRs for comment by 29 August, Approval 5 September 2003. There were no comments, and CRs created were approved at SA#21. Completed.

AP 29/03: M. Blommaert to run e-mail discussion to discuss what should be done with the information in TD S3-030402. Response LSs were provided to this meeting. Completed.

AP 29/04: A. Palanigounder to lead an e-mail discussion and draft an LS in response to TD S3-030428 (Denial of Service attacks against the 3GPP WLAN Interworking system). Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003. LS created, approved and transmitted. Completed.

AP 29/05: S. Nguyen Ngoc was asked to lead an e-mail discussion over LSs in TD S3-030433 and to produce a response LS. Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003. LS created, approved and transmitted. Completed.

AP 29/06: C. Blanchard to lead an e-mail discussion over LSs in TD S3-030427 and to produce a response LS. Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003. LS created, approved and transmitted. Completed.

AP 29/07: P. Howard to lead an e-mail discussion on Trust Model and provide a contribution to SA WG3 meeting#30. There had been no input on this and it was suggested that this should be re-discussed after the discussion of contributions at this meeting. The draft TS contains a new table covering this action. Completed.

AP 29/08: B. Owen to lead an e-mail discussion on TD S3-030316 (UE security aspects of the GUP architecture). Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003. There had been no input on this on the e-mail discussion. To be re-considered after GUP discussions at this meeting. Completed.

AP 29/09: G. Horn to lead an e-mail discussion on open issues related to Key Management of HTTP-based services. Deadline for collection of issues: 27 August 2003. The results were handled in the MBMS ad-hoc meeting. Completed.

AP 29/10: Tao Haukka to provide draft LS to SA WG1 on IMS watcher authentication for discussion at SA WG3 meeting #30. The results are provided as input to this meeting. Completed.

AP 29/11: C. Blanchard to set up a discussion group and elaborate the MBMS Key Management requirements based on TD S3-030335. Dealt with at the MBMS ad-hoc meeting and CRs and LS to this meeting. Completed.

AP 29/12: M. Pope to check if an ad-hoc meeting can be held at ETSI premises 3 - 4 September 2003 (20 delegates). This was not possible, the ad-hoc meeting was held in Antwerp. Completed.

5.2 Report from SA3 ad hoc meeting on GAA and MBMS, Antwerp, Belgium, 3 - 4 September, 2003

TS S3-030482: Draft Report of MBMS / GAA ad-hoc meeting. P. Howard provided the report of the ad-hoc meeting and was reviewed.

Actions from the meeting:

AP 0309/01: G. Horn to update the diagram in section 6.2 of TD S3z030011 so that it captures the architectural solutions under consideration for GAA.

AP 0309/02: Chairman to raise SA WG3 comments on MBMS architecture TS 23.246 at the TSG SA #21 plenary meeting.

AP 0309/03: A. Escott to obtain clarification on what is meant by the inclusion of security functions in Figure 7 of the MBMS architecture TS 23.246v2.0.0.

AP 0309/04: C. Blanchard to distribute any proposed pseudo CRs arising from AP29/11 which add potentially controversial MBMS security requirements to the SA WG3 email list for comment prior to SA3#30. Completed. The results are provided in **TD S3-030513, TD S3-030514 and TD S3-030515**.

P. Howard was thanked for the report which was then approved.

5.3 Report from SA#21, Frankfurt, Germany, 22-25 September, 2003

TS S3-030496: SA WG3 Chairmans Report from SA#21 plenary. The SA WG3 Chairman reported the handling of SA WG3 contribution to TSG SA #21.

1. *In all technical areas except Lawful interception, all our CR's were approved as submitted.*
2. *In the area of lawful interception, the category of a CR was changed in several cases from D (editorial modification) to F (correction). One CR (SP-030477) against 33.106 marked as "editorial modification" was rejected because it proposed to introduce an item into the reference list but it did not introduce any change in the specification where this item is referenced to.*
   It was emphasized that category D is intended exclusively for grammatical improvements, e.g. correcting spelling errors. No CR in category D can introduce any changes (however small) in the system. Furthermore, it is not a responsibility of either MCC or the WG (or SWG) chairpersons to correct the cover sheets. All people preparing CRs were encouraged to consult TR 21.801 "Specification drafting rules".
3. *Our proposed WID for "Key Management of group keys for Voice Group Call Services" was approved as submitted (SP-030491).*
4. *Some concern was raised with the timing of LI subgroup meetings: if the LI meeting is scheduled too close to the SA plenary meeting then CRs approved in the LI meeting cannot typically be done against the correct version of the specification. This happened also this time but Maurice managed to correct the CRs. There is a risk that the same problem recurs next time as LI group meeting was held simultaneously with SA#21. Therefore, I propose LI group converts any CRs accepted in Jackson Hole meeting (22-24 September) into correct form (i.e. against spec versions that exist after SA#21) before we submit them to SA plenary #22 in December.*
5. *Dr. Raziq Yaqub gave a presentation about the current stage of our Feasibility study work on (U)SIM Security Reuse by Peripheral Devices. It was explicitly explained (and also mentioned in the SA#21 meeting minutes) that the presentation was an individual company contribution with no endorsement whatsoever by SA3.*
6. *I participated also the OMA-3GPP workshop on Monday 15 September. The most immediate affect to our work was the agreement that joint meetings and liaison between OMA and 3GPP work groups are possible (and they are even encouraged). However, it was stressed that agreements reached in joint meetings are not binding; they have to be endorsed by both parties. This kind of endorsement already occurred in SA plenary for the workshop conclusions (SP-030516).*
   One consequence is that we can now send our LS (S3-030459) to OMA SEC/SCT WG and begin preparing for a joint meeting in the area of subscriber certificates.
   In addition to the workshop conclusions, it was agreed in the SA#21 that Iain Sharp (TSG T vice chair) continues to maintain a living document of OMA dependencies (i.e. a list of OMA deliverables such that 3GPP is dependent on them) in a manner similar to what Stephen Hayes (TSG CN chair) has been doing for IETF dependencies.
7. *Issues in SA1 area:*
   - *SA1 is still struggling with their reply to our earlier reply LS (S3-030273) on "Privacy and Security Requirements within GSM/UMTS Devices";*
   - *One CR (SP-030459) adds an authentication requirement in the security section of LCS stage 1 spec;*
   - *Another CR (SP-030469) cleans up the security section of GUP stage 1 spec.*
8. *Issues in SA2 area:*
   - *As agreed in our September ad hoc, I raised the issues with the security section of MBMS stage 2 spec 22.246;*
   - *The conclusion was to replace the security section with a reference to our MBMS security spec 33.246. This change would be implemented later with a CR against 22.246. The possibility to access MBMS services with a SIM has to be raised in SA3 if there is still interest in pursuing this path further. (We noted in Antwerp that this late requirement in 22.246 was against the agreement reached in the joint SA2/SA3 MBMS session in February.);*
   - *A new WID "Impacts of Speech Enabled Services on IMS, PS and CS domains" (SP-030539) has the following under the section of security aspects: "Access to Voice Recognition platforms in authenticated and authorised manner. Privacy rules may need to be defined for the access to Voice Recognition platforms.";*
   - *WLAN interworking stage 2 TS 22.234 was not approved because some more study is required to be able to confirm the tunnelling solution for scenario 3. One of the issues to be studied is lawful interception. However, the content of the draft TS is stable for scenarios 1 and 2 and the content of scenario 3 part is seen as the working assumption*
9. *Issues in CN area:*
   - *The WID for CN4 stage 3 work on the area of bootstrapping interfaces was approved.*
10. *Issues in T area:*
    - *T3 has to know very soon whether they need to do work for MBMS in release 6.*
11. *General issues about the Rel. 6 dates:*
    - *the decision of the freezing date of Rel-6 is going to be done in December 2003.*
    - *SA#21 estimated that the stage 1 content of Rel-6 is now stabilized although there is a caveat that co-operation with OMA may lead to some new requirements.*

The SA WG3 Chairman was thanked for his work at the TSG meeting and for the report back to the group. The report was then noted.

5.4 Report from SA3 LI #10, Jackson Hole, WY, USA, 22-24 September, 2003

It was verbally reported that the Vice Chairman Bernd Adams has resigned and is replaced by Burkhard Kubbutat (O2 Germany). The draft report of the meeting was provided in TD S3-030605 for information and was noted.

TS S3-030491: LS (from SA WG3 LI Group) on new acronym. This informed SA WG3 of the intention to use the acronym "Access Network Provider", ANP instead of "AN". This was agreed.

TS S3-030530: Proposed CR to 33.108: LI Reporting of Dialled Digits (Rel-6). The CR was updated slightly in TD S3-030606 to add "intercept" to the note and remove Italics from the added text. The CR was then approved. **The LI Group were asked to check that the change made is acceptable before the next SA WG3 meeting**.

TS S3-030531: Proposed CR to 33.107: MSISDN/IMEI clarification for GPRS interception (Rel-6). The CR was updated slightly in TD S3-030607 to add "intercept" to the note and remove Italics from the added text. The CR was then approved. **The LI Group were asked to check that the change made is acceptable before the next SA WG3 meeting**.

TS S3-030532: Proposed CR to 33.108: Correction to Annex G on TCP based transport (Rel-5). This CR was approved.

TS S3-030533: Proposed CR to 33.108: Correction to Annex G on TCP based transport (Rel-6). The Category was revised from "**F**" to "**A**", as this was a mirror CR, in TD S3-030608 which was approved.

6 Reports and Liaisons from other groups

6.1 3GPP working groups

TS S3-030501: LS (from CN WG2) on SA3 on Legal Interception of SCP initiated calls. This was provided by CN WG2 to the LI group and it was decided to note it at SA WG3 and leave it to the LI Group to deal with appropriately.

TS S3-030506: LS (from SA WG4) on cipher suite for DRM-protected streamed media for PSS. This was introduced by the SA WG3 Chairman and reported the DRM assumptions currently held by SA WG4 and asked for verification from SA WG3 on this. The attachment (S4-030639) was also introduced by Nokia. It was agreed that this subject would need analysis and further discussion within SA WG3 and it was decided to provide a response LS to SA WG4 informing them that the choice of ciphering suite would need further investigation by SA WG3. Comments were requested to P. Howard in order to develop the LS overnight, which was provided in TD S3-030621, which was modified in TD S3-030650 which was approved.

TS S3-030505: Liaison (from SA WG4) Response to OMA. This LS was copied to SA WG3 and concerned the information given to OMA in TD S3-030506, where SA WG4 reported that verification on the DMA assumptions would be sought from SA WG3. The LS was noted.

6.2 IETF

There were no specific contributions under this agenda item.

6.3 ETSI SAGE

TS S3-030489: Proposed CR to 55.205: Correction of reference. This CR corrected the numbers of referenced TSs. The CR was approved.

It was reported that the backup-algorithm work was currently under funding discussions with the GSMA. This was noted.

6.4 GSMA SG

TD S3-030490: LS (from GSMA SG) on introduction of A5/3 in GSM handsets. This was introduced by C. Brookson and requested SA WG3 to agree to the principle as a matter of priority due to recent reported attacks on algorithms, to introduce the both the algorithm and a **key separating mechanism** by the end of 2004 and that these security features should be a part of Rel-6. It was noted that the GSMA SG were working on potential solutions to introduce the mechanism, but this was not yet finalised. Further contributions to the meeting on this issue would be addressed later in the meeting (see agenda item 7.6).

Charles Brookson then gave a report of the GSMA SG activities. On IMEI he described the latest industry initiatives. The GSMA CEO Board had recommended to Operators to connect to the CEIR in Dublin. In addition the GSMA and EICTA (The European Mobile Manufacturers body) had written to the EU TCAM describing a proposed scheme to clearly identify mobiles which had the IMEI easily changed. TD S3-030633 is a copy of the letter sent which was provided for information and was noted.

Recently GPRS over-billing had been mentioned in recent press reports. This had previously been discussed in SA3 and it was decided to further address the proposed solutions on the email list.

AP 30/01: Eric Gauthier (Orange, Switzerland) to lead an e-mail discussion on GPRS over-billing.

6.5 3GPP2

There were no specific contributions under this agenda item. It was reported that the major topic in 3GPP2 is WLAN Interworking.

6.6 OMA

There were no specific contributions under this agenda item.

6.7 Other groups

TS S3-030486: "Letter from TIA TR-45 LAES ad-hoc Chairman to the SA WG3 Chairman: PN-4465-RV1 (to be published as J-STD-025-B)". This was considered best to be forwarded to the LI Group and was forwarded to them for consideration. The LS was then noted.

7 Work areas

7.1 IP multimedia subsystem (IMS)

TD S3-030594 Proposed CR to 33.203: SA procedures (Rel-5). This contained re-wording for the CR discussed in the joint CN WG1 meeting. The summary of change was updated and the new CR provided in TD S3-030609 which was approved. A mirror CR to Rel-6 was provided in TD S3-030611 and approved.

TD S3-030596 Proposed CR to 33.203: SA parameters and management. (Rel-5). This contained changes to the CR discussed in the joint CN WG1 meeting. The CR was corrected editorially and updated in TD S3-030610 which was approved. A mirror CR to Rel-6 was provided in TD S3-030612 and approved.

TD S3-030597 Proposed CR to 33.203: Terminology alignment (Rel-6). The CR was corrected to the Rel-6 version of the specification and was updated in TD S3-030613 which was approved. It was noted that the CR affects the ME and CN which was not marked on the cover sheet. **M. Pope agreed to update the cover sheet when preparing the CR for presentation to TSG SA**.

TD S3-030598 Proposed CR to 33.203: Terminology alignment (Rel-6). The CR was corrected editorially and updated in TD S3-030614 which was approved. A mirror CR to Rel-6 was provided in TD S3-030615 and approved.

TD S3-030599 LS to CN 4, CN1 on IMS AKA: UE populating RAND and AUTN parameters in responding to challenge. This was introduced by Nokia and was reviewed. There were some comments for clarification and it was decided to set up a drafting group to review the CN WG4 specification for relevance to their work, and to review the text in order to avoid any possible confusion by the receiving groups. This was done and the LS was revised in TD S3-030616 which was approved.

TD S3-030600 Proposed CR to 33.203: Introducing the SIP Privacy mechanism in Stage 2 specifications (Rel-5). This was introduced by Ericsson and contained changes to the CR discussed in the joint CN WG1 meeting (related to TD S3-030541). The CR was reviewed and updated in TD S3-030617 which was updated in TD S3-030648 and approved. A LS to SA WG2 asking them to review this CR was provided in TD S3-030318 which was updated in TD S3-030649 and approved.

TD S3-030601: Proposed CRs to 33.203: Correcting the text on sending an authentication response (Rel-5). This CR was reviewed and approved.

TD S3-030602: Proposed CRs to 33.203: Correcting the text on sending an authentication response (Rel-6) This CR was reviewed and approved.

TD S3-030603: Proposed CRs to 33.203: Correcting the SA handling procedures (Rel-5). The CR was reviewed and updated in TD S3-030619 which was approved.

TD S3-030604: Proposed CRs to 33.203: Correcting the SA handling procedures (Rel-6). The CR was reviewed and updated in TD S3-030620 which was approved.

TS S3-030485: LS reply on Rel-5 transport of unknown SIP signalling elements. This was introduced by the SA WG3 Chairman. The LS was a response to an LS from CN WG1. SA WG5 reported that there is no problem for charging on unknown elements. The LS was noted.

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

There were no specific contributions under this agenda item.

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

There were no specific contributions under this agenda item. NDS/IP was discussed with contributions under the IMS agenda item.

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

TS S3-030487: "Draft TS 33.310 V0.5.0: Network Domain Security; Authentication Framework". This was provided for information and use for further updates at the meeting and was noted. The Rapporteur reported that this should be ready for sending to TSG SA for information in December 2003.

TS S3-030535: Pseudo CR to 33.310: Removal of support for delta CRLs (Rel-6). This was introduced by Siemens on behalf of Siemens, Nokia, SSH, T-Mobile and Vodafone. This Pseudo-CR was approved for inclusion by the editor in the draft TS.

TS S3-030572: Adding domain component support to NDS/AF certificate profiles. This was introduced by Nokia and discussed the addition of domain component (dc) support to the certificate subject and issuer names in NDS/AF certificate protocols and to agree to the addition of the Pseudo-CR provided in TD S3-030573 to the draft TS. It was commented that the X.500 mentioned in the contribution was in fact X.400, this was noted. The principle was agreed.

TS S3-030573: Pseudo CR to 33.310: Adding domain component support to NDS/AF certificate profiles. This was introduced by Nokia on behalf of Nokia, Siemens, SSH and T-Mobile. This Pseudo-CR was approved for inclusion by the editor in the draft TS.

TS S3-030574: Pseudo CR to 33.310: Clarifications to usage of certificate repositories. This was introduced by Nokia on behalf of Nokia, Siemens, SSH and T-Mobile. This Pseudo-CR was approved for inclusion by the editor in the draft TS.

TS S3-030589: Pseudo CR to 33.310: Clarification on the use of PSK as a fallback mechanism. This was introduced by vodafone on behalf of Vodafone, Nokia, Siemens and SSH. It was comented that this fall-back system would be improtant and should be further developed in the specifications. It was agreed that this could be considered by delegates and this could be seperated into a new section in the future if considered appropriate, based on contribution at the next SA WG3 meeting. This Pseudo-CR was approved for inclusion by the editor in the draft TS.

TS S3-030590: Pseudo CR to 33.310: Correction of typos. This Pseudo-CR was approved for inclusion by the editor in the draft TS. **Future such small editorial corrections can be done by the editor without a Pseudo-CR.**

7.5 UTRAN network access security

TS S3-030499: Reply to LS (from CN WG1 - N1-031052) on 'Effects of service 27/38 on 2G/3G Interworking and emergency call' from SA WG3. This was introduced by Siemens and asked SA WG3 and T WG3 to add a scenario SCN-2a to the specifications where appropriate. A response from T WG3 was provided in TD S3-030510. It was noted that the GSM cipher key is derived from the SIM/USIM, rather than the SIM as stated in the LS.

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.

TS S3-030510: LS (from T WG3) on the effects of USIM services 27 and 38. This was introduced by Siemens and reported on the action taken by T WG3 for the addition of these requirements in their specifications and proposed that more detail should be included in core specifications, rather than in a TR. It was reported that the CR attached had been approved at TSG T meeting #21. This was acknowledged and the LS was noted.

TS S3-030585: Effects of service 27/38 on 2G/3G Interworking and emergency call. This was introduced by Siemens and proposed that SA WG3 discuss and decide whether T3-030694 provides adequate description from a 3GPP specification viewpoint or whether this should be documented in an appropriate 3GPP document. If SA WG3 decide not to document the detailed scenarios then suggested to send it to GSMA to document the scenarios in a public GSMA document. The following options were proposed and discussed:

1) SA WG3 should develop the documentation and provide the agreed text to the GSMA SIM Group for inclusion in a public GSMA document;
2) Included as a new SA WG3 TR;
3) Added as an informative annex to TS 33.102;
4) Mandate the scenarios in T WG3 specifications (SIM specifications).

It was decided to create a LS to GSMA SG (copied to SCAG) to ask them to discuss the impacts and suitability of mandating these Services. This was provided in TD S3-030624 which was approved.

TS S3-030549: Proposed CR to 33.102: Handling of key sets at inter-system change (Rel-5). This was introduced by Ericsson. The CR was updated to clarify it in TD S3-030625 which was approved. A Rel-6 mirror CR was provided in TD S3-030626 which was approved.

TD S3-030627: Reply LS (from SA WG2) on "Security issues regarding multiple PDP contexts in GPRS". This was introduced by Vodafone and asked SA WG3 to discuss the security problem regarding multiple active connections. Discussion papers were provided by Nokia in TD S3-030575 and Vodafone and Ericsson in TD S3-030587 which were considered:

TS S3-030575: Analysis of proposed network based access control solution for multiple PDP contexts. This was introduced by Nokia and discussed a threat model and proposed solutions. The SA WG2 proposed solution was shown not to provide a defence against the threat model and Nokia proposed that a terminal-based solution (e.g. a personal firewall implementation in the terminal) should be the preferred solution to the threat.

Vodafone commented that the threat model proposed in the contribution does not cover all expected scenarios for the 3GPP system (e.g. a PC using GPRS to set up Telnet sessions, rather than the assumed mobile devices) and proposed that a combination of Network-based and terminal-based solutions should be used in a complementary way in order not to restrict the services which can be provided to Corporate users from the Network Operator.

TS S3-030587: Multiple PDP context security issue. This was introduced by Vodafone on behalf of Vodafone and Ericsson and discussed the threat and proposed that a flexible, standardised, Network-based solution should be used in conjunction with the use of terminal-based solutions.

Nokia commented that the threat in the single PDP context issue when connected to the public Internet is the same as in the Multiple-PDP context when connected through a Corporate Network to the Internet and there can be no real protection against this in a Network-based solution.

It was decided to have a detailed discussion in an evening session in order to determine the way forward and attempt to come to an agreement on the solution to be developed by SA WG3 and reported to SA WG2. An LS was developed in the discussion session and provided in TD S3-030634 which was discussed and approved.

7.6 GERAN network access security

There was an analysis of proposals made at SA WG3 #29 meeting and were 2 proposals for countering the recently reported A5/2 threat:

TS S3-030584: Evaluation of secure algorithm negotiation proposals. This was introduced by Siemens and described an analysis of different proposals available at SA WG3 meeting #29. Siemens concluded that the special-RAND mechanism was the only mechanism, available at SA WG3 meeting #29, which provides the required security. Siemens also suggested that this mechanism requires further analysis to overcome identified issues.

TS S3-030542: Enhancements to GSM/UMTS AKA. This was introduced by Ericsson and suggested enhancements to key management for GSM and UMTS to limit the impact of the attack on A5/2. The proposal is to generate *algorithm-dependent* Keys so that the same key is not used for different algorithms.

It was commented that this mechanism would need to be secured to prevent MITM bidding down from support of this mechanism to no support of the mechanism and that this requires some secure signalling mechanism of the network capabilities to the UE. Ericsson reported that this could be used as a complementary mechanism to other proposals.

TS S3-030588: Further development of the Special RAND mechanism. This was introduced by Vodafone on behalf of Vodafone and Orange and discussed the mechanism of Special-RAND which is used to restrict the encryption algorithms with which an authentication vector may be used. In case the RAND does not have the initial "Special-RAND" signature bits, then the RAND is processed in the normal way. Vodafone and Orange proposed that SA WG3 adopt this mechanism for Rel-6 and develop the corresponding 3GPP security specifications, involving other 3GPP Groups to develop their specifications within the Rel-6 time frame.

It was commented that this mechanism assumes the network capabilities are signalled between the Visited and Home Network in a secure way.

It was noted that there are still many open issues which need to be analysed in order to make a decision on the best mechanisms to choose. After some discussion it was agreed that the proposal for Special-RAND would be used as a basis for the solution and the independent key proposal would be taken into consideration for further development. Concerning TD S3-030584 analysis, **The working assumption proposed, that the Special-RAND mechanism will be considered for use with further analysis to be done, was adopted by SA WG3**. It was also noted that the implementation cut-off date for A5/3 (currently agreed as October 2004) should be reviewed when the new protection (e.g. Special-RAND) mechanism is more stable. It was noted that it would be advantageous to have the new protection mechanism in place at the A5/3 cut-off date, rather than having to introduce it afterwards. **ETSI SAGE were asked to verify that the reduction of effective RAND to 80-bits does not have any significant consequences**. It was agreed to send an LS to CN WG1 and CN WG4 informing them of the agreement to develop the Special-RAND mechanism and attaching an updated version of TD S3-030588 in TD S3-030651. This was provided in TD S3-030629 which was updated in TD S3-030652 and approved (TD S3-030651 was attached).

7.7 Immediate service termination (IST)

There were no specific contributions under this agenda item.

7.8 Fraud information gathering system (FIGS)

There were no specific contributions under this agenda item.

7.9 GAA and support for subscriber certificates

TS S3-030484: LS Response (from SA WG2) on new interface names. This was introduced by Nokia and requested SA WG3 to reconsider the use of reference points Ba and Bb and to use the "Z" interface labels. This was noted. Other LSs were considered and a response was provided in TD S3-030635 which was approved.

TS S3-030502: LS Response (from CN WG4) on Stage 3 level specification directions for support for subscriber certificate work item. This was introduced by Ericsson and asked SA WG3 to provide CN WG4 with clear guidance on Stage 3 requirements for Support for Subscriber Certificates. A reply LS was provided in TD S3-030636 which was updated in TD S3-030653 and approved.

TS S3-030512: Liaison Statement (from SA WG2) on Generic Authentication Architecture. This was introduced by Nortel Networks and asked SA WG3 to develop guidelines for GAA authentication and to try to avoid multiple new solutions where possible. This had been discussed in the MBMB/GAA ad-hoc meeting and was therefore noted.

TS S3-030498: Reply LS (from CN WG1) on stage 3 level specification directions for support for subscriber certificate work item. The use of Protocol A was acceptable, but the use of Protocol B would need further analysis by SA WG3. The LS was then noted.

TS S3-030488: Draft 3GPP TS 33.109 V0.3.0: Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description. This was introduced by Nokia and included changes agreed since the previous version. The Editor was asked to include revision marks for future updates. The draft TS was then noted.

TS S3-030536: Subscriber Certificate Profiles. This was introduced by Nokia and described the status of Subscriber Certificate Profiles in standardisation bodies. It then proposes a Pseudo-CR to include a description of WAP Certificate and CRL profiles descriptions. It needed to be clarified whether this scheme would allow only a pointer to the Certificate to be sent over the radio interface, rather than the whole Certificate, for performance reasons. It was also agreed that the Editors note should stay in the draft. The Pseudo-CR was then approved for inclusion by the editor in the draft TS, leaving the editors note in place.

TS S3-030546: Generic Bootstrapping Architecture (GBA) Technical Specification and Work Item Proposal. This was introduced by Ericsson and proposed SA WG3 consider creating a new TS on Generic Bootstrapping Architecture (GBA) and to evaluate the need for a WI to manage the GBA work. The GBA TS could potentially be used for SSC, MBMS, Presence and WLAN. The Draft GBA TS and a proposed WID for GBA was attached. Nokia commented that the creation of a WID was acceptable, but that the Subscriber Certificates Draft TS should not be split up as it is a necessary part of the GAA. An off-line discussion was held and it was proposed that the following documents could be needed if the work was to be split:

- GAA - Overall TR;
- Certificate Retrieval using GBA;
- Specification of GBA;
- Authentication Proxy.

It was decided to consider the other contributions on this subject before discussing whether and how to split the work. After this, an evening discussion group was set up to agree on the split and content of the documents.

Results of GAA discussion group:

TD S3-030642: Report on GAA evening session, October 9, 2003. The report of the discussions was presented and noted. 4 TSs had been produced as follows:

> TD S3-030643: Draft TR: Generic Authentication Architecture; System Description (Rel-6).
> TD S3-030644: Draft TS: Generic Authentication Architecture; Generic Bootstrapping Architecture (Rel-6)
> TD S3-030645: Draft TS: Generic Authentication Architecture; Support for Subscriber Certificates (Rel-6). It was agreed that the Pseudo-CR in TD S3-030645 will form the baseline text of the TS, for e-mail correction. It was also agreed that Annex B of TS 33.109 will be moved to the main body of the TS.

TD S3-030646: Draft TS: Generic Authentication Architecture; Access to Network Application Function using HTTPS (Rel-6)

It was agreed to give time to check and correct the drafts and delegates were asked to provide comments to the editors. Pseudo-CRs should be written to the versions after these editorial corrections have been made.

TS S3-030537: Naming in Generic Authentication Architecture (GAA). This was introduced by Nokia and proposed a mapping between current and new interface names. The proposed interface names were as follows:

Ub **B**ootstrapping air interface (from UE to BSF)
Ua **A**pplication air interface (from UE to NAF)
Zh **H**SS interface from BSF
Zn **N**AF interface from BSF

These interface names were approved

TS S3-030551: Generic Bootstrapping Architecture evaluation. This was introduced by Siemens and continued the evaluation of alternatives for a GBA started in the Siemens contribution TD S3z030011 to the SA WG3 Ad-hoc meeting in Antwerp. Siemens asked SA WG3 to endorse the following proposal:

1. A GBA shall be based on TS 33.109, section 4. **ENDORSED.**
2. TS 33.109, section 4, shall be modified and extended to cover the case of tunnelled authentication and of authentication proxies. **ENDORSED. The position in the specifications needs to be agreed.**
3. The material in section 3.1 of this contribution shall be taken as the basis for the modification and extension of TS 33.109, section 4. With these enhancements, TS 33.109, section 4, shall constitute the mandatory part of the GBA specification. Optional further additions shall not be precluded. **NOT ENDORSED. This is dependent upon the final structuring of TS 33.109**
4. SA3 has to decide whether an optimisation, as described in section 3.2 of this contribution, shall be standardised as an option. It is proposed that this decision be taken only when the technical issues, in particular those addressed in section 3.2, are clear. **ENDORSED.**
5. A GBA should respect the requirements on a GAA defined in S3z030003. An analysis needs to be written to check that the decisions taken at SA3#30 are in line with the requirements. **ENDORSED.**
6. A GBA should respect the HSS-related guidelines in S3-030460. An analysis needs to be written to check that the decisions taken at SA3#30 are in line with the requirements. **ENDORSED.**
7. SA3 must decide whether and how the GBA should apply to 3GPP Release 6 features. **ENDORSED.**
8. Detailed security solutions for a particular 3GPP Release 6 feature shall be specified in the pertinent TS, but as much reference as possible should be made to the updated TS 33.109. **ENDORSED - some Features related to GAA need separate discussion.**
9. A GBA shall be designed in such a way that it is compatible with the use of reverse http authentication proxies. **ENDORSED. An agreed definition of the term "reverse http authentication proxy" is needed.**
10. A GBA shall be designed in such a way that it addresses man-in-the-middle attacks with tunnelled authentication. **ENDORSED.**

TS S3-030540: Protocol between authentication proxy and application server. This was introduced by Ericsson and discussed the interface between authentication proxy and application servers. Ericsson proposed that SA WG3 adopt a working assumption that 3GPP shall develop a solution for this interface because there is no standard available and to use ***cookies*** in the solution because cookies were originally developed for solving the session management problem, and they are currently used to tie the end-user identity to HTTP session. A Pseudo-CR was attached including these proposals. TD S3-030555 contained a related proposal in section 3.3, which was also considered.

TS S3-030540 assumed the following requirements for the solution which were reviewed:

REQ 1: Authentication proxy shall be able to authenticate the end-user identity using the means of Generic Bootstrapping Architecture. **ENDORSED.**

REQ 2: Authentication proxy shall be able to send the end-user identity to the application server at the beginning of new HTTP session. **ENDORSED.**

REQ 3: Application servers shall be able to use appropriate session management mechanisms with the client. **<REFORMULATE>.**

REQ 4: The client shall be able to create several parallel HTTP sessions via the authentication proxy to different application servers. **<REFORMULATE>.**

An evening session was held to discuss the possible splitting of the work into different documents, and the results of the discussions were presented in TD S3-030630:

1. *It is agreed to split to 4 specifications:*
   - *GAA, a TR gives a description of the overall architecture, and relation between each functionality. The TR will also provide some guidelines on criteria of deploying the alternative mechanisms to the services. Editor will be Annelies.*
   - *GBA, a TS, shall be largely based on the section 4 of the 33.109, gives description of the BSF functionality. Editor will be Tao Haukka.*
   - *SSC, a TS, shall be largely based on the section 5 and Annex A of the 33.109. Editor will be Pekka Laitinen and Tao Haukka.*
   - *HTTPS, a TS shall describe the TLS tunnel (33.109 v0.3.0 protocol B) by means of the GBA and SSC. Editor will be Bengt Sahlin.*
2. *No new WID to be generated, all concrete work will be under the original one with no updating.*
3. *Rapporteur of the WI is Tao Haukka.*
4. *All the work will be finished within the R6 timeframe as planed for the WI.*
5. *The Table of Contents for every specification is to be provided for Thursday evening session.*
6. *The final Table of Contents is to be endorsed by the this meeting.*

There was some objection to this splitting, and it was commented that the Presence requirements have been available from SA WG1 for some time, and also that the Presence TS needs to be ready for presentation to TSG SA in December 2003 and there was concern about being able to complete the work in time for this. there was some discussion on this and it was recognised that more evening discussion would be needed between interested companies and initial drafting of the documents should start for presentation to the meeting on Friday morning. **Material should be taken from the agreed documents on this subject in order to have reasonably acceptable and stable TSs and TRs**.

An evening discussion was held on TD S3-030540 and the Pseudo-CR was revised in TD S3-030631. This Pseudo-CR was approved for inclusion by the editor in the draft TS.

TS S3-030553: Difficulties in using one TLS tunnel to access different servers behind an authentication proxy. This was introduced by Siemens and addressed two problems, “name based virtual hosts over TLS” and “using a single TLS connection to access different hosts”. It was commented that the authentication Proxy is not well-defined and different understandings of the functionality of this existed. Ericsson reported that their intention for a solution was similar to the Workaround 3 in this contribution (section 4.3.3).

The SA WG3 Chairman summarised that it had been asked whether the GBA cannot be used for Application Servers without Proxy functionality. It was also a working assumption that Authentication of the different services should be harmonised, as far as practical, across the Services. It had also been assumed that the use of Authentication Proxy is optional.

The SA WG3 Chairman also summarised that **for HTTP-based services**, SA WG3 have a Working Assumption that for each of the Rel-6 Services, SA WG3 will decide which mechanisms are to be used and only one way will be specified for each Service. Although it has not been decided whether GBA or GAA will be used for the Presence Service, if GBA is chosen, we would need to use either an Authentication Proxy or the Application Server (i.e. the Presence Server) with the BSF. If the Authentication Proxy is identified, should it be made mandatory for the Presence Service.

It was decided to check other contributions before deciding whether the SA WG3 Working Assumptions need to be modified as a result of the Siemens analysis:

Ericsson stated that they thought that the mechanisms described need further security analysis before agreeing to them.

3 things to decide:

a) Use Authentication Proxy

b) Don't use Authentication Proxy
c) If Authentication Proxy is used, Should it be Mandated or Not?

It was agreed that it needs to be confirmed whether the Authentication Proxy will be transparent to the terminal or not before it can be decided whether it can be Mandated, as if not transparent, then the terminal implementation would need to be mandated. The current Working Assumption should be reviewed at the next meeting after this is known.

SA WG3 delegates were asked to study this issue and contribute to the next meeting in order for a decision to be made and the work progress.

TS S3-030555: Using shared key TLS with GAA NAFs. This was introduced by Nokia and described how shared key TLS can be used in GAA. Nokia concluded that this provides an attractive way to use GBA based shared secret within GAA. It also does not require any changes in TLS protocol itself. However, minor modifications in TLS implementations are needed. This was noted and should be kept in mind when developing solutions.

TS S3-030576: Comparison of different solutions for GBA and AP based AS: standard TLS versus shared secret based TLS. This was introduced by Alcatel and was mainly in line with the contribution TD S3-030555.

TS S3-030556: Use of shared keys in the TLS protocol: IETF status update. This was introduced by Nokia and provided information on the IETF Draft. It reported that this was intended to become an informational RFC and appears likely to be completed in the Rel-6 time frame.

TS S3-030545: Initiation of bootstrapping procedure. This was introduced by Ericsson and proposed the addition of the Bootstrapping initiation procedure in an attached Pseudo-CR. Changes were agreed to the editors note, and the changes were then agreed. The editor was asked to include the agreed changes in the draft TS.

TS S3-030538: Pseudo CR to draft TS on Subscriber Certificates: Requirements for A and C interface. This was introduced by Nokia. For Clause 4.1.4, an editors note should be added to show the difference between the meaning of bullets 1 and 2. For Clause 4.1.5, the 3rd bullet was clarified to allow the vectors to be sent in batches. 4th bullet point should be clarified with an editors note that there are open issues on the GAA profiles and the 6th bullet was clarified as all procedures in the BSF are initiated by the BSF. An additional bullet should be added stating that it is desirable to allow re-use of existing interfaces to implement the Zh interface. **With these changes**, the Pseudo-CR was approved for inclusion by the editor in the draft TS.

It was agreed that the interface names should be updated with the ones agreed at this meeting and editors of the draft TSs and TRs were tasked to update their documents for the next meeting (rather than asking for Pseudo-CRs to do this).

NOTE: A response to the LS from CN WG1 in TD S3-030502 was provided in TD S3-030636 (see below).

TS S3-030552: Key separation in a Generic Bootstrapping Architecture. This was introduced by Siemens and proposed that SA WG3 adopt the mechanisms discussed in the contribution. It was clarified that there should be no restrictions set on the Authentication Proxy with this mechanism. It was clarified that the threat in Variant 1 was tackled by the BSF deriving a key from NAF1 and the attacked server NAF1 can only obtain keys from the BSF which are specific to NAF1 and cannot be used with the rogue server. The proposals were considered in order and the following agreements made:

1. *The Generic Bootstrapping Architecture is meant to be a generic tool to provide shared keys to UEs and application servers, independent of particular key uses. Section 2 showed threats, which become possible if only one application server is successfully attacked. SA3 is asked to endorse that the threats should be mitigated by appropriate provisions in the standard. In particular, it shall be prevented that a security breach in one application server can spread across the entire system.* Agreed.

2. *It was proposed in section 3 to limit the effect of a security breach in one part of the system to a small part of the system by introducing key derivation for the keys shared between UE and NAF. SA3 is asked to endorse the use of a suitable key derivation procedure.* It was recognised that further

discussion is needed on the choice of key derivation mechanisms which binds keys with adequate identity to mitigate the threat. Agreed to look for a suitable solution.

3. *Section 4 proposed certain alternatives for the NAF identifier which is input to the key derivation parameters. The NAF identifier would determine the degree of assurance the UE gets about the identity of the NAF in NAF-to-UE authentication. SA3 is asked to agree to study only alternatives 1 (use DNS server name) or 2 (use defined parts of DNS server name) further and select between these alternatives at the next meeting.* It was decided to allow delegates to analyse this proposal and make a decision at the next meeting based on available scheme proposals.

4. *Section 5 proposed a flexible mechanism to signal that one out of possibly multiple key derivation schemes be used with a certain key. As a minimum, the mechanism could be used to signal whether no key derivation or some pre-determined key derivation is used. SA3 is asked to endorse the use of this flexible signalling mechanism.* It was decided to allow delegates to analyse this proposal and make adopt this at the next meeting if there are no alternative proposals.

TS S3-030558: GAA-Application-Profiles definition. This was introduced by Nokia and provided a description of how the requirements in draft TS 33.109, Clause A.2.4 (home operator control) could be implemented. Nokia recommended to send this contribution to CN WG4 as an LS to guide them on their stage 3 specification work for the C/Zh and D/Zn interfaces. It was not considered appropriate to send this Stage 3 information to CN WG4 as a Liaison from SA WG3, so Nokia were encouraged to input this to CN WG4 as a company input.

TS S3-030561: Pseudo-CR to 33.109: Informative annex on key pair storage. This was provided by Gemplus and SchlumbergerSema and proposed a new Annex C to cover Key Pair Storage, as decided in the previous meeting to include in the draft TS as an informative Annex. There were some comments and suggestions for enhancement of the annex with additional threats and modifications to the text, which, due to lack of time, were deferred for e-mail discussion to be run by Mireille Pauliac, with 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.

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.

7.10 WLAN interworking

TS S3-030492: Draft TS 33.234 V0.6.0 (2003-09): Wireless Local Area Network (WLAN) Interworking Security; (Release 6). It was noted that the interfaces needed correction in Figure 4.1. There were contributions to correct reference points, so this should be corrected by the next meeting anyhow. There are empty clauses in the document which will be considered for deletion at the next meeting if there is no input. It is intended to finalise this for presentation to TSG SA for information in December 2003.

TS S3-030508: LS response (from T WG2) to SA2 on UE Tunnelling. This was introduced by Nokia and was provided for information. The LS was noted.

TS S3-030547: Pseudo-CR to 33.234: Re-authentication procedures. This was introduced by Ericsson and discussed. The WLAN-AN initiation of re-authentication was questioned and further clarification was requested from Ericsson. Contributions were invited to the next meeting for the Stage 2 re-authentication mechanism. The document was revised to take comments into account in TD S3-030638 which was approved for inclusion by the editor in the draft TS. If there was an unwanted change between the two versions this can be dealt with by further Pseudo-CRs.

TS S3-030548: Pseudo-CR to 33.234: Alignment with WLAN architecture definition. This was introduced by Ericsson and discussed. The Wp interface should be added between WAG and PDG in figure 4.2, rather than Wn. With this change, this Pseudo-CR was approved for inclusion by the editor in the draft TS.

TS S3-030550: Evaluation of alternatives for secure set-up of UE initiated tunnels. This was introduced by Siemens and analysed possibilities for secure set-up of UE initiated tunnels. The use of IKEv2 was questioned as the preferred solution, as this could be done with IKE, which is available already. The conclusions on the use of Certificates were also questioned.

Siemens proposed 3 working assumptions and asked SA WG3 to endorse them:

WA1: Use IPsec ESP to protect the tunnels between UE and PDG required by scenario 3.
Endorsed as a Working Assumption.

WA2: The security mechanisms used in context with the IP tunnel in scenario 3 are to be independent of the link layer security in scenario 2.
Endorsed as a Working Assumption. (It was noted that the independence requirement is not for security reasons). It was agreed that if the solution developed implies significant inefficiencies then this would be reported to SA WG2 for possible revision of this independence requirement.

WA3: SA WG3 will concentrate their further study on IKE and IKEv2.
The following modified Working Assumption was endorsed: SA WG3 will concentrate their further study on IKE and IKEv2 for setting up the keys for IPsec ESP.

Siemens also concluded that SA WG3 need to solve the following tasks relating to the security of scenario 3 and asked SA WG3 to endorse them:

TD1: Define a profile of IPsec ESP for use with scenario 3.
Endorsed as a Task for SA WG3.

TD2: Standardise the set-up of security associations for IPsec ESP between UE and PDG.
Endorsed as a Task for SA WG3.

It was agreed that the security solution is in line with the requirements for charging, Lawful Interception and migration to further scenarios.

TS S3-030557: UE-Initiated Tunnelling with IKEv2. This was introduced by Nokia and proposed that SA WG3 studies IPsec with IKEv2 for a secure VPN solution for UE-initiated tunnelling in 3GPP-WLAN interworking scenario 3 and takes under further investigation the related design details. This proposal was covered by earlier discussions so the contribution was noted. It was noted that the LI impacts of the tunnelling solution should be analysed by the LI Group.

AP 30/034: B. Wilhelm to ask LI group to investigate the LI impacts of the tunnelling solution for WLAN interworking.

7.11 Visibility and configurability of security

There were no specific contributions under this agenda item.

7.12 Push

There were no specific contributions under this agenda item.

7.13 Priority

There were no specific contributions under this agenda item.

7.14 Location services (LCS)

There were no specific contributions under this agenda item.

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

TS S3-030595: Technical Report on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6). This was introduced by T-Mobile on behalf of Toshiba, Intel, T-Mobile, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC and Alcatel and included the changes agreed by the conference-call group since the last meeting of SA WG3. The draft TR was noted.

It was also noted that the SIM specification is frozen at Release 4 and cannot be modified as suggested in section 4.3, issues 2 and 3 and the possibilities to modify the U(SIM) needs to be modified to "USIM".

It was clarified that the ownership and control of the UICC remains with the operator which issued the UICC.

It was noted that Comments fields (i.e. before the clause 5 heading) and other editorial items would need to be tidied up to put them into normal 3GPP drafting rules format before presentation to TSG SA. **It was agreed that from the SA WG3 viewpoint, ISIM could be included in the scope of the feasibility study**. It was noted that the addition to the scope was badly formulated and should be removed or clarified.

The security issues in clause 6.3 should also be reviewed to clarify the assumptions made for successful attacks.

The downgrading of the bullet 9 to a note in clause 5 was considered confusing and the note should be re-worded to clarify the meaning.

TS S3-030571: High Level Requirements for UICC re-use by peripheral Devices on Local Interfaces. This was introduced by **3** and proposed several high level requirements for the study item on re-using a UICC over a local interface for acceptance by SA WG3. C. Blanchard agreed to help in the drafting of a Pseudo-CR for the draft TR. It was clarified that it needs to be assumed that there will be only 1 application on the UICC (i.e. current UICCs) which will be shared between devices.

The editor of the feasibility study was asked to incorporate the comments raised at the meeting and to distribute the updated version to the SA WG3 list in order that delegates can provide any necessary Pseudo-CRs to the next SA WG3 meeting.

7.16 Open service architecture (OSA)

There were no specific contributions under this agenda item.

7.17 Generic user profile (GUP)

TS S3-030509: LS response (from T WG2) on usage of GUP reference points. This was introduced by the SA WG3 Chairman and was copied to SA WG3 for information. The LS was noted.

TS S3-030581: GUP security directions. This was introduced by Nokia and was provided in order to start the work on the Generic User Profile (GUP) Security. Nokia proposed that SA WG3 should discuss the handling of the GUP security work to support the work of CN WG4 and SA WG2, including the scope and format of the security work (e.g. via CRs to relevant TSs). Nokia also suggested that CN WG4 specifications should be mentioned in the SA WG3 GUP Security WID. Furthermore it was suggested that SA WG3 should consider taking the Liberty Alliance Project ID-WSF security solutions as the basis for the work. The requirements leading to the adoption of the Liberty Alliance work was questioned. Nokia agreed to try to provide additional information on their work and report back to SA WG3. It was also reported that the Liberty Alliance specifications may not be openly available which would make a problem for referencing from 3GPP specifications. This would need to be investigated.

AP 30/045: B Owen to respond to LSs on GUP from meeting #29, informing the senders that there are still open issues in SA WG3.

7.18 Presence

TS S3-030525: Draft TR 33.9bc V0.6.0 Presence Service; Security. This was introduced by the editor (K. Boman) and included changes agreed at the last meeting. The TR was noted.

TS S3-030524: Draft TS 33.1bc V0.1.0 Presence Service; Security. This was introduced by the editor (K. Boman) and was an implementation of the text that he was asked to insert into the new TS at the previous SA WG3 meeting.

NOTE: The draft TS had not been allocated a specification number officially, but was likely to be allocated to TS 33.141.

TS S3-030578: P-CR for Presence TR 33.abc v0.6.0. This was introduced by Nokia. There was some concern over the apparent mandating of the Authentication Proxy (NAF). It was clarified that this was not the intention at this time. It was also clarified that the proposal was based on the shared-key TLS (which is not currently agreed in SA WG3). The changes in clause 6.2 were agreed with some changes which were noted by the Editor for inclusion in the draft TS.

The draft TS for presence security was updated with the agreed changes and provided in TD S3-030647 which was agreed as a basis for further Pseudo-CRs.

7.19 User equipment management (UEM)

There were no specific contributions under this agenda item.

7.20 Multimedia broadcast/multicast service (MBMS)

TS S3-030517: Latest version of MBMS TS. This was provided for information and was noted.

TS S3-030503: Reply LS (from SA WG1) on clarification of MBMS charging issues. This was introduced by the SA WG3 Chairman. This had been considered in the MBMS ~~A~~ ad-hoc meeting and was noted.

TS S3-030504: LS (from SA WG1) regarding progress of work for MBMS User Services. This was introduced by Motorola and was copied to SA WG3 for information. The LS was noted.

TS S3-030507: LS (from SA WG4) on “Update of WID on MBMS". This was introduced by Nokia and informed SA WG3 that the WID for MBMS had been updated. The LS was noted.

TS S3-030511: LS (from T WG3) on potential USIM impact of the MBMS security framework. This had been considered in the MBMA ad-hoc meeting and was noted. The SA WG3 Chairman reminded delegates that TSG SA had asked SA WG3 to inform T WG3 as soon as possible about the MBMS security impacts on the USIM. Based on the current agreements in SA WG3 an LS to reply to T WG3 informing them that they can start work will be provided by e-mail approval.

AP 30/05~~5~~6: 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. This LS was discussed and approved over e-mail and allocated to TD S3-030660 (for information to SA WG3 at meeting #31).

TS S3-030528: Progress report on MBMS 3GPP2 solution. This was provided by BT, Gemplus, Oberthur, Qualcomm and SchlumbergerSema. It was suggested that this is used for detailed discussion of the proposals at the meeting. The report was then noted.

TS S3-030582: Pseudo-CR to 33.246: MBMS broadcast security requirements clarification. This Pseudo-CR was revised in TD S3-030640 and approved.

TS S3-030513: Proposed CR to TS 33.246 MBMS Security Requirements CR (non controversial) - (Rel-6). Many changes were made to the proposals and the Pseudo-CR was updated in TD S3-030641 which was approved for inclusion by the editor in the draft TS..

TS S3-030514: Proposed CR to TS 33.246 MBMS Security Requirements CR (controversial) - (Rel-6). This Pseudo-CR was rejected as more contribution on the Key Management Centre position in the architecture and functionality is needed. Contribution was invited on the various proposals in the Pseudo-CR.

TS S3-030519: Re-keying resource , security and quality. Postponed: Contribution invited on proposals for next meeting.

TS S3-030522: Differentiation of MBMS traffic protection mechanisms. Postponed: Contribution invited on proposals for next meeting.

TS S3-030523: MBMS service activation and Initial TEK distribution. Postponed: Contribution invited on proposals for next meeting.

TS S3-030529: MBMS Usage and Quality of Service based on BAK Distribution. Postponed: Contribution invited on proposals for next meeting.

TS S3-030521: Simple PTP method in detail. This was introduced by Huawei Technologies Co., Ltd and proposed that if simple PTP model is accepted, a figure and explanation is added to the draft TS. There was

no agreement on the choice of mechanism reached at the meeting. This should be reconsidered if appropriate when agreement is reached.

TS S3-030520: Improved combined re-keying method. This was introduced by Huawei Technologies Co., Ltd and proposed that if combined re-keying method is accepted, then SA WG3 select either clause 2.1 or clause 2.2 of the contribution to enhance the combined re-keying performance. There was no agreement on the choice of mechanism reached at the meeting. This should be reconsidered if appropriate when agreement is reached.

TS S3-030539: Key management considerations for MBMS. This was introduced by Ericsson and discussed different key management methods that are non-UICC based and UICC based. Ericsson concluded that the UICC based solutions need further study. The OTA contribution in TD S3-030534 was considered. The contribution was then noted.

TS S3-030534: Over-The-Air (OTA) technology. This was provided by Gemplus, Oberthur and Schlumberger. It was recommended to adopt the MBMS 3GPP2 solution for MBMS security. The backward compatibility issues for pre-Rel-6 UICCs may be solved using OTA mechanisms for Remote Applet/File Management in order to properly update the legacy USIMs. It was asked whether the OTA security issues for MMS presented to the meeting were applicable to MBMS. This required more investigation. The authors were thanked for doing this study and presenting the results to the meeting. The contribution was then noted.

TS S3-030583: Key distribution protocol selection. This was introduced by Siemens and studied the Key distribution protocol selection issues. Siemens concluded that OTA has been restricted by design to be used only by the Home Network. If OTA is selected as the Key distribution mechanism to transfer an MBMS key to the card then many application servers will need to be connected to the Home Network OTA server. The OTA server in the Home Network will also get knowledge of MBMS keys of Visited Network MBMS services. Siemens proposed that OTA should not be adopted as a solution to update MBMS keys to the UICC or to the terminal. It was clarified that Siemens considered DRM to be in competition in respect that they both target high-value content markets. The contribution was noted.

TS S3-030586: MBMS Key distribution. Siemens introduced the conclusion of this contribution which proposed that SA WG3 adopt the working assumption that an authentication proxy with shared TLS tunnel shall not be used for MBMS key distribution. **This Working Assumption was adopted**.

TS S3-030580: MBMS – Overhead of the Re-keying. This was introduced by Nokia and provided an analysis on the overheads in data for Combined and PTP Re-Keying methods. Operators had been asked at the previous meeting to investigate how important it is to offer MBMS without an upgrade to the UICC. In practice, it was reported that at least the OTA upgrade of the UICC to support MBMS was important. It was clarified that pre-Rel-6 UICC can support OTA if it implements the optional USIM Toolkit feature (and has sufficient free space for the application). Operators indicated that this was an acceptable pre-requisite for the support of MBMS with pre-Rel-6 UICC. With this agreement, companies were asked to indicate support for each of the methods. **The document was noted and delegates were asked to consider the order of preference for each of the 3 methods so that a decision can be made at the next SA WG3 meeting.**

TS S3-030515: Proposed Draft LS on clarification of MBMS Service Requirements/assumptions. The CR did not reflect agreements that have been reached at this meeting, and substantial changes would be required. As the Author was no longer at the meeting and the timescales for this were not critical to the work, the LS was not approved. The Author will be informed of this and may re-submit another LS to the next meeting if he wishes.

TS S3-030544: 3GPP Over the Air (OTA) procedures applied to BAK Distribution and MBMS Subscription management. There was insufficient time to deal with this document and delegates asked to consider the contents and send any comments to the authors.

7.21 Key Management of group keys for Voice Group Call Services

TS S3-030559: Voice Group Call Services. This was provided by Vodafone and Siemens and proposed that SA WG3 adopt the following principles:

1. For each voice group up to 15 group keys can be defined (identified by a group key number).
   Endorsed.
2. The group keys are stored in
   - the group call register (GCR) on the network side (which is co-located to an MSC),
   - USIM on the UE side.
   Endorsed.
3. 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.
   Endorsed.
4. A key management centre (KMC) takes care that the group keys are up to date at all locations and are exchanged from time to time (which is up to the operator's policy).
   Endorsed. It was recognised that the Keys must be refreshed frequently enough. A study is needed to determine an appropriate Key refresh rate.
5. The interface between KMC and the GCRs and between the KMC and the USIM are out of scope of the 3GPP specifications. However for the latter transmission via OTA is recommended.
   Further study is needed on whether this interface should be in the Scope of 3GPP.
6. The KMC is out of scope of 3GPP specification. In an informative annex the most important tasks of the KMC can be described.
7. For encryption the same algorithms are used as for normal GSM-speech calls (i.e. A5/0-A5/7).
   Endorsed, it was recognised that the Key Management system will need to be investigated to ensure regular Key refreshing.
8. It is FFS how the UE gets the information which cipher algorithm is used for a group call. There are two options: signal the cipher algorithm via the air-interface or store it on the USIM.
   First sentence is endorsed. The second sentence requires further investigation and LS to T WG3.

A proposed CR to 43.020 was attached and it was proposed to send this with a liaison statement to T WG3 requesting them to make the appropriate changes to their specifications.

It was commented that the security of such a service would need consideration, in order to counter the possible voice stream key repeat (i.e. regular key changes / SQN system) which implies key distribution and management issues.

It was commented that draft CRs had been sent to SA WG1 along with LSs asking if this service is still required. It appeared that the answer was yes. The proposals were reviewed and agreed as shown above. The CR could not be approved as it stood as the proposals had not been agreed without change. It was agreed to provide an LS to T WG3, to be approved by e-mail. **M. Blommaert agreed to provide the LS by 14 October and run the e-mail approval process. Comments by 20 October, approval 23 October 2003**. TD S3-030639 was allocated for the approved LS.

7.22 Guide to 3G security (TR 33.900)

There were no specific contributions under this agenda item.

8 Review and update of work programme

AP 30/067: Rapporteurs of SA WG3 Work Items to provide the SA WG3 Secretary with updates to the Work Plan by 24 October 2003.

9 Future meeting dates and venues

TD S3-030628: Invitation to SA WG3 meeting #31, Munich, Germany. This was provided for information as the deadline for Hotel booking is fairly short, delegates were asked to register and book the Hotel in good time for the meeting. The invitation was then noted.

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#31	18-21 November 2003	Munich, Germany	European Friends of 3GPP
S3#32	**09-13 February 2004**	Australia (TBC)	Qualcomm (TBC)
S3#33	**04-07 May 2004**	Korea (TBC)	Samsung (TBC)
S3#34	06-09 July 2004 (TBC)	USA (TBC)	"NA Friends of 3GPP" (TBC)
S3#35	October 2004	Host required	Host required

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#11	18-20 November 2003	London	DTI
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**
TSG#23	March 9-12 & 15-18 2004	Phoenix, USA	
TSG#24	June 1-4 & 7-10 2004	Korea	
TSG#25	7-10 & 13-16 September 2004	USA	
TSG#26	7-10 & 13-16 December 2004	To Be Decided	

10 Any other business

TD S3-030637 MMS Charging Principles Handbook. This was presented by Ansgar Bergmann and described the current GSMA MMS Charging principles handbook. Mr Bergmann was thanked for his presentation which was noted.

TD S3-030622 First draft of MMS Security Paper - version 0.1.1. This was presented by Ansgar Bergmann for information as an introduction to the status of MMS security work in the GSMA. This interesting report should be further considered by delegates and contribution and comments should be sent to Mr. Ansgar Bergmann or Mr. Stefan Andersson. The document was then noted.

Close

The Chairman, V. Niemi, thanked delegates for their hard work during the meeting and the Hosts for the facilities. He thanked Sebastien Nguyen Ngoc had announced that this was his last regular attendance to the SA WG3 meetings. He was applauded and thanked for his excellent work in the group and wished good luck with his future work. He then closed the meeting.

Annex A: List of attendees at the SA WG3#3028 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. Nigel Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	+44 7785 31 86 31	+44 1 256 790 169	+44 1 256 790190	GB	ETSI
Dr. Ansgar Bergmann	GSM Association	ansgar_bergmann@yahoo.co.uk	+33 6 09 97 07 01	+33 6 09 97 07 01	+33 4 9312 1824	IE	MKT_REP
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. Charles Brookson	DTI	cbrookson@iee.org	+44 7956 567 102	+44 20 7215 3691	+44 20 7931 7194	GB	ETSI
Mr. Holger Butscheidt	BMWi	Holger.Butscheidt@RegTP.de		+49 6131 18 2224	+49 6131 18 5613	DE	ETSI
Mr. Lorenzo Casaccia	QUALCOMM EUROPE S.A.R.L.	lorenzoc@qualcomm.com		+1 858 651 4319	+1 858 658 2113	FR	ETSI
Mr. Mauro Castagno	TELECOM ITALIA S.p.A.	mauro.castagno@telecomitalia.it		+39 0112285203	+39 0112287056	IT	ETSI
Mr. Sharat Chander	AT&T Wireless Services, Inc.	sharat.chander@attws.com	+1 435 894 7756	+1 425 580 6596	+1 425 580 6811	US	T1
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp		+81 467 41 2181	+81 467 41 2185	JP	ARIB
Mr. Per Christoffersson	TeliaSonera AB	per.christoffersson@teliasonera.com		+46 705 925100		SE	ETSI
Mr. Kevin England	mmO2 plc	kevin.england@o2.com	+447710016799	+447710016799		GB	ETSI
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. John B Fenn	SAMSUNG Electronics	johnbfenn@aol.com	+44 78 02 339070	+44 1784 428 600	+44 1784 428 629	GB	ETSI
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 FRANCE	sylvie.fouquet@francetelecom.com		+33 145 29 49 19	+33 145 29 65 19	FR	ETSI
Dr. Eric Gauthier	ORANGE FRANCE	eric.gauthier@orange.ch		+41 21 216 53 08	+41 21 216 18 88	FR	ETSI
Ms. Tao Haukka	Nokia Korea	tao.haukka@nokia.com		+358 40 5170079		KR	TTA
Mr. Philip Hawkes	QUALCOMM EUROPE S.A.R.L.	phawkes@qualcomm.com		+61-2-9817-4188	+61-2-9817-5199	FR	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@siemens.com		+49 8963 641494	+49 8963 648000	DE	ETSI
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vodafone.com	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB	ETSI
Mr. Yu Inamura	NTT DoCoMo, Inc.	jane@mml.yrp.nttdocomo.co.jp		+81-46-840-3975	+81-46-840-3364	JP	ARIB
Mr. Edouard Issenmann	ALCATEL S.A.	edouard.issenmann@alcatel.fr		+33 1 30 77 93 01	+33 1 30 77 0369	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@ccrle.nec.de		+49 6221 905 11 50	+49 62219051155	GB	ETSI
Mr. Alex Leadbeater	BT Group Plc	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. Michael Marcovici	Lucent Technologies	marcovici@lucent.com		+1 630 979 4062	+1 630 224 9955	US	T1
Mr. David Mariblanca	ERICSSON LM	david.mariblanca@ericsson.com		+34 646004736	+34 913392538	SE	ETSI
Mr. Georg Mayer	NOKIA Corporation	georg.mayer@nokia.com	+358 50 48 21437	+358 5048 21437	+358 7180 68222	FI	ETSI
Mr. Sebastien Nguyen Ngoc	ORANGE FRANCE	sebastien.nguyenngoc@francetelecom.com		+33 1 45 29 47 31	+33 1 45 29 65 19	FR	ETSI
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. 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

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
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. Bengt Sahlin	ERICSSON LM	Bengt.Sahlin@lmf.ericsson.se		+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 22893633309	DE	ETSI
Mr. James Semple	QUALCOMM EUROPE S.A.R.L.	c_jsemple@qualcomm.com		+447880791303		FR	ETSI
Mr. Vesa Torvinen	ERICSSON LM	vesa.torvinen@ericsson.com	+358 407230822	+358407230822	+358 9 299 2171	SE	ETSI
Ms. Annelies Van Moffaert	ALCATEL S.A.	annelies.van_moffaert@alcatel.be		+32 3 240 83 58	+32 3 240 48 88	FR	ETSI
Mr. Tommi Viitanen	Nokia Telecommunications Inc.	tommi.viitanen@nokia.com		+358405131090	+358718075300	US	T1
Ms. Monica Wifvesson	ERICSSON LM	monica.wifvesson@ericsson.com		+46 46 193634	+46 46 231650	SE	ETSI
Mr. Berthold Wilhelm	BMWi	berthold.wilhelm@regtp.de		+49 681 9330 562	+49 681 9330 725	DE	ETSI
Mr. Yanmin Zhu	SAMSUNG Electronics	yanmin.zhu@samsung.com		+86-10-68427711	+86-10-68481891	GB	ETSI

48 attendees

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #28, #29 and #30, the following companies are eligible to vote at SA WG3 meeting #31:

Company	Country	Status	Partner Org
3	GB	3GPPMEMBER	ETSI
ALCATEL S.A.	FR	3GPPMEMBER	ETSI
AT&T Wireless Services, Inc.	US	3GPPMEMBER	T1
BT Group Plc	GB	3GPPMEMBER	ETSI
BUNDESMINISTERIUM FUR WIRTSCHAFT	DE	3GPPMEMBER	ETSI
China Mobile Communications Corporation (CMCC)	CN	3GPPMEMBER	CCSA
DTI - Department of Trade and Industry	GB	3GPPMEMBER	ETSI
GEMPLUS S.A.	FR	3GPPMEMBER	ETSI
GIESECKE & DEVRIENT GmbH	DE	3GPPMEMBER	ETSI
HUAWEI TECHNOLOGIES Co. Ltd.	CN	3GPPMEMBER	ETSI
Intel Corporation S.A.	BE	3GPPMEMBER	ETSI
Lucent Technologies	US	3GPPMEMBER	T1
Lucent Technologies Network Systems 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
Nortel Networks (USA)	US	3GPPMEMBER	T1
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
OBERTHUR CARD SYSTEMS S.A.	FR	3GPPMEMBER	ETSI
ORANGE FRANCE	FR	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
Research In Motion Limited	CA	3GPPMEMBER	ETSI
Samsung Electronics Ind. Co., Ltd.	KR	3GPPMEMBER	TTA
SAMSUNG Electronics Research Institute	GB	3GPPMEMBER	ETSI
SchlumbergerSema - Schlumberger Systèmes S.A	FR	3GPPMEMBER	ETSI
SIEMENS AG	DE	3GPPMEMBER	ETSI
Siemens nv/sa	BE	3GPPMEMBER	ETSI
SSH Communications Security Corp	FI	3GPPMEMBER	ETSI
T-MOBILE DEUTSCHLAND	DE	3GPPMEMBER	ETSI
TELECOM ITALIA S.p.A.	IT	3GPPMEMBER	ETSI
Telefon AB LM Ericsson	SE	3GPPMEMBER	ETSI
TeliaSonera AB	SE	3GPPMEMBER	ETSI
Toshiba Corporation, Digital Media Network Company	JP	3GPPMEMBER	ARIB
TruePosition Inc.	US	3GPPMEMBER	ETSI
Vodafone D2 GmbH	DE	3GPPMEMBER	ETSI
VODAFONE Group Plc	GB	3GPPMEMBER	ETSI

42 Individual Member Companies

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030480	Draft Agenda for SA WG3 meeting #30	SA WG3 Chairman	2	Approval	S3-030495	Revised in S3-030495
S3-030481	Draft report of TSG SA meeting #29	SA WG3 Secretary	5.1	Approval		Approved.
S3-030482	Draft Report of MBMS / GAA ad-hoc meeting	SA WG3 Vice-Chairman (P. Howard)	5.2	Approval		Approved
S3-030483	Draft agenda for joint SA3-CN1 session on IMS security	SA WG3 Chairman	4 + Joint	Approval		Approved. Also reviewed at S3 meeting
S3-030484	LS Response (from SA WG2) on new interface names	SA WG2	7.9	Action		Request to use Z interface names noted
S3-030485	LS reply on Rel-5 transport of unknown SIP signalling elements	SA WG5	7.1	Information		Noted
S3-030486	Letter to SA WG3 Chairman: PN-4465-RV1 (to be published as J-STD-025-B)	Chair, TIA TR-45 LAES Ad Hoc (Mrs. Terri L. Brooks)	6.7	Action		Noted. LI Group asked to look at this LS
S3-030487	Draft TS 33.310 V0.5.0: Network Domain Security; Authentication Framework	NDS/AF Rapporteur	7.4	Information		Noted. To be used for further updates
S3-030488	Draft 3GPP TS 33.109 V0.3.0: Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description	Editor	7.9	Information		Noted. Rev marks to be used in future
S3-030489	Proposed CR to 55.205: Correction of reference	TeliaSonera	6.3	Approval		Approved
S3-030490	LS (from GSMA-SG) on introduction of A5/3 in GSM handsets	GSMA SG	6.4	Action		Taken into account in discussions
S3-030491	LS (from SA WG3 LI Group) on new acronym	SA WG3-LI Group	5.4	Action		ANP acronym agreed
S3-030492	Draft TS 33.234 V0.6.0 (2003-09): Wireless Local Area Network (WLAN) Interworking Security; (Release 6)	Rapporteur	7.10	Information		Noted. To be finalised for submission to SA for info Nov 2003
S3-030493	Proposed CRs to 33.203: Correcting the text on sending an authentication response (Rel-5)	3	Joint - 5.1	Approval		Agreed with changes - to be endorsed by SA WG3 (in S3-030601)
S3-030494	Proposed CRs to 33.203: Correcting the text on sending an authentication response (Rel-6)	3	Joint - 5.1	Approval		Agreed with changes - to be endorsed by SA WG3 (in S3-030602)
S3-030495	Revised Draft Agenda for SA WG3 meeting #30	SA WG3 Chairman	2	Approval		Approved
S3-030496	SA WG3 Chairmans Report from SA#21 plenary	SA WG3 Chairman	5.3	Information		Noted
S3-030497	Liaison statement (from CN WG1) on Profiling of RFC3325 for IMS	CN WG1	Joint - 6.1	Action		Dealt with in joint session. No response LS needed
S3-030498	Reply LS (from CN WG1) on stage 3 level specification directions for support for subscriber certificate work item	CN WG1	7.9	Action		Protocol A OK, Protocol B for analysis.
S3-030499	Reply to LS (from CN WG1 - N1-031052) on 'Effects of service 27/38 on 2G/3G Interworking and emergency call' from SA3	CN WG1	7.5	Action		Discussed with S3-030510 and S3-030585. LS in S3-030624
S3-030500	Liaison statement (from CN WG1) on requesting a joint CN1-SA3 meeting	CN WG1	Joint -6.1	Action		Noted
S3-030501	LS (from CN WG2) on SA3 on Legal Interception of SCP initiated calls	CN WG2	6.1	Action		Noted. LI Group to deal with this LS.
S3-030502	LS Response (from CN WG4) on Stage 3 level specification directions for support for subscriber certificate work item	CN WG4	7.9	Action		Response LS in S3-030635
S3-030503	Reply LS (from SA WG1) on clarification of MBMS charging issues	SA WG1	7.20	Information		Noted
S3-030504	LS (from SA WG1) regarding progress of work for MBMS User Services	SA WG1	7.20	Information		Noted
S3-030505	Liaison (from SA WG4) Response to OMA	SA WG4	6.1	Information		Noted
S3-030506	LS (from SA WG4) on cipher suite for DRM-protected streamed media for PSS	SA WG4	6.1	Action		Response LS in S3-030621
S3-030507	LS (from SA WG4) on "Update of WID on MBMS"	SA WG4	7.20	Information		Noted
S3-030508	LS response (from T WG2) to SA2 on UE Tunnelling	T WG2	7.20	Information		Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030509	LS response (from T WG2) on usage of GUP reference points	T WG2	7.10	Information		Noted
S3-030510	LS (from T WG3) on the effects of USIM services 27 and 38	T WG3	7.17	Action		Discussed with S3-030499 and S3-030585. Noted. LS in S3-030624
S3-030511	LS (from T WG3) on potential USIM impact of the MBMS security framework	T WG3	7.5	Action		Noted
S3-030512	Liaison Statement (from SA WG2) on Generic Authentication Architecture	SA WG3	7.9	Action		Dealt with in ad-hoc meeting. Noted
S3-030513	Proposed Pseudo-CR to TS 33.246 MBMS Security Requirements CR (non controversial) - (Rel-6)	BT Group	7.20	Approval	S3-030641	revised in S3-030641
S3-030514	Proposed Pseudo-CR to TS 33.246 MBMS Security Requirements CR (controversial) - (Rel-6)	BT Group	7.20	Approval		Rejected. Contribution invited on proposals in this Pseudo-CR
S3-030515	Proposed Draft LS on clarification of MBMS Service Requirements/assumptions	BT Group	7.20	Approval		Postponed to next meeting as agreements have changed since written
S3-030516	Documents approved by e-mail after SA WG3 meeting #29	SA WG3 Secretary	5.1	Information	S3-030592	Updated in S3-030592
S3-030517	Latest version of MBMS TS	Rapporteur	7.20	Information		Noted
S3-030518	Proposed Technical Report on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces v0.0.7 (Release 6)	Toshiba, Intel, T-Mobile, Nokia, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel	7.15	Information	S3-030595	Revised in S3-030595 due to word processor errors
S3-030519	Re-keying resource , security and quality	Huawei Technologies Co., Ltd	7.20	Discussion		Postponed: Contribution invited on proposals
S3-030520	Improved combined re-keying method	Huawei Technologies Co., Ltd	7.20	Discussion / Decision		Depends on acceptance of combined re-keying. Return
S3-030521	Simple PTP method in detail	Huawei Technologies Co., Ltd	7.20	Discussion / Decision		Depends on acceptance of Simple PTP. Return
S3-030522	Differentiation of MBMS traffic protection mechanisms	Samsung Electronics	7.20	Discussion / Decision		Postponed: Contribution invited on proposals
S3-030523	MBMS service activation and Initial TEK distribution	Samsung Electronics	7.20	Discussion / Decision		Postponed: Contribution invited on proposals
S3-030524	Draft TS 33.cde V0.1.0 Presence Service; Security	Rapporteur	7.18	Information		Noted
S3-030525	Draft TR 33.cde V0.6.0 Presence Service; Security	Rapporteur	7.18	Information		Noted
S3-030526	Proposed CR to 33.203: UE populates RAND and AUTN when sending Digest response to the network (Rel-5)	Nokia	Joint - 5.5	Approval		Rejected. LS to CN1, CN4 produced in S3-030599
S3-030527	Proposed CR to 33.203: UE populates RAND and AUTN when sending Digest response to the network (Rel-6)	Nokia	Joint - 5.5	Approval		Rejected. LS to CN1, CN4 produced in S3-030599
S3-030528	Progress report on MBMS 3GPP2 solution	BT, Gemplus, Oberthur, QUALCOMM, SchlumbergerSema	7.20	Discussion / Decision		Noted. Take into account for detailed proposals
S3-030529	MBMS Usage and Quality of Service based on BAK Distribution	Gemplus, Oberthur, QUALCOMM Europe, SchlumbergerSema	7.20	Discussion		Postponed: Contribution invited on proposals
S3-030530	Proposed CR to 33.108: LI Reporting of Dialed Digits (Rel-6)	SA WG3 LI Group	5.4	Approval	S3-030606	Updated to latest version of 33.108. Revised in S3-030606
S3-030531	Proposed CR to 33.107: MSISDN/IMEI clarification for GPRS interception (Rel-6)	SA WG3 LI Group	5.4	Approval	S3-030607	Updated to Rel-6 version of 33.107. Revised in S3-030607
S3-030532	Proposed CR to 33.108: Correction to Annex G on TCP based transport (Rel-5)	SA WG3 LI Group	5.4	Approval		Updated to latest version of 33.108. Approved.

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030533	Proposed CR to 33.108: Correction to Annex G on TCP based transport (Rel-6)	SA WG3 LI Group	5.4	Approval	S3-030608	Updated to latest version of 33.108. Category corrected in S3-030608
S3-030534	Over-The-Air (OTA) technology	Gemplus, Oberthur, Schlumberger	7.20	Discussion / Decision		Noted
S3-030535	Pseudo CR to 33.310: Removal of support for delta CRLs (Rel-6)	Nokia, Siemens, SSH, T-Mobile, Vodafone	7.4	Approval		Approved
S3-030536	Subscriber Certificate Profiles	Nokia	7.9	Information		Presented and noted. Pseudo-CR agreed, but keep editors note
S3-030537	Naming in Generic Authentication Architecture (GAA)	Nokia	7.9	Discussion / Decision		Interface names approved
S3-030538	Pseudo CR to draft TS on Subscriber Certificates: Requirements for A and C interface	Nokia	7.9	Approval		Agreed with changes
S3-030539	Key management considerations for MBMS	Ericsson	7.20	Discussion / Decision		Noted
S3-030540	Protocol between authentication proxy and application server	Ericsson	7.9	Discussion / Decision		Pseudo-CR Updated in S3-030631
S3-030541	Proposed CR to 33.203: Introducing the SIP Privacy mechanism (Rel-6)	Ericsson	Joint - 6.1	Approval	S3-030600	Needs to be written to version 6.0.0. 1st para of 5.3 accepted for Rel-5. Revised in S3-030600
S3-030542	Enhancements to GSM/UMTS AKA	Ericsson	7.6	Discussion		Taken with S3-030584 and S3-030588. Special-RAND adopted for development. LS in S3-030629
S3-030543	IMS R5 profile of RFC 3329	Ericsson	7.1	Information	S3-030593	Revised in S3-030593
S3-030544	3GPP Over the Air (OTA) procedures applied to BAK Distribution and MBMS Subscription management	Schlumberger, QUALCOMM, GEMPLUS, OCS	7.20	Discussion / Decision		No time - delegates to send comments to authors
S3-030545	Initiation of bootstrapping procedure	Ericsson	7.9	Discussion / Decision		Agreed with modification
S3-030546	Generic Bootstrapping Architecture (GBA) Technical Specification and Work Item Proposal	Ericsson	7.9	Discussion / Decision		Draft TS and WID attached.
S3-030547	Pseudo-CR to 33.234: Re-authentication procedures	Ericsson	7.10	Approval	S3-030638	Revised in S3-030638
S3-030548	Pseudo-CR to 33.234: Alignment with WLAN architecture definition	Ericsson	7.10	Approval		Approved with minor change
S3-030549	Proposed CR to 33.102: Handling of key sets at inter-system change (Rel-5)	Ericsson	7.5	Approval	S3-030625	Revised in S3-030625
S3-030550	Evaluation of alternatives for secure set-up of UE initiated tunnels	Siemens	7.10	Discussion / Decision		Some working assumptions endorsed
S3-030551	Generic Bootstrapping Architecture evaluation	Siemens	7.9	Discussion / Decision		Proposals endorsed depending other discussions
S3-030552	Key separation in a Generic Bootstrapping Architecture	Siemens	7.9	Discussion / Decision		Proposals 1 and 2 accepted other proposals for further consideration for decision at next meeting
S3-030553	Difficulties in using one TLS tunnel to access different servers behind an authentication proxy	Siemens	7.9	Discussion / Decision		Need contribution to next meeting confirming transparency of Auth Proxy
S3-030554	Handling of Security Associations	Siemens	Joint - 5.2	Discussion / Decision		Return when Nokia CRs discussed
S3-030555	Using shared key TLS with GAA NAFs	Nokia	7.9	Discussion / Decision		Noted. To be kept in mind for discussion of solutions
S3-030556	Use of shared keys in the TLS protocol: IETF status update	Nokia	7.9	Information		Noted. Inf. RFC is likely to be ready for Rel-6
S3-030557	UE-Initiated Tunneling with IKEv2	Nokia	7.10	Discussion		Handled in evening session

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030558	GAA-Application-Profiles definition	Nokia	7.9	Discussion		Nokia to input to CN4 as company input
S3-030559	Voice Group Call Services	Vodafone, Siemens	7.21	Discussion / Decision		Most principles endorsed
S3-030560	Correction and Alignment of SA handling procedures	3	Joint - 5.2	Discussion / Approval		Reviewed in evening session. CRs provided for SA WG3 in S3-030603 and S3-030604
S3-030561	Pseudo-CR to 33.109: Informative annex on key pair storage	Gemplus, Schlumberger	7.9	Approval		Deferred to e-mail approval
S3-030562	Proposed CR to 33.203: Terminology alignment (Rel-5)	Nokia	Joint - 5.3	Approval	S3-030597	Some parts agreed for Rel-6 and included in S3-030597
S3-030563	Proposed CR to 33.203: Lifetime of old SAs (Rel-5)	Nokia	Joint - 5.2	Approval		Reviewed in evening session. To be developed off-line for next S3 meeting
S3-030564	Trustworthiness of the previous hop (IMS?) network (Rel-6)	Nokia	Joint - 5.4	Discussion		SA WG3 to consider a solution. Contributions invited
S3-030565	Trustworthiness of the next hop (IMS?) network	Nokia	Joint - 5.4	Discussion		Solution 3 for Rel-5, Solution 1 as basis for Rel-6. To be verified and elaborated by SA WG3
S3-030566	Proposed CR to 33.203: Reject instead of discard (Rel-5)	Nokia	Joint - 5.3	Approval	S3-030598	Agreed to update the CR to make symmetric for P-CSCF and UE unprotected ports in S3-030598.
S3-030567	Proposed CR to 33.203: SA Management (Rel-5)	Nokia	Joint - 5.2	Approval		Reviewed in evening session. CN1 can continue their work based on clarifications
S3-030568	Proposed CR to 33.203: SA procedures (Rel-5)	Nokia	Joint - 5.2	Approval	S3-030594	Updated in S3-030594
S3-030569	Proposed CR to 33.203: SA parameters and management. (Rel-5)	Nokia	Joint - 5.2	Approval	S3-030596	Updated in S3-030596
S3-030570	Security issues	Nokia	Joint - 5.2	Discussion		It was discussed and agreed tat the content of "Security Server" shall be mirrored in the "Security Verify header". CN WG1 were asked to take this into account in their work.
S3-030571	High Level Requirements for UICC re-use by peripheral Devices on Local Interfaces	3	7.15	Discussion / Decision		agreements to be edited into draft FS
S3-030572	Adding domain component support to NDS/AF certificate profiles	Nokia, Siemens, SSH, T-Mobile	7.4	Discussion / Decision		Agreed to add this proposal.
S3-030573	Pseudo Cr to 33.310: Adding domain component support to NDS/AF certificate profiles	Nokia, Siemens, SSH, T-Mobile	7.4	Approval		Approved
S3-030574	Pseudo CR to 33.310: Clarifications to usage of certificate repositories	Nokia, Siemens, SSH, T-Mobile, Vodafone	7.4	Approval		Approved
S3-030575	Analysis of proposed network based access control solution for multiple PDP contexts	Nokia	7.5	Discussion / Decision		Terminal-based solution proposed. Network-based proposed in S3-030587. To be further discussed.
S3-030576	Comparison of different solutions for GBA and AP based AS: standard TLS versus shared secret based TLS	Alcatel	7.9	Discussion		Mainly in line with S3-030555.
S3-030577	WITHDRAWN - Proposed CR to 33.203: Clarifying formulation and notation related to protected port numbers (Rel-6)	Alcatel	7.1	Approval		WITHDRAWN
S3-030578	P-CR for Presence TR 33.abc v0.6.0	Nokia	7.18	Discussion / Approval		Clause 6.2 with modifications accepted for insertion in the new TS

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030579	Proposed LS (to SA WG1): The requirement and feasibility of IMS watcher authentication	Nokia	4	Approval	S3-030654	Reviewed for CN1 experts to comment. Revised in S3-030654
S3-030580	MBMS – Overhead of the Re-keying	Nokia	7.20	Discussion		Noted. Companies to consider their preferences for methods for decision at next meeting
S3-030581	GUP security directions	Nokia	7.17	Discussion		Nokia to get more info on Liberty Alliance. B Owen to send LS to groups about open issues
S3-030582	Pseudo-CR to 33.246: MBMS broadcast security requirements clarification	Nokia	7.20	Approval	S3-030640	revised in S3-030640
S3-030583	Key distribution protocol selection	Siemens	7.20	Discussion / Decision		Noted
S3-030584	Evaluation of secure algorithm negotiation proposals	Siemens	7.6	Discussion / Decision		Taken with S3-030542 and S3-030588. Special-RAND adopted for development. LS in S3-030629
S3-030585	Effects of service 27/38 on 2G/3G Interworking and emergency call	Siemens	7.5	Discussion / Decision		Used as basis for LS to GSMA SG / SCAG in S3-030624
S3-030586	MBMS Key distribution	Siemens	7.20	Discussion		Working Assumption adopted
S3-030587	Multiple PDP context security issue	Ericsson, Vodafone	7.5	Discussion / Decision		Network-based solution proposed. Terminal-based proposed in S3-030575. To be further discussed.
S3-030588	Further development of the Special RAND mechanism	Orange, Vodafone	7.6	Discussion / Decision	S3-030651	Taken with S3-030542 and S3-030584. Special-RAND adopted for development. Revised in S3-030651
S3-030589	Pseudo CR to 33.310: Clarification on the use of PSK as a fallback mechanism	Nokia, Siemens, SSH, Vodafone	7.4	Approval		Approved
S3-030590	Pseudo CR to 33.310: Correction of typos	Nokia, Siemens, SSH, Vodafone	7.4	Approval		Approved
S3-030591	Documents approved by e-mail after SA WG3 meeting #29	SA WG3 Secretary	5.1	Information	S3-030592	WITHDRAWN due to missing entry in cover table
S3-030592	Documents approved by e-mail after SA WG3 meeting #29	SA WG3 Secretary	5.1	Information		Noted
S3-030593	IMS R5 profile of RFC 3329	Ericsson	Joint - 5.5	Information		Noted
S3-030594	Proposed CR to 33.203: SA procedures (Rel-5)	Nokia	7.1	Approval	S3-030609	Revised in S3-030609
S3-030595	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	7.15	Information		Editor to update with agreed comments from discussion and distribute on e-mail list
S3-030596	Proposed CR to 33.203: SA parameters and management. (Rel-5)	Nokia	7.1	Approval	S3-030610	Revised in S3-030610
S3-030597	Proposed CR to 33.203: Terminology alignment (Rel-5)	Nokia	7.1	Approval	S3-030613	Revised in S3-030613
S3-030598	Proposed CR to 33.203: Reject instead of discard (Rel-6)	Nokia	7.1	Approval	S3-030615	Revised in S3-030615
S3-030599	LS to CN 4, CN1 on IMS AKA: UE populating RAND and AUTN parameters in responding to challenge	SA WG3	7.1	Approval	S3-030616	Revised in S3-030616
S3-030600	Proposed CR to 33.203: Introducing the SIP Privacy mechanism in Stage 2 specifications (Rel-5)	Ericsson	7.1	Approval	S3-030617	Revised in S3-030617

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030601	Proposed CRs to 33.203: Correcting the text on sending an authentication response (Rel-5)	3	7.1	Approval		Approved
S3-030602	Proposed CRs to 33.203: Correcting the text on sending an authentication response (Rel-6)	3	7.1	Approval		Approved
S3-030603	Proposed CRs to 33.203: Correcting the SA handling procedures (Rel-5)	Joint CN1 meeting (A Escott)	7.1	Approval	S3-030619	Revised editorially in S3-030619
S3-030604	Proposed CRs to 33.203: Correcting the SA handling procedures (Rel-6)	Joint CN1 meeting (A Escott)	7.1	Approval	S3-030620	Revised editorially in S3-030620
S3-030605	Draft Report of SA WG3 LI meeting in Jackson Hole	SA WG3 LI Group	5.4	Information		Noted
S3-030606	Proposed CR to 33.108: LI Reporting of Dialed Digits (Rel-6)	SA WG3 LI Group	5.4	Approval		Approved
S3-030607	Proposed CR to 33.107: MSISDN/IMEI clarification for GPRS interception (Rel-6)	SA WG3 LI Group	5.4	Approval		Approved
S3-030608	Proposed CR to 33.108: Correction to Annex G on TCP based transport (Rel-6)	SA WG3 LI Group	5.4	Approval		Approved
S3-030609	Proposed CR to 33.203: SA procedures (Rel-5)	Nokia	7.1	Approval		Approved
S3-030610	Proposed CR to 33.203: SA parameters and management. (Rel-5)	Nokia	7.1	Approval		Approved
S3-030611	Proposed CR to 33.203: SA procedures (Rel-6)	Nokia	7.1	Approval		Approved
S3-030612	Proposed CR to 33.203: SA parameters and management. (Rel-6)	Nokia	7.1	Approval		Approved
S3-030613	Proposed CR to 33.203: Terminology alignment (Rel-5)	Nokia	7.1	Approval		Approved
S3-030614	Proposed CR to 33.203: Reject instead of discard (Rel-5)	Nokia	7.1	Approval		Approved
S3-030615	Proposed CR to 33.203: Reject instead of discard (Rel-6)	Nokia	7.1	Approval		Approved
S3-030616	LS to CN 4, CN1 on IMS AKA: UE populating RAND and AUTN parameters in responding to challenge	SA WG3	7.1	Approval		Approved
S3-030617	Proposed CR to 33.203: Introducing the SIP Privacy mechanism in Stage 2 specifications (Rel-5)	Ericsson	7.1	Approval	S3-030648	Revised in S3-030648
S3-030618	LS to SA WG2: Introducing the Privacy Mechanism in Stage 2	Ericsson	7.1	Approval	S3-030649	Revised in S3-030649
S3-030619	Proposed CRs to 33.203: Correcting the SA handling procedures (Rel-5)	Joint CN1 meeting (A Escott)	7.1	Approval		Approved
S3-030620	Proposed CRs to 33.203: Correcting the SA handling procedures (Rel-6)	Joint CN1 meeting (A Escott)	7.1	Approval		Approved
S3-030621	Reply LS on cipher suite for DRM-protected streamed media for PSS	SA WG3	6.1	Approval	S3-030650	Revised in S3-030650
S3-030622	First draft of MMS Security Paper - version 0.1.1	A Bergmann, MMS TF	10	Information		Presented and noted
S3-030623	WITHDRAWN - Invitation to SA WG3 meeting #31, Munich, Germany	EF3	9	Information		WITHDRAWN - Cut-off date wrong for hotel booking
S3-030624	LS to GSMA SG, SCAG on 2G/3G interworking Emergency Call Scenarios	SA WG3	7.5	Approval		Approved
S3-030625	Proposed CR to 33.102: Handling of key sets at inter-system change (Rel-5)	Ericsson	7.5	Approval		Approved
S3-030626	Proposed CR to 33.102: Handling of key sets at inter-system change (Rel-6)	Ericsson	7.5	Approval		Approved
S3-030627	Reply LS (from SA WG2) on "Security issues regarding multiple PDP contexts in GPRS"	SA WG2	7.5	Action		Noted. Threat analysis in S3-030575
S3-030628	Invitation to SA WG3 meeting #31, Munich, Germany	EF3	9	Information		Noted
S3-030629	LS on Special-RAND mechanism	SA WG3	7.5	Approval	S3-030652	Revised in S3-030652
S3-030630	Results of Wed evening session for 33.109 split	Discussion Group	7.9	Information		Noted. Evening session to draft 4 proposed TSs/TRs
S3-030631	Pseudo-CR: Protocol between authentication proxy and application server	Ericsson	7.9	Approval		Revised in S3-030632
S3-030632	Pseudo-CR: Protocol between authentication proxy and application server	Ericsson	7.9	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030633	GSM Association and EICTA joint statement: IMEI Integrity on the theft of mobile phones	GSMA, EICTA	6.4	Information		Noted
S3-030634	Reply LS on "Security issues regarding multiple PDP contexts in GPRS"	Discussion Group	7.9	Approval		Approved
S3-030635	LS Response on “new interface names”	SA WG3	7.9	Approval		Approved
S3-030636	LS to CN WG, CN WG4 - Interface requirements	SA WG3	7.9	Approval	S3-030653	revised in S3-030653
S3-030637	MMS Charging Principles Handbook	Fred Hillebrand (Ansgar Bergmann)	10	Information		Presented and Noted
S3-030638	Pseudo-CR to 33.234: Re-authentication procedures	Ericsson	7.10	Approval		Approved
S3-030639	LS to T3 and SA1 on Group Voice Call requirements	~~E-mail approval 23 October~~SA WG3	7.21	E-mail Approval		E-mail approved~~al by 23~~ 21 October
S3-030640	Pseudo-CR to 33.246: MBMS broadcast security requirements clarification	Nokia	7.20	Approval		Approved
S3-030641	Proposed Pseudo-CR to TS 33.246 MBMS Security Requirements CR (non controversial) - (Rel-6)	BT Group	7.20	Approval		Approved
S3-030642	Report on GAA evening session, October 9, 2003	GAA discussion group	7.9	Information		Noted
S3-030643	Draft TS: Generic Authentication Architecture; System Description (Release 6)	GAA discussion group	7.9	Information		Noted
S3-030644	Draft TS: Generic Authentication Architecture; Generic Bootstrapping Architecture (Release 6)	GAA discussion group	7.9	Information		Noted
S3-030645	Draft TS: Generic Authentication Architecture; Support for Subscriber Certificates (Release 6)	GAA discussion group	7.9	Information		Noted
S3-030646	Draft TS: Generic Authentication Architecture; Access to Network Application Function using HTTPS (Release 6)	GAA discussion group	7.9	Information		Noted
S3-030647	Draft TS 33.cde V0.1.1 Presence Service; Security	Rapporteur	7.18	Information		Noted
S3-030648	Proposed CR to 33.203: Introducing the SIP Privacy mechanism in Stage 2 specifications (Rel-5)	Ericsson	7.1	Approval		Approved
S3-030649	LS to SA WG2: Introducing the Privacy Mechanism in Stage 2	SA WG3	7.1	Approval		Approved
S3-030650	Reply LS on cipher suite for DRM-protected streamed media for PSS	SA WG3	6.1	Approval		Approved
S3-030651	Further development of the Special RAND mechanism	Orange, Vodafone	7.6	Discussion / Decision		attach to LS in S3-030652
S3-030652	LS on Special-RAND mechanism	SA WG3	7.5	Approval		Approved
S3-030653	LS to CN WG, CN WG4 - Interface requirements	SA WG3	7.9	Approval		Approved
S3-030654	LS on the requirement and feasibility of IMS watcher authentication	SA WG3	4	Approval		Approved

Annex C: Status of specifications under SA WG3 responsibility

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

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

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
TS	35.206	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TS	35.207	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	4.0.1	Rel-4	S3	WRIGHT, Tim	
TR	41.033	Lawful Interception requirements for GSM	4.0.1	Rel-4	S3	MCKIBBEN, Bernie	
TS	41.061	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	4.0.0	Rel-4	S3	WALKER, Michael	
TS	42.009	Security Aspects	4.0.0	Rel-4	S3	CHRISTOFFERSSON, Per	
TS	42.033	Lawful Interception; Stage 1	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
TS	43.020	Security-related network functions	4.0.0	Rel-4	S3	GILBERT, Henri	
TS	43.033	Lawful Interception; Stage 2	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
Release 5 3GPP Specifications and Reports							
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	5.0.0	Rel-5	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards).
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031.
TS	23.035	Immediate Service Termination (IST); Stage 2	5.1.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards).
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	

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

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
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	
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
33.102	183	-	Rel-5	Handling of key sets at inter-system change	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	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	F	5.7.0	S3-30	S3-030601	IMS-ASEC
33.203	048	-	Rel-6	Correcting the text on sending an authentication response	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	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
S3-030484	LS Response (from SA WG2) on new interface names	S2-033235	Request to use Z interface names noted
S3-030485	LS reply on Rel-5 transport of unknown SIP signalling elements	S5-034447	Noted
S3-030486	Letter to SA WG3 Chairman: PN-4465-RV1 (to be published as J-STD-025-B)	<none>	Noted. LI Group asked to look at this LS
S3-030490	LS (from GSMA-SG) on introduction of A5/3 in GSM handsets	SG Doc XX_03	Taken into account in discussions
S3-030491	LS (from SA WG3 LI Group) on new acronym	S3LI03_084	ANP acronym agreed
S3-030497	Liaison statement (from CN WG1) on Profiling of RFC3325 for IMS	N1-031199	Dealt with in joint session. No response LS needed
S3-030498	Reply LS (from CN WG1) on stage 3 level specification directions for support for subscriber certificate work item	N1-031200	Protocol A OK, Protocol B for analysis.
S3-030499	Reply to LS (from CN WG1 - N1-031052) on 'Effects of service 27/38 on 2G/3G Interworking and emergency call' from SA3	N1-031201	Discussed with S3-030510 and S3-030585. LS in S3-030624
S3-030500	Liaison statement (from CN WG1) on requesting a joint CN1-SA3 meeting	N1-031330	Noted
S3-030501	LS (from CN WG2) on SA3 on Legal Interception of SCP initiated calls	N2-030437	Noted. LI Group to deal with this LS.
S3-030502	LS Response (from CN WG4) on Stage 3 level specification directions for support for subscriber certificate work item	N4-031061	Response LS in S3-030635
S3-030503	Reply LS (from SA WG1) on clarification of MBMS charging issues	S1-030997	Noted
S3-030504	LS (from SA WG1) regarding progress of work for MBMS User Services	S1-031002	Noted
S3-030505	Liaison (from SA WG4) Response to OMA	S4-030647	Noted
S3-030506	LS (from SA WG4) on cipher suite for DRM-protected streamed media for PSS	S4-030660	Response LS in S3-030621
S3-030507	LS (from SA WG4) on "Update of WID on MBMS"	S4-030670	Noted
S3-030508	LS response (from T WG2) to SA2 on UE Tunnelling	T2-030516	Noted
S3-030509	LS response (from T WG2) on usage of GUP reference points	T2-030518	Noted
S3-030510	LS (from T WG3) on the effects of USIM services 27 and 38	T3-030693	Discussed with S3-030499 and S3-030585. Noted. LS in S3-030624
S3-030511	LS (from T WG3) on potential USIM impact of the MBMS security framework	T3-030697	Noted
S3-030512	Liaison Statement (from SA WG2) on Generic Authentication Architecture	S2-033262	Dealt with in ad-hoc meeting. Noted
S3-030627	Reply LS (from SA WG2) on "Security issues regarding multiple PDP contexts in GPRS"	S2-033240	Noted. Threat analysis in S3-030575
S3-030633	GSM Association and EICTA joint statement: IMEI Integrity on the theft of mobile phones	<None>	Noted

E.2 Liaisons from the meeting

TD number	Title	Comment/Status	TO	CC
S3-030616	LS to CN 4, CN1 on IMS AKA: UE populating RAND and AUTN parameters in responding to challenge	Approved	**CN WG1, CN WG4**	--
S3-030624	LS to GSMA SG, SCAG on 2G/3G interworking Emergency Call Scenarios	Approved. Attached S3-030585	**GSMA SG**	**T WG3**
S3-030634	Reply LS on "Security issues regarding multiple PDP contexts in GPRS"	Approved	**SA WG2, CN WG4**	--
S3-030635	LS Response on "new interface names"	Approved	**SA WG2, CN WG1, CN WG4**	**SA WG5**
S3-030639	LS to T3 and SA1 on Group Voice Call requirements	**For e-mail discussion and approval by 23 October**. Attached S3-030559	**T WG3, SA WG1**	**ETSI EP RT**

TD number	Title	Comment/Status	TO	CC
S3-030649	LS to SA WG2: Introducing the Privacy Mechanism in Stage 2	Approved Attached S3-030648	SA WG2	CN WG1
S3-030650	Reply LS on cipher suite for DRM-protected streamed media for PSS	Approved	OMA-SEC, OMA-DRM+DL, 3GPP SA WG4	--
S3-030652	LS on Special-RAND mechanism	Approved Attached S3-030651	CN WG1, CN WG4, GERAN WG2	T WG2
S3-030653	LS to CN WG, CN WG4 - Interface requirements	Approved	CN WG1, CN WG4	--
S3-030654	LS on the requirement and feasibility of IMS watcher authentication	Approved	SA WG1, SA WG2, CN WG1	--

Annex F: Actions from the meeting

AP 30/01: Eric Gauthier (Orange, Switzerland) to lead an e-mail discussion on GPRS over-billing.

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.

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.

AP 30/034: B. Wilhelm to ask LI group to investigate the LI impacts of the tunnelling solution for WLAN interworking.

AP 30/045: B Owen to respond to LSs on GUP from meeting #29, informing the senders that there are still open issues in SA WG3.

AP 30/056: 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.

AP 30/067: Rapporteurs of SA WG3 Work Items to provide the SA WG3 Secretary with updates to the Work Plan by 24 October 2003.