3GPP TSG SA WG3 Security — S3#34 **S3-040451**
06 - 09 July 2004
Alcapulco, Mexico

3GPP TSG SA WG3 (Security) meeting #33 **DRAFT REPORT**
10-14 May 2004 **Version 0.0.6rm**
Beijing, China

Source:	**Secretary of SA WG3**
Title:	**Draft report of SA3#33 - version 0.0.6 (with revision marks)**
Status:	**Draft for Comment**

The Forbidden Palace Courtyard, Beijing, China

Contents

1 Opening of the meeting

The Chairman, Mr. V. Niemi opened the meeting. The Hosts, **Samsung**, welcomed delegates to Beijing, China and provided the domestic arrangements which had been made and wished SA WG3 a constructive and successful meeting.

2 Agreement of the agenda and meeting objectives

The draft agenda was provided in TD S3-040202 which was reviewed and approved. The SA WG3 Chairman provided the objectives for the meeting and the preliminary schedule as follows:

Meeting objectives:

- The major objective of the meeting is to develop the still pending TSs and TRs into a state where they can be submitted to SA#24 for approval (33.141, 33.222, 33.246, 33.919).
- Another important objective is to agree on necessary CRs against those release 6 TSs and TRs that were put under change control in SA#23 (33.220, 33.221, 33.234, 33.310, 33.817).

Preliminary schedule of the meeting:

- Progress of MBMS security by using the early deadline and email discussions prior to this Beijing meeting had been tried. However, no clear conclusions had been reached. Therefore the Chairman proposed that MBMS is handled as the first technical item. As some of the GBA contributions are closely linked to MBMS they should also be handled under the same agenda item. It was noted, however, that the majority of the MBMS contributions had been available for a whole month before the meeting, therefore the meeting should manage with fairly brief oral presentations.
- The planned milestones for each day of the meeting were as follows:
  - Monday: completion of items 1-5 and presentation of most contributions under 6.20 (MBMS);
  - Tuesday: completion of 6.20 (continue later in break-out session if needed) and also complete 6.1-6.4, preferably also 6.5-6.6;
  - Wednesday: completion of 6.5 – 6.9 and also 6.18 (Presence);
  - Thursday: completion of rest of items 6.10-6.23;
  - Friday: handling of output documents and agenda items 7-9.
- These milestones were based on the experience from previous two meetings. The schedules have to be adjusted to the number of contributions submitted to each agenda item.
- Additional break-out sessions are probably arranged in some evenings.

It was proposed that GUP Security should be taken first on the Monday afternoon as CN WGs also have a meeting this week and could then deal with any resulting LSs. This was agreed.

2.1 3GPP IPR Declaration

The Chairman made the following call for IPRs:

> The attention of the delegates to the meeting of this Working Group was 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 delegates were asked to take note that they were thereby invited:
>
> - to investigate whether their organization or any other organization owns IPRs which were, or were likely to become Essential in respect of the work of 3GPP.
>
> - to notify their respective Organizational Partners of all potential IPRs, e.g., for ETSI, by means of the IPR Statement and the Licensing declaration forms (http://webapp.etsi.org/Ipr/).

3 Assignment of input documents

The available documents were allocated to their relevant agenda items.

4 Meeting reports

4.1 Approval of the report of SA3#32, Edinburgh, Scotland, UK, 9-13 February, 2004

TD S3-040203 Draft Report of SA WG3 meeting #32 v0.0.8rm. The report was reviewed. A ~~change~~ correction to change MT to GSM/UMTS UE was made to section 6.10 and the Action Point 3 was corrected to read "Integrity" instead of "Encryption". The report was then approved and will be placed on the FTP Server as version 1.0.0.

Review of Actions taken at the meeting:

AP 32/01: *V. Niemi to try to find out (with the help of TSG SA Plenary) whether any further MMS Security work should be carried out and which body such work should be done in.* V. Niemi reported that there are no immediate impacts on the work of SA WG3. **Action Closed**.

AP 32/02: *M. Pope to check the status of Liaison with Bluetooth and any further action needed to allow this.* An informal Bluetooth liaison was formed and SA WG3 LSs forwarded to the Bluetooth contact people. **Action Closed**.
NOTE: A list of authorised Liaison bodies is maintained by MCC at: http://www.3gpp.org/Management/Liaisons.htm

AP 32/03: *C. Brookson, P. Christofferssen to contact SAGE Chairman to see if a reduced funding request would be acceptable for the alternative 3G Ciphering and Integrity Algorithm work*. It was reported that this had been done and a reply had been forwarded to the GSMA for a lower funding request. No decision has yet been made by the GSMA. **Action Closed.**

AP 32/04: A. Palanigounder, M. Blommaert and P. Howard to analyse the Special-RAND proposal in TD S3 040036 and provide contribution to the next SA WG3 meeting. An alternative to Special-RAND had been contributed to this meeting. **Action Closed.**

AP 32/04a: C. Blanchard to check that the interface names used in TS 33.234 (WLAN Interworking) are synchronised with SA WG2 architecture Specification (TS 23.234). This had been done in the draft presented for approval. **Action Closed.**

AP 32/05: J. Abellan Sevilla to collect comments and prepare a response LS. Deadlines for comments: 27 February 2004, LS drafted by 5 March 2004, e-mail approval by 12 March 2004. A response LS will be provided at this meeting. **Action Closed.**

AP 32/06: Editor to update draft TR 33.817 in line with agreements and send to e-mail list by 22 February 2004 for comments by 01 March 2004 and approval for forwarding to M. Pope by 08 March 2004 for input to TSG SA #23 for approval. This was completed for TSG SA Plenary. **Action Closed.**

AP 32/06a: A. Escott to organise an e-mail discussion on MBMS Download security solutions for providing contribution to the next meeting. The e-mail discussion was started, but few comments received. **Action Closed.**

AP 32/07: M. Pope to try to book ETSI for October meeting 5 - 8 October 2004. EF3 kindly offered to organise this meeting in Malta as there were no free meeting rooms in the ETSI Secretariat. **Action Closed.**

4.2 Report from SA#23, Phoenix, USA, 15-18 March, 2004

TD S3-040204 Chairman's Report from TSG SA meeting #23. The Chairman reported the SA WG3-related issues at TSG SA Meeting #23. It was proposed that A5/4 and GEA4 work is moved into Release 7 in order that all related Specifications can handle the 128-bit keys in the same Release. This was agreed as the best way forward by SA WG3. It was noted that a new WID form had not been approved, but was under e-mail review by TSG SA and a new version is expected to be approved at the next TSG SA meeting.

TD S3-040205 Draft report of TSG SA meeting #23, version 0.0.5rm. This was provided for information and was noted.

TD S3-040215 LS Reply (from TSG SA) to Request for close cooperation on future NGN Standardisation. ~~This was introduced by Ericsson and informed SA WG3 (and SA WG4) that DLDRM had received, understood and noted the~~

~~information given in the liaison statements they had received. It further informed SA WG4 that DLDRM understands SA WG4 will define the final specification text for the content and streaming format and signalling of encrypted Rel-6 **PSS** streams and Rel-6 **3GP** files. DLDRM is looking forward to receive knowledge about the final specification text as soon as possible.~~ C. Blanchard reported that he had told the TISPAN group that other TSs (other than IMS Security) needed to be taken into account. He also pointed out that the security is not only dependent on IMS Security. He reported that TISPAN do not intend to make any changes for the fixed-network use unless absolutely necessary and commented that SA WG3 should ensure that they are fully aware of the necessary Security work. SA WG3 members were asked to consider attending and contribution to the planned Workshop (expected June 2003) and to discuss with colleagues in their companies.

4.3 Report from SA3 LI #13, Rome, Italy, 14-16 April, 2004

TD S3-040300 Draft Report of SA WG3 LI Group meeting #13 (Rome, Italy). This was introduced by B. Wilhelm and was noted.

CRs for approval: TD S3-040301, to TD S3-040314: It was agreed that unless enough time is available at the end of this meeting, the CRs would be approved by e-mail after the meeting. **Comments to the SA WG3 LI List by 24 May 2004, Final approval of CRs 31 May 2004.**

5 Reports and Liaisons from other groups

5.1 3GPP working groups

TD S3-040214 LS (from SA WG5) on Security of the Management Plane. This was introduced by Huawei and was related to the LS in TD S3-040250 which was considered.

TD S3-040250 LS response (from SA WG5) to ITU-T SG 4 regarding Security of the Management Plane. This was introduced by Huawei and contained the response that SA WG5 had sent to ITU-T SG4. The LS was noted and delegates were asked to consider the ITU-T document in order to provide any further Security-related comments to SA WG5. It was decided to collect comments off-line and provide an LS to SA WG5 and ITU-T SG4. Yingxin (Huawei) agreed to collect comments over e-mail by ~~24~~ 18 May 2004 and provide a new LS by ~~26~~ 20 May in order to approve and send the LS by ~~31~~24 May. The Liaison was allocated to TD S3-040382. This was approved on Monday 24 May and transmitted.

AP 33/01: Yingxin (Huawei) agreed to collect comments on the ITU-T Security of the Management Plane document over e-mail by 18 May 2004 and provide a new LS by 20 May in order to approve and send the LS by 24 May to the ITU-T electronic meeting 25 May 2004.

TD S3-040369 LS (from T WG2) on Potential Security issues relating to use of AT Commands to access UICC. This was introduced by Axalto and asked SA WG3 to review TS 27.007 and the CR in T2-040228 from a security perspective and to provide feedback over and issues over the remote access aspects. TS 27.007 was provided for delegates to check this and provide comments to Axalto by Thursday 12.00. A response LS was provided in TD S3-040383 which was reviewed and approved.

5.2 IETF

There were no specific contributions under this agenda item.

5.3 ETSI SAGE

There were no specific contributions under this agenda item.

5.4 GSMA

Charles Brookson reported on the work of the GSM Association Security Group. Current work includes:

- A special working group had been looking at the issues of SPAM. Some of the issues arose because of access to SS7, and also to SMSCs. It was noted that MAPSec might be one of the possible potential solutions to the problems.

- An input document had been submitted to SA WG3 on the subject of A5/2. The GSMA had indications that the export of A5/1 was being eased, and this could prove to be one of the ways to minimise recent threats on GSM security.
- Handset security and the IMEI were still a priority, because of stolen mobiles. There are two ways that this is being handled: Firstly, a reporting procedure to fix handsets that had easily changeable IMEIs, and a document explaining technical methods of securing the IMEI. The GSMA was encouraging operators to roll out EIRs and connect to the CEIR, which was also being upgraded.
- Other issues were Bluetooth security issues raised by recent public reports.

The SG Chairman was happy to involve those people in SA WG3 who were not members of GSMA, and who wanted to attend their meetings. This was subject to the GSMA rules, and in the first case interested people should contact him by email. The next meetings are provisionally scheduled as:

- SG 51 21-JUN-2004 22-JUN-2004 Amsterdam, Netherlands
- SG 52 13-SEP-2004 14-SEP-2004 Madrid, Spain
- SG 53 10-NOV-2004 11-NOV-2004 Madrid, Spain

5.5 3GPP2

No special issues in 3GPP2 were reported. It was noted that 3GPP2 had responded to the ITU-T (via TIA TR-45 AHAG) on the Security of the Management Plane document.

5.6 OMA

TD S3-040211 Response (from SA WG2) to LS on “IMS messaging, Group management and Presence work overlap between 3GPP and OMA”. This was introduced by Ericsson and was provided to SA WG3 for information. The LS was noted.

5.7 Other groups

TD S3-040223 LS from ITU-T SG17: Information of new ITU-T Recommendations for secure mobile end-to-end data communication, X.1121 and X.1122. This was introduced by the SA WG3 Chairman and informed 3GPP and 3GPP2 of new Recommendations consented at the SG 17 meeting:

- *X.1121 (formerly X.msec-1) describes the framework of security technologies for mobile end-to-end data communication. It contains descriptions of security threats, security requirements and security functions.*
- *X.1122 (formerly X.msec-2) is a guideline for implementing secure mobile systems based on PKI and describes models of secure mobile systems, usage models and considerations for secure mobile systems based on PKI.*

It was noted that they do not reference the 3GPP specifications, in particular the Lawful Interception specifications and it was suggested that these should be sent to them. in a response LS which was provided in TD S3-040384 which was reviewed and approved.

6 Work areas

6.1 IP multimedia subsystem (IMS)

TD S3-040374 LS (from SA WG2) on non-compliance to IMS security. This was introduced by Vodafone. SA WG2 asked SA WG3 to consider and, if necessary, provide feedback on possible security mechanisms that take into account early implementations of IMS that do not fully support TS 33.203. Any mechanism should be such that impacts on existing entities, especially on the UE, are minimised and would be quick to implement. TD S3-040264 and TD S3-040265 addressed this issue and were considered.

TD S3-040264 Security for early IMS implementations. This was introduced by Vodafone and considered security aspects of early IMS implementations and proposed that 3GPP specify interim security features to address security requirements of early IMS implementation. A proposal for this was provided in TD S3-040265. This was noted and the proposal in TD S3-040265 considered.

TD S3-040265 Interim security solution for early IMS implementations. This was introduced by Vodafone and, in response to the LS from SA WG2 in TD S3-040374, proposed an interim security solution to be standardised by SA WG3 that minimizes the impact on IMS terminals, and requires only a limited set of changes to the IMS core. The solution avoids key/password distribution issues during provisioning, and does not restrict the type of charging models that can be applied by the IMS operators. A concern for the compatibility with the 3GPP2 IMS security architecture with this interim solution was reported and this concern was noted. **It was acknowledged that a solution to this problem is needed for early IMS implementations and SA WG3 regret that the recommended solution had not been deployed in the market. SA WG3 will study this further before the next meeting and make a decision at that meeting based upon contributions. The proposed solution provided in section 3 was taken by SA WG3 as a working assumption and delegates were asked to study it and provide contribution to the next SA WG3 meeting to help in making a final SA WG3 decision.** A response LS to SA WG2 was provided in TD S3-040396 which was approved.

TD S3-040318 Proposed CR to 33.203: Correction on IMS confidentiality protection (Rel-6). This was introduced by Siemens and was discussed and clarified in TD S3-040397 which was approved.

TD S3-040357 Privacy handling for Rel-6. This was introduced by Nokia and introduces the requirements for Privacy handling for Rel-6 IMS confidentiality protection. A companion CR was provided in TD S3-040358.

TD S3-040358 Proposed CR to 33.203: SIP Privacy mechanism when IMS interworking with non-IMS network (Rel-6). It was agreed that Note 2 of section 6.5 is still relevant and should not be deleted. It was clarified that a list of trusted networks would be kept, only to which Privacy information may be forwarded. Nokia clarified that they would like to use TLS between 3GPP IMS networks too and the CR would need further work to include this. The CR was revised in TD S3-040398 and was revised in TD S3-040429 and approved. It was noted that a CR to 33.210 may also be needed as a consequence of this CR.

AP 33/02: T Haukka to start an e-mail discussion on TD S3-040357. Comments to be provided by 11 June 2004 for reporting the result of the discussions to the next meeting.

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

There were no specific contributions under this agenda item.

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

TD S3-040291 Proposed CR to 33.210: Diffie-Hellman groups in NDS/IP (Rel-6). This was introduced by Nokia and was approved. It was not considered necessary to consult ETSI SAGE on this profiling of IKE for NDS/IP.

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

Tiina Koskinen (Nokia) agreed to take over the Rapporteurship for this work after the departure of ~~K. Boman~~ T. Viitanen from SA WG3.

TD S3-040266 Proposed CR to 33.310: Removal of inconsistencies regarding SEG actions during IKE phase 1 (Rel-6). This was introduced by Vodafone and was approved.

TD S3-040267 Proposed CR to 33.310: Removal of unnecessary restriction on CA path length (Rel-6) . This was introduced by Vodafone and was approved.

TD S3-040296 Proposed CR to 33.310: Correction of 'Extended key usage' extension in SEG Certificate profile (Rel-6). This was introduced by Nokia on behalf of Nokia and Vodafone and was approved.

It was reported that the ITU-T have a meeting 25 May to discuss their Management Plane security.

6.5 UTRAN network access security

TD S3-040207 LS (from CN WG1) on Re-authentication and key set change during inter-system handover. This was introduced by Siemens. CN WG1 asked SA WG3 to confirm the following:

- TS 33.102, v 5.3.0, subclause 6.8.5, Intersystem handover for CS Services – from GSM BSS to UTRAN. CN WG1's understanding of the specification that the RNC will initiate the integrity protection of signalling messages without receiving an explicit RANAP Security Mode Command procedure from the MSC.

Furthermore it is CN WG1's understanding of the RANAP specification TS 25.413 that during the inter-system handover the MSC can provide only one key set to the RNC with the RANAP Relocation Request message, and that this is the old key set.

CRs to 33.102 for Rel-5 and Rel-6 to align the specifications had been provided by Siemens and Ericsson in TD S3-040273 and TD S3-040274.

Need to check if RNC has all information needed for Security Mode Control handling The understanding of CN WG1 was confirmed and a reply LS to CN WG1 was provided in TD S3-040399 which was revised to remove "DRAFT" in TD S3-040436 and approved.

TD S3-040273 Proposed CR to 33.102: Handling of key sets at inter-system change (Rel-5). This proposal was checked off line and approved.

TD S3-040274 Proposed CR to 33.102: Handling of key sets at inter-system change (Rel-6). This proposal was checked off line approved.

TD S3-040208 Reply LS (from CN WG4) to S3-040187(N4-040240) on use of authentication re-attempt IE. This was introduced by NEC. CN WG4 asked SA WG3 to update TS 33.102 (Rel-6) with the information described in section 1 in the LS (conditions that the serving network sets the Re-attempt to “true” if the second authentication failed). A corresponding CR was provided by NEC in TD S3-040251.

TD S3-040251 Proposed CR to 33.102: Clarification on Authentication re-attempt parameter (Rel-6). This was introduced by NEC. It was decided to remove the references to the CN specifications in the text and the CR was revised in TD S3-040400 and approved.

A response LS was sent to CN WG4 to confirm this in TD S3-040401 which was reviewed and updated editorially in TD S3-040430 which was approved.

TD S3-040297 Proposed CR to 33.105: Correction of inconsistencies in AK computation for re-synchronisation (Rel-4). This was introduced by Orange. It was noted that this was a Rel-4 CR because there is no Rel-5 and Rel-6 version of this specification. It was agreed that there was no reason why this could not be included in Rel-5 and Rel-6 as new Algorithms may be created in Releases. The SA WG3 Chairman will explain this to SA Plenary and ask for the upgrade of the TSs to Rel-5 and Rel-6 after approval of this Rel-4 CR. The CR was revised to show the changes more clearly (with change bars) in TD S3-040402 which was approved.

6.6 GERAN network access security

TD S3-040376 A5/2 withdrawal from handsets. This was introduced by C. Brookson on behalf of the GSMA Security Group and proposed the withdrawal of A5/2 from handsets to reduce the threat of easily deriving the key Kc, and using this knowledge to exploit GSM. As a result, the specifications would need to be changed to remove mandatory support of A5/2 :(TS 22.221 and TS 42.007 were identified). An LS to inform groups of the removal of support for A5/2 was provided in TD S3-040403 which was reviewed and updated in TD S3-040431 which was approved. It was noted that GSM TS 02.07 does not exist in recent Releases and had not been transferred into the 3GPP Specification set.

The contributions on A5/2 protection mechanisms were presented and discussed:

TD S3-040389 Another Countermeasure for the Barkan-Biham-Keller Attack on A5/2. This was presented by Vodafone on behalf of SFR and described a countermeasure which could be taken to protect against the theoretical A5/2 attack. The proposal was discussed and the presentation was noted. The countermeasure will be considered along with other proposed mechanisms.

TD S3-040262 Analysis of the authenticated GSM cipher command mechanism. This was introduced by Vodafone. At SA WG3 Meeting #32 it was decided that the mechanism of adding a Message Authentication Code (MAC) to the Cipher Mode Command sent by the BSS to the MS should be analysed. This contribution constituted the analysis performed by Vodafone. As well as analysing the basic mechanism described in TD S3-040036 some variants and extensions were also studied. The following conclusions were drawn regarding the suitability of mechanism described in TD S3-040036:

- The possibility to adapt the mechanism so that it can be implemented without any impact on the BSS was considered, **but found not to be feasible**.

- The basic mechanism has the disadvantage that SRES is used in the calculation of the MAC to protect against codebook attacks. This disadvantage can be overcome by including a "salt" in the Cipher Mode Command and using this as an input to the calculation instead of SRES.

TD S3-040360 Eavesdropping without breaking the GSM encryption algorithm. This was introduced by Lucent Technologies and was presented using a set of slides describing a MITM attack on A5. The presentation was noted.

TD S3-040341 Comparison of Suggested A5/2 Attack Countermeasures. This was introduced by Ericsson and compared the proposed countermeasures to the A5/2 attack scenario. It concludes that regardless of the chosen solution, A5/2 should be disabled in the long term.

TD S3-040377 Reaction to S3-040371: Comments to S3-040263 Evaluations of mechanisms to protect against Barkan-Biham-Keller attack. This was introduced by Vodafone and compared the proposed countermeasures to the A5/2 attack scenario. It also included comments and responses provided in TD S3-040263 and TD S3-040371 It concludes that the authenticated ciphering instruction mechanism should be adopted in preference to the special RAND mechanism as a medium/long-term solution to mitigate the Barkan-Biham-Keller attacks. Vodafone believed that A5/2 removal/replacement and the application of timing analysis techniques to detect/prevent dynamic cloning in the short term mean that more time is available to standardise, implement and deploy a more comprehensive medium/long-term solution.

TD S3-040298 Proposed CR to 43.020: Introducing the special RAND mechanism as a principle for GSM/GPRS (Rel-5). This was introduced by Orange and provided changes from the previous version to section C.4 as discussed over e-mail.

TD S3-040299 Proposed CR to 33.102: Introducing the special RAND mechanism as a principle for GSM/GPRS (Rel-6). This was introduced by Orange and provided changes from the previous version as discussed over e-mail.

TD S3-040288 Proposed CR to 43.020: Introducing the special RAND mechanism with GSM/GPRS and WLAN separation (Rel-6) . This was introduced by Nokia and provided changes from the previous version as discussed over e-mail.

General discussion and conclusions:

There was general support to the proposal from the GSM SG Chairman to the removal of A5/2 in the medium/long-term. This was therefore agreed to be presented to TSG SA for their endorsement and the other solutions to further protect against potential A5/x algorithm attacks should be discussed further over e-mail and contributions brought to the next meeting for a selection of the mechanism. There was also general support that A5/0, A5/1 and A5/3 should be made mandatory in Rel-6. The proposals at this meeting should be used as a basis for e-mail discussions.

AP 33/03: SA WG3 Chairman to report to TSG SA the proposal to remove the use of A5/2.

AP 33/04: C. Brookson to run an e-mail discussion on protection mechanisms against the fraud potential implied by the A5/2 weaknesses (and potential future attacks against other A5/x algorithms) and report conclusions to next SA WG3 meeting.

6.7 Immediate service termination (IST)

There were no specific contributions under this agenda item.

6.8 Fraud information gathering system (FIGS)

There were no specific contributions under this agenda item.

6.9 GAA and support for subscriber certificates

6.9.1 TR 33.919 GAA

TD S3-040289 Draft TR 33.919 V1.2.1: Generic Authentication Architecture (GAA); System Description (Rel-6). This was introduced by the Rapporteur. The draft contained editorial changes from version 1.2.0. Clause 7 was still

fairly empty and it was asked whether this should be removed or enhanced. C. Blanchard considered this clause important and agreed to ~~trry~~ try to provide contribution on this at the next SA WG3 meeting. The Rapporteur reported that the draft TR was now stable and may only change as a result of changes to the other drafts that it relies upon. It was agreed to present this to TSG SA for information in June 2004 and finalise for approval at the next SA WG3 meeting, and subsequently to the September TSG SA meeting for approval.

AP 33/05: C. Blanchard to provide contribution to clause 7 of TR 33.919 at next SA WG3 meeting.

6.9.2 TS 33.220 GBA

TD S3-040210 LS (from CN WG4) on Requirements for transfer of GAA-User-Profile. This was introduced by CN WG4. This was introduced by ~~-~~Nortel Networks. CN WG4 asked SA WG3 to provide the reasoning for the inclusion of GAA-User-Profile in GAA Messages. A proposed response LS was provided by Nokia in TD S3-040326 which was reviewed. It was necessary to verify the impact of other proposed CRs and to update the LS in line with the decisions made. The LS will be updated at the next meeting and an e-mail discussion was encouraged to get an agreeable version before the meeting.

TD S3-040373 Reply (from SA WG2) to Liaison on Service Discovery of BSF and PKI portal. This was introduced by Nortel Networks. SA WG2 reviewed the address discovery mechanisms for the PKI portal and Generic Bootstrapping Function within TS 33.221 and TS 33.220 respectively and asked SA WG3 to take account of SA WG2 comments in SA WG3 specifications. It was considered necessary to further discuss the issues raised by SA WG2 and it was agreed to do this over e-mail for decision at the next meeting.

AP 33/06: Operators to consider the default domain name suggestion by SA WG2 in TD S3-040373 and contribute to the next meeting.

TD S3-040290 Proposed CR to 33.220: Editorial corrections to TS 33.220 (Rel-6). This was introduced by Alcatel and introduced editorial changes to the TS. There was overlap with some of the editorial proposals in TD S3-040329 and it was agreed to align both sets of agreed changes into revised CRs. TD S3-040290 was updated and provided in TD S3-040414 which was approved.

TD S3-040329 Proposed CR to 33.220: Editorial changes and clarifications to TS 33.220 (Rel-6). This was introduced by Siemens and introduced editorial changes to the TS. The proposals were discussed and some modifications suggested. There was overlap with some of the editorial proposals in TD S3-040290 and it was agreed to align both sets of agreed changes into revised CRs. TD S3-040329 was updated and provided in TD S3-040406 which was reviewed and revised in TD S3-040433 which was approved.

TD S3-040333 Proposed CR to 33.220: Removal of Annex A (Rel-6). This was introduced by Siemens and proposed the removal of informative Annex A as it duplicates information in TS 33.222 and 33.141. This CR was approved.

TD S3-040330 Proposed CR to 33.220: Removal of editors notes on Transaction Identifiers (Rel-6). This was introduced by Siemens. The wording of the note was discussed off-line and a revised version provided in TD S3-040410 which was approved.

TD S3-040342 Authenticated GBA transaction identifier. This was introduced by Ericsson and proposed an enhancement to transaction identifier in order to further secure GBA infrastructure also in roaming scenarios. Ericsson also proposed that the transaction identifier is generated in the UE and BSF independently in order to save resources in the Ub interface. CRs implement these changes to 33.220 were attached. Siemens commented that the Problem Statement appeared flawed, as the BSF authentication of the NAF should be secured under the requirements of the Zb interface where mutual authentication is specified. The problem statement therefore needed further analysis.

- CR "Authenticated GBA transaction identifier": This was not discussed as the Problem Statement required further analysis.

- CR "Generation of GBA transaction identifier": Siemens commented that the BSF server name has not been standardised yet and it is important that both ends agree on the name. This was a subject of an e-mail discussion and if this is agreed and specified, then this would no longer be a problem in this specification. This CR was therefore left until finalisation of the e-mail discussions.

TD S3-040327 Proposed CR to 33.220: Terminology changes (Rel-6). This was introduced by Siemens on behalf of Nokia and Siemens. Nortel Networks objected to the proposal and it was agreed to have an e-mail discussion allow time to provide **alternative proposals to be sent to the e-mail list by June 7 2004**. This issue will be finalised at the next SA WG3 meeting.

TD S3-040331 Proposed CR to 33.220: Clarification of GBA specific profiles in HSS and over Zh and Zn reference points (Rel-6). This was introduced by Siemens. This was dependent upon agreements for the CR in TD S3-040327 so it was agreed to have an e-mail discussion allow time to provide **alternative proposals to be sent to the e-mail list by June 7 2004**. This issue will be finalised at the next SA WG3 meeting.

TD S3-040335 Proposed CR to 33.220: NAF's public hostname verification (Rel-6). This was introduced by Nokia and identified a need where the public identity of NAF is explicitly sent over Zn interface to the BSF in order for the BSF to be able to derive the NAF specific key material Ks_NAF and asked SA WG3 to approve a CR to TS 33.220 implementing the corresponding changes. An alternative proposal was provided by Siemens in TD S3-040332 which was also considered. This was discussed off-line with TD S3-040332 and resulted in the combined CR in TD S3-040411 which was reviewed and revised in TD S3-040435 which was approved.

~~TD S3-040332 Proposed CR to 33.220: Multiple key derivation mandatory (Rel-6). This was introduced by Siemens. Nokia objected to the 3rd bullet and this was discussed. It was decided to leave this to off-line discussion to come to a mutual understanding of the intended mechanisms. This was discussed off-line with TD S3-040335 and resulted in the combined CR in TD S3-040435 (see above).~~

TD S3-040378 Proposed CR to 33.220: Generic Ua interface requirements. (Received after document deadline) This was introduced by Nokia. Due to previous discussion and agreement, the second bullet and note needed removal from the CR. There was discussion over the other bullets and it was decided to leave this CR to e-mail discussion to be completed by 7 June 2004.

TD S3-040315 NAF remove the security associations. This was introduced by Huawei and discussed different remove/update methods and suggested that the NAF remove the security association, with some deletion conditions, after the security association is invalid. A CR was attached to implement this proposal which was revised in TD S3-040407 to make the proposal into notes which was approved.

TD S3-040316 Validity condition set by NAF. This was introduced by Huawei and proposed that the NAF can set the local validity condition of TID and key material according the special requirements and that the limited number of times is a preferred method. A CR was attached to implement this proposal. After some discussion it was agreed that the full impact on other interfaces needs to be determined before making such a change and **Huawei were asked to further study and discuss this and to return with an updated proposal if appropriate.**

TD S3-040340 Proposed CR to 33.220: Private identity for GBA procedure (Rel-6). This was introduced by Nokia on behalf of Nokia, Motorola, Gemplus and Alcatel. A related proposal was provided in TD S3-040317 which was also considered. Telecom Italia stated that the statement that separable ISIM is not precluded after Rel-5 did not imply it was separable in Rel-6 and that SA WG1 have not put this as a Rel-6 requirement. Even though the ISIM is independent from the USIM, the USIM is always available with the ISIM in Rel-6. Nokia stated that this CR did not imply a mandatory stand-alone ISIM. Siemens suggested that the essence is to convert the IMSI into IMPI as required by TS 23.003. It was considered that this CR needed further development and improvement to ensure that all the possible cases are covered by the changes. The CR should also be divided into the generation of IMPI from IMSI (which was agreed by SA WG3) and the procedures for handling of the identities (which needs further discussion). **Interested companies were asked to develop this CR for presentation at the next SA WG3 meeting.**

TD S3-040317 User identity transform. This was introduced by Huawei and proposed that the BSF should have ability to derive the IMPI from the IMSI. A CR was attached to implement this proposal. As the derivation function is fairly simple, it was not seen necessary to place the conversion in the BSF, as it could be done on the UE. Due to lack of support this proposal was rejected.

TD S3-040268 LS from ETSI SAGE: SAGE work on key derivation for the Generic Bootstrapping Architecture. This was introduced by TeliaSonera. This was a reply from ETSI SAGE to SA WG3 LS TD S3-040162 to which they replied that they can propose a function if the following questions can be answered (answers from SA WG3 in **underline text**):

- Are we right to interpret NAF_Id as an arbitrary length ASCII-coded text string?

The actual format of NAF_Id needs be checked in companies to determine whether it should be ASCII or Octet String and then verify whether it is case-sensitive or case-insensitive. Peter Howard to collect responses on the e-mail list and report to next meeting in order that SA WG3 can define the coding for the NAF_Id. **SAGE can assume arbitrary-length bit-stream and the coding will be specified by SA WG3**.

- Is it OK to fix the IMSI length as 15 digits, or might it be necessary to support longer IMSIs in future?
  No, as the IMPI format conversion needs to be taken into account. This, again will be an arbitrary-length bit-stream and the coding will be defined by SA WG3.
- Will a representation of IMSI as ASCII-coded characters be convenient, or would some other format be better (e.g. binary coded decimal)?
  Obsolete due to second answer.
- Are you happy with the use of HMAC-SHA-256? (We could use HMAC-SHA1 if only 160 bits of output were required, and HMAC-SHA1 may well be implemented by manufacturers already. SA WG3 may wish to consider how important the requirement is to support outputs greater than 160 bits.)
  SA WG3 require an output of 256 bits (the NAF can then have access to two independent keys of 128 bits each). SAGE should also take into account that this function may be run in the UICC. Another function will be needed to generate a 256-bit key from 128 bits (derivation of Ks from Ks_int and Ks_ext)
- Do you have any other comments on our tentative proposal?
  No, but see response LS for further detail.

A response LS to ETSI SAGE was provided in TD S3-040408 which was revised in TD S3-040448 and approved.

TD S3-040332 , TD S3-040334 and TD S3-040343 were considered together in order to agree on a single CR.

TD S3-040332 Proposed CR to 33.220: Multiple key derivation mandatory (Rel-6). This was introduced by Siemens and proposed to standardise multiple key derivation for keys used over the Ua interface as mandatory, for security reasons and in order to reduce the number of options and flags defined. Nokia objected to the 3rd bullet and this was discussed. It was decided to leave this to off-line discussion to come to a mutual understanding of the intended mechanisms. This was aligned and joined with TD S3-040334 in the revised CR TD S3-040434.

TD S3-040334 Proposed CR to 33.220: Removal of key derivation options (Rel-6). This was introduced by Nokia and proposed to always allow multiple key derivation. This was aligned and joined with TD S3-040332 in the revised CR TD S3-040434.

TD S3-040343 Multiple key derivation in GBA. This was introduced by Ericsson and proposed that multiple key derivation is made optional in the UE side and that the BSF should be able to store multiple Ks for one UE. This was addressed with a note in the revised CR TD S3-040434.

TD S3-040409 Proposed CR to 33.220: Multiple key derivation mandatory (Rel-6). This was reviewed and revised in TD S3-040434 which was approved.

TD S3-040224 GBA: Support of NAFs within the Visited Network. This was introduced by Siemens on behalf of Siemens, Nokia and Ericsson and analysed the possible GBA-solutions to fulfil the MBMS-service requirement, with the aim to select an MBMS independent solution. The contribution concluded that:

1. The authentication vectors used by GBA shall not leave the Home Network i.e. the BSF shall be placed within the HN.
2. IPsec and TLS mechanism can both be used for protecting the GBA-interface Zn.
3. For scalability reasons, NAFs in the visited network shall communicate with the BSF in the Home Network through Diameter proxy. In that case the Diameter proxy needs to check that the NAF_ID sent to BSF, and the identity used by NAF in its communications with Diameter proxy match.

A related CR was provided in TD S3-040328 which was reviewed and revised in TD S3-040412 which was revised in TD S3-040432 which was approved.

TD S3-040225 MBMS key management scenarios and GBA. See also GBA_U topic if needed. This was presented by Siemens and contained an overview of MBMS scenarios and the use of GBA. The presentation was noted and related contributions were then discussed.

TD S3-040218 GBA_U: Bootstrapping secrets to the UICC. This was covered in the handling of TD S3-040346.

TD S3-040346 Comments on S3-040218: GBA_U: Bootstrapping secrets to the UICC. This was introduced by Siemens on behalf of Siemens and Ericsson and contained the comments from Gemplus to TD S3-040218 and the

response from Siemens. There was a concern about using the Special-RAND for GBA_U when it has not been agreed for A5 improvement for GSM at present. Siemens responded that there were no other proposals for indicating the use of GBA_U at present and the Special-RAND indication was all that was currently available. It was commented that this proposal would require the support of Multiple Key derivations on the UICC. An associated CR was provided in TD S3-040216 to implement the proposal. Comments from Gemplus were summarised in TD S3-040350 which was then considered.

TD S3-040350 GBA_U: comments to S3-040217 and S3-040218. This was introduced by Gemplus and proposed that as GBA is a Rel-6 feature without legacy issue, that a GBA-aware ME shall support both GBA_ME and GBA_U interface procedure in order to avoid security issues. Siemens commented that "in order to avoid security issues" was confusing, as this requirement was not a security issue. Gemplus stated that having GBA_U on the ME would allow flexibility for future applications and provide a minimum level of Security for the applications. After some discussion it was decided that this requires further study and will be addressed at the next meeting.

TD S3-040216 Proposed CR TS 33.220: Introducing the Special-RAND mechanism for GBA_U. This was introduced by- Siemens. Due to the comments received in discussion of related documents on the use of Special-RAND it was decided to allow until the next meeting for alternative proposals to be presented. **This is intended to be finalised and agreed at the next SA WG3 meeting.**

TD S3-040344 Proposed CR to 33.220: Introduction of a UICC-based Generic Bootstrapping Architecture (Rel-6). This was introduced by Siemens. It was noted that some editors notes had been agreed for issues for further study and this CR would need to be updated with the agreements already reached at this meeting. The revised CR was provided in TD S3-040413 which was reviewed and approved.

6.9.3 TS 33.221 Subscriber certificates

TD S3-040292 Proposed CR to 33.221: Editorial change to correct the reference's sources (Rel-6). This was introduced by Nokia. The CR was postponed to the next meeting and the SA WG3 Chairman undertook to ask TSG SA about the correct referencing of OMA documents.

6.9.4 TS 33.222 HTTPS-based services

TD S3-040319 Text for sub-sections 6.4 "Interfaces" and 6.5 "Management of UE Identity" within section 6 "Authentication Proxy" of TS 33.222 – Pseudo-CR. This was introduced by Siemens on behalf of Nokia and Siemens. The proposals for this CR had been sent to the e-mail list for some time before the meeting and no comments received. An editor's note should be added to 6.5 stating that "The changes made to handling of application specific user profiles in TS 33.220 may effect this clause". The editor was asked to include this. With this change, the Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040295 Pseudo-CR to 33.141: UE's identities in Presence server access. This was introduced by Nokia on behalf of Nokia and Siemens. It was agreed to remove the text "*which was sent by the BSF ... Zn reference point*" from the first paragraph of 6.1.3. The note of 6.1.3 should also be deleted. With these modifications, the Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040321 Removal of Annex B of TS 33.222 – Pseudo-CR. This was introduced by Siemens on behalf of Nokia and Siemens. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040323 Definition of TLS profile for shared key based UE authentication according to clause 5.3 of TS 33.222 – Pseudo-CRs to 33.222 and 33.141. This was introduced by Siemens on behalf of Nokia and Siemens. This Pseudo-CR was agreed for inclusion by the editors in the draft TSs. **It was noted that if there is any problem with TS 33.222 being ready for Rel-6 then this would need to be moved back into TS 33.141.**

TD S3-040348 AP-AS Interface Protection. This was introduced by Ericsson. The Pseudo-CR to 33.222 included a new figure 2: It was noted that the Zb/Za interface should not extend between the UE and Presence service. The editor was asked to change this in the draft TS. With this change, Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040320 New text for section 5.3 "Shared key-based UE authentication with certificate-based NAF authentication "of TS 33.222 – Pseudo-CR. This was introduced by Siemens on behalf of Nokia and Siemens. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040325 Definition of Authentication Mechanisms in TS 33.222 – Pseudo-CR. This was introduced by Siemens. Ericsson reported that they had considered this and reached the same conclusion, to reduce the options available in Rel-6. Alternative proposals to specify the use of Certificates and Shared Key TLS were provided by Nokia in TD S3-040336 and TD S3-040337 respectively, which were then reviewed (see decisions below).

TD S3-040336 Pseudo-CR: Subscriber certificate based authentication in GAA. This was introduced by Nokia. Siemens asked why the TLS specification could not be enough to implement Certificate based authentication and it needed to be specified in the TS. Nokia responded that the NAF interface needs to be able to handle the possible variances. It was commented that there was a place for guidance on the mechanisms to use in section 7of TR 33.919. It was suggested that the text could be replaced by a reference to the IETF RFCs, but should not be removed completely.

It was agreed that the best solution is to include references to the IETF RFCs in clause 5.5 and to include **the guidance proposed by Nokia as an informative Annex**. It was agreed that this should not be mandated in TS 33.222 but could be referred to from other Services.

TD S3-040337 Shared key TLS usage within Ua interface. This was introduced by Nokia and asked SA WG3 to:

- add psk TLS internet draft to the 3GPP ~~I~~" IETF dependency list";
- endorse the usage of psk TLS within GAA; and
- add descriptions of psk TLS usage into relevant specifications in both SA3 (stage 2) and CN1 (stage 3) domain.

A pseudo-CR was annexed to the contribution to include this method in TS 33.222.

It was commented that the shared key TLS was not needed for Rel-6 implementations as, although technically promising as a mechanism, it was not yet mature enough for Rel-6. Nokia agreed to this but argued that the psk TLS is needed and it is possible that the IETF may finalise their TLS work in the Rel-6 time frame. Siemens stated that this was not only a matter of maturity of the IETF work, but also how many options should be included in a Rel-6 UE.

It was agreed that the mechanism in section 5.4 of TS 33.222 should be optional for implementation and the mechanism in section ~~5.~~5.3 of TS 33.222 mandatory for implementation and the IETF Dependency list should be updated appropriately. **The SA WG3 Chairman will report this to Stephen Hayes to add the PSK draft to the dependency list.** The Pseudo-CR in the contribution was agreed for inclusion by the editor in the draft TS.

TD S3-040322. General Requirements and Principles for Access to NAF using HTTPS – Pseudo-CR. This was introduced by Siemens. This Pseudo-CR was agreed for inclusion by the editor in the draft TS. It was noted that "interface" needs to be changed to "reference point" throughout the draft TS.

Status of HTTPS draft TS 33.222: It was agreed that this was ready for presentation to TSG SA for approval and placing under change control as Rel-6.

6.10 WLAN interworking

TD S3-040252 Reply LS (from SA WG2) to Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0. This was introduced by France Telecom. SA WG2 provided comments to the Wi-Fi Alliance and mentioned that SA WG3 may provide security related comments to this (see TD S3-040253). The LS was noted.

TD S3-040253 LS (from SA WG2) on Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0. This was introduced by France Telecom. SA WG2 asked some WGs, including SA WG3 to study the Letter from the Chairman of the Wi-Fi Alliance Public Access Task Group in S2-0401110 and to provide a reply. It was decided to gather comments over an e-mail discussion and D Mariblanca agreed to run this task.

AP 33/07: D. Mariblanca to collect comments for the WiFi Alliance document in TD S3-040253. Deadlines: Comments by 31 May 2004. Draft reply by 2 June 2004. Approval of reply by 7 June 2004.

NOTE: This LS was approved by e-mail and allocated to TD S3-040464 in meeting #34 for information.

TD S3-040278 Proposed CR to 33.234: Sending of temporary identities from WLAN UE (Rel-6). This was introduced by Ericsson on behalf of Nokia and Ericsson. The CR was reviewed and modified in TD S3-040416 which was approved.

TD S3-040352 Proposed CR to 33.234: WLAN handover scenario (Rel-6). This was introduced by Nokia and proposed to add detail on how to handle multiple registrations of the WLAN-UE, based on local policy defined for AAA server and HSS. It was questioned whether simultaneous sessions are an SA WG1 service requirement and if so, do they specify the maximum number which should be supported. The answer to these questions was not known. After some discussion it was decided to revise the CR for re-presentation to the meeting. The CR was revised in TD S3-040417 which was revised in TD S3-040440 and approved.

TD S3-040256 Proposal about the efficient mechanism for the set-up of UE-initiated tunnels (Scenario 3) in WLAN interworking. This was introduced by ETRI and proposed a method for the set-up of UE-initiated tunnels which minimally modifies EAP-AKA based authentication mechanism, described in TS 33.234. It included the additional parameter "*PS_Service*", and the generation of *PS_Key*. ETRI asked SA WG3 to determine whether this mechanism was valid for the intended use. It was commented that the secret Key would not be suitable to protect the user data and it appeared that another mechanism (i.e. IPsec) would still be needed for this. It was considered that there were many open issues which would need to be solved before considering this mechanism. The contribution was then noted.

TD S3-040275 Proposed CR to 33.234: EAP in IKEv2 (Rel-6). This was introduced by Nokia on behalf of Nokia and Ericsson. Comments were provided by Siemens in TD S3-040372 which was introduced by Siemens and proposed that S3-040275 should only be accepted if:

- the man-in-the-middle attacks described in section 1 of the contribution are satisfactorily addressed, and a corresponding note is added to TS 33.234, describing how it is addressed;
- the issues arising from non-compliance with the IKEv2 standard are resolved.

It was therefore proposed that the CR is not accepted at this time but that SA WG3 wait until a stable IETF specification is available. It was agreed that this proposed CR would be revisited at the next meeting and the work progressed by e-mail discussion for contributions to the next meeting.

TD S3-040277 Proposed CR to 33.234: Extension of IKEv2 and IPsec profiles (Rel-6). This was introduced by Ericsson on behalf of Nokia and Ericsson and was modified in TD S3-040418 which was approved.

TD S3-040284 Use of IKE in End-to-end tunnelling. This was introduced by Nortel Networks and analysed some practical difficulties or issues in mandating only IKEv2 in the specification and recommend that 3GPP allow the use of IKEv1 with subscriber certificates for establishing UE-initiated tunnels when an operator has the infrastructure to issue subscriber certificates. Furthermore, Nortel Networks also requested SA WG3 to allow the use of IKEv2 with subscriber certificates in order to enable the migration of any installed base of users who are using IKE with subscriber certificates. After some discussion there was some objection to implementing this proposal and so the CR in TD S3-040285 was rejected pending further study and discussion.

TD S3-040394 Profiling of IKEv2 and ESP for NAT traversal. This was introduced by Siemens and provided a brief discussion of the relevant NAT issues as well as a section proposed to be added to TS 33.234. The contribution was noted, a related CR was provided in TD S3-040395.

TD S3-040395 Proposed CR to 33.234: Profiling of IKEv2 and ESP for NAT traversal (Rel-6). This was introduced by Siemens and was approved.

TD S3-040279 EAP method policies and release 6 non-compliant implementations. This was introduced by Nokia on behalf of Nokia and Ericsson and studied EAP method policies and implications of ME and AAA server implementations which do not conform to Rel-6 specifications. The contribution concluded that the only way to avoid EAP method downgrading attacks is to enforce EAP method policies that do not accept EAP-SIM for USIM subscribers in both the ME and the AAA server and proposed some EAP method policy rules. A related CR was provided in TD S3-040280.

TD S3-040280 Proposed CR to 33.234: Support of EAP SIM and AKA in AAA server and WLAN UE (Rel-6). This was introduced by Nokia on behalf of Nokia and Ericsson. It was suggested that the terminology for SIM/USIM insertion should be clarified and the abnormalities part moved to a new informative Annex. The CR was revised to take this into account and provided in TD S3-040420 which was approved.

TD S3-040281 Proposed CR to 33.234: Re-authentication failure notification to HSS (Rel-6). This was introduced by Ericsson. The text was found in need of clarification and the CR was edited off-line to take comments into account and provided in TD S3-040421 which was revised in TD S3-040438 and was approved.

TD S3-040276 Proposed CR to 33.234: Introduction of UE split alternative 2 in TS 33.234 (Rel-6). This was introduced by Ericsson on behalf of Nokia and Ericsson. It was commented that the agreement for alternative 2 (UICC can be the end-point) was not reflected in this CR and that "MT" should be replaced with "MT or UICC" in the CR. There were also some terminology problems which needed correction. The CR was updated in TD S3-040422 which included changes from the original CR. The CR was revised to make it show the real changes in TD S3-040437 and was approved.

TD S3-040282 Proposed CR to 33.234: Identity request procedure clarification (Rel-6). This was provided by Ericsson to align the specification with EAP-AKA operation. The new figure was noted to be badly numbered for the sequence flow steps and would need correction. It was confirmed that intermediate nodes could not change anything between steps 6 and 10. The CR was updated in TD S3-040423 which was revised in TD S3-040439 and was approved.

TD S3-040351 WLAN application. This was introduced by Gemplus and proposed that SA WG3 to adopt the WLAN solution to prevent attacks on vulnerability spreading between WLAN and GSM/GPRS domains and to send a LS to T WG3 asking them to work on WLAN application. It was asked whether this technique offers a higher security level than using EAP-AKA using a USIM. It was clarified that this allows the high security while avoiding the transmission of the IMSI. It was suggested that this could be taken as an option. It was considered necessary to have more explanation of the justification for crating this functionality over the use of EAP-AKA with USIM. Gemplus were asked to discuss this over e-mail by 7 June in order to provide justification for the introduction of this and finalisation of this would be done at the next meeting. It was noted that this work would also need consultation with SA WG1 if it is agreed to.

TD S3-040353 Proposed CR to 33.234: Requirement on keeping WLAN accessing keys independent from 3G accessing keys stored in USIM (Rel-6). This was introduced by Nokia. It was clarified that the keys were CK, IK and KC. The CR was updated in TD S3-040424 which was revised in TD S3-040441 and approved.

TD S3-040270 Bluetooth Security Overview for TS 33.234 WLAN interworking security specification (Annex A4). This was introduced by BT Group. TS 33.234-6.0.0 contains an empty Clause A.4 which was intended to give an overview of Bluetooth security and configuration considerations. The contribution provided background material that was be used to create a CR to add appropriate text. The related CR was provided in TD S3-040271 which was also presented by BT Group. The need for this information in the TS was questioned, and it was clarified that something should be included in order to help with implementation issues to be taken account of. It was also suggested that this information could be captured in TR 33.817 which deals with USIM re-use. It was decided to postpone the decision on this until closer to Rel-6 freezing time and try to improve the text and decide what should be put where in the specifications. **Delegates were asked to consider this until the next meeting, particularly in the content of the table in the CR.**

TD S3-040272 Use of a Trusted Tunnel to Secure Local Terminal Interfaces. This was introduced by Intel on behalf of Intel and Gemplus and proposed the use of a TLS-based Trusted Tunnel, which can provide the adequate level of protection required for several use scenarios that require a secure Local Terminal Interface, including Bluetooth as well as other types of local transport protocols. The earliest that this could be included in specifications would be Rel-7 so SA WG3 delegates were asked to study this proposal and provide comment and contribution for future work. The contribution was then noted.

TD S3-040375 LS from SA WG2: MMS over 3GPP Interworking WLANs. This was introduced by T-Mobile and was provided to SA WG3 for information. The LS was noted.

TD S3-040379 Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces) (Rel-6). (Received after document deadline) This was introduced by BT Group on behalf of Toshiba and other supporting companies. There was a comment that there were a lot of additional requirements being introduced near the freeze date of Rel-6. Also, that "potential requirements" should not be part of a system specification. Due to the far-reaching impacts of this proposal, it was decided to allow until the next meeting to consider the best way of including the recommendations and requirements in the specification set. **Members were asked to consider this and provide contribution to the next meeting.**

AP 33/08: C. Blanchard to lead an e-mail discussion on (U)SIM Security re-use by Peripheral devices. Final comments by 22 June for input to next meeting.

TD S3-040283 Resolving the editors notes in Wireless Local Area Network (WLAN) interworking security 3GPP TS 33.234 V6.0.0 (2004-03). This was introduced by BT Group and indicated the impacts of the editors notes in TS 33.234 in order to have solutions to the notes and be able to remove them. The list was reviewed and

discussed and it was considered a useful overview to the outstanding editors notes in the TS. C. Blanchard was asked to maintain this list and delegates were asked to provide comments for this purpose. It was noted that some issues may be resolved without the need for action by SA WG3 as the other bodies progress their documents.

6.11 Visibility and configurability of security

There were no specific contributions under this agenda item.

6.12 Push

There were no specific contributions under this agenda item.

6.13 Priority

There were no specific contributions under this agenda item.

6.14 Location services (LCS)

TD S3-040365 LS from TSG GERAN: Use of Kc in the Uplink TDOA location method. This was introduced by TruePosition. In response to SA WG3 LS to TSG GERAN (TD S3-040152), TSG GERAN asked SA WG3 to review and endorse the attached CR 043 to TS 43.059 (GP-040634). The proposed CR was reviewed and SA WG3 endorsed the CR. A LS to inform TSG GERAN of this was provided in TD S3-040404 which was approved.

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

There were no specific contributions under this agenda item.

6.16 Open service architecture (OSA)

There were no specific contributions under this agenda item.

6.17 Generic user profile (GUP)

TD S3-040209 LS (from CN WG4) on Relationship between 3GPP and Liberty Alliance related to GUP work. This was introduced by Nortel Networks. CN WG4 asked CN and SA WGs to clarify the nature of the formal relationship (if any) between 3GPP and Liberty Alliance in general, and with regard to the specific concerns expressed in the LS, covering:

1) The use of Liberty Alliance specification text in 3GPP.
2) Access to Liberty Alliance documents and ability to contribute to Liberty Alliance work relevant to 3GPP.
3) IPR implications of using Liberty Alliance standards in 3GPP.

It was noted that information should be taken from the proposals in TD S3-040338 to answer this liaison (see below, LS in TD S3-040385).

TD S3-040362 LS from CN WG4: Application Layer vs Transport Layer security for GUP. This was introduced by Lucent Technologies. CN WG4 asked SA WG3 for the status within SA WG3 regarding the security requirements concerning GUP and more specifically, CN WG4 would like to know what kind of security mechanism(s) will be recommended by SA WG3 for GUP security. It was noted that information should be taken from the proposals in TD S3-040338 to answer this liaison (see below, LS in TD S3-040385).

TD S3-040338 GUP security follow-up. This was introduced by Ericsson on behalf of Ericsson and Nokia and provided a follow-up on previous discussions held around GUP security in SA3#32. It captured the current status of the Generic User Profile (GUP) work in 3GPP and proposed recommendation for SA WG2 and CN WG4 to be considered in their respective specifications in this area. It invited SA WG3 to review security related sections in the SA WG2 TS 23.240 in order to agree on the fact that there is no need for GUP security material to be included in any of existing or new SA3 specifications and to review security related sections in the CN WG4 TS 29.240 in order to decide if the proposed way of referencing the Liberty Security related specifications would be appropriate. It proposed that SA WG3 inform SA WG2 and CN WG4 of the results of these reviews.

It was noted that there was a potential problem with the restricted nature of Liberty Alliance documents but this was thought to be a problem for 3GPP as a whole to look into in co-operation with the Liberty Alliance. It was

understood that the Liberty Alliance were intending to use the 3GPP GBA specification. A concern was also expressed that TS 29.240 only covered NE-NE interfaces and some additional work may be needed to specify the GUP Application to the ME. It was agreed to provide an LS covering the proposals in Annexes B and C of this contribution along with a note that this is not a complete analysis of what may be needed and that the necessary CRs should not be approved yet. This LS was provided in TD S3-040385 and was approved.

6.18 Presence

TD S3-040347 Pseudo CR to 33.141: Editorial Updates to draft TS 33.141. This was introduced by Ericsson. The word "stateless" will be removed from the session management mechanism definition. The note on interleaving attack in clause 5.1.1 should be removed. With these changes, the Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040294 Pseudo-CR to 33.141: Applying NDS for Network side security for Presence. This was introduced by Nokia on behalf of Nokia and Siemens. It was noted that the reference should be to TS 33.222 in reference [18]. This Pseudo-CR was agreed for inclusion by the editor in the draft TS. The proposals in TD S3-040348 from Ericsson were reviewed and agreed and the attached Pseudo-CR to TS 33.141 was agreed for inclusion in the draft TS.

TD S3-040349 Presence Security Updates. This was introduced by Ericsson and proposed not to specify TLS v1.1, TLS extensions and shared key TLS for Rel-6. Ericsson also proposed to choose the reverse proxy as the Authentication Proxy solution. A Pseudo-CR was attached to remove editors notes on options for Rel-6. The changes in the Pseudo-CR were accepted. The implications of this were that it was agreed not to use TLS v1.1 and the reverse proxy is now accepted. If any further changes are proposed, this should be done by Pseudo-CRs to the next meeting.

TD S3-040293 Using SSC as optional in Presence service TS33.141. This was introduced by Nokia. There was some difference in interpretation of these changes and it was decided to leave this for further clarification by e-mail and proposals can be provided to at the next meeting. The e-mail discussion will be lead by Bengt and conclude by 22 June 2004.

TD S3-040339 Pseudo-CR to 33.141: ISIM Support (Rel-6). This was postponed to the next meeting in line with the handling of TD S3-040340.

Status of Presence draft TS 33.141: It was agreed that this was ready for presentation to TSG SA for approval and placing under change control as Rel-6. Rapporteur to forward to SA WG3 list for final check by 19 May 2004. Final version to Secretary by 24 June 2004.

6.19 User equipment management (UEM)

There were no specific contributions under this agenda item.

6.20 Multimedia broadcast/multicast service (MBMS)

Incoming LSs:

TD S3-040206 Liaison (from Download+DRM) to 3GPP SA4 and SA3 on DRM for PSS and MBMS streams. This was introduced by Ericsson. It provided responses to LSs from SA WG4 and SA WG3. In response to S3-030805:

- DLDRM notes that SA WG3 regards harmonization between DRM and MBMS security and re-use of cryptographic algorithms as necessary, and that SA3 has not decided on a protocol to be used for MBMS streaming, but is considering SRTP as defined by IETF or as described in S3-030750.
- DLDRM notes that there is an integrity protection requirement for MBMS.
- DLDRM notes that selective encryption may not be compliant with MBMS requirements as contained in 3GPP TS 33.246. DLDRM would like the solution to be provided by 3GPP to allow for selective encryption. The use of selective encryption is optional for the content issuer to use.
- DLDRM notes that SA WG3 finds AES in Counter Mode with 128 bit key length acceptable for DRM purposes.

This was noted. (A LS on MBMS matters was provided in TD S3-040393).

TD S3-040212 Reply LS (from SA WG4) on “LS on HTTP based services and order of procedures”. This was introduced by Ericsson and informed SA WG3 that SA WG4 is currently not in the position to answer the questions asked by SA WG3. SA WG4 recognised their responsibility to define the service architecture but have not yet defined the service architecture nor looked at the security requirements. SA WG4 has a working assumption to use HTTP as the transport protocol but this is only agreed for the repair service. The LS was noted.

TD S3-040213 Reply (from SA WG4) to “LS on service announcement and UE joining procedure”. This was introduced by Nokia and SA WG4 informed SA WG3 that it believes that it is not a problem to specify the indication of any feature in the MBMS service announcement. However, regarding the “Joining availability time” feature, while this is still theoretically feasible from SA WG4 point of view, SA WG1 “*does not see the need for this concept*” and SA2 “*is not convinced of the need of such an indication*”. SA WG4, therefore, prefers to refrain from specifying a feature until this is a needed requirement and/or described in the MBMS architecture. This LS was noted.

TD S3-040363 Reply LS on HTTP based services and order of procedures. This was introduced by Nortel Networks and responded to questions asked by SA WG3 on the use of GBA and HTTP for MBMS Application Layer Authentication. SA2’s architecture does not place any restrictions on the ordering of application layer procedures (joining or otherwise) and bearer level joining procedures. SA2’s architecture does not require any relationship between application layer joining (or other) procedures and bearer layer joining procedures. These responses were noted.

TD S3-040364 LS on moving security requirements to SA3 MBMS TS. This was introduced by Ericsson. SA WG2 intend to remove some requirements from TS 23.246, section 5.1.1 and asked SA WG3 to include these requirements in TS 33.246. The Rapporteur for TS 33.246 (A. Escott) was asked to check the need for these requirements and to provide a Pseudo-CR and LS to incorporate this. These were provided in TD S3-040386 and TD S3-040387. The Pseudo-CR in TD S3-040386 was agreed for inclusion in the draft TS and the LS in TD S3-040387 was reviewed and revised in TD S3-040442 which was approved.

TS and Independent Pseudo-CRs:

TD S3-040261 Latest version of the MBMS TS. This Draft TS contained agreed changes since the last meeting and was provided for information and was noted.

TD S3-040324 Editorial Modifications to the MBMS TS. This was introduced by the Rapporteur (A. Escott) and was reviewed. It was commented that many editors notes still remained and this should be reviewed and an attempt made to remove as many as possible (in particular the note in C.5). The changes were then agreed.

TD S3-040226 pseudo-CR to 33.246: Additions to threats section (Annex B). This was introduced by Siemens and was agreed (note: "lateron" needs to be corrected in two places).

TD S3-040221 pseudo-CR to TS 33.246: Clarification on MSK keys and MBMS user/bearer service. Make clear when User service or Bearer Service is meant. This was introduced by Siemens and discussed. The changes were agreed and the editor agreed to include also an editors note in section 5.1.

Discussions on Joining and MSK distribution:

TD S3-040244 Bearer level joining and application level joining for MBMS security. This was introduced by Samsung and proposed to agree on the presented understanding about bearer level joining and security level joining from security point of view, and if necessary to provide LSs to other related WGs about SA3’s understanding. It was considered that these proposals made non-security related assumptions and would need to be agreed in other groups before SA WG3 considered the security aspects of the schemes.

TD S3-040239 Order of MBMS UE context establishment and key delivery. This was introduced by **3** and suggested that it is better to establish the MBMS UE context before delivering the MSK. However, application layer joining needs to be taken into account before making a final decision. It could not be agreed on the order of MSK delivery and Bearer joining and the decision would be made by other groups or market factors. The document was therefore noted at this time.

TD S3-040240 MSK update rules. This was introduced by Huawei and proposed adding a "request delay time" for individual UEs before requesting the Key after receiving the "key available" signal. There was some discussion on the mechanism to signal this delay time, the enforcing of the UE action and the possibility of disadvantages for UEs which have longer delay times allocated. After some discussion it was considered that the real issue is not a

security issue, but that SA WG4 and SA WG2 should be consulted. A Liaison Statement was drafted in TD S3-040388 which was reviewed and revised in TD S3-040444 which was approved.

TD S3-040245 MBMS MSK distribution procedure. This was introduced by Samsung and proposed to come to an agreement on the overall MBMS MSK distribution procedure and capture it into the current TS. It was considered that the section 3 issues needed clarification over the service architecture before including it, but may be used when the service architecture is well defined.

During discussions it was recognised that clarification is needed to distinguish between the terms of Service Subscription, Service Joining and Service Announcement. It is also necessary to be sure that the bearer and user levels are distinguished.

Discussion: OTA model or 'GBA-based' model:

TD S3-040380 Joining based key management – comments by Ericsson to Axalto comments on original paper TD S3-040236. This was introduced by Ericsson and asks how the UICC can know when to give the Key to a UE which has the MSK and joins at a non-pre-defined time. There was some discussion over the issues raised here and clarification was necessary. Off-line discussion was required and delegates were asked to review and discuss these contributions overnight.

TD S3-040232 MBMS key management: OTA- versus GBA-based Point-to-Point key distribution. This was introduced by Telecom Italia and proposed to choose OTA as a point-to-point method to distribute the expected MBMS Keys. Nokia had made comments over e-mail which were presented by Nokia. Comments to this contribution were provided by Ericsson in TD S3-040257.

TD S3-040356 Reply to Comments on S3-040247: OTA for MBMS. This was introduced by Gemplus and included the comments made to the original contribution in TD S3-040247 by Siemens and the response to these comments by Gemplus.

S3-040222 MBMS: Key distribution architectures analysis. This was provided by Siemens, Nokia and Ericsson and comments were provided in TD S3-040345.

TD S3-040345 Reply to Comments on S3-040222: MBMS: Key distribution architectures analysis. This was introduced by Siemens on behalf of Siemens, Nokia and Ericsson and included comments to the original contribution in TD S3-040222 after e-mail discussion.

TD S3-040220 MBMS: The use of registration Keys. This was introduced by Siemens and analysed and compared the key layers that are needed within the different key management models that were available at SA WG3 meeting #32. Siemens concluded that the use of a 'Registration Key' bound tightly to subscription as proposed by the OTA-model is misleading; it needs further specification and adds additional complexity to MBMS keys management.

TD S3-040354 Comments to S3-040241: MBMS Pay per view charging model. This was introduced by Oberthur Card System and contained comments from Siemens on the original contribution from Oberthur Card System in TD S3-040241.

TD S3-040249 MBMS key Management comparison (overhead calculation). This was introduced by Axalto and analysed two key distribution architectures which have been proposed for MBMS key management, based on network/radio resource consumption. Axalto concluded that there was a radio resource efficiency of around 2000 / 100 in advantage of using the OTA approach. Comments to this contribution, based on e-mail discussions were provided by Ericsson in TD S3-040257. Ericsson commented that the comparisons of the messages between the two cases did not seem equivalent or a fair comparison. It was clarified that this was only an Application data comparison and did not include, e.g., PDP-context establishment messages.

TD S3-040257 Comments to 232, 243 and 249. This was introduced by Ericsson and provided comments to contributions TD S3-040232, TD S3-040243 and TD S3-040249 and also covered the contribution from Ericsson in TD S3-040237. Ericsson concluded that MIKEY can be used with push method and carried over UDP and asked SA WG3 to take this into account when deciding on MBMS Key Management. The use of a defined UDP port for MIKEY was noted. Any potential security issues on having this USP port open for use with Push services should be considered.

TD S3-040259 Key deletion in the UICC model using S3-04235. This was introduced by Ericsson and discussed some problems with key deletion and how it can be solved in the combined model. Ericsson only consider deletion of the MSK, since there is no apparent benefit in the ability to remove MTK's. Ericsson questioned the need for a key delete function for MBMS, but if SA WG3 agree that this is useful, this contribution shows how it could be done in the combined model. The case of lost or stolen UICC was mentioned, where the operator may wish to use a key deletion function. This contribution was noted.

TD S3-040234 MBMS key management with MIKEY. This was introduced by Ericsson on behalf of Ericsson and Nokia and discussed the suitability of MIKEY for MBMS key management and proposed that the enhanced MIKEY is chosen as key management protocol for MBMS. A companion document on IKEY payloads was provided in TD S3-040258.

S3-040258 Extension payloads to MIKEY to support MBMS (update of TD S3-040235). This was introduced by Ericsson and described how MBMS key management can be achieved with MIKEY in both ME- and UICC-based models and proposed MIKEY as the MBMS key management method. It was suggested that SA WG3 decide whether to agree on an encrypted MTK or a RAND generated method. **It was agreed that the encrypted MTK method will be used**.

Discussion on approach to adopt: "GBA_U + GBA_ME + MIKEY" method or "OTA + Authentiction" method:

There were comments that the GBA method appears to be fairly mature, compared to the OTA method which has many open issues. It was noted that the full requirements from SA WGs are still needed before the full applicability could be done. It was mentioned that if GBA is chosen then all Terminals would need to support GBA_U in Rel-6.

It was agreed that the GBA method will be used for MBMS Security (GBA_U + GBA_ME + MIKEY). Based on this, it was noted that if a Terminal is to support MBMS, then it will need to support GBA_U.

S3-040233 MBMS key management: UICC-based only solution versus combined method. This was introduced by Telecom Italia and proposed to choose the UICC-based only solution as MBMS key distribution mechanism, based on an analysis of the technical aspects from an Operators viewpoint. Comments had been provided by Nokia by e-mail which were presented. The burden on the operator to upgrade all the UICCs in order to be able to effectively deploy MBSS was mentioned. It was also commented that the UICC solution would solve the major security issues. Some operators indicated that they do not discount the ME-based solution for key storage for certain types of content.

It was agreed that the work would continue under the assumption of there being both the UICC-based solution and ME-based solution. If a problem is encountered in one of the solutions, then it can be re-considered. Some companies objected to the keeping of both solutions and advocated the UICC-based solution only.

It was commented that the additional burden of specifying both solutions was not large as both solutions share common protocols and signalling flows. It was agreed to send an LS to SA WG1 (and other impacted WGs) informing them of this decision. This was provided in TD S3-040390 which was reviewed and revised in TD S3-040445 which was approved.

Pseudo-CRs dependent on decisions above:

S3-040238 Pseudo-CR to 33.246: Authenticating user in MBMS with HTTP digest. This was introduced by Ericsson. It needs to be confirmed that the section "Procedures using the bootstrapped Security Association" referred to was still in the GBA specification and the Editor was asked to check this. The editors' note should be extended to show that this can also be used for key requests. It should also be noted that the use of HTTP is pending final decision in SA WG4, according to their LS to SA WG3. With these additions, this Pseudo-CR was agreed for inclusion by the editor in the draft TS. It was noted that this overlapped with changes in TD S3-040219 (see below).

S3-040219 pseudo-CR to TS 33.246 Using GBA for MBMS. This was introduced by Siemens. Some minor changes were suggested to the text and the last editors note should be extended for the study of MRK derivation. It was noted that this overlapped with the changes proposed by Ericsson in TD S3-040219 and it was agreed to combine these into a single Pseudo-CR in order to clarify the final changes. This was provided in TD S3-040391 which was reviewed and agreed for inclusion in the draft TS.

S3-040260 Pseudo-CR to 33.246: Calculating validity for MIKEY message. This was introduced by Ericsson. The sending of the MSK only for efficiency should be studied off-line. The Pseudo-CR was discussed off-line and a new version produced in TD S3-040392 which was reviewed and agreed for inclusion in the draft TS.

S3-040248 Pseudo-CR to 33.246: CR on MBMS key Management procedures. This was superseded by agreements made in discussions.

S3-040355 Comments to S3-040248: Pseudo-CR to 33.246: CR on MBMS key Management procedures (Rel-6). This was superseded by agreements made in discussions.

S3-040359 Pseudo-CR to 33.246: CR on MBMS key Management procedures (Rel-6)Update of 248. This was superseded by agreements made in discussions.

Data protection techniques:

S3-040228 SRTP for streaming protection in MBMS. This was introduced by Ericsson and proposed to use SRTP for protecting streaming MBMS data. After some discussion, it was decided to consider TD S3-040230 before this could be finalised.

S3-040230 On the need for Integrity and Source Origin Authentication (SOA) in MBMS. This was introduced by Ericsson and discussed the need and sufficiency of integrity protection and source origin authentication in MBMS. Ericsson concluded that omitting integrity protection and SOA would be a premature decision, and some analysis should be made to assess the threats involved. Ericsson did not see insurmountable technical problems if SOA is found to be required. The DoS attack scenarios needed further study. The cost of protecting against attacks compared to the level of the threat also needs to be studied. It was noted that SRTP can be used for encryption and also Authentication, and that TESLA required a Public Key system. It was also commented that TESLA could be included now as a hook to authentication for future Releases. It was agreed to write an LS to SA WG4 and OMA DRM commenting on this. It was also commented that if integrity protection is not required and encryption is used, this could be done without authentication, etc. It was reported that 3GPP2 have adopted the use of SRTP. The LS was provided in TD S3-040393 which was reviewed and updated in TD S3-040443 which was approved.

S3-040227 Applying DRM in to MBMS security. This was introduced by Nokia and discussed further issues regarding usage of DRM in MBMS as an extension to the contribution TD S3-040080. Nokia recommended the selection of their Proposal 2 (Selective Use of DRM Features in MBMS) due to the complications identified in their Proposal 1 (Integration of MBMS and DRM). It was noted that the analysis can only be performed at the lowest level at present. The contribution was noted.

S3-040231 Discussion paper on MBMS data protection for download. This was introduced by Ericsson and proposed to use S/MIME for protection of MBMS download traffic. Ericsson also suggested that S/MIME also fits well in the two-level key hierarchy proposed in TD S3-040080. Ericsson noted that re-use for streaming will not be possible with S/MIME. There was some doubt that this could be used to replace DRM for MBMS download. It was clarified that this was not the intention of this, but to provide MBMS download traffic protection only. It was discussed and agreed that the issue of DRM and MBMS traffic/channel protection are independent issues. It was agreed to include these issues in the LS in TD S3-040393 clarifying it is intended to use this without the need for a PKI infrastructure.

The idea of organising an ad-hoc meeting / Workshop with SA WG4 experts (and possibly some OMA experts) on MBMS issues was raised in order to allow SA WG3 to progress their work on a more certain basis. This was considered a good idea and the suggestion was added to the LS in TD S3-040393.

S3-040229 Pseudo CR to 33.246: SRTP for streaming protection in MBMS. This was covered by MBMS discussions and agreements.

S3-040381 Initial discussion on security requirements in the OTA server interfaces. This was a late document, received after the document deadline and was noted.

6.21 Key Management of group keys for Voice Group Call Services

TD S3-040255 Reply (from TSG GERAN) to LS on 'Ciphering for Voice Group Call Services'. This was introduced by Siemens. This was sent in response to SA WG3 questions in TD S3-030804 and provided GERAN WG2 understanding of the issues. SA WG3 were asked to inform GERAN WG2 about the final decision regarding the provision of the RAND and CGI as VGCS ciphering parameters, such that the necessary CRs can be prepared.

Siemens reported that they believed their proposed CR in TD S3-040415 was in compliance with the responses from GERAN WG2. A reply LS was provided in TD S3-040428 which was reviewed and revised in TD S3-040447 and approved.

TD S3-040370 LS (from T WG3) on VGCS and VBS security. This was introduced by Axalto. T WG3 informed SA WG3 that they have prepared a CR to 31.102 to support the VGCS key derivation process on the USIM and asked SA WG3 to provide any comments on it (T3-040327 which was attached). T WG3 also asked for confirmation on the following issues:

1 Does SA WG3 intend to assign one ciphering algorithm identifier per VGCS group (which is the current assumption of T WG3), or one per key (assuming that there are two keys for each group), or one algorithm for the VGCS?
This needs clarification.

2 Does the SA WG3 work encompass VBS security in the same way as VGCS? Applying a similar mechanism to VBS could enable the operator to charge the subscriber accordingly.
VBS is a subset of VGCS.

The CR was reviewed and it was verified that it was in line with SA WG3 working assumptions. A reply LS was provided in TD S3-040425 which was reviewed and approved.

TD S3-040286 VGCS: Status of principles and further proceeding. This was introduced by Siemens on behalf of Siemens and Vodafone and gave an overview of the decisions that SA WG3 had made so far on VGCS/VBS ciphering. It is also proposed to add two more decisions to this list of agreed principles and to allow GERAN WG2 more time to study a solution to provide the global-count. It was also proposed that a LS is sent to ETSI SAGE to inform them to verify the suitability of the 32-bit challenge proposal. This was agreed and a LS was provided in TD S3-040426 which was reviewed and revised in TD S3-040446~~7~~ which was approved. A related CR was provided in TD S3-040415 to demonstrate the changes needed if the proposal is acceptable to ETSI SAGE.

TD S3-040415 Proposed CR to 43.020: Introducing VGCS/VBS ciphering (Rel-6). This was introduced by Vodafone on behalf of Siemens and Vodafone. The CR was not provided for full approval at this time, but for agreement in principle so that it can be easily approved if all the issues are found to be OK. It was noted that the whole Annex F was intended to be added to TS 43.020 and would be fully marked with change bars when the final CR is produced for approval. Some minor editorials were suggested and the proposed annex was endorsed by SA WG3 as the expected content to be included when all verifications have been made with impacted bodies. It was agreed to attach an updated version with all change bars showing in TD S3-040427 to the LSs in TD S3-040428~~5~~ (revised in TD S3-040447) and TD S3-040426 (revised in TD S3-040446).

6.22 Guide to 3G security (TR 33.900)

There were no specific contributions under this agenda item.

6.23 Other areas

There were no specific contributions under this agenda item.

7 Review and update of work programme

There were no specific contributions under this agenda item. Rapporteurs were asked to provide Work Programme updates to the Secretary by 21 May 2004.

8 Future meeting dates and venues

TD S3-040405 Invitation to the 3GPP and ETSI TISPAN joint Workshop to be held on 22 - 23 June 2004 in Mediathel in Sophia Antipolis. This was sent on the e-mail list. Concerned delegates were asked to try to attend if possible and the document was noted.

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#34	06-09 July 2004	Acapulco, Mexico	"NA Friends of 3GPP"
S3#35	5-8 October 2004	Malta	EF3
S3#36	23-26 November 2004	Shenzhen, China	HuaWei Technologies
S3#37	22-25 February 2005	Australia (TBC)	Qualcomm (TBC)

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#14	19-21 July 2004	Povoa de Varzim, Portugal. Combined with ETSI TC LI	ET3
SA3 LI-#15	11-13 October 2004	USA. Co-located with TR45 LAES	NA Friends

TSGs RAN/CN/T and SA Plenary meeting schedule

Meeting	2004	Location	Primary Host
TSGs#24	June 2-4 & 7-10 2004	Korea	TTA
TSGs#25	8-10 & 13-16 September 2004	Palm Springs, USA	"NA Friends of 3GPP"
TSGs#26	8-10 & 13-16 December 2004	Athens, Greece	"European Friends of 3GPP"
Meeting	**2005 DRAFT TBD**	**Location**	**Primary Host**
TSGs#27	March 9-11 & 14-16 2005	Tokyo, Japan	TBD
TSGs#28	June 1-3 & 6-9 2005	Europe (TBC)	TBD
TSGs#29	September 21-23 & 26-29 2005	TBD	TBD
TSGs#30	Nov 30-2 Dec & 5-8 Dec 2005	Europe (TBC)	TBD

9 Any other business

TD S3-040419 Liaison statement (from SA WG1) on Network Protection against Virus Infected Mobiles. This was introduced by the SA WG3 Chairman and was provided for information. The attached WID was thought to be of some impact for Security and delegates were asked to consider this and provide comments.

Close

The Chairman, V. Niemi, thanked delegates for their hard work during the meeting and the Hosts, Samsung, for the facilities at the Jade Palace Hotel, Beijing. He then closed the meeting.

Annex A: List of attendees at the SA WG3#33 meeting and Voting List

A.1 List of attendees

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Jorge Abellan Sevilla	Axalto S.A.	jsevilla@axalto.com		+33 1 46 00 59 33	+33 1 46 00 59 31	FR	ETSI
Dr. Selim Aissi	INTEL CORPORATION SARL	selim.aissi@intel.com		+01-503 264-3349	+01-503 264-1578	FR	ETSI
Mr. Hiroshi Aono	NTT DoCoMo Inc.	aono@mml.yrp.nttdocomo.co.jp		+81 468 40 3509	+81 468 40 3788	JP	ARIB
Mr. Sundeep Bajikar	INTEL CORPORATION SARL	sundeep.bajikar@intel.com		+1 408-765-3705	+1 408-765-4614	FR	ETSI
Mr. Colin Blanchard	BT Group Plc	colin.blanchard@bt.com	+44 7711 191835	+44 1473 605353	+44 1473 623910	GB	ETSI
Mr. Marc Blommaert	Siemens nv/sa	marc.blommaert@siemens.com		+32 14 25 34 11	+32 14 25 33 39	BE	ETSI
Mr. Charles Brookson	DTI - Department of Trade and Industry	cbrookson@iee.org	+44 20 7215 3691	+44 20 7215 3691	+44 20 7215 1814	GB	ETSI
Mr. Holger Butscheidt	BUNDESMINISTERIUM FUR WIRTSCHAFT	holger.butscheidt@regtp.de		+49 6131 18 2224	+49 6131 18 5613	DE	ETSI
Mr. Mauro Castagno	TELECOM ITALIA S.p.A.	mauro.castagno@telecomitalia.it		+39 0112285203	+39 0112287056	IT	ETSI
Dr. Jianyong Chen	Zhongxing Telecom Ltd.	chen.jianyong@zte.com.cn		+86-75526773000-6938	+86-75526773000-6943	CN	CCSA
Mr. Jing Chen	Zhongxing Telecom Ltd.	chen.jing3@zte.com.cn		+86-75526773000-7163	+86-75526773000-6943	CN	CCSA
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	Hutchison 3G UK Ltd (3)	adrian.escott@three.co.uk		+44 7782 325254	+44 1628 766012	GB	ETSI
Mr. Louis Finkelstein	MOTOROLA Ltd	louis.finkelstein@motorola.com		+1 847 576 4441	+1 847 538 4593	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 SA	sylvie.fouquet@francetelecom.com		+33 145 29 49 19	+33 145 29 65 19	FR	ETSI
Mr. Robert Gross	TruePosition Inc.	rlgross@trueposition.com		+1610 680 1119	+1 610 680 1199	US	ETSI
Ms. Tao Haukka	Nokia Japan Co, Ltd	tao.haukka@nokia.com		+358 40 5170079		JP	ARIB
Mr. Guenther Horn	SIEMENS AG	guenther.horn@siemens.com		+49 8963 641494	+49 8963 648000	DE	ETSI
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vodafone.com	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB	ETSI
Ms. Yingxin Huang	HuaWei Technologies Co., Ltd	huangyx@huawei.com		+86-10-82882752	+86-10-82882940	CN	CCSA
Mr. Bradley Kenyon	Hewlett-Packard, Centre de Compétences France	brad.kenyon@hp.com		+1 402 384 7265	+1 402 384 7030	FR	ETSI
Mr. Geir Koien	Telenor AS	geir-myrdahl.koien@telenor.com		+47 90752914	+47 37 04 52 84	NO	ETSI
Ms. Tiina Koskinen	Nokia Telecommunications Inc.	tiina.s.koskinen@nokia.com		+358504821347	+358718075300	US	ATIS
Mr. Bernd Lamparter	NEC Technologies (UK) Ltd	bernd.lamparter@netlab.nec.de		+49 6221 905 11 50	+49 6221 905 11 55	GB	ETSI
Mr. Alex Leadbeater	BT Group Plc	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. Vesa Lehtovirta	Ericsson Incorporated	vesa.lehtovirta@ericsson.com		+358405093314	+	US	ATIS
Mrs. Fei Liu	China Mobile Communications Corporation (CMCC)	liufei@chinamobile.com	+86 13910036595	+86 10 66006688 3118	+86 10 63600340	CN	CCSA
Mr. Michael Marcovici	Lucent Technologies	marcovici@lucent.com		+1 630 979 4062	+1 630 224 9955	US	ATIS
Mr. David Mariblanca	Telefon AB LM Ericsson	david.mariblanca@ericsson.com		+34 646004736	+34 913392538	SE	ETSI
Mr. Huang Ming	UTStarcom, Inc	huangm@utstar.com		+861085205202		US	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. Anand Palanigounder	Nortel Networks (USA)	anand@nortelnetworks.com		+1 972 684 4772	+1 972 685 3123	US	ATIS
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 Korea	bengt.sahlin@ericsson.com		+358 40 778 4580	+358 9 299 3401	KR	TTA
Mr. Stefan Schroeder	T-MOBILE DEUTSCHLAND	stefan.schroeder@t-mobile.de		+49 228 9363 3312	+49 228 9363 3309	DE	ETSI

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. James Semple	QUALCOMM EUROPE S.A.R.L.	jsemple@qualcomm.com		+447880791303		FR	ETSI
Mr. Guangyu Shan	China Academy of Telecommunications Technology	shanguangyu@datangmobile.cn		+861082029090*6525	+861062303127	CN	CCSA
Mr. Benno Tietz	Vodafone D2 GmbH	benno.tietz@vodafone.com		+49 211 533 2168	+49 211 533 1649	DE	ETSI
Ms. Annelies Van Moffaert	ALCATEL S.A.	annelies.van_moffaert@alcatel.be		+32 3 240 83 58	+32 3 240 48 88	FR	ETSI
Mr. Berthold Wilhelm	BUNDESMINISTERIUM FUR WIRTSCHAFT	berthold.wilhelm@regtp.de		+49 681 9330 562	+49 681 9330 725	DE	ETSI
Mr. Dajiang Zhang	NOKIA Corporation	dajiang.zhang@nokia.com		+86-13901168924	+86-010-84210576	FI	ETSI
Mr. Yanmin Zhu	SAMSUNG Electronics Research Institute	yanmin.zhu@samsung.com		+86-10-68427711	+86-10-68481891	GB	ETSI

47 participants

A.2 SA WG3 Voting list

Based on the attendees lists for meetings- #31, #32, and #33, the following companies are eligible to vote at SA WG3 meeting #34:

Company	Country	Status	Partner Org
ALCATEL S.A.	FR	3GPPMEMBER	ETSI
AT&T Wireless Services, Inc.	US	3GPPMEMBER	ATIS
Axalto S.A.	FR	3GPPMEMBER	ETSI
BT Group Plc	GB	3GPPMEMBER	ETSI
BUNDESMINISTERIUM FUR WIRTSCHAFT	DE	3GPPMEMBER	ETSI
China Academy of Telecommunications Technology	CN	3GPPMEMBER	CCSA
China Mobile Communications Corporation (CMCC)	CN	3GPPMEMBER	CCSA
DTI - Department of Trade- and Industry	GB	3GPPMEMBER	ETSI
Ericsson Incorporated	US	3GPPMEMBER	ATIS
Ericsson Korea	KR	3GPPMEMBER	TTA
GEMPLUS S.A.	FR	3GPPMEMBER	ETSI
GIESECKE & DEVRIENT GmbH	DE	3GPPMEMBER	ETSI
Hewlett-Packard, Centre de Compétences France	FR	3GPPMEMBER	ETSI
HUAWEI TECHNOLOGIES Co. Ltd.	CN	3GPPMEMBER	ETSI
HuaWei Technologies Co., Ltd	CN	3GPPMEMBER	CCSA
Hutchison 3G UK Ltd (3)	GB	3GPPMEMBER	ETSI
INTEL CORPORATION SARL	FR	3GPPMEMBER	ETSI
Lucent Technologies	US	3GPPMEMBER	ATIS
Lucent Technologies Network Systems UK	GB	3GPPMEMBER	ETSI
Mitsubishi Electric Co.	JP	3GPPMEMBER	ARIB
mmO2 plc	GB	3GPPMEMBER	ETSI
MOTORAOLA SEMICONDUCTOR ISRAEL LTD	IL	3GPPMEMBER	ETSI
MOTOROLA A/S	DK	3GPPMEMBER	ETSI
MOTOROLA JAPAN LTD	JP	3GPPMEMBER	ARIB
MOTOROLA Ltd	GB	3GPPMEMBER	ETSI
NEC EUROPE LTD	GB	3GPPMEMBER	ETSI
NEC Technologies (UK) Ltd	GB	3GPPMEMBER	ETSI
Nippon Ericsson K.K.	JP	3GPPMEMBER	ARIB
NOKIA Corporation	FI	3GPPMEMBER	ETSI
Nokia Japan Co, Ltd	JP	3GPPMEMBER	ARIB
Nokia Telecommunications Inc.	US	3GPPMEMBER	ATIS
NORTEL NETWORKS (EUROPE)	GB	3GPPMEMBER	ETSI
Nortel Networks (USA)	US	3GPPMEMBER	ATIS
NTT DoCoMo Inc.	JP	3GPPMEMBER	ETSI
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
OBERTHUR CARD SYSTEMS S.A.	FR	3GPPMEMBER	ETSI
ORANGE SA	FR	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
Research In Motion Limited	CA	3GPPMEMBER	ETSI
Samsung Electronics Ind. Co., Ltd.	KR	3GPPMEMBER	TTA
SAMSUNG Electronics Research Institute	GB	3GPPMEMBER	ETSI
SIEMENS AG	DE	3GPPMEMBER	ETSI
Siemens nv/sa	BE	3GPPMEMBER	ETSI
T-MOBILE DEUTSCHLAND	DE	3GPPMEMBER	ETSI
TELECOM ITALIA S.p.A.	IT	3GPPMEMBER	ETSI
Telefon AB LM Ericsson	SE	3GPPMEMBER	ETSI
Telenor AS	NO	3GPPMEMBER	ETSI
TeliaSonera AB	SE	3GPPMEMBER	ETSI
Toshiba Corporation, Digital Media Network Company	JP	3GPPMEMBER	ARIB
TruePosition Inc.	US	3GPPMEMBER	ETSI
UTStarcom, Inc	US	3GPPMEMBER	ETSI
Vodafone D2 GmbH	DE	3GPPMEMBER	ETSI
VODAFONE Group Plc	GB	3GPPMEMBER	ETSI
Zhongxing Telecom Ltd.	CN	3GPPMEMBER	CCSA

54 Voting Members

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040202	Draft agenda for SA WG3 meeting #33	SA WG3 Chairman	2	Approval		Approved
S3-040203	Draft Report of SA WG3 meeting #32 v0.0.8rm	SA WG3 Secretary	4.1	Approval		Minor changes made. Approved. V1.0.0 will be placed on FTP server
S3-040204	Chairmans Report from TSG SA meeting #23	SA WG3 Chairman	4.2	Information		Noted
S3-040205	Draft report of TSG SA meeting #23, version 0.0.5rm	SA WG3 Secretary	4.2	Information		Noted
S3-040206	Liaison (from Download+DRM) to 3GPP SA4 and SA3 on DRM for PSS and MBMS streams	OMA Download+DRM	6.20	Information		Noted
S3-040207	LS (from CN WG1) on Re-authentication and key set change during inter-system handover	CN WG1	6.5	Action		Response LS in S3-040399
S3-040208	Reply LS (from CN WG4) to S3-040187(N4-040240) on use of authentication re-attempt IE	CN WG4	6.5	Action		Proposed CR in S3-040251
S3-040209	LS (from CN WG4) on Relationship between 3GPP and Liberty Alliance related to GUP work	CN WG4	6.17	Action		Response LS in S3-040385
S3-040210	LS (from CN WG4) on Requirements for transfer of GAA-User-Profile	CN WG4	6.9.2	Action		Response LS in S3-040405
S3-040211	Response (from SA WG2) to LS on “IMS messaging, Group management and Presence work overlap between 3GPP and OMA”	SA WG2	5.6	Information		Noted
S3-040212	Reply LS (from SA WG4) on “LS on HTTP based services and order of procedures”	SA WG4	6.20	Information		Noted
S3-040213	Reply (from SA WG4) to “LS on service announcement and UE joining procedure”	SA WG4	6.20	Information		Noted
S3-040214	LS (from SA WG5) on Security of the Management Plane	SA WG5	5.1	Action		Related to S3-040250. E-mail comments to make LS in S3-040382
S3-040215	LS Reply (from TSG SA) to Request for close cooperation on future NGN Standardisation	TSG SA	4.2	Information		Noted
S3-040216	Proposed CR TS 33.220: Introducing the Special-RAND mechanism for GBA_U	Siemens	6.9.2	Approval		Alternative proposals to S-RAND by next meeting for decision
S3-040217	Proposed CR TS 33.220: Introduction of a UICC-based Generic Bootstrapping Architecture	Siemens	6.9.2	Approval		Revised in S3-040344
S3-040218	GBA_U: Bootstrapping secrets to the UICC	Siemens, Ericsson	6.9.2	Discussion / Decision		Comments in S3-040346
S3-040219	pseudo-CR to TS 33.246 Using GBA for MBMS	Siemens	6.20	Approval		Agreed in principle with changes. Incorporated in S3-040391
S3-040220	MBMS: The use of registration Keys	Siemens	6.20	Discussion / Decision		Used in MBMS discussions
S3-040221	pseudo-CR to TS 33.246: Clarification on MSK keys and MBMS user/bearer service. Make clear when User service or Bearer Service is meant	Siemens	6.20	Approval		Agreed. Ed Note in 5.1 to be added
S3-040222	MBMS: Key distribution architectures analysis	Siemens, Nokia, Ericsson	6.20	Discussion / Decision		Comments in S3-040345
S3-040223	LS from ITU-T SG17: Information of new ITU-T Recommendations for secure mobile end-to-end data communication, X.1121 and X.1122	ITU-T SG17	5.7	Information / Comment		Response in S3-040384
S3-040224	GBA: Support of NAFs within the Visited Network	Siemens, Nokia, Ericsson	6.9.2	Discussion / Decision		Related CR in S3-040328
S3-040225	MBMS key management scenarios and GBA	Siemens	6.20	Information		Noted. Related contributions discussed
S3-040226	pseudo-CR to 33.246: Additions to threats section (Annex B)	Siemens	6.20	Approval		Agreed
S3-040227	Applying DRM in to MBMS security	Nokia	6.20	Discussion / Decision		Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040228	SRTP for streaming protection in MBMS	Ericsson	6.20	Discussion / Decision		LS to OMA Download and SA 4 in S3-040393
S3-040229	Pseudo CR to 33.246: SRTP for streaming protection in MBMS	Ericsson	6.20	Approval		Covered in MBMS discussions
S3-040230	On the need for integrity and source origin authentication in MBMS	Ericsson	6.20	Discussion / Decision		LS in S3-040393
S3-040231	Discussion paper on MBMS data protection for download	Ericsson	6.20	Discussion / Decision		LS in S3-040393
S3-040232	MBMS key management: OTA- versus GBA-based Point-to-Point key distribution	Telecom Italia	6.20	Discussion / Decision		Comments in S3-040257 and by Nokia over e-mail.
S3-040233	MBMS key management: UICC-based only solution versus combined method	Telecom Italia	6.20	Discussion / Decision		UICC and ME based solutions to be assumed. LS in S3-040390
S3-040234	MBMS key management with MIKEY	Ericsson, Nokia	6.20	Discussion / Decision		Agreed that the encrypted MTK method will be used
S3-040235	Extension payloads to MIKEY to support MBMS	Ericsson, Nokia	6.20	Discussion / Decision	S3-040258	Updated in S3-040258
S3-040236	Joining based key management	Ericsson	6.20	Discussion / Decision		Comments in S3-040380
S3-040237	Push versus pull based key management	Ericsson	6.20	Discussion / Decision		Covered by S3-040257
S3-040238	Pseudo-CR to 33.246: Authenticating user in MBMS with HTTP digest	Ericsson	6.20	Approval		Agreed in principle with changes. Incorporated in S3-040391
S3-040239	Order of MBMS UE context establishment and key delivery	**3**	6.20	Discussion / Decision		Order of MSK delivery and Bearer joining decision made by other groups or market factors. Noted at this time
S3-040240	MSK update rules	Huawei	6.20	Discussion / Decision		LS to SA WG4 in S3-040388
S3-040241	MBMS Pay per view charging model	Oberthur Card System	6.20	Discussion		Comments in S3-040354
S3-040242	OTA for MBMS	Axalto, Gemplus, Oberthur	6.20	Discussion / Decision		Same as S3-040247
S3-040243	MBMS UICC-based solution	Axalto, Gemplus, Oberthur	6.20	Discussion / Decision		Comments in S3-040256
S3-040244	Bearer level joining and application level joining for MBMS security	Samsung	6.20	Discussion / Decision		non-security related assumptions and would need to be agreed in other groups before SA WG3
S3-040245	MBMS MSK distribution procedure	Samsung	6.20	Discussion / Decision		clarification needed to distinguish between Service Subscription, Service Joining and Service Announcement
S3-040246	MBMS UICC-based solution	Axalto, Gemplus, Oberthur	6.20	Discussion / Decision		Same as S3-040243
S3-040247	OTA for MBMS	Axalto, Gemplus, Oberthur	6.20	Discussion / Decision		Comments in S3-040356
S3-040248	Pseudo-CR to 33.246: CR on MBMS key Management procedures	Axalto, Gemplus, Oberthur	6.20	Approval		LATE_MBMS_DOC. Comments in S3-040355. superseded by agreements made in discussions
S3-040249	MBMS key Management comparison	Axalto	6.20	Discussion / Decision		MBMS RESPONSE DOCUMENT. Comments in S3-040257
S3-040250	LS response (from SA WG5) to ITU-T SG 4 regarding Security of the Management Plane	SA WG5	5.1	Information		Noted. Considered in conjunction with S3-040214. E-mail comments to make LS in S3-040382

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040251	Proposed CR to 33.102: Clarification on Authentication re-attempt parameter (Rel-6)	NEC	6.5	Approval		Revised in S3-040400, LS in S3-040401
S3-040252	Reply LS (from SA WG2) to Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0	SA WG2	6.10	Information		Noted
S3-040253	LS (from SA WG2) on Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0	SA WG2	6.10	Action		D. Mariblanca to collect comments and agree reply by 7 June
S3-040254	LS from TSG GERAN: Use of Kc in the Uplink TDOA location method	TSG GERAN	6.14	Action		Duplicated in S3-040365
S3-040255	Reply (from TSG GERAN) to LS on 'Ciphering for Voice Group Call Services'.	TSG GERAN	6.21	Action		Response LS in S3-040428
S3-040256	Proposal about the efficient mechanism for the setup of UE-initiated tunnels (Scenario 3) in WLAN interworking	ETRI	6.10	Discussion / Decision		Many open issues to be solved. Noted
S3-040257	Comments to 232, 243 and 249	Ericsson	6.20	Discussion / Decision		Comments to S3-040232, S3-040243 and S3-040249
S3-040258	Extension payloads to MIKEY to support MBMS	Ericsson	6.20	Discussion		Encrypted MTK assumed as method to use. GBA-based solution chosen for MBMS
S3-040259	Key deletion in the UICC model using S3-04235	Ericsson	6.20	Discussion / Decision		Noted
S3-040260	Pseudo-CR to 33.246: Calculating validity for MIKEY message	Ericsson	6.20	Approval		Updated after discussion in S3-040392
S3-040261	Latest version of the MBMS TS	Rapporteur (A. Escott)	6.20	Discussion / Decision		Noted
S3-040262	Analysis of the authenticated GSM cipher command mechanism	Vodafone	6.6	Discussion / Decision		Presented and discussed
S3-040263	Evaluations of mechanisms to protect against Barkan-Biham-Keller attack	Vodafone	6.6	Discussion / Decision		Comments in S3-040371
S3-040264	Security for early IMS implementations	Vodafone	6.1	Discussion / Decision		Noted. Proposal in S3-040265. LS to SA2 in S3-040396
S3-040265	Interim security solution for early IMS implementations	Vodafone	6.1	Discussion / Decision		LS to SA2 in S3-040396
S3-040266	Proposed CR to 33.310: Removal of inconsistencies regarding SEG actions during IKE phase 1 (Rel-6)	Vodafone, Siemens, Nokia	6.4	Approval		Approved
S3-040267	Proposed CR to 33.310: Removal of unnecessary restriction on CA path length (Rel-6)	Vodafone, Siemens, Nokia	6.4	Approval		Approved
S3-040268	LS from ETSI SAGE: SAGE work on key derivation for the Generic Bootstrapping Architecture	ETSI SAGE	6.9.2			Response LS in S3-040408
S3-040269	Another Countermeasure for the Barkan-Biham-Keller Attack on A5/2	SFR	6.6	Presentation		Revised in S3-040389
S3-040270	Bluetooth Security Overview for TS 33.234 WLAN interworking security specification (Annex A4)	BT Group	6.10	Discussion / Decision		Related CR in S3-040271
S3-040271	Proposed CR to 33.234: Bluetooth security and configuration considerations for Wireless Local Area Network (WLAN) interworking security for TS 33.234 Annex A4 (Rel-6)	BT Group	6.10	Approval		Not agreed to include at this time. Delegates to consider content to add
S3-040272	Use of a Trusted Tunnel to Secure Local Terminal Interfaces	Intel Corporation, Gemplus	6.10	Discussion		Noted. To be considered for future work
S3-040273	Proposed CR to 33.102: Handling of key sets at inter-system change (Rel-5)	Siemens, Ericsson	6.5	Approval		~~Conditionally approved.~~ Checked if info is carried by other messages. Approved
S3-040274	Proposed CR to 33.102: Handling of key sets at inter-system change (Rel-6)	Siemens, Ericsson	6.5	Approval		~~Conditionally approved.~~ Checked if info is carried by other messages. Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040275	Proposed CR to 33.234: EAP in IKEv2 (Rel-6)	Nokia, Ericsson	6.10	Approval		Comments in S3-040372. Need stable IETF reference. E-mail discussion to progress
S3-040276	Proposed CR to 33.234: Introduction of UE split alternative 2 in TS 33.234 (Rel-6)	Nokia, Ericsson	6.10	Approval	S3-040422	Revised in S3-040422
S3-040277	Proposed CR to 33.234: Extension of IKEv2 and IPsec profiles (Rel-6)	Nokia, Ericsson	6.10	Approval	S3-040418	Revised in S3-040418
S3-040278	Proposed CR to 33.234: Sending of temporary identities from WLAN UE (Rel-6)	Nokia, Ericsson	6.10	Approval	S3-040416	Revised in S3-040416
S3-040279	EAP method policies and release 6 non-compliant implementations	Nokia, Ericsson	6.10	Discussion / Decision		Discussed and noted
S3-040280	Proposed CR to 33.234: Support of EAP SIM and AKA in AAA server and WLAN UE (Rel-6)	Nokia, Ericsson	6.10	Approval	S3-040420	Revised in S3-040420
S3-040281	Proposed CR to 33.234: Re-authentication failure notification to HSS (Rel-6)	Ericsson	6.10	Approval	S3-040421	Revised in S3-040421
S3-040282	Proposed CR to 33.234: Identity request procedure clarification (Rel-6)	Ericsson	6.10	Approval	S3-040423	Revised in S3-040423
S3-040283	Resolving the editors notes in Wireless Local Area Network (WLAN) interworking security 3GPP TS 33.234 V6.0.0 (2004-03)	BT Group	6.10	Discussion / Decision		Noted. C Blanchard to maintain for next meeting. Comments from delegates to C. Blanchard
S3-040284	Use of IKE in End-to-end tunneling	Nortel Networks	6.10	Discussion / Decision		Objection to proposal
S3-040285	Proposed CR to 33.234: Allow use of IKEv1 and IKEv2 with subscriber certificates (Rel-6)	Nortel Networks	6.10	Approval		Issue postponed pending further study on S3-040284
S3-040286	VGCS: Status of principles and further proceeding	Siemens, Vodafone	6.21	Discussion / Decision		LS to SAGE in S3-040426
S3-040287	Proposed CR to 43.020: Introducing VGCS/VBS ciphering (Rel-6)	Siemens, Vodafone	6.21	Approval	S3-040415	Revised in S3-040415
S3-040288	Proposed CR to 43.020: Introducing the special RAND mechanism with GSM/GPRS and WLAN separation (Rel-6)	Nokia	6.6	Approval		Comments in S3-040372. Used in A5/2 discussions
S3-040289	Draft TR 33.919 V1.2.1: Generic Authentication Architecture (GAA); System Description (Rel-6)	Rapporteur (Alcatel)	6.9.1	Information		Noted. To be sent to SA for info. C Blanchard to provide text for clause 7
S3-040290	Proposed CR to 33.220: Editorial corrections to TS 33.220 (Rel-6)	Alcatel	6.9.2	Approval	S3-040414	Revised in S3-040414
S3-040291	Proposed CR to 33.210: Diffie-Hellman groups in NDS/IP (Rel-6)	Nokia	6.3	Approval		Approved
S3-040292	Proposed CR to 33.221: Editorial change to correct the reference's sources (Rel-6)	Nokia	6.9.3	Approval		Postponed to next meeting. Chairman to ask SA about OMA referencing
S3-040293	Using SSC as optional in Presence service TS33.141	Nokia	6.18	Discussion / Decision		Needs clarification. Review at next meeting. E-mail discussion lead by Bengt
S3-040294	Pseudo-CR to 33.141: Applying NDS for Network side security for Presence	Nokia, Siemens	6.18	Approval		Agreed with modifications for inclusion in draft TS.
S3-040295	Pseudo-CR to 33.141: UE's identities in Presence server access	Nokia, Siemens	6.18	Approval		Agreed with modifications for inclusion in draft TS.
S3-040296	Proposed CR to 33.310: Correction of 'Extended key usage' extension in SEG Certificate profile (Rel-6)	Nokia, Vodafone	6.4	Approval		Approved
S3-040297	Proposed CR to 33.105: Correction of inconsistencies in AK computation for re-synchronisation (Rel-4)	Orange	6.5	Approval	S3-040402	Revised in S3-040402
S3-040298	Proposed CR to 43.020: Introducing the special RAND mechanism as a principle for GSM/GPRS (Rel-5)	Orange	6.6	Approval		Used in A5/2 discussions
S3-040299	Proposed CR to 33.102: Introducing the special RAND mechanism as a principle for GSM/GPRS (Rel-6)	Orange	6.6	Approval		Used in A5/2 discussions

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040300	Draft Report of SA WG3 LI Group meeting #13 (Rome, Italy)	SA WG3 LI Group	4.3	Information		Noted
S3-040301	Proposed CR to 33.106: Clarification on delivery of IRI and CC (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040302	Proposed CR to 33.107: Correction on Network initiated Mobile Station Detach signalling flow (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040303	Proposed CR to 33.107: TEL-URL missing in activation of LI in the CSCFs (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040304	Proposed CR to 33.107: Correction on the use of session initiator parameter (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040305	Proposed CR to 33.108: Correction on interception identities in multi-media domain (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040306	Proposed CR to 33.108: WGS 84 coordinates length correction (Rel-5)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040307	Proposed CR to 33.108: WGS 84 coordinates length correction (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040308	Proposed CR to 33.107: Correction to HLR interception event name (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040309	Proposed CR to 33.107: Clarification for Push to talk over Cellular (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040310	Proposed CR to 33.107: Adding an encryption parameter to IRI across X2 interface (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040311	Proposed CR to 33.108: CR offering alignment to ETSI TS 101 671 (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040312	Proposed CR to 33.107: References (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040313	Proposed CR to 33.108: Additional text for Definition and Acronym section (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040314	Proposed CR to 33.107: Enhancements for the Functional Architecture chapter (Rel-6)	SA WG3 LI Group	4.3	Approval		For e-mail approval
S3-040315	NAF remove the security associations	Huawei	6.9.2	Discussion / Decision	S3-040407	CR Revised in S3-040407
S3-040316	Validity condition set by NAF	Huawei	6.9.2	Discussion / Decision		Issue needs further discussion and development
S3-040317	User identity transform	Huawei	6.9.2	Discussion / Decision		Discussed and CR Rejected
S3-040318	Proposed CR to 33.203: Correction on IMS confidentiality protection (Rel-6)	Siemens	6.1	Approval		Revised in S3-040397
S3-040319	Text for sub-sections 6.4 “Interfaces” and 6.5 “Management of UE Identity” within section 6 “Authentication Proxy” of TS 33.222 – Pseudo-CR	Nokia, Siemens	6.9.4	Discussion / Decision		Agreed for inclusion in TS by the editor
S3-040320	New text for section 5.3 “Shared key-based UE authentication with certificate-based NAF authentication “of TS 33.222 – Pseudo-CR	Nokia, Siemens	6.9.4	Discussion / Decision		Agreed for inclusion in TS by the editor
S3-040321	Removal of Annex B of TS 33.222 – Pseudo-CR	Nokia, Siemens	6.9.4	Discussion / Decision		Agreed for inclusion in TS by the editor
S3-040322	General Requirements and Principles for Access to NAF using HTTPS – Pseudo-CR	Siemens	6.9.4	Discussion / Decision		Agreed for inclusion in TSs by the editors
S3-040323	Definition of TLS profile for shared key based UE authentication according to clause 5.3 of TS 33.222 – Pseudo-CRs to 33.222 and 33.141	Nokia, Siemens	6.9.4 / 6.18	Discussion / Decision		Agreed for inclusion in TSs by the editors
S3-040324	Editorial Modifications to the MBMS TS	Rapporteur (A. Escott)	6.20	Discussion / Decision		Agreed for inclusion in TS
S3-040325	Definition of Authentication Mechanisms in TS 33.222 – Pseudo-CR	Siemens	6.9.4	Discussion / Decision		5.3 mandatory for implementation, 5.4 kept and text added as optional, 5.5 text moved to inf. annex
S3-040326	[DRAFT] Reply LS on Requirements for transfer of GAA-User-Profile	Nokia, Siemens	6.9.2	Approval		To be discussed over e-mail for completion at next meeting
S3-040327	Proposed CR to 33.220: Terminology changes (Rel-6)	Nokia, Siemens	6.9.2	Approval		Alternative proposals by 7 June

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040328	Proposed CR to 33.220: NAF in visited network (Rel-6)	Nokia, Siemens	6.9.2	Approval	S3-040412	Revised in S3-040412
S3-040329	Proposed CR to 33.220: Editorial changes and clarifications to TS 33.220 (Rel-6)	Siemens	6.9.2	Approval	S3-040406	Revised in S3-040406
S3-040330	Proposed CR to 33.220: Removal of editors notes on Transaction Identifiers (Rel-6)	Siemens	6.9.2	Approval	S3-040410	Revised in S3-040410
S3-040331	Proposed CR to 33.220: Clarification of GBA specific profiles in HSS and over Zh and Zn reference points (Rel-6)	Siemens	6.9.2	Approval		Alternative proposals by 7 June
S3-040332	Proposed CR to 33.220: Multiple key derivation mandatory (Rel-6)	Siemens	6.9.2	Approval	S3-040409	Considered with S3-040334 and S3-040343. Revised in S3-040409
S3-040333	Proposed CR to 33.220: Removal of Annex A (Rel-6)	Siemens	6.9.2	Approval		Approved
S3-040334	Proposed CR to 33.220: Removal of key derivation options (Rel-6)	Nokia	6.9.2	Approval	S3-040409	Considered with S3-040332 and S3-040343. Revised in S3-040409
S3-040335	Proposed CR to 33.220: NAF's public hostname verification (Rel-6)	Nokia	6.9.2	Approval	S3-040411	Revised in S3-040411
S3-040336	Pseudo-CR: Subscriber certificate based authentication in GAA	Nokia	6.9.4	Discussion / Decision		Agreed to add refs to IETF and move to inf annex
S3-040337	Shared key TLS usage within Ua interface	Nokia	6.9.4	Discussion / Decision		Agreed that this should be optional for impl.
S3-040338	GUP security follow-up	Ericsson, Nokia	6.17	Discussion		Response LS in S3-040385
S3-040339	Pseudo-CR to 33.141: ISIM Support (Rel-6)	Nokia, Motorola, Gemplus, Alcatel	6.18	Approval		To be further developed for next meeting
S3-040340	Proposed CR to 33.220: Private identity for GBA procedure (Rel-6)	Nokia, Motorola, Gemplus, Alcatel	6.9.2	Approval		To be further developed for next meeting
S3-040341	Comparison of Suggested A5/2 Attack Countermeasures	Ericsson	6.6	Discussion		Discussed
S3-040342	Authenticated GBA transaction identifier	Ericsson	6.9.2	Discussion / Decision		Await results of related e-mail discussions
S3-040343	Multiple key derivation in GBA	Ericsson	6.9.2	Discussion / Decision	S3-040409	CR Considered with S3-040332 and S3-040334. Revised in S3-040409
S3-040344	Proposed CR to 33.220: Introduction of a UICC-based Generic Bootstrapping Architecture (Rel-6)	Siemens	6.9.2	Approval	S3-040413	Revised to include agreements at meeting in S3-040413
S3-040345	Comments on S3-040222: MBMS: Key distribution architectures analysis	Gemplus	6.20	Discussion / Decision		Comments to S3-040222
S3-040346	Comments on S3-040218: GBA_U: Bootstrapping secrets to the UICC	Siemens	6.9.2	Discussion / Decision		Comments to S3-040218
S3-040347	Pseudo CR to 33.141: Editorial Updates to draft TS 33.141	Ericsson	6.18	Approval		Agreed with modifications for inclusion in draft TS.
S3-040348	AP-AS Interface Protection	Ericsson	6.9.4 / 6.18	Discussion / Decision		Pseudo-CRs agreed with modifications for inclusion in draft TSs.
S3-040349	Presence Security Updates	Ericsson	6.18	Discussion / Decision		Agreed with modifications for inclusion in draft TS.
S3-040350	GBA_U: comments to S3-040217 and S3-040218	Gemplus	6.9.2	Discussion / Decision		Comments to S3-040217 and S3-040218
S3-040351	WLAN application	Gemplus	6.10	Discussion / Decision		More justification needed. Gemplus to discuss by e-mail (7 June) and supply for next meeting
S3-040352	Proposed CR to 33.234: WLAN handover scenario (Rel-6)	Nokia	6.10	Approval	S3-040417	CR revised in S3-040417
S3-040353	Proposed CR to 33.234: Requirement on keeping WLAN accessing keys independent from 3G accessing keys stored in USIM (Rel-6)	Nokia	6.10	Approval	S3-040424	CR revised in S3-040424

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040354	Comments to S3-040241: MBMS Pay per view charging model	Siemens	6.20	Discussion		Comments to S3-040241
S3-040355	Comments to S3-040248: Pseudo-CR to 33.246: CR on MBMS key Management procedures (Rel-6)	Siemens	6.20	Discussion		Comments to S3-040248. superseded by agreements made in discussions
S3-040356	Comments to S3-040247: OTA for MBMS	GemPlus	6.20	Discussion / Decision		Comments to S3-040247
S3-040357	Privacy handling for Rel-6	Nokia	6.1	Discussion / Decision		Companion CR in S3-040358
S3-040358	Proposed CR to 33.203: SIP Privacy mechanism when IMS interworking with non-IMS network (Rel-6)	Nokia	6.1	Approval	S3-040398	Revised in S3-040398
S3-040359	Pseudo-CR to 33.246: CR on MBMS key Management procedures (Rel-6)	AXALTO, Gemplus, OCS	6.20	Approval		Superseded by agreements made in discussions
S3-040360	Eavesdropping without breaking the GSM encryption algorithm	Lucent Technologies	6.6	Discussion / Decision		Presented using slides.
S3-040361	Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces) (Rel-6)	Toshiba and supporting Companies	6.10	Approval		WITHDRAWN - Revised in S3-040379
S3-040362	LS from CN WG4: Application Layer vs Transport Layer security for GUP	CN WG4	6.17	Action		Response LS in S3-040385
S3-040363	Reply LS (from SA WG2) on HTTP based services and order of procedures	SA WG2	6.20	Action		Responses Noted
S3-040364	LS (from SA WG2) on moving security requirements to SA3 MBMS TS	SA WG2	6.20	Action		Pseudo-CR and LS in S3-040386 and S3-040387
S3-040365	LS from TSG GERAN: Use of Kc in the Uplink TDOA location method	TSG GERAN	6.14	Action		CR endorsed. LS in S3-040404
S3-040366	Reply (from TSG GERAN) to LS on 'Ciphering for Voice Group Call Services'	TSG GERAN	6.21	Action		WITHDRAWN - Same as S3-040255
S3-040367	Reply LS (from SA WG2) to Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0	SA WG2	6.10	Information		WITHDRAWN - Same As S3-040252
S3-040368	LS (from SA WG2) on Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0	SA WG2	6.10	Action		WITHDRAWN - Same As S3-040253
S3-040369	LS (from T WG2) on Potential Security issues relating to use of AT Commands to access UICC	T WG2	5.1	Action		Off-line check and response LS in S3-040383
S3-040370	LS (from T WG3) on VGCS and VBS security	T WG3	6.21	Action		Reply LS in S3-040425
S3-040371	Comments to: S3-040263 Evaluations of mechanisms to protect against Barkan-Biham-Keller attack	Orange	6.6	Discussion / Decision		Comments to S3-040263. Reaction in S3-040377
S3-040372	Comments on S3-040275 (Ericsson, Nokia) and S3-040288 (Nokia) relating to PDG authentication using IKEv2 in scenario 3	Siemens	6.10	Discussion / Decision		Comments to S3-040275 and S3-040288
S3-040373	Reply (from SA WG2) to Liaison on Service Discovery of BSF and PKI portal	SA WG2	6.9.2	Action		Operators to consider and CRs to be produced
S3-040374	LS (from SA WG2) on non-compliance to IMS security	SA WG2	6.1	Action		Proposal in S3-040265. Response LS in S3-040396
S3-040375	LS from SA WG2: MMS over 3GPP Interworking WLANs	SA WG2	6.10	Information		Noted
S3-040376	A5/2 withdrawal from handsets	GSMA Security Group, SG Chairman	6.6	Action		LS to impacted groups in S3-040403
S3-040377	Reaction to S3-040371: Comments to S3-040263 Evaluations of mechanisms to protect against Barkan-Biham-Keller attack	Vodafone	6.6	Discussion / Decision		Reaction to comments to S3-040263 in S3-040371
S3-040378	Proposed CR to 33.220: Generic Ua interface requirements	Nokia	6.9.2	Approval		LATE_DOC - For e-mail discussion by 7 June

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040379	Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces) (Rel-6)	Toshiba and supporting Companies	6.10	Approval		LATE_DOC Delegates to consider inclusion of recs and reqts in spec set by next meeting and contribute proposals
S3-040380	Comments to S3-040236: Joining based key management	Ericsson	6.20	Discussion / Decision		Comments to S3-040236
S3-040381	Initial discussion on security requirements in the OTA server interfaces	Axalto Systems	6.20	Discussion		LATE_DOC Noted.
S3-040382	Reserved for Response to 214 and 250	Yingxin (Huawai)	5.1 / e-mail	Approval		For Email discussion and approval
S3-040383	Reply LS on Potential Security issues relating to use of AT Commands to access UICC	SA WG3	5.1	Approval		Approved
S3-040384	LS on new ITU-T Recommendations for secure mobile end-to-end data communication, X.1121 and X.1122	SA WG3	5.7	Approval		Approved
S3-040385	LS on GUP security status in SA3 and on collaboration of 3GPP and Liberty Alliance Project	SA WG3	5.17	Approval		Approved
S3-040386	Pseudo-CR to 33.246: Adding requirements for SA WG2	**3**	6.20	Approval		Agreed for inclusion in the draft TS
S3-040387	LS to SA2 informing them of requirements added to 33.246	SA WG3	6.20	Approval	S3-040442	Revised in S3-040442
S3-040388	LS to S4, S2 on Delay for key request	SA WG3	6.20	Approval	S3-040444	Revised in S3-040444
S3-040389	Another Countermeasure for the Barkan-Biham-Keller Attack on A5/2	SFR	6.6	Presentation		Noted
S3-040390	LS to SA ans S1 on UICC and ME solutions for MBMS	SA WG3	6.20	Approval	S3-040445	Revised in S3-040445
S3-040391	Pseudo-CR to cover 238 and 219	SA WG3	6.20	Approval		Agreed for inclusion in the draft TS
S3-040392	Pseudo-CR to 33.246: Calculating validity for MIKEY message	Ericsson	6.20	Approval		Agreed for inclusion in the draft TS
S3-040393	[DRAFT] LS on Protection of streaming and download MBMS data	SA WG3	6.20	Approval	S3-040443	Revised in S3-040443
S3-040394	Profiling of IKEv2 and ESP for NAT traversal	Siemens	6.10	Discussion / Decision		Noted. CR in S3-040395
S3-040395	Proposed CR to 33.234: Profiling of IKEv2 and ESP for NAT traversal (Rel-6)	Siemens	6.10	Approval		Approved
S3-040396	LS on non-compliance to IMS security	SA WG3	5.1	Approval		Approved
S3-040397	Proposed CR to 33.203: Correction on IMS confidentiality protection (Rel-6)	Siemens	6.1	Approval		Approved
S3-040398	Proposed CR to 33.203: SIP Privacy mechanism when IMS interworking with non-IMS network (Rel-6)	Nokia	6.1	Approval	S3-040429	Revised in S3-040429
S3-040399	[DRAFT] Reply LS on "Re-authentication and key set change during inter-system handover"	SA WG3	6.5	Approval	S3-040436	Revised in S3-040436
S3-040400	Proposed CR to 33.102: Clarification on Authentication re-attempt parameter (Rel-6)	SA WG3	6.5	Approval		Approved
S3-040401	Reply LS to N4-040247 (S3-040208) on use of authentication re-attempt IE	SA WG3	6.5	Approval	S3-040430	Revised in S3-040430
S3-040402	Proposed CR to 33.105: Correction of inconsistencies in AK computation for re-synchronisation (Rel-4)	Orange	6.6	Approval		Approved
S3-040403	LS on removal of A5/2 support	SA WG3	6.6	Approval	S3-040431	Revised in S3-040431
S3-040404	Reply LS on the use of Kc in the Uplink TDOA location method	SA WG3	6.14	Approval		Approved
S3-040405	Invitation to the 3GPP and TISPAN joint Workshop to be held on 22 - 23 June 2004 in Mediathel in Sophia Antipolis	SA WG3 Secretary	8	Information		Noted
S3-040406	Proposed CR to 33.220: Editorial changes and clarifications to TS 33.220 (Rel-6)	Alcatel, Siemens	6.9.2	Approval	S3-040433	Revised in S3-040433
S3-040407	Proposed CR to 33.220: NAF remove the security associations (Rel-6)	Huawei	6.9.2	Approval		Approved
S3-040408	[DRAFT] Response to LS (S3-040268) on key derivation for the Generic Bootstrapping Architecture	SA WG3	6.9.2	Approval	S3-040448	Revised in S3-040448
S3-040409	Proposed CR to 33.220: Multiple key derivation mandatory (Rel-6)	Siemens	6.9.2	Approval	S3-040434	Revised in S3-040434

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040410	Proposed CR to 33.220: Removal of editors notes on Transaction Identifiers (Rel-6)	Siemens	6.9.2	Approval		Approved
S3-040411	Proposed CR to 33.220: NAF's public hostname verification (Rel-6)	Nokia	6.9.2	Approval	S3-040435	Revised in S3-040435
S3-040412	Proposed CR to 33.220: NAF in visited network (Rel-6)	Nokia, Siemens	6.9.2	Approval	S3-040432	Revised in S3-040432
S3-040413	Proposed CR to 33.220: Introduction of a UICC-based Generic Bootstrapping Architecture (Rel-6)	Siemens	6.9.2	Approval		Approved
S3-040414	Proposed CR to 33.220: Editorial corrections to TS 33.220 (Rel-6)	Alcatel	6.9.2	Approval		Approved
S3-040415	Proposed CR on VGCS	Siemens	6.21	Endorsement		Principles agreed if issues are found to be OK. Revision marked version in S3-040427
S3-040416	Proposed CR to 33.234: Sending of temporary identities from WLAN UE (Rel-6)	Nokia, Ericsson	6.10	Approval		Approved
S3-040417	Proposed CR to 33.234: WLAN handover scenario (Rel-6)	Nokia	6.10	Approval	S3-040440	Revised in S3-040440
S3-040418	Proposed CR to 33.234: Extension of IKEv2 and IPsec profiles (Rel-6)	Nokia, Ericsson	6.10	Approval		Approved
S3-040419	Liaison statement (from SA WG1) on Network Protection against Virus Infected Mobiles	SA WG1	9	Information		Noted
S3-040420	Proposed CR to 33.234: Support of EAP SIM and AKA in AAA server and WLAN UE (Rel-6)	Nokia, Ericsson	6.10	Approval		Approved
S3-040421	Proposed CR to 33.234: Re-authentication failure notification to HSS (Rel-6)	Ericsson	6.10	Approval	S3-040438	Revised in S3-040438
S3-040422	Proposed CR to 33.234: Introduction of UE split alternative 2 in TS 33.234 (Rel-6)	Nokia, Ericsson	6.10	Approval	S3-040437	Revised in S3-040437
S3-040423	Proposed CR to 33.234: Identity request procedure clarification (Rel-6)	Ericsson	6.10	Approval	S3-040439	Revised in S3-040439
S3-040424	Proposed CR to 33.234: Requirement on keeping WLAN accessing keys independent from 3G accessing keys stored in USIM (Rel-6)	Nokia	6.10	Approval	S3-040440	Revised in S3-040441
S3-040425	Reply LS to T3-040329 (S3-040370) on VGCS and VBS security	SA WG3	6.21	Approval		Approved
S3-040426	Liaison Statement on VGCS and VBS security	SA WG3	6.21	Approval	S3-040446	Revised in S3-040446
S3-040427	Proposed CR to 43.020: Introducing VGCS/VBS ciphering	Siemens, Vodafone	6.21	Information		Noted for adding to LSs
S3-040428	LS to impacted WGs on VGCS/VBS ciphering	SA WG3	6.21	Approval	S3-040447	Revised in S3-040447
S3-040429	Proposed CR to 33.203: SIP Privacy mechanism when IMS interworking with non-IMS network (Rel-6)	Nokia	6.1	Approval		Approved
S3-040430	Reply LS to N4-040247 (S3-040208) on use of authentication re-attempt IE	SA WG3	6.5	Approval		Approved
S3-040431	LS on removal of A5/2 from handsets	SA WG3	6.6	Approval		Approved
S3-040432	Proposed CR to 33.220: NAF in visited network (Rel-6)	Nokia, Siemens	6.9.2	Approval		Approved
S3-040433	Proposed CR to 33.220: Editorial changes and clarifications to TS 33.220 (Rel-6)	Alcatel, Siemens	6.9.2	Approval		Approved
S3-040434	Proposed CR to 33.220: Multiple key derivation mandatory (Rel-6)	Siemens	6.9.2	Approval		Approved
S3-040435	Proposed CR to 33.220: NAF's public hostname verification (Rel-6)	Nokia	6.9.2	Approval		Approved
S3-040436	Reply LS on "Re-authentication and key set change during inter-system handover"	SA WG3	6.5	Approval		Approved
S3-040437	Proposed CR to 33.234: Introduction of UE split alternative 2 in TS 33.234 (Rel-6)	Nokia, Ericsson	6.10	Approval		Approved
S3-040438	Proposed CR to 33.234: Re-authentication failure notification to HSS (Rel-6)	Ericsson	6.10	Approval		Approved
S3-040439	Proposed CR to 33.234: Identity request procedure clarification (Rel-6)	Ericsson	6.10	Approval		Approved
S3-040440	Proposed CR to 33.234: WLAN handover scenario (Rel-6)	Nokia	6.10	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040441	Proposed CR to 33.234: Requirement on keeping WLAN accessing keys independent from 3G accessing keys stored in USIM (Rel-6)	Nokia	6.10	Approval		Approved
S3-040442	Response to LS (S2-041630 = S3-040364) on moving security requirements to SA3 MBMS TS	SA WG3	6.20	Approval		Approved
S3-040443	LS on Protection of streaming and download MBMS data	SA WG3	6.20	Approval		Approved
S3-040444	LS on MBMS MSK key update	SA WG3	6.20	Approval		Approved
S3-040445	LS on MBMS key Management	SA WG3	6.20	Approval		Approved
S3-040446	Liaison Statement on VGCS and VBS security	SA WG3	6.21	Approval		Approved
S3-040447	Liaison Statement on VGCS and VBS security	SA WG3	6.21	Approval		Approved
S3-040448	Response to LS (S3-040268) on key derivation for the Generic Bootstrapping Architecture	SA WG3	6.9.2	Approval		Approved
S3-040449	Update of Editor's note in TS to reflect decisions made in SA3#33	Editor (A. Escott)	6.20	Discussion / Decision		Comments by e-mail 24 May for finalisation 28 May

Annex C: Status of specifications under SA WG3 responsibility

Type	Number	Title	Ver at SA3#33	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	TSG#10:8.1.0
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. Created from 02.31 R99.
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). SP-16: Takes over from 02.32 R99.
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. Created from 03.31 R99.
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). SP-16: takes over from 03,35 R99.
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 Formerly 33.904.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	3.2.0	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
Release 4 3GPP Specifications and Reports							
TS	21.133	3G security; Security threats and requirements	4.1.0	Rel-4	S3	CHRISTOFFERSSON, Per	
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	4.1.0	Rel-4	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
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. Created from 42.031 Rel-4.
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). SP-16: Takes over from 42.032 Rel-4.
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. Created from 43.031 Rel-4.
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). SP-16: takes over from 43.035 Rel-4
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	SP-15: Not to be promoted to Rel-5.
TS	33.105	Cryptographic Algorithm requirements	4.1.0	Rel-4	S3	CHIKAZAWA, Takeshi	SP-15: Not to be promoted to Rel-5.
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	SP-15: Not to be promoted to Rel-5.
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	SP-15: Not to be promoted to Rel-5.
TR	33.902	Formal Analysis of the 3G Authentication Protocol	4.0.0	Rel-4	S3	HORN, Guenther	SP-15: Not to be promoted to Rel-5.
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 SP-15: Not to be promoted to Rel-5.
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. SP-15: Not to be promoted to Rel-5.
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. TSG#11:changed to Rel-4.
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 TSG#11:changed to Rel-4
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 TSG#11:changed to Rel-4

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:changed to Rel-4
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 TSG#11:Formerly 35.209 Rel-99 (but never made available)
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	SP-15: Not to be promoted to Rel-5.
TS	42.009	Security Aspects	4.0.0	Rel-4	S3	CHRISTOFFERSSON, Per	SP-15: Not to be promoted to Rel-5.
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. Created from 42.031 Rel-5.
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. Created from 43.031 Rel-5.
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)	5.7.0	Rel-5	S3	WILHELM, Berthold	2001-12-04 Title changed from "Lawful Interception; Interface between core network and law agency equipment" (Berthold.Wilhelm@RegTP.de). .
TS	33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	5.1.0	Rel-5	S3	ESCOTT, Adrian	2001-05-24: title grows MAP; see 33.210 for IP equivalent. .
TS	33.201	Access domain security	none	Rel-5	S3	POPE, Maurice	.
TS	33.203	3G security; Access security for IP-based services	5.8.0	Rel-5	S3	BOMAN, Krister	
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	5.5.0	Rel-5	S3	KOIEN, Geir	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210).
TR	33.900	Guide to 3G security	0.4.1	Rel-5	S3	BROOKSON, Charles	.
TR	33.903	Access Security for IP based services	none	Rel-5	S3	VACANT,	.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.205	3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE. 2002-06: clarified that deliverable is TS not TR. .
TS	35.206	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification	5.1.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TS	35.207	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	5.0.0	Rel-5	S3	WRIGHT, Tim	.
TR	41.033	Lawful Interception requirements for GSM	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
TS	42.033	Lawful Interception; Stage 1	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
TS	43.020	Security-related network functions	5.0.0	Rel-5	S3	GILBERT, Henri	.
TS	43.033	Lawful Interception; Stage 2	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
Release 6 3GPP Specifications and Reports							
TS	33.102	3G security; Security architecture	6.0.0	Rel-6	S3	BLOMMAERT, Marc	.
TS	33.106	Lawful interception requirements	6.0.0	Rel-6	S3	WILHELM, Berthold	.
TS	33.107	3G security; Lawful interception architecture and functions	6.1.0	Rel-6	S3	WILHELM, Berthold	.
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	6.5.0	Rel-6	S3	WILHELM, Berthold	2001-12-04 Title changed from "Lawful Interception; Interface between core network and law agency equipment" (Berthold.Wilhelm@RegTP.de). .
TS	33.141	Presence service; Security	1.1.1	Rel-6	S3	BOMAN, Krister	.
TS	33.203	3G security; Access security for IP-based services	6.2.0	Rel-6	S3	BOMAN, Krister	.
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	6.4.0	Rel-6	S3	KOIEN, Geir	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210). .
TS	33.220	Generic Authentication Architecture (GAA); Generic bootstrapping architecture	6.0.0	Rel-6	S3	HAUKKA, Tao	WI = SEC1-SC (UID 33002) Based on 33.109 §4. .
TS	33.221	Generic Authentication Architecture (GAA); Support for subscriber certificates	6.0.0	Rel-6	S3	HAUKKA, Tao	WI = SEC1-SC (UID 33002) Based on 33.109 §5 & annex A. .
TS	33.222	Generic Authentication Architecture (GAA); Access to network application functions using secure hypertext transfer protocol (HTTPS)	0.2.0	Rel-6	S3	SAHLIN, Bengt	WI = SEC1-SC (UID 33002) Based on 33.109 v0.3.0 protocol B. .
TS	33.234	3G security; Wireless Local Area Network (WLAN) interworking security	6.0.0	Rel-6	S3	LOPEZ SORIA, Luis	.

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	33.246	3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)	1.1.1	Rel-6	S3	ESCOTT, Adrian	SP-22: target for v2.0.0 is SP-23, but this will be challenging.
TS	33.310	Network domain security; Authentication framework (NDS/AF)	6.0.0	Rel-6	S3	VIITANEN, Tommi	.
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. SP-17: expect v2.0.0 at SP-18.
TR	33.817	Feasibility study on (Universal) Subscriber Interface Module (U)SIM security reuse by peripheral devices on local interfaces	6.0.0	Rel-6	S3	YAQUB, Raziq	Original WID = SP-030341. 2003-11-26: S3 Secretary indicates that TR is to be internal, so number changed from 33.917. .
TR	33.919	Generic Authentication Architecture (GAA); System description	1.2.1	Rel-6	S3	VAN MOFFAERT, Annelies	WI = SEC1-SC (UID 33002) .
TR	33.941	Presence service; Security	0.6.0	Rel-6	S3	BOMAN, Krister	.
TS	55.205	Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8	6.1.0	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	2003-09-30: Note: document only available with French export license. .
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	2003-09-30: Note: document only available with French export license. .
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	2003-09-30: Note: document only available with French export license. .
TS	55.226	Specification of the A5/4 encryption algorithms for GSM and ECSD, and the GEA4 encryption algorithm for GPRS; Document 1: A5/4 and GEA4 specification	1.0.0	Rel-6	S3	CHRISTOFFERSSON, Per	Work item UID = 1571 (SEC1) SP-23: likely that this will -> Rel-7
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	2003-09-30: Note: document only available with French export license. .

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

To be updated after e-mail approval of SA WG3 LI CRs.

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WI
33.102	183	-	Rel-6	Clarification on Authentication re-attempt parameter	F	6.0.0	S3-33	S3-040400	SEC1
33.102	184	-	Rel-5	Handling of key sets at inter-system change	F	5.3.0	S3-33	S3-040273	SEC-NDS
33.102	185	-	Rel-6	Handling of key sets at inter-system change	A	6.0.0	S3-33	S3-040274	SEC-NDS
33.105	021	-	Rel-4	Correction of inconsistencies in AK computation for re-synchronisation	F	4.1.0	S3-33	S3-040402	SEC1
33.106	007	-	Rel-6	Clarification on delivery of IRI and CC For e-mail approval	F	6.0.0	S3-33	S3-040301	SEC1-LI
33.107	036	-	Rel-6	Correction on Network initiated Mobile Station Detach signalling flow For e-mail approval	F	6.1.0	S3-33	S3-030302	SEC1-LI
33.107	037	-	Rel-6	TEL-URL missing in activation of LI in the CSCFs For e-mail approval	F	6.1.0	S3-33	S3-030303	SEC1-LI
33.107	038	-	Rel-6	Correction on the use of session initiator parameter For e-mail approval	F	6.1.0	S3-33	S3-030304	SEC1-LI
33.107	039	-	Rel-6	Correction to HLR interception event name For e-mail approval	F	6.1.0	S3-33	S3-030308	SEC1-LI
33.107	040	-	Rel-6	Clarification for Push to talk over Cellular For e-mail approval	F	6.1.0	S3-33	S3-030309	SEC1-LI
33.107	041	-	Rel-6	Adding an encryption parameter to IRI across X2 interface For e-mail approval	F	6.1.0	S3-33	S3-030310	SEC1-LI
33.107	042	-	Rel-6	References For e-mail approval	F	6.1.0	S3-33	S3-030312	SEC1-LI
33.107	043	-	Rel-6	Enhancements for the Functional Architecture chapter For e-mail approval	F	6.1.0	S3-33	S3-030314	SEC1-LI
33.108	045	-	Rel-6	Correction on interception identities in multi-media domain For e-mail approval	F	6.5.0	S3-33	S3-040305	SEC1-LI
33.108	046	-	Rel-5	WGS 84 coordinates length correction For e-mail approval	F	5.7.0	S3-33	S3-040306	SEC1-LI
33.108	047	-	Rel-6	WGS 84 coordinates length correction For e-mail approval	A	6.5.0	S3-33	S3-040307	SEC1-LI
33.108	048	-	Rel-6	CR offering alignment to ETSI TS 101 671 For e-mail approval	F	6.5.0	S3-33	S3-040311	SEC1-LI
33.108	049	-	Rel-6	Additional text for Definition and Acronym section For e-mail approval	F	6.5.0	S3-33	S3-040313	SEC1-LI
33.203	066	-	Rel-6	Correction on IMS confidentiality protection	F	6.2.0	S3-33	S3-040397	IMS-ASEC
33.203	067	-	Rel-6	SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network	F	6.2.0	S3-33	S3-040429	IMS-ASEC
33.210	016	-	Rel-6	Diffie-Hellman groups in NDS/IP	F	6.4.0	S3-33	S3-040291	SEC-NDS-IP
33.220	001	-	Rel-6	Removal of Annex A	D	6.0.0	S3-33	S3-040333	SEC1-SC
33.220	002	-	Rel-6	NAF remove the security associations	F	6.0.0	S3-33	S3-040407	SEC1-SC
33.220	003	-	Rel-6	Removal of editors notes on Transaction Identifiers	D	6.0.0	S3-33	S3-040410	SEC1-SC
33.220	004	-	Rel-6	Introduction of a UICC-based Generic Bootstrapping Architecture	B	6.0.0	S3-33	S3-040413	SEC1-SC
33.220	005	-	Rel-6	Editorial corrections to TS 33.220	D	6.0.0	S3-33	S3-040414	SEC1-SC
33.220	006	-	Rel-6	Support for NAF in visited network	B	6.0.0	S3-33	S3-040432	SEC1-SC
33.220	007	-	Rel-6	Editorial changes and clarifications to TS 33.220	D	6.0.0	S3-33	S3-040433	SEC1-SC
33.220	008	-	Rel-6	Multiple key derivation mandatory	C	6.0.0	S3-33	S3-040434	SEC1-SC
33.220	009	-	Rel-6	NAF's public hostname verification	C	6.0.0	S3-33	S3-040435	SEC1-SC
33.234	001	-	Rel-6	Profiling of IKEv2 and ESP for NAT traversal	F	6.0.0	S3-33	S3-040395	WLAN
33.234	002	-	Rel-6	Sending of temporary identities from WLAN UE	F	6.0.0	S3-33	S3-040416	WLAN
33.234	003	-	Rel-6	Extension of IKEv2 and IPsec profiles	F	6.0.0	S3-33	S3-040418	WLAN
33.234	004	-	Rel-6	Support of EAP SIM and AKA in AAA server and WLAN UE	F	6.0.0	S3-33	S3-040420	WLAN
33.234	005	-	Rel-6	Introduction of UE split alternative 2 in TS 33.234	F	6.0.0	S3-33	S3-040437	WLAN
33.234	006	-	Rel-6	Re-authentication failure notification to HSS	F	6.0.0	S3-33	S3-040438	WLAN
33.234	007	-	Rel-6	Identity request procedure clarification	F	6.0.0	S3-33	S3-040439	WLAN
33.234	008	-	Rel-6	WLAN mechanism to allow restrictions on simultaneous sessions	C	6.0.0	S3-33	S3-040440	WLAN
33.234	009	-	Rel-6	Requirement on keeping WLAN access keys independent from 2G/3G access keys stored in USIM	F	6.0.0	S3-33	S3-040441	WLAN
33.310	001	-	Rel-6	Removal of inconsistencies regarding SEG actions during IKE phase 1	F	6.0.0	S3-33	S3-040266	SEC1-NDS-AF
33.310	002	-	Rel-6	Removal of unnecessary restriction on CA path length	F	6.0.0	S3-33	S3-040267	SEC1-NDS-AF
33.310	003	-	Rel-6	Correction of 'Extended key usage' extension in SEG Certificate profile	F	6.0.0	S3-33	S3-040296	SEC1-NDS-AF

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	From	Source TD	Comment/Status
S3-040206	Liaison (from Download+DRM) to 3GPP SA4 and SA3 on DRM for PSS and MBMS streams	OMA Download+DRM	OMA-BAC-DLDRM-2004-0017R2	Noted
S3-040207	LS (from CN WG1) on Re-authentication and key set change during inter-system handover	CN WG1	N1-040501	Response LS in S3-040399
S3-040208	Reply LS (from CN WG4) to S3-040187(N4-040240) on use of authentication re-attempt IE	CN WG4	N4-040247	Proposed CR in S3-040251
S3-040209	LS (from CN WG4) on Relationship between 3GPP and Liberty Alliance related to GUP work	CN WG4	N4-040262	Response LS in S3-040385
S3-040210	LS (from CN WG4) on Requirements for transfer of GAA-User-Profile	CN WG4	N4-040352	Response LS in S3-040405
S3-040211	Response (from SA WG2) to LS on “IMS messaging, Group management and Presence work overlap between 3GPP and OMA”	SA WG2	S2-041050	Noted
S3-040212	Reply LS (from SA WG4) on “LS on HTTP based services and order of procedures”	SA WG4	S4-040133	Noted
S3-040213	Reply (from SA WG4) to “LS on service announcement and UE joining procedure”	SA WG4	S4-040157	Noted
S3-040214	LS (from SA WG5) on Security of the Management Plane	SA WG5	S5-046209	Related to S3-040250. E-mail comments to make LS in S3-040382
S3-040215	LS Reply (from TSG SA) to Request for close cooperation on future NGN Standardisation	TSG SA	SP-040218	Noted
S3-040223	LS from ITU-T SG17: Information of new ITU-T Recommendations for secure mobile end-to-end data communication, X.1121 and X.1122	ITU-T SG17	COM17-LS31	Response in S3-040384
S3-040250	LS response (from SA WG5) to ITU-T SG 4 regarding Security of the Management Plane	SA WG5	S5-046378	Noted. Considered in conjunction with S3-040214. E-mail comments to make LS in S3-040382
S3-040252	Reply LS (from SA WG2) to Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0	SA WG2	S2-041646	Noted
S3-040253	LS (from SA WG2) on Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0	SA WG2	S2-041648	D. Mariblanca to collect comments and agree reply by 7 June
S3-040255	Reply (from TSG GERAN) to LS on ‘Ciphering for Voice Group Call Services’.	TSG GERAN	GP-041210	Response LS in S3-040428
S3-040268	LS from ETSI SAGE: SAGE work on key derivation for the Generic Bootstrapping Architecture	ETSI SAGE	SAGE (04) 01	Response LS in S3-040408
S3-040362	LS from CN WG4: Application Layer vs Transport Layer security for GUP	CN WG4	N4-040488	Response LS in S3-040385
S3-040363	Reply LS (from SA WG2) on HTTP based services and order of procedures	SA WG2	S2-041629	Responses Noted
S3-040364	LS (from SA WG2) on moving security requirements to SA3 MBMS TS	SA WG2	S2-041630	Pseudo-CR and LS in S3-040386 and S3-040387
S3-040365	LS from TSG GERAN: Use of Kc in the Uplink TDOA location method	TSG GERAN	GP-041195	CR endorsed. LS in S3-040404
S3-040369	LS (from T WG2) on Potential Security issues relating to use of AT Commands to access UICC	T WG2	T2-040230	Off-line check and response LS in S3-040383
S3-040370	LS (from T WG3) on VGCS and VBS security	T WG3	T3-040329	Reply LS in S3-040425
S3-040373	Reply (from SA WG2) to Liaison on Service Discovery of BSF and PKI portal	SA WG2	S2-041665	Operators to consider and CRs to be produced
S3-040374	LS (from SA WG2) on non-compliance to IMS security	SA WG2	S2-041674	Proposal in S3-040265. Response LS in S3-040396

TD number	Title	From	Source TD	Comment/Status
S3-040375	LS from SA WG2: MMS over 3GPP Interworking WLANs	SA WG2	S2-041675	Noted
S3-040419	Liaison statement (from SA WG1) on Network Protection against Virus Infected Mobiles	SA WG1	S1-040483	Noted

E.2 Liaisons from the meeting

TD number	Title	TO	CC
S3-040383	Reply LS on Potential Security issues relating to use of AT Commands to access UICC	**T WG2**	**T WG3**
S3-040384	LS on new ITU-T Recommendations for secure mobile end-to-end data communication, X.1121 and X.1122	**ITU-T SG17**	**SA WG3-LI, ETSI TC-LI**
S3-040385	LS on GUP security status in SA3 and on collaboration of 3GPP and Liberty Alliance Project	**CN WG4, SA WG2**	**-**
S3-040396	LS on non-compliance to IMS security	**SA WG2**	**CN WG4, ETSI TISPAN**
S3-040404	Reply LS on the use of Kc in the Uplink TDOA location method	**TSG GERAN**	**-**
S3-040425	Reply LS to T3-040329 (S3-040370) on VGCS and VBS security	**T WG3**	**-**
S3-040430	Reply LS to N4-040247 (S3-040208) on use of authentication re-attempt IE	**CN WG4**	**CN WG1**
S3-040431	LS on removal of A5/2 from handsets	**SA WG1, T WG1, T WG2, GERAN WG2**	**GSMA SG, DIG**
S3-040436	Reply LS on "Re-authentication and key set change during inter-system handover"	**CN WG1**	**RAN WG2, RAN WG3**
S3-040442	Response to LS (S2-041630 = S3-040364) on moving security requirements to SA3 MBMS TS	**SA WG2**	**-**
S3-040443	LS on Protection of streaming and download MBMS data	**SA WG4**	**OMA Download + DRM**
S3-040444	LS on MBMS MSK key update	**SA WG4**	**SA WG2**
S3-040445	LS on MBMS key Management	**SA WG1, T WG3, SA WG4**	**-**
S3-040446	Liaison Statement on VGCS and VBS security	**ETSI SAGE**	**-**
S3-040447	Liaison Statement on VGCS and VBS security	**SA WG1, CN WG1, CN WG4, GERAN WG2, T WG3**	**ETSI EP RT**
S3-040448	Response to LS (S3-040268) on key derivation for the Generic Bootstrapping Architecture	**ETSI SAGE**	**-**
S3-040382	~~Reserved for Response to 214 and 250 (e-mail approval)~~Reply LS on Security of the Management Plane	**SA WG5, ITU-T SG4**	**-**
S3-040464	Reply LS on Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0	**Wi-Fi Alliance**	**CN WG1, CN WG3, CN WG4, SA WG2, SA WG5/SWG-B**

Annex F: Actions from the meeting

AP 33/01: Yingxin (Huawei) agreed to collect comments on the ITU-T Security of the Management Plane document over e-mail by 18 May 2004 and provide a new LS by 20 May in order to approve and send the LS by 24 May to the ITU-T electronic meeting 25 May 2004.

AP 33/02: T Haukka to start an e-mail discussion on TD S3-040357. Comments to be provided by 11 June 2004 for reporting the result of the discussions to the next meeting.

AP 33/03: SA WG3 Chairman to report to TSG SA the proposal to remove the use of A5/2.

AP 33/04: C. Brookson to run an e-mail discussion on protection mechanisms against the fraud potential implied by the A5/2 weaknesses (and potential future attacks against other A5/x algorithms) and report conclusions to next SA WG3 meeting.

AP 33/05: C. Blanchard to provide contribution to clause 7 of TR 33.919 at next SA WG3 meeting.

AP 33/06: Operators to consider the default domain name suggestion by SA WG2 in TD S3-040373 and contribute to the next meeting.

AP 33/07: D. Mariblanca to collect comments for the WiFi Alliance document in TD S3-040253. Deadlines: Comments by 31 May 2004. Draft reply by 2 June 2004. Approval of reply by 7 June 2004.

AP 33/08: C. Blanchard to lead an e-mail discussion on (U)SIM Security re-use by Peripheral devices. Final comments by 22 June for input to next meeting.