3GPP TSG SA WG3 Security — S3#33 **S3-040203**
10 - 14 May 2004
Beijing, China

3GPP TSG SA WG3 (Security) meeting #32 **Draft Report**

9-13 February 2004

Edinburgh, Scotland, UK

Source: **Secretary, SA WG3 (Maurice Pope, MCC)**

Title: **Draft Report of SA WG3 meeting#32**

Status: **Draft for Approval** **Version 0.0.8 (with revision marks)**

Edinburgh Castle

Contents

1 Opening of the meeting 4

2 Agreement of the agenda and meeting objectives 4
2.1 3GPP IPR Declaration 4

3 Assignment of input documents 4

4 Meeting reports 5
4.1 Approval of the report of SA3#31, Munich, Germany, 18-21 November, 2003 5
4.2 Report from SA#22, Maui, Hawaii, USA, 15-18 December, 2003 6
4.3 Report from SA3 LI #11, London, UK, 16-18 November, 2003 6
4.4 Report from SA3 LI #01/2004, Miami, USA, 27-29 January, 2004 6

5 Reports and Liaisons from other groups 6
5.1 3GPP working groups 6
5.2 IETF 7
5.3 ETSI SAGE 7
5.4 GSMA 7
5.5 3GPP2 7
5.6 OMA 8
5.7 Other groups 8

6 Work areas 8
6.1 IP multimedia subsystem (IMS) 8
6.2 Network domain security: MAP layer (NDS/MAP) 8
6.3 Network domain security: IP layer (NDS/IP) 8
6.4 Network domain security: Authentication Framework (NDS/AF) 8
6.5 UTRAN network access security 9
6.6 GERAN network access security 9
6.7 Immediate service termination (IST) 9
6.8 Fraud information gathering system (FIGS) 9
6.9 GAA and support for subscriber certificates 10
6.9.1 TR 33.919 GAA 10
6.9.2 TS 33.220 GBA 10
6.9.3 TS 33.221 Subscriber certificates 13
6.9.4 TS 33.222 HTTPS-based services 13
6.10 WLAN interworking 14
6.11 Visibility and configurability of security 18
6.12 Push 18
6.13 Priority 18
6.14 Location services (LCS) 18
6.15 Feasibility Study on (U)SIM Security Reuse by Peripheral Devices 18
6.16 Open service architecture (OSA) 18
6.17 Generic user profile (GUP) 18
6.18 Presence 18
6.19 User equipment management (UEM) 19
6.20 Multimedia broadcast/multicast service (MBMS) 19
6.21 Key Management of group keys for Voice Group Call Services 23
6.22 Guide to 3G security (TR 33.900) 23
6.23 Other areas 23

7 Review and update of work programme 23

8 Future meeting dates and venues 24

9 Any other business 24

10 Close 24

Annex A: List of attendees at the SA WG3#32 meeting and Voting List 25
A.1 List of attendees 25
A.2 SA WG3 Voting list 27

Annex B: List of documents 28

Annex C: Status of specifications under SA WG3 responsibility 39

Annex D: List of CRs to specifications under SA WG3 responsibility agreed at this meeting 44

Annex E: List of Liaisons 45
E.1 Liaisons to the meeting 45
E.2 Liaisons from the meeting 45

Annex F: Actions from the meeting 47

1 Opening of the meeting

The SA WG3 Chairman, Mr. V. Niemi, welcomed delegates to the meeting. Mr. K. England welcomed delegates to Edinburgh on behalf of the meeting hosts, European Friends of 3GPP (EF3) and provided the domestic arrangements for the meeting.

2 Agreement of the agenda and meeting objectives

The draft agenda was provided in TD S3-040001 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 was to develop all TSs and TRs into a state where they can be submitted to TSG SA #23 for approval.*
- *Another important objective was to agree on CRs that are needed for Release 6 versions of existing SA WG3 TSs.*

Preliminary schedule of the meeting:

The planned milestones for each day of the meeting were as follows:

- *Monday: completion of items 1-5 and a good start with 6.20 (MBMS);*
- *Tuesday: completion of 6.20 and 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 are 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 may be arranged in some evenings.

2.1 3GPP IPR Declaration

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

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

3 Assignment of input documents

The available documents were allocated to their relevant agenda items.

4 Meeting reports

4.1 Approval of the report of SA3#31, Munich, Germany, 18-21 November, 2003

The draft report of SA WG3 meeting #31 was provided in TD S3-040002 and was reviewed. The actions from the previous meeting were dealt with as follows:

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

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

AP 31/03: A. Bergmann to run an e-mail discussion on the MMS standardisation work and to organise a Workshop in January/February 2004 across the involved bodies if necessary.
Status unknown. The SA WG3 Chairman was asked 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.

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.

AP 31/04: T Haukka to run an e-mail discussion on TD S3-030727. Comments by 23 December 2003, conclusions to e-mail list 15 January 2004.
Completed. - No comments were received on the e-mail list and a contribution was provided by Nokia to this meeting in TD S3-040053.

AP 31/05: C. Blanchard to lead an e-mail discussion on the questions from CN WG4 in TD S3-030672. Discussion and comment deadline 17 December 2003. Draft response created by 24 December 2003. Approved response by 5 January 2004.
Completed. Discussion was held but no agreement on the usefulness of the Feature was reached. Contribution provided to this meeting in TD S3-040028.

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

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

AP 31/08: C. Blanchard was asked to check the changes made to the figures in TS 33.234 are reflected in the SA WG2 specification where they were originally copied from.
Completed. Duplicated diagram with differences were reported and some correction will be needed before forwarding to TSG SA for approval. Pseudo-CRs to be provided to correct the discrepancies.

AP 31/09: D. Mariblanca to lead an e-mail discussion on the editors notes in section 6.1.5 of the Pseudo-CR in TD S3-030790.
Completed. Input contribution in TD S3-040090.

AP 31/010: M. Pope to send SA WG3 Work Plan status details to the mailing list on 24 November 2003. Rapporteurs and Editors to provide feedback to M. Pope by 27 November 2003 in order to have an accurate SA WG3 status in the work plan presented to TSG SA #22.
Completed. Work Plan updates will be required again before the TSG SA Plenary in March 2004.

The report from SA WG3 meeting #31 was then approved. Approved version 1.0.0 will be put on the FTP server by the Secretary.

4.2 Report from SA#22, Maui, Hawaii, USA, 15-18 December, 2003

TD S3-040115: Draft Report of TSG SA meeting #22, version 0.0.8. This was introduced by P. Howard, SA WG3 Vice Chairman who provided the SA WG3 report to TSG SA meeting #22. A summary had been distributed to SA WG3 members via e-mail just after the meeting. It was reported that IETF dependencies had been discussed off-line with S. Hayes and some corrections were provided. Rapporteurs were asked to ensure the IETF dependency list is maintained as changes to the status of drafts occur or the assumptions / decisions made in SA WG3 affect the list. The list is available from the 3GPP web site: http://www.3gpp.org/TB/Other/IETF.htm

It was also noted that TSG SA had agreed that liaison with Bluetooth was acceptable and this needed to be included in the TSG SA report.

P. Howard was thanked for presenting the SA WG3 report to TSG SA.

AP 32/02: M. Pope to check the status of Liaison with Bluetooth and any further action needed to allow this.

TD S3-040017: (Forwarded from TSG SA): MMS WID MM4 Private addressing. This was introduced by the SA WG3 Chairman. The LS from TSG T to TSG SA had been forwarded to SA WG3 for consideration of the Security aspects of the proposed WI. Supporting Companies for the WI were asked to consider this off-line and provide comments to be taken to TSG SA. The drafting group provided a response LS in TD S3-040124 which was reviewed and updated in TD S3-040183 which was approved.

4.3 Report from SA3 LI #11, London, UK, 16-18 November, 2003

TD S3-040125 Report of SA3 LI #11, London, UK, 16-18 November, 2003. This was provided for information and was noted.

TD S3-040173: LS on Legal Interception of SCP initiated calls. This was introduced by the SA WG3-LI Group Chairman and was copied to SA WG3 for information. The LS was noted.

TD S3-040165 Concerning CR “33.108r6 Corrections to US Requirements” from SA3 LI (S3-040129, S3LI04_005r1). This was introduced by Motorola. It was agreed that the related CR in TD S3-040129 would be returned to the LI Group for further discussion and agreement.

TD S3-040129 CR to 33.108: Corrections to U.S. Requirements (Rel-6). Due to the objections received in TD S3-040165, this CR was returned to the SA WG3 LI Group for further elaboration and agreement.

This meeting produced an LS to SA WG3 which was provided to SA WG3 under agenda item 6.10.

4.4 Report from SA3 LI #01/2004, Miami, USA, 27-29 January, 2004

TD S3-040128 Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting on lawful interception. Miami, Florida 27-29 January 2004. This was provided for information and was noted.

The CR in TD S3-040129 was withdrawn after objections raised in TD S3-040165 and returned to the SA WG3 LI Group for further discussion.

CRs in TD S3-040130 to TD S3-040141 (TD S3-040138 was an LS withdrawn due to duplication of TD S3-040119) were postponed for e-mail approval. **Deadline for objections: 25 February 2004.**

5 Reports and Liaisons from other groups

5.1 3GPP working groups

TD S3-040004: Reply LS (from SA WG2) on security implications of Gq interface. This was introduced by Nokia. SA WG2 asked SA WG3 to note the statements relating to proxy agents and Application Functions within the network architecture, and consider these factors in the development of the stage 3 specifications. This was noted.

TD S3-040007: LS (from SA WG5) about SA WG5 Security Requirements. This was introduced by Lucent Technologies and provided the work done by SA WG5 on the security requirements for IRPs used on the Itf-N. SA WG5 asked SA WG3:

1. SA WG5 asks SA WG3 to review and provide comments on the attached documents.

2. Is there a possibility that SA WG5 can re-use any of the work done by SA WG3?

3. Does SA WG3 think that the SA WG5 WT is an overlap of any of the SA WG3 WTs?

It was agreed that the document should be reviewed off-line and comments collected. B. Owen agreed to collect together the comments and draft a response to SA WG5. This was provided in TD S3-040201 which was reviewed and approved.

TD S3-040116: LS from TSG GERAN: Protection of Kc in the Uplink TDOA location method. This was introduced by TruePosition. TSG GERAN requested SA WG3s recommendation for the protection of Kc during the transfer of the encryption key from the SMLC to the LMUs during the U-TDOA location process.

TD S3-040146 Kc security for the U-TDOA LCS method. This was presented by TruePosition. It was decided that the related information in TD S3-040116 (and the attachments) should be considered overnight and an LS provided to TSG GERAN on the TDOA Key protection issue. The response LS was provided in TD S3-040145 which was reviewed and revised in TD S3-040152 which was approved.

Due to the timing of GERAN meetings and SA WG3 meetings it was agreed that the GERAN CRs would be sent to the e-mail list after the March GERAN WG2 meeting, for endorsement by 9 April 2004.

5.2 IETF

There were no specific contributions under this agenda item.

5.3 ETSI SAGE

P. Christoffersson reported that ETSI SAGE are currently discussing key derivation functions~~algorithms for the bootstrapping function~~. UEA2/UIA2 - Some ETSI SAGE members indicated they were willing to do this work with support from their companies and a reduced funding request may be made to the GSMA.

TD S3-040102: Specification of the A5/4 Encryption Algorithms for GSM and EDGE, and the GEA4 Encryption Algorithm for GPRS. This was introduced by TeliaSonera and proposed a new TS for A5/4 and GEA4. The attached TS 55.226 version 0.1.0 was approved for forwarding to TSG SA for information. It was noted that this is a Release 6 document, but other specifications would need to be updated in order for this to be implemented. **The Chairman agreed to explain this to TSG SA Plenary.**

5.4 GSMA

TD S3-040003: GSMA response to Action PCG 10/1: Alternative 3G Ciphering and Encryption Algorithm. The GSMA did not agree to fund the algorithm work. It was indicated that the ETSI SAGE Proposal for a reduced funding of the work may be considered by the GSMA.

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 Encryption Algorithm algorithm work.

Mr. Brookson reported that there were international agreements being put in place to reduce the theft of mobile terminals by using IMEI information to block reportedly stolen handsets. Details of the impact on the 3GPP specifications would be made available some time in the future.

The next meeting is expected to be in March 2004 in London, UK (to be confirmed).

5.5 3GPP2

Because the 3GPP2 meeting was being held in parallel with the SA WG3 meeting, nobody was available to provide a report to SA WG3.

5.6 OMA

TD S3-040018: LS (from SA WG1) on "IMS messaging, Group management and Presence work overlap between 3GPP and OMA". This was introduced by T-Mobile and invited SA WG2, SA WG3 and CN WG1 to study and make proposals on how the work on Presence, IMS Messaging and Group management could be split between 3GPP and OMA from Release 7 onwards. It was agreed that the contributions and proposals should be studied and an off-line group was set up to do this. A response LS was provided in TD S3-040126 and revised in TD S3-040185 which was approved.

5.7 Other groups

6 Work areas

NOTE: TSs and TRs agreed here for presentation to TSG SA #23: Any comments need to be sent to the editors by 22 February 2004. The editors are to send them to M. Pope for editorial clean-up and presentation to TSG SA by 5 March 2004.

6.1 IP multimedia subsystem (IMS)

TD S3-040053: Proposed CR to 33.203: Deploying TLS (sips:) for interoperation between IMS and non-IMS network (Rel-6). This was provided by Nokia after an e-mail discussion was initiated, but no comments were received on the subject. It was noted that Key management and certification was outside the scope of 33.203 and it was clarified that mutual authentication of the TLS connection using certificates was needed. The CR was updated to include comments made in TD S3-040148 which was reviewed and revised in TD S3-040184 which was approved.

TD S3-040084: Proposed CR to 33.203: Addition of AES transform (Rel-6). This was introduced by Nokia on behalf of Nokia and Telenor. It was discussed that the formulation would allow different algorithms to be supported at the UE and C-CSCF. The intention was to mandate support of both Algorithms and the CR was updated to clarify this in TD S3-040149 which was revised in TD S3-040186 and approved.

TD S3-040106: Lucent Input for Information: Draft LS from RAN WG2 on Optimisation of Voice over IMS. This LS was not sent to SA WG3, but Lucent Technologies thought early notice of the LS should be provided as the security issues raised will probably come to SA WG3 from addressed groups. The LS was noted and delegates were asked to talk to their colleagues in the addressed WGs.

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 S3-040082: Sending IMSI over Gn/Gp. This was presented by Ericsson and proposed that SA WG3 sends an LS to CN WG4 to inform them that they can send the IMSI in GTP messages between GSNs. This was agreed and the contribution was attached to the LS which was provided in TD S3-040150 and updated in TD S3-040153 which was approved.

TD S3-040085: Proposed CR to 33.210: Addition of AES transform (Rel-6). This CR was presented by Nokia and was approved.

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

TD S3-040021: Pseudo CR to 33.310: Clarification on interface to access public CRL database. This was presented by Siemens on behalf of Siemens, Nokia, T-Mobile and Vodafone. This Pseudo-CR was agreed for inclusion by the editor in the draft TS, **with the second and third sentences re-formulated as a note** (also, "policy database" should read "IPsec policy database).

TD S3-040022: Pseudo CR to 33.310: Clarification on the SA lifetimes. This was presented by Siemens on behalf of Siemens, Nokia, T-Mobile and Vodafone. This Pseudo-CR was agreed for inclusion by the editor in the draft TS. (the expiry time should be clarified to show the limit is to the peer certificate which expires earliest).

TD S3-040023: NDS/AF: pki4ipsec work within IETF. This was presented by Siemens on behalf of Siemens, Nokia, T-Mobile and Vodafone to inform SA WG3 of some new work that had started within the IETF. The result of this work may have implications on the NDS/AF work (TS 33.310) which should be decided on a case-by-case basis when the IETF work is complete. The supporting companies of the NDS/AF work have started monitoring this work. The contributors were thanked for monitoring this work and the document was noted.

TD S3-040092: Pseudo-CR to 33.310: Certificate enrolment. This was presented by Nokia on behalf of Nokia, Siemens, T-Mobile and Vodafone. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040093: Pseudo-CR to 33.310: Certificate issuer name limitations removal. This was presented by Nokia on behalf of Nokia, Siemens and T-Mobile. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040094: Pseudo-CR to 33.310: Sending a CERTREQ. This was presented by Nokia on behalf of Nokia, Siemens and T-Mobile. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

The Editor reported that with these changes the draft was considered at least 90% complete and can be sent to TSG SA for approval. **It was agreed to send the updated draft to TSG SA #23 meeting for approval.**

TD S3-040182 Draft TS 33.310 v1.1.0 - Updated with changes at the meeting. This was provided for information and contained the changes agreed at the meeting and was noted.

6.5 UTRAN network access security

TD S3-040028: Draft Reply to S3-030672 on use of authentication re-attempt IE. This was introduced by BT Group and was produced in response to an action taken at the previous meeting and following discussion over the e-mail list. The draft LS was discussed and updated in TD S3-040151 which was updated in TD S3-040187 and approved.

Ericsson and Lucent agreed to check Case 2.

6.6 GERAN network access security

TD S3-040036: Authentication: A mechanism for preventing man-in-the-middle attacks. This was introduced by C. Brookson, DTI and proposed a simple solution to the man-in-the-middle attack scenario for the A5 algorithm by ensuring that the classmark message cannot be modified by cryptographically authenticating it. It was considered necessary to discuss the Special-RAND solution before making a decision on the mechanism to choose for protection against the A5 attack scenario. Discussion on the use of Special-RAND for WLAN interworking security issues was discussed under agenda item 6.10. It was decided that a small group would analyse this proposal and contribute to the next SA WG3 meeting.

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.

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 S3-040086: Draft TR 33.909 v1.0.1: Generic Authentication Architecture (GAA); System Description. This was introduced by the Editor and also included editorial changes ~~agreed~~ done by the Editor since the last meeting. The draft was noted.

TD S3-040066: GAA use guideline. This was presented by Ericsson and included a pseudo-CR to include guidelines on the applicability of GAA as section 7.1. The document was revised in a drafting session in TD S3-040178 and was agreed for inclusion by the editor in the draft TR.

TD S3-040071: Pseudo-CR to 33.919: Relationships of GAA specifications figure. This was presented by Nokia and proposed the addition of a figure to clarify the protocols and interfaces inter-relationships in GAA specifications. It was agreed that the figure was not really appropriate for the Scope section and it was agreed to include it under another section instead (more appropriate section to be found by editor). It was decided that the figure requires some additional editing to ensure it is complete and correct and the Pseudo-CR was updated in TD S3-040155 and the Pseudo-CR was agreed for inclusion by the editor in the draft TR.

TD S3-040087: Proposed additional text for TR 33.919 GAA. This was introduced by Alcatel and reviewed. It was agreed that the editor would update this with comments received and this was provided in TD S3-040193 and was agreed for inclusion by the editor in the draft TR.

The updated draft TR will not be forwarded to TSG SA #23 as it is dependent on the completion of the other specifications and will be completed later.

6.9.2 TS 33.220 GBA

TD S3-040024: GBA Spec Editorial Review. This was presented by Siemens and discussed. The changes, with some minor changes, noted by the editor, were agreed for inclusion by the editor in the draft TS.

TD S3-040060: Pseudo-CR to 33.220: Editorial changes. This was presented by Vodafone and discussed. It was commented that the Zh interface could have physical or proprietary security and mutual authentication, confidentiality and integrity may not be needed. It was decided to change the following editors' note into a normal note stating that the requirement may be fulfilled by physical or proprietary security measures. The changes, with the comments, noted by the editor, were agreed for inclusion by the editor in the draft TS.

TD S3-040078: Pseudo-CR to 33.220: Removal of unnecessary text. This was presented by Nokia and reviewed. The changes were agreed for inclusion by the editor in the draft TS.

TD S3-040079: Pseudo-CR to 33.220: Service discovery for bootstrapping procedure. This was presented by Nokia and reviewed. The changes were agreed for inclusion by the editor in the draft TS. It was decided to attach the draft TS and the Pseudo-CR to a LS to SA WG2 for their information and comments. This was provided in TD S3-040156 which was updated in TD S3-040188 and was approved. The attached Draft TSs were allocated to TD S3-040189 and TD S3-040190 with versions 1.1.0. The potential SA WG2 comments will be incorporated by CRs later if needed.

TD S3-040065: Requirements for Transaction Identifier in GBA. This was presented by Ericsson and tried to identify requirements and open issues related to TID in order to make it useful and secure in GBA.

Ericsson also proposed that SA WG3 considers adding the following requirement for TS 33.220:

- TID shall be globally unique. Different BSFs must not use the same TID values.
- TID shall be usable as a key identifier in protocols used in the Ua interface.
- NAF shall be able to detect the home network of the UE from the Transaction identifier. Home network information may be used to locate BSF.
- It should be infeasible to guess the next value of TID for specific UE.

Ericsson also proposed that SA WG3 considers adding the following Editors notes to TS 33.220:

- Add an Editors note stating that GBA must further specify on how TID is related to different identities of the subscriber (e.g. IMPI, or IMPUs), and how the NAF knows which identity has been authenticated.

- Add an Editors note stating that the TID name space control problem in the Ua interface should be further studied in the case when both GBA and non-GBA based security is used at the same time.
- Add an Editors note stating that GBA must further specify on how security associations are removed and/or updated in NAF.

The contribution included an attached Pseudo-CR to show the changes. Some re-wording was considered necessary and the Pseudo-CR was updated in TD S3-040157 and was agreed for inclusion by the editor in the draft TS.

TD S3-040063: Pseudo-CR to TS 33.220. This was presented by Nokia and reviewed. It was asked if it is necessary to hash the parameters or whether RAND@BSF_servers_domain_name would be enough. No security problem with this could be identified so it was agreed to use the simple RAND identifier and the author were asked to check for any security concerns with this approach. The editor was asked to check whether "Tid" was already used as another abbreviation and update accordingly.

TD S3-040033: Validity of the TID and key material. This was introduced by Huawei Technologies Co., Ltd. and proposed that the BSF may manage the validity of key material and when NAF shares the key material with UE, the NAF may check the validity of key material. Necessary changes were included in the contribution with revision marks. The key validity issue was considered to be a service-dependent and NAF-dependent issue and was not thought relevant for standardisation. TD S3-040077 was related to the lifetime issue and was reviewed.

TD S3-040077: Bootstrapping key lifetime and timestamp. This was presented by Nokia and asked SA WG3 to endorse the following:

1. BSF shall be able to indicate to NAF the expiration time of the bootstrapping information. This should be added as a new requirement into TS 33.220 for Zn interface.
2. BSF shall be able to indicate to NAF the creation time of the bootstrapping information. This should be added as a new requirement into TS 33.220 for Zn interface.
3. BSF shall send the key lifetime value to NAF with other bootstrapping information over Zn interface. This should be incorporated into TS 29.109.
4. BSF shall encode the key timestamp value into the TID value. The method of creating the TID should be incorporated into TS 33.220.

It was commented that only an expiration time would be adequate and not a creation time and validity time. It was clarified that it may happen that the NAF may have a requirement on the freshness of bootstrapped keys.

Proposal 1 were endorsed by SA WG3, with "bootstrapping information" replaced by "Ks".

An off-line discussion took place and it was decided to combine the proposals of TD S3-040033 and TD S3-040077 with agreements reached into TD S3-040158 which was revised in TD S3-040191 and was agreed for inclusion by the editor in the draft TS.

TD S3-040076: UE triggered unsolicited push from BSF to NAF. This was presented by Nokia and proposed to add the unsolicited push mechanism to the bootstrapping procedure described in TS 33.220. A pseudo-CR was attached implementing the required changes on the TS. The advantages of this optimisation compared to the potential added complexity was questioned as either a race condition could occur or the signalling flows do not bring much advantage. It was agreed that more study is needed on this and more justification of adopting the scheme should be provided.

TD S3-040154 Deletion of parameter n – Pseudo-CR. This was presented by Siemens and proposed not to use the parameter **n** and always use the full DNS name of the application server as input to the derivation of Ks_NAF instead. A corresponding pseudo-CR implementing the proposal was included in the contribution. It was proposed that DER_FLAG could be removed and key derivation made mandatory. It was agreed to leave the flag for the moment, but to consider whether the key derivation should be made mandatory or not in the future. The removal of the parameter **n** was agreed and the Pseudo-CR agreed for inclusion by the editor in the draft TS. **This agreement superseded contributions in TD S3-040044 and TD S3-040064 which were then withdrawn, and TD S3-040031 which was revised in TD S3-040159.**

TD S3-040044: Informational annex on the use of parameter n – Pseudo-CR. This was withdrawn as it was superseded by the TD S3-040154 agreement.

TD S3-040064: Pseudo-CR to 33.220: ‘n’ parameter in bootstrapping phase. This was withdrawn as it was superseded by the TD S3-040154 agreement.

TD S3-040159: Pseudo CR to 33.220: The NAF id in bootstrapping procedure (Rel-6). This was introduced by Huawei Technologies Co., Ltd. and proposed that the request message should include the user identity and the NAF identity to which the UE wishes to connect. The reason for including this information was questioned as the need to differentiate individual NAFs or groups of NAFs was unclear. It was decided to wait until key derivation issues are decided upon and see if this is still valid. The contribution was then noted.

TD S3-040041: Key handling in the UE in a Generic Bootstrapping Architecture - Pseudo-CR. This was presented by Siemens and proposed deleting keys when the UE is powered down. A Pseudo-CR was included implementing the proposal. The proposals were discussed and the changes reviewed. The proposed changes were agreed for inclusion by the editor in the draft TS, with the second bullet changed from "obtained" to "agreed on".

TD S3-040042: Multiple key derivation in a Generic Bootstrapping Architecture - Pseudo-CR. This was presented by Siemens and in order to overcome the performance disadvantages of very regular re-keying due to rapid access to different application servers by the user, the following was proposed:

- When the UE accesses the first NAF1, the procedure is as described in TS 33.220 v100. However, the UE and the BSF store the key Ks with the associated transaction identifier TID for further use, even after Ks_NAF1 was derived.
- When the UE accesses a second NAF2, the UE sends the stored TID to the NAF2, and the UE and the BSF use the stored Ks to derive Ks_NAF2. There is no need for a new run of the protocol over the Ub interface.
- The UE continues to use the stored key Ks for further derivations of keys Ks_NAF with further NAFs until the key Ks is required to be updated.
- The key Ks is required to be updated when its lifetime has expired, or when a NAF requests a key update (according to TS 33.220 v100, section 4.3.3).
- The key Ks is updated in a new run of the protocol over the Ub interface with the BSF. When the protocol run is complete, the old Ks is replaced by the new Ks in both, UE and BSF. The keys Ks_NAF stored in the UE and in the NAFs are not affected by this update of Ks (cf. also companion contribution on key handling).
- In order for the proposed procedure to be efficient the lifetime of Ks in the UE shall be less or equal the lifetime of Ks in the BSF. In order to ensure this it is proposed that the BSF communicates the lifetime of Ks to the UE in the 200 OK message over the Ub interface, together with the TID. In addition the BSF shall indicate to the UE whether multiple key derivation is allowed to be used. The transport format used for the TID can also be used for the key lifetime and this indication, see the XML schema provided in Nokia’s CN1 contribution N1-040086.

A pseudo-CR was included in the contribution implementing the proposal.

TD S3-040114 had been submitted by Nokia with concerns over this proposal and a response provided in TD S3-040121. Nokia reported that the issues had been clarified by discussion in TD S3-040154 and there were no outstanding issues.

It was commented that key derivation would need to be mandated as a consequence of this mechanism. It was noted that it could still be left optional, if it is specified that if key derivation is used it shall be uniformly applied. This clarification should also be added to the draft TS. The pseudo-CR was updated with the clarification in TD S3-040161 which was agreed for inclusion by the editor in the draft TS.

TD S3-040056: Draft LS on key derivation for the Generic Bootstrapping Architecture. This was presented by Siemens and proposed a liaison to ETSI SAGE on key derivation for GBA. The LS was discussed and it was considered useful to keep ETSI SAGE aware of developments so far in SA WG3 in order that they can plan some potential work that will be requested to verify the techniques to be used. It was recognised that the requirements were not fixed and may be modified by SA WG3. The LS was revised in TD S3-040162 which was reviewed and approved.

TD S3-040032: User identity in NAF. This was introduced by Huawei Technologies Co., Ltd. and proposed that because user identity is a common user information which may often be needed in generic applications, it should be provided to the NAF. A pseudo-CR was included in the contribution to implement the proposal. The meaning of the user identity was questioned and it was decided that the identity actually used should be carefully studied as part of the other open issues on identities being studied (see editors notes in TD S3-040157). Once this has been clarified, the changes may be re-presented to SA WG3.

TD S3-040043: Transfer of an asserted User Identity – Discussion and Pseudo-CRs to TSs on GAA/HTTPS-based-services and Presence Security. This was presented by Siemens. TD S3-040068 on presence and TD S3-040108 were related to this so they were then considered.

TD S3-040068: Pseudo-CR to 33.141: The user identity management. This was presented by Nokia and proposes changes to 33.141 so that user identity is handled by Authentication Proxy or Application Server in universal manner. Comments to this were provided by Siemens in TD S3-040108.

TD S3-040108: Comments on S3-040043, S3-040065, S3-040068, and on Functions and Interfaces of NAF/AP. This was presented by Siemens and argued that more study is needed for the Proxy functionality and therefore the proposal should not be decided upon at this time.

It was decided to hold an e-mail discussion on this and G. Horn agreed to kick-off this. Deadline for discussion in order to prepare contributions to the next SA WG3 meeting was set as 3 weeks before the meeting (19 April 2004).

TD S3-040089 *Introducing a UICC-based Generic Bootstrapping Architecture* and TD S3-040095 *GBA_U: Bootstrapping secrets to the UICC* were presented and discussed together. Contribution TD S3-040089 showed how the needed changes could be incorporated with minimal effects on the current specification text. **The proposed preferences of TD S3-040095 in section 2.3 and section 2.4 were adopted as a working assumption.**

It was agreed that whether a new UICC would work in an older GBA-ME terminal needed to be studied. It was also mentioned that the GBA_U-request flag on the Ub-interface could be superfluous and simplify the handling. It was clarified that MBMS as user of GBA_U would still need to realize own security procedures towards the UICC. Further input on these issues was requested. Siemens was asked to further develop the mechanism and~~s~~ provide the contributions (for those parts that are relevant for MBMS) with the same contributions deadline as agreed for MBMS contributions to SA WG3 meeting #33.

It was agreed as a working principle that the GBA_U is added as a generic mechanism, it is for further study to decide if it could be used for MBMS.

The updated draft TS will be forwarded to TSG SA #23 for approval.

6.9.3 TS 33.221 Subscriber certificates

TD S3-040073: Pseudo-CR to 33.221: Certificate chain content type. This was presented by Nokia. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040074: Pseudo-CR to 33.221: Further clarifications on certificate profiles and certificate request. This was presented by Nokia. It was suggested to leave the editors' note in the draft to enable further study of alternative certificate profile specifications. It was considered unnecessary as if further changes are wanted for future Releases of the TS, this can be done via the CR method. This Pseudo-CR was then agreed for inclusion by the editor in the draft TS.

TD S3-040072: Pseudo-CR to 33.221: Service discovery for bootstrapping procedure. This was presented by Nokia and was related to TD S3-040079, handled under agenda item 6.9.2. This Pseudo-CR was agreed for inclusion by the editor in the draft TS, replacing "terminal" by "UE" in the text. This was attached to the LS in TD S3-040079.

TD S3-040061: Pseudo-CR to 33.221: Editorial changes. This was presented by Vodafone on behalf of Nokia and Vodafone. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

The updated draft TS will be forwarded to TSG SA #23 for approval.

6.9.4 TS 33.222 HTTPS-based services

TD S3-040010: Draft TS 33.222 V0.2.0: Generic Authentication Architecture (GAA); Access to Network Application Functions using HTTPS (Release 6). this was provided for information and included agreements since the last meeting. The draft TS was noted.

TD S3-040067: Pseudo-CR to 33.222: Updates to draft HTTPS TS. This was presented by Ericsson. The introduction and scope need to be updated to indicate that this TS shows how HTTPS can be used with GBA. It was agreed to clarify in the introduction that only examples of possible services are given and that the scope is not limited to the examples given. With these modifications the pseudo-CR was updated in TD S3-040166 which was agreed for inclusion by the editor in the draft TS.

TD S3-040069: Pseudo-CR to 33.222: The virtual hosts identity. This was presented by Nokia. It was proposed that instead of deleting the annex, that the proposed additional text is used to enhance it. This was agreed. This Pseudo-CR was agreed for inclusion by the editor in the draft TS **as an enhancement to Annex A**.

TD S3-040070: Pseudo-CR to TS 33.222 (HTTPS). There was some discussion on the restriction to SIP-based services, and it was agreed to form an off-line discussion group to re-edit this proposal to clarify the general nature of the Authentication Proxy use. The revised pseudo-CR was provided in TD S3-040167 and revised in TD S3-040192 which was agreed for inclusion by the editor in the draft TS.

The updated draft TS will be forwarded to TSG SA #23 for information.

It was agreed that the 3GPP Work Plan should reflect the title of this WI: "Generic Authentication Architecture and Support for Subscriber Certificates".

6.10 WLAN interworking

TD S3-040163: A man-in-the-middle attack using Bluetooth in a WLAN interworking environment. This was introduced by Orange and discusses an attack scenario. Contributions reacting to this document were provided in TD S3-040047, TD S3-040113, TD S3-040123 which were presented in order, for an overall discussion.

> TD S3-040047: Replay attacks in the split UE scenario. This was introduced by Ericsson and concludes that integrity and replay protection over the Bluetooth interface is necessary in the WLAN application. In particular, the Laptop needs to introduce some randomness into the Bluetooth encryption key to prevent replay attacks.
>
> TD S3-040113: Response on S3-040049. This was presented by Nokia and concluded that there are several ways how the application is able to ensure that both the Laptop and the mobile contribute to the randomness of the Bluetooth encryption key, so that it cannot be replayed by any of the parties. In particular:
>
> - The Bluetooth specifications allow the application to have control on the modes of authentication and key generation that are used;
> - To utilize any existing suitable modes in Bluetooth specifications that enable both parties to contribute to the randomness of the encryption key.
>
> TD S3-040123: Notes on Gauthier’s replay attack on the UE functionality split scenario. This was presented by Siemens and contained remarks on the scope of the attack in TD S3-040163. The contribution discussed a number of possible countermeasures. The choice of countermeasure(s) will depend on, among other criteria, Bluetooth performance and implementation issues, and the threat model (compromise of laptop).

It was decided to provide a liaison to Bluetooth, outlining the possible countermeasures, without asking them to put any priority or preference on them, but to provide information on their feasibility and impact on the specifications. The use of the link keys will also be questioned in the LS. The LS was provided in TD S3-040164 (with TD S3-040163 and an updated version of TD S3-040123 attached) which was approved.

TD S3-040048, TD S3-040083 and TD S3-040109 were on the same topic and were presented in turn and discussed together:

> TD S3-040048: Split WLAN UE: Termination of EAP-AKA/SIM protocol. This was presented by Ericsson and suggested that SA WG3 take a decision on whether EAP-AKA and EAP-SIM shall terminate in the TE or the MT, to update TS 33.234 accordingly and to send an LS to the Bluetooth forum. Either of Alternative 2 (Termination of EAP-AKA/SIM in MT~~E except MK derivation~~) and Alternative 3 (Termination of EAP-AKA/SIM in ~~M~~TT except MK derivation) is acceptable to Ericsson. Integrity protection needs to be added to the local interface between the TE and MT to counter the attack presented by Orange (e-mail paper: " A man-in-the-middle attack using Bluetooth in a WLAN interworking environment").
>
> TD S3-040083: WLAN BT alternatives. This was presented by Nokia and provided the Nokia view of the pros and cons of different alternatives for accessing smart card over Bluetooth for WLAN authentication. Nokia concluded that Alternative 2 seems to be a better approach with more advantages, compared to Alternatives 1 and 3. Nokia proposed that SA WG3 adopt the approach for 3GPP-WLAN UE split, and proceed with the Bluetooth community.
>
> TD S3-040109: Comments on S3-040048 and S3-040083 - comparison of alternatives for UE functionality split. This was presented by Siemens and concluded that both Alternatives 2 and 3 provide good security and seem feasible. Siemens suggested that some arguments against Alternative 3 in TD S3-040083 seem not valid, while the advantage regarding implementation was overlooked. Therefore, Siemens prefers Alternative 3 for performance and implementation reasons, in contrast to the conclusion in TD S3-040083.

After some discussion it was agreed that the most acceptable solution was for Alternative 2 and so **SA WG3 decided on Alternative 2 (Termination of EAP-AKA/SIM in MT~~E except MK derivation~~) as a working assumption**. A LS to Bluetooth was provided in TD S3-040172 which was updated in TD S3-040197 and approved.

TD S3-040009 , TD S3-040046 , TD S3-040110 , TD S3-040030 and TD S3-040100 were all related contributions and so were presented in order and discussed together:

> TD S3-040009: Protecting GSM/GPRS networks from attacks from compromised WLAN networks when interworking. This was introduced by BT and proposed that some simple mechanism is used to protect against a potential A5/2 vulnerability in the WLAN network.
>
> TD S3-040046: The Spreading of Vulnerabilities between WLAN and GSM. This was presented by Ericsson and concluded that, based on the analysis, the compromise of proxy AAA nodes, access points, and laptops does not result in any vulnerability against GSM or UMTS authentication and that the compromise of the home AAA server does result in vulnerabilities even for GSM and UMTS, although the exact nature of the threat depends on the detailed protocol design.
>
> TD S3-040110: Comments on S3-040009 and S3-040100 on measures for separation of domains. This was presented by Siemens and discusses necessary protection. It was concluded ~~taht~~that the special RAND mechanism is required to prevent a GSM security breach to affect the 3G-WLAN access. To prevent false base station attacks on pre-Rel-6 mobiles and impersonation of EAP-SIM servers when a split UE is used an appropriate functionality split of EAP-SIM and EAP-AKA needs to be used such that MK or MSK, but not the GSM and UMTS session keys Kc, CK, IK are given to the WLAN-TE.
>
> TD S3-040030: Proposed CR to 43.020: Introducing the special RAND mechanism (Rel-6). This was introduced by Orange on behalf of Orange and Vodafone. Nokia proposed a modification to this CR in TD S3-040112.
>
> TD S3-040100: Using Special RANDs to separate WLAN and GSM/GPRS. This was presented by Nokia and proposed that the special RAND mechanism should be implemented in a way that would allow the terminals to use disjoint RAND spaces for GSM/GPRS and EAP-SIM. This would prevent an attacker from using GSM/GPRS weaknesses to impersonate WLAN network towards the terminal. Separating these contexts also means that a compromise of some component in one context (e.g. AAA server) does not allow the attacker to impersonate the network towards the client in some other context. The CR to implement the necessary changes to TS 43.020 was provided in TD S3-040112.

TD S3-040112: Proposed CR to 43.020: Introducing the special RAND mechanism with GSM/GPRS and WLAN separation (Rel-6). This was presented by Nokia and introduced modifications to the proposed CR in TD S3-040030.

Many issues surrounding the use of Special-RAND and the compatibility with different Releases of equipment were raised. It was decided that the proposals and consequences need further analysis before a final decision can be made by SA WG3. **However, it was agreed to take the use of the Special-RAND for GSM/GPRS and WLAN separation as a working assumption and the suitability of this will be analysed.**

TD S3-040014: Reply (from SA WG2) to LS (S2-030027/S3LI03_124r1) on 3GPP WLAN interworking Lawful Interception Requirements. This was introduced by Nortel Networks and was copied to SA WG3 for information. A response from SA WG3 LI group was provided in TD S3-040119 and this LS was noted.

TD S3-040119 LS from SA WG3 LI Group: Reply to LS (S2-040468) on 3GPP WLAN interworking Lawful Interception Requirements. This was introduced by the SA WG3 LI Chairman (B. Bonner) and was noted. A Pseudo-CR to cover these requirements was provided in TD S3-040101.

TD S3-040101: Pseudo-CR to 33.234: Editorial changes. This was presented by Vodafone and proposed the addition of Lawful Interception requirements (see LS in TD S3-040119). It was commented that "subscriber" should be changed to "user" in line with the rest of the document. This was agreed. It was noted that the protection of the identification and location is equivalent to "identity privacy". It was also noted that the intent of adding this sentence is not to add any new functionality into the specifications. with this change and clarification to the intent, this Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040147 Pseudo-CR to 33.234: Alignment of WLAN reference model with 23.234v2.4.0. It was agreed that the figures, copied from the SA WG2 specification, were useful for the moment in the draft TS, but if SA WG2 changed their corresponding figures, they would be removed with a CR to prevent inconsistencies between the specifications. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

AP 32/04a: C. Blanchard to check that the interface names used in TS 33.234 (WLAN Interworking) are synchronised with SA WG2 archtecture Specification (TS 23.234).

TD S3-040103: Pseudo-CR to 33.234: Link layer keys generation from EAP SIM/AKA procedures. This was presented by Ericsson. The reference [rfc2406] should be replaced with the correct reference. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040105: Pseudo-CR to 33.234: Re-authentication clarifications and check of MAC in WLAN UE. This was presented by Ericsson. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040104: Pseudo-CR to 33.234: Profiling of IKEv2 and IPsec. This was presented by Ericsson. The editors' note in section 6.6 should be enhanced to cover the need to study a further profile. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040090: PDG authentication with IKEv2 in scenario 3: clarification - Pseudo-CR. This was presented by Siemens and proposed removing the editors' note in section 6.1.5 as the study is complete (Public Key Signatures are needed). Although the schedule for the IETF work on IKEv2 is not known, SA WG3 noted that work had started on this. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040118 LS from SA WG2: Questions on re-authentication for end-to-end tunnel establishment. This was introduced by Nortel Networks. SA WG2 asked SA WG3 to consider whether subsequent tunnel establishment requests can be authenticated using a shortened authentication mechanism and if so, to provide feedback to SA WG2 on the advantages and disadvantages of such an approach. Ericsson thought that the fast EAP authentication procedure could be used as the UE and AAA server have already derived the authentication keys, but the advantages and disadvantages of the procedure should be considered. It was decided to produce a response LS to SA WG2 which was provided in TD S3-040175 which was revised in TD S3-040198 and approved.

TD S3-040013: Reply LS (from SA WG2) on Parameters and files for WLAN interworking. This was presented by Nokia. The LS was copied to SA WG3 for information and was noted. SA WG2 responded that SA WG3 advice should be sought on pseudonym list and re-authentication identity list. A Liaison from CN WG1 was available in TD S3-040019 asking SA WG3 for advice on this topic.

TD S3-040019: Reply LS (from CN WG1) on Parameters and files for WLAN interworking. This was presented by Nokia. CN WG1 asked SA WG3 whether there is a need to store the re-authentication identity in the USIM and whether it should be a list or a single item. SA WG3 decided to reply to this LS informing CN WG1 that the re-authentication identity storage issue was not considered a security issue by SA WG3. Storing to save time in case of power-off is a performance issue and if stored, SA WG3 would prefer it to be stored on the UICC. The LS was provided in TD S3-040176 which was reviewed and updated in TD S3-040196 which was approved.

TD S3-040020: LS (from CN WG1) on WLAN authentication and authorization. This was presented by Ericsson. CN WG1 reported the following working assumptions:

- *The 3GPP AAA server shall support both EAP SIM and EAP AKA based authentication as specified in the EAP SIM and EAP AKA specifications.*
  This is in line with SA WG3 assumptions.
- *The ME shall support both EAP SIM and EAP AKA based authentication, if the ME supports the ME-SIM interface.*
  This is in line with SA WG3 assumptions.
- *By default, the EAP AKA method shall be used as primary authentication method in the EAP method negotiation.*
  This would be determined by the subscription type of the user. The threat of a bidding-down attack needs to be studied and addressed if necessary by SA WG3.

- *The ME-SIM interface support is assumed to be optional for Rel-6 ME.*
  This is in line with SA WG3 assumptions.

  CN1 pointed out that the SIM specifications GSM 11.11 / TS 51.011 do not exist from Rel-5 onwards, so the support of ME-SIM interface from Rel-5 is optional.

  SA WG3 agreed with the working assumptions of CN WG1 with the current understanding.

CN WG1 Open issues:

- *If the ME supports the EAP AKA and EAP SIM methods and the 3GPP AAA server initiates authentication (i.e. EAP-Request/challenge) by means of the EAP SIM method rather than EAP AKA, what should be the ME behaviour? Does the ME have to use the EAP AKA method as primary authentication method?*
  Support of EAP-SIM method will depend upon the users card. SIM will support only EAP-SIM and USIM will support both EAP-SIM and EAP-AKA, but shall only use EAP-AKA in this case.
- *If 3GPP AAA server is aware that the ME supports the EAP AKA method, is the 3GPP AAA server mandated to always initiate the authentication (i.e. EAP-Request/challenge) by using the EAP AKA method, or is it allowed to use the EAP SIM method?*
  This would be determined by the subscription type of the user, if a SIM subscription, EAP-SIM will be allowed.

It was noted that this behaviour will need to be made explicit in the WLAN security specification.

A response LS was provided in TD S3-040177 which was reviewed and updated in TD S3-040195 which was approved.

TD S3-040120 LS (from EP-SCP) on ETSI TS 102 310 for information. This was provided for information. Delegates were asked to consider the ETSI TS and comment to the e-mail list. J. Ebellan agreed 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.

AP 32/05: Ebellan 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.

TD S3-040015: LS (from LI Group) on 3GPP WLAN interworking Lawful Interception Requirements. This was dealt with at SA WG3 meeting #31 and was re-submitted by the Secretary in error.

The updated draft TS will be forwarded to TSG SA #23 for approval.

6.11 Visibility and configurability of security

There were no specific contributions under this agenda item.

6.12 Push

There were no specific contributions under this agenda item.

6.13 Priority

There were no specific contributions under this agenda item.

6.14 Location services (LCS)

There were no specific contributions under this agenda item.

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

TD S3-040029: Technical Report on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6). This was provided for information and included the changes made since version 1.0.0 of TR 33.817. The draft was reviewed and changes agreed. The editor was asked to make the corrections, along with those from TD S3-040027 and send the updated draft to SA WG3 e-mail approval.

TD S3-040027: Pseudo CR for High Level Requirements for UICC re-use. This was introduced by **3**. The second new bullet was removed and the Pseudo-CR was agreed for inclusion by the editor in the draft TR.

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.

6.16 Open service architecture (OSA)

There were no specific contributions under this agenda item.

6.17 Generic user profile (GUP)

TD S3-040035: GUP security directions follow-up. This was presented by Nokia and suggested that SA WG3 consider taking the Liberty Alliance Project ID-WSF security solutions as the basis for their work. Furthermore, Nokia proposed to send a LS to SA WG2 and CN WG4 to provide SA WG3 view on adopting the Liberty ID-WSF for GUP security. It was commented that CN WG4 are responsible for the Rg reference point definition and there is a working assumption that they will reference Liberty Alliance work. It was noted that in Figure 4.1, reference point Rg, the application could also reside on the terminal. Open issues identified at the meeting should be included in the proposed LS. The LS was provided in TD S3-040179 which was reviewed and updated in TD S3-040199 and approved.

SA WG3 agreed to adopt the Liberty Alliance Project ID-WSF security solutions as the basis for the GUP security work.

6.18 Presence

TD S3-040045: TLS profile for Presence Security. This was presented by Ericsson and suggested that:

- 3GPP should, as a working assumption, implement the TLS profile developed in WAP, c.f. [WAP-219-TLS] as well as [WAPCert] for certificate profiles.
- SA WG3, as a working assumption for Presence security, implements also future OMA defined TLS profiles that should consider the existing IETF TLS extensions like AES cipher suites and TLSv1.1.
- SA WG3 sends an LS to OMA to ask them to report on the time schedule for implementation of these extensions for enhancing the OMA TLS profile since e.g. the implementation of an AES cipher suite should be essential for Presence Security.
- SA WG3 to endorse the attached Pseudo CR.

It was agreed to send an LS to OMA, highlighting the progress on Presence security and the identified issues. This was provided in TD S3-040168 which was reviewed and revised in TD S3-040194 which was approved.

A Pseudo CR was included as an attachment which was discussed and modifications were needed. A drafting group was set up to update the pseudo-CR. The updated pseudo-CR was included in TD S3-040169 (see below).

TD S3-040075: Pseudo-CR to 33.141: GAA in Presence, general view. This was presented by Nokia. There was some objection to the references to IMS authentication and ISIM. Other parts of the changes also needed discussion and clarification and it was decided to update the pseudo-CR after detailed discussion in the off-line drafting group. The pseudo-CR was revised in TD S3-040169 which was agreed for inclusion by the editor in the draft TS.

The editors' note in TD S3-040157 should be copied into Section 4 of the draft TS.

6.19 User equipment management (UEM)

There were no specific contributions under this agenda item.

6.20 Multimedia broadcast/multicast service (MBMS)

TD S3-040005: LS (from SA WG4) on DRM streaming service. This was introduced by Ericsson. SA WG4 hoped that in point-to-point and MBMS streaming, the greatest possible commonality of DRM techniques will be used, subject to their suitability in each environment. SA WG4 asked SA WG3 to comment on their outlined proposal. This was noted and kept in mind for the dealing with other contributions on MBMS.

TD S3-040006: Reply LS (from SA WG4) on issues on DRM for PSS and MBMS streams. This was introduced by Nokia and asked the OMA DRM group to consider the time 3GPP needs for finalizing the file format, signalling and streaming of protected media and asked to reference 3GPP TS 26.244 for the encryption extensions to the file format and TS 26.234 for the signalling and streaming of protected media. This was copied to SA WG3 for information and was noted.

TD S3-040008: LS from ETSI SAGE: Response on protection of MBMS and DRM Streaming Services. This was introduced by TeliaSonera and provided comments from ETSI SAGE on the DRM protection requirements. The comments by ETSI SAGE were noted and kept in mind when dealing with other contributions.

TD S3-040011: LS (from RAN WG1) on updated version of TR 25.803. This was introduced by Qualcomm and was provided for information and was noted.

TD S3-040012: Reply (from SA WG2) to LS on service announcement and UE joining procedure. This was introduced by Nortel Networks and informed SA WG3 that SA WG2 considered the feasibility of including the traffic protection mechanism indication in the Service Announcement to be a matter for SA WG4. Similarly, for the "Joining Availability Time", SA WG2 considered this an SA WG4 matter and indicated that SA WG2 do not see any particular need for such an indication. The LS had been copied to SA WG4 so they would be expected to also comment on these issues. This was noted for further discussion of contributions.

TD S3-040016: LS from SA WG1: Response to SA3 LS on service announcement and UE joining procedure. This was introduced by Samsung and informed SA WG3 that SA WG1 considered that a user should be able to join an MBMS user service as soon as possible after announcement of the service and do not see the need for a "Joining Availability Time" parameter. This was noted for further discussion of contributions.

TD S3-040034: high level key update. This was introduced by Huawei Technologies Co., Ltd. and discussed and concluded that when a UE joins the multicast service, the BM-SC gives some rules to UE. The UE requests the new high level key based on those rules when it needs the new high level key. Textual changes to implement this was also provided in the contribution. Section 3 of TD S3-040059 also addressed this issue and was considered in the discussion. The contribution was updated with comments received in TD S3-040127. The first proposed changed sentence was approved, the second sentence containing the example was moved into an editors' note which should also contain a reference to the Ericsson proposal of an alternative mechanism to handle the rules.

TD S3-040037: BMSC handing of the previous keys. This was introduced by Samsung Electronics and proposed 3 methods of BMSC operation when the UE does not receive a new key due to e.g. network congestion. Samsung proposed that SA WG3 make a decision on the BMSC operation and capture this decision into the specification. It was considered a rare event that the BAK is not available when needed as it is intended that the terminal will request the Key well in advance of the use time. It was also questioned how much encrypted content could be stored on the terminal while waiting for a Key? After discussion of this it was considered that so far, the assumption has been for streaming data and storage of data Key management would need further study. The contribution was therefore noted at this time.

AP 32/06a: A. Escott to organise an e-mail discussion on MBMS Download security solutions for providing contribution to the next meeting.

TD S3-040038: Pseudo-CR to 33.246: MBMS key update rejection CR. This was introduced by Samsung Electronics and was agreed for inclusion by the editor in the draft TS. It was agreed that the figure should be modified to combine the final 2 flows as a single "OR" flow.

TD S3-040099: Proposed terminology for MBMS keys. This was introduced by Siemens and proposed to adopt their clarifications for Key terminology (MMK and MSK) and to inform T WG3 of the adopted naming. It was considered that MSK could cause confusion in other groups as SA WG1 have a concept of an MBMS Session which is not protected by this Key. It was also agreed that the User-specific Key should be defined to differentiate between the 3 levels of Keys. This was revised by the author in TD S3-040160 (see below).

TD S3-040160: Update on Proposed terminology for MBMS keys. This was presented by Siemens. Proposal 1 was agreed and the pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040096: MBMS: Key Replay Protection. This was introduced by Siemens. Based on agreements to the contribution TD S3-030701, this contribution further detailed the solution for the requirement and proposed some text to be incorporated into TS 33.246.

The Siemens proposals were handled as follows:

A) *to accept the modifications to requirement R5h, as listed in section 2.1 of this contribution.*
This change was agreed.

B) *to adopt one of the Pseudo-CR's as listed in section 4.1 respectively section 4.2, depending on the two-tiered model that is chosen by SA WG3 #32. If SA WG3 #32 does not take a decision on the two-tiered model, then it is proposed to add both alternatives to the MBMS security specification and add an editors note to describe the outstanding decision.*
It was agreed that the two proposals will be added with an editors note until a mechanism is chosen.

C) *to adopt the working assumption NOT to use both SEQ and RAND as a seed for the MSK generation but only to use RAND, if the SK_RAND model would be chosen by SA WG3 (relates to section 4.1).*
It was agreed as a working assumption, but noted that any optimisation agreed at a later date may need to be included.

D) *to decide on how to realize functions Ff, Fg, Fs, Fm. A possibility could be to ask ETSI SAGE to take on the work to specify these functions. In principle, the key derivation functions (Ff, Fg, Fs, Fm) may be decided by the MBMS service provider, but it is proposed to standardize these functions.*
It was agreed that these need to be standardized and ETSI SAGE could be asked to do this.
P. Christofferssen was asked to tell ETSI SAGE that there may be a request for this type of functions for their consideration.

TD S3-040052, TD S3-040040 and TD S3-040050 contained different proposals for MBMS Key Management approaches and were discussed together.

TD S3-040052: MBMS key management: follow up from SA#22 meeting. This was introduced by TIM on behalf of TIM, Orange, Oberthur and Gemplus. Following the discussion held within SA#22 meeting, the contributors proposed to take in the SA comments and particularly the request that the final solution should not include any options. In particular, it was proposed to allow only the UICC-based key distribution mechanism.

TD S3-040040: MBMS key management approach. This was introduced by Nokia on behalf of Nokia, Siemens and Ericsson and concluded that while the reasons that were brought forward by SP-030743 (TSG SA #22 document) seem to be unjustified, there seems currently no reason to change the SA3#31 working assumption.

TD S3-040050: MBMS UICC-based solution. This was introduced by Gemplus on behalf of Gemplus, Axalto, Giesecke & Devrient and Oberthur and discussed MBMS Key Management scenarios, and concluded that the MBMS UICC solution, based on 3GPP existing infrastructure, offers a higher security level, low impact on the network resources and is ready for Rel-6 timescale. Moreover, at TSG SA#22 plenary meeting several operators expressed a preference for the UICC-based only solution and TSG SA recommended that options should be kept to a minimum. The contributors recommended that SA WG3 choose the UICC-based solution as the unique solution for the MBMS service.

TD S3-040051: Discussion paper on MBMS key management. This was introduced by Axalto on behalf of Gemplus, Axalto, Giesecke & Devrient and Oberthur and proposed that:

- Only UICC solution is addressed in Rel-6 timeframe.
- Existing OTA mechanisms are used for MBMS key management.

Comments to contributions TD S3-040050 and TD S3-040051 were collected in TD S3-040111 which was presented by Siemens.

Concerns were expressed for the need to define additional interfaces and the capacity of OTA Servers. It was also commented that the MBMS services offered may not be planned in advance, but could include dynamically broadcast services when key distribution would be needed on-demand.

It was agreed that the OTA interface should be standardised (although not necessarily mandated). It was also agreed that there was no need for an interface between BMSCs and solutions avoiding an interface should receive preference for SA WG3.

TD S3-040088: Pseudo-CR to 33.246: CR on MBMS key Management procedures. This was introduced by Axalto and proposed the changes needed to implement the proposals in TD S3-040051.

TD S3-040098: MBMS: OTA security considerations. This was introduced by Siemens and made some security recommendations when using OTA for MBMS key management.

It was proposed (under the assumption that OTA is selected)

- to incorporate these recommendations into TS 33.246.
- that SA WG3 decides on the best strategy in fulfilling Issue-3 (*Limiting the effects of security breaches*) and document it within the TS.

The recommendations were modified as follows and agreed:

REC-1: OTA shall not use DES in CBC mode for transporting new key set versions to the UICC.

REC-2: The used keys for point-to-point transport of MBMS keys shall not be shared among subscribers.

It was understood that the security impacts of the implied increased use of the OTA Server and the protocols used need to be carefully studied.

TD S3-040097: Using GBA_U within MBMS. This was introduced by Siemens and showed how the ME can handle the GBA_U secrets for MBMS and explained the advantages in using GBA for both ME and UICC based MBMS services. Siemens proposed to adopt the working assumption that the point-to-point MBMS key delivery protocol shall use a GBA bootstrapped secret Ks_xxx_NAF to protect the MBMS service specific key delivery. This Ks_xxx_NAF was either bootstrapped to the ME using GBA_ME or bootstrapped to the UICC using GBA_U. After some discussion, it was agreed that **if the GBA_U can be specified in time for Rel-6**, then this solution could be adopted.

TD S3-040039: Usage of GBA in MBMS. This was introduced by Nokia and described GBA usage for MBMS authentication is according to the working assumption reached in SA WG3 Meeting #31. Nokia proposed that SA WG3 include the GBA authentication related steps presented in the contribution in TS 33.246. This was not agreed, instead an LS was sent to SA WG4 (see TD S3-040200) after discussion of TD S3-040058.

TD S3-040058: Usage of GBA, MIKEY and HTTP digest for MBMS key delivery. This was presented by Ericsson and proposed that the procedure using GBA and HTTP digest with MBMS described in this contribution is taken as a basis for further development of GBA usage in MBMS. It was proposed that SA WG3 sends a LS to SA WG2 to inquire further information whether SA WG2 sees problems in having the BSF and NAF in different networks. It was also proposed that SA WG3 make the following working assumption:

- *The MBMS service is identified with URI and no client payload is included.*

It was realised that more information on the support of GBA in the Visited Network was intended to be included in Rel-6 was needed before firm decisions could be made in SA WG3. It was confirmed that the possibility for having BMSC in the visited network is included in the SA WG2 specifications.

An LS to SA WG4 and SA WG2 was developed in TD S3-040142 which was reviewed and revised in TD S3-040200 and approved.

TD S3-040057: Status of SRTP and MIKEY in IETF. This was presented by Ericsson for information and was noted.

TD S3-040059: Enhanced MIKEY in MBMS key management. This was presented by Ericsson and proposed to adopt two-tiered MIKEY as key management protocol for MBMS and that SA WG3 endorse the requirements in chapter 3 (*Load balancing in key requests*, dealt with under discussions including TD S3-040034). Due to the Rel-6 timescale, it was proposed that any extensions needed for MIKEY should be specified in 3GPP rather than the IETF. It was clarified that until now there was no security requirement to delete the BAK and if this was needed it would need to be added to MIKEY. It was also clarified that the mechanism was intended to be UE-initiated ("Pull") and not a "Push" mechanism.

TD S3-040081: Use of MIKEY in the Combined method. This was presented by Nokia and presented enhancements to MIKEY protocol so that it can be used to deliver encrypted keys to UEs. Nokia proposed that the following actions are taken to standardise enhancements:

1. *IETF MSEC working group is contacted and informed about the enhancements.*
2. *A new "MIKEY MBMS extensions" Internet-Draft is published via IETF MSEC working group.*
3. *MIKEY MBMS extensions are published as an Informational RFC. If it impossible to publish RFC in time then required enhancements are incorporated into relevant 3GPP specifications.*

The two approaches presented in TD S3-040059 and TD S3-040081 were dependent on the use of MIKEY for Key distribution. **Delegates were asked to consider and discuss these proposals off-line, particularly between Ericsson and Nokia and come to some agreement on the way forward.**

TD S3-040080: Further updates on DRM usage for MBMS security. This was presented by Nokia and proposed that SA WG3 adopt OMA DRMv2 mechanisms for protecting MBMS content for both download and streaming.

Nokia also suggested that the extent that OMA rights issuing mechanisms may be utilized for MBMS key management should be further studied. It was agreed that if the mechanisms can be used for point-to-multipoint then SA WG3 should study their re-use. TD S3-040005 and TD S3-040008 were also considered to check the SA WG4 and ETSI SAGE positions on this.

TD S3-040107: Discussion paper on MBMS key compromising and fraud recovery. This was introduced by Oberthur on behalf of Gemplus and Oberthur CS. The contribution analysed the reality of the threat and proposes strategies to recover from an attack where a pirate obtains the keys and distributes them. The analysis shows that there are simple ways to find a pirate that is leaking the BAK keys and to exclude him from the system. It was clarified that this was a recovery method in case of BAK leaking, rather than a way of tracing the pirate.

There was a lot of discussion and a number of solutions at the meeting and no firm conclusions could be drawn on the best way forward for SA WG3. **In order to allow good progress and finalisation of MBMS Security work, it was agreed that MBMS contributions to the next meeting should be available 4 weeks before the meeting (12 April 2004) with comments available ~~3~~ 2 weeks before the meeting (26 April 2004) and then given time to update the initial 12 April contributions and submit them to the final deadline.**

TD S3-040171 LS from T WG3: LS Response on potential USIM impact of the MBMS security framework (S3-030660, T3-040942). This was introduced by Gemplus. T WG3 asked SA WG3 to provide the final requirements to them for MBMS management onto the USIM. It was agreed that it was too soon to answer as the discussions outside the meeting on MBMS needed to be carried out. **This LS will be revisited at the next SA WG3 meeting for response.**

6.21 Key Management of group keys for Voice Group Call Services

TD S3-040117: Draft reply (from TSG GERAN) to LS on 'Ciphering for Voice Group Call Services'. This was presented by Siemens. TSG GERAN asked SA WG3 the following questions, with initial responses in blue:

A. Is a UICC/USIM mandatory for the mobile that supports the new VGCS ciphering mechanism?
Yes.

B. How will a Release 6 MS that supports the new VGCS mechanism react with a SIM card?
VGCS ciphering will not be possible as the SIM is unable to derive the short term key from the RAND. A Rel-6 UICC will be required.

C. What happens if a UICC/USIM with voice group id X is inserted into a Release-5 MS and the MS is camped on to a cell where this group call is active?
Ciphering will not be possible since the Rel-5 MS does not support the needed ciphering functions.

D. Are the proposed changes also applicable to the VBS service?
Yes.

E. Are the proposed changes to be applied only from Release-6?
Yes.

F. Is a cell based global_count as in C(i) an acceptable method for providing this parameter ?
Yes.

A draft response was provided by Siemens in TD S3-040143 which was revised to correct the Release from 5 to 4 and updated in TD S3-040180 which was approved.

TD S3-040025: Securing VGCS calls: signalling the encryption algorithm indicator. This was presented by Siemens on behalf of Siemens and Vodafone. After discussion, solution 1 was chosen and this will be communicated to t WG3.

TD S3-040026: Updated WID: Key Management of group keys for Voice Group Call Services. The time scales and supporting companies were updated. Motorola also indicated their support. The changes were noted but it was thought unnecessary to update the work item at TSG SA for these changes and the Work Plan will be updated to reflect the changes.

TD S3-040174 Response LS (from T WG3) on Status of VGCS work in SA WG3. This was presented by Axalto. After discussion, and agreement on the answers to the questions, a response was provided in TD S3-040181 which was reviewed and approved.

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

Due to lack of time at the meeting it was decided that the SA WG3 Secretary would send the SA WG3 Work Plan to Rapporteurs for update before the TSG SA Plenary. **Deadline for updates: 27 February 2004.**

8 Future meeting dates and venues

AP 32/07: M. Pope to try to book ETSI for October meeting 5 - 8 October 2004.

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#33	10 (13.00) -14 (16.00) May 2004	Beijing, China	Samsung
S3#34	06-09 July 2004 (TBC)	USA (TBC)	"NA Friends of 3GPP" (TBC)
S3#35	5-8 October 2004	Host required (Sophia?)	Host required (ETSI/EF3?)
S3#36	23-26 November 2004	Shenzhen, China	HuaWei Technologies
S3#37	February 2005	Australia (TBC)	Qualcomm (TBC)

LI meetings planned

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

TSGs RAN/CN/T and SA Plenary meeting schedule

Meeting	**2004**	**Location**	**Primary Host**
TSGs#23	March 9-12 & 15-18 2004	Phoenix, USA	"NA Friends of 3GPP"
TSGs#24	June 1-4 & 7-10 2004	Korea	TTA
TSGs#25	7-10 & 13-16 September 2004	Palm Springs, USA	"NA Friends of 3GPP"
TSGs#26	7-10 & 13-16 December 2004	Athens, Greece	"European Friends of 3GPP"
Meeting	**2005 DRAFT TBD**	**Location**	**Primary Host**
TSGs#23	March 9-11 & 14-16 2005	Tokyo, Japan	TBD

9 Any other business

The Chairman announced that Mr. Krister Boman (Ericsson) and Mr. Tommi Viitanen (Nokia) were not going to attend SA WG3 any longer due to new responsibilities within their respective companies. The SA WG3 Chairman and delegates thanked these two hard-working delegates for their excellent contribution to the work of SA WG3 and wished them good fortune in their future roles.

10 Close

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

Annex A: List of attendees at the SA WG3#32 meeting and Voting List

A.1 List of attendees

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Jorge Abellan Sevilla	AXALTO, SCHLUMBERGER SYSTÈMES	jorge.abellan@slb.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. Colin Blanchard	BT GROUP PLC	colin.blanchard@bt.com	+44 7711 191835	+44 1473 605353	+44 1473 623910	GB	ETSI
Mr. Marc Blommaert	SIEMENS NV/SA	marc.blommaert@siemens.com		+32 14 25 34 11	+32 14 25 33 39	BE	ETSI
Mr. Krister Boman	NIPPON ERICSSON K.K.	krister.boman@ericsson.com	+46 70 246 9095	+46 31 747 4055		JP	ARIB
Ms. Brye Bonner	MOTOROLA SEMICONDUCTOR ISRAEL	brye.bonner@motorola.com		+1 847.576.5920	+1.847.538.5564	IL	ETSI
Mr. Charles Brookson	DTI	cbrookson@iee.org	+44 7956 567 102	+44 20 7215 3691	+44 20 7931 7194	GB	ETSI
Mr. Mauro Castagno	TELECOM ITALIA S.P.A.	mauro.castagno@telecomitalia.it		+39 0112285203	+39 0112287056	IT	ETSI
Ms. Lily Chen	MOTOROLA A/S	lchen1@email.mot.com		+1 847 632 3033	+1 847 435 2264	DK	ETSI
Mr. Takeshi Chikazawa	MITSUBISHI ELECTRIC CO.	chika@isl.melco.co.jp		+81 467 41 2181	+81 467 41 2185	JP	ARIB
Mr. Per Christoffersson	TELIASONERA AB	per.christoffersson@teliasonera.com		+46 705 925100		SE	ETSI
Mr. Kevin England	MMO2 PLC	kevin.england@o2.com	+447710016799	+447710016799		GB	ETSI
Mr. Hubert Ertl	GIESECKE & DEVRIENT GMBH	hubert.ertl@de.gi-de.com	+49 172 8691159	+49 89 4119 2796	+49 89 4119 2921	DE	ETSI
Dr. Adrian Escott	3	adrian.escott@three.co.uk		+44 7782 325254	+44 1628 766012	GB	ETSI
Mr. Jean-Bernard Fischer	OBERTHUR CARD SYSTEMS S.A.	jb.fischer@oberthurcs.com		+33 141 38 18 93	+33 141 38 48 23	FR	ETSI
Miss Sylvie Fouquet	ORANGE SA	sylvie.fouquet@francetelecom.com		+33 145 29 49 19	+33 145 29 65 19	FR	ETSI
Dr. Eric Gauthier	ORANGE SA	eric.gauthier@orange.ch		+41 21 216 53 08	+41 21 216 56 00	FR	ETSI
Mr. Philip Ginzboorg	NOKIA CORPORATION	philip.ginzboorg@nokia.com		+358 5 0483 6224	+358 9 4376 6852	FI	ETSI
Mr. Robert Gross	TRUEPOSITION INC.	rlgross@trueposition.com		+1610 680 1119	+1 610 680 1199	US	ETSI
Ms. Tao Haukka	NOKIA CORPORATION	tao.haukka@nokia.com		+358 40 5170079		FI	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@siemens.com		+49 8963 641494	+49 8963 648000	DE	ETSI
Mr. Peter Howard	VODAFONE GROUP PLC	peter.howard@vodafone.com	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB	ETSI
Ms. Yingxin Huang	HUAWEI TECHNOLOGIES CO., LTD	huangyx@huawei.com		+86-10-82882752	+86-10-82882940	CN	CCSA
Mr. Yu Inamura	NTT DOCOMO INC.	jane@mml.yrp.nttdocomo.co.jp		+81-468-40-3809	+81-468-40-3364	JP	ARIB
Mr. Bradley Kenyon	HEWLETT-PACKARD	brad.kenyon@hp.com		+1 402 384 7265	+1 402 384 7030	FR	ETSI
Mr. Bernd Lamparter	NEC EUROPE LTD	bernd.lamparter@netlab.nec.de		+49 6221 905 11 50	+49 6221 905 11 55	GB	ETSI
Mr. Alex Leadbeater	BT GROUP PLC	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. Vesa Lehtovirta	ERICSSON INC.	vesa.lehtovirta@ericsson.com		+358405093314	+	US	T1
Mr. David Mariblanca	ERICSSON LM	david.mariblanca@ericsson.com		+34 646004736	+34 913392538	SE	ETSI
Dr. Valtteri Niemi	NOKIA CORPORATION	valtteri.niemi@nokia.com		+358504837327	+358718036850	FI	ETSI
Mr. Petri Nyberg	TELIASONERA AB	petri.nyberg@teliasonera.com		+358 204066824	+358 2040 0 3168	SE	ETSI
Mr. Bradley Owen	LUCENT TECHNOLOGIES N. S. UK	bvowen@lucent.com		+44 1793 897312	+44 1793 897414	GB	ETSI
Mr. Anand Palanigounder	NORTEL NETWORKS (EUROPE)	anand@nortelnetworks.com		+1 972 684 4772	+1 972 685 3123	GB	ETSI
Miss Mireille Pauliac	GEMPLUS S.A.	mireille.pauliac@gemplus.com		+33 4 42365441	+33 4 42365792	FR	ETSI
Mr. Maurice Pope	ETSI SECRETARIAT	maurice.pope@etsi.org	+33 (0)6 07 59 08 49	+33 4 92 94 42 59	+33 4 92 38 52 59	FR	ETSI
Mr. Anand Prasad	NTT DOCOMO	prasad@docomolab-euro.com		+49-89-56824112	+49-89-56824300	JP	ETSI
Mr. Bengt Sahlin	ERICSSON 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.	c_jsemple@qualcomm.com		+447880791303		FR	ETSI
Mr. Benno Tietz	VODAFONE D2 GMBH	benno.tietz@vodafone.com		+49 211 533 2168	+49 211 533 1649	DE	ETSI
Mr. Tommi Viitanen	NOKIA TELECOMMUNICATIONS INC.	tommi.viitanen@nokia.com		+358405131090	+358718075300	US	T1
Mr. Berthold Wilhelm	BMWI	berthold.wilhelm@regtp.de		+49 681 9330 562	+49 681 9330 725	DE	ETSI
Mr. Wenlin Zhang	HUAWEI TECHNOLOGIES CO. LTD.	zhangwenlin@huawei.com		+86 82882753	+86 82882940	CN	ETSI
Mr. Yanmin Zhu	SAMSUNG ELECTRONICS CO., LTD	yanmin.zhu@samsung.com		+86-10-68427711	+86-10-68481891	KR	TTA

44 participants

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #30, #31, and #32, the following companies are eligible to vote at SA WG3 meeting #33:

Company	Country	Status	Partner Org
3	GB	3GPPMEMBER	ETSI
ALCATEL S.A.	FR	3GPPMEMBER	ETSI
AT&T Wireless Services, Inc.	US	3GPPMEMBER	T1
Axalto, Schlumberger Systèmes S.A.	FR	3GPPMEMBER	ETSI
BT Group Plc	GB	3GPPMEMBER	ETSI
BUNDESMINISTERIUM FUR WIRTSCHAFT	DE	3GPPMEMBER	ETSI
DTI - Department of Trade and Industry	GB	3GPPMEMBER	ETSI
Ericsson Incorporated	US	3GPPMEMBER	T1
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
INTEL CORPORATION SARL	FR	3GPPMEMBER	ETSI
Lucent Technologies	US	3GPPMEMBER	T1
Lucent Technologies Network Systems UK	GB	3GPPMEMBER	ETSI
Mitsubishi Electric Co.	JP	3GPPMEMBER	ARIB
mmO2 plc	GB	3GPPMEMBER	ETSI
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
Nippon Ericsson K.K.	JP	3GPPMEMBER	ARIB
NOKIA Corporation	FI	3GPPMEMBER	ETSI
NOKIA KOREA	KR	3GPPMEMBER	TTA
Nokia Telecommunications Inc.	US	3GPPMEMBER	T1
NORTEL NETWORKS (EUROPE)	GB	3GPPMEMBER	ETSI
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
TeliaSonera AB	SE	3GPPMEMBER	ETSI
Toshiba Corporation, Digital Media Network Company	JP	3GPPMEMBER	ARIB
TruePosition Inc.	US	3GPPMEMBER	ETSI
Vodafone D2 GmbH	DE	3GPPMEMBER	ETSI
VODAFONE Group Plc	GB	3GPPMEMBER	ETSI

47 Voting Members

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040001	Draft Agenda for SA WG3 meeting #32	SA WG3 Chairman	2	Approval		Approved
S3-040002	Draft Report of SA WG3 meeting #31	SA WG3 Secretary	4.1	Approval		Approved. To be placed on 3GPP FTP server
S3-040003	GSMA response to Action PCG 10/1: Alternative 3G Ciphering and Encryption Algorithm	GSMA Security Group	5.4	Information		GSMA not willing to fully fund the work. Reduced funding request would be considered.
S3-040004	Reply LS (from SA WG2) on security implications of Gq interface	SA WG2	5.1	Action		Comments on draft TS to be provided to B. Owen
S3-040005	LS (from SA WG4) on DRM streaming service	SA WG4	6.20	Action		Noted. Considered for other MBMS contributions
S3-040006	Reply LS (from SA WG4) on issues on DRM for PSS and MBMS streams	SA WG4	6.20	Information		Noted
S3-040007	LS (from SA WG5) about SA WG5 Security Requirements	SA WG5	5.1	Action		review off-line and comments collected by B. Owen
S3-040008	LS from ETSI SAGE: Response on protection of MBMS and DRM Streaming Services	ETSI SAGE	6.20	Information		Comments noted. To be kept in mind when dealing with other contributions
S3-040009	Protecting GSM/GPRS networks from attacks from compromised WLAN networks when interworking	BT Group	6.10	Discussion / Decision		Used in WLAN discussions
S3-040010	Draft TS 33.222 V0.2.0: Generic Authentication Architecture (GAA); Access to Network Application Functions using HTTPS (Release 6)	Rapporteur (B. Sahlin)	6.9.4	Information		Noted
S3-040011	LS (from RAN WG1) on updated version of TR 25.803	RAN WG1	6.20	Information		Noted
S3-040012	Reply (from SA WG2) to LS on service announcement and UE joining procedure	SA WG2	6.20	Information		Noted
S3-040013	Reply LS (from SA WG2) on Parameters and files for WLAN interworking	SA WG2	6.10	Information		Noted
S3-040014	Reply (from SA WG2) to LS (S2-030027/S3LI03_124r1) on 3GPP WLAN interworking Lawful Interception Requirements	SA WG2	6.10	Information		Noted. LI response in S3-040119
S3-040015	LS (from LI Group) on 3GPP WLAN interworking Lawful Interception Requirements	SA WG3-LI Group	6.10	Action		Dealt with at meeting #31
S3-040016	LS from SA WG1: Response to SA3 LS on service announcement and UE joining procedure	SA WG1	6.20	Information		Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040017	(Forwarded from TSG SA): MMS WID MM4 Private addressing	TSG SA	4.2	Discussion		Off-line group to discuss. Response in S3-040124
S3-040018	LS (from SA WG1) on "IMS messaging, Group management and Presence work overlap between 3GPP and OMA"	SA WG1	5.6	Action		Response in S3-030126
S3-040019	Reply LS (from CN WG1) on Parameters and files for WLAN interworking	CN WG1	6.10	Action		Response in S3-040176
S3-040020	LS (from CN WG1) on WLAN authentication and authorization	CN WG1	6.10	Action		Response in S3-040177
S3-040021	Pseudo CR to 33.310: Clarification on interface to access public CRL database	Siemens, Nokia, T-Mobile, Vodafone	6.4	Approval		Agreed for inclusion in draft TS
S3-040022	Pseudo CR to 33.310: Clarification on the SA lifetimes	Siemens, Nokia, T-Mobile, Vodafone	6.4	Approval		Agreed for inclusion in draft TS
S3-040023	NDS/AF: pki4ipsec work within IETF	Siemens, Nokia, T-Mobile, Vodafone	6.4	Information		Noted. Changes to 33.310 may be necessary later
S3-040024	GBA Spec Editorial Review	Siemens	6.9.2	Discussion / Decision		Agreed for inclusion in draft TS.
S3-040025	Securing VGCS calls: signalling the encryption algorithm indicator	Siemens, Vodafone	6.21	Discussion / Decision		Solution 1 agreed. To inform T3
S3-040026	Updated WID: Key Management of group keys for Voice Group Call Services	Siemens, Vodafone	6.21	Approval		Work Plan to be updated. Noted
S3-040027	Pseudo CR for High Level Requirements for UICC re-use	**3**	6.15	Discussion / Decision		Agreed with modifications for inclusion in draft TS.
S3-040028	Draft Reply to S3-030672 on use of authentication re-attempt IE	E-mail drafting (C Blanchard)	6.5	Discussion / Decision	S3-040151	Revised in S3-040151
S3-040029	Technical Report on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6)	Toshiba, Intel, T-Mobile, Nokia, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel, AT&T Wireless	6.15	Approval		Updated TR to be sent to S3 e-mail for approval and then to M Pope for pres to SA for approval
S3-040030	Proposed CR to 43.020: Introducing the special RAND mechanism (Rel-6)	Orange, Vodafone	6.10	Approval		Used in WLAN discussions
S3-040031	Pseudo CR to 33.220: The NAF id in bootstrapping procedure (Rel-6)	Huawei Technologies Co., Ltd.	6.9.2	Approval	S3-040159	Revised in S3-040159
S3-040032	User identity in NAF	Huawei Technologies Co., Ltd.	6.9.2	Discussion / Approval		Open issues on identities need to be solved before accepting the proposal
S3-040033	Validity of the TID and key material	Huawei Technologies Co., Ltd.	6.9.2	Discussion / Decision		Combined with S3-040077 in S3-040158

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040034	high level key update	Huawei Technologies Co., Ltd.	6.20	Discussion / Decision	S3-040127	Revised after discussion in S3-040127
S3-040035	GUP security directions follow-up	Nokia, Ericsson	6.17	Discussion	S3-040179	LS in S3-040179
S3-040036	Authentication: A mechanism for preventing man-in-the-middle attacks	DTI (Charles Brookson)	6.6	Discussion / Decision		Noted. Special-RAND needs to be discussed before choosing a solution
S3-040037	BMSC handing of the previous keys	Samsung Electronics	6.20	Discussion / Decision		Key Management for stored MBMS data would need more study
S3-040038	Pseudo-CR to 33.246: MBMS key update rejection CR	Samsung Electronics	6.20	Approval		Used in MBMS discussions
S3-040039	Usage of GBA in MBMS	Nokia	6.20	Discussion / Decision		Used in MBMS discussions
S3-040040	MBMS key management approach	Nokia, Siemens, Ericsson	6.20	Discussion / Decision		Used in MBMS discussions
S3-040041	Key handling in the UE in a Generic Bootstrapping Architecture - Pseudo-CR	Siemens	6.9.2	Discussion / Decision		Changes agreed for inclusion in draft TS
S3-040042	Multiple key derivation in a Generic Bootstrapping Architecture - Pseudo-CR	Siemens	6.9.2	Discussion / Decision	S3-040161	Pseudo-CR updated in S3-040161
S3-040043	Transfer of an asserted User Identity – Discussion and Pseudo-CRs to TSs on GAA/HTTPS-based-services and Presence Security	Siemens	6.9.2	Discussion / Decision		Comments in S3-040068 and S3-040108
S3-040044	Informational annex on the use of parameter n – Pseudo-CR	Siemens	6.9.2	Discussion / Decision		Withdrawn after agreement to S3-040154
S3-040045	TLS profile for Presence Security	Ericsson	6.18	Discussion / Decision		LS to OMA in S3-040168. Updated Pseudo-CR in S3-040169
S3-040046	The Spreading of Vulnerabilities between WLAN and GSM	Ericsson	6.10	Discussion		Used in WLAN discussions
S3-040047	Replay attacks in the split UE scenario	Ericsson	6.10	Discussion		Used in WLAN discussions
S3-040048	Split WLAN UE: Termination of EAP-AKA/SIM protocol	Ericsson	6.10	Discussion / Decision		Alternative 2 working assumption. LS in S3-040172
S3-040049	A man-in-the-middle attack using Bluetooth in a WLAN interworking environment	Orange	6.10	Discussion	S3-040122	Revised by e-mail comments in S3-040122
S3-040050	MBMS UICC-based solution	Gemplus, Axalto, Giesecke & Devrient, Oberthur	6.20	Discussion / Decision		Used in MBMS discussions
S3-040051	Discussion paper on MBMS key management	Axalto, Gemplus, Giesecke & Devrient, Oberthur	6.20	Discussion / Decision		See also S3-030088 (Pseudo-CR)

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040052	MBMS key management: follow up from SA#22 meeting	TIM, Orange, Oberthur, Gemplus	6.20	Discussion / Decision		Used in MBMS discussions
S3-040053	Proposed CR to 33.203: Deploying TLS (sips:) for interoperation between IMS and non-IMS network (Rel-6)	Nokia	6.1	Approval	S3-040148	Revised in S3-040148
S3-040054	Pseudo-CR to 33.220: Service discovery for bootstrapping procedure	Nokia	6.9.2	Approval		WITHDRAWN - Duplicated in S3-040079
S3-040055	Pseudo-CR to 33.221: Service discovery for bootstrapping procedure	Nokia	6.9.3	Approval		WITHDRAWN - Duplicated in S3-040072
S3-040056	Draft LS on key derivation for the Generic Bootstrapping Architecture	Siemens	6.9.2	Approval	S3-040162	LS updated in S3-040162
S3-040057	Status of SRTP and MIKEY in IETF	Ericsson	6.20	Information		Noted
S3-040058	Usage of GBA, MIKEY and HTTP digest for MBMS key delivery	Ericsson	6.20	Discussion / Decision		LS in S3-040142
S3-040059	Enhanced MIKEY in MBMS key management	Ericsson	6.20	Discussion / Decision		Used in MBMS discussions
S3-040060	Pseudo-CR to 33.220: Editorial changes	Vodafone, Nokia	6.9.2	Approval		Agreed for inclusion in the draft TS with some changes
S3-040061	Pseudo-CR to 33.221: Editorial changes	Vodafone, Nokia	6.9.3	Approval		Agreed for inclusion in the draft TS
S3-040062	Specification of the A5/4 Encryption Algorithms for GSM and EDGE, and the GEA4 Encryption Algorithm for GPRS	TeliaSonera	5.3	Approval	S3-040102	Revised in S3-040102
S3-040063	Pseudo-CR to TS 33.220	Nokia	6.9.2	Approval		Hash function removed. Agreed for inclusion in draft TS
S3-040064	Pseudo-CR to 33.220: ‘n’ parameter in bootstrapping phase	Ericsson	6.9.2	Approval		Withdrawn after agreement to S3-040154
S3-040065	Requirements for Transaction Identifier in GBA	Ericsson	6.9.2	Discussion / Decision		Uopdated Pseudo-CR provided in S3-040157
S3-040066	GAA use guideline	Ericsson	6.9.1	Discussion / Decision	S3-030178	revised in S3-040178
S3-040067	Pseudo-CR to 33.222: Updates to draft HTTPS TS	Ericsson	6.9.4	Approval	S3-040166	Modifications made and updated in S3-040166
S3-040068	Pseudo-CR to 33.141: The user identity management	Nokia	6.18	Approval		further study these proposals and revisit at the next meeting
S3-040069	Pseudo-CR to 33.222: The virtual hosts identity	Nokia	6.9.4	Approval		Agreed for inclusion in draft TS as enhancement to Annex A
S3-040070	Pseudo-CR to TS 33.222 (HTTPS)	Nokia	6.9.4	Approval	S3-040167	Revised after off-line drafting in S3-040167

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040071	Pseudo-CR to 33.919: Relationships of GAA specifications figure.	Nokia	6.9.1	Approval	S3-040155	Revised in S3-040155
S3-040072	Pseudo-CR to 33.221: Service discovery for bootstrapping procedure	Nokia	6.9.3	Approval		Agreed for inclusion in draft TS
S3-040073	Pseudo-CR to 33.221: Certificate chain content type	Nokia	6.9.3	Approval		Agreed for inclusion in draft TS
S3-040074	Pseudo-CR to 33.221: Further clarifications on certificate profiles and certificate request	Nokia	6.9.3	Approval		Agreed for inclusion in draft TS
S3-040075	Pseudo-CR to 33.141: GAA in Presence, general view	Nokia	6.18	Approval	S3-040170	Revised after off-line drafting in S3-040167
S3-040076	UE triggered unsolicited push from BSF to NAF	Nokia	6.9.2	Discussion / Decision		More justification needed and further study on advantages given needed
S3-040077	Bootstrapping key lifetime and timestamp	Nokia	6.9.2	Discussion / Decision		Combined with S3-040033 in S3-040158
S3-040078	Pseudo-CR to 33.220: Removal of unnecessary text	Nokia	6.9.2	Approval		Agreed for inclusion in draft TS
S3-040079	Pseudo-CR to 33.220: Service discovery for bootstrapping procedure	Nokia	6.9.2	Approval		Agreed for inclusion in draft TS. LS to S1 in S3-040156
S3-040080	Further updates on DRM usage for MBMS security	Nokia	6.20	Discussion / Decision		Used in MBMS discussions
S3-040081	Use of MIKEY in the Combined method	Nokia	6.20	Discussion / Decision		Used in MBMS discussions
S3-040082	Sending IMSI over Gn/Gp	Ericsson, Vodafone	6.3	Discussion / Decision		LS in S3-040150
S3-040083	WLAN BT alternatives	Nokia	6.10	Discussion / Decision		Alternative 2 working assumption. LS in S3-040172
S3-040084	Proposed CR to 33.203: Addition of AES transform (Rel-6)	Nokia, Telenor	6.1	Approval	S3-040149	Revised in S3-040149
S3-040085	Proposed CR to 33.210: Addition of AES transform (Rel-6)	Nokia, Telenor	6.3	Approval		Approved
S3-040086	Draft TR 33.909 v1.0.1: Generic Authentication Architecture (GAA); System Description	Editor (A Van Moffaert)	6.9.1	Approval		Noted
S3-040087	Proposed additional text for TR 33.919 GAA	Alcatel	6.9.1	Discussion / Decision	S3-040193	Revised in S3-040193
S3-040088	Pseudo-CR to 33.246: CR on MBMS key Management procedures	AXALTO, Gemplus, Oberthur	6.20	Approval		See S3-040051
S3-040089	Introducing a UICC-based Generic Bootstrapping Architecture	Siemens	6.9.2	Discussion / Decision		Further study and contr. To next meeting
S3-040090	PDG authentication with IKEv2 in scenario 3: clarification - Pseudo-CR	Siemens	6.10	Discussion / Decision		Agreed for inclusion in draft TS

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040091	Notes on Gauthier's replay attack on the UE functionality split scenario	Siemens	6.10	Discussion	S3-040123	Revised in S3-040123
S3-040092	Pseudo-CR to 33.310: Certificate enrolment	Nokia, Siemens, T-Mobile, Vodafone	6.4	Approval		Agreed for inclusion in draft TS
S3-040093	Pseudo-CR to 33.310: Certificate issuer name limitations removal	Nokia, Siemens, T-Mobile	6.4	Approval		Agreed for inclusion in draft TS
S3-040094	Pseudo-CR to 33.310: Sending a CERTREQ	Nokia, Siemens, T-Mobile	6.4	Approval		Agreed for inclusion in draft TS
S3-040095	GBA_U: Bootstrapping secrets to the UICC	Siemens	6.9.2	Discussion / Decision		Further study and contr. To next meeting
S3-040096	MBMS: Key Replay Protection	Siemens	6.20	Discussion / Decision		Used in MBMS discussions
S3-040097	Using GBA_U within MBMS	Siemens	6.20	Discussion / Decision		If in time for Rel-6
S3-040098	MBMS: OTA security considerations	Siemens	6.20	Discussion / Decision		If GBA_U can be specified in time, consider this solution
S3-040099	Proposed terminology for MBMS keys	Siemens	6.20	Discussion / Decision	S3-040160	revised in S3-040160
S3-040100	Using Special RANDs to separate WLAN and GSM/GPRS	Nokia	6.10	Discussion / Decision		
S3-040101	Pseudo-CR to 33.234: Editorial changes	Vodafone	6.10	Approval		LATE_DOC.
S3-040102	Specification of the A5/4 Encryption Algorithms for GSM and EDGE, and the GEA4 Encryption Algorithm for GPRS	TeliaSonera	5.3	Approval		LATE_DOC. Draft TS approved for forwarding to SA for Information
S3-040103	Pseudo-CR to 33.234: Link layer keys generation from EAP SIM/AKA procedures	Ericsson, Siemens, Nokia	6.10	Approval		Agreed for inclusion in draft TS
S3-040104	Pseudo-CR to 33.234: Profiling of IKEv2 and IPsec	Ericsson	6.10	Approval		Agreed for inclusion in draft TS. Other minor changes also agreed
S3-040105	Pseudo-CR to 33.234: Re-authentication clarifications and check of MAC in WLAN UE	Ericsson	6.10	Approval		Agreed for inclusion in draft TS. Other minor changes also agreed
S3-040106	Lucent Input for Information: Draft LS from RAN WG2 on Optimisation of Voice over IMS	Lucent Technologies	6.1	Information		LATE_DOC LS from RAN2 not addressed to S3 - For information. Noted
S3-040107	Discussion paper on MBMS key compromising and fraud recovery	Gemplus, Oberthur CS	6.20	Discussion		LATE_DOC: Used in MBMS Discussions
S3-040108	Comments on S3-040043, S3-040065, S3-040068, and on Functions and Interfaces of NAF/AP	Siemens	6.9.2, 6.9.4, 6.18	Discussion		Comments to 043, 065, 068: E-mail discussion. G Horn.
S3-040109	Comments on S3-040048 and S3-040083 - comparison of alternatives for UE functionality split	Siemens	6.10	Discussion / Decision		Alternative 2 working assumption. LS in S3-040172

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040110	Comments on S3-040009 and S3-040100 on measures for separation of domains	Siemens	6.10	Discussion / Decision		Comments to 009, 100:
S3-040111	Comments on S3-040050/51: 'UICC based MBMS key management'	Ericsson, Nokia, Siemens	6.20	Discussion / Decision		Comments to 050, 051:
S3-040112	Proposed CR to 43.020: Introducing the special RAND mechanism with GSM/GPRS and WLAN separation (Rel-6)	Nokia	6.10	Approval		Comments to 030: More analysis of Special-RAND needed.
S3-040113	Response on S3-040049	Nokia	6.10	Discussion / Decision		Comments to 049: LS in S3-040164
S3-040114	Remarks on S3-040042	Nokia	6.9.2	Discussion / Decision		Comments to 042: Covered by explanations in S3-030121 and developments in meeting
S3-040115	Draft Report of TSG SA meeting #22, version 0.0.8	SA WG3 Secretary	4.2	Information		LATE_DOC. Noted
S3-040116	LS from TSG GERAN: Protection of Kc in the Uplink TDOA location method	TSG GERAN	5.1	Action		Response LS in S3-040152
S3-040117	Draft reply (from TSG GERAN) to LS on 'Ciphering for Voice Group Call Services'.	TSG GERAN	6.21	Action		Response in S3-040180
S3-040118	LS from SA WG2: Questions on re-authentication for end-to-end tunnel establishment	SA WG2	6.10	Action		Response LS in S3-040175
S3-040119	LS from SA WG3 LI Group: Reply to LS (S2-040468) on 3GPP WLAN interworking Lawful Interception Requirements	SA WG3 LI Group	6.10	Action		Noted. Pseudo-CR in S3-040101
S3-040120	LS (from EP-SCP) on ETSI TS 102.310 for information	EP-SCP		Action		J. Ebellan agreed to collect comments and prepare a response LS
S3-040121	Remarks on S3-040042 by Nokia and replies by Guenther Horn (Siemens), dated 6 Feb 2004	Siemens	6.9.2	Discussion / Decision		LATE_DOC. Covered by explanations and developments in meeting
S3-040122	A man-in-the-middle attack using Bluetooth in a WLAN interworking environment	Orange	6.10	Discussion	S3-040163	LATE_DOC. Revised in S3-040163
S3-040123	Notes on Gauthier's replay attack on the UE functionality split scenario	Siemens	6.10	Discussion	S3-030163	LATE_DOC. Revised in S3-040163
S3-040124	Response to S3-040017: [DRAFT] LS on MMS WID MM4 Private addressing	SA WG3	4.2	Approval	S3-040183	Revised in S3-040183
S3-040125	Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #11/03 on lawful interception. London 19-21 November 2003	SA WG3 LI Group	4.3	Information		Noted
S3-040126	Draft LS: reply to LS S1-040253 (=S3-040018) on "IMS messaging, Group management and Presence work overlap between 3GPP and OMA"	SA WG3	5.6	Approval	S3-040185	Revised in S3-040185

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040127	high level key update	Huawei Technologies Co., Ltd.	6.20	Discussion / Decision		First sentence approved. Second moved to editors note to include ref to ericsson proposal for rules handling.
S3-040128	Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting on lawful interception. Miami, Florida 27-29 January 2004	SA WG3 LI Group	4.3	Information		Noted
S3-040129	CR to 33.108: Corrections to U.S. Requirements (Rel-6)	SA WG3 LI Group	4.3	Approval		LATE_DOC. Returned to S3-LI after objection in S3-040165
S3-040130	CR to 33.108: Corrections to Tables 6.2, 6.7 (Rel-6)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040131	CR to 33.108: Corrections to Correlation Number (Rel-6)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040132	CR to 33.108: Correction to Identifiers (Rel-6)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040133	CR to 33.108: Implications of R5 onwards QoS parameters on ASN.1 module in 33.108. (Rel-5)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040134	CR to 33.108: Implications of R5 onwards QoS parameters on ASN.1 module in 33.108. (Rel-6)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040135	CR to 33.108: Syntax error in Annex B.4 (Rel-6)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040136	CR to 33.108: Correction on the description of “initiator” in “PDP Context Modification CONTINUE Record” (Rel-5)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040137	CR to 33.108: Correction on the description of “initiator” in “PDP Context Modification CONTINUE Record” (Rel-6)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040138	LS from SA WG3 LI Group: Reply to LS (S2-040468) on 3GPP WLAN interworking Lawful Interception Requirements	SA WG3 LI Group	4.3	Information		WITHDRAWN - Duplicated S3-040119
S3-040139	CR to 33.108: Clarification on the use of IRI-END record in PS interception (Rel-6)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040140	CR to 33.108: Editorial Corrections (Rel-6)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040141	CR to 33.108: Syntax error in Annex B.4 (Rel-5)	SA WG3 LI Group	4.3	Approval		LATE_DOC. E-mail approval by 27 Feb 2004
S3-040142	DRAFT LS on HTTP based services and order of procedures	SA WG3	6.20	Approval	S3-040200	Revised in S3-040200
S3-040143	Draft Reply LS on ‘Ciphering for Voice Group Call Services’	SA WG3	6.21	Approval	S3-040180	Revised in S3-040180

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040144	Update on Proposed terminology for MBMS keys	Siemens	6.20	Approval	S3-040160	LATE_DOC revised in S3-040160
S3-040145	Reply LS on security recommendations for the protection of Kc in the Uplink TDOA location method	SA WG3	5.1	Approval	S3-040152	revised in S3-040152
S3-040146	Kc security for the U-TDOA LCS method	TruePosition	5.1	Information		LATE_DOC. Presented. Related to S3-040116. LS to GERAN in S3-040152
S3-040147	Pseudo-CR to 33.234: Alignment of WLAN reference model with 23.234v2.4.0	Vodafone, BT	6.10	Approval		LATE_DOC. Agreed for inclusion in the draft TS
S3-040148	Proposed CR to 33.203: Deploying TLS (sips:) for interoperation between IMS and non-IMS network (Rel-6)	Nokia	6.1	Approval	S3-040184	revised in S3-040184
S3-040149	Proposed CR to 33.203: Addition of AES transform (Rel-6)	Nokia, Telenor	6.1	Approval	S3-040186	revised in S3-040186
S3-040150	DRAFT Sending IMSI across Gn/Gp interfaces and security implications	SA WG3	6.3	Approval	S3-040153	Revised in S3-040153
S3-040151	Draft Reply to S3-030672 on use of authentication re-attempt IE	SA WG3	6.5	Approval	S3-040187	revised in S3-040187
S3-040152	Reply LS on security recommendations for the protection of Kc in the Uplink TDOA location method	SA WG3		Approval		Approved
S3-040153	Sending IMSI across Gn/Gp interfaces and security implications	SA WG3	6.3	Approval		Approved
S3-040154	Deletion of parameter n – Pseudo-CR	Siemens	6.9.2	Discussion / Decision		parameter n removed
S3-040155	Pseudo-CR to 33.919: Relationships of GAA specifications figure.	Nokia	6.9.1	Approval		Agreed for inclusion in draft TR
S3-040156	Liaison on Service Discovery of BSF and PKI portal	SA WG3	6.9.2	Approval	S3-040188	Revised in S3-040188
S3-040157	Pseudo-CR to 33.220: Requirements for Transaction Identifier in GBA	Ericsson	6.9.2	Approval		Agreed for inclusion in draft TR
S3-040158	Combined S3-040077 and S3-040033: Life time of the bootstrapping information	Huawei, Nokia	6.9.2	Approval	S3-040191	Revised in S3-040191
S3-040159	Pseudo CR to 33.220: The NAF id in bootstrapping procedure (Rel-6)	Huawei Technologies Co., Ltd.	6.9.2	Approval		Noted. Wait for key derivation agreements before re-considering if needed
S3-040160	Update on Proposed terminology for MBMS keys	Siemens	6.20	Approval		Endorsed proposal 1. Pseudo CR to be included in draft TS
S3-040161	Pseudo-CR to 33.220: Multiple key derivation in a Generic Bootstrapping Architecture	Siemens	6.9.2	Approval		Agreed for inclusion in draft TS
S3-040162	LS on key derivation for the Generic Bootstrapping Architecture	SA WG3	6.9.2	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040163	A man-in-the-middle attack using Bluetooth in a WLAN interworking environment	Orange	6.10	Discussion		attached to LS in S3-040164
S3-040164	LS to Bluetooth on WLAN man-in-the-middle attack scenario (Guenther)	SA WG3	6.10	Approval		Approved
S3-040165	Concerning CR "33.108r6 Corrections to US Requirements" from SA3 LI (S3-040129, S3LI04_005r1)	Alcatel, Lucent, mm02, Motorola, Nokia	4.3	Discussion / Approval		Agreed to return CR to LI group for further discussion and agreement
S3-040166	Pseudo-CR to 33.222: Updates to draft HTTPS TS	Ericsson	6.9.4	Approval		Agreed for inclusion in draft TS
S3-040167	Pseudo-CR to TS 33.222 (HTTPS)	Drafting Group/ Nokia	6.9.4	Approval	S3-040192	Revised in S3-040192
S3-040168	DRAFT LS on Presence Security	SA WG3	6.18	Approval	S3-040194	Revised in S3-040194
S3-040169	Pseudo-CR to Presence Security (Drafting Group - Krister)	Drafting Group	6.18	Approval		Agreed for inclusion in draft TS
S3-040170	WITHDRAWN - included in S3-040169					WITHDRAWN
S3-040171	LS from T WG3: LS Response on potential USIM impact of the MBMS security framework (S3-030660, T3-040942)	T WG3	6.20	Action		Revisit at next meeting after MBMS off-line discussions
S3-040172	Further Liaison on Termination of EAP authentication over Bluetooth for 3GPP UE function split	SA WG3	6.10	Approval	S3-040197	Revised in S3-040197
S3-040173	LS on Legal Interception of SCP initiated calls	SA WG3 LI Group	4.3	Action		Noted
S3-040174	Response LS (from T WG3) on Status of VGCS work in SA WG3	T WG3	6.21	Action		Response LS in S3-040181
S3-040175	Reply LS on Questions on re-authentication for end-to-end tunnel establishment	SA WG3	6.10	Approval	S3-040198	Revised in S3-040198
S3-040176	Reply LS on Parameters and files for WLAN interworking	SA WG3	6.10	Approval	S3-040196	Revised in S3-040196
S3-040177	Reply LS on WLAN authentication and authorization	SA WG3	6.10	Approval	S3-040195	Revised in S3-040195
S3-040178	Pseudo-CR to 33.919: GAA use guideline	Ericsson	6.9.1	Approval		Agreed for inclusion in draft TS
S3-040179	DRAFT LS on GUP security directions	SA WG3	6.15	Approval	S3-040199~~8~~	Revised in S3-040199~~8~~
S3-040180	Reply LS on 'Ciphering for Voice Group Call Services'	SA WG3	6.21	Approval		Approved
S3-040181	Reply LS on 'Status of VGCS work in SA3'	SA WG3	6.21	Approval		Approved
S3-040182	Draft TS 33.310 v1.1.0 Updated with changes at the meeting	Editor	6.4	Information		Noted
S3-040183	LS on MMS WID MM4 Private addressing	SA WG3	4.2	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040184	Proposed CR to 33.203: Deploying TLS (sips:) for interoperation between IMS and non-IMS network (Rel-6)	Nokia	6.1	Approval		Approved
S3-040185	Reply to LS S1-040253 (=S3-040018) on "IMS messaging, Group management and Presence work overlap between 3GPP and OMA"	SA WG3	5.6	Approval		Approved
S3-040186	Proposed CR to 33.203: Addition of AES transform (Rel-6)	Nokia, Telenor	6.1	Approval		Approved
S3-040187	Reply to S3-030672 on use of authentication re-attempt IE	SA WG3	6.5	Approval		Approved
S3-040188	Liaison on Service Discovery of BSF and PKI portal	SA WG3	6.9.2	Approval		Approved
S3-040189	Draft TS 33.220 v1.1.0: Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (Release 6)	Editor	6.9.2	Information		Noted
S3-040190	Draft TS 33.221 v1.1.0: Generic Authentication Architecture (GAA); Support for Subscriber Certificates (Release 6)	Editor	6.9.3	Information		Noted
S3-040191	Combined S3-040077 and S3-040033: Life time of the bootstrapping information	Huawei, Nokia	6.9.2	Approval		Agreed for inclusion in draft TS
S3-040192	Pseudo-CR to TS 33.222 (HTTPS)	Drafting Group/ Nokia	6.9.4	Approval		Agreed for inclusion in draft TS
S3-040193	Proposed additional text for TR 33.919 GAA	Alcatel	6.9.1	Discussion / Decision		Agreed for inclusion in draft TS
S3-040194	LS on Presence Security	SA WG3	6.18	Approval		Approved
S3-040195	Reply LS on WLAN authentication and authorization	SA WG3	6.10	Approval		Approved
S3-040196	Reply LS on Parameters and files for WLAN interworking	SA WG3	6.10	Approval		Approved
S3-040197	Further Liaison on Termination of EAP authentication over Bluetooth for 3GPP UE function split	SA WG3	6.10	Approval		Approved
S3-040198	Reply LS on Questions on re-authentication for end-to-end tunnel establishment	SA WG3 (David)	6.10	Approval		Approved
S3-040199	LS on GUP security directions	SA WG3	6.15	Approval		Approved
S3-040200	LS on HTTP based services and order of procedures	SA WG3	6.20	Approval		Approved
S3-040201	LS to SA WG5: SA5 Security Requirements	SA WG3	5.1	Approval		Approved

Annex C: Status of specifications under SA WG3 responsibility

Type	Number	Title	Ver at SA3#32	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#32	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#32	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)	5.6.0	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#32	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	02.09	Security aspects	5.2.1	R96	S3	CHRISTOFFERSSON, Per	
TS	03.20	Security-related Network Functions	5.2.1	R96	S3	NGUYEN NGOC, Sebastien	SMG#29: CRs but postponed, then forgotten!
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)	6.4.0	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	1.0.0	Rel-6	S3	BOMAN, Krister	.
TS	33.203	3G security; Access security for IP-based services	6.1.0	Rel-6	S3	BOMAN, Krister	.
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	6.3.0	Rel-6	S3	KOIEN, Geir	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210). .
TS	33.220	Generic Authentication Architecture (GAA); Generic bootstrapping architecture	1.0.0	Rel-6	S3	HAUKKA, Tao	WI = SEC1-SC (UID 33002) Based on 33.109 §4. .
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	1.0.0	Rel-6	S3	LOPEZ SORIA, Luis	.

Type	Number	Title	Ver at SA3#32	Rel	TSG/ WG	Editor	Comment
TS	33.246	3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)	1.0.0	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)	1.0.0	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	1.1.0	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	1.0.0	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 licence. .
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 licence. .
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 licence. .
TS	55.226	Specification of the A5/4 encryption algorithms for GSM and ECSD, and the GEA4 encryption algorithm for ECSD; Document 1: A5/4 and GEA4 specification	none	Rel-6	S3	CHRISTOFFERSSON, Per	Work item UID = 1571 (SEC1) .
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 licence. .

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

To be completed with CR numbers, etc. after e-mail approval of SA WG3 LI CRs.

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WI
33.210			Rel-6	Addition of AES transform			S3#32	S3-040085	
33.203			Rel-6	Deploying TLS (sips:) for interoperation between IMS and non-IMS network			S3#32	S3-040184	
33.203			Rel-6	Addition of AES transform			S3#32	S3-040186	
33.108			Rel-6	Corrections to Tables 6.2, 6.7			S3#32 +e-mail	S3-040130	
33.108			Rel-6	Corrections to Correlation Number			S3#32 +e-mail	S3-040131	
33.108			Rel-6	Correction to Identifiers			S3#32 +e-mail	S3-040132	
33.108			Rel-5	Implications of R5 onwards QoS parameters on ASN.1 module in 33.108			S3#32 +e-mail	S3-040133	
33.108			Rel-6	Implications of R5 onwards QoS parameters on ASN.1 module in 33.108	A		S3#32 +e-mail	S3-040134	
33.108			Rel-6	Syntax error in Annex B.4			S3#32 +e-mail	S3-040135	
33.108			Rel-5	Correction on the description of “initiator” in “PDP Context Modification CONTINUE Record”			S3#32 +e-mail	S3-040136	
33.108			Rel-6	Correction on the description of “initiator” in “PDP Context Modification CONTINUE Record”	A		S3#32 +e-mail	S3-040137	
33.108			Rel-6	Clarification on the use of IRI-END record in PS interception			S3#32 +e-mail	S3-040139	
33.108			Rel-6	Editorial Corrections			S3#32 +e-mail	S3-040140	
33.108			Rel-5	Syntax error in Annex B.4			S3#32 +e-mail	S3-040141	

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	Source TD	Comment/Status
S3-040003	GSMA response to Action PCG 10/1: Alternative 3G Ciphering and Encryption Algorithm	GSMA Doc PCG2003_01	GSMA not willing to fully fund the work. Reduced funding request would be considered.
S3-040004	Reply LS (from SA WG2) on security implications of Gq interface	S2-034362	Comments on draft TS to be provided to B. Owen
S3-040005	LS (from SA WG4) on DRM streaming service	S4-030843	Noted. Considered for other MBMS contributions
S3-040006	Reply LS (from SA WG4) on issues on DRM for PSS and MBMS streams	S4-030846	Noted
S3-040007	LS (from SA WG5) about SA WG5 Security Requirements	S5-037280	review off-line and comments collected by B. Owen
S3-040008	LS from ETSI SAGE: Response on protection of MBMS and DRM Streaming Services	SAGE 03-03	Comments noted. To be kept in mind when dealing with other contributions
S3-040011	LS (from RAN WG1) on updated version of TR 25.803	R1-031414	Noted
S3-040012	Reply (from SA WG2) to LS on service announcement and UE joining procedure	S2-040458	Noted
S3-040013	Reply LS (from SA WG2) on Parameters and files for WLAN interworking	S2-040467	Noted
S3-040014	Reply (from SA WG2) to LS (S2-030027/S3LI03_124r1) on 3GPP WLAN interworking Lawful Interception Requirements	S2-040468	Noted. LI response in S3-040119
S3-040015	LS (from LI Group) on 3GPP WLAN interworking Lawful Interception Requirements	S3LI03_124r1	Dealt with at meeting #31
S3-040016	LS from SA WG1: Response to SA3 LS on service announcement and UE joining procedure	S1-040224	Noted
S3-040017	(Forwarded from TSG SA): MMS WID MM4 Private addressing	SP-030746	Off-line group to discuss. Response in S3-040124
S3-040018	LS (from SA WG1) on "IMS messaging, Group management and Presence work overlap between 3GPP and OMA"	S1-040253	Response in S3-030126
S3-040019	Reply LS (from CN WG1) on Parameters and files for WLAN interworking	N1-040162	Response in S3-040176
S3-040020	LS (from CN WG1) on WLAN authentication and authorization	N1-040163	Response in S3-040177
S3-040116	LS from TSG GERAN: Protection of Kc in the Uplink TDOA location method	GP-040561	Response LS in S3-040152
S3-040117	Draft reply (from TSG GERAN) to LS on 'Ciphering for Voice Group Call Services'.	GP-040566	Response in S3-040180
S3-040118	LS from SA WG2: Questions on re-authentication for end-to-end tunnel establishment	S2-034384	Response LS in S3-040175
S3-040119	LS from SA WG3 LI Group: Reply to LS (S2-040468) on 3GPP WLAN interworking Lawful Interception Requirements	S3LI04_042r1	Noted. Pseudo-CR in S3-040101
S3-040120	LS (from EP-SCP) on ETSI TS 102.310 for information	SCP-040101	J. Ebellan agreed to collect comments and prepare a response LS
S3-040171	LS from T WG3: LS Response on potential USIM impact of the MBMS security framework (S3-030660, T3-040942)	T3-040140	Revisit at next meeting after MBMS off-line discussions
S3-040173	LS on Legal Interception of SCP initiated calls	S3LI04_052r1	Noted
S3-040174	Response LS (from T WG3) on Status of VGCS work in SA WG3	T3-040125	Response LS in S3-040181

E.2 Liaisons from the meeting

TD number	Title	TO	CC
S3-040152	Reply LS on security recommendations for the protection of Kc in the Uplink TDOA location method	**TSG GERAN**	**-**
S3-040153	Sending IMSI across Gn/Gp interfaces and security implications	**CN WG4**	**-**
S3-040162	LS on key derivation for the Generic Bootstrapping Architecture	**ETSI SAGE**	**-**
S3-040164	LS to Bluetooth on WLAN man-in-the-middle attack scenario (Guenther)	**Bluetooth Security Experts Group**	**Bluetooth Car Working Group**
S3-040180	Reply LS on 'Ciphering for Voice Group Call Services'	**GERAN WG2**	**ETSI EP RT, T WG 3**
S3-040181	Reply LS on 'Status of VGCS work in SA3'	**T WG3**	**ETSI EP RT, GERAN WG2**
S3-040183	LS on MMS WID MM4 Private addressing	**TSG SA**	**TSG T**

TD number	Title	TO	CC
S3-040185	Reply to LS S1-040253 (=S3-040018) on "IMS messaging, Group management and Presence work overlap between 3GPP and OMA"	**SA WG1, TSG SA, TSG CN, SA WG2, CN WG1**	**-**
S3-040187	Reply to S3-030672 on use of authentication re-attempt IE	**CN WG4**	**-**
S3-040188	Liaison on Service Discovery of BSF and PKI portal	**SA WG2**	**-**
S3-040194	LS on Presence Security	**OMA-SEC**	**-**
S3-040195	Reply LS on WLAN authentication and authorization	**CN WG1**	**SA WG2, CN WG4**
S3-040196	Reply LS on Parameters and files for WLAN interworking	**CN WG1, SA WG2, T WG3**	**-**
S3-040197	Further Liaison on Termination of EAP authentication over Bluetooth for 3GPP UE function split	**Bluetooth Security Expert Group, Bluetooth Architecture Review Board (BARB), Bluetooth CAR group**	**ETSI EP SCP**
S3-040198	Reply LS on Questions on re-authentication for end-to-end tunnel establishment	**SA WG2**	**CN WG1**
S3-040199	LS on GUP security directions	**CN WG4, SA WG2**	**-**
S3-040200	LS on HTTP based services and order of procedures	**SA WG4, SA WG2**	**CN WG1**
S3-040201	LS to SA WG5: SA5 Security Requirements	**SA WG5**	**-**

Annex F: Actions from 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.**

AP 32/02: **M. Pope to check the status of Liaison with Bluetooth and any further action needed to allow this.**

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 Encryption Algorithm algorithm work.**

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.**

AP 32/04a: **C. Blanchard to check that the interface names used in TS 33.234 (WLAN Interworking) are synchronised with SA WG2 archtecture Specification (TS 23.234).**

AP 32/05: **Ebellan 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.**

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.**

AP 32/06a: **A. Escott to organise an e-mail discussion on MBMS Download security solutions for providing contribution to the next meeting.**

AP 32/07: **M. Pope to try to book ETSI for October meeting 5 - 8 October 2004.**