Technical Specification Group Services and System Aspects **TSGS#27(05)0124**

Meeting #27, 14 - 17 March 2005,

Tokyo, Japan

3GPP TSG SA WG3 Security — S3#37 **Draft Report**
21 - 25 February 2005
Sophia Antipolis, France

Source: **Secretary of 3GPP TSG-SA WG3**

Title: **Draft Report of SA3 meeting #37 for TSG SA information**

Document for: **Information**

Status: **Draft version 0.0.6 (with revision marks)**

Nice in February:
This freak weather caused chaos with the Scandinavian delegates driving
from Nice to Sophia Antipolis, who have trouble with such severe weather conditions.

Contents

1 Opening of the meeting

The SA WG3 Chairman, Mr. V. Niemi opened the meeting which was hosted by ETSI in Sophia Antipolis, France.

SA WG3 had received the sad news of the loss of our SA WG3 Vice Chairman, Mr. Michael Marcovici, who died suddenly on 2 February 2005. The meeting held a 3 minute silence in memory and contemplation of Michael.

2 Agreement of the agenda and meeting objectives

TD S3-050001 Draft Agenda for SA WG3 meeting #37. This was introduced by the SA WG3 Chairman and was reviewed. The objectives for the meeting were also introduced as follows:

Meeting objectives:

- *The major objective of this meeting is to solve remaining open issues related to MBMS security and TS 33.246.*
- *We also try to get rid of all editor's notes in the other release 6 TSs and TRs.*
- *As a third objective, we should get work in Release 7 properly started*

The preliminary schedule was also introduced as follows:

Preliminary schedule of the meeting:

- *We begun with MBMS last time but it still has most open issues to be solved. Therefore, it may be good to begin again with MBMS issues in agenda item 6 to allow sufficient time for CR creation during the week.*
- *Then, the planned milestones for each day of the meeting are as follows:*
    - *Monday: completion of items 1-5 and good start with 6.20 (MBMS)*
    - *Tuesday: completion of 6.20 (MBMS) and also 6.21-6.25 and 6.1-6.4;*
    - *Wednesday: items 6.5-6.8, then 6.9 (GAA) and 6.18 (Presence);*
    - *Thursday: items 6.10-6.17 and 6.19;*
    - *Friday: handling of output documents and agenda items 7-10.*
- *These milestones are based on the experience from previous meetings. The schedules have to be adjusted to the number of contributions submitted to each agenda item.*
- *Additional break-out sessions are probably arranged in some evenings.*

The draft agenda was then approved.

2.1 3GPP IPR Declaration

The SA WG3 Chairman reminded delegates of their companies' obligations under their SDO's IPR policies:

IPR Declaration:

The attention of the delegates to the meeting of this Technical Specification Group was drawn to the fact that 3GPP Individual Members have the obligation under the IPR Policies of their respective Organizational Partners to inform their respective Organizational Partners of Essential IPRs they become aware of.

The delegates were asked to take note that they were thereby invited:

- to investigate whether their organization or any other organization owns IPRs which were, or were likely to become Essential in respect of the work of 3GPP.

- to notify their respective Organizational Partners of all potential IPRs, e.g., for ETSI, by means of the IPR Statement and the Licensing declaration forms (http://webapp.etsi.org/ipr/).

3 Assignment of input documents

The documents available at the beginning of the meeting were allocated to their appropriate agenda items, which is reflected in the document list.

4 Meeting reports

4.1 Approval of the report of SA3#36, Shenzhen, China, 23-26 November, 2004

TD S3-050002 Draft Report of SA WG3 meeting #36. The draft report was reviewed. It was reported that a further change had been requested by Axalto under document TD S3-041024 for clarification of the sentence. This was acceptable.

Action points from meeting #36:

AP 36/01: B. Sahlin to run an e mail discussion on IMS Security extensions (TD S3-040990, TD S3-040991 and TD S3-041038).
Completed. Input to this meeting.

AP 36/02: SA WG3 Chairman to request the upgrade of TR 33.878 to the 33.9xx series in order to allow reference to the Early-IMS work from within the Rel-6 specification set. If agreed, the SA WG3 Chairman to ask if SA WG3 can bring a CR to 33.102 to add a reference to this TR from a new informative Annex.
Completed. Presented to TSG SA (should be 33.203, not 33.102).

AP 36/03: Silke Holtmanns to provide a WID for Liberty Alliance / GAA work for the next SA WG3 meeting.
Completed. Input to this meeting (TD S3-050058).

AP 36/04: Silke Holtmanns to provide a CR to 33.220 to clarify the coding of P2 as characters into octet strings.
Completed. Input to this meeting (TD S3-050006).

AP 36/05: Yanmin Zhu to lead an e-mail discussion group on TD S3-041131 in order to try to solve the issue on MSK deletion and a revised CR submitted to the next SA WG3 meeting.
Completed. Input to this meeting (TD S3-050088,agreed in principle and TD S3-050089, for further discussion).

AP 36/06: M. Blommaert to run an e-mail discussion group and produce a LS to OMA BAC. SA WG3 members to review TD S3-041064 and provide comments by 13 January 2005. Draft LS provided by 17 January 2005, to be approved on 20 January 2004.
Completed, SA WG1 have noted the LS and output LS to OMA to be discussed at this meeting, based on the e-mail discussion.

4.2 Report from SA#26, Athens, Greece, 13-16 December, 2004

TD S3-050003 Report from SA#26 plenary. This was introduced by the SA WG3 Chairman and had been sent to the SA WG3 e-mail list after TSG SA meeting #26. The report was reviewed and noted.

4.3 Report from SA3-LI#16, Barcelona, Spain, 18-20 January, 2005

TD S3-050045 Draft report of SA WG3 -LI Group meeting (Barcelona). This was introduced by Berthold Wilhelm. Some CRs were produced and were sent on e-mail approval.

TD S3-050011 CR to TS 33.108: Aligning comments in National-HI3-ASN1parameters with comments in National-HI2-ASN1parameters (Rel-7). This CR had been approved by e-mail.

5 Reports and Liaisons from other groups

5.1 3GPP working groups

TD S3-050028 LS (from SA WG2) on protection of Rx and Gx interfaces. This was introduced by Ericsson and asked SA WG3 and CN WG3 to include protection of Rx and Gx interfaces in their specifications. A proposed response to this was provided in TD S3-050040 which was reviewed. The response LS was revised to take into account comments in TD S3-050112 which was reviewed and approved.

5.2 IETF

There were no specific contributions under this agenda item.

5.3 ETSI SAGE

Per Christoffersson gave a report on ETSI SAGE: Work is on-going on UEA2/UIA2 and is progressing to the expectations in the Work Plan (Draft reports expected Summer 2005).

AP 37/01: Chairman to ask the Specifications Manager for the best way to handle the UE2 / UIA2 work in the specifications set (numbering etc.)

5.4 GSMA

Charles Brookson provided a report from the GSMA Security Group. IMEI work is ongoing for countering the Stolen Handsets. The GSMA and the Manufacturers (EICTA) were giving regular reports to the EU TCAM Committee on the status. A new CEIR was being brought into operation, and handset with weak IMEIs were being investigated and listed. An increasing number of countries were introducing legislation to criminalise the changing of IMEIs.

The Security Group was working on countering Trojan Horses and Virus threats to mobile terminals. This was seen to be an important item for this year, as there was increasing evidence that executable code on smart phones was capable of being compromised. This could lead to an increase in fraud.

The GSMA had funded the work of SAGE in the definition of a new UMTS algorithm. A5/1 was now available throughout the world to all operators, and the GSMA Board have committed to phasing out A5/2 within two years. This strategy had also been the subject of negotiation with mobile and infrastructure manufacturers. It was expected that this would help any possible compromises from the proposed A5/2 weaknesses.

The next meeting will on the 7/8 June in Paris. An invitation was extended to anyone who might want to intend the meeting (and who were not GSMA members) to contact Charles Brookson to discuss attendance.

5.5 3GPP2

Due to the sad loss of the Vice Chairman, Michael Marcovici, the report of 3GPP2 security work was provided by Anand Palanigounder **<RETURN - few words from Anand>**

5.6 OMA

There were no specific contributions under this agenda item. An incoming LS (TD S3-050004) was dealt with under agenda item 6.20.

5.7 TR-45 AHAG

TR-45 AHAG had informed the SA WG3 Chairman that they would like another joint session with SA WG3. It was suggested that AHAG may be able to join SA WG3 during the Toronto meeting, otherwise another suitable venue would be looked for later in the year.

5.8 Other groups

TD S3-050005 Liaison Statement (from Q.9/17 Rapporteur Group) on General Security Policy for Secure Mobile End-to-End Data Communication. This was introduced by the SA WG3 Chairman. It was decided that this should be considered off-line and an e-mail discussion held in order to provide a response LS at the next SA WG3 meeting.

AP 37/02: Qiuling Pan, (ZTE to lead an e-mail discussion on the LS in TD S3-050005 and provide a draft answer to the LS to the next SA WG3 meeting.

6 Work areas

6.1 IP multimedia subsystem (IMS)

6.1.1 TS 33.203 issues

TD S3-050009 LS from TSG SA: Reply to TISPAN on Workshop on "IMS over Fixed Access". This was introduced by Ericsson. TSG SA informed ETSI TISPAN that 3GPP would like to ensure that the invitation is open to participants from all 3GPP OPs. 3GPP notes that even if CN1 and SA2 expert participation is requested, companies will send experts as they see appropriate. 3GPP also ask ETSI TISPAN to note that a workshop is not binding on the parent bodies; hence, agreements made at the WS will need endorsement in the parent bodies. The LS was noted.

TD S3-050024 LS from ETSI TISPAN: About the Workshop on "IMS over Fixed Access" (30-31 March 2005). This was introduced by France Telecom. ETSI TISPAN expect that the agenda for the Workshop will be arranged so as to cover the following aspects:

- status of 3GPP Release 6 and Release 7 IMS-related aspects,
- status of TISPAN_NGN Release 1 work,
- review of the status of the NGN-IMS issues raised in the June 2004 Workshop,
- identification of areas requiring coordinated resolution, and,
- future coordination/cooperation arrangements.

This LS was copied to SA WG3 for information and actioned SA WG2 to ensure the smooth organisation of 3GPP participation in the workshop. A response from SA WG2 was provided in TD S3-050030. The LS was noted.

TD S3-050030 LS from SA WG2: Reply LS on the Workshop on "IMS over Fixed Access" (30th – 31st March 2005). This was introduced by France Telecom. SA WG2 believe it would be relevant for the following 3GPP working groups to be involved in those discussions:

- IMS Specifications endorsement (Architecture, Requirements, SIP Profile…): SA WG1, SA WG2, CN WG1
- Services and Supplementary services specification: CN WG1, CN WG3
- User identification: SA WG2, CN WG4, **SA WG3**
- Authentication (ISIM/Login-password/EAP) and Security (IPsec/TLS) mechanisms: **SA WG3**
- "Gq" requirements: SA WG2, CN WG3
- QoS Classes: SA WG2, CN WG3
- Audio and Video Codecs use: SA WG4
- Emergency communications and Legal interception requirements: SA WG2, **SA WG3**

The LS was noted. It was agreed to forward this to the SA WG3 LI Group by sending it to their e-mail list. **A. Leadbeater agreed to inform the LI Group of this workshop and request participation of an LI member in the Workshop.** Some SA WG3 Members signalled that they were expecting to attend the Workshop.

TD S3-050048 Security extensions for IP Multimedia Sub-system - Issues identified and contributions presented at TISPAN. This was introduced by BT Group and provided SA WG3 members with a summary of issues that have been identified with TS 33.203 IMS security specification to provide security for IMS use in fixed network as is being defined by ETSI TISPAN NGN and future 3G scenarios as defined by 3GPP. BT Group concluded that when developing security extensions for IP Multimedia Sub-system, SA WG3 need to take the outlined issues into account when IMS is operated over the same operators GPRS network. BT Group were thanked for this comprehensive analysis of the TISPAN NGN work. It was agreed that SA WG3 should take the issues raised in this contribution into account when developing IMS security.

TD S3-050060 Proposed WID: Security extensions for IP Multimedia Sub-system. This was introduced by Ericsson, on behalf of Ericsson and Nokia and proposed changes to the WID to include the objective to include work on Fixed Access to IMS. It was reported that Vodafone and Nortel also support this WID proposal. Comments were provided in TD S3-050096 which was reviewed.

TD S3-050096 Comments on S3-050060 WID: IMS security extensions. This was introduced by Gemplus on behalf of Gemplus, Axalto and OCS and noted that the WID does not use the latest WID Template and proposed to indicate "Don't Know" for "UICC Applications" in section 9 of the WID, in order not to preclude necessary modifications of UICC applications. The TSG approved SA WG2 WID (TD SP-040686) was reviewed. The objective clause 4 states:

"*The objective of this work item is to provide possible IMS architectural enhancements necessary in the 3GPP system to support fixed broadband access to IMS, (e.g. as stated in ETSI TISPAN release 1). Where there are impacts to the IMS core, 3GPP intends to develop specifications or changes to specifications necessary to enable reuse of IMS as a platform for session control in systems with fixed broadband access. Any enhancements shall not break the integrity of the 3GPP system.*"

It was agreed that SA WG3 should only create a work item for additional access to IMS in order not to have any overlap with the SA WG2 WID. A revised version of the WID in TD S3-050060 should be provided to the next SA WG3 meeting, taking into account also the outcome of the TISPAN NGN Workshop.

AP 37/03: B. Sahlin to provide an updated WID, based on TD S3-050060 for next SA WG3 meeting, taking into account the outcome of the TISPAN NGN Workshop.

TD S3-050064 Access Security Requirements. This was introduced by Ericsson and examined some of the requirements that wired access networks pose to the access security solution. Ericsson proposed that the current access security solution needs to be expanded to accommodate these new requirements. Furthermore, this access security solution should be done in 3GPP, since it inherently has a lot of competence on IMS security related issues. A proposed CR was attached which added a requirement clause 5.5 to the IMS specification on Fixed-mobile convergence. Comments on this contribution were provided in TD S3-050095.

TD S3-050095 Comments on S3-050064 Access Security Requirements. This was introduced by Gemplus on behalf of Gemplus, Axalto and OCS and proposed that the current mandatory presence of a ISIM/USIM (i.e. smart card device) for IMS Access should be maintained for extensions to IMS Access and the presence of the ISIM/USIM application on a tamper-proof device in the UE should be mandated for fixed network access to IMS. There was some support for this requirement and it was also commented that the TISPAN "Soft smart card" approach may be adequate and not ruled out immediately.

It was agreed by SA WG3 that whatever solution is chosen for Fixed IMS Access should not reduce the level of security for the Existing 3GPP IMS Access.

It was considered that the concerns of companies should be taken to the TISPAN NGN Workshop in order to input their requirements which can then be reviewed and endorsed by SA WG1. **Member companies were asked to ensure that the requirements are discussed in the Workshop if they have any security implications from the SA WG3 view.** It was also recognised that the avoidance of duplication of work between ETSI TISPAN and 3GPP should be ~~avoided~~ ensured and guidelines for future work and co-operation should be developed and agreed. It was decided that the outcome from the Workshop should be reviewed by SA WG3 before sending any LSs on any security concerns and work-split and co-operation proposals.

TD S3-050065 TLS based access security to IMS. This was introduced by Ericsson and further discussed IMS security extensions, and why TLS should be seen as a very promising solution for Rel-7 IMS Access Security. Even though there is no decision in SA WG3 on the use of TLS for IMS Access Security, Ericsson encouraged other companies to take an open look at the idea, and invite interested companies to contribute to the technical work if TLS is chosen for Rel-7 IMS Access Security. It was suggested that these IMS Security enhancements should be handled as before, and SA WG1 should be involved in the requirements. It was therefore agreed to review these issues after the outcome of the TISPAN NGN Workshop. Members were asked to provide comments on this over the e-mail list and to reconsider the issues after the TISPAN NGN Workshop.

TD S3-050066 Co-operation between TISPAN WG7 and 3GPP SA3 on IMS security extensions. This was introduced by Ericsson and proposed to initiate formal co-operation with TISPAN and provide LSs. It was agreed that this should be postponed until after the TISPAN NGN Workshop. The attached draft LS was therefore noted at this time.

6.1.2 Security for early IMS

TD S3-050109 LS from CN WG1 on Early IMS Security TR 33.878. This was introduced by Vodafone and proposed some changes to the Early IMS draft TR. The changes were shown in an attachment which was reviewed. The proposed changes from CN WG1 were acceptable, but highlighted an inconsistency in section 6.2.4, so the text *"The UE shall apply this rule even if a UICC containing an ISIM is present in the UE."* will be removed from this section. The text "Full support of 3GPP TS 33.203 security features is preferred from a security perspective" was kept in the Introduction, to guide readers that the full IMS solution is preferred, if it is supported.

TD S3-050019 Pseudo-CR to 33.878: additional interworking cases. This was introduced by ZTE Corporation. Siemens requested not to add "*but the IMS network supports fully compliant IMS access security only*" and "*error*" in Step 10. With these changes the Pseudo-CR was agreed and the Editor was asked to include these changes in the draft TR.

TD S3-050035 security architecture of early IMS. This was introduced by ZTE Corporation and proposed to add a security architecture description in the draft TR. A Pseudo-CR was provided in TD S3-050036 to implement these changes in the draft TR. There were concerns that the interface between the UE and the SIP Transform device in the proposed architecture was not specified. It was considered that this should be discussed in SA WG2 in order to see if SA Wg2 see a need for this and decide the impacts and way forward if it is needed. ZTE Corporation were invited to provide contributions to SA WG2 on this. The Pseudo-CR was therefore rejected.

TD S3-050061 Proposed Pseudo-CR to 33.978: Correction of P-Asserted-Identity usage. This was introduced by Ericsson and was agreed for inclusion in the draft TR.

TD S3-050062 Proposed Pseudo-CR to 33.978: Clarification of IMPI/IMPU relationship. This was introduced by Ericsson and was covered by TD S3-050100.

TD S3-050100 Proposed Pseudo CR to 33.878: Clarifications and corrections. This covered changes in TD S3-050062. The use of "barred" in 6.2.4 was questioned, it was clarified that this was related to the IMS text in 22.228 and had the same meaning. This should anyway be checked after the meeting and a contribution brought in to change it if necessary. The contribution was agreed with minor changes and the editor was asked to include these changes in the draft TR.

TD S3-050063 HTTPS with early IMS. This was introduced by Ericsson and discussed the problem of HTTP traffic in early IMS context and included a Pseudo-CR with proposed changes. It was agreed that the added text should be a note. The second sentence "It is recommended ... UE authentication" was not needed and this should not be included in the draft TR.

The editor provided a new version of the TR in TD S3-050138 which was presented and revised to update the version number to 1.1.0 to reduce confusion over the change in number of the TR versus status of the two TR numbers in TD S3-050173 which was approved for sending to TSG SA for approval. The SA WG3 Secretary will provide version 2.0.0 to TSG SA Plenary after minor editorial clean-up.

TD S3-050044 Proposed CR to 33.203: Addition of reference to early IMS security TR (Rel-6). This was introduced by Vodafone and was reviewed and revised in TD S3-050139 which was approved.

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

TD S3-050013 Proposed CR to 33.200: Correcting address terminology for TCAP handshake (Rel-6). This was introduced by T-Mobile. The changes were agreed in principle, but it was noted that other proposed CRs overlap with these changes and may need to be combined for clarity. ~~<NEED TO KNOW FINAL STATUS AFTER CRs TD S3-050121 and TD S3-050122 were approved on TCAP>~~ The Early IMS evening discussions considered the combination of this CR with another TCAP handshake CR, and it was decided not to do this, so the CR in TD S3-050013 was confirmed as approved.

TD S3-050025 Proposed CR to 33.200: Addition of TCAP-Handshake for MO-ForwardSM (Rel-6). This was introduced by T-Mobile on behalf of T-Mobile, Siemens and Vodafone. It was reported that CN WG4 had received a proposed CR from Siemens and T-Mobile on this mechanism but the status was not known. Siemens and T-Mobile agreed to check this with CN WG4 colleagues and confirmed the MO-ForwardSM TCAP handshake had been approved by CN WG4. The changes were agreed in principle, but it was noted that other proposed CRs overlap with these changes and may need to be combined for clarity. The CR was modified to take into account the agreement made on TD S3-050121 and was provided in TD S3-050122 which was approved.

TD S3-050106 Addressing limitations of TCAP handshake for SMS transfer. This was introduced by Vodafone and discussed solutions for TCAP handshake for mobile terminated SMS transfer. Vodafone believed that the problem and solutions described in the contribution are equally applicable if TCAP handshake is also applied to mobile originated SMS transfer. The following approaches were foreseen:

1) **Mandate one of the proposed solutions:** This option should be taken if one solution is clearly better than the other from the point of view of feasibility and impact on existing entities.
2) **Specify the two solutions and mandate that one of them should be implemented, but do not specify which one:** This option should be taken if both solutions are of similar feasibility, or if the feasibility depends on existing vendor-specific implementations. This option is implemented in the CR provided in TD S3-050051.
3) **Specify the two solutions and mandate that one of them or an equivalently-secure alternative should be implemented:** This option should be taken if it is felt that vendors should be given the freedom to implement alternative solutions.

A proposed CR implementing approach 2) was provided in TD S3-050051 which was reviewed. It was commented that the average cost of the messages may be useful in order to judge the probability level needed. It was thought that this was not easy to determine and cannot be foreseen for future pricing schemes which may be used. It was reported that the cost should be measured in terms of the effort needed rather than monetary cost, i.e. the risk of detection and identification of the attacker will also be a cost factor. It was suggested that CN WG4 should be asked about the delay time of 1s and the probability value of 1/1000, recognising that this would delay the inclusion of the mechanism in Rel-6 by 3 months. The CR was revised in TD S3-050121 which was approved. Siemens asked for an example scheme for determining the probability (in terms of bits) in order to help implementers, to the next meeting.

TD S3-050012 Next steps for MAPsec. This was provided by T-Mobile and comments were provided by Siemens in TD S3-050071 which was reviewed. SA WG3 was asked to consider the following proposals, and to accept them as working assumptions:

1. The gateway concept will only include two ‘protection profiles’: ‘Integrity only and ’integrity and confidentiality’.
   Agreed as a working assumption.
2. Any protocol on top of TCAP will be protected when passing through the gateway.
   Agreed as a working assumption.
3. Explicit verification of SCCP and MAP-payload addresses against MAPsec SPI will be studied.
   Agreed to study this.
4. The MAPsec Gateway concept and the MAPsec Rel-4 NE-based solution need not coexist. A solution needs to be found, how to ‘delete’ the MAPsec Rel-4 NE-based solution from the 3GPP specs.
   Agreed - the existence of Rel-4 NE Gateways should be checked and a way of removing the Rel-4 support should be determined.

AP 37/04: M. Pope to discuss the best way to handle the removal of MAPsec Rel-4 NE-based solution from the 3GPP specs and report back to SA WG3.

It was proposed to ask CN WG4 feedback on the above proposals. This was agreed and a LS was provided in TD S3-050123 which was reviewed and revised to clarify the layer of protection intended in TD S3-050167. This was again revised to correct the document number and remove "draft" in TD S3-050174 which was approved.

Stefan agreed to be the Rapporteur for the MAP Security work.

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

There were no specific contributions under this agenda item.

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

TD S3-050050 Proposed WID: NDS Authentication Framework Extension for TLS. This was introduced by Nokia and was reviewed. Siemens and T-Mobile expressed concern that there was no good justification for this WID and asked for more justification from Nokia at the next meeting. More supporting companies would also be required to agree this WID.

6.5 UTRAN network access security

TD S3-050101 Review of recently published papers on GSM and UMTS security. This was introduced by Siemens on behalf of Vodafone and Siemens and reviewed the papers by Ulrike Meyer (Darmstadt University of Technology, Germany) and Susanne Wetzel (Stevens Institute of Technology, New Jersey, USA):

- Meyer, U, Wetzel, S.: On the impact of GSM Encryption and Man-in-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks. Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC2004), September 2004, IEEE, 2004.
- Meyer, U., Wetzel, S.: A Man-in-the-Middle Attack on UMTS. Proceedings of ACM Workshop on Wireless Security (WiSe 2004), October 2004, ACM, 2004.

Siemens and Vodafone do not believe that the papers require 3GPP to make any changes to the UMTS security specifications. The most significant contribution of the papers in this area is to highlight the case when a UMTS subscriber is authenticated via a GSM BSS connected to a 2G MSC and then handed over to UMTS (case 5 in section V.A of the PIMRC paper) and believe that re-authentication at 2G -> 3G MSC/SGSN change in idle mode can be implemented by suitable configuration of authentication policy settings on existing MSCs and SGSNs. If the proposed countermeasures are agreed by SA WG3 then they should be forwarded to the GSM Association who could turn them into recommendations for operators.

The proposals were discussed briefly in the meeting and it was agreed that an e-mail discussion should be held on this and a new contribution on the agreeable proposals should be contributed to the next SA WG3 meeting in order to allow a liaison to be sent to the next GSMA meeting in June 2005.

AP 37/05: G. Horn to run an e-mail discussion based on TD S3-050101 (Review of recently published papers on GSM and UMTS security) and provide a contribution to the next SA WG3 meeting.

TD S3-050107 LS from CN WG1: Misalignment amongst the 3GPP specifications, “Re-authentication and key set change during inter-system handover”. This was introduced by Ericsson and reports a misalignment among 3GPP specifications and asked TSG SA to instruct WGs appropriately to resolve the problem. There was no identified impact on SA WG3 specifications and the LS was noted.

6.6 GERAN network access security

TD S3-050037 Adoption of key separation for GSM/GPRS in the short term. This was introduced by Orange and recommends that Key Separation should be introduced in the short-term to prevent any potential loss in confidence in the system:

The advantage of this is that if the introduction of key separation is done in the short term, it can prevent that vulnerabilities spread from A5/1 to A5/3 from the beginning of the introduction of A5/3. It would also be in accordance with the recommendation made by GSMA Security Group in the LS in TD S3-030490 (September 2003) to introduce a key separation mechanism together with A5/3 introduction. "Having considered the matter at its last meeting, in the light of the new attacks that have recently been presented on GSM ciphering, SG came to the conclusion that it should be a priority to introduce a mechanism that separates keys for use with different encryption algorithms. For this reason SG wishes to express that the introduction of such a key separating mechanism should be aligned with the introduction of A5/3."

It was reported that the GSMA SG had changed it's opinion since the LS in TD S3-030490 and believe the removal of A5/2 is a sufficient short-term measure.

There were differing views over the introduction of Key Separation and on the urgency to do so if it is found to be necessary in the GERAN Security Feasibility Study (expected completion June 2005).

It was clarified that the intention of this contribution was not to delay A5/3 introduction, but to deploy Key Separation as soon as possible and ideally at the same time as A5/3.

The LS from SAGE in TD S3-050093 was reviewed and it was decided to await the result of the GERAN Security FS before deciding on Key Separation deployment.

TD S3-050093 LS from ETSI SAGE: LS from ETSI SAGE: Response on key separation for GSM/GPRS encryption algorithms. This was introduced by Per Christoffersson and provided SAGE comments on the strengths of the members of the A5 algorithm family. It was agreed to include this information in the GERAN Security FS. It was clarified that A5/1 could be regarded as the next weak spot for cryptanalysis aiming at non-real time eavesdropping (days-hours-minutes depending on resources) and thus potentially making also A5/3 encrypted traffic vulnerable. However, real time fraud using A5/1 and BBK techniques does not seem possible for the near future.

TD S3-050068 Update for Access Security Enhancements Feasibility Study. This was introduced by Ericsson. It was pointed out by Ericsson that the text on Threats in section 8 had not been fully analysed and should be studied further. Section 7.5 should be re-worded to clarify it is the network which does the detection, not the terminals. Comments were requested to the Editor (Bengt Sahlin) in order to produce a baseline TR at the next meeting. It was also requested that a better title for the TR should be found to clarify that it is primarily a GERAN Access Security study.

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 S3-050102 LS from CN WG5 (OSA) to SA WG3 on updating TR 33.919. CN WG5 asked SA WG3 to agree to the CR proposed against the "Application guidelines to use GAA" and “References” clauses in Rel-6 TR 33.919 attached to the LS. The Proposed CR to 33.919 had been discussed over e-mail and was reviewed. The proposal was acceptable and the CR was editorially cleaned to add CR number, etc in TD S3-050150 which was approved.

TD S3-050055 GAA Enhancements. This was introduced by Nokia and proposed a new WID on GAA enhancements. There was some concern over the list of enhancements, it was clarified that these were possible enhancements and may not be done, whereas there is also possibility to add other enhancements. The idea for the WID is to study and propose potential useful enhancements to GAA. It was decided that more background is needed for the scope of this work and more supporting companies were required. It was suggested that service requirements from SA WG1 should be checked to see if this work would be useful. It was decided that more discussion on the scope and requirements for GAA enhancements should be done before the next SA WG3 meeting, including an indication of the service requirements.

AP 37/06: S. Holtmanns to discuss GAA Enhancements WID and develop the scope and need for the work, and present the WID again with enough supporting companies (re: TD S3-050055).

TD S3-050053 Introducing 2G GBA. This was introduced by Nokia and suggests that there should be a way to offer services whose authentication is based on GAA also to 2G subscribers. This document introduces the concept and needed changes to GAA related specifications. Also, it should be noted that the approach taken in this contribution is meant for existing SIMs, i.e. it does not cause any change needs to the existing SIM specifications, in particular GBA_U as in 3G will not be included in 2G GBA. A WID was attached to cover the work on 2G GBA. There was some discussion over the use of 2G security for 3G services, such as GBA. It was reported that OMA have some support for using SIM for 3G-based services due to the high penetration of SIMs on the market and the time it will take to change them for USIM devices. It was commented that this proposal would allow the use of SIM-based authentication for non-3GPP applications. Rogers Wireless signalled their support for SIM-based access to GBA.

It was decided that both the general principle of allowing SIM-based access and therefore 2G security for access to 3G systems and the impacts of not allowing this on the take-up of 3G services (e.g. OMA service definition). **Members were asked to discuss this both on the e-mail list and internally within their companies to try to obtain a firm view on these issues. Contributions should be brought to the next SA WG3 meeting.**

Comments to this proposal were provided by Qualcomm in TD S3-050097 which was also reviewed.

TD S3-050097 Response to S3-050053: Alternative approach to 2G GBA. This was introduced by Qualcomm and proposed alternate cryptographic principles for consideration to the proposal in TD S3-050053. Qualcomm concluded that there are potential security benefits to using mutually-authenticated Diffie Hellman for key agreement between UE and BSF, and proposed that SA WG3 consider the feasibility of this alternative in the event that there is support for a 2G GBA work item. This should await the outcome of 2G Security to 3G services contributions at next meeting.

6.9.2 TS 33.220 GBA

TD S3-050006 Proposed CR to 33.220: Key derivation function: character encoding (Rel-6). This was introduced by Nokia. Editorial errors were noted (less-than-equal signs lost and use of letter "l" for the variable is mistaken as number 1) so this was revised in TD S3-050140 and reviewed and revised to remove UICC impact in TD S3-050168 which was approved.

TD S3-050056 GBA User Security Settings (GUSS) transfer optimisation. This was introduced by Nokia. The mechanism of the GUSS counter was clarified and it was explained that the comparison of the timestamps was used. It was noted that the "~~timestamp~~ GUSS not available" mechanism is not described so the CR was rejected for Rel-6 and may be reconsidered for Rel-7 when further clarifications are available.

TD S3-050079 Optimisation of GBA. This was introduced by Ericsson and discussed some possible optimisations for GBA and shows two possible ways to optimise the GBA procedure. Ericsson proposed that SA WG3 take these alternatives into account when GAA enhancement are studied further. The optimisations may also be useful in Liberty – GAA interworking. Siemens commented that the messages shown in Figure 1 included repeated Authz Header in the same message from the UE which could not be done according to the specifications. Siemens also asked whether this was an alternative GBA architecture proposal, rather than a GBA optimisation. Ericsson were asked to discuss and develop this further and consider proposing further optimisation in a future meeting.

TD S3-050058 Proposed WID: Liberty Alliance and 3GPP Security Interworking. This was introduced by Nokia and included the discussion and comments received since the last SA WG3 meeting. Vodafone were willing to be added to the supporting Companies for this proposed WID. It was noted that at least one more supporting company was needed for this WID. The work of Liberty Alliance on this was not clear in the WID and could be made more explicit in the results part of section 4. The supporting companies for this WID were asked to discuss this further and solicit more company support before re-submitting this proposed WID (Siemens indicated that they would support such a revised WID). The WID was updated in TD S3-050142 and reviewed. This was considered to be a Feature-level WID and was revised in TD S3-050169 which was approved.

TD S3-050067 Bootstrapping timestamp. This was introduced by Nokia on behalf of Nokia, Siemens and Vodafone and discussed why the current approach causes unnecessary complexity in the NAF, and argued why the bootstrapping timestamp is needed in the Zn reference point. It was concluded that to simplify the NAF procedures and management, and to avoid unnecessary complexity in the NAF, the bootstrapping timestamp should be transferred over the Zn reference point from the BSF to the NAF. An associated proposed CR was attached to the contribution which was revised to update figures 4.4 and 4.5 and to remove UICC impacts from the cover sheet in TD S3-050143 which was approved. **Silke Holtmanns agreed to report the approval of this CR approval to the CN WG4 Chairman so their conditionally approved CR can be approved.**

TD S3-050086 Proposed CR to 33.220: Storage of B-TID in GBA_U NAF Derivation procedure (Rel-6). This was introduced by Gemplus on behalf of Gemplus and Axalto and was reviewed and approved.

TD S3-050020 Security capability negotiation in GBA. This was introduced by ZTE Corporation and suggested to add security capability negotiation procedure in GBA and to specify the detail. ZTE Corporation also introduced the idea and mechanism of a security grade proposal. A related CR to implement these proposals was provided in TD S3-050021. It was commented that the GBA specification is not designed for algorithm negotiation, but is intended for shared secret transport between arbitrary entities. The number of algorithms that may be used in the generic case would be very wide and many would include their own algorithm negotiation mechanisms. ZTE responded that the scope of the GBA specification should be checked to ensure that it is clear for the intention of GBA. This was checked off-line and the security grade proposal was not considered acceptable for Rel-6. The CR in TD S3-050021 was therefore rejected.

TD S3-050021 Proposed CR to 33.220: Security capability negotiation in GBA (Rel-6) (Note: This document was given the wrong CR number and should have been marked as CR049). This was introduced by ZTE Corporation and provided the changes needed to implement their proposals in TD S3-050020. This CR was rejected as the base proposal in TD S3-050020 had not been accepted.

6.9.3 TS 33.221 Subscriber certificates

There were no specific contributions under this agenda item.

6.9.4 TS 33.222 HTTPS-based services

TD S3-050042 Proposed CR to 33.222: Clarification to TS 33.222 (Rel-6). This was introduced by Ericsson and proposed adding a note to clarify the need for having AP between the UE and AS. This CR revised in TD S3-050144 and was approved.

TD S3-050057 Proposed CR to 33.222: Keeping PSK TLS in 3GPP Rel-6 (Rel-6). This was introduced by Nokia and introduces the PSK TLS in the specification. These changes had already been endorsed by SA WG3 but the completion of PSK TLS was not clear so the CR was not sent for TSG approval in December 2004. The CR was reviewed again in TD S3-050145 and was approved.

TD S3-050069 Proposed CR to 33.222: Clarify the GBA requirements for https supporting applications at Ua reference point (Rel-6). Siemens revised this after off-line discussions and a new version of the CR was provided in TD S3-050146 which was revised again to merge the content of TD S3-050103 in TD S3-050175 (see below).

TS 31.111, TS 31.130, TS 31.116 specify the USIM Application Toolkit and Applets.

TD S3-050103 Proposed CR to 33.222: Clarify the GBA requirements for https supporting applications at Ua reference point (Rel-6). This was introduced by Gemplus on behalf of Gemplus, Axalto and OCS as an alternative to the CR in TD S3-050069 (TD S3-050146).

TD S3-050098 Comments to S3-050069 “Clarify the GBA requirements for https applications at Ua reference point”. The attached CR was revised in TD S3-050103. A presentation was provided describing a way to use the Ks_int_NAF for HTTPS which was presented by Gemplus on behalf of Gemplus, Axalto and OCS in TD S3-050147. It was argued that there was no use-case identified for Rel-6 and the Key support could be restricted for simplicity, which does not preclude extension in Rel-7 onwards if use-cases are identified.

TD S3-050175 Proposed CR to 33.222: Clarify the GBA requirements for https supporting applications at Ua reference point (Rel-6). This was provided after an evening discussion in order to include the requirements of TD S3-050069 and TD S3-050103 which was introduced by Axalto and reviewed and approved. A LS to TSG SA was provided to explain the need for further study on HTTP in TD S3-050175.

TD S3-050176 LS (to TSG SA) on HTTPS connection between an UICC and a network application function. This LS included a request for time to study the HTTP issues and NAF impacts and was approved. It was noted that if TSG SA do not grant time to study this, then the editors' note in TD S3-050175 will be removed at TSG SA Plenary and the CR revised for approval.

It was agreed that the deadline for contributions on this topic, in order to give time for discussion and response will be Tuesday 12 April 2005, 16.00 CET, comment deadline remains the usual document Tuesday 19 April 2005, 16.00 CET.

6.10 WLAN interworking

TD S3-050027 LS from SA WG2: RE:LS on Control of simultaneous accesses for WLAN 3GPP IP access. This was introduced by Qualcomm and asked for clarification on what type of “fraud” that SA3 would like to prevent and asked if a simple counter could be used instead of the Boolean flag to indicate if the W-APN tunnel is active. Ericsson provided a CR in TD S3-050041 to try to clarify this. After the discussion and update of the CR, a response LS to SA WG2 was provided in TD S3-050152 which was revised in TD S3-050179 and approved.

TD S3-050041 Proposed CR to 33.234: Clarification on the handling of simultaneous sessions (Rel-6). This was introduced by Ericsson and was reviewed. The CR was revised to make other consistency corrections to show that there can be a generalised "N" IKE SAs, rather than only one. The consequences also required improvement and was modified accordingly in TD S3-050151 which was reviewed and approved. **Further discussion on the IKE SA sharing should be held off-line and further CRs provided to the next SA WG3 meeting if needed.**

TD S3-050108 LS from CN WG1: Alignment of specifications between CN1 and SA3 with respect to fallback to full authentication. This was introduced by Nokia. CN WG1 asked SA WG3 to consider the approved CN WG1 CR and align specifications to it. A proposed CR to make the corresponding changes was provided by Nokia and Ericsson in TD S3-050149 which was reviewed and an issue found with including pseudonyms with fast re-authentication in the internet drafts. After off-line discussion, the CR was withdrawn and an LS provided in TD S3-050153 which was approved.

TD S3-050010 LS from SA WG3-LI Group: Reply to LS on Need for the IMSI at the PDG. This was introduced by BT Group and was a response to CN WG4 on questions about the need for IMSI at the PDG. CN WG4 were asked to confirm whether the MSISDN is available at the PDG for a PS domain only subscriber. This was sent to SA WG3 for information and was noted. A response to this from CN WG4 was provided in TD S3-050111.

TD S3-050111 LS from CN WG4: Reply to Reply LS on Need for the IMSI at the PDG. This was introduced by BT Group and confirmed to the LI Group that MSISDN is available at the PDG for PS Domain only subscriber. The LS was input to SA WG3 for information in connection with the LS in TD S3-050010 and was noted. The security implications related to sending the IMSI over the interface should be checked by SA WG3 Members.

TD S3-050018 Discussion about Using OCSP to Check Validity of PDG Certificate in 3GPP IP Access. This was introduced by ZTE Corporation. The CR approved in TD S3-041100 introduced that it is mandatory for the UE to support OCSP to check the validity of a PDG certificate. This contribution discussed how to use OCSP in 3GPP IP Access and proposed that SA WG3 asks the IETF IPsec WG to consider enveloping certificate status in IKEv2 messages. Nokia reported that they didn't think enveloping would give any security improvement. Ericsson commented that there may be some advantages, but these would need to be studied and that such a request should be taken directly to the IETF instead of SA WG3 in order to propose the creation of a draft which SA WG3 could consider when it is available. It should also be checked whether this work is currently being done in the OMA. It was also suggested that the solution (1) given in the contribution could be included as a note in the TS in order to indicate how this can be done. After some discussion it was decided that a CR should be produced and this was provided in TD S3-050155 and was reviewed and revised in TD S3-050177 which was approved.

TD S3-050031 Threat of users accessing each other in link layer. This was introduced by ZTE Corporation. User access in link layer is a threat to the assets of both user and 3GPP operator. There is a requirement to segregate user traffic at AP and access controller in WLAN AN. ZTE Corporation suggested discussing this topic, adding the threat of users accessing each other in the link layer to Annex C.2, and adding corresponding requirements in section 4.2. The CR on these changes was provided in TD S3-050032 which was reviewed. The addition of the new section 4.2.6 was not agreed and it was agreed that recommendations should be added to Annex C instead. The CR was revised in TD S3-050156 and was reviewed and revised in TD S3-050178 which was approved.

TD S3-050059 Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages. This was introduced by Nokia and proposed that the 3GPP AAA server should use the Diameter/RADIUS accounting start message instead of a successful EAP authentication exchange to detect when a WLAN Direct IP Access session has been created. If proposal this is accepted, some modifications would be needed to both TS 23.234 and TS 33.234. A proposed CR to 33.234 was attached to this contribution which was reviewed. The corresponding changes in TS 33.234 had not been done and it was doubted whether this could be completed for Rel-6. It was therefore considered a potential for Rel-7. After off-line discussion between companies, a revision to the attached CR was provided in TD S3-050181 which was reviewed and approved. **The termination part should be checked and the impact and need for CRs for other specifications should be checked**.

AP 37/07: Nokia to check the termination part of TD S3-050181 and the impact and need for CRs for other specifications

TD S3-050039 Proposed CR to 33.234: WLAN AN providing protection against IP address spoofing (Rel-6). This was introduced by Nokia on behalf of Nokia and ZTE Corporation. If charging is based on IP addresses, then there is a recognised IP address spoofing threat, which is outside the scope of 3GPP WLAN Interworking work and is the responsibility of the WLAN AN provider to protect against this if this charging method is used. It was suggested that this is clarified in the TS in a note to provide a recommendation not to use this charging method or that sufficient protection against IP address spoofing is implemented in the WLAN AN. The CR was revised to include this recommendation in TD S3-050157 which was reviewed and revised in TD S3-050180 and approved.

TD S3-050022 Proposed CR to 33.234: Clarification on EAP-AKA(SIM) description in 3GPP IP access authentication and authorization (Rel-6). This was introduced by ZTE Corporation. It was revised to clarify the (SIM) in TD S3-050158 which was approved.

TD S3-050038 Proposed CR to 33.234: Clarifying the status that can’t be changed in the security requirement of WLAN-UE split (Rel-6). This was introduced by Nokia on behalf of Nokia and Ericsson. The UICC impact was removed and the CR revised in TD S3-050159 which was approved.

TD S3-050014 Proposed CR to 33.234: Wu Reference Point Description (Rel-6). This was introduced by ZTE Corporation on behalf of ZTE Corporation and NOKIA and was approved.

TD S3-050148 Proposed CR to 33.234: Removal of editors' notes (Rel-6). This was introduced by Nokia on behalf of Nokia and BT. This was revised in TD S3-050160 and was approved.

TD S3-050015 Proposed CR to 33.234: Replacing PDGW with PDG (Rel-6). This was introduced by ZTE Corporation and was revised to Category D in TD S3-050161 which was approved.

6.11 Visibility and configurability of security

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

There were no specific contributions under this agenda item.

6.16 Open service architecture (OSA)

There were no specific contributions under this agenda item.

6.17 Generic user profile (GUP)

There were no specific contributions under this agenda item.

6.18 Presence

There were no specific contributions under this agenda item.

6.19 User equipment management (UEM)

There were no specific contributions under this agenda item.

6.20 Multimedia broadcast/multicast service (MBMS)

TD S3-050004 LS from OMA BAC: Status of OMA Mobile Broadcast Services. This was introduced by Ericsson and provided further status on the Mobile Broadcast Services work within OMA. An e-mail discussion on this had been held, and a response draft LS to be used as a base for further discussion was provided in TD S3-050113 and reviewed and revised in TD S3-050171 which was approved.

TD S3-050029 LS from SA WG2: Reply to Liaison Statement on Status of OMA Mobile Broadcast Services. this was taken into account with TD S3-050004 discussions and was noted.

TD S3-050008 LS from SA WG4: Reply on "LS on MBMS Security finalisation". This was introduced by Ericsson and informed SA WG3 that SA WG4 supports the proposal in TD S3-040884 that “SA WG3 would provide a detailed description of the SA WG3 procedures, so that SA WG4 could do the actual stage 3. SA WG3 will do the stage 3 of the MIKEY messages”. SA WG4 is willing to do the stage 3 work, for the security functions defined in stage 2 by SA WG3. The work split agreed on is in more detail described in TD S3-040847. Siemens commented that the reply to SA WG4 should be finalised after the SA WG3 CRs proposed on these subjects are agreed or rejected. This was therefore postponed until after the handling of TD S3-050075. A LS was provided in response to SA WG4 LS (TD S3-050008) in TD S3-050131 which was reviewed and approved.

TD S3-050026 LS from SA WG2: Reply to Liaison Statement on MBMS User Service architecture. This was introduced by Siemens and confirmed that the assumptions made in TS 26.346 seem to be correct. SA WG2 pointed out that since the SA WG3 LS was raised, SA WG2 passed a number of CRs on 23.246 at its November meeting which may have impact on 26.346. The LS in TD S4-050166 was reviewed. MBMS Security Function had received comments and it was proposed that SA WG3 look again and decide what is required for Security Sub-Functions. After the handling of the SA WG3 MBMS CRs, the SA WG2 CR was reviewed for any conflicts. Some conflict was found and it was also recognised that SA WG4 had received LSs from SA WG3 and SA WG2 with conflicting requirements. it was decided that an LS to SA WG2 should be produced to explain the situation in TD S3-050172 which was revised in TD S3-050182 and was approved.

TD S3-050080 Status of MIKEY related IETF work. This was introduced by Ericsson and provided the status of MIKEY related IETF work. Needed changes were implemented in the attached Proposed CR to TS 33.246. The Attached CR was reviewed. It was debated whether the other editors' note in section 6.4.4 should be replaced by a reference to the RFC which will contain the Type Value when it is ready. It was decided that the editors' note should stay in the specification for the moment and removed when the RFC is available.

TD S3-050114 Proposed CR to 33.246: Alignment according to MIKEY related IETF work. This CR was produced as a revision of the attached CR in TD S3-050080 and was approved.

TD S3-050105 Proposed CR to 33.246: Clarify MUK key synchronisation for MSK push procedure (Rel-6). This was introduced by Siemens. The CR was revised in TD S3-050115 which was approved.

TD S3-050077 Proposed CR to 33.246: Clarify the usage of the MUK in the BM-SC solicited pull procedure (Rel-6). This was introduced by Gemplus on behalf of Gemplus and Axalto. It was noted that the figure is also changed by another CR and this may need review after dealing with the other CR in order to merge the changes into a single CR if possible. The changes were therefore approved in principle and the changes were harmonised with changes in TD S3-050084 in the evening session (this CR was then withdrawn and the CR in TD S3-050084 was revised in TD S3-050133).

TD S3-050074 Proposed CR to 33.246: Add missing parts of CR033 (SA3#36) (Rel-6). This was introduced by Siemens and proposed re-introducing the changes which were omitted from the agreed CR033 when the combined CR was drafted. This CR was approved.

TD S3-050092 Proposed CR to 33.246: Removing IDi from MTK message (Rel-6). This was introduced by Ericsson and included changes which were omitted a previously agreed CR. This CR was approved.

TD S3-050078 Proposed CR to 33.246: Annex D1: correction of the description of the GBA run (Rel-6). This was introduced by Gemplus on behalf of Gemplus and Axalto. This CR was approved.

TD S3-050110 Proposed CR to 33.246: Incompletely implemented CRs from SA3#36 (Rel-6). This was introduced by Ericsson. The change in 6.3.2.1 was covered by the CR in TD S3-050074 and so was removed from the proposed CR in TD S3-050116 which was approved.

TD S3-050072 MSK verification message handling. This was introduced by Siemens and discussed MSK verification handling and proposed a CR to implement the proposed solution in the specification. This was revised in TD S3-050117 and was approved.

TD S3-050076 Proposed CR to 33.246: Clarify Time Stamp verification in MSK Verification Message procedure (Rel-6). This was offered as an alternative to the proposal agreed in TD S3-050117 and was therefore withdrawn.

TD S3-050033 Discussion about MSK MIKEY Message Reception in the ME. This was introduced by ZTE Corporation. A CR to implement this proposal was provided in TD S3-050034. The procedure for success/failure reporting was discussed in the off-line MBMS session and the CR updated in TD S3-050118 which was discussed off-line and reviewed again. It was updated editorially in TD S3-050166 which was approved.

TD S3-050082 Proposed CR to 33.246: Usage of security policy payload (Rel-6). This was introduced by Ericsson. Siemens commented that this changed back what had already been agreed by SA WG3 in CRs. This was left for off-line discussion and the CR revised in TD S3-050135 which was reviewed and approved.

TD S3-050119 Reply LS (from SA WG4) on Reception Acknowledgement for MBMS. SA WG4 asked for urgent answers on their 2 questions regarding MBMS Reception Acknowledgement for the following:

1) SA WG4 understands TS 22.246 (MBMS Stage 1) explicitly requires a secured mechanism for delivery verification. SA WG4 would like to get confirmation that SA WG3 will provide integrity protection using HTTP Digest within MBMS Rel-6 for this procedure.
2) SA WG4 would like to get confirmation that SA WG3 will provide secure charging based on a delivery acknowledgement - according to the solution indicated in the discussion part - within MBMS Rel-6.

It was decided to allow this to be considered overnight in order to provide an agreed response quickly to SA WG4. For question 1), it was considered that this was already covered by SA WG3 specifications, using HTTP-Digest and the terminology used in SA WG3 should be checked to match with that used by SA WG4. For Question 2) it was advised that the charging should be based on MSK delivery, as if the user doesn't receive it on first send, it can use the pull procedure to get the MSK. An LS was provided after off-line discussion in TD S3-050126 which was reviewed and approved.

TD S3-050046 ME based MBMS key derivation for ME based MBMS key management. This was introduced by Nokia on behalf of Nokia and Siemens. The current MBMS specification (TS 33.246) lacks the key derivation details when the UE is equipped with a UICC that does not support MBMS key management functions (i.e. a GBA_U-unaware UICC has been inserted). In this case, both the MRK and the MUK must be derived from the single NAF specific key Ks_NAF as specified in TS 33.246. This paper discussed the possible methods to derive the needed MBMS keys and proposed that for ME based key management a simple MRK key derivation function (Variant-1 using GBA's key derivation function) is used. A proposed CR implementing this was provided in TD S3-050047 which was reviewed, it was clarified that MUK is not derived from MRK (i.e. the opposite derivation from that proposed) because if MIKEY is successfully attacked, MRK still cannot be obtained. The issues were resolved and the CR revised to remove UICC Apps impact in TD S3-050162 which was approved.

TD S3-050049 Proposed CR to 33.246: On the derivation of the GBA keys for MBMS (Rel-6). This was withdrawn as it was covered by the CR in TD S3-050047.

TD S3-050054 Protection of Service Announcements. This was introduced by Nokia and presented some possible methods to protect service announcements and evaluates them. The paper also considered whether it is practical to protect service announcements or not. Nokia proposed that service announcements are not protected, because if an attacker can modify a service announcement, then it is also possible to modify broadcast or multicast MBMS data. If the protection is required anyway then the binding model should be used, because it requires only modifications to the MRK derivation and it is more secure than pre-shared key and two-layered model. The proposal was agreed (i.e. not to protect). It was also noted that a CR would be needed to correct the reason for not protecting the service announcements. This CR was prepared in an evening session in TD S3-050124 which was reviewed and approved.

TD S3-050104 Proposed CR to 33.246: MBMS download protection details. This was introduced by Nokia and provided a CR in response a the LS from OMA (attached to the contribution). The LS in OMA-DLDRM-2005-0044 was reviewed. OMA-DLDRM reported that they could specify the requirements, but would need to update the specification versions first. It was concluded that this may be available for Rel-7 and should be revisited when OMA DLDRM have specified the protection details. **It was clarified that any future upgrades to OMA DRM V2.0 do not apply to this Rel-6 MBMS specification and a note was added to 6.6.3.2 to clarify this.** If the OMA finalise their specification work in time to include it in Rel-6, then this can be reviewed later by SA WG3 for inclusion. The CR revised in TD S3-050125 which was reviewed and it was noted that the profiling would need to be checked to ensure it was compatible. This was done and the CR updated again to take the profiling into account in TD S3-050154 which was reviewed and approved.

TD S3-050170 LS from OMA BAC DLDRM: Answer to LS on Adapting OMA DRM v2.0 DCF for MBMS download protection. This was received late in the meeting but had already been handled with TD S3-050104 as it had been attached to that contribution. A CR was produced as a result of this LS in TD S3-050154.

TD S3-050099 More reliable acknowledgement of MSK delivery. This was introduced by Ericsson and contained a proposal to increase the reliability of the acknowledgement of MSK delivery and gives a more robust way of charging users based on MSK reception than the current two-way “handshake”. A proposed CR to implement this proposal was attached to the contribution. It was commented that this did not really add any deterrent for the malicious user, but added extra reliability for MSK delivery in some radio conditions. It was commented that this procedure would improve UICC key management, but does not solve the problem of a malicious ME not sending the acknowledgement. Another solution would be to base charging on MSK availability (it is pushed to the user, if the user receives content it cannot use, it can then do a Pull to get the MSC. No agreement could be made on the use of the mechanism and it was decided to consider the result of the LS in TD S3-050119 on this issue (see above). A response LS was provided in TD S3-050126.

TD S3-050088 Proposed CR to 33.246: MGV-F functionality related to MTK-ID upper limit (Rel-6). This was introduced by Samsung. It was proposed to define the variables SEQs and SEQu in the definitions and remove it from re-definition in the main body of the CR. The CR was revised in TD S3-050127 which was further updated to add consistent abbreviations and definitions in TD S3-050163 which was reviewed and approved.

TD S3-050137 Proposed CR to 33.246: Introduction of missing abbreviation, symbols and definitions (Rel-6). This was introduced by Axalto and was produced after drafting collaboration to provide a necessary set of abbreviations and definitions. The CR was reviewed and approved.

TD S3-050089 Proposed CR to 33.246: Stop the usage of one MSK (Rel-6). This was introduced by Samsung. There was objection to the fifth bullet point and the first bullet point was unclear as the specification of the maximum number of MSKs should be better defined. The other bullets did not seem to add any new requirements or clarification and could be left to implementation. it was agreed to have an off-line MBMS discussion. The CR was revised in TD S3-050128 which was still unacceptable and was revised again in TD S3-050164. This was covered by the CR in TD S3-050133 and was therefore withdrawn.

TD S3-050085 Proposed CR to 33.246: Requesting specific MSK (Rel-6). This was introduced by Ericsson. Some clarification was needed and this was discussed in an off-line MBMS session and the CR revised in TD S3-050129 and reviewed and agreed in principle, as it was considered best if this is merged with the CR in TD S3-050133 if that CR is also acceptable. TD S3-050129 was withdrawn after approval of TD S3-050133.

TD S3-050081 Details of HTTP procedures. This was introduced by Ericsson and described how the MBMS security related HTTP procedures could be implemented in the specifications. A proposed CR to implement this was attached. The attached CR was reviewed. **It was noted that the removal of editors' notes in the TS was becoming urgent and the issues raised by them should be considered seriously by SA WG3 Members.** Comments had been provided by Siemens in TD S3-050094.

TD S3-050094 Comments on (S3-050081/S3-050090). This was introduced by Siemens and provided comments on the analysis and CR in TD S3-050081. The comments were discussed and necessary changes to the CR in TD S3-050081 were made in an off-line MBMS session and was provided in TD S3-050130 which was reviewed and approved.

TD S3-050075 Comments to TS 26.346 V150. This was introduced by Siemens and proposed the following actions for SA WG3:

1 *Discuss the security functions (and appropriate naming) of the BM-SC sub functional structure (Figure 4).*

2 *Align the SA WG3/SA WG4 terminology that is used for MBMS user service application layer joining and leaving i.e. it is proposed to distinguish MBMS User Service registration, MSK Key Request and MBMS User Service deregistration within TS 33.246. This would fit with the envisaged SA WG4 sub function called ‘(de)registration function’. This also separates the application layer terminology from the bearer level terminology (I.e. MBMS multicast bearer join/leave).*

3 *Inform SA WG4 on the need for a MSK key deregistration procedure.*

SA WG3 needs to clarify the relationship between an MBMS User Service registration and key management i.e. An MBMS User Service registration is not needed when the MBMS user service needs no protection. The MBMS User Service registration procedure is equal to the first MSK key request of the UE towards the BM-SC.

This was discussed in MBMS evening session and was taken into account in the resultant CRs. It was also decided to include this in the LS to SA WG4 in TD S3-050131.

TD S3-050090 Proposed CR to 33.246: Alignment to SA4 terminology (Rel-6). This was introduced by Ericsson. The CR was reviewed and overlap with other CRs was noted. The CR was updated in the MBMS evening session and included in TD S3-050132.

TD S3-050132 Proposed CR to 33.246: Using the term "MBMS User Service" instead of "multicast". This was produced after the MBMS evening session and ~~which~~ was reviewed and approved.

TD S3-050084 Proposed CR to 33.246: Clarification of MSK and MTK procedures (Rel-6). This was introduced by Ericsson. The proposals were accepted in principle, but some harmonisation with other CRs was required and some other issues were raised not related to this proposal, so these issues were discussed in the MBMS off-line session and the CR revised in TD S3-050133 which was reviewed and approved.

TD S3-050091 Proposed CR to 33.246: Introduction of BM-SC sub-functions (Rel-6). This was introduced by Ericsson. Some corrections and completion was needed and the figures could be improved for this CR, so it was revised in TD S3-050134 which was reviewed and approved.

TD S3-050136 LS to CT WG6: LS on MBMS work progress. This was introduced by Axalto and was reviewed and approved and the appropriate MBMS CRs attached for CT WG6 review.

Editorial corrections needed for terminology and abbreviation use in 33.246:

It was decided that editorial corrections should be collected together and a CR provided to the April 2005 meeting. This should be produced as early as possible, so that other CRs to this specifications can also make the changes in the affected clauses.

As the Rapporteur for MBMS Security had changed companies and no longer attends SA WG3, a new Rapporteur was appointed: **Vesa Lehtovirta (Ericsson) agreed to take on this task.**

6.21 Key Management of group keys for Voice Group Call Services

TD S3-050023 LS from GERAN WG2: Ciphering of access bursts on VGCS channel. This was introduced by T-Mobile. GERAN WG2 asked SA WG3 to review and endorse the attached CR. In order to solve the issue in Rel-6 timeframe, GERAN WG2 asked SA WG3 to confirm whether the CR is acceptable before the GERAN WG2 Meeting #24. In case the proposed change is not acceptable GERAN WG2 asked SA WG3 to provide an answer earlier. An analysis on this was provided by Siemens in TD S3-050070 which was reviewed:

TD S3-050070 Access burst ciphering for VGCS. This was introduced by Siemens and clarifies the particular VGCS access burst scenario under concern and analyses the security risks. The contribution shows that the effects of the attack (when using plaintext Access Bursts) are limited and the effect is not worse than a ‘brute-force’ jamming attack on the VGCS uplink channel. It is also shown that AB ciphering introduces additional complexity for realization which effects would need further investigation by GERAN WG2, if SA WG3 cannot endorse the recommendation to use plaintext Access Bursts. It was considered acceptable not to cipher the Access Bursts for Rel-6, but mechanisms to mitigate a DoS attack should be investigated for Rel-7 and contributions were requested on this if suitable mechanisms are proposed. A response LS to TD S3-050023 was provided in TD S3-050120 and reviewed. The LS was revised again in TD S3-050165 to remove "draft" and was approved.

6.22 Guide to 3G security (TR 33.900)

There were no specific contributions under this agenda item.

6.23 Selective disabling of UE capabilities

TD S3-050007 Reply LS (from SA WG1) on Clarification of SA WG3 work on Selective Disabling of UE Capabilities WI. This was introduced by Vodafone. SA WG1 agree that operator's resources can be protected transparently with the technology already available today (e.g. firewalls) and no specific new requirements at this time are needed for the stage 1. The LS was noted and it was recognised that more input may be needed by SA WG3 as SA WG2 progress their work.

6.24 Trust requirements for open platforms

There were no specific contributions under this agenda item.

6.25 Other areas

There were no specific contributions under this agenda item.

7 Review and update of work programme

TD S3-0401132 Issue list to complete MBMS Security (from meeting #36) was reviewed. The status was updated in TD S3-050183 and was agreed to be forwarded as the MBMS completion status to TSG SA.

8 Future meeting dates and venues

Deadlines for contributions to next meeting: First Deadline: Tuesday 19 April 2005, 16.00 CET. Comments deadline: Thursday 21 April 2005, 16.00 CET.

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#38	25 - 29 April 2005	Geneva, Switzerland	EF3
S3#39	28 June - 1 July 2005	Toronto, Canada (possibly with SA WG2)	NAF
S3#40	13- 16 September 2005	ETSI or EF3 / TBD	ETSI or EF3 / TBD
S3#41	15 - 18 November 2005	TBD	Qualcomm / TBD

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#17	5 - 7 April 2005	Sophia Antipolis, France	ETSI

TSGs RAN/CN/T and SA Plenary meeting schedule

Meeting	2005	Location	Primary Host
TSGs#27	March 9-11 & 14-16 2005	Tokyo, Japan	TBD
TSGs#28	June 1-3 & 6-9 2005	Quebec, Canada	TBD
TSGs#29	September 21-23 & 26-29 2005	Tallinn, Estonia	TBD
TSGs#30	Nov 30-2 Dec & 5-8 Dec 2005	Malta	TBD

9 Any other business

The Chairman announced that a report from TCG mobile phone group would be added to the agenda in future and a report on relevant activities would be given by Lily Chen (Motorola).

10 Close (Friday, 25 February, 16:00 pm at latest)

The Chairman, V. Niemi, thanked delegates for their hard work during the meeting. He thanked the Hosts, ETSI, for the excellent facilities in Sophia Antipolis. He then closed the meeting.

Annex A: List of attendees at the SA WG3#~~33~~ 37 meeting and Voting List

A.1 List of attendees

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. George Babut	Rogers Wireless Inc.	gbabut@rci.rogers.com		+1 416 935 6027	+1 416 935 7502	CA	ATIS
Mr. Nigel Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	+44 7785 31 86 31	+44 1 256 790 169	+44 1 256 790 190	GB	ETSI
Mr. Marc Blommaert	Siemens nv/sa	marc.blommaert@siemens.com		+32 14 25 34 11	+32 14 25 33 39	BE	ETSI
Mr. Charles Brookson	DTI - Department of Trade and Industry	cbrookson@iee.org	+44 20 7215 3691	+44 20 7215 3691	+44 20 7215 1814	GB	ETSI
Mr. 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 8 50452493		SE	ETSI
Dr. Hubert Ertl	GIESECKE & DEVRIENT GmbH	hubert.ertl@de.gi-de.com	+49 172 8691159	+49 89 4119 2796	+49 89 4119 2921	DE	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
Dr. Christian Gehrmann	Nippon Ericsson K.K.	christian.gehrmann@ecs.ericsson.se		+46 46 232904	+46 46 193455	JP	ARIB
Dr. Silke Holtmanns	NOKIA UK Ltd	Silke.Holtmanns@nokia.com		+358 50 4868571	+358 718036139	GB	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@siemens.com		+49 8963 641494	+49 8963 648000	DE	ETSI
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vodafone.com	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB	ETSI
Mr. Bradley Kenyon	Hewlett-Packard, Centre de Compétences France	brad.kenyon@hp.com		+1 402 384 7265	+1 402 384 7030	FR	ETSI
Mr. Geir Koien	Telenor AS	geir-myrdahl.koien@telenor.com		+47 90752914	+47 37 04 52 84	NO	ETSI
Ms. Tiina Koskinen	Nokia Telecommunications Inc.	tiina.s.koskinen@nokia.com		+358504821347	+358718075300	US	ATIS
Mr. Bernd Lamparter	NEC Technologies (UK) Ltd	bernd.lamparter@netlab.nec.de				DE	ETSI
Mr. Alex Leadbeater	BT Group Plc	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. Vesa Lehtovirta	Ericsson Incorporated	vesa.lehtovirta@ericsson.com		+358405093314	+	US	ATIS
Mr. Marcel Mampaey	ALCATEL S.A.	marcel.mampaey@alcatel.be		+32 32 40 98 03	+32 32 40 98 20	FR	ETSI
Dr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com		+358504837327	+358718036850	FI	ETSI
Mr. Petri Nyberg	TeliaSonera AB	petri.nyberg@teliasonera.com		+358 204066824	+358 2040 0 3168	SE	ETSI
Mr. Anand Palanigounder	Nortel Networks (USA)	anand@nortel.com		+1 972 684 4772	+1 972 684 3775	US	ATIS
Ms. Qiuling Pan	Zhongxing Telecom Ltd.	pan.qiuling@zte.com.cn		+	+	CN	CCSA
Miss Mireille Pauliac	GEMPLUS S.A.	mireille.pauliac@GEMPLUS.COM		+33 4 42365441	+33 4 42365792	FR	ETSI
Mr. Maurice Pope	ETSI Secretariat	maurice.pope@etsi.org	+33 (0)6 07 59 08 49	+33 4 92 94 42 59	+33 4 92 38 52 59	FR	ETSI
Mr. Bengt Sahlin	Telefon AB LM Ericsson	Bengt.Sahlin@ericsson.com		+358 40 778 4580	+358 9 299 3401	SE	ETSI
Mr. Stefan Schroeder	T-Mobile International AG	STEFAN.SCHROEDER@T-MOBILE.DE		+49 228 9363 3312	+49 228 9363 3309	DE	ETSI
Mr. Jacques Seif	Axalto S.A.	JSeif@axalto.com		+33146007228	+33146005931	FR	ETSI
Mr. James Semple	Qualcomm Europe S.A.R.L.	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. Berthold Wilhelm	BUNDESMINISTERIUM FUR WIRTSCHAFT	berthold.wilhelm@regtp.de		+49 681 9330 562	+49 681 9330 725	DE	ETSI
Mr. Dajiang Zhang	Nokia Japan Co, Ltd	dajiang.zhang@nokia.com		+86-13901168924	+86-010-84210576	JP	ARIB
Miss Jie Zhao	Zhongxing Telecom Ltd.	zhao.jie@zte.com.cn		+86 755 26772016	+86 755 26772004	CN	CCSA
Mr. Yanmin Zhu	Samsung Electronics Ind. Co., Ltd.	yanmin.zhu@samsung.com		+86-10-68427711	+86-10-68481891	KR	TTA

36 attendees

Apologies for absence were received from the following person:

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Colin Blanchard	BT Group Plc	colin.blanchard@bt.com	+44 79170 24951	+44 1473 605353	+44 1473 623910	GB	ETSI

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #35, #36, and #37, the following companies are eligible to vote at SA WG3 meeting #38:

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

44 Voting Members

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050001	Draft Agenda for SA WG3 meeting #37	SA WG3 Chairman	2	Approval		Approved
S3-050002	Draft Report of SA WG3 meeting #36	SA WG3 Secretary	4.1	Approval		Approved with minor changes
S3-050003	Report from SA#26 plenary	SA WG3 Chairman	4.2	Information		Noted
S3-050004	LS from OMA BAC: Status of OMA Mobile Broadcast Services	OMA BAC	6.20	Information		Response LS basis provided in S3-050113
S3-050005	Liaison Statement (from Q.9/17 Rapporteur Group) on General Security Policy for Secure Mobile End-to-End Data Communication	Q.9/17 Rapporteur Group	5.8	Action		E-mail discussion to provide response at next meeting
S3-050006	Proposed CR to 33.220: Key derivation function: character encoding (Rel-6)	Nokia	6.9.2	Approval	S3-050140	revised in S3-050140
S3-050007	Reply LS (from SA WG1) on Clarification of SA WG3 work on Selective Disabling of UE Capabilities WI	SA WG1	6.23	Information		Noted
S3-050008	LS from SA WG4: Reply on "LS on MBMS Security finalisation"	SA WG4	6.20	Action		LS provided after discussions and CR decisions in S3-050131
S3-050009	LS from TSG SA: Reply to TISPAN on Workshop on "IMS over Fixed Access"	TSG SA	6.1.1	Information		Noted
S3-050010	LS from SA WG3-LI Group: Reply to LS on Need for the IMSI at the PDG	SA WG3-LI Group	6.10	Information		Noted. Response from CN4 in S3-050111
S3-050011	CR to TS 33.108: Aligning comments in National-HI3-ASN1parameters with comments in National-HI2-ASN1parameters (Rel-7)	SA WG3-LI Group	4.3	Approval		Approved by e-mail before the meeting
S3-050012	Next steps for MAPsec	T-Mobile	6.2	Discussion / Decision		Comments in S3-050071
S3-050013	Proposed CR to 33.200: Correct specification of addresses used in TCAP-Handshake (Rel-6)	T-Mobile	6.2	Approval		Approved ~~in principle, to check consistency with other CRs~~
S3-050014	Proposed CR to 33.234: Wu Reference Point Description (Rel-6)	ZTE Corporation, NOKIA	6.10	Approval		Approved
S3-050015	Proposed CR to 33.234: Replacing PDGW with PDG (Rel-6)	ZTE Corporation	6.10	Approval	S3-050161	Revised in S3-050161
S3-050016	Proposed CR to 33.234: Security visibility and configurability descriptions (Rel-6)	ZTE Corporation	6.10	Approval		WITHDRAWN
S3-050017	Proposed CR to 33.234: WLAN Link Layer Security Descriptions (Rel-6)	ZTE Corporation	6.10	Approval		WITHDRAWN
S3-050018	Discussion about Using OCSP to Check Validity of PDG Certificate in 3GPP IP Access	ZTE Corporation	6.10	Discussion / Decision		CR needed. Provided in S3-050155
S3-050019	Pseudo-CR to 33.878: additional interworking cases	ZTE Corporation	6.1.2	Approval		Agreed with changes. Editor to include agreed text in draft TR
S3-050020	Security capability negotiation in GBA	ZTE Corporation	6.9.2	Discussion / Decision		Related CR in S3-050021. Not accepted for the generic GBA use
S3-050021	Proposed CR to 33.220: Security capability negotiation in GBA (Rel-6)	ZTE Corporation	6.9.2	Approval		Rejected as proposal in S3-050020 was not acceptable
S3-050022	Proposed CR to 33.234: Clarification on EAP-AKA(SIM) description in 3GPP IP access authentication and authorization (Rel-6)	ZTE Corporation	6.10	Approval	S3-050158	Revised in S3-050158
S3-050023	LS from GERAN WG2: Ciphering of access bursts on VGCS channel	GERAN WG2	6.21	Action		Response LS in S3-050120
S3-050024	LS from ETSI TISPAN: About the Workshop on "IMS over Fixed Access" (30-31 March 2005)	ETSI TISPAN	6.1.1	Information		Noted
S3-050025	Proposed CR to 33.200: Addition of TCAP-Handshake for MO-ForwardSM (Rel-6)	T-Mobile, Siemens, Vodafone	6.2	Approval		Revised in S3-050122
S3-050026	LS from SA WG2: Reply to Liaison Statement on MBMS User Service architecture	SA WG2	6.20	Information		Response to SA2 to explain conflicts in S3-050172

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050027	LS from SA WG2: RE:LS on Control of simultaneous accesses for WLAN 3GPP IP access	SA WG2	6.10	Action		Response in S3-050152
S3-050028	LS (from SA WG2) on protection of Rx and Gx interfaces	SA WG2	5.1	Action		Response in S3-050112
S3-050029	LS from SA WG2: Reply to Liaison Statement on Status of OMA Mobile Broadcast Services	SA WG2	6.20	Information		Noted
S3-050030	LS from SA WG2: Reply LS on the Workshop on "IMS over Fixed Access" (30th – 31st March 2005)	SA WG2	6.1.1	Information		Noted. A Leadbeater to forward request to LI group and request participation of LI member(s)
S3-050031	Threat of users accessing each other in link layer	ZTE Corporation	6.10	Discussion / Decision		Corresponding CR proposed in S3-050032
S3-050032	Proposed CR to 33.234: Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation (Rel-6)	ZTE Corporation	6.10	Approval	S3-050156	Revised in S3-050156
S3-050033	Discussion about MSK MIKEY Message Reception in the ME	ZTE Corporation	6.20	Discussion / Decision		Related CR in S3-050034
S3-050034	Proposed CR to 33.246: Storing SP payload after MSK message is verified (Rel-6)	ZTE Corporation	6.20	Approval	S3-050118	Revised in S3-050118
S3-050035	security architecture of early IMS	ZTE Corporation	6.1.2	Discussion / Decision		P-CR in S3-050036
S3-050036	Pseudo-CR to 33.878: Architecture of early IMS Security (Rel-6)	ZTE Corporation	6.1.2	Approval		Rejected: Should be taken to SA2 for consideration of impacts and need
S3-050037	Adoption of key separation for GSM/GPRS in the short term	Orange	6.6	Discussion / Decision		Await outcome of GERAN Sec FS
S3-050038	Proposed CR to 33.234: Clarifying the status that can't be changed in the security requirement of WLAN-UE split (Rel-6)	NOKIA, Ericsson	6.10	Approval	S3-050159	Revised in S3-050159
S3-050039	Proposed CR to 33.234: WLAN AN providing protection against IP address spoofing (Rel-6)	Nokia, ZTE Corporation	6.10	Approval	S3-050157	Revised in S3-050157
S3-050040	Draft reply LS to S3-050028 (S2-050481) "LS on protection of Rx and Gx interfaces"	Ericsson	5.1	Approval	S3-050112	Revised in S3-050112
S3-050041	Proposed CR to 33.234: Clarification on the handling of simultaneous sessions (Rel-6)	Ericsson	6.10	Approval	S3-050151	Revised in S3-050151
S3-050042	Proposed CR to 33.222: Clarification to TS 33.222 (Rel-6)	Ericsson	6.9.4	Approval	S3-050144	Revised in S3-050144
S3-050043	Review of recently published papers on GSM and UMTS security	Vodafone, Siemens	6.5	Discussion / Decision	S3-050101	WITHDRAWN
S3-050044	Proposed CR to 33.203: Addition of reference to early IMS security TR (Rel-6)	Vodafone	6.1.2	Approval	S3-050139	Revised in S3-050139
S3-050045	Draft report of SA WG3 -LI Group meeting (Barcelona)	SA WG3-LI Group	4.3	Information		Noted
S3-050046	ME based MBMS key derivation for ME based MBMS key management	Nokia, Siemens	6.20	Discussion / Decision		CR in S3-050162
S3-050047	Proposed CR to 33.246: ME based MBMS key derivation for ME based MBMS key management (Rel-6)	Nokia, Siemens	6.20	Approval	S3-050162	Revised in S3-050162
S3-050048	Security extensions for IP Multimedia Sub-system - Issues identified and contributions presented at TISPAN	BT Group	6.1	Discussion / Decision		Agreed to take issues into account for IMS Security work
S3-050049	Proposed CR to 33.246: On the derivation of the GBA keys for MBMS (Rel-6)	Oberther Card Systems	6.20	Approval		WITHDRAWN - covered by S3-050047
S3-050050	Proposed WID: NDS Authentication Framework Extension for TLS	Nokia	6.4	Approval		More justification needed and further supporting companies
S3-050051	Proposed CR to 33.200: Improving the robustness of the TCAP handshake mechanism (Rel-6)	Vodafone, T-Mobile	6.2	Approval	S3-050121	Revised in S3-050121
S3-050052	Proposed CR to 33.234: Removal of editors' notes (Rel-6)	Nokia, BT	6.10	Approval	S3-050148	Revised in S3-050148

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050053	Introducing 2G GBA	Nokia	6.9.1	Discussion / Decision		Principles of allowing 2G security in 3G system to be discussed
S3-050054	Protection of Service Announcements	Nokia	6.20	Discussion / Decision		Agreed no protection needed. CR in S3-050124
S3-050055	GAA Enhancements	Nokia	6.9.1	Discussion / Decision		More justification and support needed
S3-050056	GBA User Security Settings (GUSS) transfer optimisation	Nokia	6.9.2	Discussion / Decision		Rejected for Rel-6. Further clarification needed for Rel-7
S3-050057	Proposed CR to 33.222: Keeping PSK TLS in 3GPP Rel-6 (Rel-6)	Nokia	6.9.2	Approval	S3-050145	Revised in S3-050145
S3-050058	Proposed WID: Liberty Alliance and 3GPP Security Interworking	Nokia	6.9.2	Approval	S3-050142	More supporting companies needed. Revised in S3-050142
S3-050059	Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages	Nokia	6.10	Discussion / Decision		Attached CR revised in S3-050181
S3-050060	Proposed WID: Security extensions for IP Multimedia Sub-system	Ericsson, Nokia	6.1.1	Discussion / Decision		Comments in S3-050096. WID update after TISPAN NGN Workshop expected to next meeting
S3-050061	Proposed Pseudo-CR to 33.978: Correction of P-Asserted-Identity usage	Ericsson	6.1.2	Approval		Agreed for inclusion in the draft TR
S3-050062	Proposed Pseudo-CR to 33.978: Clarification of IMPI/IMPU relationship	Ericsson	6.1.2	Approval		Covered by S3-050100
S3-050063	HTTPS with early IMS	Ericsson	6.1.2	Discussion / Decision		Agreed with changes for inclusion in draft TR
S3-050064	Access Security Requirements	Ericsson	6.1.1	Discussion / Decision		Comments in S3-050095.
S3-050065	TLS based access security to IMS	Ericsson	6.1.1	Discussion / Decision		Comments on e-mail list. Review after TISPAN Workshop
S3-050066	Co-operation between TISPAN WG7 and 3GPP SA3 on IMS security extensions	Ericsson	6.1.1	Discussion / Decision		Reconsider after TISPAN Workshop
S3-050067	Bootstrapping timestamp	Nokia, Siemens, Vodafone	6.9.2	Discussion / Decision	S3-050143	Revised in S3-050143
S3-050068	Update for Access Security Enhancements Feasibility Study	Ericsson	6.6	Discussion / Decision		Contributions requested to provide baseline TR at next meeting
S3-050069	Proposed CR to 33.222: Clarify the GBA requirements for https supporting applications at Ua reference point (Rel-6)	Siemens	6.9.4	Approval	S3-050146	Revised to align with other contributions in S3-050146
S3-050070	Access burst ciphering for VGCS	Siemens	6.21	Discussion / Decision		Agreed not to cipher for Rel-6. Used for response LS in S3-050120
S3-050071	Comments to S3-050012: Next steps for MAPsec	Siemens	6.2	Discussion / Decision		Agreed proposals, LS to CN4 in S3-050123
S3-050072	MSK verification message handling	Siemens	6.20	Discussion / Decision		CR revised in S3-050117
S3-050073	Proposed CR to 33.246: Clarify MUK key synchronisation for MSK push procedure (Rel-6)	Siemens	6.20	Approval	S3-050105	Revised in S3-050105
S3-050074	Proposed CR to 33.246: Add missing parts of CR33 (SA3#36) (Rel-6)	Siemens	6.20	Approval		Approved
S3-050075	Comments to TS 26.346 V150	Siemens	6.20	Discussion / Decision		Taken into account in CRs. Included in LS to SA4 in S3-050131
S3-050076	Proposed CR to 33.246: Clarify Time Stamp verification in MSK Verification Message procedure (Rel-6)	Gemplus, Axalto	6.20	Approval		Withdrawn, alternative to S3-050117
S3-050077	Proposed CR to 33.246: Clarify the usage of the MUK in the BM-SC solicited pull procedure (Rel-6)	Gemplus, Axalto	6.20	Approval		Included in S3-050133. This CR withdrawn
S3-050078	Proposed CR to 33.246: Annex D1: correction of the description of the GBA run (Rel-6)	Gemplus, Axalto	6.20	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050079	Optimization of GBA	Ericsson	6.9.2	Discussion / Decision		Needs further development
S3-050080	Status of MIKEY related IETF work	Ericsson	6.20	Discussion / Decision		CR revised in S3-050114. Comments requested on attached draft
S3-050081	Details of HTTP procedures	Ericsson	6.20	Discussion / Decision		Comments provided in S3-050094. CR revised in S3-050130
S3-050082	Proposed CR to 33.246: Usage of security policy payload (Rel-6)	Ericsson	6.20	Approval	S3-050135	Revised in S3-050135
S3-050083	More reliable acknowledgement of MSK delivery	Ericsson	6.20	Discussion / Decision	S3-050099	Revised in S3-050099
S3-050084	Proposed CR to 33.246: Clarification of MSK and MTK procedures (Rel-6)	Ericsson	6.20	Approval		Revised in S3-050133
S3-050085	Proposed CR to 33.246: Requesting specific MSK (Rel-6)	Ericsson	6.20	Approval	S3-050129	Revised in S3-050129
S3-050086	Proposed CR to 33.220: Storage of B-TID in GBA_U NAF Derivation procedure (Rel-6)	Gemplus, Axalto	6.9.2	Approval		Approved
S3-050087	Proposed Pseudo CR to 33.878: Clarifications and corrections	Siemens	6.1.2	Approval	S3-050100	WITDRAWN
S3-050088	Proposed CR to 33.246: MGV-F functionality related to MTK-ID upper limit (Rel-6)	Samsung	6.20	Approval	S3-050127	Revised in S3-050127
S3-050089	Proposed CR to 33.246: Stop the usage of one MSK (Rel-6)	Samsung	6.20	Approval	S3-050128	Revised in S3-050128
S3-050090	Proposed CR to 33.246: Alignment to SA4 terminology (Rel-6)	Ericsson	6.20	Approval	S3-050132	Revised in S3-050132
S3-050091	Proposed CR to 33.246: Introduction of BM-SC subfunctions (Rel-6)	Ericsson	6.20	Approval	S3-050134	Revised in S3-050134
S3-050092	Proposed CR to 33.246: Removing IDi from MTK message (Rel-6)	Ericsson	6.20	Approval		Approved
S3-050093	LS from ETSI SAGE: Response on key separation for GSM/GPRS encryption algorithms	ETSI SAGE	5.3	Information		Noted. To be taken into account in preparation of GERAN Sec FS
S3-050094	Comments on (S3-050081/S3-050090)	Siemens	6.20	Discussion / Decision		Comments to S3-050081 and S3-050090.
S3-050095	Comments on S3-050064 Access Security Requirements	Gemplus, Axalto, OCS	6.1	Discussion / Decision		Discussed with S3-050060. New WID expected after TISPAN Workshop
S3-050096	Comments on S3-050060 WID: IMS security extensions	Gemplus, Axalto, OCS	6.1	Discussion / Decision		Discussed with S3-050060. New WID expected after TISPAN Workshop
S3-050097	Response to S3-050053: Alternative approach to 2G GBA	Qualcomm	6.9.1	Discussion / Decision		Await outcome of 2G Security to 3G services contributions at next meeting
S3-050098	Comments to S3-050069 “Clarify the GBA requirements for https applications at Ua reference point”	Gemplus, Axalto, OCS	6.9.2	Discussion / Decision		CR revised in S3-050103. LS in S3-050176
S3-050099	More reliable acknowledgement of MSK delivery	Ericsson	6.20	Discussion / Decision		LS in S3-050126. CR rejected
S3-050100	Proposed Pseudo CR to 33.878: Clarifications and corrections	Siemens	6.1.2	Approval	S3-050138	Agreed with changes noted by the editor. To be included in draft TR
S3-050101	Review of recently published papers on GSM and UMTS security	Vodafone, Siemens	6.5	Discussion / Decision		G Horn to run e-mail discussion and provide contribution to next meeting
S3-050102	LS from CN WG5 (OSA) to SA WG3 on updating TR 33.919	CN WG5 (OSA)	6.9.1	Action		CR agreed and revised in S3-050150
S3-050103	Proposed CR to 33.222: Clarify the GBA requirements for https supporting applications at Ua reference point (Rel-6)	Gemplus, Axalto, OCS	6.9.4	Approval		Covered by S3-050175
S3-050104	Proposed CR to 33.246: MBMS download protection details	Nokia	6.20	Approval	S3-050125	CR revised in S3-050125

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050105	Proposed CR to 33.246: Clarify MUK key synchronisation for MSK push procedure (Rel-6)	Siemens	6.20	Approval	S3-050115	Revised in S3-050115
S3-050106	Addressing limitations of TCAP handshake for SMS transfer	Vodafone	6.2	Discussion / Decision		CR implementing option 2 in S3-050051
S3-050107	LS from CN WG1: Misalignment amongst the 3GPP specifications, "Re-authentication and key set change during inter-system handover"	CN WG1	6.5	Information		Noted
S3-050108	LS from CN WG1: Alignment of specifications between CN1 and SA3 with respect to fallback to full authentication	CN WG1	6.10	Action		Response in S3-050153
S3-050109	LS from CN WG1 on Early IMS Security TR 33.878	CN WG1	6.1.2	Action		Changes from CN1 agreed with minor change, to be included in draft TR
S3-050110	Proposed CR to 33.246: Incompletely implemented CRs from SA3#36 (Rel-6)	Ericsson	6.20	Approval		Revised in S3-050116
S3-050111	LS from CN WG4: Reply to Reply LS on Need for the IMSI at the PDG	CN WG4	6.10	Information		Noted. Response to LI group LS in S3-050010
S3-050112	LS on protection of Rx and Gx interfaces	SA WG3	5.1	Approval		Approved
S3-050113	Draft Reply LS to 'Status of OMA Mobile Broadcast Services'	SA WG3	6.20	Approval	S3-050171	Revised in S3-050171
S3-050114	Proposed CR to 33.246: Alignment according to MIKEY related IETF work	SA WG3	6.20	Approval		Approved
S3-050115	Proposed CR to 33.246: Clarify MUK key synchronisation for MSK push procedure (Rel-6)	Siemens	6.20	Approval		Approved
S3-050116	Proposed CR to 33.246: Incompletely implemented CRs from SA3#36 (Rel-6)	Ericsson	6.20	Approval		Approved
S3-050117	MSK verification message handling	Siemens	6.20	Discussion / Decision		Approved
S3-050118	Proposed CR to 33.246: Storing SP payload after MSK message is verified (Rel-6)	ZTE Corporation	6.20	Approval	S3-050166	Revised in S3-050166
S3-050119	Reply LS (from SA WG4) on Reception Acknowledgement for MBMS	SA WG4	6.20	Action		Response in S3-050126
S3-050120	Reply LS to GERAN WG2: Ciphering of access bursts on VGCS channel	SA WG3	6.21	Approval	S3-050165	Revised in S3-050165
S3-050121	Proposed CR to 33.200: Improving the robustness of the TCAP handshake mechanism (Rel-6)	Vodafone, T-Mobile	6.2	Approval		Approved
S3-050122	Proposed CR to 33.200: Addition of TCAP-Handshake for MO-ForwardSM (Rel-6)	T-Mobile, Siemens, Vodafone	6.2	Approval		Approved. Siemens to check CR in CN4
S3-050123	LS to CN4: Next steps for MAPsec	SA WG3	6.2	Approval	S3-050167	Revised in S3-050167
S3-050124	Proposed CR to 33.246: Protection of MBMS Service Announcement sent over MBMS bearer (Rel-6)	MBMS Drafting Group	6.20	Approval		Approved
S3-050125	Proposed CR to 33.246: MBMS download protection details	Nokia	6.20	Approval	S3-050154	Profiling was checked off-line and CR revised in S3-050154
S3-050126	LS on MSK delivery acknowledgement issues	SA WG3	6.20	Approval		Approved
S3-050127	Proposed CR to 33.246: MGV-F functionality related to MTK-ID upper limit (Rel-6)	Samsung	6.20	Approval	S3-050163	Revised in S3-050163 to clarify definitions
S3-050128	Proposed CR to 33.246: Stop the usage of one MSK (Rel-6)	Samsung	6.20	Approval	S3-050164	Revised in S3-050164
S3-050129	Proposed CR to 33.246: Requesting specific MSK (Rel-6)	Ericsson	6.20	Approval		Withdrawn - covered by S3-050133
S3-050130	Proposed CR to 33.246: Clarification of HTTP procedures (Rel-6)	Ericsson	6.20	Discussion / Decision		Approved
S3-050131	LS on 'MBMS security functions, procedures and Architecture'	SA WG3	6.20	Approval		Approved
S3-050132	Proposed CR to 33.246: ~~Alignment to SA4 terminology~~ Using the term "MBMS User Service" instead of "multicast" (Rel-6)	Ericsson	6.20	Approval		Approved
S3-050133	Proposed CR to 33.246: Clarification of MSK and MTK procedures (Rel-6)	Ericsson	6.20	Approval		Approved
S3-050134	Proposed CR to 33.246: Introduction of BM-SC subfunctions (Rel-6)	Ericsson	6.20	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050135	Proposed CR to 33.246: Usage of security policy payload (Rel-6)	Ericsson	6.20	Approval		Approved
S3-050136	LS to CT WG6: LS on MBMS work progress	SA WG3	6.20	Approval		Approved. MBMS CRs to attach for review of impacts
S3-050137	Proposed CR to 33.246: Introduction of missing abbreviation, symbols and definitions (Rel-6)	Axalto	6.20	Approval		Approved
S3-050138	Updated TR 33.978: Early IMS Security	Editor	6.1.2	Approval	S3-050173	Revised in S3-050173
S3-050139	Proposed CR to 33.203: Addition of reference to early IMS security TR (Rel-6)	Vodafone	6.1.2	Approval		Approved
S3-050140	Proposed CR to 33.220: Key derivation function: character encoding (Rel-6)	Nokia	6.9.2	Approval	S3-040168	Revised in S3-050168
S3-050141	WITHDRAWN					WITHDRAWN
S3-050142	Proposed WID: Liberty Alliance and 3GPP Security Interworking	Nokia	6.9.2	Approval	S3-040169	Revised in S3-050169
S3-050143	Bootstrapping timestamp	Nokia, Siemens, Vodafone	6.9.2	Discussion / Decision		Approved
S3-050144	Proposed CR to 33.222: Clarification to TS 33.222 (Rel-6)	Ericsson	6.9.4	Approval		Approved
S3-050145	Proposed CR to 33.222: Keeping PSK TLS in 3GPP Rel-6 (Rel-6)	Nokia	6.9.2	Approval		Approved
S3-050146	Proposed CR to 33.222: Clarify the GBA requirements for https supporting applications at Ua reference point (Rel-6)	Siemens, Nokia	6.9.4	Approval	S3-050175	Revised in S3-050175
S3-050147	Comments to S3-050069: Use-case of Ks_int_NAF for HTTPS	Gemplus, Axalto	6.9.4	Information		Presented and discussed with CRs
S3-050148	Proposed CR to 33.234: Removal of editors' notes (Rel-6)	Nokia, BT	6.10	Approval	S3-050160	Revised in S3-050160
S3-050149	Proposed CR to 33.234: Fallback to full authentication (Rel-6)	NOKIA, Ericsson	6.10	Approval		Withdrawn after off-line check
S3-050150	Proposed CR to 33.919: (Rel-6)	CN WG5 (OSA)				Approved
S3-050151	Proposed CR to 33.234: Clarification on the handling of simultaneous sessions (Rel-6)	Ericsson	6.10	Approval		Approved
S3-050152	Draft Reply LS on Control of simultaneous accesses for WLAN 3GPP IP access	SA WG3	6.10	Approval	S3-050179	Revised in S3-050179
S3-050153	Reply LS on alignment of specifications between CN1 and SA3 with respect to fallback to full authentication	SA WG3	6.10	Approval		Approved
S3-050154	Proposed CR to 33.246: MBMS download protection details	Nokia	6.20	Approval		Approved
S3-050155	Proposed CR to 33.234: Using OCSP to Check Validity of PDG Certificate in 3GPP IP Access (Rel-6)	ZTE Corporation	6.10	Approval	S3-050177	Revised in S3-050177
S3-050156	Proposed CR to 33.234: Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation (Rel-6)	ZTE Corporation	6.10	Approval	S3-050178	Revised in S3-050178
S3-050157	Proposed CR to 33.234: WLAN AN providing protection against IP address spoofing (Rel-6)	Nokia, ZTE Corporation	6.10	Approval		Revised in S3-050180
S3-050158	Proposed CR to 33.234: Clarification on EAP-AKA(SIM) description in 3GPP IP access authentication and authorization (Rel-6)	ZTE Corporation	6.10	Approval		Approved
S3-050159	Proposed CR to 33.234: Clarifying the status that can't be changed in the security requirement of WLAN-UE split (Rel-6)	NOKIA, Ericsson	6.10	Approval		Approved
S3-050160	Proposed CR to 33.234: Removal of editors' notes (Rel-6)	Nokia, BT	6.10	Approval		Approved
S3-050161	Proposed CR to 33.234: Replacing PDGW with PDG (Rel-6)	ZTE Corporation	6.10	Approval		Approved
S3-050162	Proposed CR to 33.246: ME based MBMS key derivation for ME based MBMS key management (Rel-6)	Nokia, Siemens	6.20	Approval		Approved
S3-050163	Proposed CR to 33.246: MGV-F functionality related to MTK-ID upper limit (Rel-6)	Samsung	6.20	Approval		Approved
S3-050164	Proposed CR to 33.246: Stop the usage of one MSK (Rel-6)	Samsung	6.20	Approval		Withdrawn: Covered by S3-050133

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050165	Reply LS to GERAN WG2: Ciphering of access bursts on VGCS channel	Marc	6.21	Approval		Approved
S3-050166	Proposed CR to 33.246: Storing SP payload after MSK message is verified (Rel-6)	ZTE Corporation	6.20	Approval		Approved
S3-050167	DRAFT LS on next steps for MAPsec	SA WG3	6.2	Approval	S3-050174	Revised in S3-050174
S3-050168	Proposed CR to 33.220: Key derivation function: character encoding (Rel-6)	Nokia	6.9.2	Approval		Approved
S3-050169	Proposed WID: Liberty Alliance and 3GPP Security Interworking	Nokia	6.9.2	Approval		Approved
S3-050170	LS from OMA BAC DLDRM: Answer to LS on Adapting OMA DRM v2.0 DCF for MBMS download protection	OMA BAC DLDRM	6.20	Action		CR produced in S3-050154. Same as attachment to S3-050104
S3-050171	Reply LS to 'Status of OMA Mobile Broadcast Services'	SA WG3	6.20	Approval	S3-050171	Approved
S3-050172	Draft Reply to Liaison Statement on MBMS User Service architecture	SA WG3	6.20	Approval	S3-050182	Revised in S3-050182
S3-050173	Updated TR 33.978: Early IMS Security	Editor	6.1.2	Approval		Approved for presentation to SA for approval
S3-050174	LS to CN4: Next steps for MAPsec	Peter / Stefan	6.2	Approval		Approved
S3-050175	Proposed CR to 33.222: Clarify the GBA requirements for https supporting applications at Ua reference point (Rel-6)	SA WG3	6.9.4	Approval		Approved
S3-050176	LS (to TSG SA) on HTTPS connection between an UICC and a network application function	SA WG3	6.9.4	Approval		Approved
S3-050177	Proposed CR to 33.234: Using OCSP to Check Validity of PDG Certificate in 3GPP IP Access (Rel-6)	ZTE Corporation	6.10	Approval		Approved
S3-050178	Proposed CR to 33.234: Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation (Rel-6)	ZTE Corporation	6.10	Approval		Approved
S3-050179	Reply LS on Control of simultaneous accesses for WLAN 3GPP IP access	SA WG3	6.10	Approval		Approved
S3-050180	Proposed CR to 33.234: WLAN AN providing protection against IP address spoofing (Rel-6)	Nokia, ZTE Corporation	6.10	Approval		Approved
S3-050181	Proposed CR to 33.234: Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages (Rel-6)	Nokia	6.10	Discussion / Decision		Approved
S3-050182	Reply to Liaison Statement on MBMS User Service architecture	SA WG3	6.20	Approval		Approved
S3-050183	Issue list to complete MBMS Security (updated with status at SA3#37)	SA WG3	7	Information		Agreed to report status of MBMS to TSG SA

Annex C: Status of specifications under SA WG3 responsibility

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
Release 1999 GSM Specifications and Reports							
TR	01.31	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	8.0.0	R99	S3	WRIGHT, Tim	.
TR	01.33	Lawful Interception requirements for GSM	8.0.0	R99	S3	MCKIBBEN, Bernie	.
TS	01.61	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	8.0.0	R99	S3	WALKER, Michael	.
TS	02.09	Security aspects	8.0.1	R99	S3	CHRISTOFFERSSON, Per	.
TS	02.33	Lawful Interception (LI); Stage 1	8.0.1	R99	S3	MCKIBBEN, Bernie	.
TS	03.20	Security-related network functions	8.1.0	R99	S3	NGUYEN NGOC, Sebastien	
TS	03.33	Lawful Interception; Stage 2	8.1.0	R99	S3	MCKIBBEN, Bernie	TSG#10:8.1.0
Release 1999 3GPP Specifications and Reports							
TS	21.133	3G security; Security threats and requirements	3.2.0	R99	S3	CHRISTOFFERSSON, Per	.
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	3.2.1	R99	S3	NGUYEN NGOC, Sebastien	corrects change history
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	3.0.0	R99	S3	WRIGHT, Tim	Created from 02.31 R99. Technically identical to 02.31 v8.0.1.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	3.0.0	R99	S3	WRIGHT, Tim	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	Created from 03.31 R99. Technically identical to 03.31 v8.0.0
TS	23.035	Immediate Service Termination (IST); Stage 2	3.1.0	R99	S3	WRIGHT, Tim	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	Formerly 33.904. SP-000039
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	3.2.0	R99	S3	WALKER, Michael	
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	3.1.2	R99	S3	WALKER, Michael	
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	3.1.2	R99	S3	WALKER, Michael	
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	3.1.2	R99	S3	WALKER, Michael	
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	
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	4.0.0	Rel-4	S3	WRIGHT, Tim	Created from 42.031 Rel-4. Technically identical to 42.031 v4.0.0.

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	4.0.0	Rel-4	S3	WRIGHT, Tim	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	Created from 43.031 Rel-4. Technically identical to 43.031 v4.0.0
TS	23.035	Immediate Service Termination (IST); Stage 2	4.1.0	Rel-4	S3	WRIGHT, Tim	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	4.2.0	Rel-4	S3	CHIKAZAWA, Takeshi	SP-15: Not to be promoted to Rel-5. SP-24: Decision reversed, promoted to Rel-5 and -6.
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	
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	33.908	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	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	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	
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	4.0.0	Rel-4	S3	WALKER, Michael	
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	4.0.0	Rel-4	S3	WALKER, Michael	
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	
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	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	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	TSG#11:changed to Rel-4
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	TSG#11:changed to Rel-4

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
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	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	many invalid references
TS	43.033	3G security; 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	. identical to 4.1.0.
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	Created from 42.031 Rel-5. Technically identical to 43.031 v5.0.0.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	.
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	5.0.0	Rel-5	S3	WRIGHT, Tim	Created from 43.031 Rel-5. Technically identical to 43.031 v5.0.0
TS	23.035	Immediate Service Termination (IST); Stage 2	5.1.0	Rel-5	S3	WRIGHT, Tim	.
TS	33.102	3G security; Security architecture	5.5.0	Rel-5	S3	BLOMMAERT, Marc	.
TS	33.105	Cryptographic algorithm requirements	5.0.0	Rel-5	S3	CHIKAZAWA, Takeshi	.
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)	5.9.1	Rel-5	S3	WILHELM, Berthold	.
TS	33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	5.1.0	Rel-5	S3	ESCOTT, Adrian	.
TS	33.203	3G security; Access security for IP-based services	5.9.0	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	
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	.
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	5.0.0	Rel-5	S3	WALKER, Michael	.
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	.
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	.
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	.
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	.

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
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	.
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	.
TR	33.900	Guide to 3G security **NOT UNDER CHANGE CONTROL!**	0.4.1	Rel-5	S3	BROOKSON, Charles	. v number seems to have restarted. Not uploaded for fear of confusion.
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	.
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	. many invalid references
TS	43.033	3G security; Lawful Interception; Stage 2	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
Release 6 3GPP Specifications and Reports							
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	6.0.0	Rel-6	S3	NGUYEN NGOC, Sebastien	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	6.0.0	Rel-6	S3	WRIGHT, Tim	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	6.0.0	Rel-6	S3	WRIGHT, Tim	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	6.0.0	Rel-6	S3	WRIGHT, Tim	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	23.035	Immediate Service Termination (IST); Stage 2	6.0.0	Rel-6	S3	WRIGHT, Tim	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	33.102	3G security; Security architecture	6.3.0	Rel-6	S3	BLOMMAERT, Marc	.
TS	33.105	Cryptographic algorithm requirements	6.0.0	Rel-6	S3	CHIKAZAWA, Takeshi	.
TS	33.106	Lawful interception requirements	6.1.0	Rel-6	S3	WILHELM, Berthold	.
TS	33.107	3G security; Lawful interception architecture and functions	6.4.0	Rel-6	S3	WILHELM, Berthold	.
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	6.8.2	Rel-6	S3	WILHELM, Berthold	.
TS	33.141	Presence service; Security	6.1.0	Rel-6	S3	BOMAN, Krister	.
TS	33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	6.0.0	Rel-6	S3	ESCOTT, Adrian	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	33.203	3G security; Access security for IP-based services	6.5.0	Rel-6	S3	BOMAN, Krister	.
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	6.5.0	Rel-6	S3	KOIEN, Geir	.
TS	33.220	Generic Authentication Architecture (GAA); Generic bootstrapping architecture	6.3.0	Rel-6	S3	HAUKKA, Tao	.
TS	33.221	Generic Authentication Architecture (GAA); Support for subscriber certificates	6.2.0	Rel-6	S3	HAUKKA, Tao	.
TS	33.222	Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)	6.2.0	Rel-6	S3	SAHLIN, Bengt	.

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	33.234	3G security; Wireless Local Area Network (WLAN) interworking security	6.3.0	Rel-6	S3	LOPEZ SORIA, Luis	.
TS	33.246	3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)	6.1.0	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)	6.2.0	Rel-6	S3	KOSKINEN, Tiina	.
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	SP-17: expect v2.0.0 at SP-18.
TR	33.817	Feasibility study on (Universal) Subscriber Interface Module (U)SIM security reuse by peripheral devices on local interfaces	6.1.0	Rel-6	S3	YAQUB, Raziq	.
TR	33.919	Generic Authentication Architecture (GAA); System description	6.1.0	Rel-6	S3	VAN MOFFAERT, Annelies	.
TR	33.941	Presence service; Security	0.6.0	Rel-6	S3	BOMAN, Krister	.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	6.0.0	Rel-6	S3	WALKER, Michael	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	6.0.0	Rel-6	S3	WALKER, Michael	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	6.0.0	Rel-6	S3	WALKER, Michael	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	6.0.0	Rel-6	S3	WALKER, Michael	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
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	6.0.0	Rel-6	S3	WALKER, Michael	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
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	6.0.0	Rel-6	S3	WALKER, Michael	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
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	6.0.0	Rel-6	S3	WALKER, Michael	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
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	6.0.0	Rel-6	S3	WALKER, Michael	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
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	6.0.0	Rel-6	S3	WALKER, Michael	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	6.0.0	Rel-6	S3	WRIGHT, Tim	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TR	41.033	Lawful Interception requirements for GSM	6.0.0	Rel-6	S3	MCKIBBEN, Bernie	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	42.033	Lawful Interception; Stage 1	6.0.0	Rel-6	S3	MCKIBBEN, Bernie	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
TS	43.020	Security-related network functions	6.1.0	Rel-6	S3	GILBERT, Henri	.

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	43.033	3G security; Lawful Interception; Stage 2	6.0.0	Rel-6	S3	MCKIBBEN, Bernie	Rel-6 record created on freezing the Release, December 2004. Upgrade on Rel-6 freeze
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	.
TS	55.216	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 1: A5/3 and GEA3 specification	6.2.0	Rel-6	S3	N, A	.
TS	55.217	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data	6.1.0	Rel-6	S3	N, A	.
TS	55.218	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 3: Design and conformance test data	6.1.0	Rel-6	S3	N, A	.
TR	55.919	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report	6.1.0	Rel-6	S3	N, A	.
Other Specifications and Reports to be allocated to (or identified for) Release 7							
TS	55.226	Specification of the A5/4 encryption algorithms for GSM and ECSD, and the GEA4 encryption algorithm for GPRS; Document 1: A5/4 and GEA4 specification	none	Rel-7	S3	CHRISTOFFERSSON, Per	Work item UID = 1571 (SEC1) .

Annex D: List of CRs to specifications under SA WG3 responsibility agreed at meeting #37

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	Status	WI
33.108	069	-	Rel-7	Aligning comments in National-HI3-ASN1parameters with comments in National-HI2-ASN1parameters	D	6.8.2	S3-37	S3-050011	agreed	SEC1-LI
33.200	024	-	Rel-6	Correct specification of addresses used in TCAP-Handshake	F	6.0.0	S3-37	S3-050013	agreed~~Approved in principle. Overlap with CR026R1~~	SEC1-MAP
33.200	025	-	Rel-6	Addition of TCAP-Handshake for MO-ForwardSM	C	6.0.0	S3-37	S3-050025	revised	SEC1-MAP
33.200	025	1	Rel-6	Addition of TCAP-Handshake for MO-ForwardSM	C	6.0.0	S3-37	S3-050122	agreed	SEC1-MAP
33.200	026	-	Rel-6	Improving the robustness of the TCAP handshake mechanism	F	6.0.0	S3-37	S3-050051	revised	SEC1-MAP
33.200	026	1	Rel-6	Improving the robustness of the TCAP handshake mechanism	F	6.0.0	S3-37	S3-050121	agreed	SEC1-MAP
33.203	077	2	Rel-6	Addition of reference to early IMS security TR	F	6.5.0	S3-37	S3-050044	revised	IMS-EARLY
33.203	077	3	Rel-6	Addition of reference to early IMS security TR	F	6.5.0	S3-37	S3-050139	agreed	IMS-EARLY
33.203	078	-	Rel-7	Access Security Requirements	B	6.5.0	S3-37	att_S3-050064	Postponed. Review after TISPAN NGN Workshop	IMS-ASEC
33.203	079	-	Rel-7	TLS based access security in IMS	-	6.5.0	S3-37	att_S3-050065	Postponed. Review after TISPAN NGN Workshop	IMS-ASEC
33.220	045	-	Rel-6	Key derivation function: character encoding	C	6.3.0	S3-37	S3-050006	Revised	SEC1-SC
33.220	045	1	Rel-6	Key derivation function: character encoding	C	6.3.0	S3-37	S3-050140	Revised	SEC1-SC
33.220	045	2	Rel-6	Key derivation function: character encoding	C	6.3.0	S3-37	S3-050168	agreed	SEC1-SC
33.220	046	-	Rel-6	GBA User Security Settings (GUSS) transfer optimisation	C	6.3.0	S3-37	S3-050056	Rejected	SEC1-SC
33.220	047	-	Rel-6	Bootstrapping timestamp	C	6.3.0	S3-37	S3-050067	Revised	SEC1-SC
33.220	047	1	Rel-6	Bootstrapping timestamp	C	6.3.0	S3-37	S3-050143	agreed	SEC1-SC
33.220	048	-	Rel-6	Storage of B-TID in GBA_U NAF Derivation procedure	F	6.3.0	S3-37	S3-050086	agreed	SEC1-SC
33.220	049	-	Rel-6	Security capability negotiation in GBA	F	6.3.0	S3-37	S3-050021	Rejected	GBA-SSC
33.222	015	2	Rel-6	Keeping PSK TLS in 3GPP Rel-6	F	6.2.0	S3-37	S3-050057	revised	SEC1-SC
33.222	015	3	Rel-6	Keeping PSK TLS in 3GPP Rel-6	F	6.2.0	SA WG3	S3-050145	agreed	SEC1-SC
33.222	016	-	Rel-6	Clarification to TS 33.222	F	6.2.0	S3-37	S3-050042	revised	SEC1-SC
33.222	016	1	Rel-6	Clarification to TS 33.222	F	6.2.0	S3-37	S3-050144	agreed	SEC1-SC
33.222	017	-	Rel-6	Clarify the GBA requirements for https supporting applications at Ua reference point	F	6.2.0	S3-37	S3-050069	revised	GBA-SSC
33.222	017	1	Rel-6	Clarify the GBA requirements for https supporting applications at Ua reference point	F	6.2.0	S3-37	S3-050146	revised	GBA-SSC
33.222	017	2	Rel-6	Clarify the GBA requirements for https supporting applications at Ua reference point	F	6.2.0	S3-37	S3-050175	agreed	GBA-SSC
33.222	018	-	Rel-6	Clarify the GBA requirements for https supporting applications at Ua reference point	F	6.2.0	S3-37	Att_S3-050098	revised	GBA-SSC
33.222	018	1	Rel-6	Clarify the GBA requirements for https supporting applications at Ua reference point	F	6.2.0	S3-37	S3-050103	withdrawn	GBA-SSC
33.234	051	-	Rel-6	Wu Reference Point Description	F	6.3.0	S3-37	S3-050014	agreed	WLAN
33.234	052	-	Rel-6	Replacing PDGW with PDG	F	6.3.0	S3-37	S3-050015	Revised	WLAN
33.234	052	1	Rel-6	Replacing PDGW with PDG	F	6.3.0	S3-37	S3-050161	agreed	WLAN
33.234	053	-	Rel-6	Security visibility and configurability descriptions	B	6.3.0	S3-37	S3-050016	Withdrawn	WLAN
33.234	054	-	Rel-6	WLAN Link Layer Security Descriptions	B	6.3.0	S3-37	S3-050017	Withdrawn	WLAN

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	Status	WI
33.234	055	-	Rel-6	Clarification on EAP-AKA(SIM) description in 3GPP IP access authentication and authorization	D	6.3.0	S3-37	S3-050022	Revised	WLAN
33.234	055	1	Rel-6	Clarification on EAP-AKA(SIM) description in 3GPP IP access authentication and authorization	D	6.3.0	S3-37	S3-050158	agreed	WLAN
33.234	056	-	Rel-6	Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation	B	6.3.0	S3-37	S3-050032	Revised	WLAN
33.234	056	1	Rel-6	Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation	B	6.3.0	S3-37	S3-050156	Revised	WLAN
33.234	056	2	Rel-6	Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation	F	6.3.0	S3-37	S3-050178	agreed	WLAN
33.234	057	-	Rel-6	Clarifying the status that can't be changed in the security requirement of WLAN-UE split	F	6.3.0	S3-37	S3-050038	Revised	WLAN
33.234	057	1	Rel-6	Clarifying the status that can't be changed in the security requirement of WLAN-UE split	F	6.3.0	S3-37	S3-050159	agreed	WLAN
33.234	058	-	Rel-6	WLAN AN providing protection against IP address spoofing	F	6.3.0	S3-37	S3-050039	Revised	WLAN
33.234	058	1	Rel-6	WLAN AN providing protection against IP address spoofing	F	6.3.0	S3-37	S3-050157	Revised	WLAN
33.234	058	2	Rel-6	WLAN AN providing protection against IP address spoofing	F	6.3.0	S3-37	S3-050180	agreed	WLAN
33.234	059	-	Rel-6	Clarification on the handling of simultaneous sessions	F	6.3.0	S3-37	S3-050041	Revised	WLAN
33.234	059	1	Rel-6	Clarification on the handling of simultaneous sessions	F	6.3.0	S3-37	S3-050151	agreed	WLAN
33.234	060	-	Rel-6	Removal of editors' notes	D	6.3.0	S3-37	S3-050052	Revised	WLAN
33.234	060	1	Rel-6	Removal of editors' notes	D	6.3.0	S3-37	S3-050148	Revised	WLAN
33.234	060	2	Rel-6	Removal of editors' notes	D	6.3.0	S3-37	S3-050160	agreed	WLAN
33.234	061	-	Rel-6	Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages	F	6.3.0	S3-37	att_S3-050059	Revised	WLAN
33.234	061	1	Rel-6	Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages	F	6.3.0	S3-37	S3-050181	agreed	WLAN
33.234	062	-	Rel-6	Fallback to full authentication	F	6.3.1	S3-37	S3-050149	Withdrawn	WLAN
33.234	063	-	Rel-6	Using OCSP to Check Validity of PDG Certificate in 3GPP IP Access	F	6.3.1	S3-37	S3-050155	Revised	WLAN
33.234	063	1	Rel-6	Using OCSP to Check Validity of PDG Certificate in 3GPP IP Access	F	6.3.1	S3-37	S3-050177	agreed	WLAN
33.246	034	-	Rel-6	Storing SP payload after MSK message is verified	C	6.1.0	S3-37	S3-050034	Revised	MBMS
33.246	034	1	Rel-6	Storing SP payload after MSK message is verified	C	6.1.0	S3-37	S3-050118	Revised	MBMS
33.246	034	2	Rel-6	Storing SP payload after MSK message is verified	C	6.1.0	S3-37	S3-050166	agreed	MBMS
33.246	035	-	Rel-6	ME based MBMS key derivation for ME based MBMS key management	C	6.1.0	S3-37	S3-050047	Revised	MBMS
33.246	035	1	Rel-6	ME based MBMS key derivation for ME based MBMS key management	C	6.1.0	S3-37	S3-050162	agreed	MBMS
33.246	036	-	Rel-6	On the derivation of the GBA keys for MBMS	B	6.1.0	S3-37	S3-050049	withdrawn	MBMS
33.246	037	-	Rel-6	Correct the MSK verification message handling	F	6.1.0	S3-37	Att_S3-050072	revised	MBMS
33.246	037	1	Rel-6	Correct the MSK verification message handling	F	6.1.0	S3-37	S3-050117	agreed	MBMS
33.246	038	-	Rel-6	Clarify MUK key synchronisation for MSK push procedure	C	6.1.0	S3-37	S3-050073	revised	MBMS
33.246	038	1	Rel-6	Clarify MUK key synchronisation for MSK push procedure	C	6.1.0	S3-37	S3-050105	revised	MBMS
33.246	038	2	Rel-6	Clarify MUK key synchronisation for MSK push procedure	C	6.1.0	S3-37	S3-050115	agreed	MBMS
33.246	039	-	Rel-6	Add missing parts of CR33 (SA3#36)	F	6.1.0	S3-37	S3-050074	agreed	MBMS
33.246	040	-	Rel-6	Clarify Time Stamp verification in MSK Verification Message procedure	F	6.1.0	S3-37	S3-050076	withdrawn	MBMS
33.246	041	-	Rel-6	Clarify the usage of the MUK in the BM-SC solicited pull procedure	F	6.1.0	S3-37	S3-050077	withdrawn	MBMS
33.246	042	-	Rel-6	Annex D1: correction of the description of the GBA run	F	6.1.0	S3-37	S3-050078	agreed	MBMS
33.246	043	-	Rel-6	Alignment according to MIKEY related IETF work	C	6.1.0	S3-37	Att1_S3-050080	Revised	MBMS
33.246	043	1	Rel-6	Alignment according to MIKEY related IETF work	C	6.1.0	S3-37	S3-050114	agreed	MBMS
33.246	044	-	Rel-6	Clarification of HTTP procedures	C	6.1.0	S3-37	Att_S3-050081	Revised	MBMS

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	Status	WI
33.246	044	1	Rel-6	Clarification of HTTP procedures	C	6.1.0	S3-37	S3-050130	agreed	MBMS
33.246	045	-	Rel-6	Usage of security policy payload	C	6.1.0	S3-37	S3-050082	Revised	MBMS
33.246	045	1	Rel-6	Usage of security policy payload	C	6.1.0	S3-37	S3-050135	agreed	MBMS
33.246	046	-	Rel-6	More reliable MSK delivery based charging	B	6.1.0	S3-37	Att_S3-050083	Revised	MBMS
33.246	046	1	Rel-6	More reliable MSK delivery based charging	B	6.1.0	S3-37	Att_S3-050099	Rejected	MBMS
33.246	047	-	Rel-6	Clarification of MSK and MTK procedures	C	6.1.0	S3-37	S3-050084	Revised	MBMS
33.246	047	1	Rel-6	Clarification of MSK and MTK procedures	C	6.1.0	S3-37	S3-050133	agreed	MBMS
33.246	048	-	Rel-6	Requesting specific MSK	B	6.1.0	S3-37	S3-050085	Revised	MBMS
33.246	048	1	Rel-6	Requesting specific MSK	B	6.1.0	S3-37	S3-050129	withdrawn	MBMS
33.246	049	-	Rel-6	MGV-F functionality related to MTK-ID upper limit	C	6.1.0	S3-37	S3-050088	Revised	MBMS
33.246	049	1	Rel-6	MGV-F functionality related to MTK-ID upper limit	C	6.1.0	S3-37	S3-050127	Revised	MBMS
33.246	049	2	Rel-6	MGV-F functionality related to MTK-ID upper limit	C	6.1.0	S3-37	S3-050163	agreed	MBMS
33.246	050	-	Rel-6	Stop the usage of one MSK	C	6.1.0	S3-37	S3-050089	Revised	MBMS
33.246	050	1	Rel-6	Stop the usage of one MSK	C	6.1.0	S3-37	S3-050128	Revised	MBMS
33.246	050	2	Rel-6	Stop the usage of one MSK	C	6.1.0	S3-37	S3-050164	withdrawn	MBMS
33.246	051	-	Rel-6	Alignment to SA4 terminology	D	6.1.0	S3-37	S3-050090	Revised	MBMS
33.246	051	~~-~~1	Rel-6	~~Alignment to SA4 terminology~~ Using the term "MBMS User Service" instead of "multicast"	D	6.1.0	S3-37	S3-050132	agreed	MBMS
33.246	052	-	Rel-6	Introduction of BM-SC subfunctions	D	6.1.0	S3-37	S3-050091	Revised	MBMS
33.246	052	1	Rel-6	Introduction of BM-SC subfunctions	D	6.1.0	S3-37	S3-050134	agreed	MBMS
33.246	053	-	Rel-6	Removing IDi from MTK message	C	6.1.0	S3-37	S3-050092	agreed	MBMS
33.246	054	-	Rel-6	MBMS download protection details	C	6.1.0	S3-37	S3-050104	Revised	MBMS
33.246	054	1	Rel-6	MBMS download protection details	C	6.1.0	S3-37	S3-050125	Revised	MBMS
33.246	054	2	Rel-6	MBMS download protection details	C	6.1.0	S3-37	S3-050154	agreed	MBMS
33.246	055	-	Rel-6	Removal of editors' notes	F	6.1.0	S3-37	S3-050110	Revised	MBMS
33.246	055	1	Rel-6	Removal of editors' notes	F	6.1.0	S3-37	S3-050116	agreed	MBMS
33.246	056	-	Rel-6	Protection of MBMS Service Announcement sent over MBMS bearer	C	6.1.0	S3-37	S3-050124	agreed	MBMS
33.246	057	-	Rel-6	Introduction of missing abbreviation, Symbols and definitions	D	6.1.0	S3-37	S3-050137	agreed	MBMS
33.919	003	-	Rel-6	Correct the “Application guidelines to use GAA”	F	6.1.0	S3_37	S3-050150	agreed	GAA

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	From	Source TD	Comment/Status
S3-050004	LS from OMA BAC: Status of OMA Mobile Broadcast Services	OMA BAC	OMA-BAC-2004-0069	Response LS basis provided in S3-050113
S3-050005	Liaison Statement (from Q.9/17 Rapporteur Group) on General Security Policy for Secure Mobile End-to-End Data Communication	Q.9/17 Rapporteur Group	COM 17 - LS 05 - E	E-mail discussion to provide response at next meeting
S3-050007	Reply LS (from SA WG1) on Clarification of SA WG3 work on Selective Disabling of UE Capabilities WI	SA WG1	S1-050235	Noted
S3-050008	LS from SA WG4: Reply on "LS on MBMS Security finalisation"	SA WG4	S4-040760	LS provided after discussions and CR decisions in S3-050131
S3-050009	LS from TSG SA: Reply to TISPAN on Workshop on "IMS over Fixed Access"	TSG SA	SP-040929	Noted
S3-050010	LS from SA WG3-LI Group: Reply to LS on Need for the IMSI at the PDG	SA WG3-LI Group	S3LI05_024r2	Noted. Response from CN4 in S3-050111
S3-050023	LS from GERAN WG2: Ciphering of access bursts on VGCS channel	GERAN WG2	GP-050599	Response LS in S3-050120
S3-050024	LS from ETSI TISPAN: About the Workshop on "IMS over Fixed Access" (30-31 March 2005)	ETSI TISPAN	05TD266r2	Noted
S3-050026	LS from SA WG2: Reply to Liaison Statement on MBMS User Service architecture	SA WG2	S2-050171	Response to SA2 to explain conflicts in S3-050172
S3-050027	LS from SA WG2: RE:LS on Control of simultaneous accesses for WLAN 3GPP IP access	SA WG2	S2-050430	Response in S3-050152
S3-050028	LS (from SA WG2) on protection of Rx and Gx interfaces	SA WG2	S2-050481	Response in S3-050112
S3-050029	LS from SA WG2: Reply to Liaison Statement on Status of OMA Mobile Broadcast Services	SA WG2	S2-050174	Noted
S3-050030	LS from SA WG2: Reply LS on the Workshop on "IMS over Fixed Access" (30th – 31st March 2005)	SA WG2	S2-050504	Noted. A Leadbeater to forward request to LI group and request participation of LI member(s)
S3-050093	LS from ETSI SAGE: Response on key separation for GSM/GPRS encryption algorithms	ETSI SAGE	SAGE (05) 16	Noted. To be taken into account in preparation of GERAN Sec FS
S3-050102	LS from CN WG5 (OSA) to SA WG3 on updating TR 33.919	CN WG5 (OSA)	N5-050102	CR agreed and revised in S3-050150
S3-050107	LS from CN WG1: Misalignment amongst the 3GPP specifications, “Re-authentication and key set change during inter-system handover”	CN WG1	N1-050270	Noted
S3-050108	LS from CN WG1: Alignment of specifications between CN1 and SA3 with respect to fallback to full authentication	CN WG1	N1-050376	Response in S3-050153
S3-050109	LS from CN WG1 on Early IMS Security TR 33.878	CN WG1	N1-050408	Changes from CN1 agreed with minor change, to be included in draft TR
S3-050111	LS from CN WG4: Reply to Reply LS on Need for the IMSI at the PDG	CN WG4	N4-050344	Noted. Response to LI group LS in S3-050010
S3-050119	Reply LS (from SA WG4) on Reception Acknowledgement for MBMS	SA WG4	S4-050128	Response in S3-050126
S3-050170	LS from OMA BAC DLDRM: Answer to LS on Adapting OMA DRM v2.0 DCF for MBMS download protection	OMA BAC DLDRM	OMA-DLDRM-2005-0044	CR produced in S3-050154. Same as attachment to S3-050104

E.2 Liaisons from the meeting

TD number	Title	TO	CC
S3-050112	LS on protection of Rx and Gx interfaces	**CN WG3, SA WG2**	-
S3-050126	LS on MSK delivery acknowledgement issues	**SA WG4, SA WG5, SA WG2, SA WG1**	-
S3-050131	LS on ‘MBMS security functions, procedures and Architecture’	**SA WG4**	-
S3-050136	LS to CT WG6: LS on MBMS work progress	**CT WG6**	-
S3-050153	Reply LS on alignment of specifications between CN1 and SA3 with respect to fallback to full authentication	**CN WG1**	-
S3-050165	Reply LS to GERAN WG2: Ciphering of access bursts on VGCS channel	**GERAN WG2**	-

TD number	Title	TO	CC
S3-050171	Reply LS to 'Status of OMA Mobile Broadcast Services'	**OMA BAC**	**OMA SEC, TSG SA, SA WG2, SA WG4**
S3-050174	LS to CN4: Next steps for MAPsec	**CN WG4**	**-**
S3-050176	LS (to TSG SA) on HTTPS connection between an UICC and a network application function	**TSG SA**	**-**
S3-050179	Reply LS on Control of simultaneous accesses for WLAN 3GPP IP access	**SA WG2**	**CN WG1, CN WG4**
S3-050182	Reply to Liaison Statement on MBMS User Service architecture	**SA WG2**	**-**

Annex F: Actions from the meeting

AP 37/01: Chairman to ask the Specifications Manager for the best way to handle the UE2 / UIA2 work in the specifications set (numbering etc.)

AP 37/02: Qiuling Pan, (ZTE to lead an e-mail discussion on the LS in TD S3-050005 and provide a draft answer to the LS to the next SA WG3 meeting.

AP 37/03: B. Sahlin to provide an updated WID, based on TD S3-050060 for next SA WG3 meeting, taking into account the outcome of the TISPAN NGN Workshop.

AP 37/04: M. Pope to discuss the best way to handle the removal of MAPsec Rel-4 NE-based solution from the 3GPP specs and report back to SA WG3.

AP 37/05: G. Horn to run an e-mail discussion based on TD S3-050101 (Review of recently published papers on GSM and UMTS security) and provide a contribution to the next SA WG3 meeting.

AP 37/06: S. Holtmanns to discuss GAA Enhancements WID and develop the scope and need for the work, and present the WID again with enough supporting companies (re: TD S3-050055).

AP 37/07: Nokia to check the termination part of TD S3-050181 and the impact and need for CRs for other specifications