Source:	**SA WG3**
Title:	**Reports of SA WG3 meetings held since TSG SA meeting #25**
Document for:	**Information**
Agenda Item:	**7.3.1**

SA WG3 has held two meetings since TSG SA meeting #25:

TSG-SA3 Meeting #35	5-8 October 2004	Malta
TSG-SA3 Meeting #36	23-26 November 2004	Shenzhen, China

Attached for information is the SA WG3 approved report of meeting #35 and the latest draft report of meeting #36.

3GPP TSG SA WG3 (Security) meeting #35 FINAL REPORT

5-8 October 2004

Malta, EU

Source: SA WG3 Secretary (Maurice Pope, MCC)

Title: Report of SA3#35 version 1.0.0

Status: Approved at SA WG3 # 36

St. Paul's Bay, Malta

Contents

1 Opening of the meeting

The SA WG3 Chairman welcomed delegates to the meeting in Malta, on behalf of the hosts, the European Friends of 3GPP.

2 Agreement of the agenda and meeting objectives

TD S3-040690 Draft Agenda for SA WG3 meeting #35. The SA WG3 Chairman introduced the draft agenda and explained the primary meeting objectives:

- The major objective of the meeting is to develop those three TSs for which functional changes may still be needed: 33.220 (GBA), 33.234 (I-WLAN), 33.246 (MBMS).
- Another important objective is to try to close remaining open issues and get rid of editorís notes in the other release 6 TSs and TRs.

The agenda and objectives were 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 available input documents were assigned to their appropriate agenda items.

4 Meeting reports

4.1 Approval of the report of SA3#34, Acapulco, Mexico, 6-9 July, 2004

TD S3-040691 Draft Report of SA WG3 meeting #34. The draft report was reviewed and approved. The approved version 1.0.0 (with revision marks accepted) will be placed on the 3GPP FTP server after the meeting. The Actions from the previous meeting were then reviewed:

AP 34/01: SA WG3 Chairman and Secretary to look into the best way to reflect the changes for GSM Algorithm support in the specifications.
It was considered the best place would be in TS 33.102 and this should be discussed by SA WG3 on how to best include the decision on removal of A5/2 support from terminals. Completed.

AP 34/02: Nokia to prepare CRs to include default domain name information in the specifications (re: TD S3-040373).
Contribution TD S3-040695 covers this action. Completed.

AP 34/03: Chairman to bring outcome of WLAN/UICC discussions to attention of TSG SA (see TD S3-040590).
This was presented by the Chairman to TSG SA #25. Completed.

AP 34/04: Raziq Yaqub to arrange conference calls based on TD S3-040594 and the comments received in TD S3-040578 and at SA WG3 meeting #34. First Conference call 26 July 2004, next call the week 23-27 August 2004; deadline for last conference call week 13-17 September 2004. Comments to be provided at least 3 working days before the conference calls sent to SA WG3 e-mail list.
A number of conference calls were held and CRs provided to this meeting. Completed.

AP 34/05: M. Pope to check if ETSI Premises are available for the February meeting in case it is decided not to go to Australia. (4.5 day meeting starting Monday 13.00)
ETSI premises was available and booked for the February 2005 meeting. Completed.

4.2 Report from SA#25, Palm Springs, USA, 13-16 September, 2004

TD S3-040694 Report from SA#25 plenary. This report from the SA WG3 Chairman on activities concerning SA WG3 at TSG SA #25 had been distributed by e-mail after the TSG SA meeting. The report was reviewed and noted.

TD S3-040715 LS(from T WG3) on USIM support by 2G terminals of Rel-99 and Rel-4.

4.3 Report from SA3-LI#3/2004, Povoa de Varzim, Portugal, 19-20 July, 2004

TD S3-040693 SA WG3 LI Group CRs (approved by e-mail 02/09/2004). These CRs were approved by e-mail and had also been approved by TSG SA #25. The CRs were therefore noted.

TD S3-040718 Report of SA WG3-LI Group meeting - 19-20 July 2004, Povoa de Varzim, Portugal. This was introduced by B. Wilhelm and was noted

4.4 Report from SA3-SA4 joint meeting on MBMS security, Sophia Antipolis, France, 23-24 August, 2004

TD S3-040692 Report of MBMS joint Ad-hoc meeting. This was introduced by the joint ad-hoc meeting Chairman, A. Escott and was reviewed and approved by SA WG3.

5 Reports and Liaisons from other groups

5.1 3GPP working groups

There were no specific contributions under this agenda item. Liaisons from 3GPP groups were allocated under their relevant technical agenda items.

5.2 IETF

TD S3-040698 LS from IETF LEMONADE: LEMONADE for MMS over 3GPP Interworking WLANs. This was introduced by Nortel Networks. The IETF LEMONADE work group (WG) is tasked to provide a set of enhancements and profiles of Internet e-mail submission, transport, and retrieval protocols to facilitate operation on platforms with constrained resources, or communications links with high latency or limited bandwidth. A primary goal of this work is to ensure that those profiles and enhancements continue to interoperate with the existing Internet email protocols in use on the Internet, so that these environments and more traditional Internet users have access to a seamless service. LEMONADE protocols are designed to support whatever level of authentication, authorization and privacy are desired. The protocols provide encryption, authentication, and verification services, applied as needed. Much of these facilities are transparent to the application. A reply on this subject from OMA was provided in TD S3-040697 and dealt with under agenda item 5.6. The LS was copied to SA WG3 for information and was noted.

5.3 ETSI SAGE

P Christoffersson reported from GSMA SG. The A5/2 removal issue is now only awaiting GSMA Board approval. GSMA EMC has approved funding for development of new UMTS algorithms.

IMEI protection and handset theft protection has become a social issue with many EU member countries and the European Commission is threatening with regulations. Therefore GSMA has launched a programme to combat handset theft. This includes a reporting scheme for weak IMEI protection and the launch of a new CEIR. All operators are actively encouraged to have their own EIR and join the CEIR. Principles for better protection of the IMEI from modification have been agreed between GSMA and major manufacturers.
The EU committee, TCAM, will monitor progress on IMEI protection and the use of the CEIR and regulations may be introduced if not enough action is taken by the industry.

SMS Spoofing is also an issue and this is also being investigated by the GSMA and action may be taken against any operators participating in this.

More handset viruses have been reported since last meeting. Although those viruses did not cause any damage, they do represent a growing threat to mobile operators.

5.4 GSMA

P Chrisofferssen reported the A5/2 removal issue was awaiting GSMA Board approval. IMEI protection and handset theft protection has been mandated by many member countries and the European Commision has mandated to launch a programme to combat handset theft. The Identity register for stolen IMEIs and the better protection of the IMEI from modification is to be investigated. TCAM - monitor and report progress on IMEI protection and the use of the Identity register and regulation may be needed if not enough action is taken by the industry. SMS Spoofing is also an issue and this is also being investigated by the GSMA and action may be taken against any operators participating in this.

5.5 3GPP2

It was reported that 3GPP2 have approved a Stage 1 WI for *Network Firewall Configuration Control* and work has started on this.

5.6 OMA

TD S3-040697 LS from OMA MMSG: Re: MMS over 3GPP Interworking WLANs. This was introduced by Qualcomm and was a response to SA WG2 LS which asked:

> *TS 23.234 includes the capability for the WLAN User Equipment (UE) to establish IP connectivity with the 3GPP network in order to access certain 3G services. Hence, the WLAN UE can access at least those services that only require IP connectivity. SA WG2 considers the Multimedia Messaging Service (MMS) as such a service, but would like to confirm that this is the case.*

OMA MMSG confirmed that MMS is such a service, provided that an MM1 is used which requires only IP connectivity.

A response from T WG2 on this subject was provided in TD S3-040711 which was dealt with under agenda item 6.10. This LS was copied to SA WG3 for information and was noted.

5.7 TR-45 AHAG

There were no specific contributions under this agenda item.

5.8 Other groups

There were no specific contributions under this agenda item.

6 Work areas

6.1 IP multimedia subsystem (IMS)

6.1.1 TS 33.203 issues

TD S3-040700 Reply LS (from SA WG2) on provision of configuration data to a UE. This was introduced by Ericsson and asked SA WG3 to communicate to CN WG1 IMS related parameters that are required to be

provisioned in the UE from their point of view. A response LS was drafted after collection of comments and provided in TD S3-040865 which was reviewed and revised to remove "draft" in TD S3-040881 which was approved.

TD S3-040812 Proposed CR to 33.203: Editorial corrections (Rel-7). This was introduced by Vodafone and it was decided that this should be postponed to collect more editorial changes and if possible to include them in Rel-6 before the Release is frozen. **B Sahlin to collect editorials.**

TD S3-040720 Proposal for an informative Annex to the 3GPP TS 33.203 on support of end user devices behind a NA(P)T firewall and protection of RTP media flows. This was introduced by BT Group plc and proposed that this contribution forms the basis for an Informative Annex to TS 33.203, as no normative changes to the specification were considered necessary at this stage. The future adoption of a SIP application layer proxy, for example when the access gateway employs QoS mechanisms, is in no way precluded by this contribution, although considerable further work would be needed to support a SIP application layer proxy as an adjunct, and would have an impact on the normative part of TS 33.203.

It was thought that this contribution should be further developed before adding it as an informative Annex to 33.203 and impacted groups should also be consulted. It was also suggested that this may be more relevant for Rel-7 study as other Rel-7 work in this area is starting (e.g. TISPAN-type access). The Chairman reminded Members that SA WG3 had agreed that 33.203 was considered functionally frozen and this should rather be studied for Rel-7.

A CR to include this material was provided in TD S3-040721 which BT Group plc were asked to develop it further and potentially propose it as a Rel-7 CR in the future. **Members were also asked to provide comments on this paper to C. Blanchard by e-mail**.

TD S3-040762 Revisiting forwards compatibility towards TLS based access security. This was introduced by Ericsson and proposed an updated version of the CR provided at SA WG3 meeting #34 (TD S3-040639) in which the naming restrictions are limited to those naming schemes which are not visible to the user, i.e. home network names and IMPIs. In fact, from security point of view, there is no need to have naming restrictions on IMPUs. The username that is authenticated in IMS access security is IMPI, and IMPUs are not directly involved. A proposed LS to was also attached.

NOTE: The CR in TD S3-040639 agreed at SA WG3 meeting #34 on this subject was rejected by TSG SA #25 because it introduced architectural and service restrictions that should be first checked by SA WG1 and SA WG2. (The CR number on the attachment was allocated in error by MCC and should have been CR070, Rev 1).

The attached CR was considered and it was thought that this would overcome the objections received to the first CR by SA WG1 and SA WG2. There were more concerns expressed and it was decided to postpone this CR for further discussion until the next SA WG3 meeting. The CR was revised with the correct CR number in TD S3-040866 and was attached to the LS to SA WG1 and SA WG2 in TD S3-040867 for comments.

The attached LS was considered and revised in TD S3-040867 which was reviewed and further revised in TD S3-040882 which was approved.

6.1.2 Security for early IMS

TD S3-040738 Pseudo-CR to Early IMS draft: Removing an editorís note in section 7.2.1. This was introduced by Nokia and was agreed with some suggested corrections. **The editor was asked to include this Pseudo-CR with the comments.**

TD S3-040739 Pseudo-CR to Early IMS draft: Adding advantages of HTTP Digest method to Annex A. This was introduced by Nokia and added alternatives to Annex A. TD S3-040820 from Lucent Technologies also suggested changes to Annex A and this was also considered and found to include the main changes from TD S3-040739. TD S3-040846 also proposed changes to Annex A and this was also considered with these contributions.

TD S3-040846 Pseudo-CR to 33.878: Editorial changes and clarifications. This was introduced by Vodafone and proposed a compromise for Annex A which indicates that the solution was considered by was not adopted by 3GPP. There was support to include the advantages and disadvantages of alternative approaches that were not adopted for the full 3GPP solution in order to avoid readers thinking the "quick" solution is considered adequate for usual 3GPP systems.

The remaining changes in this contribution were reviewed and comments made which were noted by the editor. It was decided to combine the proposals into a single Pseudo-CR in order to clarify what will change in the draft when included. This was provided in TD S3-040868 and reviewed. Minor updates were made and the document revised in TD S3-040879 which was agreed for inclusion in the draft TR.

TD S3-040733 The choice of interim solution. This was introduced by Huawei and discussed the further network action and analyses implementation scenarios with different capable terminals and SIM/ISIM/USIM. After analysis, Huawei proposed that Alternative 2 is the recommended scheme (*After the HSS receives a Cx-MAR requesting the AKA authentication scheme, if the HSS find that user is a SIM user, then HSS selects the interim solution and returns a Cx-MAA message with the IP address that was stored in the HSS during PDP context establishment*). The proposed changes to section 7.2.4 were appended to the contribution.

It was noted that this contribution covered the situation with a fully 3GPP-complient terminal when either a SIM or USIM is inserted but was not clear about the interworking with the IMS Core Network and the terminal functionality and this should be the basis of a separate contribution. It was argued that Alternative 2 passes the decision to the network even if it knows it has a SIM inserted which can never support the full 3GPP solution. Alternative 2 was considered useful as it caters for the situation that a terminal does not check if it has a (U)SIM which supports the full solution and has low impact on the HSS. An complementary solution was proposed by Siemens in TD S3-040779 which was also reviewed.

TD S3-040779 Early-start IMS identification. This was introduced by Siemens and discussed issues of this co-existence of the early-start IMS security, and IMS security as specified in TS 33.203 for Release 5, and proposed how to handle the relevant inter-working cases. The proposed replacement of section 7.2.4 were appended to the contribution. It was questioned whether this solution prevented a bidding-down attack. Siemens responded that the idea was to control the terminals which users could use with their subscriptions and only allowing users in the long-term to access with the specified security solution, therefore preventing bidding-down attacks. It was commented that the explicit error indications need to be studied in order to reduce the impact on the network and existing codes should be used if possible.

The additions proposed in TD S3-040733 were agreed to be included in the draft TR and the editor was asked to include this on top of the changes proposed in TD S3-040779 which was also agreed, and an editors' note added to indicate that further solutions are under study. Contributions were invited to address concerns and provide any new solutions.

It was agreed draft an LS on this to CN WG1, CN WG4 and copied to SA WG2, which was provided in TD S3-040869. Telecom Italia remarked that TSG SA#25 did not ask TSG WGs to ìconditionallyî proceed with their specification work on Early IMS security but, rather, that ìthe resultant SA WG3 TR should be a 3GPP internal TR in the 33.8xx range without any impact on current specificationsî. According to this, SA WG3 decided to ask CN WG1 and CN WG4 to simply take note of the work done by SA WG3. The LS was then revised in TD S3-040880 which was approved.

TD S3-040696 Revised WID: Security for early IMS. This was provided by the Secretary for information about the version of the WID which had been modified at TSG SA #25 and approved. The updated WID was noted.

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

TD S3-040704 LS (from CN WG4) on SMS Fraud countermeasures. This was introduced by Siemens. CN WG4 asked SA WG3 to consider the attached CR 29.002 740 and to provide opinion on whether the solution proposed addresses the problem described in the LS S3-040642. In particular to provide guidance as to whether the proposal should be mandated or optional.

TD S3-040713 LS from T WG2: SMS Fraud countermeasures. This was introduced by Siemens. T WG2 asked SA WG3 to keep T WG2 informed concerning the progress of this work so that the impact on TS 23.040 can be assessed.

TD S3-040707 LS (from CN WG4) on Evaluation of the alternatives for SMS fraud countermeasures. This was introduced by Vodafone. CN WG4 asked GSM-A IREG and GSM-A SG to provide guidance to SA WG3 and CN WG4 on the expected relative timing of wide scale SIGTRAN (with IPSec) interconnect between operators in comparison with MAPsec adoption and interconnect between operators. This was copied to SA WG3 for information and was noted. A response from IREG was provided in TD S3-040826.

TD S3-040826 LS from GSMA IREG: Response to LS to 3GPP on Evaluation of the alternatives for SMS fraud countermeasures. This was introduced by Vodafone. GSMA IREG asked CN WG4 and SA WG3 to confirm that they:

1. understand the IREG response.
2. are able to proceed with the design and specification of TCAP handshake mechanism.
3. are able to complete the ìgatewayî design and specification of the MAPsec mechanism.
4. the dates when items 2 and 3 will be complete and approved by 3GPP.

It was thought that the SS7 firewalls mentioned in item 2 referred to MAP message screening functions. It was noted that MAPsec is not a complete security solution but only a part of the end-to-end signalling security support functions needed to ensure signalling integrity.

The contributions were discussed and it was noted that the requirements from IREG could be fulfilled using a Gateway solution, but it was also noted that the MAPsec work was stopped in Rel-4 due to lack of support for completing the Stage 3.

A contribution from Siemens in TD S3-040802 was considered to see if it answered some of the questions from IREG.

TD S3-040802 SMS Fraud countermeasure. This was introduced by Siemens and provided a follow-up of the discussion on ëSMS fraud countermeasuresí. It collected and analysed the received responses from CN WG4 and T WG2. Also the security and implementation variants of the TCAP handshake mechanism were analyzed. Siemens proposed:

1) To document the TCAP handshake short term solution for MT-forward-SM authentication, and the solution option 1 within an informative Annex to TS 33.200.
2) To carefully consider any additional impacts as this will delay the realization and acceptance of a solution. Therefore it is proposed not to require any change to the TCAP generation mechanisms. Additional tables with SS7/SMSC address seems to be required but cannot provide an absolute guarantee.

It was agreed that TCAP handshake mechanisms should be studied and included in the specifications as optional functionality and to try to co-operate with CN WG4 in order to finalise this within 2 or 3 meeting cycles.

A response to CN WG4 was provided in TD S3-040870 which was reviewed and approved.

A response to IREG was provided in TD S3-040871 which was reviewed and revised to remove "draft" in TD S3-040883 which was approved.

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 S3-040740 Extending NDS/AF for TLS. This was introduced by Nokia and discussed the possibility of extending NDS/AF to cover the case for establishing TLS connections between CSCF in IMS network and SIP Proxy in non-IMS network for SIP signalling protection. Nokia proposed that a new section will be added to NDS/AF in Rel 7 to extend the usage of NDS/AF for establishing TLS connections. Comments and questions should be sent to T. Koskinen and contributions on this topic should be provided to the next meeting.

6.5 UTRAN network access security

TD S3-040708 LS (from CN WG1) on Re-authentication and key set change during inter-system handover. This was introduced by Siemens. CN WG1 provided responses to RAN WG2 to their questions on re-authentication and key set change during inter-system handover and was copied to SA WG3 for information. The LS was noted.

6.6 GERAN network access security

TD S3-040702 LS (from GERAN WG1) on Feasibility Study on Generic Access to A/Gb Interface ñ Security Aspects. It was agreed to take comments and produce a response LS to TSG GERAN WG1 in TD S3-040878

which was approved. (Note: TD S3-040834 was provided and discussed by SA WG3, but the attachment required updating and so the document was revised to TD S3-040878).

TD S3-040712 LS (from T WG2) on Removal of A5/2 Algorithm from Specifications. This was introduced by the SA WG3 Chairman. T WG2 askeed SA WG3 to consider if other Specifications and 3GPP WGs may be more appropriate for the modifications recommended by SA WG3 and to clarify the guidelines to be more unambiguous, if SA WG3 plans to forward its recommendations to other WGs. These requests were noted.

TD S3-040723 Security context separation. This was introduced by Nokia and discussed the proposals for the A5/2 vulnerability problem: integrity protected A5 version negotiation, and special RANDs. Nokia concluded with a proposal that the Special RAND mechanism is introduced also for providing a generic mechanism for security context separation. It was commented that the most straightforward approach to solving the A5/2 problem is to remove it from terminals and encourage networks to upgrade to A5/1.

It was agreed that the proposals at this meeting should be presented and discussed briefly and further discussion held at the next meeting:

TD S3-040728 An observation about Special RAND in GSM QUALCOMM Europe, Ericsson

TD S3-040745 Key separation mechanism in GSM/GPRS Orange, Nokia

TD S3-040789 Future of GERAN Security Ericsson, Qualcomm Europe, Vodafone

TD S3-040790 Proposed WID: Access Network Security Enhancements Ericsson

it was agreed that B Sahlin would lead an e-mail discussion to consider the scope and try to make some progress with the proposed WID.

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 S3-040705 LS (from CN WG4) on Generic Authentication Architecture (GAA). This was introduced by Ericsson and asked SA WG2 for guidance on whether GAA should be considered as a new domain, different from CS/PS and IMS, or should instead be considered as a feature within the aforementioned domains. It was noted that the meaning of "domain" in this case should be clarified. The SA WG3 assumption is that GAA can be run independently of the IMS, CS and PS domains and this should be clarified to the groups. A LS on this was provided in TD S3-040827 which was reviewed and approved.

TD S3-040813 Relationship between GAA and Liberty. This was introduced by Vodafone and makes the following conclusions:

1. *The GAA has been developed independently of Liberty. It aims at allowing a 3GPP network operator to operate its own closely-controlled HTTP-based authentication and server/client interactions, over mobile core networks, without having to adopt Identity-based standards such as Liberty. However, it should be considered whether 3GPP should allow, as an option, the adoption of the Liberty ID-FF specs for the framework parts of GAA, like OMA have done with their OWSER.*
2. *The authentication part of GAA could be specified so that it appears as an authentication context that is compatible with Liberty ID-FF and Liberty ID-WSF. It should be considered whether GBA authentication, SSC authentication or both should be specified in this way.*

3. The work split between 3GPP and Liberty Alliance is for further study. It may be useful to send a preliminary liaison statement to Liberty Alliance.

There was some discussion over the proposal to work closely with the Liberty Alliance, and it was clarified that there were some complementary work areas and an advantage to use GAA for the Liberty Alliance and to study where the work of 3GPP overlaps with the work of the Liberty Alliance and where it is complementary work. It was agreed that this should be studied off-line by delegates and an e-mail discussion held in order to prepare an LS for the next SA WG3 meeting if appropriate. Silke Holtmanns agreed to Chair the e-mail discussion.

AP 35/01: Silke Holtmanns to chair an e-mail discussion on Liberty Alliance work and 3GPP GAA work and to prepare an LS for the next meeting if appropriate.

TD S3-040735 Safety of key material and proposed CR to 33.919. This was introduced by Huawei. The safety of GBA key material in GAA was discussed in the last SA WG3 meeting, a discussion paper and a pseudo-CR for adding the corresponding text to TR 33.919 were presented. It was thought that there was no corresponding text in the GBA TS and it was considered premature to add it at that time. Huawei think the key safety of usage is important for use of GBA and the attached CR to TR 33.919 introduces the requirement to Application guideline to use GAA. Another contribution to TS 33.220 discussing the corresponding solution and proposing to add the solution to TS 33.220 was provided in TD S3-040736 which was considered (see agenda item 6.9.2). This CR to the TR was then rejected in favour of a modified version of the CR to be added to TS 33.220.

6.9.2 TS 33.220 GBA

TD S3-040736 Impact analysis -Validity condition set by NAF:Proposed CR to 33.220. This was introduced by Huawei. In the SA WG3 meeting #33, the NAF set local validity condition of Transaction identity and key material according the special requirements was discussed and the method of limited number of times was thought as preferred method. But the concern rose about whether it will impact other interfaces. This paper analysis this issue and proposed a CR to 33.220. It was proposed that it should be clarified that these are examples on how new keys can be requested in case of expired or compromised keys. It was also noted that this does not introduce any mechanism to detect if a key has been compromised. The CR was revised in line with this in TD S3-040828 which was approved.

TD S3-040742 Proposed CR to 33.220: GBA USIM/ISIM selection. This was introduced by Siemens on behalf of Siemens and Nokia. At SA3#34 a new section 4.4.8 of TS 33.220 dealing with selection of UICC application for GBA was introduced (approved CR S3-040648). This document points to a necessary correction and, in addition, proposes improvements to the selection process as defined at SA3#34. The correction concerned the fact that a ìdefault USIMî is not defined in 3GPP specifications, and that the term ìselectionî is used in a way not compatible with other 3GPP specifications. Instead of default USIM, it was suggested that SA WG3 should use the notions of ìlast selected USIMî and ìlast selected ISIMî. The two main goals of the improvements are (i) the optional possibility for a Ua application to choose a particular UICC application (not only UICC type) and (ii) more deterministic behaviour and better understandability of the selection process by the user. A CR was attached to implement these proposals. The CR was agreed and attached to a LS in TD S3-040830.

TD S3-040714 LS (from T WG2) on USIM and ISIM selection in the UE. This was introduced by Siemens and T WG2 asked SA WG3 to continue discussions on this matter with SA1 rather than T2. It was agreed to send a response LS to SA WG1, copied to T WG2 and T WG3 attaching the CR agreed in TD S3-040742 in TD S3-040830 which was reviewed and approved.

TD S3-040695 Service discovery using default domain method. This was introduced by Nokia and proposed that the default domain method described in section 2.1 is added to TS 33.220 as one of the methods for discovering the BSF. A CR was attached which implements the necessary changes. Nokia also suggested that this discovery method is not used for the PKI portal. The CR was considered and it was agreed that only the first method should be included in which case it is implicitly the default. The CR was updated in TD S3-040831 which was approved.

TD S3-040756 Proposed CR to 33.220: TLS profile for securing Zn' reference point (Rel-6). This was introduced by Siemens on behalf of Nokia and Siemens. This CR was agreed.

TD S3-040741 GBA User Security Settings (GUSS) usage. This was introduced by Nokia on behalf of Nokia, Siemens and Huawei and was discuaaed. It was agreed to include some additional error cases and correct the definition of USS. A revised CR was provided in TD S3-040832 which was approved.

TD S3-040746 Proposed CR to 33.220: Usage control of the service in visited network. This was introduced by Huawei. It was agreed that these requirements should be discussed in the re-drafting group for TD S3-040832 and a single CR provided for approval.

TD S3-040811 Enhanced key freshness in GBA. This was introduced by "3" and discussed a weakness of GBA, in that it does not provide any key freshness, and proposed a possible solution to that problem for SA WG3 to accept the in principle at this meeting and then CRs can be prepared for agreement at the next meeting. There was some reluctance to include this protocol proposal in the TS as it may reduce the generic nature intended by GAA. It was decided that there should be an e-mail discussion on this subject until the next meeting by interested Members.

An off-line discussion to find a way forward on the support of GBA-U was held. It was reported that no conclusions could be reached and it was indicated that more time was needed for Members to consult on this and a decision should be saught at the next meeting. This would mean that no firm guidance can be given to T WG3. There was an objection from Axalto to this as the deadline for Release 6 is getting close and a decision is needed now or double work will need to be done by T WG3 in order to be ready with both solutions. Vodafone: Mandating GBA_U on the terminal would cause a dependency for terminals supporting only GBA which should be avoided.

Straw Poles (show of hands one vote per Member company):

A. Postpone to next meeting: 8 Member companies
B. Try to reach decision at this meeting: 9 Member companies

A. Leaning towards GBA_U Mandatory on ME: 7 Member companies
B. Leaning towards Keeping Optional for ME: 5 Member companies
C. No Firm Opinion: 8 Member companies

It was decided that another evening session would be needed in order to get a better idea of whether this can be resolved. This was chaired by Peter Howard (evening Thursday).

After the evening session it was reported that although no decision could be made between manufacturers, it was hoped that the operators could meet and try to come to a consensus in order to resolve the issue and allow progress. Vodafone, 3 and Nortel Networks and Rogers Wireless indicated that they were now leaning towards making GBA_U Mandatory on ME. Another show of hands was made:

A. Leaning towards GBA_U Mandatory on ME: 12 Member companies
B. Leaning towards Keeping Optional for ME: 5 Member companies
C. No Firm Opinion: 4 Member companies

Given this new indication, the Chairman asked if a decision could be made. It was argued that "GBA_U Mandatory on ME" was a vague decision as this allowed many different implementations some of which would not be acceptable from a security point of view. It was agreed that this implies the terminal can determine the UICC support of GBA and can derive the external Keys if necessary. i.e. the terminal will behave differently if a GBA-capable UICC is inserted, to when a legacy UICC without GBA support is inserted.

The following statements were discussed, but no conclusions drawn:

GBA aware ME shall support bootstrap functions
Bootstrapping keys from GBA_U bootstrap are kept in the UICC
KS_ext_NAF is derived on the UICC
The KS_ext does not leave the UICC in the case of GBA_U

P. Howard offered the following statement which summarised the agreement reached by SA WG3:

"If the UICC supports GBA_U, KS_ext shall not leave the UICC and as a direct consequence, a terminal will behave differently if a GBA-capable UICC is inserted, to when a legacy UICC without GBA support is inserted".

TD S3-040727 Modifying the MAC in AKA. This was introduced by QUALCOMM Europe and described the proposal of using a modification of MAC to indicate a standardized interpretation of the AMF provides a more flexible and future-proof approach than simply using it to indicate a GBA_U run, and asked SA WG3 to further consider and discuss this. After discussion this was not considered possible for Rel-6 and the document was noted.

TD S3-040710 LS (from T WG3) on USAT initiated GBA_U Bootstrap. T WG3 asked SA WG3 to comment on the security requirements and considerations about this procedure to enable UICC applications to initiate a GBA_U Bootstrapping procedure. Comments were collected for a response LS in TD S3-040835 which was reviewed and revised in TD S3-040877 which was approved.

The following documents were introduced by the authors and used for evening discussions:

TD S3-040773 GBA_U: finalisation of GBA_U procedure: Gemplus, Axalto, Oberthur.

TD S3-040825 Comments to S3-040773: GBA_U: finalisation of GBA_U procedure: Nokia, Siemens Ericsson.

TD S3-040776 Proposed CR to 33.220: Optimization of the GBA_U key derivation procedure (Rel-6): Gemplus, Axalto, Oberthur

TD S3-040783 Proposed CR to 33.220: Enabling optional GBA_U support for ME (Rel-6): Nokia, Siemens, Ericsson, Samsung Electronics

The following documents were dependent on the decision for mandating GBA_U support and may be re-submitted in the next meeting if they are still valid.

TD S3-040774 GBA: Support of GBA_U capabilities for Rel-6 Mes: Gemplus, Axalto, Oberthur

TD S3-040775 GBA_U: Alternatives for GBA_U derivations: Gemplus, Axalto, Oberthur

TD S3-040777 Proposed CR to 33.220: GBA_U: storage of Ks_ext in the UICC (Rel-6): Gemplus, Axalto, Oberthur

TD S3-040778 Proposed CR to 33.220: Requirement on ME capabilities for GBA_U (Rel-6): Gemplus, Axalto, Oberthur

TD S3-040784 Proposed CR to 33.220: Description of UICC-ME interface (Rel-6): Nokia, Samsung Electronics

TD S3-040824 Comments to S3-040774: GBA: Support of GBA_U capabilities for Rel-6 Mes: Nokia, Siemens, Ericsson

6.9.3 TS 33.221 Subscriber certificates

TD S3-040782 Proposed CR to 33.221: Visited network issuing subscriber certificates (Rel-6). This was introduced by Nokia and was agreed.

6.9.4 TS 33.222 HTTPS-based serrvices

TD S3-040731 Proposed CR to 33.222: GBA supported indication in PSK TLS (Rel-6). This CR was agreed.

TD S3-040734 Proposed CR to 33.222: Editorial correction of TS 33.222 (Rel-6) The principle of this proposal was agreed, but it was decided to include this in another CR to be developed for the next meeting.

6.10 WLAN interworking

TD S3-040711 LS (from T WG2) on MMS over 3GPP Interworking WLANs. This provided responses to SA WG2's questions on MMS over WLAN and was copied to SA WG3 for information. The LS was noted.

TD S3-040747 Control of simultaneous session in scenario 3. This was introduced by Ericsson. The control of simultaneous sessions in scenario 3 has to be made without the help of VPLMN id and WLAN AN id parameters, as it has been proven that these ones would have to be sent from the WLAN UE. The major drawback is that these parameters are not always available in the WLAN UE and, if they are, there is no mechanism to authenticate them so they could be spoofed by an attacker. The only exception is when the PDG is in the VPLMN. This situation can be detected by the AAA server and use the VPLMN id received by the PDG. A proposed CR to tackle this problem was provided in TD S3-040748.

TD S3-040748 Proposed CR to 33.234: Control of simultaneous accesses in scenario 3 (Rel-6). It was agreed that the editors' notes should be removed when the issues are solved and the target for this is for the December TSG SA Plenary. It was therefore decided to leave this change to an editors note and work on solutions to remove the complete editors note.

TD S3-040749 Use of MAC addresses. This was introduced by Ericsson and analysed the suitability of using the MAC address to identify the userís device in WLAN interworking and showed that only in one case the MAC addresses are reliable parameters to detect this type of fraud, but in the rest they donít help. Therefore, the AAA server has to be able to detect this situation (the first case) and enforce policies only in that case. In the rest of the situations, the MAC addresses should be discarded if received. If the AAA server is not able to determine the trustfulness in the MAC address (for example because the WLAN access point information is not available), it is recommended to NOT enforce any policy, based on the MAC addresses. A proposed CR to tackle this problem was provided in TD S3-040750.

TD S3-040750 Proposed CR to 33.234: Clarification on the use of MAC addresses (Rel-6). It was suggested that the second sentence from the change to step 18 is removed and replaced by an editors not that this requires study. As new editors notes were not desirable at this late stage for Rel-6, it was decided to remove the second sentence and remove "only" from the first sentence. Other grammatical changes were also identified and the CR will be revised by Ericsson for the next meeting.

TD S3-040751 Proposed CR to 33.234: Sending of W-APN identification (Rel-6). This was provided by Ericsson. The changes were considered confusing so the CR was revised in TD S3-040864 which was reviewed and approved.

TD S3-040752 Proposed CR to 33.234: Clean up of not completed chapters (Rel-6). This was provided by Ericsson. It was commented that the changes to 4.2.5 "*Areas in which requirements are desirable are*" was not very well worded for a specification and it was agreed to modify this to "*areas where there are relevant link-layer requirements are*". The revised CR was provided in TD S3-040836 which was reviewed andrevised to add the affected clause 2 in TD S3-040886 which was approved.

TD S3-040763 Proposed CR to 33.234: Passing keying material to the WLAN-AN during the Fast re-authentication procedure (Rel-6). This was provided by Samsung Electronics and was reviewed and agreed.

TD S3-040764 Proposed CR to 33.234: Clarification on Deletion of Temporary IDs (Rel-6). This was provided by Samsung Electronics. Minor modifications were made and the CR was revised in TD S3-040837 which was agreed.

TD S3-040765 Proposed CR to 33.234: Clarification on Protecting Re-authentication ID in FAST/FULL Re-Authentication procedure (Rel-6). This was provided by Samsung Electronics and was reviewed and agreed.

TD S3-040766 Proposed CR to 33.234: Assigning Remote IP Address to WLAN UE using IKEv2 configuration Payload (Rel-6). This was provided by Samsung Electronics. This was provided by Samsung Electronics and was reviewed and agreed. It was noted that in future, changes to figures need to be made as a deleted old figure and added new figure with change tracking.

TD S3-040767 Proposed CR to 33.234: Tunnel Redirection Procedure (Rel-6). This was provided by Samsung Electronics. It was considered unreasonable to include this in Rel-6 as changes will be needed to IETF specifications. It was clarified that the new use of an error code would be needed in the IETF. It was added that if tunnel redirection is a requirement which cannot be supported for Rel-6 then this needs to be reported back to SA WG2 in order to remove the requirement for Rel-6. It was decide that this should be further studied and the full implications understood before accepting this CR. The CR was therefore postponed until the next SA WG3 meeting. Samsung were asked to provide information about IETF status and SA WG2 situation on this.

TD S3-040768 Proposed CR to 33.234: Tunnel Establishment Procedure (Rel-6). This was provided by Samsung Electronics. It was noted that the new figure was not marked with a revision mark (as added) and the old figure was not shown (as deleted). The change from a response message to a request message was questioned in Step 3. Samsung responded that this followed the IKEv2 specification as the intermediate nodes cannot generate response messages. It was also commented that the use of DIAMETER in the message flow was not correct in this specification and the protocol choice should be left to the Stage 3 (CN WGs). It was decided to postpone this CR for further checking and clarification of the need for it. Samsung checked the IEEE specifications and submitted a revised CR in TD S3-040861 which was reviewed and approved.

TD S3-040769 Proposed CR to 33.234: Multiple Tunnels to the same PDG for different W-APN (Rel-6). This was provided by Samsung Electronics. The optimisation of the EAP procedure compared to the main session establishment using PKI was commented to be a small gain with added implementation complexity was questioned, along with the consequences if not approved, as there is an existing solution of re-running the session initiation procedure. It was considered that this optimisation should not be considered for Rel-6, but could be re-considered for Rel-7 and further study can be made along with other optimisations for Rel-7.

TD S3-040770 Proposed CR to 33.234: Multiple Tunnels establishnemt with different PDG (Rel-6). This was not agreed and to be studied for Rel-7 as for the CR in TD S3-040769.

TD S3-040699 LS (from SA WG2) on mapping tunnels for WLAN 3GPP IP access and W-APNs. This was introduced by Samsung Electronics and asked SA WG3 to consider the requirements on mapping tunnels for WLAN 3GPP IP access and W-APNs in their work. This requirement was questioned as it seemed to contradict the principle not to set up multiple PDP contexts for a single UE. It was noted that the technical means for several tunnels are in place and that there are associated risks with this in Corporate Network scenarios. A mechanism exists in SA WG3 WLAN specification to cover this requirement. Peter Howard agreed to investigate the current status restricting simultaneous PDP contexts in the Network side. The LS was then noted.

AP 35/02: Peter Howard agreed to investigate the current status in CN specifications of restricting simultaneous PDP contexts in the Network side (Ref: LS from SA WG2 in TD S3-040699).

TD S3-040701 Reply LS (from SA WG2) on Binding Scenario Information to Mutual EAP Authentication. This was introduced by Samsung Electronics. SA WG2 asked SA WG3 to consider their concerns on binding scenario information to mutual EAP authentication in any decisios made. It was noted that certificates on the PDG were expected to stay (contributions reinforcing that were availablke at the meeting) and this new mechanism was not currently proposed. The LS was then noted. **It was also noted that "scenario" needs to be replaced with the formal names in the specification and the Rapporteur and Secretary agreed to discuss a way of doing this in the specification.**

TD S3-040716 Using PDG certificate in scenario 3. This was introduced by Nokia and discussed the use of server certificates scenario 3 in preventing a WLAN Access Point (AP) from masquerading a Packet Data Gateway (PDG) or vice versa. Nokia proposed that server certificates are used in scenario 3 to authenticate the PDG. However, this solution will not protect against dishonest PDG impersonating as a WLAN AP. If this case is considered important, then support for enhanced NAI should still be included. A related CR was provided in TD S3-040717.

TD S3-040717 Proposed CR to 33.234: Profile for PDG certificates in Scenario 3 (Rel-6). This was introduced by Nokia. It was proposed that support for OCSP should be made mandatory. The use of specific "3gppnetwork.org" name was questioned as other names may be used in practice and this should have been intended as an example name. It was clarified that this is an entry point to the 3GPP network services for Rel-6 (therefore owned by "3gppnetwork.org") and this will be reviewed for Rel-7 work. **It was agreed that this should be streamlined with the NDS/AF profile, as both profiles may be needed.** Contributions were requested for the next SA WG3 meeting on this. Finalisation of this CR was therefore postponed for the next SA WG3 meeting, including the need for the restriction of using "3gppnetwork.org" for Rel-6.

TD S3-040724 Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces) (Rel-6). This was introduced by Toshiba on behalf of the supporting companies and was provided after discussions held in conference calls before this meeting. Toshiba thanked the Chairman for allowing these very active and useful conference calls, without which progress would not have been easily made. It was clarified that this CR had been sent out after the conference call and no objections had so far been received. It was noted that the CR contained Comments markers, which should be removed as they are not part of the proposed CR. The editors note added in 4.2.4.2 was thought inappropriate and it was agreed to remove this and Toshiba were asked to provide the draft LS to Bluetooth to communicate this requirement and ask for their reaction. The UICC presence detection (requirement 10) was also questioned as it may be easily falsified. It was responded that the only way of securing this mechanism is to re-authenticate and this mechanism was intended only to overcome error conditions and not to improve security of the UICC presence verification. It was kept for a general use-case, so that sharing ends when the user removes the USIM, rather than to protect against fraud scenarios. It was reported that the session keys will be in the MT for scenario 2 and therefore UICC presence is already determined by the MT. It was decided that requirement 10 should be removed at this time and requirement 5 also removed as the Network will terminate the session if the USIM is not present and a re-authentication fails. The CR was revised in TD S3-040838 which was agreed.

TD S3-040725 Proposed CR to 33.234: Bluetooth security and configuration considerations for Annex A4 of TS 33.234 (Wireless Local Area Network (WLAN) interworking security) (Rel-6). This was introduced by Toshiba on behalf of Toshiba, BT and supporting companies. It was proposed that this should be placed as an annex in TR 33.900 instead of this specification. A.4.3 item 6 refers to reserving at least 20 channels for the local communication link. It was clarified that this follows the Bluetooth requirement to mitigate DoS attacks by simple interference. The references to news and research papers were also not appropriate for the TS references section. It was also commented that the Bluetooth information is likely to change and this would need careful tracking and updates to the TS. It was therefore agreed that this information should be moved to the "Guide to 3GPP Security", TR 33.900 as an annex. A Liaison to Bluetooth-SIG including the requirements in A.4.1, A.4.2 and A.4.3 and asking them to take this into account in their profile work was provided in TD S3-040839 which was reviewed and updated in TD S3-040874 to include the attachment of TS 33.234 version 6.2.1 which was approved.

AP 35/03: Toshiba to create an update to TR 33.900 including agreements and provide to next meeting.

TD S3-040726 Comments to: Classification of security requirements on local interface. This was provided by Toshiba for information on the results of the conference calls and was noted.

TD S3-040760 3GPP UE function split for a 3GPP WLAN user equipment. This was introduced by Axalto on behalf of Axalto and Gemplus and concluded that the usage of SIM Access Profile, as currently specified by TS 33.234, may result in undesired implementations, compromising the security of the whole system and spreading the threats between WLAN and GSM/GPRS domains. A related CR was provided in TD S3-040758 , which included some specific requirements for the SIM Access Profile usage in WLAN UE functional split. It was also concluded that the usage of EAP authentication capabilities of a UICC offers higher security and improves interoperability. Moreover, this is the only implementable solution in Rel-6 timeframe as ETSI SCP has completed the standardization of the EAP support in UICC and as T WG2 completed the standardization of UICC AT commands. We kindly recommend SA3 to adopt this solution as a new functional split scenario. A related CR was provided in TD S3-040759. It was questioned whether this could be done using AT commands. Axalto responded that this was not something that could be easily standardised within the Rel-6 timeframe. It was suggested that T WG2 could be asked to standardise the necessary commands for Rel-6 and if they could do this for December 2004 this may be a better solution for Rel-6. It was also commented that current smart cards should support dunctional split so the backwards compatibility would be needed. It was agreed to send an LS to T WG2 to ask about the feasibility of using AT commands for this in the Rel-6 time frame, which was provided in TD S3-040840 and reviewed. The LS was revised in TD S3-040876 which was approved.

TD S3-040758 Poposed CR to 33.234: Alignment of TS 33.234 with SA3 decisions on WLAN UE function split (Rel-6). This was provided by Axalto and Gemplus to support the conclusions in TD S3-040760. This was discussed in an off-line session with TD S3-040759 and a combined CR was provided in TD S3-040841 along with the drafting of the LS in TD S3-040840.

TD S3-040759 Proposed CR to 33.234: Correction of WLAN UE function split (Rel-6). This was provided by Axalto and Gemplus to support the conclusions in TD S3-040760. This was discussed in an off-line session with TD S3-040758 and a combined CR was provided in TD S3-040841 along with the drafting of the LS in TD S3-040840.

TD S3-040841 Proposed CR to 33.234: Correction of WLAN UE function split. This CR was revised in TD S3-040875 which was agreed.

TD S3-040771 Proposed CR to 33.234: Deletion of inconclusive text on A5/2 countermeasures (Rel-6). This CR was provided by Siemens and was agreed.

TD S3-040772 Proposed CR to 33.234: Alignment of IPsec profile with RFC2406 (Rel-6). This CR was provided by Siemens and was updated to remove the editors' note in TD S3-040842 which was agreed.

TD S3-040709 Reply LS (from T WG3) on Storage of temporary identities for EAP authentication. This was introduced by Axalto and asked SA WG3 to examine further requirements for security enhancements of fast re-authentication procedures and to analyze the proposal solution based on EAP support in USIM, if these security enhancements are introduced in 3GPP I-WLAN. SA WG3 were asked to come back to T WG3 if further work is needed on this topic for completion of Rel-6 changes in the appropriate specification(s). It was agreed that this should should be studied for Rel-7 and whether it should be considered for Rel-6. C. Blanchard agreed to study this and report back to SA WG3. The LS was then noted.

TD S3-040722 Resolving the editors notes in Wireless Local Area Network (WLAN) interworking security 3GPP TS 33.234. This was introduced by BT Group plc and provided reasoning for the removal of certain Editors' notes from the specifications. It was agreed that all the editors' notes, including section 5.4 (which should then be renamed "Void") should be deleted. **M. Pope agreed to check that these are not already deleted by otherCRs and create a new CR for the next SA WG3 meeting**.

AP 35/04: M. Pope to create CR to 33.234 removing editors notes as defined in TD S3-040722.

6.11 Visibility and configurability of security

There were no specific contributions under this agenda item.

6.12 Push

There were no specific contributions under this agenda item.

6.13 Priority

There were no specific contributions under this agenda item.

6.14 Location services (LCS)

There were no specific contributions under this agenda item.

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

TD S3-040732 Proposed WID for Trusted Open Platforms in 3G. This was proposed by Intel, T-Mobile, Toshiba, Gemplus, Motorola, RIM and Verisign. It was agreed that the resulting draft TR should be planned for information to TSG SA for June 2005, and TSG SA approval in September 2005, because over-aggressive planning would not make any difference in the Release schedule and Members would have more time to consider the issues. However, the work may be pursued faster than planned if wished by the supporting companies. It was commented that some of the objectives may be considered or interpreted as outside of the scope of 3GPP and this should be taken into account when developing the draft TR. It was reported that more supporting companies existed which did not appear in the supporting companies list. It was also noted that charging impact was not fully known, but it was not expected to be impacted and should not be included. It was noted that the GSMA should also be consulted on this work. The title was asked to be modified to make it more specific to its scope, e.g. "Trust Requirements for Open Platforms in 3GPP". The WID was revised in TD S3-040843 which was reviewed and approved.

6.16 Open service architecture (OSA)

There were no specific contributions under this agenda item.

6.17 Generic user profile (GUP)

TD S3-040706 LS (from CN WG4) on Request for end to end example showing how the Liberty Alliance security framework fits the 3GPP GUP security requirements. This was introduced by Lucent Technologies and asked SA WG3 to provide:

- *an end-to-end example of the security mechanisms involved in GUP security, based on the Liberty Alliance security framework. This example would clarify ñ among other things ñ the various entities involved, the kind of messages exchanged and security methods used,*
- *a recommendation in terms of preferred security methods in the context of GUP.*

Related contributions were considered in TD S3-040845 and TD S3-040786:

TD S3-040845 GUP Security (cleaned-up replacement of TD S3-040729 with revisions accepted). This was introduced by Lucent Technologies and addressed a number of issues related to GUP security. In the context of GUP, security encompasses two aspects: authentication and encryption. Lucent technologies proposed that although the final decision on which specific security mechanism to be used for GUP is CN WG4ís, SA WG3 should use its' security expertise and evaluate the different available solutions, present the pros and cons of each and potentially propose a ìdefaultî protocol (or a small set of options to chose from) to CN WG4 with an LS.

TD S3-040786 GUP Security ñ Recommendations for UE implementations. This was introduced by Ericsson on behalf of Ericsson, Nokia and Intel and clarified that *LAP-WSF Security Mechanisms* provide a variety of security profiles in order to accommodate multiple deployment scenarios. The contribution also proposed that in the case where a UE acts as a GUP requestor over Rg interface, GUP specifications should refer to *LAP-WSF Client Profiles* as providing valuable guidance for this deployment case in particular. It was noted that the contribution was specifically focused on the Rg interface.

It was therefore proposed that:

- *GUP specifications should also refer to the recommendations provided at chapter 3 of [LAP-WSF Client Profiles] as providing valuable guidance for deployments where a UE acts as a GUP requestor over Rg-interface.*
- *The role of a Liberty ID-WSF Discovery Service as a Trusted Authority capable of issuing authentication and authorization statements should be also mentioned.*

CN WG4 and SA WG2 should be informed of such recommendations so they can include the reference to LAP-WSF Client Profiles and LAP WSF Discovery Service within GUP specifications as appropriate.

This draft LS to CN WG4 and SA WG2 was provided by Ericsson in TD S3-040787.

Mandating TLS with Server Certificates was proposed .in order to help with the large number of options which may otherwise cause interoperability problems. It was commented that manual installation of tokens could be a security problem as the token would probably be used for a long period (e.g. username/password system). It was clarified that the proposal would be to take the recommendation to use TLS in the draft LS and make it madatory. Ericsson reported that they preferred not to restrict the types of tokens to be used at this time.

These contributions were noted and the LS in TD S3-040787 was then considered.

TD S3-040787 Proposed Draft LS on GUP Security Recommendations. This was introduced by Ericsson and proposed the LS to send to CN WG4 and SA WG2. It was agreed that the urn:liberty:security:2004-04:TLS:Bearer security mechanism shall be mandatory for use in case the UE is acting as a GUP requestor over the Rg-interface. It was aksed what would be the impact if there is no Discovery service available and it was agreed that it should be highlighted that the Discovery service is an optional element in this proposal. It should also be checked whether the Liberty Alliance binds this with the Discovery service. The LS was revised to include the requested comments in TD S3-040844 which was reviewed and revised to remove revision marks in TD S3-040885 which was approved.

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 S3-040847 MBMS security work split. (This was an updatet of TD S3-040808). This was introduced by Ericsson and discussed the finalisation of MBMS security:

- Ericsson proposed that MBMS security work should be finalised in cooperation between SA WG3 and SA WG4 and that CN WG1 is not involved.
- ï Ericsson also proposed how the security work should be finalised. This is described in section 2.2 of the contribution.
- ï Due to the limited time schedule in Rel-6 Ericsson recommended that the information transfer from SA WG3 to SA WG4 for the topics mentioned above is handled via company contributions.

It was noted that MBMS service refers to MBMS User service security (so as not to confuse it with the MBMS bearer service security).

Ericsson proposed to send an LS to both SA WG4 and CN WG1 on the issue and attached a draft LS to the contribution which was reviewed and updated to take the comments on the main discussion document into account in TD S3-040848 attaching the main contribution of TD S3-040847. The LS was reviewed and revised in TD S3-040884 which was approved.

TD S3-040806 Scope of MBMS security. This was introduced by Ericsson and tried to clarify the following issues in order to help finalisation of MBMS security mechanisms:

1. Is MBMS security regarded as part of MBMS User Service or MBMS Transport Service activity? In other words, is MBMS security access independent?
2. What is the scope of MSBS protection? In the current TS 33.246 one can get the understanding that MBMS security provides protection for MBMS transport bearers.

It was clarified that the "Delivery method" is assumed to be part of the User Service e.g. 2 streams may be seen as a "User Service Session". It was also noted that the mapping of Download Services into Transport Bearers (SA WG4 work) is not clear at the moment.

Ericsson were thanked for this good clarification paper and the related CR proposal in TD S3-040807 was considered and updated in TD S3-040849 which was agreed.

TD S3-040761 Proposed CR to 33.246: Clean up of MBMS TS (Rel-6). This was introduced by Ericsson and was reviewed. It was commented that the moving of section 4.2 to 6.x did not seem appropriate and it was reinstated. The updated CR was provided in TD S3-040850 which was reviewed and agreed.

TD S3-040819 Proposed CR to 33.246: Clarification of MSK key management (Rel-6). This was introduced by Ericsson and was reviewed. It was noted that this proposal replaces and deletes subclauses, which should not be done for specifications under change control. The CR was updated to correct this in TD S3-040851 which was reviewed and revised again in TD S3-040889 which was agreed. **It was noted that enhancements to this would be brought to the next SA WG3 meeting and these should incorporate these changes in order not to have conflicting CRs at the meeting.**

TD S3-040801 Proposed CR to 33.246: Protection of the Gmb reference point (Rel-6). This was introduced by Siemens and was reviewed and agreed.

TD S3-040780 Proposed CR to 33.246: Traffic protection combinations (Rel-6). This was introduced byNokia and was reviewed. It was clarified that the flexibilty to allow just integrity protection without confidentiality protection was desirable for service providers. The CR was updated to remove the indication that it impacts UICC in TD S3-040852 which was agreed.

TD S3-040781 Extensions to OMA DRM V2.0 DCF for MBMS Download Protection. This was introduced by Nokia and provided a proposal for the extensions needed for DCF to support MBMS Download protection as requested in the joint SA WG3/SA WG4 MBMS ad-hoc meeting. Related contributions were provided in TD S3-040809 and TD S3-040791 which provided a comparison of the 2 proposals.

TD S3-040809 Updated: MBMS Download Protection using XML. This was introduced by Ericsson and provided another proposal for MBMS Download Protection. A comparison between this and TD S3-040781 was provided by Ericsson in TD S3-040791.

TD S3-040791 MBMS Comparison of DCF and XML-encryption. This was introduced by Ericsson and provided a comparison between the mechanisms in TD S3-040781 and TD S3-040809. Ericsson concluded that the major difference between the two approaches is that DCF requires modifications to OMA DRM standards (or an MBMS aware implementation) to be able to re-use DRM functionality.

Nokia commented that their proposal did not reqire any specification work in OMA as they have a Naming Authority who allocate identifiers and no changes are expected to the DRM specifications for this. Ericsson considered that something will be needed, but Nokia considered it could be specified in the MBMS specifications. Ericsson also highlighted that their proposal does not affect any other organisations and the control is compltely within SA WG3.

The overheads introduced by both methods was questioned but it seemed that they were both fairly low. Nokia considered the XML method would introduce extra complexity, Ericsson did not see any additional complexity in their proposal.

It was commented that the protection offered here is for MBMS Download and not for MBMS Content protection. It was also reported that while the MBMS protection can be turned off when DRM protection is available, both DRM and MBMS protection may be needed in certain cases.

It was thought that the decision on the protection made by SA WG3 should not impact the work of SA WG4 too much and therefore some more time for analysis and comparisons should be used until the next SA WG3 meeting. **It was agreed that contributions for this should be made available earlier than the main deadline, i.e. Deadline for contributions: 2 November 2004, Direct comments response contributions 9 November 2004.**

TD S3-040810 Proposed CR to 33.246: XML protection for download services (Rel-6). This was not discussed as it depended on the dicisions made for the MBMS Dowmload Protection. Ericsson were asked to re-consider an input for the next meeting, depending on the results of discussions.

TD S3-040795 MBMS download MTK transport. This was introduced by Ericsson and proposed that the accompanying CR in TD S3-040794 that specifies how the MTK is delivered over FLUTE as a separate object is implemented:

TD S3-040794 Proposed CR to 33.246: MBMS MTK Download transport (Rel-6). This was reviewed and revised in TD S3-040853 which was agreed.

TD S3-040753 MKI field transmission method for SRTP packet in MBMS. This was introduced by Samsung Electronics and proposed a solution to the need of reducing the length of MKI field used while not impacting other aspects. Samsung Electronics proposed to develop a CR to the next SA WG3 meeting if the scheme was agreed. Ericsson commented that the field size should be fixed for all operations according to the SRTP RFC and also that other methods existed which may be at least as efficient while being in accordance with the RFC. It was therefore decided that this could not be used for Rel-6 and Members were encouraged to provide other proposals.

TD S3-040796 The need for and use of salt in MBMS streaming. This was introduced by Ericsson and discussed the use of salt as a countermeasure to pre-computation attacks against the MBMS streaming system and concluded that the use of salt is required in MBMS to not shorten the effective key length, and all mechanisms to use it are already in place in the protocols used. Ericsson proposed that the accompanying CR in TD S3-040797 is implemented. It was commented that the mechanism seems to try to protect against a 128-bit streaming cipher attack which was not considered a feasible attack for well-chosen algorithms. It was agreed that this proposal would require more justification before being considered.

TD S3-040797 Proposed CR to 33.246: MBMS Transport of salt (Rel-6). This was rejected as the proposal in TD S3-040796 was not agreed.

TD S3-040798 Reliable (S)RTP index synchronization for MBMS streaming. This was introduced by Siemens and described the need for reliable (S)RTP index synchronization for MBMS streaming and proposed to adopt a solution based using the CS ID map info within the multicasted MTK messages. A proposed a CR for this was attached and was reviewed. The CR was revised in TD S3-040854 which was agreed.

TD S3-040818 Proposed CR to 33.246: MTK update procedure for streaming services (Rel-6). This was introduced by Ericsson and was reviewed. It had been commented that this was not in line with another CR from Ericsson which changed the same area of the text and Ericsson agreed to revise the CR in TD S3-040855 which was reviewed and agreed.

TD S3-040754 Proposed CR to 33.246: Delivery of multiple keys in one MIKEY message for MBMS. This was introduced by Samsung Electronics and was reviewed. It ws commented that if this were done the maximum key length and maximum number of Keys a UICC can process would need to be specified to take into account the variable key lengths. It was therefore decided to reject this proposal for Rel-6.

TD S3-040833 Proposed CR to 33.246: Modification of delivery of MIKEY RAND field in MSK updates (Rel-6). This was introduced by Axalto on behalf of Axalto Gemplus and was reviewed. It was clarified that this change was proposed for management purposes rather than security reasons. The CR was updated to correct the WID in TD S3-040856 which was agreed.

TD S3-040799 Proposed CR to 33.246: Clarify the use of mandatory MIKEY features for MBMS (Rel-6). This was introduced by Siemens and was reviewed. It was commented that this was a new functional change and it may be better to remove the mandatory part from the RFC instead. It was commented that it may be better to make this change rather than waiting for the RFC to be modified and this was thought to be the only deviation from MIKEY. It was also commented that this could be an informative annex as it does not actually mandate anything new for MBMS (it allows the Time-stamp payloads UTC and NTP not to be implemented for MBMS capable UICC/ME). It was decided to investigate this and request updated contributions to the next meeting.

TD S3-040817 IETF work for MIKEY MBMS extensions. This was introduced by Ericsson and discussed the needed work in IETF for MIKEY MBMS extensions and proposed to

- *Start the work with private numbering, i.e. needed extensions are taken from the private number space and specified in TS 33.246; and*
- *Start parallel official IETF process to get ìofficial name space numbersî*

It was also proposed that if the official IETF process is completed before TS 33.246 is completed, the private numbers in the TS are changed to ìofficial numbersî. Else the private numbers stay in use and the IETF process can be stopped. TD S3-040800 was related to this and was considered and agreed. It was then proposed that the official numbers should be sought from IANA. Member companies were asked to contribute this request to the IETF. Ericsson agreed to do this.

TD S3-040800 Proposed CR to 33.246: Adding MIKEY payload type identifiers (Rel-6). This was introduced by Siemens and was reviewed. The CR was revised in TD S3-040857 which was agreed.

TD S3-040792 MBMS Key derivation chain. This was introduced by Ericsson and shos how MBMS values can be plugged into MIKEY (and how MIKEY deals with these values internally) to achieve the delivery of the MSK and MTK and how further key-derivations are to be used and proposed that the key derivation functionality of MIKEY (the default PRF) is used in MBMS. A related CR for this was provided in TD S3-040793 which was reviewed and revised in TD S3-040858 with the acceptable changes which was agreed.

TD S3-040815 Initiation of key management in MBMS. This was introduced by Ericsson and shows how key management is initiated based on the information in the Service Announcement. It is important that the correct Service Announcement/ Discovery information is in place. It is proposed to approve the accompanying CR in TD S3-040816 which was reviewed. It was commented that a one-to-many key mapping needs to be possible and it should be checked that this is not precluded by this proposal. It was decided it merge the agreed parts of this CR with the CR in TD S3-040851 (see above).

TD S3-040755 UE handling of MSKs received. This was introduced by Samsung Electronics and proposed some change to the UE handling of received MSKs. A proposed CR was attached which was reviewed. Nokia commented that the BMSC may want to change the key before MSK reaches it's upper limit, e.g. for management reasons. Samsung responded that in this case the operator can set a low upper limit. Other changes were discussed and it was agreed to re-introduce this idea at the next meeting after investigation of the impacts.

TD S3-040805 Parallel use of MSKs and MTKs. This was introduced by Ericsson and concludes that:

- There shall be only one MSK and MTK in use within one Key Group ID. I.e. parallel use of two or more MSKs or MTKs within a Key Group ID shall not be allowed as this will cause synchronization problems in the UE due to the fact that MSK and MTK are identified by sequence numbers
- The use of the same MTK with two different transport services (or user services) should be avoided. This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic, i.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.

A CR implementing this proposal was provided in TD S3-040804 which was reviewed. It was noted that this restricted mapping to a one-to-one relationship for release 6 but was recognised that this may be necessary. It was clarified that the restriction on a single MSK ID was for replay protection and sequence numbering is only one method of achieving this. The note was therfore deleted and the CR revised in TD S3-040859 which was agreed.

TD S3-040814 Proposed CR to 33.246: Clarification of the format of MTK ID and MSK ID (Rel-6). Due to the removal of the requirement for a sequence number in the discussion of TD S3-040804 this was removed from this CR. It was condiered that 2 bytes was adequate for MTK ID and this was reduced to 2 bytes. The CR was revised in TD S3-040860 which was revised in TD S3-040888 and agreed.

TD S3-040744 Proposed CR to 33.246: Clarification on key management. This was introduced by Orange. A comment paper to this was provided in TD S3-040822 which proposed that it is clarified that if UICC Key Mangement is available then MT Key management is not allowed. A clarification table of different cases and their consequences was also included. This was provided to make everyone aware of the consequences of this CR and not against the CR. The was support for the Orange CR in TD S3-040744 which was agreed.

TD S3-040788 Proposed CR to 33.246: Clarifying ME capabilities (Rel-6), This was introduced by 3 on behalf of 3 and Siemens. It was suggested that the VMSC support for GBA_U should be added. The CR was revised in TD S3-040862 which was revised in TD S3-040887 and agreed.

TD S3-040743 Proposed CR to 33.246: Deletion of MBMS keys stored in the ME. This was provided by Orange. Siemens proposed that the mechanism should be similar as for access security keys and the keys stored in non-volatile memory and deleted if a different UICC is inserted on power-up, which was supported by Ericsson and Nokia. TIM and Axalto supported the Orange proposal to remove the keys on power-down. An alternative proposal from Siemens discussed and provided in TD S3-040863 and the basic principles agreed, although the detection of a different UICC and the possibility of multiple USIM applications in a UICC would need further investigation. After investigation, the CR was in TD S3-040863 was reviewed and agreed.

6.21 Key Management of group keys for Voice Group Call Services

TD S3-040703 LS (from GERAN WG2) on 'Ciphering for Voice Group Call Services'. This was introduced by the SA WG3 Chairman and informed SA WG3 that GERAN WG2 were happy with the proposed CR in TD S3-040638. from SA WG3 meeting #34. It was noted that this CR had already been submitted to TSG SA and approved as this response was received before the TSG SA meeting. The LS was then noted.

TD S3-040785 Proposed CR to 43.020: Clarifications to VGCS/VBS ciphering mechanism (Rel-6). This was introduced by Siemens on behalf of Siemens and Vodafone and was reviewed. The CR was revised in TD S3-040872 which was agreed.

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 S3-040737 Selective Disabling of UE Capabilities.. This was introduced by Nokia and was discussed. The contribution was updated with comments received in TD S3-040873 which should be used as a basis for future contributions.

6.24 Other areas

There were no specific contributions under this agenda item.

7 Review and update of work programme

TD S3-040719 New Work Item Form. This was provided for information by the Secretary and members were asked to use this version for any future WIDs they propose. The document was noted.

8 Future meeting dates and venues

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#36	23-26 November 2004	Shenzhen, China	HuaWei Technologies
S3#37	21-25 February 2005	Sophia Antipolis	ETSI
S3#38	25 - 29 April 2005	Switzerland (TBC)	Orange (TBC)
S3#39	TBD	TBD	NAF
S3#40	TBD	TBD	Qualcomm

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#15	11-13 October 2004	USA. Co-located with TR45 LAES	"NA Friends of 3GPP"

TSGs RAN/CN/T and SA Plenary meeting schedule

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

9 Any other business

There were no specific contributions under this agenda item.

10 Close (Friday, 8 October, 4:00 pm at latest)

The Chairman, V. Niemi, thanked delegates for their hard work during the meeting and for the extra hours in the evening sessions which were held. He thanked the Hosts, European Friends of 3GPP, for the facilities in Malta. He then closed the meeting.

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

A.1 List of attendees

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Jorge Abellan Sevilla	Axalto S.A.	jsevilla@axalto.com	+33 6 47 65 06 79	+33 1 46 00 59 33	+33 1 46 00 59 31	FR	ETSI
Dr. Selim Aissi	Intel Corporation SARL	selim.aissi@intel.com		+01-503 264-3349	+01-503 264-1578	FR	ETSI
Mr. SÈbastien Aumonier	Oberthur Card Systems S.A.	s.aumonier@oberthurcs.com		+33 1 41 38 18 78	+33 1 41 38 48 23	FR	ETSI
Mr. George Babut	Rogers Wireless Inc.	gbabut@rci.rogers.com		+1 416 935 6027	+1 416 935 7502	CA	ATIS
Mr. Colin Blanchard	BT Group PLC	colin.blanchard@bt.com	+44 7711 191835	+44 1473 605353	+44 1473 623910	GB	ETSI
Mr. Marc Blommaert	Siemens NV/SA	marc.blommaert@siemens.com		+32 14 25 34 11	+32 14 25 33 39	BE	ETSI
Mr. Holger Butscheidt	Bundesministerium fur Wirtschaft	holger.butscheidt@regtp.de		+49 6131 18 2224	+49 6131 18 5613	DE	ETSI
Mr. Mauro Castagno	Telecom Italia S.P.A.	mauro.castagno@telecomitalia.it		+39 0112285203	+39 0112287056	IT	ETSI
Ms. Lily Chen	Motorola A/S	lchen1@email.mot.com		+1 847 632 3033	+1 847 435 2264	DK	ETSI
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp		+81 467 41 2181	+81 467 41 2185	JP	ARIB
Mr. Per Christoffersson	Teliasonera AB	per.christoffersson@teliasonera.com		+46 705 925100		SE	ETSI
Dr. Hubert Ertl	Giesecke & Devrient GmbH	Hubert.Ertl@de.gi-de.com	+49 172 869 1159	+49 89 4119-2796	+49 89 4119-2921	DE	ETSI
Dr. Adrian Escott	Hutchison 3G UK Ltd (3)	adrian.escott@three.co.uk		+44 7782 325254	+44 1628 766012	GB	ETSI
Mr. 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. Silke Holtmanns	Nokia Corporation	silke.holtmanns@nokia.com		+358 50 4868571	+358 718036139	FI	ETSI
Mr. Guenther Horn	Siemens AG	guenther.horn@siemens.com		+49 8963 641494	+49 8963 648000	DE	ETSI
Mr. Peter Howard	Vodafone Group PLC	peter.howard@vodafone.com	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB	ETSI
Ms. Yingxin Huang	Huawei Technologies Co., Ltd	huangyx@huawei.com		+86-10-82882752	+86-10-82882940	CN	CCSA
Ms. Tiina Koskinen	Nokia Telecommunications Inc.	tiina.s.koskinen@nokia.com		+358504821347	+358718075300	US	ATIS
Mr. Pekka Laitinen	Nokia Corporation	pekka.laitinen@nokia.com		+358 5 0483 7438	+358 7 1803 6852	FI	ETSI
Mr. Bernd Lamparter	NEC Technologies (UK) Ltd	bernd.lamparter@netlab.nec.de		+49 6221 905 11 50	+49 6221 905 11 55	GB	ETSI
Mr. Alex Leadbeater	BT Group Plc	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. Vesa Lehtovirta	Ericsson Incorporated	vesa.lehtovirta@ericsson.com		+358405093314	+	US	ATIS
Mrs. Fei Liu	China Mobile Communications Corporation (CMCC)	liufei@chinamobile.com	+86 13910036595	+86 10 66006688 3118	+86 10 63600340	CN	CCSA
Mr. Michael Marcovici	Lucent Technologies	marcovici@lucent.com		+1 630 979 4062	+1 630 224 9955	US	ATIS
Mr. David Mariblanca	Telefon AB LM Ericsson	david.mariblanca@ericsson.com		+34 646004736	+34 913392538	SE	ETSI
Mr. Anand Palanigounder	Nortel Networks (USA)	anand@nortelnetworks.com		+1 972 684 4772	+1 972 685 3123	US	ATIS
Miss Mireille Pauliac	Gemplus S.A.	mireille.pauliac@gemplus.com		+33 4 42365441	+33 4 42365792	FR	ETSI
Mr. Maurice Pope	ETSI Secretariat	maurice.pope@etsi.org	+33 (0)6 07 59 08 49	+33 4 92 94 42 59	+33 4 92 38 52 59	FR	ETSI
Mr. Rajavelsamy Rajadurai	Samsung Electronics Co., Japan R&D Office	rajvel@samsung.com		+91 08 5119 7777	+91 08 5114 8855	JP	ARIB
Mr. Bengt Sahlin	Ericsson Korea	bengt.sahlin@ericsson.com		+358 40 778 4580	+358 9 299 3401	KR	TTA
Mr. Stefan Schroeder	T-mobile International AG	stefan.schroeder@t-mobile.de		+49 228 9363 3312	+49 228 9363 3309	DE	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
Ms. Annelies Van Moffaert	Alcatel S.A.	annelies.van_moffaert@alcatel.be		+32 3 240 83 58	+32 3 240 48 88	FR	ETSI
Mr. Berthold Wilhelm	Bundesministerium fur Wirtschaft	berthold.wilhelm@regtp.de		+49 681 9330 562	+49 681 9330 725	DE	ETSI
Dr. Raziq Yaqub	Toshiba Corporation, Digital Media Network Company	ryaqub@tari.toshiba.com	+1-908-319-8422	+1 973 829 2103	+1-973-829-5601	JP	ARIB
Mr. Dajiang Zhang	Nokia Japan Co, Ltd	dajiang.zhang@nokia.com		+86-13901168924	+86-010-84210576	JP	ARIB
Mr. Yanmin Zhu	Samsung Electronics Ind. Co., Ltd.	yanmin.zhu@samsung.com		+86-10-68427711	+86-10-68481891	KR	TTA

40 attendees

Apologies for absence were received from the following 2 people:

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
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. Jacques Seif	Axalto S.A.	jseif@axalto.com		+33146007228	+33146005931	FR	ETSI

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #33, #34, and #35, the following companies are eligible to vote at SA WG3 meeting #36:

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

50 Voting Members

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040690	Draft Agenda for SA WG3 meeting #35	SA WG3 Chairman	2	Approval		Approved
S3-040691	Draft Report of SA WG3 meeting #34	SA WG3 Secretary	4.1	Approval		Approved
S3-040692	Report of MBMS joint Ad-hoc meeting	Ad-Hoc Secretary	4.4	Approval		Approved
S3-040693	SA WG3 LI Group CRs (approved by e-mail 02/09/2004)	SA WG3 Secretary	4.3	Information		Noted
S3-040694	Report from SA#25 plenary	SA WG3 Chairman	4.2	Information		Noted
S3-040695	Service discovery using default domain method	Nokia	6.9.2	Discuaaion / Approval		CR revised in S3-040831
S3-040696	Revised WID: Security for early IMS	SA WG3 Secretary	6.1.2	Information		Noted
S3-040697	LS from OMA MMSG: Re: MMS over 3GPP Interworking WLANs	OMA MMSG	5.6	Information		Noted
S3-040698	LS from IETF LEMONADE: LEMONADE for MMS over 3GPP Interworking WLANs	IETF LEMONADE	5.2	Information		Noted
S3-040699	LS (from SA WG2) on mapping tunnels for WLAN 3GPP IP access and W-APNs	SA WG2	6.10	Action		Noted. PH to investigate impacts on CN specs
S3-040700	Reply LS (from SA WG2) on provision of configuration data to a UE	SA WG2	6.1.1	Action		Reply LS in S3-040865
S3-040701	Reply LS (from SA WG2) on Binding Scenario Information to Mutual EAP Authentication	SA WG2	6.10	Action		Noted. Mechanism no longer proposed in S3
S3-040702	LS (from GERAN WG1) on Feasibility Study on Generic Access to A/Gb Interface ñ Security Aspects	GERAN WG1	6.6	Action		Response LS in S3-040878
S3-040703	LS (from GERAN WG2) on 'Ciphering for Voice Group Call Services'	GERAN WG2	6.21	Action		Noted. SA WG3 CR was approved at TSG SA #25
S3-040704	LS (from CN WG4) on SMS Fraud countermeasures	CN WG4	6.2	Action		Response in S3-040870
S3-040705	LS (from CN WG4) on Generic Authentication Architecture (GAA)	CN WG4	6.9.1	Information		Clarifying LS in S3-040827
S3-040706	LS (from CN WG4) on Request for end to end example showing how the Liberty Alliance security framework fits the 3GPP GUP security requirements	CN WG4	6.17	Action		Response LS in S3-040844
S3-040707	LS (from CN WG4) on Evaluation of the alternatives for SMS fraud countermeasures	CN WG4	6.2	Information		Noted. IREG response in S3-040826
S3-040708	LS (from CN WG1) on Re-authentication and key set change during inter-system handover	CN WG1	6.5	Information		Noted
S3-040709	Reply LS (from T WG3) on Storage of temporary identities for EAP authentication	T WG3	6.10	Action		C Blanchard to study need for Rel-6 and Rel-7. Noted
S3-040710	LS (from T WG3) on USAT initiated GBA_U Bootstrap	T WG3	6.9.2	Action		Response LS in S3-040877
S3-040711	LS (from T WG2) on MMS over 3GPP Interworking WLANs	T WG2	6.10	Information		Noted
S3-040712	LS (from T WG2) on Removal of A5/2 Algorithm from Specifications	T WG2	6.6	Action		Noted
S3-040713	LS from T WG2: SMS Fraud countermeasures	T WG2	6.2	Action		Response in S3-040870
S3-040714	LS (from T WG2) on USIM and ISIM selection in the UE	T WG2	6.9.2	Action		LS to S1 in S3-040830
S3-040715	LS(from T WG3) on USIM support by 2G terminals of Rel-99 and Rel-4	T WG3	4.2	Action		Noted
S3-040716	Using PDG certificate in scenario 3	Nokia	6.10	Discussion / Discussion		Related CR in S3-040717
S3-040717	Proposed CR to 33.234: Profile for PDG certificates in Scenario 3 (Rel-6)	Nokia	6.10	Approval		Postponed until next meeting for checks
S3-040718	Report of SA WG3-LI Group meeting - 19-20 July 2004, Povoa de Varzim, Portugal	SA WG3 LI Group Secretary	4.3	Information		Noted
S3-040719	New Work Item Form	MCC	7	Information		Noted
S3-040720	Proposal for an informative Annex to the 3GPP TS 33.203 on support of end user devices behind a NA(P)T firewall and protection of RTP media flows	BT Group plc	6.1.1	Discussion / Decision		Not accepted for Rel-6. Comments to C. Blanchard for development for possible Rel-7 inclusion

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040721	Proposed CR to 33.203: Support of IMS end user devices behind a NA(P)T firewall, and protection of RTP media flows	BT Group plc	6.1.1	Approval		Rejected
S3-040722	Resolving the editors notes in Wireless Local Area Network (WLAN) interworking security 3GPP TS 33.234	BT Group plc	6.10	Discussion / Decision		Agreed to delete editors notes (incl. 5.4). M Pope to provide CR to next meeting
S3-040723	Security context separation	Nokia	6.6	Discussion / Decision		Discussed
S3-040724	Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces) (Rel-6)	Toshiba and supporting companies	6.10	Approval	S3-040838	Revised in S3-040838
S3-040725	Proposed CR to 33.234: Bluetooth security and configuration considerations for Annex A4 of TS 33.234 (Wireless Local Area Network (WLAN) interworking security) (Rel-6)	Toshiba, BT and supporting companies	6.10	Approval		Rejected. To be included in 33.900. LS to Bluetooth in S3-040839
S3-040726	Comments to: Classification of security requirements on local interface	Toshiba	6.10	Discussion / Decision		Noted
S3-040727	Modifying the MAC in AKA	QUALCOMM Europe	6.9.2	Discussion / Decision		Not considered possible for Rel-6. Noted.
S3-040728	An observation about Special RAND in GSM	QUALCOMM Europe, Ericsson	6.6	Discussion / Decision		Presented: To be discussed at next meeting
S3-040729	WITHDRAWN: GUP Security	Lucent Technologies	6.17	Discussion	S3-040845	WITHDRAWN Revised in S3-040845
S3-040730	TR 33.cde V0.0.2: Security Aspects of Early IMS (Release 6)	Lucent Technologies	6.1.2	Discussion / Decision	S3-040820	Revised in S3-040820
S3-040731	Proposed CR to 33.222: GBA supported indication in PSK TLS (Rel-6)	Ericsson, Nokia, Siemens	6.9.4	Approval		Approved
S3-040732	Proposed WID for Trusted Open Platforms in 3G	Intel, T-Mobile, Toshiba, Gemplus, Motorola, RIM, Verisign	6.15	Approval	S3-040843	Revised in S3-040843
S3-040733	The choice of interim solution	Huawei	6.1.2	Discussion / Decision		Also proposal in S3-04073379. Agreed for editor to include in draft TR
S3-040734	Proposed CR to 33.222: Editorial correction of TS 33.222 (Rel-6)	Nokia	6.9.4	Approval		Minor change to be included in further CRs for next meeting
S3-040735	Safety of key material and proposed CR to 33.919	Huawei	6.9.1	Discussion / Decision		Rejected but modified CR added to TS 33.220
S3-040736	Impact analysis -Validity condition set by NAF:Proposed CR to 33.220	Huawei	6.9.2	Discussion / Decision	S3-040828	Revised in S3-040828 to add note on key changes
S3-040737	Selective Disabling of UE Capabilities; updated S3-040682 based on the comments in SA3#34 meeting	Nokia	6.23	Discussion	S3-040873	Updated in S3-040873
S3-040738	Pseudo-CR to Early IMS draft: Removing an editorís note in section 7.2.1	Nokia	6.1.2	Approval		Agreed with mods. Editor asked to include in draft TR
S3-040739	Pseudo-CR to Early IMS draft: Adding advantages of HTTP Digest method to Annex A	Nokia	6.1.2	Approval	S3-040868	Updated with changes of S3-040820 and S3-040846 in S3-040868
S3-040740	Extending NDS/AF for TLS	Nokia	6.4	Discussion		For further study. Comments to Tiina and contributions to next meeting
S3-040741	GBA User Security Settings (GUSS) usage	Nokia, Siemens, Huawei	6.9.2	Discussion / Decision	S3-040832	CR revised in S3-040832
S3-040742	Proposed CR to 33.220: GBA USIM/ISIM selection	Siemens, Nokia	6.9.2	Discussion / Decision		CR approved and attached to S3-040830
S3-040743	Proposed CR to 33.246: Deletion of MBMS keys stored in the ME	Orange	6.20	Approval	S3-040863	Reviewed offline and revised in S3-040863
S3-040744	Proposed CR to 33.246: Clarification on key management	Orange	6.20	Approval		Approved. Comments in S3-040822 noted.

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040745	Key separation mechanism in GSM/GPRS	Orange, Nokia	6.6	Discussion / Decision		Presented: To be discussed at next meeting
S3-040746	Proposed CR to 33.220: Usage control of the service in visited network	Huawei	6.9.2	Approval		Amalgamated CR produced in S3-040832
S3-040747	Control of simultaneous session in scenario 3	Ericsson	6.10	Discussion / Decision		Noted. CR in S3-040748 considered
S3-040748	Proposed CR to 33.234: Control of simultaneous accesses in scenario 3 (Rel-6)	Ericsson	6.10	Approval		Better to address the issue and try to remove complete editors note
S3-040749	Use of MAC addresses	Ericsson	6.10	Discussion / Decision		Related CR in S3-040750
S3-040750	Proposed CR to 33.234: Clarification on the use of MAC addresses (Rel-6)	Ericsson	6.10	Approval		To be revised with editorial changes for next meeting
S3-040751	Proposed CR to 33.234: Sending of W-APN identification (Rel-6)	Ericsson	6.10	Approval	S3-040864	Replaced after discussion in S3-040864
S3-040752	Proposed CR to 33.234: Clean up of not completed chapters (Rel-6)	Ericsson	6.10	Approval	S3-040836	Revised in S3-040836
S3-040753	MKI field transmission method for SRTP packet in MBMS	Samsung Electronics	6.20	Discussion / Decision		Not suitable for Rel-6 as contradicts RFC
S3-040754	Proposed CR to 33.246: Delivery of multiple keys in one MIKEY message for MBMS	Samsung Electronics	6.20	Approval		Rejected due to UICC storage impacts
S3-040755	UE handling of MSKs received	Samsung Electronics	6.20	Discussion / Decision		CR Postponed for further analysis of impacts and update at next meeting
S3-040756	Proposed CR to 33.220: TLS profile for securing Zn' reference point (Rel-6)	Nokia, Siemens	6.9.2	Approval		Approved
S3-040757	WITHDRAWN: Proposed CR to 33.246: Modification of delivery of MIKEY RAND field in MSK updates (Rel-6)	Axalto, Gemplus	6.20	Approval	S3-040833	WITHDRAWN. Corrected version in S3-040833
S3-040758	Poposed CR to 33.234: Alignment of TS 33.234 with SA3 decisions on WLAN UE function split (Rel-6)	Axalto, Gemplus	6.10	Approval	S3-040841	Combined with S3-040759 in S3-040841. T2 reply in S3-040840
S3-040759	Proposed CR to 33.234: Correction of WLAN UE function split (Rel-6)	Axalto, Gemplus	6.10	Approval	S3-040841	Combined with S3-040758 in S3-040841. T2 reply in S3-040840
S3-040760	3GPP UE function split for a 3GPP WLAN user equipment	Axalto, Gemplus	6.10	Discussion / Decision		Related CRs in S3-040758 and S3-040759. LS to T2 in S3-040840
S3-040761	Proposed CR to 33.246: Clean up of MBMS TS (Rel-6)	Ericsson	6.20	Approval	S3-040850	Revised in S3-040850
S3-040762	Revisiting forwards compatibility towards TLS based access security	Ericsson	6.1.1	Discussion / Decision		CR had wrong CR number. CR revised in S3-040866 and LS in S3-040867
S3-040763	Proposed CR to 33.234: Passing keying material to the WLAN-AN during the Fast re-authentication procedure (Rel-6)	Samsung Electronics	6.10	Approval		Approved
S3-040764	Proposed CR to 33.234: Clarification on Deletion of Temporary IDs (Rel-6)	Samsung Electronics	6.10	Approval		Revised in S3-040837
S3-040765	Proposed CR to 33.234: Clarification on Protecting Re-authentication ID in FAST/FULL Re-Authentication procedure (Rel-6)	Samsung Electronics	6.10	Approval		Approved
S3-040766	Proposed CR to 33.234: Assigning Remote IP Address to WLAN UE using IKEv2 configuration Payload (Rel-6)	Samsung Electronics	6.10	Approval		Approved
S3-040767	Proposed CR to 33.234: Tunnel Redirection Procedure (Rel-6)	Samsung Electronics	6.10	Approval		More info on IETF and SA2 work needed
S3-040768	Proposed CR to 33.234: Tunnel Establishment Procedure (Rel-6)	Samsung Electronics	6.10	Approval	S3-040861	Revised in S3-040861
S3-040769	Proposed CR to 33.234: Multiple Tunnels to the same PDG for different W-APN (Rel-6)	Samsung Electronics	6.10	Approval		To be considered for Rel-7 optimisation
S3-040770	Proposed CR to 33.234: Multiple Tunnels establishnemt with different PDG (Rel-6)	Samsung Electronics	6.10	Approval		To be considered for Rel-7 optimisation

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040771	Proposed CR to 33.234: Deletion of inconclusive text on A5/2 countermeasures (Rel-6)	Siemens	6.10	Approval		Approved
S3-040772	Proposed CR to 33.234: Alignment of IPsec profile with RFC2406 (Rel-6)	Siemens	6.10	Approval	S3-040842	Revised in S3-040842
S3-040773	GBA_U: finalisation of GBA_U procedure	Gemplus, Axalto, Oberthur	6.9.2	Discussion / Decision		Used for GBA_U evening discussions
S3-040774	GBA: Support of GBA_U capabilities for Rel-6 Mes	Gemplus, Axalto, Oberthur	6.9.2	Discussion / Decision		dependent on the decision for mandating GBA_U support and may be re-submitted in the next meeting
S3-040775	GBA_U: Alternatives for GBA_U derivations	Gemplus, Axalto, Oberthur	6.9.2	Discussion / Decision		dependent on the decision for mandating GBA_U support and may be re-submitted in the next meeting
S3-040776	Proposed CR to 33.220: Optimization of the GBA_U key derivation procedure (Rel-6)	Gemplus, Axalto, Oberthur	6.9.2	Approval		Used for GBA_U evening discussions
S3-040777	Proposed CR to 33.220: GBA_U: storage of Ks_ext in the UICC (Rel-6)	Gemplus, Axalto, Oberthur	6.9.2	Approval		dependent on the decision for mandating GBA_U support and may be re-submitted in the next meeting
S3-040778	Proposed CR to 33.220: Requirement on ME capabilities for GBA_U (Rel-6)	Gemplus, Axalto, Oberthur	6.9.2	Approval		dependent on the decision for mandating GBA_U support and may be re-submitted in the next meeting
S3-040779	Early-start IMS identification	Siemens	6.1.2	Discussion / Decision		Also proposal in S3-040733. Agreed for editor to include in draft TR
S3-040780	Proposed CR to 33.246: Traffic protection combinations (Rel-6)	Nokia	6.20	Approval	S3-040852	Revised in S3-040852
S3-040781	Extensions to OMA DRM V2.0 DCF for MBMS Download Protection	Nokia	6.20	Discussion / Decision		Further discussion for next meeting
S3-040782	Proposed CR to 33.221: Visited network issuing subscriber certificates (Rel-6)	Nokia	6.9.3	Approval		Approved
S3-040783	Proposed CR to 33.220: Enabling optional GBA_U support for ME (Rel-6)	Nokia, Siemens, Ericsson, Samsung Electronics	6.9.2	Approval		Used for GBA_U evening discussions
S3-040784	Proposed CR to 33.220: Description of UICC-ME interface (Rel-6)	Nokia, Samsung Electronics	6.9.2	Approval		dependent on the decision for mandating GBA_U support and may be re-submitted in the next meeting
S3-040785	Proposed CR to 43.020: Clarifications to VGCS/VBS ciphering mechanism (Rel-6)	Siemens, Vodafone	6.21	Approval	S3-040872	Revised in S3-040872
S3-040786	GUP Security ñ Recommendations for UE implementations	Ericsson, Nokia, Intel	6.17	Discussion / Decision		LS in S3-040844
S3-040787	Proposed Draft LS on GUP Security Recommendations	Ericsson	6.17	Approval	S3-040844	Revised in S3-040844
S3-040788	Proposed CR to 33.246: Clarifying ME capabilities (Rel-6)	3, Siemens	6.20	Approval	S3-040862	Revised in S3-040862
S3-040789	Future of GERAN Security	Ericsson, Qualcomm Europe, Vodafone	6.6	Discussion / Decision		Presented: To be discussed at next meeting
S3-040790	Proposed WID: Access Network Security Enhancements	Ericsson	6.6	Approval		Presented: To be discussed at next meeting
S3-040791	MBMS Comparison of DCF and XML-encryption	Ericsson	6.20	Discussion / Decision		Further discussion for next meeting
S3-040792	MBMS Key derivation chain	Ericsson	6.20	Discussion / Decision		Related CR in S3-040793
S3-040793	Proposed CR to 33.246: MBMS Key processing (Rel-6)	Ericsson	6.20	Approval	S3-040858	Revised in S3-040858
S3-040794	Proposed CR to 33.246: MBMS MTK Download transport (Rel-6)	Ericsson	6.20	Approval	S3-040853	Revised in S3-040853
S3-040795	MBMS download MTK transport	Ericsson	6.20	Discussion / Decision		Accompanying CR in S3-040794

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040796	The need for and use of salt in MBMS streaming	Ericsson	6.20	Discussion / Decision		No justification for additional protection. Rejected
S3-040797	Proposed CR to 33.246: MBMS Transport of salt (Rel-6)	Ericsson	6.20	Approval		Rejected due to rejection of S3-040796
S3-040798	Reliable (S)RTP index synchronization for MBMS streaming	Siemens	6.20	Discussion / Decision	S3-040854	Revised in S3-040854
S3-040799	Proposed CR to 33.246: Clarify the use of mandatory MIKEY features for MBMS (Rel-6)	Siemens	6.20	Approval		Rejected for Rel-6
S3-040800	Proposed CR to 33.246: Adding MIKEY payload type identifiers (Rel-6)	Siemens	6.20	Approval	S3-040857	Revised in S3-040857
S3-040801	Proposed CR to 33.246: Protection of the Gmb reference point (Rel-6)	Siemens	6.20	Approval		Approved
S3-040802	SMS Fraud countermeasure	Siemens	6.2	Discussion / Decision		TCAP Handshake to be studied. Attached to LS to IREG in S3-040871
S3-040803	WITHDRAWN - Comments to TR 43.901	Siemens	6.6	Discussion / Decision		WITHDRAWN
S3-040804	Proposed CR to 33.246: Use of parallel MSKs and MTKs (Rel-6)	Ericsson	6.20	Approval	S3-040859	Revised in S3-040859
S3-040805	Parallel use of MSKs and MTKs	Ericsson	6.20	Discussion / Decision		Accompanying CR in S3-040804
S3-040806	Scope of MBMS security	Ericsson	6.20	Discussion / Decision		Noted. Related CR in S3-040808
S3-040807	Proposed CR to 33.246: Scope of MBMS security (Rel-6)	Ericsson	6.20	Approval	S3-040849	Revised in S3-040849
S3-040808	WITHDRAWN - MBMS security work split	Ericsson	6.20	Discussion / Decision	S3-040847	WITHDRAWN - Replaced by S3-040847
S3-040809	Updated: MBMS Download Protection using XML	Ericsson	6.20	Discussion / Decision		Further discussion for next meeting
S3-040810	Proposed CR to 33.246: XML protection for download services (Rel-6)	Ericsson	6.20	Approval		Re-consider an input for the next meeting, depending on the results of discussions
S3-040811	Enhanced key freshness in GBA	"3"	6.9.2	Discussion / Decision		e-mail discussion encouraged
S3-040812	Proposed CR to 33.203: Editorial corrections (Rel-7)	Vodafone	6.1.1	Approval		Postponed for further editorials as found by next meeting - for Rel-6 before freezing
S3-040813	Relationship between GAA and Liberty	Vodafone	6.9.1	Discussion		E-mail discussion and possible LS at next meeting
S3-040814	Proposed CR to 33.246: Clarification of the format of MTK ID and MSK ID (Rel-6)	Ericsson	6.20	Approval	S3-040860	Revised in S3-040860
S3-040815	Initiation of key management in MBMS	Ericsson	6.20	Discussion / Decision		Proposed CR in S3-040816
S3-040816	Proposed CR to 33.246: Initiation of key management (Rel-6)	Ericsson	6.20	Approval	S3-040851	Merged with S3-040851
S3-040817	IETF work for MIKEY MBMS extensions	Ericsson	6.20	Discussion / Decision		Not agreed. To get official numbers from IETF
S3-040818	Proposed CR to 33.246: MTK update procedure for streaming services (Rel-6)	Ericsson	6.20	Approval	S3-040855	Revised in S3-040855
S3-040819	Proposed CR to 33.246: Clarification of MSK key management (Rel-6)	Ericsson	6.20	Approval	S3-040851	Revised in S3-040851
S3-040820	Pseudo-CR to TR 33.cde V0.0.2: Security Aspects of Early IMS (Release 6)	Lucent Technologies	6.1.2	Discussion / Decision	S3-040868	Updated with changes of S3-040729 and S3-040846 in S3-040868
S3-040821	Comments to S3-040774: GBA: Support of GBA_U capabilities for Rel-6 Mes	Nokia, Siemens, Ericsson	6.9.2	Discussion / Decision	S3-040824	WITHDRAWN - Replaced by S3-040824
S3-040822	Ericssons comments to: Proposed CR to 33.246: Clarification on key management	Ericsson	6.20	Discussion / Decision		Consequences noted. Clarification may be needed in the TS
S3-040823	Nokia, Siemens, Ericsson comments to: GBA_U: finalisation of GBA_U procedure	Nokia, Siemens, Ericsson	6.9.2	Discussion / Decision	S3-040825	WITHDRAWN - Replaced by S3-040825

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040824	Comments to S3-040774: GBA: Support of GBA_U capabilities for Rel-6 Mes	Nokia, Siemens, Ericsson	6.9.2	Discussion / Decision		dependent on the decision for mandating GBA_U support and may be re-submitted in the next meeting
S3-040825	Comments to S3-040773: GBA_U: finalisation of GBA_U procedure	Nokia, Siemens, Ericsson	6.9.2	Discussion / Decision		Used for GBA_U evening discussions
S3-040826	LS from GSMA IREG: Response to LS to 3GPP on Evaluation of the alternatives for SMS fraud countermeasures	GSMA IREG	6.2	Information		response in S3-040871
S3-040827	Reply LS on Generic Authentication Architecture (GAA)	SA WG3	6.9.1	Approval		Approved
S3-040828	Impact analysis -Validity condition set by NAF:Proposed CR to 33.220	Huawei	6.9.2	Approval		Approved
S3-040829	LS response to SA3 regarding Security of the Management Plane	SA WG5	5.1	Action		C Blanchard to study TS and collect comments for next meeting
S3-040830	LS on USIM and ISIM selection in the UE	SA WG3	6.9.2	Approval		Approved
S3-040831	CR to 33.220	Nokia	6.9.2	Approval		Approved
S3-040832	CR to 33.220: GBA User Security Settings (GUSS) usage	Nokia, Siemens, Huawei	6.9.2	Approval		Approved
S3-040833	Proposed CR to 33.246: Modification of delivery of MIKEY RAND field in MSK updates (Rel-6)	Axalto, Gemplus	6.20	Approval	S3-040856	Revised in S3-040856
S3-040834	LS on Generic Access to A/Gb Interface ñ Security Aspects	SA WG3	6.6	Approval	S3-040878	Revised in S3-040878
S3-040835	Draft Reply LS on USAT initiated GBA_U Bootstrap	SA WG3	6.9.2	Approval	S3-040877	Revised in S3-040877
S3-040836	Proposed CR to 33.234: Clean up of not completed chapters (Rel-6)	Ericsson	6.10	Approval	S3-040886	Revised in S3-040886
S3-040837	Proposed CR to 33.234: Clarification on Deletion of Temporary IDs (Rel-6)	Samsung Electronics	6.10	Approval		Approved
S3-040838	Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces) (Rel-6)	Toshiba and supporting companies	6.10	Approval		Approved
S3-040839	LS to Bluetooth: Requirements To be Realized in SAP (SIM Access Profile) when Bluetooth is used as Local Interface for Authentication of Peripheral Devices	SA WG3	6.10	Approval	S3-040874	Revised in S3-040874
S3-040840	Draft LS on EAP Authentication commands for WLAN interworking	SA WG3	6.10	Approval	S3-040876	Revised in S3-040876
S3-040841	Proposed CR to 33.234: Correction of WLAN UE function split	Axalto, Gemplus	6.10	Approval	S3-040875	Revised in S3-040875
S3-040842	Proposed CR to 33.234: Alignment of IPsec profile with RFC2406 (Rel-6)	Siemens	6.10	Approval		Approved
S3-040843	Proposed WID for Security Requirement for Open Platforms in 3GPP	Intel, T-Mobile, Toshiba, Gemplus, Motorola, RIM, Verisign	6.15	Approval		Approved
S3-040844	Proposed Draft LS on GUP Security Recommendations	SA WG3	6.17	Approval	S3-040885	Revised in S3-040885
S3-040845	GUP Security	Lucent Technologies	6.17	Discussion		LS in S3-040844
S3-040846	PCR to Early IMS TR	Vodafone	6.1.2	Approval	S3-040868	Updated with changes of S3-040729 and S3-040820 in S3-040868
S3-040847	MBMS security work split	Ericsson	6.20	Discussion / Decision		LS in S3-040884 to attach this main contribution
S3-040848	Draft LS on MBMS Security finalisation	SA WG3	6.20	Approval	S3-040884	revised in S3-040884
S3-040849	Proposed CR to 33.246: Scope of MBMS security (Rel-6)	SA WG3	6.20	Approval		Approved
S3-040850	Proposed CR to 33.246: Clean up of MBMS TS (Rel-6)	Ericsson	6.20	Approval		Approved
S3-040851	Proposed CR to 33.246: Clarification of MSK key management (Rel-6)	Ericsson	6.20	Approval	S3-040889	revised in S3-040889
S3-040852	Proposed CR to 33.246: Traffic protection combinations (Rel-6)	SA WG3	6.20	Approval		Approved
S3-040853	Proposed CR to 33.246: MBMS MTK Download transport (Rel-6)	Ericsson	6.20	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040854	Reliable (S)RTP index synchronization for MBMS streaming	Siemens	6.20	Discussion / Decision		Approved
S3-040855	Proposed CR to 33.246: Clarification of MSK key management (Rel-6)	Ericsson	6.20	Approval		Approved
S3-040856	Proposed CR to 33.246: Modification of delivery of MIKEY RAND field in MSK updates (Rel-6)	Axalto, Gemplus	6.20	Approval		Approved
S3-040857	Proposed CR to 33.246: Adding MIKEY payload type identifiers (Rel-6)	Siemens	6.20	Approval		Approved
S3-040858	Proposed CR to 33.246: MBMS Key processing (Rel-6)	Ericsson	6.20	Approval		Approved
S3-040859	Proposed CR to 33.246: Use of parallel MSKs and MTKs (Rel-6)	Ericsson	6.20	Approval		Approved
S3-040860	Proposed CR to 33.246: Clarification of the format of MTK ID and MSK ID (Rel-6)	Ericsson	6.20	Approval	S3-040888	revised in S3-040888
S3-040861	Proposed CR to 33.234: Tunnel Establishment Procedure (Rel-6)	Samsung Electronics	6.10	Approval		Approved
S3-040862	Proposed CR to 33.246: Clarifying ME capabilities (Rel-6)	3, Siemens	6.20	Approval	S3-040887	revised in S3-040887
S3-040863	Proposed CR to 33.246: Deletion of MBMS keys stored in the ME	SA WG3	6.20	Approval		Approved
S3-040864	Proposed CR to 33.234: Sending of W-APN identification (Rel-6)	Ericsson	6.10	Approval		Approved
S3-040865	Draft LS on provision of configuration data to a UE	SA WG3	6.1.1	Approval	S3-040881	revised in S3-040881
S3-040866	Proposed CR to 33.203: Forwards compatibility to TLS based access security	Ericsson	6.1.1	Approval		Postponed for SA1 and SA2 discussion with LS in S3-040867
S3-040867	LS on Revisiting forwards compatibility towards TLS based access security	SA WG3	6.1.1	Approval	S3-040882	revised in S3-040882
S3-040868	New version of TR 33.878	Vodafone	6.1.2	Approval	S3-040879	revised in S3-040879
S3-040869	LS To: CN WG1, CN WG4, CC: SA WG2 on Security aspects of early IMS systems	SA WG3	6.1.2	Approval	S3-040880	revised in S3-040880
S3-040870	Reply LS To: CN4, CC: T2 on SMS Fraud countermeasures	SA WG3	6.2	Approval		Approved
S3-040871	Draft Reply LS on Evaluation of the alternatives for SMS fraud countermeasures	SA WG3	6.2	Approval	S3-040883	revised in S3-040883
S3-040872	Proposed CR to 43.020: Clarifications to VGCS/VBS ciphering mechanism (Rel-6)	Siemens, Vodafone	6.21	Approval		Approved
S3-040873	Selective Disabling of UE Capabilities; updated S3-040682 based on the comments in SA3#34 meeting	Nokia	6.23	Discussion		Noted. To be used as basis for CR
S3-040874	LS to Bluetooth: Requirements To be Realized in SAP (SIM Access Profile) when Bluetooth is used as Local Interface for Authentication of Peripheral Devices	SA WG3	6.10	Approval		Approved
S3-040875	CR to 33.234: Correction of WLAN UE function split (Rel-6)	SA WG3	6.10	Approval		Approved
S3-040876	LS on EAP Authentication commands for WLAN interworking	SA WG3	6.10	Approval		Approved
S3-040877	Reply LS on USAT initiated GBA_U Bootstrap	SA WG3	6.9.2	Approval		Approved
S3-040878	LS on Generic Access to A/Gb Interface ñ Security Aspects	SA WG3	6.6	Approval		Approved
S3-040879	New version of TR 33.878	Vodafone	6.1.2	Approval		Approved
S3-040880	LS To: CN WG1, CN WG4, CC: SA WG2 on Security aspects of early IMS systems	SA WG3	6.1.2	Approval		Approved
S3-040881	LS on provision of configuration data to a UE	SA WG3	6.1.1	Approval		Approved
S3-040882	LS on Revisiting forwards compatibility towards TLS based access security	SA WG3	6.1.1	Approval		Approved
S3-040883	Reply LS on Evaluation of the alternatives for SMS fraud countermeasures	SA WG3	6.2	Approval		Approved
S3-040884	LS on MBMS Security finalisation	SA WG3	6.20	Approval		Approved
S3-040885	LS on GUP Security Recommendations	SA WG3	6.17	Approval		Approved
S3-040886	Proposed CR to 33.234: Clean up of not completed chapters (Rel-6)	Ericsson	6.10	Approval		Approved
S3-040887	Proposed CR to 33.246: Clarifying ME capabilities (Rel-6)	3, Siemens	6.20	Approval		Approved
S3-040888	Proposed CR to 33.246: Clarification of the format of MTK ID and MSK ID (Rel-6)	Ericsson	6.20	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040889	Proposed CR to 33.246: Clarification of MSK key management (Rel-6)	Ericsson	6.20	Approval		Approved

Annex C: Status of specifications under SA WG3 responsibility

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
Release 1999 GSM Specifications and Reports							
TR	01.31	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	8.0.0	R99	S3	WRIGHT, Tim	.
TR	01.33	Lawful Interception requirements for GSM	8.0.0	R99	S3	MCKIBBEN, Bernie	.
TS	01.61	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	8.0.0	R99	S3	WALKER, Michael	.
TS	02.09	Security aspects	8.0.1	R99	S3	CHRISTOFFERSSON, Per	.
TS	02.33	Lawful Interception (LI); Stage 1	8.0.1	R99	S3	MCKIBBEN, Bernie	.
TS	03.20	Security-related Network Functions	8.1.0	R99	S3	NGUYEN NGOC, Sebastien	
TS	03.33	Lawful Interception; Stage 2	8.1.0	R99	S3	MCKIBBEN, Bernie	TSG#10:8.1.0
Release 1999 3GPP Specifications and Reports							
TS	21.133	3G security; Security threats and requirements	3.2.0	R99	S3	CHRISTOFFERSSON, Per	.
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	3.2.1	R99	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	3.0.0	R99	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031. Created from 02.31 R99.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	3.0.0	R99	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards). SP-16: Takes over from 02.32 R99.
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	3.0.0	R99	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031. Created from 03.31 R99.
TS	23.035	Immediate Service Termination (IST); Stage 2	3.1.0	R99	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards). SP-16: takes over from 03,35 R99.
TS	33.102	3G security; Security architecture	3.13.0	R99	S3	BLOMMAERT, Marc	
TS	33.103	3G security; Integration guidelines	3.7.0	R99	S3	BLANCHARD, Colin	
TS	33.105	Cryptographic algorithm requirements	3.8.0	R99	S3	CHIKAZAWA, Takeshi	
TS	33.106	Lawful interception requirements	3.1.0	R99	S3	WILHELM, Berthold	.
TS	33.107	3G security; Lawful interception architecture and functions	3.5.0	R99	S3	WILHELM, Berthold	
TS	33.120	Security Objectives and Principles	3.0.0	R99	S3	WRIGHT, Tim	.
TR	33.901	Criteria for cryptographic Algorithm design process	3.0.0	R99	S3	BLOM, Rolf	.
TR	33.902	Formal Analysis of the 3G Authentication Protocol	3.1.0	R99	S3	HORN, Guenther	.
TR	33.908	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	3.0.0	R99	S3	WALKER, Michael	TSG#7: S3-000105=NP-000049 Formerly 33.904.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	3.2.0	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
Release 4 3GPP Specifications and Reports							
TS	21.133	3G security; Security threats and requirements	4.1.0	Rel-4	S3	CHRISTOFFERSSON, Per	
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	4.1.0	Rel-4	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031. Created from 42.031 Rel-4.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards). SP-16: Takes over from 42.032 Rel-4.
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031. Created from 43.031 Rel-4.
TS	23.035	Immediate Service Termination (IST); Stage 2	4.1.0	Rel-4	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards). SP-16: takes over from 43.035 Rel-4
TS	33.102	3G security; Security architecture	4.5.0	Rel-4	S3	BLOMMAERT, Marc	
TS	33.103	3G security; Integration guidelines	4.2.0	Rel-4	S3	BLANCHARD, Colin	SP-15: Not to be promoted to Rel-5.
TS	33.105	Cryptographic algorithm requirements	4.2.0	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	2001-05-24: title grows MAP; see 33.210 for IP equivalent.
TR	33.901	Criteria for cryptographic Algorithm design process	4.0.0	Rel-4	S3	BLOM, Rolf	SP-15: Not to be promoted to Rel-5.
TR	33.902	Formal Analysis of the 3G Authentication Protocol	4.0.0	Rel-4	S3	HORN, Guenther	SP-15: Not to be promoted to Rel-5.
TR	33.908	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	4.0.0	Rel-4	S3	WALKER, Michael	TSG#7: S3-000105=NP-000049 SP-15: Not to be promoted to Rel-5.
TR	33.903	Access Security for IP based services	none	Rel-4	S3	VACANT,	.
TR	33.909	3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions	4.0.1	Rel-4	S3	WALKER, Michael	TSG#7: Is a reference in 33.908. Was withdrawn, but reinstated at TSG#10. SP-15: Not to be promoted to Rel-5.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	4.1.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.205	3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE. 2002-06: clarified that deliverable is TS not TR. TSG#11:changed to Rel-4.
TS	35.206	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:changed to Rel-4
TS	35.207	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementorsí test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:changed to Rel-4

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:changed to Rel-4
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:Formerly 35.209 Rel-99 (but never made available)
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	4.0.1	Rel-4	S3	WRIGHT, Tim	
TR	41.033	Lawful Interception requirements for GSM	4.0.1	Rel-4	S3	MCKIBBEN, Bernie	
TS	41.061	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	4.0.0	Rel-4	S3	WALKER, Michael	SP-15: Not to be promoted to Rel-5.
TS	42.009	Security Aspects	4.0.0	Rel-4	S3	CHRISTOFFERSSON, Per	SP-15: Not to be promoted to Rel-5.
TS	42.033	Lawful Interception; Stage 1	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
TS	43.020	Security-related network functions	4.0.0	Rel-4	S3	GILBERT, Henri	
TS	43.033	Lawful Interception; Stage 2	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
Release 5 3GPP Specifications and Reports							
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	5.0.0	Rel-5	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4 .
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031. Created from 42.031 Rel-5.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards). .
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031. Created from 43.031 Rel-5.
TS	23.035	Immediate Service Termination (IST); Stage 2	5.1.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards). .
TS	33.102	3G security; Security architecture	5.5.0	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)	5.8.0	Rel-5	S3	WILHELM, Berthold	2001-12-04 Title changed from "Lawful Interception; Interface between core network and law agency equipment" (Berthold.Wilhelm@RegTP.de). .
TS	33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	5.1.0	Rel-5	S3	ESCOTT, Adrian	2001-05-24: title grows MAP; see 33.210 for IP equivalent. .
TS	33.203	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	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210).
TR	33.900	Guide to 3G security	0.4.1	Rel-5	S3	BROOKSON, Charles	.
TR	33.903	Access Security for IP based services	none	Rel-5	S3	VACANT,	.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.205	3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE. 2002-06: clarified that deliverable is TS not TR. .
TS	35.206	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification	5.1.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TS	35.207	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementorsí test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	5.0.0	Rel-5	S3	WRIGHT, Tim	.
TR	41.033	Lawful Interception requirements for GSM	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
TS	42.033	Lawful Interception; Stage 1	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
TS	43.020	Security-related network functions	5.0.0	Rel-5	S3	GILBERT, Henri	.
TS	43.033	Lawful Interception; Stage 2	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
Release 6 3GPP Specifications and Reports							
TS	33.102	3G security; Security architecture	6.2.0	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	6.3.0	Rel-6	S3	WILHELM, Berthold	.
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	6.7.0	Rel-6	S3	WILHELM, Berthold	2001-12-04 Title changed from "Lawful Interception; Interface between core network and law agency equipment" (Berthold.Wilhelm@RegTP.de). .
TS	33.141	Presence service; Security	6.1.0	Rel-6	S3	BOMAN, Krister	.
TS	33.203	3G security; Access security for IP-based services	6.4.0	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	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210). .
TS	33.220	Generic Authentication Architecture (GAA); Generic bootstrapping architecture	6.2.0	Rel-6	S3	HAUKKA, Tao	WI = SEC1-SC (UID 33002) Based on 33.109 ß4. .
TS	33.221	Generic Authentication Architecture (GAA); Support for subscriber certificates	6.1.0	Rel-6	S3	HAUKKA, Tao	WI = SEC1-SC (UID 33002) Based on 33.109 ß5 & annex A. .
TS	33.222	Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)	6.1.0	Rel-6	S3	SAHLIN, Bengt	WI = SEC1-SC (UID 33002) Based on 33.109 v0.3.0 protocol B. .

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	33.234	3G security; Wireless Local Area Network (WLAN) interworking security	6.2.1	Rel-6	S3	LOPEZ SORIA, Luis	.
TS	33.246	3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)	6.0.0	Rel-6	S3	ESCOTT, Adrian	SP-25: Approved
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	2002-07-22: was formerly 33.910. SP-17: expect v2.0.0 at SP-18.
TR	33.817	Feasibility study on (Universal) Subscriber Interface Module (U)SIM security reuse by peripheral devices on local interfaces	6.0.0	Rel-6	S3	YAQUB, Raziq	Original WID = SP-030341. 2003-11-26: S3 Secretary indicates that TR is to be internal, so number changed from 33.917. .
TR	33.919	3G Security; Generic Authentication Architecture (GAA); System Description	6.0.0	Rel-6	S3	VAN MOFFAERT, Annelies	WI = SEC1-SC (UID 33002) . SP-25: Approved
TR	43.020	3G Security; Security-related network functions	6.0.0	Rel-6	S3	GILBERT, Henri	Approved TSG SA #25
TS	55.205	Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8	6.1.0	Rel-6	S3	WALKER, Michael	Not subject to export control. .
TS	55.216	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 1: A5/3 and GEA3 specification	6.2.0	Rel-6	S3	N, A	2003-09-30: Note: document only available with French export licence. .
TS	55.217	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data	6.1.0	Rel-6	S3	N, A	2003-09-30: Note: document only available with French export licence. .
TS	55.218	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 3: Design and conformance test data	6.1.0	Rel-6	S3	N, A	2003-09-30: Note: document only available with French export licence. .
TR	55.919	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report	6.1.0	Rel-6	S3	N, A	2003-09-30: Note: document only available with French export licence. .
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 this meeting

Note: Some of the agreed CRs were revised again at meeting #36. The report of SA WG3 meeting #36 provides the definitive list of CRs agreed at meetings #35 and #36.

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WI
33.220	018	1	Rel-6	BSF discovery using default domain method	C	6.2.0	S3-35	S3-040831	SEC1-SC
33.220	019	1	Rel-6	Local validity condition set by NAF	F	6.2.0	S3-35	S3-040828	SEC1-SC
33.220	020	1	Rel-6	GBA User Security Settings (GUSS) usage in GAA	C	6.2.0	S3-35	S3-040832	SEC1-SC
33.220	021	-	Rel-6	Details of USIM/ISIM selection in GAA	C	6.2.0	S3-35	S3-040742	SEC1-SC
33.220	023	-	Rel-6	TLS profile for securing Zn' reference point	C	6.2.0	S3-35	S3-040756	SEC1-SC
33.221	005	-	Rel-6	Visited network issuing subscriber certificates	B	6.1.0	S3-35	S3-040782	SEC1-SC
33.222	005	-	Rel-6	GBA supported indication in PSK TLS	C	6.1.0	S3-35	S3-040731	SEC1-SC
33.234	020	1	Rel-6	Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces)	B	6.2.1	S3-35	S3-040838	WLAN
33.234	024	1	Rel-6	Sending of W-APN identification	B	6.2.1	S3-35	S3-040864	WLAN
33.234	025	2	Rel-6	Clean up of not completed chapters	F	6.2.1	S3-35	S3-040886	WLAN
33.234	027	2	Rel-6	Correction of WLAN UE function split	F	6.2.1	S3-35	S3-040875	WLAN
33.234	028	-	Rel-6	Passing keying material to the WLAN-AN during the Fast re-authentication procedure	F	6.2.1	S3-35	S3-040763	WLAN
33.234	029	1	Rel-6	Clarification on Deletion of Temporary IDs	F	6.2.1	S3-35	S3-040837	WLAN
33.234	030	-	Rel-6	Clarification on Protecting Re-authentication ID in FAST/FULL Re-Authentication procedure	F	6.2.1	S3-35	S3-040765	WLAN
33.234	031	-	Rel-6	Assigning Remote IP Address to WLAN UE using IKEv2 configuration Payload	B	6.2.1	S3-35	S3-040766	WLAN
33.234	033	1	Rel-6	Tunnel Establishment Procedure	F	6.2.1	S3-35	S3-040861	WLAN
33.234	036	-	Rel-6	Deletion of inconclusive text on A5/2 countermeasures	F	6.2.1	S3-35	S3-040771	WLAN
33.234	037	1	Rel-6	Alignment of IPsec profile with RFC2406	F	6.2.1	S3-35	S3-040842	WLAN
33.246	001	2	Rel-6	Deletion of MBMS keys stored in the ME	F	6.0.0	S3-35	S3-040863	MBMS
33.246	002	-	Rel-6	Clarification on key management	C	6.0.0	S3-35	S3-040744	MBMS
33.246	005	1	Rel-6	Clean up of MBMS TS	D	6.0.0	S3-35	S3-040850	MBMS
33.246	006	1	Rel-6	Traffic protection combinations	F	6.0.0	S3-35	S3-040852	MBMS
33.246	007	2	Rel-6	Clarifying ME and BM-SC capabilities	F	6.0.0	S3-35	S3-040887	MBMS
33.246	008	1	Rel-6	MBMS Key processing	C	6.0.0	S3-35	S3-040858	MBMS
33.246	009	1	Rel-6	MBMS MTK Download transport	C	6.0.0	S3-35	S3-040853	MBMS
33.246	011	1	Rel-6	SRTP index synchronisation within ME	C	6.0.0	S3-35	S3-040854	MBMS
33.246	013	1	Rel-6	Adding MIKEY payload type identifiers	F	6.0.0	S3-35	S3-040857	MBMS
33.246	014	-	Rel-6	Protection of the Gmb reference point	C	6.0.0	S3-35	S3-040801	MBMS
33.246	015	1	Rel-6	Use of parallel MSKs and MTKs	C	6.0.0	S3-35	S3-040859	MBMS
33.246	016	1	Rel-6	Scope of MBMS security	C	6.0.0	S3-35	S3-040849	MBMS
33.246	018	2	Rel-6	Clarification of the format of MTK ID and MSK ID	C	6.0.0	S3-35	S3-040888	MBMS
33.246	020	1	Rel-6	MTK update procedure for streaming services	B	6.0.0	S3-35	S3-040855	MBMS
33.246	021	2	Rel-6	Clarification of MSK key management	C	6.0.0	S3-35	S3-040889	MBMS
33.246	022	1	Rel-6	Modification of delivery of MIKEY RAND field in MSK updates	C	6.0.0	S3-35	S3-040856	MBMS
43.020	002	1	Rel-6	Clarifications to VGCS/VBS ciphering mechanism	F	6.0.0	S3-35	S3-040872	SECGKYV

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	From	Source TD	Comment/Status
S3-040697	LS from OMA MMSG: Re: MMS over 3GPP Interworking WLANs	OMA MMSG	OMA-MWG-2004-0110R01	Noted
S3-040698	LS from IETF LEMONADE: LEMONADE for MMS over 3GPP Interworking WLANs	IETF LEMONADE		Noted
S3-040699	LS (from SA WG2) on mapping tunnels for WLAN 3GPP IP access and W-APNs	SA WG2	S2-042887	Noted. PH to investigate impacts on CN specs
S3-040700	Reply LS (from SA WG2) on provision of configuration data to a UE	SA WG2	S2-042974	Reply LS in S3-040865
S3-040701	Reply LS (from SA WG2) on Binding Scenario Information to Mutual EAP Authentication	SA WG2	S2-042951	Noted. Mechanism no longer proposed in S3
S3-040702	LS (from GERAN WG1) on Feasibility Study on Generic Access to A/Gb Interface ñ Security Aspects	GERAN WG1	GP-042291	Response LS in S3-040878
S3-040703	LS (from GERAN WG2) on 'Ciphering for Voice Group Call Services'	GERAN WG2	GP-042284	Noted. SA WG3 CR was approved at TSG SA #25
S3-040704	LS (from CN WG4) on SMS Fraud countermeasures	CN WG4	N4-041193	Response in S3-040870
S3-040705	LS (from CN WG4) on Generic Authentication Architecture (GAA)	CN WG4	N4-041166	Clarifying LS in S3-040827
S3-040706	LS (from CN WG4) on Request for end to end example showing how the Liberty Alliance security framework fits the 3GPP GUP security requirements	CN WG4	N4-041202	Response LS in S3-040844
S3-040707	LS (from CN WG4) on Evaluation of the alternatives for SMS fraud countermeasures	CN WG4	N4-041204	Noted. IREG response in S3-040826
S3-040708	LS (from CN WG1) on Re-authentication and key set change during inter-system handover	CN WG1	N1-041519	Noted
S3-040709	Reply LS (from T WG3) on Storage of temporary identities for EAP authentication	T WG3	T3-040518	C Blanchard to study need for Rel-6 and Rel-7. Noted
S3-040710	LS (from T WG3) on USAT initiated GBA_U Bootstrap	T WG3	T3-040562	Response LS in S3-040877
S3-040711	LS (from T WG2) on MMS over 3GPP Interworking WLANs	T WG2	T2-040315	Noted
S3-040712	LS (from T WG2) on Removal of A5/2 Algorithm from Specifications	T WG2	T2-040326	Noted
S3-040713	LS from T WG2: SMS Fraud countermeasures	T WG2	T2-040329	Response in S3-040870
S3-040714	LS (from T WG2) on USIM and ISIM selection in the UE	T WG2	T2-040349	LS to S1 in S3-040830
S3-040715	LS(from T WG3) on USIM support by 2G terminals of Rel-99 and Rel-4	T WG3	T3-040531	Noted
S3-040826	LS from GSMA IREG: Response to LS to 3GPP on Evaluation of the alternatives for SMS fraud countermeasures	GSMA IREG	IREG Doc 47_056 Rev 1	response in S3-040871
S3-040829	LS response to SA3 regarding Security of the Management Plane	SA WG5	S5-046988	C Blanchard to study TS and collect comments for next meeting

E.2 Liaisons from the meeting

TD number	Title	TO	CC
S3-040827	Reply LS on Generic Authentication Architecture (GAA)	**SA WG2, CN WG4**	**-**
S3-040830	LS on USIM and ISIM selection in the UE	**SA WG1**	**SA WG2, T WG2, T WG3**
S3-040870	Reply LS To: CN4, CC: T2 on SMS Fraud countermeasures	**CN WG4**	**T WG2**
S3-040874	LS to Bluetooth: Requirements To be Realized in SAP (SIM Access Profile) when Bluetooth is used as Local Interface for Authentication of Peripheral Devices	**Bluetooth BARB, Bluetooth CAR, Bluetooth SEG**	**-**
S3-040876	LS on EAP Authentication commands for WLAN interworking	**T WG2**	**T WG3**
S3-040877	Reply LS on USAT initiated GBA_U Bootstrap	**T WG3**	**-**
S3-040878	LS on Generic Access to A/Gb Interface ñ Security Aspects	**GERAN WG1**	**SA WG1, SA WG2**
S3-040880	LS To: CN WG1, CN WG4, CC: SA WG2 on Security aspects of early IMS systems	**CN WG1, CN WG4, SA WG2**	**T WG2**
S3-040881	LS on provision of configuration data to a UE	**CN WG1,**	**SA WG2**
S3-040882	LS on Revisiting forwards compatibility towards TLS based access security	**SA WG2, SA WG1**	**CN WG1, CN WG4**
S3-040883	Reply LS on Evaluation of the alternatives for SMS fraud countermeasures	**GSMA IREG**	**CN WG4, GSMA SG**
S3-040884	LS on MBMS Security finalisation	**CN WG1, SA WG4**	**-**
S3-040885	LS on GUP Security Recommendations	**CN WG4, SA WG2**	**-**

Annex F: Actions from the meeting

AP 35/01: Silke Holtmanns to chair an e-mail discussion on Liberty Alliance work and 3GPP GAA work and to prepare an LS for the next meeting if appropriate.

AP 35/02: Peter Howard agreed to investigate the current status in CN specifications of restricting simultaneous PDP contexts in the Network side (Ref: LS from SA WG2 in TD S3-040699).

AP 35/03: Toshiba to create an update to TR 33.900 including agreements and provide to next meeting.

AP 35/04: M. Pope to create CR to 33.234 removing editors notes as defined in TD S3-040722.

3GPP TSG SA WG3 (Security) meeting #36 **Draft Report**

23-26 November 2004

Shenzhen, China

Source:	**Secretary of 3GPP TSG-SA WG3**
Title:	**Draft Report of SA3 meeting #36**
Document for:	**Approval**
Status:	**Draft version 0.0.5 including comments (with revision marks)**

MING WAH International Conference Centre, Shenzhen, China

Service at the social Event, Organised by Hauwei

Contents

1 Opening of the meeting

The SA WG3 Chairman, Mr. V. Niemi opened the meeting and Huawei, the meeting hosts, welcomed delegates to the meeting and provided the domestic arrangements and wished the delegates a successful meeting in Shenzhen, China.

2 Agreement of the agenda and meeting objectives

TD S3-040890 Draft Agenda for SA WG3 meeting #36. This was introduced by the SA WG3 Chairman and was reviewed. The objectives for the meeting were also introduced as follows:

- *The major objective of this meeting is still to develop further those three TSs for which functional changes may need to be agreed: 33.220 (GBA), 33.234 (I-WLAN), 33.246 (MBMS)*
- *We also try to close remaining open issues and get rid of editorís notes in the other release 6 TSs and TRs. After the December SA plenary it is going to be significantly harder to get any CRís accepted.*

The preliminary schedule was also introduced.

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

TD S3-040892 Specs lists per Release; a comparison. This was introduced by the SA WG3 Chairman and was received from the MCC Specifications manager and asked WGs to indicate if there are any specification to be upgraded to Rel-6 when the Release is frozen which should not be automatically upgraded.

Delegates were asked to review the specifications lists for SA WG3. There were no comments received in the meeting, and **the lists for automatic upgrade as proposed by the MCC Specifications manager was therefore considered acceptable**.

4.1 Approval of the report of SA3#35, St. Paulís Bay, Malta, 5-8 October, 2004

TD S3-040891 Draft Report of SA WG3 meeting #35. The draft report was reviewed and approved. The approved version 1.0.0 (with revision marks accepted) will be placed on the 3GPP FTP server after the meeting. The Actions from the previous meeting were then reviewed:

AP 35/01: Silke Holtmanns to chair an e-mail discussion on Liberty Alliance work and 3GPP GAA work and to prepare an LS for the next meeting if appropriate. No feedback was received to e-mail discussion, so no LS was prepared. Input to this meeting was provided in TD S3-040980. Completed.

AP 35/02: Peter Howard agreed to investigate the current status in CN specifications of restricting simultaneous PDP contexts in the Network side (Ref: LS from SA WG2 in TD S3 040699). Completed and reported on e-mail list.

AP 35/03: Toshiba to create an update to TR 33.900 including agreements and provide to next meeting. Completed. Contribution provided to this meeting in TD S3-040906.

AP 35/04: M. Pope to create CR to 33.234 removing editors notes as defined in TD S3-040722. This CR was produced during the meeting (TD S3-0401139). Completed.

4.2 Report from SA3-LI#4/2004, San Antonio, Texas, USA, 11-13 October, 2004

TD S3-040912 . This was introduced by B. Wilhelm and provided the summary of the last SA WG3 LI Group meeting. Resultant agreed CRs were provided in TD S3-040913 which should normally be approved by e-mail by SA WG3. It was decided to check these at the meeting to see if they can be agreed because the TSG SA meeting is soon. Comments to be made until 30 November 2004. If no comments the CRs will be assumed to be approved.

Secretary's note: No comments were received by 30 November, so these CRs were approved.

5 Reports and Liaisons from other groups

5.1 3GPP working groups

There were no specific contributions under this agenda item. LSs from other WGs were allocated to their relevant agenda items.

5.2 IETF

TD S3-040989 IETF status report on HTTP Digest AKAv2. This was introduced by Ericsson and was provided for information and was noted.

It was reported that a contribution discussing the MBMS draft will be provided by Ericsson, and no specific issues were identified at this time. This was provided in TD S3-040995 and discussed under the MBMS agenda item. It was agreed that the IETF internet draft:

"The Key ID Information Type for the General Extension Payload in MIKEYî <draft-carrara-newtype-keyid-00.txt>, October 2004

should be added to the list of IETF dependencies.

5.3 ETSI SAGE

Per reported that the new Algorithms work has started and a WID is provided for SA WG3 to include this in the 3GPP Work Plan in TD S3-0401051.

5.4 GSMA

Charles Brookson presented some of the current work within the GSM Association:

- The CEO Board had approved the removal of the A5/2 from the infrastructure equipment. A meeting will be held on 16th December in London on the issue, and to discuss future work required. Please contact him if you are interested in attending.
- Funding had been provided to SAGE for the new UMTS algorithm.
- The Central Equipment Identity Register, used for barring stolen mobiles, is due to be upgraded. Resources have been made available. Stolen mobiles are proving to be a big issue worldwide.

Work was continuing in the areas of GPRS and 3G network security, handset security (smart phones are increasingly causing new security issues), and a new work plan is existence for next year.

5.5 3GPP2

M. Marcovici reported that WLAN CDMA2000 interworking was almost complete. There were no other issues of importance to SA WG3.

5.6 OMA

M. Marcovici reported as follows:

OMA-SEC met in Barcelona during the week of 15th of November, 2004. A number of major issues have been addressed during the meeting (a) "Location Services Security (SUPL)" - what are the advantages/disadvantages of using only TLS 1.0 vs. using PSK TLS (evaluation still in progress), (b) "Security Common Functions Enablers for OMA" - work in preliminary requirements stages, (c) "Security Requirement Template" - to be used by other OMA working groups when defining their security requirements; document sent to the OMA-REC for evaluation. Those projects are on-going, and progressing towards completion. In addition, OMA-SEC Smartcard Subgroup completed the requirements for a smartcard based WEB server. The requirements have been sent out for technical review. Next OMA-SEC meeting will take place during the week of Jan-31-05 to Feb-04-05 in Frankfurt, Germany."

5.7 TR-45 AHAG

There were no specific contributions under this agenda item. It was noted that Qualcomm had offered a meeting in the USA in 2005, which may be co-located with AHAG if possible.

5.8 Other groups

There were no specific contributions under this agenda item.

6 Work areas

6.1 IP multimedia subsystem (IMS)

6.1.1 TS 33.203 issues

TD S3-040905 Proposed CR to 33.203: Corrections to Section 7.1 & 7.2 (Rel-6). This was introduced by Lucent Technologies and corrected some editorial errors in the specification. It was decided to include these changes in a single editorial CR, collecting all editorial changes, which was provided in TD S3-041066 which was revised in TD S3-0401143 and approved.

TD S3-040930 TLS Compatibility in IMS. This was introduced by Nortel Networks and investigated whether the naming restriction is the right approach to mitigate some of the man-in-the-middle security threats in the deployment models wherein certificates are used for authentication between the UE and the P-CSCF for establishing the TLS connection. Nortel Networks also outlined two possible alternative approaches to support TLS without requiring such restrictions on naming. Nortel Networks proposed that SA WG3 agrees that no change requests are needed to Rel-5 and Rel-6 versions of TS 33.203 at this stage in order to support TLS for IMS. A solution can be studied in detail when TLS is introduced for IMS security. Siemens pointed out that a problem existed with HTTP set-up and the use of TLS extensions may be necessary, which means mandating TLS extension support for all clients.

TD S3-041058 Reply LS (from SA WG2) on Revisiting forwards compatibility towards TLS based access security. This was introduced by Ericsson. SA WG3 were asked to note the SA WG2 understanding that IMS Private User Identities and the Home Network Domain Name as stored on the ISIM would normally not be made visible to the user, i.e. from that perspective the new naming requirement would be acceptable from SA WG2 point of view. SA WG2 expected SA WG3 to complete the study before approving any CRs. The consequences of this is that the CR in TD S3-040866 is not approved at this time and more study on this is carried out by SA WG3.

TD S3-040990 IMS security extensions. This was introduced by Ericsson and discussed options for IMS security extensions. A proposed WID was provided in TD S3-040991 which was also considered. Comments were provided in TD S3-041038 which was then introduced. The proposal, comments and work item proposal were discussed and

there was some support for the work, although the scope and relationship with other work items were not fully clear. It was decided that an e-mail discussion should be held in order to finalise the WID and consider it's position in the existing 3GPP Work Plan. The points raised by Ericsson and BT comments should also be discussed by e-mail in order to try to get acceptable proposals at the next meeting. These e-mail discussions will be led by B. Sahlin (Ericsson).

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).

6.1.2 Security for early IMS

TD S3-041036 LS (from SA WG2) on Security Aspects of Early IMS Systems. This was introduced by Ericsson. SA WG2 asked many questions about the draft TR 33.878 and requested some changes and justifications for certain parts. A number of contributions dealing with the points raised in the LS were available and were considered before drafting a reply LS to SA WG2. It was agreed to draft an LS from the agreements made and this was provided in TD S3-041068 and updated to remove DRAFT in TD S3-041145 which was approved.

TD S3-041047 Reply LS (from CN WG4) on Security aspects of early IMS systems. This was introduced by Vodafone. CN WG4 asked SA WG3 to consider the information within the attached document N4-041643 and either to include it within TR 33.878 or inform CN WG4 that the content of N4-041643 should be added to TS 29.228. Vodafone had prepared a proposal to include this information in the TR in TD S3-041063.

TD S3-041048 Reply LS (from CN WG1) on Security aspects of early IMS systems. This was introduced by Vodafone. CN WG1 gave similar advice to CN WG4 and Vodafone had also prepared a proposal to include this information in the TR in TD S3-041061.

TD S3-041053 LS (from CN WG3) on CN WG3 impacts on Early IMS Security mechanisms. This was introduced by Vodafone. CN WG3 asked SA WG3 to consider the information within N3-040881 and N3-040882 and either to include it within TR 33.878 or inform CN WG3 that the content of N3-040881, N3-040882 should be added to TS 29.061. Vodafone had also prepared a proposal to include this information in the TR in TD S3-041062.

The CN WGs all showed a similar approach and it was agreed that this information should be included in the draft TR. The Pseudo-CRs to the TR were then considered:

TD S3-041000 Pseudo-CR to 33.878: Completion of introductory sections and other editorial changes. This was introduced by Vodafone and was agreed for inclusion in the draft TR.

TD S3-040921 Pseudo-CR to 33.878: A correction about context relationship. This was introduced by CCSA/ZTE Corporation and was agreed for inclusion in the draft TR.

TD S3-041006 Pseudo-CR to 33.878: Correction of identity related issues. This was introduced by Siemens. IMSI should be added to the second flow of figure 3 and the text aligned with the Pseudo-CR proposed in TD S3-0401063. The Pseudo-CR was therefore agreed in principle for inclusion in the draft TR.

TD S3-041031 Vodafone comments to TD S3-041005: Pseudo-CR to 33.878: Clarification of IP address related issue. This was introduced by Vodafone. There was some comment on the restriction to a single IP address for an IMS APN. It was clarified that without this restriction, the use of multiple IP addresses would need to be studied and changes made throughout the TR and this would inevitably add complication to the early-IMS implementation. This restriction and explanation will be added to the LS to SA WG2 to clarify the reasons for the requirements. This Pseudo-CR was then agreed for inclusion in the draft TR (and covered the proposals in TD S3-041005).

TD S3-041052 Pseudo-CR to 33.878: Clarification of issues raised in LS from SA WG2 (S3-041036). This was introduced by Siemens and proposed changes to include the concerns raised by SA WG2 in their LS (TD S3-041036). The Pseudo-CR was agreed for inclusion in the draft TR.

TD S3-041030 Vodafone comments to TD S3-041004: Pseudo-CR to 33.878: Correction of idle timer-related issues. This was introduced by Siemens and included improvements proposed by Vodafone to their original contribution. After some discussion it was decided to discuss the incorporation of issues in TD S3-040938 in this Pseudo-CR off-line. The Pseudo-CR was updated and provided in TD S3-041069 which was agreed for inclusion in the draft TR.

TD S3-041062 Pseudo CR to 33.878: Specification of GGSN-HSS interaction based on LS from CN WG3 (S3-041053). This was introduced by Vodafone and proposed changes to include the concerns raised by CN WG3 in their LS (TD S3-041053). The attached CR in TD S3-041053 (N3-040882) was considered and Vodafone considered that the change was not acceptable for inclusion in TS 29.061, or the draft TR 33.878. The changes in the attached CR in N4-040881 was agreed for inclusion in the draft TR. A LS to CN WG3 explaining the SA WG3 position was provided in TD S3-041067 which was reviewed and revised to remove DRAFT in TD S3-041144 and approved.

TD S3-041061 Pseudo CR to 33.878: Detailed specification of registration and authentication procedures based on LS from CN1 (S3-041048). This was introduced by Vodafone and proposed changes to include the concerns raised by CN WG3 in their LS (TD S3-041048). It was indicated that other contributions contained proposals for modification to the procedures changed and it may need re-visiting if these contributions are agreed. The changes were therefore conditionally agreed for inclusion in the draft TR, to be re-visited only if any changes to the current working assumptions due to TD S3-041013.

TD S3-040974 Pseudo-CR to 33.878: Clarifications and corrections to Early IMS Security TR. This was introduced by Ericsson and clarified that the via header is provided by the UE. (The figure changes were no longer necessary as they were covered by TD S3-041006). The textual changes were then agreed for inclusion in the draft TR. It was noted that the change for top via header will be needed in more places due to agreed Pseudo-CRs adding this text.

TD S3-040998 Pseudo-CR to 33.878: UE behaviour when a UICC containing an ISIM is present. This was introduced by Vodafone and was agreed for inclusion in the draft TR.

TD S3-041063 Pseudo-CR to 33.878: Impact on Cx interface based on LS from CN WG4 (S3-041047) . This was introduced by Vodafone and proposed changes to include the concerns raised by CN WG3 in their LS (TD S3-041047). This was agreed to be added after the section introduced in TD S3-040974.

TD S3-041013 Early IMS indication. This was introduced by Nokia. Ericsson and Siemens asked how the mechanism works if the absence of a Security Client header is assumed to be Early IMS and tagged as such by the P-CSCF if there are other future services which also do not include a header: How will the P-CSCF differentiate between the services? It was clarified that the current assumption does not allow for other mechanisms which do not provide the header in the same way as this proposal. The proposal was not agreed, as it did not fully cover the possible cases under the current working assumptions or offer much improvement on the currently specified mechanism.

TD S3-041007 Pseudo-CR to 33.878: Different versions of IMS. This was introduced by Siemens and provided a solution for Early IMS. It was noted that the proposal restricted the Elements to the Home Network for Early IMS. Another proposed solution to the same issue was provided by Huawei in TD S3-040973 which was also reviewed. This contribution relied upon Network pre-configuration in order that the I-CSCF knows which S-CSCF supports Early-IMS and passes on Early-IMS requests to it. The Huawei solution was not considered complete enough to include for Rel-6 and it was agreed to accept the Siemens proposal in TD S3-041007 , including the note related to the text from point 1 of the Huawei proposal in TD S3-040973 and the rest of the roaming mechanism from the Huawei proposal should be further studied for a potential future 3GPP Release.

TD S3-040939 Pseudo-CR to 33.878: Correction of figures. This was introduced by Huawei and was agreed to be included in the draft TR.

TD S3-040999 Pseudo-CR to 33.878: Removal of remaining Editorís Notes. This was introduced by Vodafone and was agreed to be included in the draft TR.

TD S3-041001 Proposed CR to 33.203: Addition of reference to early IMS security TR (Rel-6). Vodafone reported that the 3GPP rules did not allow reference from within TSs to 8xx-series TRs (because they will not be transposed by the SDOs) and proposed that TSG SA is asked to upgrade TR 33.878 to a 9xx-series TR and to agree a modified version of this CR. There was an objection from T.I.M to this as the WID (as modified and agreed by TSG SA) states that this work should not have an impact on existing specifications. The WID was checked off-line by Vodafone and it was clarified that changes to existing specifications could be made if they were informative, so an informative annex can be added, however, T.I.M. did not share this interpretation of the WID text.

THE FOLLOWING TEXT AND ACTION MAY BE REVISED AS DIFFERENT INTERPRETATIONS WERE EXPRESSED AT THE MEETING

It was agreed to ask TSG SA for the upgrade of the TR to the 9xx-series and if agreed, this CR will be revisited at the next SA WG3 meeting.

The CR in TD S3-041001 was revised in TD S3-041130 to be presented to TSG SA if it is upgraded to the 33.9xx-series by TSG SA. There was continued objection to this CR being approved before TSG SA make a decision, so **it was agreed that the SA WG3 Chairman would ask TSG SA whether it is possible to bring a CR for 33.102 to refer to the TR from a new informative Annex in case TSG SA agrees to upgrade this to the 33.9xx-series.**

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.

TD S3-041091 Updated TR 33.878 version 0.0.4. This contained the updates agreed at the meeting and it was agreed that this should be sent to TSG SA and approval requested. **M Pope to create version 1.0.0 from the attached version 0.0.4**. (Note that the final number to be used for this TR depends upon the decision of TSG SA on the request to upgrade it to the 33.9xx series).

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

TD S3-041044 Reply (from CN WG4) to LS on Reply to Evaluation of the alternatives for SMS fraud countermeasures. This was introduced by Vodafone. CN WG4 responded to questions from GSMA IREG on their intentions to study MAPsec work for SMS Fraud countermeasures. **The LS was noted and contributions were invited on the MAPsec Gateway solution outlined in this LS in order to provide a reply LS at the next SA WG3 meeting.**

TD S3-040954 Proposed CR to 33.200: SMS fraud countermeasures (Rel-6). This was introduced by Siemens. Nokia asked if Siemens had considered the large size of the table that would need to be kept for this short-term solution. The Nokia contribution in TD S3-040967 was considered to analyse it's suitability. After discussion, the CR was revised in TD S3-041070 which was approved.

TD S3-040967 Detecting a falsified SMSC address. This was introduced by Nokia and offered another solution for SMS Fraud countermeasures. Siemens highlighted that this does not address the problem of address falsification which is what the aim of their solution was. Nokia argued that this does not prevent the problem, but reduces it and will help to handle it and was less resource-consuming than the Siemens solution (i.e. no large tables to maintain). It was also suggested that if the attacker continuously changes the spoofed SMSC address then the number of barred addresses would grow very fast. After discussion of and agreement of the CR in TD S3-040954 (TD S3-041070) this proposal was re-assessed. It was decided that the justification of this would need to be revised and a proposed CR created. This was therefore postponed for further study.

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 S3-040968 Certificate management for TLS connections between IMS and non-IMS networks. This was introduced by Nokia and discussed several approaches of certificate management for establishing TLS connections for SIP traffic between IMS CSCFs and non-IMS SIP proxies and proposed extending the usage of NDS/AF for establishing TLS connections in Rel-7. Ericsson commented that the NDS/AF implied TLS extensions. The definition of "non-IMS network" was questioned. It was explained that this was described in 33.203 v6.4.0, clause 6.5. This was noted for further study and a WID is expected to be contributed to the next meeting.

6.5 UTRAN network access security

TD S3-040896 Reply LS (from SA WG2) on Generic Access Network (GAN). This was introduced by Nokia and was copied to SA WG3 for information. The LS was noted.

TD S3-040904 Proposed CR to 33.102: Correction of Abbreviation for USIM (Rel-6). This was introduced by the MCC after receipt of an e-mail pointing out the inconsistency in the USIM abbreviation. This CR was approved.

TD S3-040918 Proposed CR to 33.102: Correction of TMUI to TMSI in a figure (Rel-6). This was introduced by CCSA/ZTE Corporation. This was revised to put it into correct CR format in TD S3-041071 which was approved.

TD S3-041051 Proposed WID: Development of UEA2 and UIA2. This was introduced by Teliasonera on behalf of ETSI SAGE. The WID was requested in order to allow proper control of the new back-up algorithm work. This WI description was revised to complete the affected areas in TD S3-041072 which was approved.

6.6 GERAN network access security

TD S3-041033 Siemens comments to S3-0401029 and S3-040935: Proposed CR to 33.102: Support of algorithms in UEs (Rel-6). This was introduced by Siemens and comprised an update to TD S3-040935 and TD S3-041029. This CR was approved.

TD S3-041028 Vodafone comments to S3-040955: Proposed CR to 43.020: Clarifying the support of algorithms within mobile stations (Rel-6). This was introduced by Vodafone and comprised an update to TD S3-040955. It was reported that phasing out A5/2 was acceptable for the GSMA Board. The effect on other operators who implement only A5/2 ~~(if any)~~ was unknown, as they do not participate in the GSM/3GPP standardisation bodies). The CR was revised in TD S3-041075, which was approved.

TD S3-040969 Security context separation (contributed by Nokia). This was postponed for the next meeting and should be re-submitted by the authors.

TD S3-040970 Key separation mechanism in GSM/GPRS (contributed by Orange and Nokia). This was postponed for the next meeting and should be re-submitted by the authors.

TD S3-040983 Adoption of key separation for GSM/GPRS in the short term. This was contributed by Orange, but was not discussed due to lack of time. Orange asked to forward this to ETSI SAGE in an LS, in order to give visibility of the issue. An LS was provided in TD S3-041076 which was revised to remove DRAFT in TD S3-041146 and approved.

TD S3-041014 Revised WID: Access Security Enhancements. This was introduced by Ericsson. Comments from Nokia were provided in TD S3-041040 which was reviewed. The WID was updated and revisions removed in TD S3-041077 which was approved.

TD S3-041015 Access Security Review. This was introduced by Ericsson. This was noted and contribution on this proposed WI was requested.

TD S3-041034 Liaison Statement (from IREG): Request for Comments on Proposed Security Enhancements to GSM/GPRS Networks. This was introduced by Vodafone. It was explained that Vodafone had input a paper to IREG as the SA WG3 meeting had taken place just before the IREG, rather than proposed an official SA WG3 liaison, because the IREG meeting took place just before the last SA WG3 meeting and the next opportunity to receive feedback would not be until the next IREG plenary meeting in March 2005 ~~meeting and there was no time to input an official Liaison to their meeting~~. The views of operators to the proposed security enhancements for GSM/GPRS Networks was reported in the LS and it was noted that there was some support and some concerns raised, the average timescale for implementation averaged around 3 years (average of individual views expressed). The LS was noted. The GSMA Security Group Chairman (C. Brookson) reported that there will be a meeting of GSMA-SEG 16 December 2005 and anyone who wishes more details or requests for attendance should be addressed to him by e-mail.

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 S3-040895 LS from SA WG2 on GAA. This was introduced by Nokia. SA WG2 pointed out their view that the GAA parameters are best stored in the HSS independently from the data stored for CS & PS domains and the IM CN subsystem, as the capability for a service to utilize GAA is not tied to any of these particular domains. However, a user utilizing GAA for service authentication must have a subscription (CS and/or PS) with the mobile operator providing GAA. At the same time, GAA shall not be considered as a separate domain in the same sense as the notion of a ìdomainî is considered for CS and PS. It was noted that the thinking of SA WG2 was in line with SA WG3 and the LS was noted.

TD S3-040977 Proposed CR to 33.919: Removal of unnecessary editor's notes (Rel-6). This was introduced by Nokia and was approved.

TD S3-040980 Liberty and GAA relationship. This was introduced by Nokia reported the result of their investigation into Liberty GAA work. The contribution gave details on the possible relationship between GAA and Liberty, and invited further comments on the details of the relationship and possible interaction methods. Comments to this were provided by Siemens in TD S3-041039.

TD S3-041039 Ericsson Comments to Nokia's TD S3-040980 on "Liberty and GAA relationship". This was introduced by Ericsson and provided substantial comments to the analysis in TD S3-040980. After discussion it was agreed that the conclusions reached by Ericsson were acceptable and more study is required to gain more understanding of the possible interworking scenarios. **Silke Holtmanns agreed to provide a WID for Liberty Alliance / GAA work for the next meeting.**

AP 36/03: Silke Holtmanns to provide a WID for Liberty Alliance / GAA work for the next meeting.

6.9.2 TS 33.220 GBA

TD S3-040894 Response LS (from SA WG1) regarding application selection for GBA. This was introduced by TeliaSonera and was provided for information. The LS was noted. SA WG3 members were asked to provide information to their SA WG1 colleagues in order to help their understanding of the issues.

TD S3-040923 Proposed CR to 33.220: Clarification of GBA_U AUTN generation procedure in the BSF (Rel-6). These issues were covered by TD S3-040956.

TD S3-040956 Proposed CR to 33.220: Complete the MAC modification for GBA_U (Rel-6). This was introduced by Siemens. This CR covered the proposal in TD S3-040923 and completed the MAC definition. The CR was reviewed and updated to make the Hash function SHA1 work on the complete key and truncating the most significant 64 bits. The CR was revised in TD S3-041078 which was approved.

TD S3-040950 GBA_U: GBA_U derivations. This was introduced by Gemplus on behalf of Axalto, Gemplus and Oberthur and proposed alternative CRs to complete TS 33.220 taking into account the agreement reached at SA3#35 meeting. The recommended CR was provided in TD S3-040951.

TD S3-040951 Proposed CR to 33.220: Optimisation of the GBA_U key derivation procedure (Rel-6). This was introduced by Gemplus on behalf of Axalto, Gemplus and Oberthur. The CR was reviewed and **it was noted that figure 2 was also updated in the CR in TD S3-041078 and the SA WG3 Secretary was asked to take this into account in the CR implementation if they are both approved by TSG SA**. The CR was revised in TD S3-041136 which was approved.

It was also noted that important clarification is needed in this section, not related to this CR and Axalto and Nokia provided a new CR with this clarification in TD S3-041079 which was reviewed and revised in TD S3-041137 which was approved.

TD S3-040953 Proposed CR to 33.220: GBA_U: storage of Ks_ext in the UICC (Rel-6). This was withdrawn because the option provided in TD S3-040951 had been agreed by SA WG3.

TD S3-040952 Requirement on ME capabilities for GBA_U. This was introduced by Gemplus on behalf of Axalto, Gemplus and Oberthur. The CR was revised in TD S3-041080 which was approved.

TD S3-040937 LS from ETSI SAGE: Proposed key derivation function for the Generic Bootstrapping Architecture. This was introduced by Teliasonera. ETSI SAGE asked SA WG3 to confirm their assumptions which were made to simplify the design of the algorithm. The assumptions were reviewed and confirmed by SA WG3. The information provided in this LS will be used in related work in SA WG3 (e.g. Key derivation function specification).

TD S3-041027 Proposed CR to 33.220: Key derivation function (Rel-6). This was introduced by Nokia. The proposed section B.4 was not needed as the changes proposed in TD S3-040952 had been agreed and the proposed new Editor's notes were not needed and were removed. The CR was revised in TD S3-0401081 which was approved.

AP 36/04: Silke Holtmanns to provide a CR to 33.220 to clarify the coding of P2 as characters into octet strings.

TD S3-040978 Proposed CR to 33.220: Removal of unnecessary editor's notes (Rel-6). This was introduced by Nokia and was modified slightly in TD S3-041082 which was approved.

TD S3-040988 Proposed CR to 33.220: Clean up of TS 33.220 (Rel-6). This was introduced by Ericsson. The CR was revised editorially in TD S3-041083 which was approved.

TD S3-041024 Proposed CR to 33.220: New key management for ME based GBA keys (Rel-6). This was introduced by Nokia. Comments to this CR were provided in TD S3-041043. The CR was revised in TD S3-041084 which was approved. Axalto commented that an appropriate wording is "all GBA related keys shall be deleted from the ME when a different UICC is inserted**/removed**".

TD S3-040981 Proposed CR to 33.220: GBA USIM/ISIM selection (Rel-6). This was introduced by Nokia. The definition was updated editorially in TD S3-041085, which was approved.

TD S3-040924 key lifetime of GBA. This was introduced by CCSA/ZTE Corporation and proposed that renegotiation should start, to get a new key before the original key that is shared by UE and NAF has expired, which can ensure communications are not terminated. The need to include such a procedure in the specifications was questioned, as the User can initiate a Bootstrapping whenever necessary before Key expiry. It was recognised that the specification implies that the protocol is terminated when Key negotiation is initiated and it was agreed that this should be removed in order to enable the re-keying during the current lifetime of keys without termination the protocol. A CR to remove this was provided in TD S3-041086 which was revised in TD S3-041140 and approved.

TD S3-040982 Proposed CR to 33.220: Key lifetime clarifications (Rel-6). This was introduced by Nokia. The need for this in Rel-6 was questioned. After some discussion it was not thought really necessary and could be re-considered for Rel-7 if some use-cases could be presented justifying this addition.

TD S3-040940 Key freshness in GBA. This was introduced by **3**. CRs were proposed in TD S3-040941 and TD S3-040942 . Comments to this from Siemens was provided in TD S3-041049 which was reviewed. Siemens concluded that this was not needed for Rel-6 but proposed adding the note, in a modified format.

TD S3-040942 Adding note about replay protection. The Note text was replaced with the proposal in TD S3-041043 and the CR revised in TD S3-041087 which was approved.

TD S3-040941 Proposed CR to 33.220: Adding a note about replay protection (Rel-6). This was withdrawn, as the proposal in TD S3-040940 was not agreed.

TD S3-040932 Usage of B-TID in reference point Ub. This was introduced by Huawei and proposed to use B-TID in re-bootstrapping procedure instead of IMPI within the lifetime of Ks and to approve the CR attached to this contribution. Siemens commented that there was complication in this proposal, in storing B-TIDs on the mobile for the GBA_U case. After some discussion no support for this proposal was received for Rel-6 and it was therefore rejected.

TD S3-040987 GBA User Security Settings (GUSS) usage in GAA and introduction of NAF groups. This was introduced by Siemens and asked SA WG3 to endorse the introduction of NAF groups as described in the attached CR implementing the changes to TS 33.220. The CR was reviewed and Huawei asked to be added to the source companies as they were happy with this version of the CR. Attachment 2 was revised in TD S3-041135 and approved.

Some concerns were expressed that the introduction of NAF Groups in GAA introduces administrative and HSS complexities without any clear advantages. Furthermore, the requirement of allowing different policies between groups of NAFs can be supported with the existing GAA architecture by having different application identifiers for each group of NAFs. Despite the concerns, the CR was reviewed and approved as the concern was not shared by others.

TD S3-040986 Proposed CR to 33.220: Fetching of one AV only on each Zh run between BSF and HSS (Rel-6). This was introduced by Siemens on behalf of Siemens and Nokia. It was noted that the issue "(iii) No special handling of sequence numbers in AuC, in particular if more than one BSF exists in home network" given in the CR reason for change still needed study and solved. The CR was revised in TD S3-041090 which was approved.

TD S3-040976 Proposed CR to 33.220: No GUSS/USS update procedures in Release-6 (Rel-6). This was introduced by Siemens on behalf of Nokia and Siemens. After consideration and rejection of the alternative proposal in TD S3-040934 this CR was revised in TD S3-0401089 which was approved.

TD S3-040933 Update of GUSS in BSF. This was introduced by Huawei and proposed a different procedure than the Siemens and Nokia proposal in TD S3-040976. A proposed CR to implement the proposals was provided in TD S3-040934.

TD S3-040934 Proposed CR to 33.220: Update of GUSS (Rel-6). This was introduced by Huawei. Siemens commented that the introduction of push information and revocation adds complication to what should be kept as a simple system. Siemens added that the introduction of these protocols would need to be sent to CN WG4 in order for them to add the functionality in the Stage 3 specifications. Huawei commented that this could probably be included by CN WG4 in a single meeting and it would avoid the risk of BSF overloading with the messages generated if the Siemens and Nokia proposal was adopted in Rel-6. It was considered too late in Rel-6 to add this functionality and this could be further studied for Rel-7. The CR was therefore rejected.

6.9.3 TS 33.221 Subscriber certificates

TD S3-040979 Proposed CR to 33.221: Editorial correction (Rel-6). This was introduced by Nokia. This CR was approved.

6.9.4 TS 33.222 HTTPS-based services

TD S3-040962 Including AES in the TLS profile of TS 33.222. This was introduced by Ericsson and described the need for the CR provided in TD S3-040963 and was reviewed and noted.

TD S3-040963 Proposed CR to 33.222: Adding Support for AES in the TLS Profile (Rel-6). This was introduced by Ericsson and was revised in TD S3-041092 which was approved.

TD S3-040975 Authorization flag transfer between AP and AS. This was introduced by Nokia on behalf of Nokia and Siemens. It was agreed that this CR should be merged with the CR in TD S3-040734 from the previous meeting and a combined CR was provided in TD S3-041093 which was approved.

TD S3-041026 Proposed CR to 33.222: Visited AS using subscriber certificates (Rel-6). This was introduced by Nokia This CR was approved.

TD S3-040985 Proposed CR to 33.222: Correction of inconsistencies within AP specification (Rel-6). This was introduced by Siemens. This CR was approved.

TD S3-040964 Postponing PSK TLS to 3GPP Rel-7. This was introduced by Ericsson and proposed to postpone PSK TLS to release 7, according to the SA WG3 agreement that PSK TLS should be postponed if the Internet Draft "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)" is not ready when Rel-6 is frozen. Nokia reported that version 0.3 had been published and received few comments and changes and 0.4 was ~~published~~ submitted on 24 November. It will be published soon after Thanksgiving and is progressing towards publication as an RFC. It was decided to explain the dilemma for the inclusion or removal of TLS to TSG SA Plenary. It was

agreed to provide 2 CRs, one to include TLS and one to remove it (TD S3-040965) and to ask TSG SA which one they wish to approve. The CR to keep TLS was provided in TD S3-041094 which was revised in TD S3-041142 and approved. A LS to TSG SA explaining the problem and asking for a decision was provided in TD S3-0401095 which was revised in TD S3-041141 and approved.

TD S3-040965 Proposed CR to 33.222: Removing PSK TLS from 3GPP rel-6 (Rel-6). This was approved conditionally upon the decision of TSG SA for inclusion or removal of TLS.

TD S3-040966 Proposed CR to 33.222: Clean-up of TS 33.222 (Rel-6). This was introduced by Ericsson and proposed deleting editor's notes. It was agreed that these changes should be included in other CRs.

TD S3-041025 Proposed CR to 33.222: TLS extensions support (Rel-6). This was introduced by Nokia. This was modified slightly and revised in TD S3-041096 which was approved.

6.10 WLAN interworking

TD S3-041045 LS from CN WG4: The relationship between Scenario 2 and Scenario 3 authentication procedures. A response was provided in TD S3-041101 which was reviewed and revised in TD S3-041147 which was approved.

TD S3-041037 LS from SA WG2: RE: The relationship between Scenario 2 and Scenario 3 authentication procedures. This was covered by the response in TD S3-041147.

TD S3-041046.LS from CN WG4: Need for the IMSI at the PDG. A response was provided in TD S3-041102 which was reviewed and revised in TD S3-041148 which was approved.

TD S3-040929 Explanation of PDG certificate profile. This was introduced by Nokia and explained the difference between the PDG certificate profile and NDS/AF profile. The contribution was noted. A related CR was provided in TD S3-040927 which was reviewed.

TD S3-040927 Proposed CR to 33.234: Profile for PDG certificates in Scenario 3 (Rel-6). This was introduced by Nokia and was reviewed. It was agreed that OCSP should be made mandatory and the CR was revised in TD S3-041100 which was approved.

TD S3-040915 LS (from T WG2) on EAP Authentication commands for WLAN interworking and improved security for UICC generic access. This was introduced by the SA WG3 Chairman. T WG2 suggested that SA WG3 considers updating TS 33.234 to modify the EAP authentication procedure description by utilising the AT commands introduced in TS 27.007. A ~~contribution~~ CR to implement AT Commands in line with T WG2 proposals was provided in TD S3-0401022 and ~~a response LS was approved~~ was reviewed and revised in TD S3-041149, which was approved.

TD S3-040957 Proposed CR to 33.234: Clarification on storage of Temporary Identities in UICC (Rel-6). This was introduced by Samsung. The changes were agreed in principle but it was considered better to include these changes in the CR in TD S3-041104.

TD S3-041022 Correction of WLAN UE function split, Cover letter to attached CR. This was introduced by Axalto on behalf of Axalto, Gemplus, Siemens and T-mobile. The Proposed CR which was attached was updated in TD S3-041103 which was reviewed. The proposed changes were agreed in principle and the CR was cleaned up to remove double revisions etc. and provided in TD S3-041104 which was revised again in TD S3-041149 and approved.

TD S3-040926 Proposed CR to 33.817: Bluetooth security and configuration considerations for Annex of TR 33.817 (Rel-6). This was introduced by Nokia and was based on the input from Toshiba and supporting Companies, but inserting an annex in TR 33.817 instead of TR 33.900, as TR 33.900 is not likely to be approved for Rel-6. It was agreed that the references acknowledging papers and publications should be moved into a Bibliography within the proposed Annex. The CR was revised in TD S3-041105 and reviewed. The CR was again revised in TD S3-041150 which was approved.

TD S3-040906 Pseudo-CR to 33.900: Bluetooth security and configuration considerations for Annex of TR 33.900 (Rel-6). This was provided by Toshiba, BT and supporting Companies, but was no longer needed as the corresponding CR in TD S3-041150 had been approved.

TD S3-041003 Update of S3-040838. This was introduced by Gemplus and proposed a revision of the CR provided to the previous meeting in TD S3-040838. The CR was reviewed and the changes to bullet 8) was discussed, as it mandates the entity holding the USIM shall schedule accesses to the UICC by itself and a external local interface device. The CR was revised with only the agreed changes in TD S3-041106 which was reviewed and revised in TD S3-041151 which was approved.

TD S3-041002 Proposed CR to 33.817: Terminology update to not rule out the use of the smart card for security enhancements (Rel-6). This was introduced by Gemplus. The CR was revised in TD S3-041107 which was reviewed and revised in TD S3-041152 which was approved.

TD S3-040916 Correction WRAP to CCMP. This was introduced by CCSA/ZTE Corporation and proposed to align with changes in IEEE. A CR to implement this was provided in TD S3-041088 which were updated editorially in TD S3-041108 which was reviewed and approved.

TD S3-040958 Proposed CR to 33.234: Wn Reference Point Description (Rel-6). This was introduced by Samsung on behalf of Samsung, Nokia and Ericsson. This CR was approved.

TD S3-040945 Proposed CR to 33.234: Completion of definition and abbreviations (Rel-6). This was introduced by Ericsson and was revised to remove unnecessary abbreviations in TD S3-041109 which was reviewed and approved.

TD S3-040959 Proposed CR to 33.234: Removal of word ìscenarioî (Rel-6). This was introduced by Samsung on behalf of Samsung and Nokia This CR was approved.

TD S3-040946 Proposed CR to 33.234: Fallback from re-authentication to full authentication (Rel-6). This was introduced by Ericsson. The cover sheet was corrected to change IMS to IMSI and the CR was revised in TD S3-041110 which was approved.

TD S3-040947 Proposed CR to 33.234: Clarification on the use of IMSI in WLAN 3GPP IP access (Rel-6). This was introduced by Ericsson. This CR was approved.

TD S3-040949 Proposed CR to 33.234: Clarification on the use of IMSI in WLAN 3GPP IP access (Rel-6). This was introduced by Ericsson. This CR was approved.

TD S3-040943 Control of simultaneous session in WLAN 3GPP IP access (scenario 3). This was introduced by Ericsson on behalf of Ericsson and Siemens and proposed a CR in TD S3-040944. It was also proposed that LSs are sent to to the proper groups were potential changes are needed (SA WG2, CN WG1) attaching this contribution and any approved CR. The LS was provided in TD S3-041111 which was approved.

TD S3-040944 Proposed CR to 33.234: Control of simultaneous sessions in WLAN 3GPP IP access (Rel-6). This was introduced by Ericsson on behalf of Ericsson and Siemens. It was suggested to put the explanation of the problem from TD S3-040943 into the reasons for change to better describe the need for the CR. It was also suggested that old security associations are deleted when a new one is requested. This was done and the CR was revised in TD S3-041112 which was revised again in TD S3-041153 and was approved.

TD S3-040948 Proposed CR to 33.234: Clarification on the use of MAC addresses (Rel-6). This was introduced by Ericsson. The CR was revised in order to reformulate the proposed text for step 25 in TD S3-041113 and again in TD S3-0401138 which was reviewed and approved.

TD S3-041139 Proposed CR to 33.234: WLAN removal of Editors' notes (Rel-6). This was provided by MCC and was revised in TD S3-041155 and approved.

6.11 Visibility and configurability of security

There were no specific contributions under this agenda item.

6.12 Push

There were no specific contributions under this agenda item.

6.13 Priority

There were no specific contributions under this agenda item.

6.14 Location services (LCS)

There were no specific contributions under this agenda item.

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

There were no specific contributions under this agenda item.

6.16 Open service architecture (OSA)

There were no specific contributions under this agenda item.

6.17 Generic user profile (GUP)

TD S3-041035 Response LS (from SA WG2) on GUP Security Recommendations. This was introduced by Ericsson. SA WG2 asked SA WG3 to review the proposed changes to TS 23.240 in relation to the support of the Discovery Service as a Trusted Authority and confirm whether these changes satisfy SA WG3 concerns. Ericsson reported that they had reviewed the changes and found them acceptable. A response LS to inform SA WG2 that the changes are acceptable was provided in TD S3-0401099 which was reviewed and revised in TD S3-041154 and approved.

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 S3-040907 Liaison Statement (from SA WG4) on Reception Acknowledgement for MBMS. This was introduced by Ericsson and asked SA WG3 to consider the implications of using reception reports for acknowledgement collection noting that acknowledgement collection may be used by the BM-SC to take further action and also to consider the feasibility of extending the delivery acknowledgement mechanism for charging purposes and to report back to SA WG4 on whether this is possible. A response LS was approved in TD S3-041033.

TD S3-040908 Liaison Statement (from SA WG4) on MBMS User Service architecture. This was introduced by NEC Technologies and asked SA WG2 for feedback on their assumptions concerning MBMS User Service and was copied to SA WG3 for information. The LS was noted and a response included in TD S3-041059.

TD S3-0401054 Reply Liaison Statement (from SA WG2) on Reception Acknowledgement for MBMS. This was introduced by Siemens and was copied to SA WG3 for information. SA WG3 were expected to discuss this and provide a response on the security issues associated with reception acknowledgement mechanisms. A response to TD S3-040908 and TD S3-041054 LS was provided in TD S3-041059 and was reviewed and updated in TD S3-0401133 which was approved.

TD S3-041056 Reply LS (from SA WG5) on Reception Acknowledgement for MBMS Charging. This LS was reviewed and noted.

TD S3-041010 Proposed CR to 33.246: Clarifying ME capabilities (Rel-6). This was introduced by Siemens and proposed changes which have overlap with CR005 and CR007. The proposals were agreed in principle and an evening session to resolve the overlaps and finalise the changes was arranged. A further update was included in a package from Siemens in TD S3-041018 (see below).

TD S3-041018 CR corrections. This was introduced by Ericsson and provided corrections to previous CRs which had been made to the wrong version of the base specification. The contribution proposed revisions to the CRs to

the correct version and some other editorial enhancements. The proposals were agreed in principle and further clashing CRs will be checked in this meeting. The final documents contained the revised CRs which were dealt with as follows: CR005R2 revised in TD S3-04115, CR007R4 ~~approved~~rejected, CR008R2 rejected, CR016R2 revised in TD S3-041116, CR018R3 revised in TD S3-041120, CR020R2 revised in TD S3-041117, CR021R5 revised in TD S3-041124.

TD S3-041008 Proposed CR to 33.246: Clarify the use of mandatory MIKEY features for MBMS (Rel-6). This was introduced by Siemens and was modified slightly in TD S3-041055 which was approved.

TD S3-040972 Proposed CR to 33.246: Clarification of MSK key management (Rel-6). This was introduced by Nokia and the principles of the CR were agreed. The name "DNS Name" should be changed to "Domain Name" and this should be considered in the MBMS evening sessions. A proposal from Siemens was provided in TD S3-041011 and the MBMS evening sessions finally provided a revised CR in TD S3-041124 (see below).

TD S3-040984 Proposed CR to 33.246: Clarification of MSK key management (Rel-6). This was introduced by Orange. It was noted that the deleted text on the cover page was to highlight the revisions proposed. It was also noted that the terminal reaction to the new flag also needed to be specified. The CR was re-worked in the evening MBMS session with other contributions and a revised CR was provided in TD S3-041124 (see below).

TD S3-040995 IETF work needed for MBMS security. This was introduced by Ericsson and described the content and status of the IETF drafts. The dependency of the internet draft (IETF internet draft "The Key ID Information Type for the General Extension Payload in MIKEYî <draft-carrara-newtype-keyid-00.txt>, October 2004) was discussed and considered useful, and the timescale of this for Rel-6 inclusion should be monitored. The Dependency was approved to be added to the IETF dependency list and the RFC should be made available as soon as possible and use of the Draft should also be considered if necessary.

TD S3-041021 MUK ID and UE ID in MBMS. This was introduced by Ericsson and discussed different alternatives for MUK ID and proposed that a hash of (B-TID || NAF ID) is used as MUK ID. It was clarified tht the UE should do the collision check and re-run if collision occurs. A related contribution was provided in TD S3-041012.

TD S3-041012 MUK ID. This was introduced by Siemens and analysed the possibilities to identify the key MUK which is shared between a particular BM-SC and a particular UE. The MUK identification is necessary for the outer Key ID of a point-to-point MIKEY message to transfer a MSK from a BM-SC to the UE. It was also noted that T WG3 should receive a LS outlining the decisions made by SA WG3. After off-line discussions and the MBMS evening sessions the proposed CR was rejected.

TD S3-040997 Replacing Network ID with NAF ID. This was introduced by Ericsson and discussed some concerns on usage of MCC/MNC and studies if NAF ID could be used instead. CRs were provided containing the 2 alternative solutions and SA WG3 were asked to decide the solution and approve the appropriate CR. After some discussion, Alternative A was chosen, with the notes made informative. The implementation of this CR was moved to the MBMS evening sessions in order to include other agreements. The principles of the CR were included in other CRs in the MBMS evening sessions and this CR was then rejected.

TD S3-041011 Reliable MSK updating. This was introduced by Siemens and was reviewed. Three alternatives for implementation was included. The proposal was agreed in principle and the interaction with the push case should be investigated along with the finalisation of the choice of CR text in the evening MBMS session. This was updated in the evening session in TD S3-041122 (see below).

TD S3-041041 Update of S3-041017: Key group ID and MSK ID. This was introduced by Ericsson and discussed. It was decided to discuss the alternative to select in the evening MBMS session. The evening session took this into account with the original proposal in TD S3-041017 and created a revised version of the CR in TD S3-041124 (see below).

TD S3-041009 Proposed CR to 33.246: Specify CSB-ID format (Rel-6). This was introduced by Siemens and was handled in the evening MBMS Session as it depended on the results of other issues. This was included in the MBMS evening sessions and was rejected.

TD S3-040922 Efficient Solutions of MSK update. This was introduced by CCSA/ZTE Corporation and discussed two solutions which can reduce the overload of BM-SC when performing the MSK update. It was noted that this depends on how the MSK is re-Keyed and how charging is done. It was also pointed out that the current SA WG3 assumption was to do point-to-point Key update as the point-to-multipoint reliability could not be guaranteed. It was

agreed that this mechanism was too late to introduce for Rel-6 at this stage but the proposal would be re-considered for development and possible inclusion in Release 7. The document was therefore noted.

TD S3-041023 MBMS MSK management. This was introduced by Samsung and proposed to agree on the MSK management principles as follows:

> *ìThe UE shall delete one MSK when the corresponding MTK ID of one MTK whose delivery is protected by this MSK reaches the upper limit defined in the Key Validity Data subfield present in the KEMAC payload when this MSK is distributed. To stop the use of one dedicated MSK immediately, BMSC may set the MTK ID of one MTK to the upper limit when the corresponding MTK is updated.î*

A CR implementing the change was provided in TD S3-040961. Siemens commented that the Key deletion procedure was deleted and the replacement did not guarantee the delivery of the new Keys and deletion of the old ones. It was agreed to investigate some solutions in the evening MBMS Session to see if any solution could be agreed upon. The CR was revised in TD S3-041131 and was reviewed. There were some concerns over the implentability of the mechanism and also that a point-to-multipoint MSK update would affect all UEs and not only the UE intended by the CR. It was suggested that this is further discussed off-line and an e-mail discussion group was set-up to discuss this and submit a revised CR at the next meeting.

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.

TD S3-041019 Proposed CR to 33.246: Shorter MKI (Rel-6). This was introduced by Ericsson and reviewed. It was agreed in principle but needed to be aligned at the evening session to remove overlapping changes with other CRs. This was discussed in the MBMS evening sessions and a revised CR provided in TD S3-041119 (see below).

TD S3-041020 Proposed CR to 33.246: Removal of ID_i in MIKEY response messages for MSKs (Rel-6). This was introduced by Ericsson and was reviewed and approved in substance. Overlaps with other CRs will be checked in the evening MBMS session. The MBMS evening session proposed to include these modifications in CR030 (TD S3-041021).

TD S3-040992 The need for and use of salt in MBMS streaming (Updated). This was introduced by Ericsson on behalf of Ericsson and TeliaSonera. A CR to 33.246 was attached to the contribution which was approved in substance. The CR will be considered for alignment in the evening MBMS session. This was updated in the evening session in TD S3-041118 (see below).

TD S3-040897 Updated: MBMS Download Protection using XML. This was introduced by Ericsson and was discussed with other related contributions and a LS to OMA was later approved in TD S3-041073.

TD S3-040901 An Update to Using OMA DRM V2.0 DCF for MBMS Download Protection. This was introduced by Nokia and was discussed with other related contributions and a LS to OMA was later approved in TD S3-041073.

TD S3-040899 MBMS Performance Comparison of DCF and XML-encryption. This was introduced by Ericsson and was discussed with other related contributions and a LS to OMA was later approved in TD S3-041073.

TD S3-040900 Comparison of DCF and XML encryption for MBMS Download. This was introduced by Ericsson and analysed the use of XML encryption for MBMS Download. Ericsson concluded that XML encryption is favourable with respect to the aspects discussed in the contribution and proposed that XML encryption is adopted as encryption method for MBMS download. A related proposal was provided in TD S3-040909 which was also considered.

TD S3-040909 Comments to Ericsson contribution (S3-040900) on Comparison of DCF and XML encryption for MBMS Download. This was introduced by Nokia and described that there had been some confusion and misunderstanding about the proposal to use OMA DRM for MBMS and proposed proposal to re-use the DCF file format for MBMS, without imposing the other requirements and assumptions needed in OMA DRM V2.0. This was discussed with other related contributions and a LS to OMA was later approved in TD S3-041073.

TD S3-040910 Required Changes in OMA DRM specifications for using the DCF for MBMS Download protection. This was introduced by Ericsson and proposed the modifications needed to DRM specifications if the DCF proposal described by Nokia are agreed. This was discussed with other related contributions and a LS to OMA was later approved in TD S3-041073.

TD S3-040902 Overhead and Performance Comparison of OMA DRM V2.0 DCF and XML for MBMS Download Protection. This was introduced by Nokia. Comments were provided by Ericsson in TD S3-040911.

TD S3-040911 Comments to S3-040902: Overhead and Performance Comparison of OMA DRM V2.0 DCF and XML for MBMS Download Protection. This was introduced by Ericsson and was discussed in conjunction with the comparison paper provided by Nokia, who had provided a response in TD S3-040971.

TD S3-040971 Response to S3_040911: Comments to S3-040902: Overhead and Performance Comparison of OMA DRM V2.0 DCF and XML for MBMS Download Protection. This was introduced by Nokia and provided responses to the comments made by Ericsson. This was discussed with other related contributions and a LS to OMA was later approved in TD S3-041073.

The above proposals and comments were discussed. It was indicated that the DRM solution appeared the most desirable and the OMA should be asked whether their specifications can be modified in order to allow the proposal to be used in 3GPP. A LS to OMA was provided in TD S3-0401057 which was reviewed and revised in TD S3-041129 which was again revised in TD S3-041033 and finalised in TD S3-041073 which was approved.

TD S3-041056 Reply LS (from SA WG5) on Reception Acknowledgement for MBMS Charging. This was provided to SA WG3 for information and was noted.

TD S3-041042 General comment contribution to MBMS: Feature list to complete MBMS in Release 6. This was introduced by Ericsson and proposed a list of actions that need to be taken to ensure that the MBMS security work is complete as possible for the expected functional freezing of the specifications in December 2004. It was agreed that such a list was very useful and it should be enhanced in order to report open issues to TSG SA Plenary in December 2004. The evening MBMS session were asked to check and enhance this list in TD S3-041060. This updated list was reviewed, the table was updated where information was missing and the document was revised in TD S3-041132. **It was agreed that this list should be submitted to TSG SA Plenary during the SA WG3 Report in order to clarify the status of the MBMS Security work in SA WG3 and expected completion dates.**

TD S3-041064 LS from OMA BAC: Status of OMA Mobile Broadcast Services. This was introduced by the SA WG3 Chairman. OMA BAC asked 3GPP and 3GPP2 to provide feedback on applicability of the preliminary OMA Mobile Broadcast Services architecture to their broadcast-multicast work items. SA WG3 delegates were asked to review the attached documents with regard to the compatibility with the 3GPP Security system. An e-mail discussion was initiated to provide comments to OMA BAC. comments by 13 January 2004, to be transmitted by 20 January 2005. M. Blommaert agreed to run this e-mail discussion group and prepare the draft LS.

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.

TD S3-040898 Revised CR to 33.246: XML protection for download services. This was contributed by Ericsson and was discussed in the MBMS evening sessions and was rejected.

TD S3-041114 MBMS CR Status Update. This was introduced by the MBMS Drafting group secretary (A. Escott) and provided an overview of how the MBMS documents were handled at the evening sessions.

The CRs in table 2, TD S3-041115, TD S3-041010, TD S3-041055, TD S3-041116 and TD S3-041117 were approved.

TD S3-041122 Proposed CR to 33.246: Deletion of MBMS keys stored in the ME (Rel-6). This was introduced by Siemens and was approved.

TD S3-041118 Proposed CR to 33.234: MBMS Transport of salt (Rel-6). This was revised in TD S3-0401125 which was approved.

TD S3-041119 Proposed CR to 33.234: Shorter MKI (Rel-6). This CR was approved.

TD S3-041120 Proposed CR to 33.234: Clarification of the format of MTK ID and MSK ID (Rel-6). This CR was approved.

TD S3-041124 Proposed CR to 33.246: Clarification of MSK key management (Rel-6). This was revised in TD S3-0401126 which was approved.

TD S3-041121 Proposed CR to 33.246: Handling of MBMS identities and definition completion/modification (Rel-6). This was introduced by Siemens on behalf of the MBMS Drafting group. This was revised in TD S3-0401127 which was approved.

TD S3-041123 Proposed CR to 33.246: OMA DRM DCF for protection of download services. This was introduced by Nokia. This was revised in TD S3-0401128 which was approved. An LS to OMA BAC was provided in TD S3-041057.

TD S3-041098 LS on MBMS work progress. This was reviewed and modified in TD S3-041134 which was approved.

6.21 Key Management of group keys for Voice Group Call Services

TD S3-041893 LS (from GERAN WG2) on "Ciphering for Voice Group Call Services". This was introduced by Siemens and was copied to SA WG3 for information. It was reported that SA WG1 had received this LS and noted it without response. SA WG3 noted that their opinion was the same as GERAN WG2.

TD S3-041925 Clarification to VGCS/VBS ciphering mechanism. This was introduced by Siemens and contained two Proposed CRs, one showing the differences to the CR agreed in the previous meeting and a "clean" copy showing only the proposed revisions. The clean version in Attachment 2 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

The SA WG3 Chairman reported that feedback had been received from he SA WG1 chairman that the LS sent from SA WG3 meeting #34 in TD S3-040683 was misleading and seemed to propose that SA WG3 were intending to standardise firewalls, etc. TD S3-040683 was reviewed by SA WG3 and it was thought that another LS should be sent to clarify the intentions of SA WG3. An LS was drafted in TD S3-0401065 which was reviewed and approved.

6.24 Other areas

TD S3-040917 Proposed CR to 21.133: Correction of description of 3G identity (Rel-4). This was introduced by CCSA/ZTE Corporation. This was an editorial correction to the Rel-4 version of 21.133 which was not maintained into subsequent Releases and Editorial CRs are not permitted to this frozen Release. The only way to include this change would therefore be to upgrade the specification to Rel-6, which may create the impression that the specification is being updated in Rel-6, therefore the CR was rejected.

TD S3-040919 Proposed CR to 33.103: Correction of TMUI to TMSI (Rel-4). This was introduced by CCSA/ZTE Corporation and although correct in substance, was rejected for the same reasons as for TD S3-040917.

7 Review and update of work programme

Due to lack of time, this agenda item was not completed. Rapporteurs were asked to review the SA WG3 Work Plan, to be sent out to the SA WG3 e-mail list by the Secretary and respond as quickly as possible with any updates to ensure the accuracy of the Work Plan.

8 Future meeting dates and venues

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#37	21-25 February 2005	Sophia Antipolis	ETSI
S3#38	25 - 29 April 2005	Switzerland (TBC)	Orange (TBC)
S3#39	28 June - 1 July 2005	USA (possibly located with SA WG2)	NAF (TBC)
S3#40	TBD	TBD	Qualcomm

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#16	18 - 20 January 2005	Barcelona, Spain	"European Friends of 3GPP"
SA3 LI-#17	5 - 7 April 2005	Sophia Antipolis, France	ETSI

TSGs RAN/CN/T and SA Plenary meeting schedule

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

9 Any other business

There was no other business signalled at the meeting.

10 Close

The Chairman, V. Niemi, thanked delegates for their hard work during the meeting and for the extra hours in the MBMS evening sessions which were held. He thanked the Hosts, Huawei, for the excellent facilities in Shenzhen, China. He then closed the meeting.

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

A.1 List of attendees

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. SÈbastien Aumonier	OBERTHUR CARD SYSTEMS S.A.	s.aumonier@oberthurcs.com		+33 1 41 38 18 78	+33 1 41 38 48 23	FR	ETSI
Mr. Colin Blanchard	BT Group Plc	colin.blanchard@bt.com	+44 7711 191835	+44 1473 605353	+44 1473 623910	GB	ETSI
Mr. Marc Blommaert	Siemens nv/sa	marc.blommaert@siemens.com		+32 14 25 34 11	+32 14 25 33 39	BE	ETSI
Mr. Charles Brookson	DTI - Department of Trade and Industry	cbrookson@iee.org	+44 20 7215 3691	+44 20 7215 3691	+44 20 7215 1814	GB	ETSI
Mr. Holger Butscheidt	BUNDESMINISTERIUM FUR WIRTSCHAFT	holger.butscheidt@regtp.de		+49 6131 18 2224	+49 6131 18 5613	DE	ETSI
Mr. Mauro Castagno	TELECOM ITALIA S.p.A.	mauro.castagno@telecomitalia.it		+39 0112285203	+39 0112287056	IT	ETSI
Mr. Jing Chen	Zhongxing Telecom Ltd.	chen.jing3@zte.com.cn		+86-75526773000-7163	+86-75526773000-6943	CN	CCSA
Ms. Lily Chen	MOTOROLA A/S	lchen1@email.mot.com		+1 847 632 3033	+1 847 435 2264	DK	ETSI
Mr. Per Christoffersson	TeliaSonera AB	per.christoffersson@teliasonera.com		+46 705 925100		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
Dr. Adrian Escott	Hutchison 3G UK Ltd (3)	adrian.escott@three.co.uk		+44 7782 325254	+44 1628 766012	GB	ETSI
Miss Sylvie Fouquet	ORANGE SA	sylvie.fouquet@francetelecom.com		+33 145 29 49 19	+33 145 29 65 19	FR	ETSI
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
Ms. Yingxin Huang	HuaWei Technologies Co., Ltd	huangyx@huawei.com		+86-10-82882752	+86-10-82882940	CN	CCSA
Mr. Bradley Kenyon	Hewlett-Packard, Centre de CompÈtences France	brad.kenyon@hp.com		+1 402 384 7265	+1 402 384 7030	FR	ETSI
Ms. Tiina Koskinen	Nokia Telecommunications Inc.	tiina.s.koskinen@nokia.com		+358504821347	+358718075300	US	ATIS
Mr. Bernd Lamparter	Telecom Modus Limited	bernd.lamparter@netlab.nec.de		+49 6221 905 11 50	+49 6221 905 11 55	GB	ETSI
Mr. Alex Leadbeater	BT Group Plc	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. Vesa Lehtovirta	Ericsson Incorporated	vesa.lehtovirta@ericsson.com		+358405093314	+	US	ATIS
Ms. CHANGHONG LI	NOKIA Corporation	changhong.li@nokia.com		+358405812138	+358718029400	FI	ETSI
Miss Rui Li	China Communications Standards Association	li.rui2@zte.com.cn		+86-755-26772015	+	CN	CCSA
Mr. Zhuo-ming Li	Zhongxing Telecom Ltd.	li.zhuoming@zte.com.cn		+86-755-26772015	+86-755-26772004	CN	CCSA
Mrs. Fei Liu	China Mobile Communications Corporation (CMCC)	liufei@chinamobile.com	+86 13910036595	+86 10 66006688 3118	+86 10 63600340	CN	CCSA
Prof. Lu chen Lu chen	Zhongxing Telecom Ltd.	lu.chen@zte.com.cn		+86-755-26771910	+86-755-26771910	CN	CCSA
Miss Dongxu Lv	Zhongxing Telecom Ltd.	lv.dongxu@zte.com.cn		+8613590369978	+86-755-26772004	CN	CCSA
Mr. Michael Marcovici	Lucent Technologies	marcovici@lucent.com		+1 630 979 4062	+1 630 224 9955	US	ATIS
Mr. David Mariblanca	Telefon AB LM Ericsson	david.mariblanca@ericsson.com		+34 646004736	+34 913392538	SE	ETSI
Mr. sun min	Zhongxing Telecom Ltd.	sun.min1@zte.com.cn		+862552870448		CN	CCSA
Dr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com		+358504837327	+358718036850	FI	ETSI
Mr. Anand Palanigounder	Nortel Networks (USA)	anand@nortelnetworks.com		+1 972 684 4772	+1 972 685 3123	US	ATIS
Miss Mireille Pauliac	GEMPLUS S.A.	mireille.pauliac@GEMPLUS.COM		+33 4 42365441	+33 4 42365792	FR	ETSI
Mr. Maurice Pope	ETSI Secretariat	maurice.pope@etsi.org	+33 (0)6 07 59 08 49	+33 4 92 94 42 59	+33 4 92 38 52 59	FR	ETSI
Mr. Bengt Sahlin	Ericsson Korea	Bengt.Sahlin@ericsson.com		+358 40 778 4580	+358 9 299 3401	KR	TTA
Mr. Jacques Seif	Axalto S.A.	JSeif@axalto.com		+33146007228	+33146005931	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

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Dajiang Zhang	Nokia Japan Co, Ltd	dajiang.zhang@nokia.com		+86-13901168924	+86-010-84210576	JP	ARIB
Mr. Wenlin Zhang	HUAWEI TECHNOLOGIES Co. Ltd.	zhangwenlin@huawei.com		+86 82882753	+86 82882940	CN	ETSI
Mr. Yan Zhang	China Mobile Communications Corporation (CMCC)	zhangyanyf@chinamobile.com		+86 10 63150300-3047	+86 10 63600340	CN	CCSA
Miss Jeanne Zhao	Zhongxing Telecom Ltd.	zhao.jie@zte.com.cn		+86-755-26772015	+86-755-26772004	CN	CCSA
Mr. Zhifei Zhao	Zhongxing Telecom Ltd.	zhao.zhifei@zte.com.cn		+86-755-26772016	+86-755-26772004	CN	CCSA
Mr. Fenqin Zhu	HUAWEI TECHNOLOGIES Co. Ltd.	zfq@huawei.com		+86-755-89650901	+86-755-26540263	CN	ETSI
Mr. Yanmin Zhu	Samsung Electronics Ind. Co., Ltd.	yanmin.zhu@samsung.com		+86-10-68427711	+86-10-68481891	KR	TTA

45 attendees

Apologies for absence were received from the following 2 people:

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
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. James Semple	QUALCOMM EUROPE S.A.R.L.	jsemple@qualcomm.com		+447880791303		FR	ETSI

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #34, #35, and #36, the following companies are eligible to vote at SA WG3 meeting #37:

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 CompÈtences France	FR	3GPPMEMBER	ETSI
HUAWEI TECHNOLOGIES Co. Ltd.	CN	3GPPMEMBER	ETSI
HuaWei Technologies Co., Ltd	CN	3GPPMEMBER	CCSA
Hutchison 3G UK Ltd (3)	GB	3GPPMEMBER	ETSI
INTEL CORPORATION SARL	FR	3GPPMEMBER	ETSI
Lucent Technologies	US	3GPPMEMBER	ATIS
Lucent Technologies Network Systems UK	GB	3GPPMEMBER	ETSI
Mitsubishi Electric Co.	JP	3GPPMEMBER	ARIB
MOTOROLA A/S	DK	3GPPMEMBER	ETSI
MOTOROLA Ltd	GB	3GPPMEMBER	ETSI
NEC EUROPE LTD	GB	3GPPMEMBER	ETSI
NEC Technologies (UK) Ltd	GB	3GPPMEMBER	ETSI
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
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
OBERTHUR CARD SYSTEMS S.A.	FR	3GPPMEMBER	ETSI
ORANGE SA	FR	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
Research In Motion Limited	CA	3GPPMEMBER	ETSI
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
TeliaSonera AB	SE	3GPPMEMBER	ETSI
T-MOBILE DEUTSCHLAND	DE	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

47 Voting Members

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040890	Draft Agenda for SA WG3 meeting #36	SA WG3 Chairman	2	Approval		Approved
S3-040891	Draft Report of SA WG3 meeting #35	SA WG3 Secretary	4.1	Approval		Approved with minor modification. V1.0.0 to be placed on FTP server
S3-040892	Specs lists per Release; a comparison	TSG SA	4	Action		List to be considered and exceptions listed
S3-040893	LS (from GERAN WG2) on "Ciphering for Voice Group Call Services"	GERAN WG2	6.21	Information		Noted
S3-040894	Response LS (from SA WG1) regarding application selection for GBA	SA WG1	6.9.2	Information		Noted
S3-040895	Reply LS (from SA WG2) on Generic Authentication Architecture (GAA)	SA WG2	6.9.1	Information		Noted
S3-040896	Reply LS (from SA WG2) on Generic Access Network (GAN)	SA WG2	6.5	Information		Noted
S3-040897	Updated: MBMS Download Protection using XML	Ericsson	6.20	Discussion / Decision		Discussed with other related contributions. LS to OMA in S3-041073.
S3-040898	Revised CR to 33.246: XML protection for download services	Ericsson	6.20	Approval		Discussed in MBMS evening session and rejected
S3-040899	MBMS Performance Comparison of DCF and XML-encryption	Ericsson	6.20	Discussion / Decision		Discussed with other related contributions. LS to OMA in S3-041073.
S3-040900	Comparison of DCF and XML encryption for MBMS Download	Ericsson	6.20	Discussion / Decision		Discussed with other related contributions. LS to OMA in S3-041073.
S3-040901	An Update to Using OMA DRM V2.0 DCF for MBMS Download Protection	Nokia	6.20	Discussion / Decision		Discussed with other related contributions. LS to OMA in S3-041073.
S3-040902	Overhead and Performance Comparison of OMA DRM V2.0 DCF and XML for MBMS Download Protection	Nokia	6.20	Discussion		Comments provided in S3-040911
S3-040903	Proposed CR to 33.246: OMA DRM DCF for protection of download services	Nokia	6.20	Approval	S3-041123	Revised in S3-041123
S3-040904	Proposed CR to 33.102: Correction of Abbreviation for USIM (Rel-6)	MCC	6.5	Approval		Approved
S3-040905	Proposed CR to 33.203: Corrections to Section 7.1 & 7.2 (Rel-6)	Lucent Technologies	6.1.1	Approval	S3-041066	To be included in Editorial CR in S3-041066
S3-040906	Pseudo-CR to 33.900: Bluetooth security and configuration considerations for Annex of TR 33.900 (Rel-6)	Toshiba, BT and supporting Companies	6.15	Approval		Convered by S3-041150
S3-040907	Liaison Statement (from SA WG4) on Reception Acknowledgement for MBMS	SA WG4	6.20	Action		Response in S3-041033
S3-040908	Liaison Statement (from SA WG4) on MBMS User Service architecture	SA WG4	6.20	Information		Noted
S3-040909	Comments to Ericsson contribution (S3-040900) on Comparison of DCF and XML encryption for MBMS Download	Nokia	6.20	Discussion		Discussed with other related contributions. LS to OMA in S3-041073.
S3-040910	Required Changes in OMA DRM specifications for using the DCF for MBMS Download protection	Ericsson	6.20	Discussion		Discussed with other related contributions. LS to OMA in S3-041073.
S3-040911	Comments to S3-040902: Overhead and Performance Comparison of OMA DRM V2.0 DCF and XML for MBMS Download Protection	Ericsson	6.20	Discussion		Discussed with other related contributions. LS to OMA in S3-041073.
S3-040912	Draft report of SA WG3 LI Group meeting - Saint Antonio	SA WG3 LI Group	4.2	Information		Noted
S3-040913	SA WG3 LI Group CRs which were agreed at the previous SA WG3 LI meeting	SA WG3 LI Group	4.2	Approval		Review by 30 Nov. If no comment, CRs approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040914	LS from ETSI SAGE: Proposed key derivation function for the Generic Bootstrapping Architecture	ETSI SAGE	5.3	Action	S3-040937	WITHDRAWN - Updated in S3-040937
S3-040915	LS (from T WG2) on EAP Authentication commands for WLAN interworking and improved security for UICC generic access	T WG2	6.10	Action		Contribution in S3-041022. LS out in S3-041149
S3-040916	Correction WRAP to CCMP	CCSA/ZTE Corporation	6.10	Approval		CR in S3-041088
S3-040917	Proposed CR to 21.133: Correction of description of 3G identity (Rel-4)	CCSA/ZTE Corporation	6.24	Approval		Rejected as editorial to Rel-4 not allowed
S3-040918	Proposed CR to 33.102: Correction of TMUI to TMSI in a figure (Rel-6)	CCSA/ZTE Corporation	6.5	Approval		Revised in S3-041071
S3-040919	Proposed CR to 33.103: Correction of TMUI to TMSI (Rel-4)	CCSA/ZTE Corporation	6.24	Approval		Rejected as editorial to Rel-4 not allowed
S3-040920	Proposed CR to 33.234: Update the status of reference IEEE802.11i (Rel-6)	CCSA/ZTE Corporation	6.10	Approval		WITHDRAWN
S3-040921	Pseudo-CR to 33.878: A correction about context relationship	CCSA/ZTE Corporation	6.1.2	Approval		Agreed for inclusion in the draft TR
S3-040922	Efficient Solutions of MSK update	CCSA/ZTE Corporation	6.20	Discussion / Decision		Noted. May be considered for Rel-7
S3-040923	Proposed CR to 33.220: Clarification of GBA_U AUTN generation procedure in the BSF (Rel-6)	Axalto	6.9.2	Approval		Covered by S3-040956
S3-040924	key lifetime of GBA	CCSA/ZTE Corporation	6.9.2	Discussion / Decision		Related CR provided in S3-041086
S3-040925	Clarification to VGCS/VBS ciphering mechanism	Siemens	6.21	Approval		CR in Att2 approved
S3-040926	Proposed CR to 33.817: Bluetooth security and configuration considerations for Annex of TR 33.817 (Rel-6)	Nokia	6.15	Approval	S3-041105	revised in S3-041105
S3-040927	Proposed CR to 33.234: Profile for PDG certificates in Scenario 3 (Rel-6)	Nokia	6.10	Approval	S3-041100	Revised in S3-041100
S3-040928	Proposed CR to 33.234: Confidentiality and integrity canít be both NULL in the IPsec tunnel (Rel-6)	Nokia	6.10	Approval		WITHDRAWN
S3-040929	explanation of PDG certificate profile	Nokia	6.10	Discussion / Decision		CR in S3-041100
S3-040930	TLS Compatibility in IMS	Nortel Networks	6.1.1	Discussion / Decision		Could be studied for Rel-7 onwards
S3-040931	Pseudo-CR to 33.878: Add optional use of IMSI	Nortel Networks	6.1.2	Approval		WITHDRAWN - Covered by S3-041006
S3-040932	Usage of B-TID in reference point Ub	Huawei	6.9.2	Discussion / Decision		Rejected for Rel-6
S3-040933	Update of GUSS in BSF	Huawei	6.9.2	Discussion / Decision		CR in S3-040934
S3-040934	Proposed CR to 33.220: Update of GUSS (Rel-6)	Huawei	6.9.2	Approval		Rejected
S3-040935	Proposed CR to 33.102: Support of algorithms in UEs (Rel-6)	Nokia	6.6	Approval	S3-041029	Revised proposal in S3-041029
S3-040936	LS from CN WG4: The relationship between Scenario 2 and Scenario 3 authentication procedures	CN WG4	6.10	Action		WITHDRAWN - Repeated in S3-041045
S3-040937	LS from ETSI SAGE: Proposed key derivation function for the Generic Bootstrapping Architecture	ETSI SAGE	6.9.2	Action		Assumptions confirmed.
S3-040938	Optimization of de-registration	Huawei	6.1.2	Discussion / Decision		Included in S3-01069
S3-040939	Pseudo-CR to 33.878: Correction of figures	Huawei	6.1.2	Approval		Agreed to be included in the draft TR
S3-040940	Key freshness in GBA	3	6.9.2	Discussion / Decision		Not agreed for Rel-6
S3-040941	Proposed CR to 33.220: Enhanced key freshness in GBA (Rel-6)	3	6.9.2	Approval		Withdrawn as proposal in S3-040940 was not agreed
S3-040942	Proposed CR to 33.220: Adding a note about replay protection (Rel-6)	3	6.9.2	Discussion / Decision	S3-041087	Revised in S3-041087
S3-040943	Control of simultaneous session in WLAN 3GPP IP access (scenario 3)	Ericsson, Siemens	6.10	Discussion / Decision		LS to affected groups in S3-041112
S3-040944	Proposed CR to 33.234: Control of simultaneous sessions in WLAN 3GPP IP access (Rel-6)	Ericsson, Siemens	6.10	Approval	S3-041112	Revised in S3-041112

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040945	Proposed CR to 33.234: Completion of definition and abbreviations (Rel-6)	Ericsson	6.10	Approval	S3-041109	Revised in S3-041109
S3-040946	Proposed CR to 33.234: Fallback from re-authentication to full authentication (Rel-6)	Ericsson	6.10	Approval	S3-041110	Revised in S3-041110
S3-040947	Proposed CR to 33.234: Clarification on the use of IMSI in WLAN 3GPP IP access (Rel-6)	Ericsson	6.10	Approval		Approved
S3-040948	Proposed CR to 33.234: Clarification on the use of MAC addresses (Rel-6)	Ericsson	6.10	Approval	S3-041113	Revised in S3-041113
S3-040949	Proposed CR to 33.234: Clarification on the use of IMSI in WLAN 3GPP IP access (Rel-6)	Ericsson	6.10	Approval		Approved
S3-040950	GBA_U: GBA_U derivations	Gemplus, Axalto, Oberthur	6.9.2	Discussion / Decision		Noted. CR in S3-040951
S3-040951	Proposed CR to 33.220: Optimization of the GBA_U key derivation procedure (Rel-6)	Gemplus, Axalto, Oberthur	6.9.2	Approval	S3-041136	Revised in S3-041136
S3-040952	Proposed CR to 33.220: Requirement on ME capabilities for GBA_U (Rel-6)	Gemplus, Axalto, Oberthur	6.9.2	Approval	S3-041180	Revised in S3-041080
S3-040953	Proposed CR to 33.220: GBA_U ..GBA_U: storage of Ks_ext in the UICC (Rel-6)	Gemplus, Axalto, Oberthur	6.9.2	Approval		Withdrawn as S3-040951 was approved
S3-040954	Proposed CR to 33.200: SMS fraud countermeasures (Rel-6)	Siemens	6.2	Approval	S3-041070	Revised in S3-041070
S3-040955	Proposed CR to 43.020: Clarifying the mandatory support of A5 algorithms within mobile stations (Rel-6)	Siemens	6.6	Approval		Update in S3-041028
S3-040956	Proposed CR to 33.220: Complete the MAC modification for GBA_U (Rel-6)	Siemens	6.9.2	Approval	S3-041078	Revised in S3-041078
S3-040957	Proposed CR to 33.234: Clarification on storage of Temporary Identities in UICC (Rel-6)	Samsung	6.10	Approval		Included in S3-041104
S3-040958	Proposed CR to 33.234: Wn Reference Point Description (Rel-6)	Samsung, Nokia, Ericsson	6.10	Approval		Approved
S3-040959	Proposed CR to 33.234: Removal of word ìscenarioî (Rel-6)	Samsung, Nokia	6.10	Approval		Approved
S3-040960	MBMS MSK management	Samsung	6.20	Discussion / Decision	S3-041023	Revised in S3-041023
S3-040961	Proposed CR to 33.246: MBMS MSK management (Rel-6)	Samsung	6.20	Approval		Revised in S3-041131
S3-040962	Including AES in the TLS profile of TS 33.222	Ericsson	6.9.4	Discussion / Decision		Noted. CR in S3-040963
S3-040963	Proposed CR to 33.222: Adding Support for AES in the TLS Profile (Rel-6)	Ericsson	6.9.4	Approval	S3-041092	Revised in S3-041092
S3-040964	Postponing PSK TLS to 3GPP rel-7	Ericsson	6.9.4	Discussion / Decision		TSG SA to be asked to decide whether to remove TLS from Rel-6. LS in S3-041095
S3-040965	Proposed CR to 33.222: Removing PSK TLS from 3GPP rel-6 (Rel-6)	Ericsson	6.9.4	Approval		Approved (depends on SA decision)
S3-040966	Proposed CR to 33.222: Clean-up of TS 33.222 (Rel-6)	Ericsson	6.9.4	Approval		To be included in other CRs
S3-040967	Detecting a falsified SMSC address	Nokia	6.2	Discussion / Decision		Needs more study and justification and CR proposal
S3-040968	Certificate management for TLS connections between IMS and non-IMS networks	Nokia	6.4	Discussion / Decision		Noted. WID expected for next meeting
S3-040969	Security context separation	Nokia	6.6	Discussion / Decision		Postponed to next meeting
S3-040970	Key separation mechanism in GSM/GPRS	Orange, Nokia	6.6	Discussion / Decision		Postponed to next meeting
S3-040971	Response to S3_040911: Comments to S3-040902: Overhead and Performance Comparison of OMA DRM V2.0 DCF and XML for MBMS Download Protection	Nokia	6.20	Discussion		Discussed with other related contributions. LS to OMA in S3-041073.
S3-040972	Proposed CR to 33.246: Clarification of MSK key management (Rel-6)	Nokia	6.20	Approval		Revised in MBMS evening sessions to include other CRs in S3-041124

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040973	Pseudo-CR to 33.878 Impact on network entity considering the interworking requirement	Huawei	6.1.2	Discussion / Decision		Not accepted for Rel-6. Note from point 1 to be included in draft TR. Roaming mechanism to be studied further for Rel-7
S3-040974	Pseudo-CR to 33.878: Clarifications and corrections to Early IMS Security TR	Ericsson	6.1.2	Approval		Figure changes covered by S3-041006. Other changes agreed for inclusion in the draft TR
S3-040975	Proposed CR to 33.222: Authorization flag transfer between AP and AS (Rel-6)	Nokia, Siemens	6.9.4	Approval		Combined with S3-040735 in S3-041093
S3-040976	Proposed CR to 33.220: No GUSS/USS update procedures in Release-6 (Rel-6)	Nokia, Siemens	6.9.2	Approval	S3-041089	Revised in S3-041089
S3-040977	Proposed CR to 33.919: Removal of unnecessary editor's notes (Rel-6)	Nokia	6.9.1	Approval		Approved
S3-040978	Proposed CR to 33.220: Removal of unnecessary editor's notes (Rel-6)	Nokia	6.9.2	Approval	S3-041082	Revised in S3-041082
S3-040979	Proposed CR to 33.221: Editorial correction (Rel-6)	Nokia	6.9.3	Approval		Approved
S3-040980	Liberty and GAA relationship	Nokia	6.9.1	Information		Noted. Comments in S3-041039
S3-040981	Proposed CR to 33.220: GBA USIM/ISIM selection (Rel-6)	Nokia	6.9.2	Approval	S3-041085	Revised in S3-041085
S3-040982	Proposed CR to 33.220: Key lifetime clarifications (Rel-6)	Nokia	6.9.2	Approval		Not supported for Rel-6
S3-040983	Adoption of key separation for GSM/GPRS in the short term	Orange	6.6	Discussion / Decision		LS to SAGE in s3-041076
S3-040984	Proposed CR to 33.246: Clarification of MSK key management (Rel-6)	Orange	6.20	Approval		Revised in MBMS evening sessions to include other CRs in S3-041124
S3-040985	Proposed CR to 33.222: Correction of inconsistencies within AP specification (Rel-6)	Siemens	6.9.4	Approval		Approved
S3-040986	Proposed CR to 33.220: Fetching of one AV only on each Zh run between BSF and HSS (Rel-6)	Siemens, Nokia	6.9.2	Approval	S3-041090	Revised in S3-041090
S3-040987	Introduction of NAF groups	Siemens	6.9.2	Discussion / Decision		Attachment 2 revised in S3-01135
S3-040988	Proposed CR to 33.220: Clean up of TS 33.220 (Rel-6)	Ericsson	6.9.2	Approval	S3-041083	Revised in S3-041083
S3-040989	IETF status report on HTTP Digest AKAv2	Ericsson	5.2	Information		Noted
S3-040990	IMS security extensions	Ericsson	6.1.1	Discussion		WID in S3-040991, Comments in S3-031038. e-mail discussion to be held
S3-040991	Proposed WID: IMS security extensions	Ericsson	6.1.1	Discussion / Decision		Discussion paper in S3-040990, Comments in S3-031038. e-mail discussion to be held
S3-040992	The need for and use of salt in MBMS streaming (Updated)	Ericsson, TeliaSonera	6.20	Discussion / Decision	S3-041118	Updated after evening session in S3-041118
S3-040993	Proposed CR to 33.246: Shorter MKI (Rel-6)	Ericsson	6.20	Approval	S3-041019	WITHDRAWN - WRONG CR NUMBER
S3-040994	Proposed CR to 33.246: Removal of ID_i in MIKEY response messages for MSKs (Rel-6)	Ericsson	6.20	Approval	S3-041020	WITHDRAWN - WRONG CR NUMBER
S3-040995	IETF work needed for MBMS security	Ericsson	6.20	Discussion / Decision		Approved to be added to the IETF dependency list. RFC should be made available as soon as possible
S3-040996	MUK ID and UE ID in MBMS	Ericsson	6.20	Discussion / Decision	S3-041021	WITHDRAWN - WRONG CR NUMBER
S3-040997	Replacing Network ID with NAF ID	Ericsson	6.20	Discussion / Decision		included in other CRs in the MBMS evening sessions and this CR was rejected.

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040998	Pseudo-CR to 33.878: UE behaviour when a UICC containing an ISIM is present	Vodafone	6.1.2	Approval		Agreed for inclusion in the draft TR
S3-040999	Pseudo-CR to 33.878: Removal of remaining Editorís Notes	Vodafone	6.1.2	Approval		Agreed to be included in the draft TR
S3-041000	Pseudo-CR to 33.878: Completion of introductory sections and other editorial changes	Vodafone	6.1.2	Approval		Agreed for inclusion in the draft TR
S3-041001	Proposed CR to 33.203: Addition of reference to early IMS security TR (Rel-6)	Vodafone	6.1.2	Approval	S3-041130	Revised in S3-041130
S3-041002	Proposed CR to 33.817: Terminology update to not rule out the use of the smart card for security enhancements (Rel-6)	Gemplus	6.15	Approval	S3-041107	Revised in S3-041107
S3-041003	Update of S3-040838	Gemplus	6.10	Discussion / Decision	S3-041106	Revised in S3-041106
S3-041004	Pseudo-CR to 33.878: Correction of idle timer-related issues	Siemens	6.1.2	Approval		Covered by S3-041030
S3-041005	Pseudo-CR to 33.878: Clarification of IP address related issue	Siemens	6.1.2	Approval		Covered by S3-041031
S3-041006	Pseudo-CR to 33.878: Correction of identity related issues	Siemens	6.1.2	Approval		Agreed for inclusion in the draft TR
S3-041007	Pseudo-CR to 33.878: Different versions of IMS	Siemens	6.1.2	Approval		Agreed for inclusion in the draft TR. Note to be added about restriction to home case and a note from point 1 of S3-040973 to be included
S3-041008	Proposed CR to 33.246: Clarify the use of mandatory MIKEY features for MBMS (Rel-6)	Siemens	6.20	Approval	S3-041055	Revised in S3-041055
S3-041009	Proposed CR to 33.246: Specify CSB-ID format (Rel-6)	Siemens	6.20	Approval		included in other CRs in the MBMS evening sessions and this CR was rejected.
S3-041010	Proposed CR to 33.246: Clarifying ME capabilities (Rel-6)	Siemens	6.20	Approval	S3-041018	Revised in S3-041018
S3-041011	Reliable MSK updating	Siemens	6.20	Discussion / Decision	S3-041122	Revised in S3-041122
S3-041012	MUK ID	Siemens	6.20	Discussion / Decision		included in other CRs in the MBMS evening sessions and this CR was rejected.
S3-041013	Early IMS indication	Nokia	6.1.2	Approval		Not agreed
S3-041014	Revised WID: Access Security Review	Ericsson	6.6	Approval	S3-041077	Revised in S3-041077
S3-041015	Access Security Review	Ericsson	6.6	Discussion / Decision		Noted. Contributions expected on this proposed WI requested
S3-041016	Correction of WLAN UE function split, Cover letter to attached CR	Gemplus, Siemens, T-mobile	6.10	Discussion / Decision		WITHDRAWN - REVISED IN S3-041022
S3-041017	Key group ID and MSK ID	Ericsson	6.20	Discussion / Decision	S3-041041	Revised in S3-041041
S3-041018	CR corrections	Ericsson	6.20	Discussion / Decision		CR005R2 revised in S3-041115, CR007R4 approved, CR008R2 rejected, CR016R2 revised in S3-041116, CR018R3 revised in S3-041120, CR020R2 revised in S3-041117, CR021R5 revised in S3-041124.
S3-041019	Proposed CR to 33.246: Shorter MKI (Rel-6)	Ericsson	6.20	Approval	S3-041119	Revised by MBMS drafting group in S3-041119
S3-041020	Proposed CR to 33.246: Removal of ID_i in MIKEY response messages for MSKs (Rel-6)	Ericsson	6.20	Approval		Included in CR030 (S3-041021). This CR was then rejected
S3-041021	MUK ID and UE ID in MBMS	Ericsson	6.20	Discussion / Decision		Further proposals in S3-041012
S3-041022	Correction of WLAN UE function split, Cover letter to attached CR	Axalto, Gemplus, Siemens, T-mobile	6.10	Discussion / Decision	S3-041103	Attached CR Revised in S3-041103

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-041023	MBMS MSK management	Samsung	6.20	Discussion / Decision		Discussed. Related CR in S3-040961
S3-041024	Proposed CR to 33.220: New key management for ME based GBA keys (Rel-6)	Nokia	6.9.2	Approval	S3-041084	Revised in S3-041084
S3-041025	Proposed CR to 33.222: TLS extensions support (Rel-6)	Nokia	6.9.4	Approval	S3-041096	Revised in S3-041096
S3-041026	Proposed CR to 33.222: Visited AS using subscriber certificates (Rel-6)	Nokia	6.9.4	Approval		Approved
S3-041027	Proposed CR to 33.220: Key derivation function (Rel-6)	Nokia	6.9.2	Approval	S3-041081	Revised in S3-041081
S3-041028	Vodafone comments to S3-040955: Proposed CR to 43.020: Clarifying the support of algorithms within mobile stations (Rel-6)	Vodafone	6.6	Approval		CR revised in S3-041075
S3-041029	Vodafone comments to S3-040935: Proposed CR to 33.102: Support of algorithms in UEs (Rel-6)	Vodafone	6.6	Approval	S3-041033	Updated in S3-041033
S3-041030	Vodafone comments to S3-041004: Pseudo-CR to 33.878: Correction of idle timer-related issues	Vodafone	6.1.2	Approval		Revised after off-line discussion in S3-041069
S3-041031	Vodafone comments to S3-041005: Pseudo-CR to 33.878: Clarification of IP address related issue	Vodafone	6.1.2	Approval		Agreed for inclusion in the draft TR
S3-041032	Reply (from CN WG4) to LS on Reply to Evaluation of the alternatives for SMS fraud countermeasures	CN WG4	6.2	Information	S3-041044	Approved version in S3-041044
S3-041033	Siemens comments to S3-0401029 and S3-040935: Proposed CR to 33.102: Support of algorithms in UEs (Rel-6)	Siemens	6.6	Approval	S3-041073	Revised in S3-041073
S3-041034	Liaison Statement (from IREG): Request for Comments on Proposed Security Enhancements to GSM/GPRS Networks	GSMA IREG	6.6	Information		Noted
S3-041035	Response LS (from SA WG2) on GUP Security Recommendations	SA WG2	6.17	Action		Response LS in S3-041099
S3-041036	LS (from SA WG2) on Security Aspects of Early IMS Systems	SA WG2	6.1.2	Action		Response in S3-041045
S3-041037	LS from SA WG2: RE: The relationship between Scenario 2 and Scenario 3 authentication procedures	SA WG2	6.10	Information		N oted. Included in response in S3-041101
S3-041038	BT Comments on S3-040990: IMS security extensions	BT Group plc	6.1.1	Discussion / Decision		Discussion paper in S3-040990, WID in S3-040991. e-mail discussion to be held
S3-041039	Ericsson Comments to Nokia's TD S3-040980 on "Liberty and GAA relationship"	Ericsson	6.9.1	Information		Silke to provide WID for Liberty Alliance work co-ordination
S3-041040	Comments from Nokia on S3-041014: Revised WID: Access Security Review	Nokia	6.6	Approval		WID revised in S3-041077
S3-041041	Update of S3-041017: Key group ID and MSK ID	Ericsson	6.20	Discussion / Decision		CR021R6 Revised by drafting group in S3-041124
S3-041042	LATE_DOC: General comment contribution to MBMS: Feature list to complete MBMS in Release 6	Ericsson	6.20	Discussion / Decision	S3-041060	List to be checked and enhanced in off-line session for submission to TSG SA to clarify open issues. Updated in S3-041060
S3-041043	Comments on S3-040940, 941, 942 on ìKey freshness in GBAî (all by ì3î) and on S3-041024 ìNew key management for ME based GBA keysî (by Nokia)	Siemens	6.9.2	Discussion / Decision		WITHDRAWN - replaced in S3-041049
S3-041044	Reply (from CN WG4) to LS on Reply to Evaluation of the alternatives for SMS fraud countermeasures	CN WG4	6.2	Information		Noted. Contributions to next meeting to provide response LS
S3-041045	LS from CN WG4: The relationship between Scenario 2 and Scenario 3 authentication procedures	CN WG4	6.10	Action		Response in S3-041101
S3-041046	LS from CN WG4: Need for the IMSI at the PDG	CN WG4	6.10	Action		Response in S3-041102
S3-041047	Reply LS (from CN WG4) on Security aspects of early IMS systems	CN WG4	6.1.2	Action		proposal from Vodafone in S3-041063

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-041048	Reply LS (from CN WG1) on Security aspects of early IMS systems	CN WG1	6.1.2	Action		proposal from Vodafone in S3-041061
S3-041049	Comments on S3-040940, 941, 942 on ìKey freshness in GBAî (all by ì3î) and on S3-040982 ìKey lifetime clarificationsî (by Nokia)	Siemens	6.9.2	Discussion / Decision		Noted
S3-041050	Proposed WID: Development of UEA2 and UIA2	Teliasonera	6.5	Approval		WITHDRAWN - replaced in S3-041051
S3-041051	Proposed WID: Development of UEA2 and UIA2	Teliasonera	6.5	Approval		Revised in S3-041072
S3-041052	Pseudo-CR to 33.878: Clarification of issues raised in LS from SA2 (S3-041036)	Siemens	6.1.2	Approval		Agreed for inclusion in the draft TR
S3-041053	LS (from CN WG3) on CN3 impacts on Early IMS Security mechanisms	CN WG3	6.1.2	Action		N4-040881 agreed, N4-040882 not accepted. Response LS in S3-041067
S3-041054	Reply Liaison Statement (from SA WG2) on Reception Acknowledgement for MBMS	SA WG2	6.20	Information		Noted
S3-041055	Proposed CR to 33.246: Clarify the use of mandatory MIKEY features for MBMS (Rel-6)	Siemens	6.20	Approval		Approved
S3-041056	Reply LS (from SA WG5) on Reception Acknowledgement for MBMS Charging	SA WG5	6.20	Information		Noted
S3-041057	LS to OMA DOWNLOAD on DRM for MBMS	SA WG3	6.20	Approval		Revised in S3-041129
S3-041058	Reply LS (from SA WG2) on Revisiting forwards compatibility towards TLS based access security	SA WG2	6.1.1	Action		Noted. CR in S3-040886 not approved
S3-041059	Response LS on Reception Acknowledgement for MBMS	SA WG3	6.20	Approval		Revised in S3-041133
S3-041060	General comment contribution to MBMS: Feature list to complete MBMS in Release 6	Ericsson	6.20	Discussion / Decision		Revised in S3-041132
S3-041061	Pseudo-CR to 33.878: Detailed specification of registration and authentication procedures based on LS from CN1 (S3-041048)	Vodafone	6.1.2	Approval		Principles agreed to be included in the draft TR
S3-041062	Pseudo-CR to 33.878: Specification of GGSN-HSS interaction based on LS from CN3 (S3-041053)	Vodafone	6.1.2	Approval		Included in part when aligned with other contributions
S3-041063	Pseudo-CR to 33.878: Impact on Cx interface based on LS from CN4 (S3-041047)	Vodafone	6.1.2	Approval		Agreed for inclusion in the draft TR
S3-041064	LS from OMA BAC: Status of OMA Mobile Broadcast Services	OMA BAC	6.20	Action		M Blommaert to run e-mail discussion and create LS response
S3-041065	LS on Clarification of SA3 work on Selective Disabling of UE Capabilities WI	SA WG3	6.23	Approval		Approved
S3-041066	Proposed CR to 33.203: Editorial corrections (Rel-6)	Vodafone	6.1.2	Approval	S3-041143	Revised in S3-041143
S3-041067	[DRAFT] LS on ~~key separation for GSM/GPRS encryption algorithms~~ impacts of early IMS security mechanisms	SA WG3	6.1.2	Approval	S3-041144	Revised in S3-041144
S3-041068	LS to SA2 on Early IMS issues	SA WG3	6.1.2	Approval	S3-041145	Revised in S3-041145
S3-041069	revised S3-041030: Pseudo-CR to 33.878: Correction of idle timer-related issues	Guenther	6.1.2	Approval		Agreed for inclusion in draft TR
S3-041070	Proposed CR to 33.200: SMS fraud countermeasures (Rel-6)	Siemens	6.2	Approval		Approved
S3-041071	Proposed CR to 33.102: Correction of TMUI to TMSI in a figure (Rel-6)	CCSA/ZTE Corporation	6.5	Approval		Approved
S3-041072	Proposed WID: Development of UEA2 and UIA2	Teliasonera	6.5	Approval		Approved
S3-041073	Siemens comments to S3-0401029 and S3-040935: Proposed CR to 33.102: Support of algorithms in UEs (Rel-6)	Siemens	6.6	Approval		Approved
S3-041074	reserved Siemens Early IMS					Agreed for inclusion in draft TR
S3-041075	Vodafone comments to S3-040955: Proposed CR to 43.020: Clarifying the support of algorithms within mobile stations (Rel-6)	Vodafone	6.6	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-041076	[DRAFT] LS on key separation for GSM/GPRS encryption algorithms	SA WG3	6.6	Approval	S3-041146	Revised in S3-01146
S3-041077	Proposed WID: Access Security Enhancements	SA WG3	6.6	Approval		Approved
S3-041078	Proposed CR to 33.220: Complete the MAC modification for GBA_U (Rel-6)	Siemens	6.9.2	Approval		Approved
S3-041079	Proposed CR to 33.220: Clarify the number of NAF-specific keys stored in the UE per NAF-Id (Rel-6)	Gemplus, Axalto, Oberthur	6.9.2	Approval	S3-041137	Revised in S3-01137
S3-041080	Proposed CR to 33.220: Requirement on ME capabilities for GBA_U (Rel-6)	Gemplus, Axalto, Oberthur	6.9.2	Approval		Approved
S3-041081	Proposed CR to 33.220: Key derivation function (Rel-6)	Nokia	6.9.2	Approval		Approved
S3-041082	Proposed CR to 33.220: Removal of unnecessary editor's notes (Rel-6)	Nokia	6.9.2	Approval		Approved
S3-041083	Proposed CR to 33.220: Clean up of TS 33.220 (Rel-6)	Ericsson	6.9.2	Approval		Approved
S3-041084	Proposed CR to 33.220: New key management for ME based GBA keys (Rel-6)	Nokia	6.9.2	Approval		Approved
S3-041085	Proposed CR to 33.220: GBA USIM/ISIM selection (Rel-6)	Nokia	6.9.2	Approval		Approved
S3-041086	Proposed CR to 33.220: Re-negotiation of keys (Rel-6)	Siemens, ZTE	6.9.2	Approval	S3-041140	Revised in S3-041140
S3-041087	Proposed CR to 33.220: Adding a note about replay protection (Rel-6)	3	6.9.2	Discussion / Decision		Approved
S3-041088	Proposed CR to 33.220: Correction of WRAP to CCMP (Rel-6)	CCSA/ZTE Corporation	6.10	Approval	S3-041108	Revised in S3-041108
S3-041089	Proposed CR to 33.220: No GUSS/USS update procedures in Release-6 (Rel-6)	Nokia, Siemens	6.9.2	Approval		Approved
S3-041090	Proposed CR to 33.220: Fetching of one AV only on each Zh run between BSF and HSS (Rel-6)	Siemens, Nokia	6.9.2	Approval		Approved
S3-041091	Updated TR 33.878	Peter H	6.1.1	Approval		TR 33.878v0.4.0 approved to be sent to TSG SA for approval (MCC to create v1.0.0)
S3-041092	Proposed CR to 33.222: Adding Support for AES in the TLS Profile (Rel-6)	Ericsson	6.9.4	Approval		Approved
S3-041093	Proposed CR to 33.222: Authorization flag transfer between AP and AS (Rel-6)	Nokia	6.9.3	Approval		Approved
S3-041094	Proposed CR to 33.222: Keeping PSK TLS in 3GPP rel-6 (Rel-6)	Nokia	6.9.3	Approval	S3-041142	Revised in S3-041142
S3-041095	DRAFT LS Request for advise on handling IETF draft for R6	SA WG3	6.9.3	Approval	S3-041141	Revised in S3-041141
S3-041096	Proposed CR to 33.222: TLS extensions support (Rel-6)	Nokia	6.9.4	Approval		Approved
S3-041097	MBMS Drafting group report	Adrian/Marc	6.20	Information		Noted
S3-041098	LS on MBMS work progress	SA WG3	6.20	Approval	S3-041134	Revised in S3-041134
S3-041099	LS to SA WG2: Response to S3-041035	Bengt	6.17	Approval	S3-041154	Revised in S3-041154
S3-041100	Proposed CR to 33.234: Profile for PDG certificates in Scenario 3 (Rel-6)	Nokia	6.10	Approval		Approved
S3-041101	Response LS to CN WG4: The relationship between Scenario 2 and Scenario 3 authentication procedures	SA WG3	6.10	Approval	S3-041147	Revised in S3-041147
S3-041102	Response LS to CN WG4: Response to 1046	David	6.10	Approval	S3-041148	Revised in S3-041148
S3-041103	Correction of WLAN UE function split, Cover letter to attached CR	Axalto, Gemplus, Siemens, T-mobile	6.10	Discussion / Decision	S3-041104	Revised (clean up) in S3-041104
S3-041104	Correction of WLAN UE function split, Cover letter to attached CR	Axalto, Gemplus, Siemens, T-mobile	6.10	Discussion / Decision	S3-041149	Revised in S3-041149
S3-041105	Proposed CR to 33.817: Bluetooth security and configuration considerations for Annex of TR 33.817 (Rel-6)	Nokia	6.15	Approval	S3-041150	Revised in S3-041150
S3-041106	Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces) (Rel-6)	Gemplus	6.10	Discussion / Decision	S3-041151	Revised in S3-041151
S3-041107	Proposed CR to 33.817: Terminology update to not rule out the use of the smart card for security enhancements (Rel-6)	Gemplus	6.15	Approval	S3-041152	Revised in S3-041152

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-041108	Proposed CR to 33.234: Correction of WRAP to CCMP (Rel-6)	CCSA/ZTE Corporation	6.10	Approval		Approved
S3-041109	Proposed CR to 33.234: Completion of definition and abbreviations (Rel-6)	Ericsson	6.10	Approval		Approved
S3-041110	Proposed CR to 33.234: Fallback from re-authentication to full authentication (Rel-6)	Ericsson	6.10	Approval		Approved
S3-041111	LS on Control of simultaneous sessions in WLAN 3GPP IP access	David	6.10	Approval		Approved
S3-041112	Proposed CR to 33.234: Control of simultaneous sessions in WLAN 3GPP IP access (Rel-6)	Ericsson, Siemens	6.10	Approval	S3-041153	Revised in S3-041153
S3-041113	Proposed CR to 33.234: Clarification on the use of MAC addresses (Rel-6)	Ericsson	6.10	Approval	S3-041138	Revised in S3-041138
S3-041114	MBMS CR Status Update	MBMS Drafting group	6.20	Information		Noted
S3-041115	Proposed CR to 33.234: Clean up of MBMS TS (Rel-6)	MBMS Drafting group	6.20	Approval		Approved
S3-041116	Proposed CR to 33.234: Scope of MBMS security (Rel-6)	MBMS Drafting group	6.20	Approval		Approved
S3-041117	Proposed CR to 33.234: MTK update procedure for streaming services (Rel-6)	MBMS Drafting group	6.20	Approval		Approved
S3-041118	Proposed CR to 33.234: MBMS Transport of salt (Rel-6)	MBMS Drafting group	6.20	Approval	S3-041125	Revised in S3-041125
S3-041119	Proposed CR to 33.234: Shorter MKI (Rel-6)	MBMS Drafting group	6.20	Approval		Approved
S3-041120	Proposed CR to 33.234: Clarification of the format of MTK ID and MSK ID (Rel-6)	MBMS Drafting group	6.20	Approval		Approved
S3-041121	Proposed CR to 33.246: Handling of MBMS identities and definition completion/modification (Rel-6)	MBMS Drafting group	6.20	Approval	S3-041127	Revised in S3-041127
S3-041122	Proposed CR to 33.246: Deletion of MBMS keys stored in the ME (Rel-6)	MBMS Drafting group	6.20	Discussion / Decision		Approved
S3-041123	Proposed CR to 33.246: OMA DRM DCF for protection of download services	Nokia	6.20	Approval	S3-041128	Revised in S3-041128
S3-041124	Proposed CR to 33.246: Clarification of MSK key management (Rel-6)	MBMS Drafting group	6.20	Approval	S3-041126	Revised in S3-041126
S3-041125	Proposed CR to 33.234: MBMS Transport of salt (Rel-6)	MBMS Drafting group	6.20			Approved
S3-041126	Proposed CR to 33.246: Clarification of MSK key management (Rel-6)	MBMS Drafting group	6.20	Approval		Approved
S3-041127	Proposed CR to 33.246: Handling of MBMS identities and definition completion/modification (Rel-6)	MBMS Drafting group	6.20	Approval		Approved
S3-041128	Proposed CR to 33.246: OMA DRM DCF for protection of download services	Nokia	6.20	Approval		Approved
S3-041129	LS to OMA DOWNLOAD on DRM for MBMS	SA WG3	6.20	Approval		Approved. S3-041128 and TS 33.246 attached
S3-041130	Proposed CR to 33.203: Addition of reference to early IMS security TR (Rel-6)	Vodafone	6.1.2	Approval		SA to be asked if a CR is acceptable
S3-041131	Proposed CR to 33.246: MBMS MSK management (Rel-6)	Samsung	6.20	Approval		e-mail discussion to develop this proposal for next meeting
S3-041132	General comment contribution to MBMS: Feature list to complete MBMS in Release 6	Ericsson	6.20	Discussion / Decision		Agreed to forward this list to TSG SA Plenary
S3-041133	Response LS on Reception Acknowledgement for MBMS	SA WG3	6.20	Approval		Approved
S3-041134	LS on MBMS work progress	SA WG3	6.20	Approval		Approved
S3-041135	Proposed CR to 33.220: GBA User Security Settings (GUSS) usage in GAA and Introduction of NAF groups (Rel-6)	Nokia, Siemens	6.9.2	Approval		Approved.
S3-041136	Proposed CR to 33.220: Optimisation of the GBA_U key derivation procedure (Rel-6)	Gemplus, Axalto, Oberthur	6.9.2	Approval		Approved
S3-041137	Proposed CR to 33.220: Clarify the number of NAF-specific keys stored in the UE per NAF-Id (Rel-6)	Gemplus, Axalto, Oberthur	6.9.2	Approval		Approved
S3-041138	Proposed CR to 33.234: Clarification on the use of MAC addresses (Rel-6)	Ericsson	6.10	Approval		Approved
S3-041139	Proposed CR to 33.234: WLAN removal of Editors' notes (Rel-6)	MCC	6.10	Approval	S3-041155	Revised in S3-041155

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-041140	Proposed CR to 33.220: Re-negotiation of keys (Rel-6)	Siemens, ZTE	6.9.2	Approval		Approved
S3-041141	LS Request for advise on handling IETF draft for Rel-6	SA WG3	6.9.3	Approval		Approved
S3-041142	Proposed CR to 33.222: Keeping PSK TLS in 3GPP rel-6 (Rel-6)	Nokia	6.9.3	Approval		Approved
S3-041143	Proposed CR to 33.203: Editorial corrections (Rel-6)	Vodafone	6.1.2	Approval		Approved
S3-041144	~~LS on key separation for GSM/GPRS encryption algorithms~~ LS on impacts of early IMS security mechanisms	SA WG3	6.1.2	Approval		Approved
S3-041145	LS to SA2 on Early IMS issues	SA WG3	6.1.2	Approval		Approved
S3-041146	LS on key separation for GSM/GPRS encryption algorithms	SA WG3	6.6	Approval		Approved
S3-041147	Response LS to CN WG4: The relationship between Scenario 2 and Scenario 3 authentication procedures	SA WG3	6.10	Approval		Approved
S3-041148	Reply to LS on Need for the IMSI at the PDG	SA WG3	6.10	Approval		Approved
S3-041149	Proposed CR to 33.234: Correction of WLAN UE function split (Rel-6)	Axalto, Gemplus, Siemens, T-mobile	6.10	Approval		Approved
S3-041150	Proposed CR to 33.817: Bluetooth security and configuration considerations for Annex of TR 33.817 (Rel-6)	Nokia	6.15	Approval		Approved
S3-041151	Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces) (Rel-6)	Toshiba, BT and supporting Companies	6.10	Discussion / Decision		Approved
S3-041152	Proposed CR to 33.817: Terminology update to not rule out the use of the smart card for security enhancements (Rel-6)	Gemplus	6.15	Approval		Approved
S3-041153	Proposed CR to 33.234: Control of simultaneous sessions in WLAN 3GPP IP access (Rel-6)	Ericsson, Siemens	6.10	Approval		Approved
S3-041154	LS to SA WG2: Response to S3-041035	SA WG3	6.17	Approval		Approved
S3-041155	Proposed CR to 33.234: WLAN removal of Editors' notes (Rel-6)	MCC	6.10	Approval		Approved

Annex C: Status of specifications under SA WG3 responsibility

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
Release 1999 GSM Specifications and Reports							
TR	01.31	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	8.0.0	R99	S3	WRIGHT, Tim	.
TR	01.33	Lawful Interception requirements for GSM	8.0.0	R99	S3	MCKIBBEN, Bernie	.
TS	01.61	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	8.0.0	R99	S3	WALKER, Michael	.
TS	02.09	Security aspects	8.0.1	R99	S3	CHRISTOFFERSSON, Per	.
TS	02.33	Lawful Interception (LI); Stage 1	8.0.1	R99	S3	MCKIBBEN, Bernie	.
TS	03.20	Security-related Network Functions	8.1.0	R99	S3	NGUYEN NGOC, Sebastien	
TS	03.33	Lawful Interception; Stage 2	8.1.0	R99	S3	MCKIBBEN, Bernie	TSG#10:8.1.0
Release 1999 3GPP Specifications and Reports							
TS	21.133	3G security; Security threats and requirements	3.2.0	R99	S3	CHRISTOFFERSSON, Per	.
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	3.2.1	R99	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	3.0.0	R99	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031. Created from 02.31 R99.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	3.0.0	R99	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards). SP-16: Takes over from 02.32 R99.
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	3.0.0	R99	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031. Created from 03.31 R99.
TS	23.035	Immediate Service Termination (IST); Stage 2	3.1.0	R99	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards). SP-16: takes over from 03,35 R99.
TS	33.102	3G security; Security architecture	3.13.0	R99	S3	BLOMMAERT, Marc	
TS	33.103	3G security; Integration guidelines	3.7.0	R99	S3	BLANCHARD, Colin	
TS	33.105	Cryptographic algorithm requirements	3.8.0	R99	S3	CHIKAZAWA, Takeshi	
TS	33.106	Lawful interception requirements	3.1.0	R99	S3	WILHELM, Berthold	.
TS	33.107	3G security; Lawful interception architecture and functions	3.5.0	R99	S3	WILHELM, Berthold	
TS	33.120	Security Objectives and Principles	3.0.0	R99	S3	WRIGHT, Tim	.
TR	33.901	Criteria for cryptographic Algorithm design process	3.0.0	R99	S3	BLOM, Rolf	.
TR	33.902	Formal Analysis of the 3G Authentication Protocol	3.1.0	R99	S3	HORN, Guenther	.
TR	33.908	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	3.0.0	R99	S3	WALKER, Michael	TSG#7: S3-000105=NP-000049 Formerly 33.904.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	3.2.0	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
Release 4 3GPP Specifications and Reports							
TS	21.133	3G security; Security threats and requirements	4.1.0	Rel-4	S3	CHRISTOFFERSSON, Per	
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	4.1.0	Rel-4	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031. Created from 42.031 Rel-4.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards). SP-16: Takes over from 42.032 Rel-4.
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031. Created from 43.031 Rel-4.
TS	23.035	Immediate Service Termination (IST); Stage 2	4.1.0	Rel-4	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards). SP-16: takes over from 43.035 Rel-4
TS	33.102	3G security; Security architecture	4.5.0	Rel-4	S3	BLOMMAERT, Marc	
TS	33.103	3G security; Integration guidelines	4.2.0	Rel-4	S3	BLANCHARD, Colin	SP-15: Not to be promoted to Rel-5.
TS	33.105	Cryptographic algorithm requirements	4.2.0	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	2001-05-24: title grows MAP; see 33.210 for IP equivalent.
TR	33.901	Criteria for cryptographic Algorithm design process	4.0.0	Rel-4	S3	BLOM, Rolf	SP-15: Not to be promoted to Rel-5.
TR	33.902	Formal Analysis of the 3G Authentication Protocol	4.0.0	Rel-4	S3	HORN, Guenther	SP-15: Not to be promoted to Rel-5.
TR	33.908	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	4.0.0	Rel-4	S3	WALKER, Michael	TSG#7: S3-000105=NP-000049 SP-15: Not to be promoted to Rel-5.
TR	33.903	Access Security for IP based services	none	Rel-4	S3	VACANT,	.
TR	33.909	3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions	4.0.1	Rel-4	S3	WALKER, Michael	TSG#7: Is a reference in 33.908. Was withdrawn, but reinstated at TSG#10. SP-15: Not to be promoted to Rel-5.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	4.1.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.205	3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE. 2002-06: clarified that deliverable is TS not TR. TSG#11:changed to Rel-4.
TS	35.206	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:changed to Rel-4
TS	35.207	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementorsí test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:changed to Rel-4

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:changed to Rel-4
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:Formerly 35.209 Rel-99 (but never made available)
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	4.0.1	Rel-4	S3	WRIGHT, Tim	
TR	41.033	Lawful Interception requirements for GSM	4.0.1	Rel-4	S3	MCKIBBEN, Bernie	
TS	41.061	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	4.0.0	Rel-4	S3	WALKER, Michael	SP-15: Not to be promoted to Rel-5.
TS	42.009	Security Aspects	4.0.0	Rel-4	S3	CHRISTOFFERSSON, Per	SP-15: Not to be promoted to Rel-5.
TS	42.033	Lawful Interception; Stage 1	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
TS	43.020	Security-related network functions	4.0.0	Rel-4	S3	GILBERT, Henri	
TS	43.033	Lawful Interception; Stage 2	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
Release 5 3GPP Specifications and Reports							
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	5.0.0	Rel-5	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4 .
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031. Created from 42.031 Rel-5.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards). .
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031. Created from 43.031 Rel-5.
TS	23.035	Immediate Service Termination (IST); Stage 2	5.1.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards). .
TS	33.102	3G security; Security architecture	5.5.0	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)	5.8.0	Rel-5	S3	WILHELM, Berthold	2001-12-04 Title changed from "Lawful Interception; Interface between core network and law agency equipment" (Berthold.Wilhelm@RegTP.de). .
TS	33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	5.1.0	Rel-5	S3	ESCOTT, Adrian	2001-05-24: title grows MAP; see 33.210 for IP equivalent. .
TS	33.203	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	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210).
TR	33.900	Guide to 3G security	0.4.1	Rel-5	S3	BROOKSON, Charles	.
TR	33.903	Access Security for IP based services	none	Rel-5	S3	VACANT,	.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.205	3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE. 2002-06: clarified that deliverable is TS not TR. .
TS	35.206	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification	5.1.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TS	35.207	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementorsí test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	5.0.0	Rel-5	S3	WRIGHT, Tim	.
TR	41.033	Lawful Interception requirements for GSM	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
TS	42.033	Lawful Interception; Stage 1	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
TS	43.020	Security-related network functions	5.0.0	Rel-5	S3	GILBERT, Henri	.
TS	43.033	Lawful Interception; Stage 2	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
Release 6 3GPP Specifications and Reports							
TS	33.102	3G security; Security architecture	6.2.0	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	6.3.0	Rel-6	S3	WILHELM, Berthold	.
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	6.7.0	Rel-6	S3	WILHELM, Berthold	2001-12-04 Title changed from "Lawful Interception; Interface between core network and law agency equipment" (Berthold.Wilhelm@RegTP.de). .
TS	33.141	Presence service; Security	6.1.0	Rel-6	S3	BOMAN, Krister	.
TS	33.203	3G security; Access security for IP-based services	6.4.0	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	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210). .
TS	33.220	Generic Authentication Architecture (GAA); Generic bootstrapping architecture	6.2.0	Rel-6	S3	HAUKKA, Tao	WI = SEC1-SC (UID 33002) Based on 33.109 ß4. .
TS	33.221	Generic Authentication Architecture (GAA); Support for subscriber certificates	6.1.0	Rel-6	S3	HAUKKA, Tao	WI = SEC1-SC (UID 33002) Based on 33.109 ß5 & annex A. .
TS	33.222	Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)	6.1.0	Rel-6	S3	SAHLIN, Bengt	WI = SEC1-SC (UID 33002) Based on 33.109 v0.3.0 protocol B. .

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	33.234	3G security; Wireless Local Area Network (WLAN) interworking security	6.2.1	Rel-6	S3	LOPEZ SORIA, Luis	.
TS	33.246	3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)	6.0.0	Rel-6	S3	ESCOTT, Adrian	SP-25: Approved
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	2002-07-22: was formerly 33.910. SP-17: expect v2.0.0 at SP-18.
TR	33.817	Feasibility study on (Universal) Subscriber Interface Module (U)SIM security reuse by peripheral devices on local interfaces	6.0.0	Rel-6	S3	YAQUB, Raziq	Original WID = SP-030341. 2003-11-26: S3 Secretary indicates that TR is to be internal, so number changed from 33.917. .
TR	33.919	3G Security; Generic Authentication Architecture (GAA); System Description	6.0.0	Rel-6	S3	VAN MOFFAERT, Annelies	WI = SEC1-SC (UID 33002) . SP-25: Approved
TR	43.020	3G Security; Security-related network functions	6.0.0	Rel-6	S3	GILBERT, Henri	Approved TSG SA #25
TS	55.205	Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8	6.1.0	Rel-6	S3	WALKER, Michael	Not subject to export control. .
TS	55.216	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 1: A5/3 and GEA3 specification	6.2.0	Rel-6	S3	N, A	2003-09-30: Note: document only available with French export licence. .
TS	55.217	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data	6.1.0	Rel-6	S3	N, A	2003-09-30: Note: document only available with French export licence. .
TS	55.218	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 3: Design and conformance test data	6.1.0	Rel-6	S3	N, A	2003-09-30: Note: document only available with French export licence. .
TR	55.919	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report	6.1.0	Rel-6	S3	N, A	2003-09-30: Note: document only available with French export licence. .
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 meetings #35 and #36

Note: Some CRs agreed at meeting #35 were further reviewed and revised or included in other CRs. This list shows the status of all CRs presented and their results. Agreed versions of CRs are shown in blue text.

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	Status	WI
21.133	004	-	Rel-4	Correction of description of 3G identity	D	4.1.0	S3-36	S3-040917	rejected	SEC1
33.102	189	-	Rel-6	Correction of Abbreviation for USIM	D	6.2.0	S3-36	S3-040904	agreed	SEC1
33.102	190	-	Rel-6	Correction of TMUI to TMSI in a figure	D	6.2.0	S3-36	S3-040918	revised	SEC1
33.102	190	1	Rel-6	Correction of TMUI to TMSI in a figure	D	6.2.0	S3-36	S3-041071	agreed	SEC1
33.102	191	-	Rel-6	Support of algorithms in UEs	C	6.2.0	S3-36	S3-040935	revised	SEC1
33.102	191	1	Rel-6	Support of algorithms in UEs	C	6.2.0	S3-36	S3-041029	revised	SEC1
33.102	191	2	Rel-6	Support of algorithms in UEs	C	6.2.0	S3-36	S3-041033	revised	SEC1
33.102	191	3	Rel-6	Support of algorithms in UEs	C	6.2.0	S3-36	S3-041073	agreed	SEC1
33.103	018	-	Rel-4	Correction of USIM data elements for AKA	D	4.1.0	S3-36	S3-040919	rejected	SEC1
33.107	048	-	Rel-6	Lawful Interception for WLAN Interworking (e-mail approved)	B	6.3.0	S3-36	S3-030913	agreed	SEC1-LI
33.107	049	-	Rel-6	33.107 Cleanup (e-mail approved)	F	6.3.0	S3-36	S3-030913	agreed	SEC1-LI
33.107	050	-	Rel-6	Clarification on MMS interception (e-mail approved)	B	6.3.0	S3-36	S3-030913	agreed	SEC1-LI
33.108	060	-	Rel-5	Correction to ULIC header (e-mail approved)	F	5.8.0	S3-36	S3-040913	agreed	SEC1-LI
33.108	061	-	Rel-6	Correction to ULIC header (e-mail approved)	A	6.7.0	S3-36	S3-040913	agreed	SEC1-LI
33.108	062	-	Rel-6	Correction on parameter GprsOperationErrorCode (e-mail approved)	F	6.7.0	S3-36	S3-040913	agreed	SEC1-LI
33.108	063	-	Rel-6	Correction to the IMPORTS statements (e-mail approved)	F	6.7.0	S3-36	S3-040913	agreed	SEC1-LI
33.108	064	-	Rel-6	Syntax Error in Annex B.3 (e-mail approved)	F	6.7.0	S3-36	S3-040913	agreed	SEC1-LI
33.108	065	-	Rel-6	Deleting CC from SIP message (e-mail approved)	B	6.7.0	S3-36	S3-040913	agreed	SEC1-LI
33.108	066	-	Rel-6	Adding domain ID to HI3 CS domain module (e-mail approved)	B	6.7.0	S3-36	S3-040913	agreed	SEC1-LI
33.108	067	-	Rel-6	Syntax Error in Annex B.3a (e-mail approved)	F	6.7.0	S3-36	S3-040913	agreed	SEC1-LI
33.108	068	-	Rel-6	HI2 SIP Content clarification (e-mail approved)	C	6.7.0	S3-36	S3-040913	agreed	SEC1-LI
33.200	023	-	Rel-6	SMS fraud countermeasures	B	5.1.0	S3-36	S3-040954	revised	SEC1-MAP
33.200	023	1	Rel-6	SMS fraud countermeasures	B	5.1.0	S3-36	S3-041070	agreed	SEC1-MAP
33.203	070	1	Rel-6	Forwards compatibility to TLS based access security	F	6.4.0	S3-35	S3-040762	postponed	IMS-ASEC
33.203	073	-	Rel-6	Support of IMS end user devices behind a NA(P)T firewall, and protection of RTP media flows	C	6.4.0	S3-35	S3-040721	rejected	IMS-ASEC
33.203	074	-	Rel-6	Forwards compatibility to TLS based access security	F	6.4.0	S3-35	S3-040762	withdrawn	IMS-ASEC
33.203	075	-	Rel-6	Editorial corrections	D	6.4.0	S3-36	S3-041066	revised	IMS-ASEC
33.203	075	1	Rel-6	Editorial corrections	D	6.4.0	S3-36	S3-041143	agreed	IMS-ASEC
33.203	076	-	Rel-6	Corrections to Section 7.1 & 7.2	F	6.4.0	S3-36	S3-040905	withdrawn	IMS-ASEC
33.203	077	-	Rel-6	Addition of reference to early IMS security TR	F	6.4.0	S3-36	S3-041001	revised	IMS-EARLY
33.203	077	-	Rel-6	Addition of reference to early IMS security TR	F	6.4.0	S3-36	S3-041030	postponed	IMS-EARLY
33.220	018	-	Rel-6	BSF discovery using default domain method	C	6.2.0	S3-35	S3-040695	Revised	SEC1-SC
33.220	018	1	Rel-6	BSF discovery using default domain method	C	6.2.0	S3-35	S3-040831	agreed	SEC1-SC
33.220	019	-	Rel-6	Local validity condition set by NAF	F	6.2.0	S3-35	S3-040736	Revised	SEC1-SC
33.220	019	1	Rel-6	Local validity condition set by NAF	F	6.2.0	S3-35	S3-040828	agreed	SEC1-SC
33.220	020	-	Rel-6	GBA User Security Settings (GUSS) usage in GAA	C	6.2.0	S3-35	S3-040741	Revised	SEC1-SC
33.220	020	1	Rel-6	GBA User Security Settings (GUSS) usage in GAA	C	6.2.0	S3-35	S3-040832	Revised	SEC1-SC
33.220	020	2	Rel-6	GBA User Security Settings (GUSS) usage in GAA and Introduction of NAF groups	C	6.2.0	S3-36	S3-040987	Revised	SEC1-SC
33.220	020	3	Rel-6	GBA User Security Settings (GUSS) usage in GAA and Introduction of NAF groups	C	6.2.0	S3-36	S3-041135	agreed	SEC1-SC
33.220	021	-	Rel-6	Details of USIM/ISIM selection in GAA	C	6.2.0	S3-35	S3-040742	Revised	SEC1-SC
33.220	021	1	Rel-6	Details of USIM/ISIM selection in GAA	C	6.2.0	S3-36	S3-040981	Revised	SEC1-SC

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	Status	WI
33.220	021	2	Rel-6	Details of USIM/ISIM selection in GAA	C	6.2.0	S3-36	S3-041085	agreed	SEC1-SC
33.220	022	-	Rel-6	Usage control of the service in visited network	F	6.2.0	S3-35	S3-040746	Rejected	SEC1-SC
33.220	023	-	Rel-6	TLS profile for securing Zn' reference point	C	6.2.0	S3-35	S3-040756	agreed	SEC1-SC
33.220	024	-	Rel-6	Modification of delivery of MIKEY RAND field in MSK updates	C	6.2.0	S3-35	S3-040757	Rejected	SEC1-SC
33.220	025	-	Rel-6	Optimization of the GBA_U key derivation procedure	C	6.2.0	S3-35	S3-040776	Revised	SEC1-SC
33.220	025	1	Rel-6	Optimization of the GBA_U key derivation procedure	C	6.2.0	S3-36	S3-040951	Revised	SEC1-SC
33.220	025	2	Rel-6	Optimization of the GBA_U key derivation procedure	C	6.2.0	S3-36	S3-041136	agreed	SEC1-SC
33.220	026	-	Rel-6	GBA_U: storage of Ks_ext in the UICC	C	6.2.0	S3-35	S3-040777	Revised	SEC1-SC
33.220	026	1	Rel-6	GBA_U: storage of Ks_ext in the UICC	C	6.2.0	S3-36	S3-040953	withdrawn	SEC1-SC
33.220	027	-	Rel-6	Requirement on ME capabilities for GBA_U	B	6.2.0	S3-35	S3-040778	Revised	SEC1-SC
33.220	027	1	Rel-6	Requirement on ME capabilities for GBA_U	B	6.2.0	S3-36	S3-040952	Revised	SEC1-SC
33.220	027	2	Rel-6	Requirement on ME capabilities for GBA_U	B	6.2.0	S3-36	S3-041080	agreed	SEC1-SC
33.220	028	-	Rel-6	Enabling optional GBA_U support for ME	C	6.2.0	S3-35	S3-040783	Postponed	SEC1-SC
33.220	029	-	Rel-6	Description of UICC-ME interface	C	6.2.0	S3-35	S3-040784	Postponed	SEC1-SC
33.220	030	-	Rel-6	Clarification of GBA_U AUTN generation procedure in the BSF	F	6.2.0	S3-36	S3-040923	Rejected	SEC1-SC
33.220	031	-	Rel-6	Usage of B-TID in reference point Ub	C	6.2.0	S3-36	S3-040932	Rejected	SEC1-SC
33.220	032	-	Rel-6	Update of GUSS	C	6.2.0	S3-36	S3-040934	Rejected	SEC1-SC
33.220	033	-	Rel-6	Enhanced key freshness in GBA	B	6.2.0	S3-36	S3-040941	withdrawn	SEC1-SC
33.220	034	-	Rel-6	Adding a note about replay protection	F	6.2.0	S3-36	S3-040942	Revised	SEC1-SC
33.220	034	1	Rel-6	Adding a note about replay protection	F	6.2.0	S3-36	S3-041087	agreed	SEC1-SC
33.220	035	-	Rel-6	Complete the MAC modification for GBA_U	F	6.2.0	S3-36	S3-040956	Revised	SEC1-SC
33.220	035	1	Rel-6	Complete the MAC modification for GBA_U	F	6.2.0	S3-36	S3-041078	agreed	SEC1-SC
33.220	036	-	Rel-6	Removal of unnecessary editor's notes	D	6.2.0	S3-36	S3-040978	Revised	SEC1-SC
33.220	036	1	Rel-6	Removal of unnecessary editor's notes	D	6.2.0	S3-36	S3-041082	agreed	SEC1-SC
33.220	037	-	Rel-6	Key lifetime clarifications	C	6.2.0	S3-36	S3-040982	Rejected	SEC1-SC
33.220	038	-	Rel-6	Fetching of one AV only on each Zh run between BSF and HSS	C	6.2.0	S3-36	S3-040986	Revised	SEC1-SC
33.220	038	1	Rel-6	Fetching of one AV only on each Zh run between BSF and HSS	C	6.2.0	S3-36	S3-041090	agreed	SEC1-SC
33.220	039	-	Rel-6	Clean up of TS 33.220	F	6.2.0	S3-36	S3-040988	Revised	SEC1-SC
33.220	039	1	Rel-6	Clean up of TS 33.220	F	6.2.0	S3-36	S3-041083	agreed	SEC1-SC
33.220	040	-	Rel-6	New key management for ME based GBA keys	C	6.2.0	S3-36	S3-041024	Revised	SEC1-SC
33.220	040	1	Rel-6	New key management for ME based GBA keys	C	6.2.0	S3-36	S3-041084	agreed	SEC1-SC
33.220	041	-	Rel-6	Key derivation function	B	6.2.0	S3-36	S3-041027	Revised	SEC1-SC
33.220	041	1	Rel-6	Key derivation function	B	6.2.0	S3-36	S3-041081	agreed	SEC1-SC
33.220	042	-	Rel-6	Re-negotiation of keys	F	6.2.0	S3-36	S3-041086	Revised	SEC1-SC
33.220	042	1	Rel-6	Re-negotiation of keys	F	6.2.0	S3-36	S3-041140	agreed	SEC1-SC
33.220	043	-	Rel-6	No GUSS/USS update procedures in Release-6	D	6.1.0	S3-36	S3-040976	Revised	GBA-SSC
33.220	043	1	Rel-6	No GUSS/USS update procedures in Release-6	C	6.1.0	S3-36	S3-041089	agreed	GBA-SSC
33.220	044	-	Rel-6	Clarify the number of NAF-specific keys stored in the UE per NAF-Id	D	6.1.0	S3-36	S3-041079	Revised	SEC1-SC
33.220	044	1	Rel-6	Clarify the number of NAF-specific keys stored in the UE per NAF-Id	D	6.1.0	S3-36	S3-041137	agreed	SEC1-SC
33.221	005	-	Rel-6	Visited network issuing subscriber certificates	B	6.1.0	S3-35	S3-040782	agreed	SEC1-SC
33.221	006	-	Rel-6	Editorial correction	D	6.1.0	S3-36	S3-040979	agreed	SEC1-SC
33.222	005	-	Rel-6	GBA supported indication in PSK TLS	C	6.1.0	S3-35	S3-040731	agreed	GBA-SSC
33.222	006	-	Rel-6	Editorial correction of TS 33.222	D	6.1.0	S3-35	S3-040734	rejected	GBA-SSC
33.222	007	-	Rel-6	Adding Support for AES in the TLS Profile	C	6.1.0	S3-36	S3-040963	revised	GBA-SSC
33.222	007	1	Rel-6	Adding Support for AES in the TLS Profile	C	6.1.0	S3-36	S3-041092	agreed	GBA-SSC
33.222	008	-	Rel-6	Removing PSK TLS from 3GPP rel-6	F	6.1.0	S3-36	S3-040965	agreed	GBA-SSC
33.222	009	-	Rel-6	Clean-up of TS 33.222	D	6.1.0	S3-36	S3-040966	rejected	GBA-SSC
33.222	010	-	Rel-6	Authorization flag transfer between AP and AS	C	6.1.0	S3-36	S3-040975	revised	GBA-SSC

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	Status	WI
33.222	010	1	Rel-6	Authorization flag transfer between AP and AS	C	6.1.0	S3-36	S3-041093	agreed	GBA-SSC
33.222	011	-	Rel-6	Keeping PSK TLS in 3GPP rel-6	F	6.1.0	S3-36	S3-040000	withdrawn	GBA-SSC
33.222	012	-	Rel-6	Correction of inconsistencies within AP specification	F	6.1.0	S3-36	S3-040985	agreed	GBA-SSC
33.222	013	-	Rel-6	TLS extensions support	C	6.1.0	S3-36	S3-041025	revised	SEC1-SC
33.222	013	1	Rel-6	TLS extensions support	C	6.1.0	S3-36	S3-041096	agreed	SEC1-SC
33.222	014	-	Rel-6	Visited AS using subscriber certificates	C	6.1.0	S3-36	S3-041026	agreed	SEC1-SC
33.222	015	-	Rel-6	Keeping PSK TLS in 3GPP rel-6	F	6.1.0	S3-36	S3-041094	revised	SEC1-SC
33.222	015	1	Rel-6	Keeping PSK TLS in 3GPP rel-6	F	6.1.0	S3-36	S3-041142	agreed	SEC1-SC
33.234	019	-	Rel-6	Profile for PDG certificates in Scenario 3	F	6.2.0	S3-35	S3-040717	Revised	WLAN
33.234	019	1	Rel-6	Profile for PDG certificates in Scenario 3	F	6.2.1	S3-36	S3-040927	Revised	WLAN
33.234	019	2	Rel-6	Profile for PDG certificates in Scenario 3	F	6.2.1	S3-36	S3-041100	agreed	WLAN
33.234	020	-	Rel-6	Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces)	B	6.2.0	S3-35	S3-040724	Revised	WLAN
33.234	020	1	Rel-6	Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces)	B	6.2.1	S3-35	S3-040838	Revised	WLAN
33.234	020	2	Rel-6	Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces)	B	6.2.1	S3-36	S3-041003	Revised	WLAN
33.234	020	3	Rel-6	Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces)	B	6.2.1	S3-36	S3-041106	Revised	WLAN
33.234	020	4	Rel-6	Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces)	B	6.2.1	S3-36	S3-041151	agreed	WLAN
33.234	021	-	Rel-6	Bluetooth security and configuration considerations for Annex A4 of TS 33.234 (Wireless Local Area Network (WLAN) interworking security)	B	6.2.0	S3-35	S3-040725	Rejected	WLAN
33.234	022	-	Rel-6	Control of simultaneous accesses in scenario 3	F	6.2.0	S3-35	S3-040748	Rejected	WLAN
33.234	023	-	Rel-6	Clarification on the use of MAC addresses	F	6.2.0	S3-35	S3-040750	Postponed	WLAN
33.234	024	-	Rel-6	Sending of W-APN identification	B	6.2.0	S3-35	S3-040751	Revised	WLAN
33.234	024	1	Rel-6	Sending of W-APN identification	B	6.2.0	S3-35	S3-040~~751~~1864	agreed	WLAN
33.234	025	-	Rel-6	Clean up of not completed chapters	F	6.2.0	S3-35	S3-040752	Revised	WLAN
33.234	025	1	Rel-6	Clean up of not completed chapters	F	6.2.1	S3-35	S3-040836	Revised	WLAN
33.234	025	2	Rel-6	Clean up of not completed chapters	F	6.2.1	S3-35	S3-040886	agreed	WLAN
33.234	026	-	Rel-6	Alignment of TS 33.234 with SA3 decisions on WLAN UE function split	F	6.2.0	S3-35	S3-040758	Rejected	WLAN
33.234	027	-	Rel-6	Correction of WLAN UE function split	F	6.2.0	S3-35	S3-040759	Revised	WLAN
33.234	027	1	Rel-6	Correction of WLAN UE function split	F	6.2.0	S3-35	S3-040841	Revised	WLAN
33.234	027	2	Rel-6	Correction of WLAN UE function split	F	6.2.0	S3-35	S3-040875	Revised	WLAN
33.234	027	3	Rel-6	Correction of WLAN UE function split	F	6.2.0	S3-36	S3-041022	Revised	WLAN
33.234	027	4	Rel-6	Correction of WLAN UE function split	F	6.2.0	S3-36	S3-041103	Revised	WLAN
33.234	027	5	Rel-6	Correction of WLAN UE function split	C	6.2.0	S3-36	S3-041104	Revised	WLAN
33.234	027	6	Rel-6	Correction of WLAN UE function split	C	6.2.0	S3-36	S3-041149	agreed	WLAN
33.234	028	-	Rel-6	Passing keying material to the WLAN-AN during the Fast re-authentication procedure	F	6.2.1	S3-35	S3-040763	agreed	WLAN
33.234	029	-	Rel-6	Clarification on Deletion of Temporary IDs	F	6.2.0	S3-35	S3-040764	Revised	WLAN
33.234	029	1	Rel-6	Clarification on Deletion of Temporary IDs	F	6.2.1	S3-35	S3-040837	agreed	WLAN
33.234	030	-	Rel-6	Clarification on Protecting Re-authentication ID in FAST/FULL Re-Authentication procedure	F	6.2.0	S3-35	S3-040765	agreed	WLAN
33.234	031	-	Rel-6	Assigning Remote IP Address to WLAN UE using IKEv2 configuration Payload	B	6.2.0	S3-35	S3-040766	agreed	WLAN
33.234	032	-	Rel-6	Tunnel Redirection Procedure	B	6.2.0	S3-35	S3-040767	Postponed	WLAN
33.234	033	-	Rel-6	Tunnel Establishment Procedure	F	6.2.0	S3-35	S3-040768	Revised	WLAN
33.234	033	1	Rel-6	Tunnel Establishment Procedure	F	6.2.0	S3-35	S3-040861	agreed	WLAN

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	Status	WI
33.234	034	-	Rel-6	Multiple Tunnels to the same PDG for different W-APN	B	6.2.0	S3-35	S3-040769	Postponed	WLAN
33.234	035	-	Rel-6	Multiple Tunnels establishment with different PDG	B	6.2.0	S3-35	S3-040770	Postponed	WLAN
33.234	036	-	Rel-6	Deletion of inconclusive text on A5/2 countermeasures	F	6.2.0	S3-35	S3-040771	agreed	WLAN
33.234	037	-	Rel-6	Alignment of IPsec profile with RFC2406	F	6.2.0	S3-35	S3-040772	Revised	WLAN
33.234	037	1	Rel-6	Alignment of IPsec profile with RFC2406	F	6.2.0	S3-35	S3-040842	agreed	WLAN
33.234	038	-	Rel-6	Update the status of reference IEEE802.11i	F	6.2.1	S3-36	S3-040920	Withdrawn	WLAN
33.234	039	-	Rel-6	Confidentiality and integrity canít be both NULL in the IPsec tunnel	F	6.2.1	S3-36	S3-040928	Withdrawn	WLAN
33.234	040	-	Rel-6	Control of simultaneous sessions in WLAN 3GPP IP access	C	6.2.1	S3-36	S3-040944	Revised	WLAN
33.234	040	1	Rel-6	Control of simultaneous sessions in WLAN 3GPP IP access	C	6.2.1	S3-36	S3-041112	Revised	WLAN
33.234	040	2	Rel-6	Control of simultaneous sessions in WLAN 3GPP IP access	C	6.2.1	S3-36	S3-041153	agreed	WLAN
33.234	041	-	Rel-6	Completion of definition and abbreviations	D	6.2.1	S3-36	S3-040945	Revised	WLAN
33.234	041	1	Rel-6	Completion of definition and abbreviations	D	6.2.1	S3-36	S3-041109	agreed	WLAN
33.234	042	-	Rel-6	Fallback from re-authentication to full authentication	F	6.2.1	S3-36	S3-040946	Revised	WLAN
33.234	042	1	Rel-6	Fallback from re-authentication to full authentication	F	6.2.1	S3-36	S3-041110	agreed	WLAN
33.234	043	-	Rel-6	Clarification on the use of IMSI in WLAN 3GPP IP access	F	6.2.1	S3-36	S3-040947	agreed	WLAN
33.234	044	-	Rel-6	Clarification on the use of MAC addresses	F	6.2.1	S3-36	S3-040948	Revised	WLAN
33.234	044	1	Rel-6	Clarification on the use of MAC addresses	F	6.2.1	S3-36	S3-041113	Revised	WLAN
33.234	044	2	Rel-6	Clarification on the use of MAC addresses	F	6.2.1	S3-36	S3-041138	agreed	WLAN
33.234	045	-	Rel-6	Clarifications and corrections on the use of pseudonyms	F	6.2.1	S3-36	S3-040949	agreed	WLAN
33.234	046	-	Rel-6	Clarification on storage of Temporary Identities in UICC	F	6.2.1	S3-36	S3-040957	Withdrawn	WLAN
33.234	047	-	Rel-6	Wn Reference Point Description	D	6.2.1	S3-36	S3-040958	agreed	WLAN
33.234	048	-	Rel-6	Removal of word ìscenarioî	F	6.2.1	S3-36	S3-040959	agreed	WLAN
33.234	049	-	Rel-6	Correction of WRAP to CCMP	F	6.2.1	S3-36	S3-041088	Revised	WLAN
33.234	049	1	Rel-6	Correction of WRAP to CCMP	F	6.2.1	S3-36	S3-041108	agreed	WLAN
33.234	050	-	Rel-6	Removal of resolved editors' notes	D	6.2.1	S3-36	S3-041139	Revised	WLAN
33.234	050	1	Rel-6	Removal of resolved editors' notes	D	6.2.1	S3-36	S3-041155	agreed	WLAN
33.246	001	-	Rel-6	Deletion of MBMS keys stored in the ME	B	6.0.0	S3-35	S3-040743	Revised	MBMS
33.246	001	1	Rel-6	Deletion of MBMS keys stored in the ME	B	6.0.0	S3-35	S3-04xxxx	Revised	MBMS
33.246	001	2	Rel-6	Deletion of MBMS keys stored in the ME	B	6.0.0	S3-35	S3-040743	Revised	MBMS
33.246	001	3	Rel-6	Deletion of MBMS keys stored in the ME	F	6.0.0	S3-36	S3-041011	Revised	MBMS
33.246	001	4	Rel-6	Deletion of MBMS keys stored in the ME	C	6.0.0	S3-36	S3-041122	agreed	MBMS
33.246	002	-	Rel-6	Clarification on key management	C	6.0.0	S3-35	S3-040744	agreed	MBMS
33.246	003	-	Rel-6	Delivery of multiple keys in one MIKEY message for MBMS	C	6.0.0	S3-35	S3-040754	Rejected	MBMS
33.246	004	-	Rel-6	UE handling of MSKs received	C	6.0.0	S3-35	S3-040755	Postponed	MBMS
33.246	005	-	Rel-6	Clean up of MBMS TS	D	6.0.0	S3-35	S3-040761	Revised	MBMS
33.246	005	1	Rel-6	Clean up of MBMS TS	D	6.0.0	S3-35	S3-040850	Revised	MBMS
33.246	005	2	Rel-6	Clean up of MBMS TS	D	6.0.0	S3-36	S3-041018	Revised	MBMS
33.246	005	3	Rel-6	Clean up of MBMS TS	D	6.0.0	S3-36	S3-041115	agreed	MBMS
33.246	006	-	Rel-6	Traffic protection combinations	F	6.0.0	S3-35	S3-040780	Revised	MBMS
33.246	006	1	Rel-6	Traffic protection combinations	F	6.0.0	S3-35	S3-040852	agreed	MBMS
33.246	007	-	Rel-6	Clarifying ME capabilities	F	6.0.0	S3-35	S3-040788	Revised	MBMS
33.246	007	1	Rel-6	Clarifying ME and BM-SC capabilities	F	6.0.0	S3-35	S3-040862	Revised	MBMS
33.246	007	2	Rel-6	Clarifying ME and BM-SC capabilities	F	6.0.0	S3-35	S3-040887	Revised	MBMS
33.246	007	3	Rel-6	Clarifying ME and BM-SC capabilities	F	6.0.0	S3-36	S3-041010	~~Revised~~agreed	MBMS
33.246	007	4	Rel-6	Clarifying ME and BM-SC capabilities	F	6.0.0	S3-36	S3-041018	~~agreed~~rejected	MBMS
33.246	008	-	Rel-6	MBMS Key processing	C	6.0.0	S3-35	S3-040793	Revised	MBMS

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	Status	WI
33.246	008	1	Rel-6	MBMS Key processing	C	6.0.0	S3-35	S3-040858	Revised	MBMS
33.246	008	2	Rel-6	MBMS Key processing	C	6.0.0	S3-36	S3-041018	rejected	MBMS
33.246	008	3	Rel-6	MBMS Key processing	C	6.0.0	S3-36	S3-041041	rejected	MBMS
33.246	009	-	Rel-6	MBMS MTK Download transport	C	6.0.0	S3-35	S3-040794	Revised	MBMS
33.246	009	1	Rel-6	MBMS MTK Download transport	C	6.0.0	S3-35	S3-040853	agreed	MBMS
33.246	010	-	Rel-6	MBMS Transport of salt	C	6.0.0	S3-35	S3-040797	Revised	MBMS
33.246	010	1	Rel-6	MBMS Transport of salt	C	6.0.0	S3-36	S3-040992	Revised	MBMS
33.246	010	2	Rel-6	MBMS Transport of salt	C	6.0.0	S3-36	S3-041118	Revised	MBMS
33.246	010	3	Rel-6	MBMS Transport of salt	C	6.0.0	S3-36	S3-041125	agreed	MBMS
33.246	011	-	Rel-6	SRTP index synchronisation within ME	C	6.0.0	S3-35	S3-040798	Revised	MBMS
33.246	011	1	Rel-6	SRTP index synchronisation within ME	C	6.0.0	S3-35	S3-040854	agreed	MBMS
33.246	012	-	Rel-6	Clarify the use of mandatory MIKEY features for MBMS	F	6.0.0	S3-35	S3-040799	Revised	MBMS
33.246	012	1	Rel-6	Clarify the use of mandatory MIKEY features for MBMS	F	6.0.0	S3-36	S3-041008	Revised	MBMS
33.246	012	2	Rel-6	Clarify the use of mandatory MIKEY features for MBMS	F	6.0.0	S3-36	S3-041055	agreed	MBMS
33.246	013	-	Rel-6	Adding MIKEY payload type identifiers	F	6.0.0	S3-35	S3-040800	Revised	MBMS
33.246	013	1	Rel-6	Adding MIKEY payload type identifiers	F	6.0.0	S3-35	S3-040857	Revised	MBMS
33.246	013	2	Rel-6	Adding MIKEY payload type identifiers	F	6.0.0	S3-36	S3-040994	withdrawn	MBMS
33.246	013	3	Rel-6	Adding MIKEY payload type identifiers	F	6.0.0	S3-37	S3-041041	rejected	MBMS
33.246	014	-	Rel-6	Protection of the Gmb reference point	C	6.0.0	S3-35	S3-040801	agreed	MBMS
33.246	015	-	Rel-6	Use of parallel MSKs and MTKs	C	6.0.0	S3-35	S3-040804	Revised	MBMS
33.246	015	1	Rel-6	Use of parallel MSKs and MTKs	C	6.0.0	S3-35	S3-040859	agreed	MBMS
33.246	016	-	Rel-6	Scope of MBMS security	C	6.0.0	S3-35	S3-040807	Revised	MBMS
33.246	016	1	Rel-6	Scope of MBMS security	C	6.0.0	S3-35	S3-040849	Revised	MBMS
33.246	016	2	Rel-6	Scope of MBMS security	C	6.0.0	S3-36	S3-041018	Revised	MBMS
33.246	016	3	Rel-6	Scope of MBMS security	C	6.0.0	S3-36	S3-041116	agreed	MBMS
33.246	017	-	Rel-6	XML protection for download services	C	6.0.0	S3-35	S3-040810	Revised	MBMS
33.246	017	1	Rel-6	XML protection for download services	C	6.0.0	S3-36	S3-040898	rejected	MBMS
33.246	018	-	Rel-6	Clarification of the format of MTK ID and MSK ID	C	6.0.0	S3-35	S3-040814	Revised	MBMS
33.246	018	1	Rel-6	Clarification of the format of MTK ID and MSK ID	C	6.0.0	S3-35	S3-040860	Revised	MBMS
33.246	018	2	Rel-6	Clarification of the format of MTK ID and MSK ID	C	6.0.0	S3-35	S3-040888	Revised	MBMS
33.246	018	3	Rel-6	Clarification of the format of MTK ID and MSK ID	C	6.0.0	S3-36	S3-041018	Revised	MBMS
33.246	018	4	Rel-6	Clarification of the format of MTK ID and MSK ID	C	6.0.0	S3-36	S3-041120	agreed	MBMS
33.246	019	-	Rel-6	Initiation of key management	C	6.0.0	S3-35	S3-040816	Rejected	MBMS
33.246	020	-	Rel-6	MTK update procedure for streaming services	C	6.0.0	S3-35	S3-040818	Revised	MBMS
33.246	020	1	Rel-6	MTK update procedure for streaming services	C	6.0.0	S3-35	S3-040855	Revised	MBMS
33.246	020	2	Rel-6	MTK update procedure for streaming services	B	6.0.0	S3-36	S3-040888	Revised	MBMS
33.246	020	3	Rel-6	MTK update procedure for streaming services	B	6.0.0	S3-36	S3-041117	agreed	MBMS
33.246	021	-	Rel-6	Clarification of MSK key management	C	6.0.0	S3-35	S3-040819	Revised	MBMS
33.246	021	1	Rel-6	Clarification of MSK key management	C	6.0.0	S3-35	S3-040851	Revised	MBMS
33.246	021	2	Rel-6	Clarification of MSK key management	C	6.0.0	S3-35	S3-040889	Revised	MBMS
33.246	021	3	Rel-6	Clarification of MSK key management	C	6.0.0	S3-36	S3-040972	Revised	MBMS
33.246	021	4	Rel-6	Clarification of MSK key management	C	6.0.0	S3-36	S3-041011	Revised	MBMS
33.246	021	5	Rel-6	Clarification of MSK key management	C	6.0.0	S3-36	S3-041018	Revised	MBMS
33.246	021	6	Rel-6	Clarification of MSK key management	C	6.0.0	S3-36	S3-041041	Revised	MBMS
33.246	021	7	Rel-6	Clarification of MSK key management	C	6.0.0	S3-36	S3-041124	Revised	MBMS
33.246	021	8	Rel-6	Clarification of MSK key management	C	6.0.0	S3-36	S3-041126	agreed	MBMS
33.246	022	-	Rel-6	Modification of delivery of MIKEY RAND field in MSK updates	C	6.0.0	S3-35	S3-040833	Revised	MBMS
33.246	022	1	Rel-6	Modification of delivery of MIKEY RAND field in MSK updates	C	6.0.0	S3-35	S3-040856	agreed	MBMS

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	Status	WI
33.246	023	-	Rel-6	OMA DRM DCF for protection of download services	C	6.0.0	S3-36	S3-040903	Revised	MBMS
33.246	023	1	Rel-6	OMA DRM DCF for protection of download services	C	6.0.0	S3-36	S3-041123	Revised	MBMS
33.246	023	2	Rel-6	OMA DRM DCF for protection of download services	C	6.0.0	S3-36	S3-041128	agreed	MBMS
33.246	024	-	Rel-6	MBMS MSK management	F	6.0.0	S3-36	S3-040961	Revised	MBMS
33.246	024	1	Rel-6	MBMS MSK management	F	6.0.0	S3-36	S3-040961	Postponed	MBMS
33.246	025	-	Rel-6	NAF ID in MBMS	C	6.0.0	S3-36	S3-040997	rejected	MBMS
33.246	026	-	Rel-6	Specify CSB-ID format	F	6.0.0	S3-36	S3-041009	rejected	MBMS
33.246	027	-	Rel-6	MUK lifetime handling with push solicited pull procedure	C	6.0.0	S3-36	S3-041011	rejected	MBMS
33.246	028	-	Rel-6	Shorter MKI	C	6.0.0	S3-36	S3-041019	Revised	MBMS
33.246	028	1	Rel-6	Shorter MKI	C	6.0.0	S3-36	S3-041119	agreed	MBMS
33.246	029	-	Rel-6	Removal of ID_i in MIKEY response messages for MSKs	F	6.0.0	S3-36	S3-041020	rejected	MBMS
33.246	030	-	Rel-6	MUK ID in MBMS	C	6.0.0	S3-36	S3-041021	rejected	MBMS
33.246	031	-	Rel-6	Specify how to identify the MUK	C	6.0.0	S3-36	S3-041012	rejected	MBMS
33.246	032	-	Rel-6	Specify how to identify the MUK and MRK	C	6.0.0	S3-36	S3-041012	rejected	MBMS
33.246	033	-	Rel-6	Handling of MBMS identities and definition completion/modification Specify how to identify the MUK and MRK	C	6.0.0	S3-36	S3-041121	Revised	MBMS
33.246	033	1	Rel-6	Handling of MBMS identities and definition completion/modification Specify how to identify the MUK and MRK	C	6.0.0	S3-36	S3-041127	agreed	MBMS
33.817	001	-	Rel-6	Bluetooth security and configuration considerations for Annex of TR 33.817	B	6.0.0	S3-36	S3-040926	revised	WLAN
33.817	001	1	Rel-6	Bluetooth security and configuration considerations for Annex of TR 33.817	B	6.0.0	S3-36	S3-041105	revised	WLAN
33.817	001	2	Rel-6	Bluetooth security and configuration considerations for Annex of TR 33.817	B	6.0.0	S3-36	S3-041150	agreed	WLAN
33.817	002	-	Rel-6	Terminology update to not rule out the use of the smart card for security enhancements	F	6.0.0	S3-36	S3-041002	revised	USIM-Reuse
33.817	002	1	Rel-6	Terminology update to not rule out the use of the smart card for security enhancements	F	6.0.0	S3-36	S3-041107	revised	USIM-Reuse
33.817	002	2	Rel-6	Terminology update to not rule out the use of the smart card for security enhancements	F	6.0.0	S3-36	S3-041152	agreed	USIM-Reuse
33.919	001	-	Rel-6	Key safety with usage	F	6.0.0	S3_35	S3-040735	rejected	GAA
33.919	002	-	Rel-6	Removal of unnecessary editor's notes	D	6.0.0	S3_36	S3-040977	agreed	GAA
43.020	002	-	Rel-6	Clarifications to VGCS/VBS ciphering mechanism	F	6.0.0	S3-35	S3-040785	Revised	SECGKYV
43.020	002	1	Rel-6	Clarifications to VGCS/VBS ciphering mechanism	F	6.0.0	S3-35	S3-040872	Revised	SECGKYV
43.020	002	2	Rel-6	Clarifications to VGCS/VBS ciphering mechanism	F	6.0.0	S3-36	S3-040925	agreed	SECGKYV
43.020	003	-	Rel-6	Clarifying the mandatory support of A5 algorithms within mobile stations	F	6.0.0	S3-36	S3-040955	Revised	SECGKYV
43.020	003	1	Rel-6	Clarifying the mandatory support of A5 algorithms within mobile stations	C	6.0.0	S3-36	S3-041028	Revised	SECGKYV
43.020	003	2	Rel-6	Clarifying the mandatory support of A5 algorithms within mobile stations	C	6.0.0	S3-36	S3-041075	agreed	SECGKYV

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	From	Source TD	Comment/Status
S3-040893	LS (from GERAN WG2) on ëCiphering for Voice Group Call Servicesí	GERAN WG2	G2-040627	Noted
S3-040894	Response LS (from SA WG1) regarding application selection for GBA	SA WG1	S1-040924	Noted
S3-040895	Reply LS (from SA WG2) on Generic Authentication Architecture (GAA)	SA WG2	S2-043406	Noted
S3-040896	Reply LS (from SA WG2) on Generic Access Network (GAN)	SA WG2	S2-043413	Noted
S3-040907	Liaison Statement (from SA WG4) on Reception Acknowledgement for MBMS	SA WG4	S4-040631	Response in S3-041033
S3-040908	Liaison Statement (from SA WG4) on MBMS User Service architecture	SA WG4	S4-040633	Noted
S3-040915	LS (from T WG2) on EAP Authentication commands for WLAN interworking and improved security for UICC generic access	T WG2	T2-040471	Contribution in S3-041022. LS out in S3-041149
S3-040937	LS from ETSI SAGE: Proposed key derivation function for the Generic Bootstrapping Architecture	ETSI SAGE	SAGE (04) 23	Assumptions confirmed.
S3-041034	Liason Statement (from IREG): Request for Comments on Proposed Security Enhancements to GSM/GPRS Networks	GSMA IREG	IREG Doc 48_016	Noted
S3-041035	Response LS (from SA WG2) on GUP Security Recommendations	SA WG2	S2-043841	Response LS in S3-041099
S3-041036	LS (from SA WG2) on Security Aspects of Early IMS Systems	SA WG2	S2-043846	Response in S3-041045
S3-041037	LS from SA WG2: RE: The relationship between Scenario 2 and Scenario 3 authentication procedures	SA WG2	S2-043859	Noted. Included in response in S3-041101
S3-041044	Reply (from CN WG4) to LS on Reply to Evaluation of the alternatives for SMS fraud countermeasures	CN WG4	N4-041691	Noted. Contributions to next meeting to provide response LS
S3-041045	LS from CN WG4: The relationship between Scenario 2 and Scenario 3 authentication procedures	CN WG4	N4-041589	Response in S3-041101
S3-041046	LS from CN WG4: Need for the IMSI at the PDG	CN WG4	N4-041590	Response in S3-041102
S3-041047	Reply LS (from CN WG4) on Security aspects of early IMS systems	CN WG4	N4-041605	proposal from Vodafone in S3-041063
S3-041048	Reply LS (from CN WG1) on Security aspects of early IMS systems	CN WG1	N1-042078	proposal from Vodafone in S3-041061
S3-041054	Reply Liaison Statement (from SA WG2) on Reception Acknowledgement for MBMS	SA WG2	S2-043863	Noted
S3-041056	Reply LS (from SA WG5) on Reception Acknowledgement for MBMS Charging	SA WG5	S5-044786	Noted
S3-041058	Reply LS (from SA WG2) on Revisiting forwards compatibility towards TLS based access security	SA WG2	S2-043893	Noted. CR in S3-040886 not approved
S3-041064	LS from OMA BAC: Status of OMA Mobile Broadcast Services	OMA BAC	OMA-BAC-2004-0069	M Blommaert to run e-mail discussion and create LS response

E.2 Liaisons from the meeting

TD number	Title	TO	CC
S3-041065	LS on Clarification of SA3 work on Selective Disabling of UE Capabilities WI	**SA WG1**	**-**
S3-041111	LS on Control of simultaneous sessions in WLAN 3GPP IP access	**SA WG2, CN WG1, CN WG4**	**-**
S3-041129	LS on Adapting OMA DRM v2.0 DCF for MBMS download protection	**OMA BAC DLDRM**	**-**
S3-041133	Response LS on Reception Acknowledgement for MBMS	**SA WG4**	**SA WG5, SA WG2, SA WG1**
S3-041134	LS on MBMS work progress	**TSG T, T WG3**	**-**
S3-041141	LS Request for advise on handling IETF draft for Rel-6	**TSG SA**	**CN WG1**
S3-041144	~~LS on key separation for GSM/GPRS encryption algorithms~~ LS on impacts of early IMS security mechanisms	**CN WG3**	**-**

TD number	Title	TO	CC
S3-041145	LS to SA2 on Early IMS issues	**SA WG2**	**CN WG1, CN WG3, CN WG4**
S3-041146	LS on key separation for GSM/GPRS encryption algorithms	**ETSI SAGE**	**-**
S3-041147	Response LS to CN WG4: The relationship between Scenario 2 and Scenario 3 authentication procedures	**CN WG4**	**SA WG2, CN WG1**
S3-041148	Reply to LS on Need for the IMSI at the PDG	**CN WG4**	**SA WG3 LI Group**
S3-0411546	LS on GUP Security and the Proposed Changes to TS 23.240	**~~CN~~SA WG2**	**CN WG4**

Annex F: Actions from the meeting

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).

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.

AP 36/03: Silke Holtmanns to provide a WID for Liberty Alliance / GAA work for the next meeting.

AP 36/04: Silke Holtmanns to provide a CR to 33.220 to clarify the coding of P2 as characters into octet strings.

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.

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.