3GPP TSG SA WG3 Security — SA3#36 S3-040891
November 23-26, 2004
Shenzhen, China

3GPP TSG SA WG3 (Security) meeting #35 DRAFT REPORT
5-8 October 2004
Malta, EU

Source: SA WG3 Secretary (Maurice Pope, MCC)

Title: Draft Report of SA3#35 version 0.0.5 (with revision marks)

Status: Draft for Approval 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 editor's 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 app~~or~~roved 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

~~It was reported that the UEA2/UAI2 algorithm work is planned to start in November 2004 as agreement has been reached for the funding of the work.~~

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 editor’s 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 “conditionally” proceed with their specification work on Early IMS security but, rather, that “the resultant SA WG3 TR should be a 3GPP internal TR in the 33.8xx range without any impact on current specifications”. 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 ~~which was~~ 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 “gateway” 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 ‘SMS fraud countermeasures’. 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 – 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 “default USIM” is not defined in 3GPP specifications, and that the term “selection” 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 “last selected USIM” and “last selected ISIM”. 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) Nokia

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 user’s 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 don’t 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 ~~were~~ 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 it~~'~~s 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 – among other things – 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 WG4's, SA WG3 should use its' security expertise and evaluate the different available solutions, present the pros and cons of each and potentially propose a "default" protocol (or a small set of options to chose from) to CN WG4 with an LS.

TD S3-040786 GUP Security – 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 us of TLS with Server certificates should be made mandatory.~~ 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.
- Ericsson also proposed how the security work should be finalised. This is described in section 2.2 of the contribution.
- 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 "official name space numbers"*

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 "official numbers". 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~~7~~ 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~~8~~ 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. Sébastien 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 Compétences 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 – 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 editor's 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 – 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~~59~~	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 – 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 – 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: Implementors' test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:changed to Rel-4

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:changed to Rel-4
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE TSG#11:Formerly 35.209 Rel-99 (but never made available)
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	4.0.1	Rel-4	S3	WRIGHT, Tim	
TR	41.033	Lawful Interception requirements for GSM	4.0.1	Rel-4	S3	MCKIBBEN, Bernie	
TS	41.061	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	4.0.0	Rel-4	S3	WALKER, Michael	SP-15: Not to be promoted to Rel-5.
TS	42.009	Security Aspects	4.0.0	Rel-4	S3	CHRISTOFFERSSON, Per	SP-15: Not to be promoted to Rel-5.
TS	42.033	Lawful Interception; Stage 1	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
TS	43.020	Security-related network functions	4.0.0	Rel-4	S3	GILBERT, Henri	
TS	43.033	Lawful Interception; Stage 2	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
Release 5 3GPP Specifications and Reports							
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	5.0.0	Rel-5	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4 .
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031. Created from 42.031 Rel-5.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards). .
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031. Created from 43.031 Rel-5.
TS	23.035	Immediate Service Termination (IST); Stage 2	5.1.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards). .
TS	33.102	3G security; Security architecture	5.5.0	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: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	5.0.0	Rel-5	S3	WRIGHT, Tim	.
TR	41.033	Lawful Interception requirements for GSM	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
TS	42.033	Lawful Interception; Stage 1	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
TS	43.020	Security-related network functions	5.0.0	Rel-5	S3	GILBERT, Henri	.
TS	43.033	Lawful Interception; Stage 2	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
Release 6 3GPP Specifications and Reports							
TS	33.102	3G security; Security architecture	6.2.0	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 §4. .
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 §5 & 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

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~~Visited network issuing subscriber certificates~~	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 – 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 – 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.