3GPP TSG SA WG3 Security — SA3#35 **S3-040691**
October 5-8, 2004
St Paul's Bay, Malta

3GPP TSG SA WG3 (Security) meeting #34 **Draft Report**
6-9 July 2004
Acapulco, Mexico

Source: **SA WG3 Secretary (M. Pope, MCC)**

Title: **Draft report of SA WG3 meeting #34 - Version 0.0.6rm**

Status: **Draft Report version 0.0.6 with revision marks**

Report for: **Approval**

View from Hyatt Hotel, Acapulco, Mexico

Contents

Draft Report

1 Opening of the meeting

The SA WG3 Chairman welcomed delegates to the meeting on behalf of the hosts, the North American Friends of 3GPP.

2 Agreement of the agenda and meeting objectives

TD S3-040450 Draft Agenda for SA WG3 meeting #34. The SA WG3 Chairman introduced the draft agenda and explained the primary meeting objectives:

- The major objective of the meeting is to develop TS 33.246 (and also TR 33.919) into a state where they can be submitted to TSG SA Meeting #25 for approval.
- Another important objective is to try to close the remaining open issues and to eliminate the editor's notes in the Rel-6 TSs and TRs that are already under change control (33.141, 33.220, 33.221, 33.222, 33.234, 33.310, 33.817).

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. New documents were also recorded in the list.

4 Meeting reports

It was noted that no SA WG3 LI Group meetings had been held since the last SA WG3 meeting. CRs from their next meeting will be sent for approval via e-mail for 2 weeks for comments and a further 2 weeks for final approval.

4.1 Approval of the report of SA3#33, Beijing, China, 10-14 May, 2004

TD S3-040451 Draft report of SA3#33 - version 0.0.6 (with revision marks). This was provided by the SA WG3 Secretary and was reviewed. Minor changes were made and the report was approved as version 1.0.0, which will be placed on the FTP server by the Secretary.

Status of actions from the last meeting:

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

AP 33/02: T. Haukka to start an e-mail discussion on TD S3-040357. Comments to be provided by 11 June 2004 for reporting the result of the discussions to the next meeting. Result in S3-040558. Completed.

AP 33/03: SA WG3 Chairman to report to TSG SA the proposal to remove the use of A5/2. This was reported in the presentation to TSG SA and received no comment. Completed.

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

AP 33/05: C. Blanchard to provide contribution to clause 7 of TR 33.919 at next SA WG3 meeting. Result in S3-040530. Completed.

AP 33/06: Operators to consider the default domain name suggestion by SA WG2 in TD S3-040373 and contribute to the next meeting. No feedback was forthcoming. This will be dealt with again under 7.9.2 at this meeting to develop a response to SA WG2. Ongoing.

AP 33/07: D. Mariblanca to collect comments for the WiFi Alliance document in TD S3-040253. Deadlines: Comments by 31 May 2004. Draft reply by 2 June 2004. Approval of reply by 7 June 2004. Response LS sent, included in TD S3-040464 for information. Completed.

AP 33/08: C. Blanchard to lead an e-mail discussion on (U)SIM Security re-use by Peripheral devices. Final comments by 22 June for input to next meeting. Result in TD S3-040468. Completed.

4.2 Report from SA#24, Seoul, South Korea, 7-10 June, 2004

TD S3-040452 Chairman's Report from SA#24 plenary. This was introduced by the SA WG3 Chairman which provided feedback from the TSG SA meeting #24. The report had been sent to the SA WG3 e-mail list after the TSG SA meeting and was reviewed and noted.

5 Reports and Liaisons from other groups

5.1 3GPP working groups

There were no specific contributions under this agenda item. Liaisons from other 3GPP WGs were handled under their relevant Work Item agenda points.

5.2 IETF

There were no specific contributions under this agenda item.

5.3 ETSI SAGE

There were no specific contributions under this agenda item. Liaisons from ETSI SAGE were handled under their relevant Work Item agenda points.

5.4 GSMA

TD S3-040492 LS from GSMA Security Group: Report and request for work item on IST. This was introduced by the GSMA Chairman (C. Brookson and encouraged SA WG3 to again take forward the work item on IST). GSMA is looking for support at SA WG3 for this issue. ~~<RETURN> <Charles to give more text on A5/2 issues>~~

5.5 3GPP2

The 3GPP2 Liaison officer (M. Marcovici) reported the relevant developments in 3GPP2 security work. Among other items, it was reported that WLAN Security was progressing well and bootstrapping schemes are soon to be approved. Wireless firewall work is progressing and stage 1 is expected to be completed in 1 or 2 cycles. PoC work is also progressing and expected preliminary output in a month or 2. A report from the 3GPP2 Security group to 3GPP2 was provided in TD S3-040588 for further information. This report was noted.

5.6 OMA

There were no specific contributions under this agenda item. Liaisons from OMA Groups were handled under their relevant Work Item agenda points.

5.7 Other groups

TD S3-040569 TISPAN-3GPP June 04 joint meeting notes. This was introduced by C. Blanchard (BT Group) and provided personal notes on the joint meeting. C. Blanchard was thanked for the useful report and delegates were asked to take this into account during the IMS discussions at this meeting. The report was then noted.

6 Joint session with TR-45 AHAG on AKA issues (Thursday 8 July, 2pm-4pm)

6.1 Presentation of AKA usage at AHAG side

TD S3-040626 Status of AKA in TIA Standards. The 3GPP2 TIA TR-45 AHAG Chairman (F. Quick) presented the status of AKA work in TIA Standards.

Questions asked by AHAG:

- Are the jointly-controlled clause numbers still correct?
  Yes. Members were reminded that the joint control agreement should be considered when any changes to these clause numbers are proposed, where AHAG also need to be consulted before finalising changes. The AHAG Chairman agreed to check on the status of this in the 3GPP2 SDO (ATIS)
- Are the document revisions referenced in TIA-946 still applicable?
  It was clarified that TS 33.103 is not maintained by SA WG3 as it was intended to provide initial integration guidelines and it is not necessary to update it. The referenced version is therefore correct. The creation of new releases creates a new version and this should be considered for the joint control reference list.
- Is there any additional material that might be considered for joint control?
  None identified at present.
- Any other issues?
  None identified.

6.2 Presentation of AKA usage at 3GPP side

TD S3-040645 Presentation of AKA usage in 3GPP. The SA WG3 Vice Chairman (P. Howard) presented the status of AKA work in 3GPP.

Slide 18: It was clarified that session keys are derived on an application specific basis and not shared between all applications.

6.3 Discussion about future co-operation

It was agreed that there was currently no need to change the co-operation agreement and this can be revisited at the next joint session.

7 Work areas

7.1 IP multimedia subsystem (IMS)

TD S3-040463 LS (from SA WG2) on interim IMS security. This was dealt with at TSG SA Plenary and copied to SA WG3 for information and was noted.

TD S3-040482 Proposed CR to 33.203: Deletion of old authentication vectors in S-CSCF after re-synchronization (Rel-5). This was introduced by Nokia and was modified to show impacted specification in TD S3-040634 which was approved.

TD S3-040483 Proposed CR to 33.203: Deletion of old authentication vectors in S-CSCF after re-synchronization (Rel-5). This was introduced by Nokia and was modified to show impacted specification in TD S3-040635 which was approved.

TD S3-040484 Proposed CR to 33.203: IMS Service Profile is independent from Implicit Registration Set (Rel-6). This was introduced by Nokia and was discussed. It was agreed that there should be a reference to 23.228 rather than changing text to align with this specification. The CR was revised in TD S3-040636 and approved.

TD S3-040531 Forwards compatibility to TLS based access security. This was introduced by Ericsson and discussed standardization gaps in current IMS standards that may make the potential use of TLS difficult in the future. Ericsson proposed that SA WG3 adapts a new naming requirement in 33.203 both in Rel-5 and Rel-6 and CRs to implement this proposal were attached. Ericsson also proposed that SA WG3 sends an LS to CN WG1, CN WG4, SA WG2 and GSMA on the issue. A proposal for the LS was provided in TD S3-040532.

It was questionable whether this informative annex could be added to release 5 and the need for it at present for Rel-6 was also questioned. It was agreed that the change should be limited to the additional text in section 8.2 for Rel-6 only. The CR was updated in TD S3-040639 and was approved.

TD S3-040532 Draft LS to CN WG1 and CN WG4: Forwards compatibility to TLS based access security in IMS. This was modified editorially in line with the agreements for the ~~CR~~ LS in TD S3-040646 which was revised to remove GSMA from the CC: list in TD S3-040684 and was approved.

TD S3-040558 Authenticating the CSCF peer in a hybrid network (IMS and non-IMS interworking). This was introduced by Nokia and was provided as a result of an e-mail discussion which Nokia were asked to run concerning issues about authenticating the CSCF peer in a Rel-6 IMSd and the feasibility of re-using the available Rel-5 IMS to IMS internetwork signalling. It was concluded that an IPsec based tunnel is insufficient to resolve the authenticating issue in hybrid-mode of IMS in Rel-6. It was proposed that SA WG3 identify the issue and endorse the main idea presented in the contribution. There was some objection to abandoning the IPsec from Rel-5 when providing Rel-6 security and the issues raised could be overcome by using different (logical) ~~Security Gateways~~ CSCFs for handling traffic to IMS and non-IMS networks ~~traffic~~. The parts of the changes which were agreed were provided in a CR in TD S3-040641 which was approved.

Early IMS Security:

TD S3-040548 Proposed WID: Security for early IMS. This was introduced by Vodafone in response to the request at TSG SA Plenary. It was commented that the reasons that this is needed was not clear in the WID and it was questioned whether this could be added to the justification part. It was clarified that there is an initial draft TR available in TD S3-040549 which could be used to clarify the requirements to TSG SA. The WID was updated after discussion in TD S3-040637 and was approved.

TD S3-040549 New TR on early IMS security. This was introduced by Vodafone and proposed a first draft of the TR for early IMS security requirements. Related documents TD S3-040485 and TD S3-040579 were considered.

TD S3-040485 Interim security solution for early IMS implementations (S3-040265 commented by Nokia). This was introduced by Nokia and provided comments on a contribution used as base text for the draft TR on early IMS security.

TD S3-040579 Comments to S3-040549: New TR on early IMS security. This was introduced by Ericsson and provided comments to the initial draft TR on early IMS security. It was commented that some of these comments were beyond the early IMS security requirements. It was commented that the intention of this work would be for existing equipment to access IMS and the advanced features of terminals and UICCs should not be expected to use this as they can use the Rel-5 or Rel-6 standardised security mechanisms. It was agreed that the solution should be kept as simple as possible, while providing the maximum security possible and the scope of this needs further discussion.

It was decided that interested Members should discuss these issues off-line and provide a new draft TR version and an LS to other groups.

After the discussion new proposed text for the Early IMS access security was produced and reviewed. It was suggested to present this TR for information to TSG SA in order that a wider audience can consider the ideas involved in this. It was agreed to provide this to TSG SA as an informative TD, clarifying that this is an initial draft and that the provisions are open for discussion and modification within SA WG3. The draft version 0.0.2 was allocated to TD S3-040685.

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

TD S3-040550 MAPsec contributions from SA plenary. This was provided for information and was noted.

TD S3-040581 Comments to S3-040550: SMS Fraud countermeasure. This was introduced by Siemens on behalf of Siemens and Vodafone. This was provided as a comment to the contribution in TD S3-040550 and proposed a solution specifically for SMS fraud that could be deployed within a much shorter timeframe than MAPsec. Siemens suggested that the proposed solution seems to require minimal standardisation/implementation effort. It was proposed to send an LS to CN WG4 and T WG2 (copied SA WG2) asking for comments on the feasibility of the proposed solution. It was noted that this only shows SMS threats that can be tackled using MAPsec and there are other threats which MAPsec can be used to fight against. It was decided to draft an LS referring to this contribution asking for comments on the feasibility which was provided in TD S3-040642 which was reviewed and approved.

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

TD S3-040560 Proposed CR to 33.210: SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network (Rel-6). This was withdrawn by Nokia as it depended upon the agreement for introducing TLS.

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

TD S3-040545 Proposed CR to 33.310: Splitting the Roaming CA into a SEG CA and an Interconnection CA (Rel-6). This was introduced by Vodafone on behalf of Vodafone, T-Mobile and Siemens. Nokia added their support to this CR. The CR was updated to show a figure as a deletion and addition (which did not show properly in this CR) in TD S3-040643 which was approved.

7.5 UTRAN network access security

TD S3-040455 Reply LS (from RAN WG3) on LS on Re-authentication and key set change during inter-system handover. This was introduced by Siemens and was noted.

TD S3-040462 Response LS to N1-040501 (from RAN WG2) on Re-authentication and key set change during inter-system handover. This was introduced by Siemens. RAN WG2 asked CN WG1, RAN WG3 and SA WG3 to reply to the following questions where the answers lie within their domain of expertise:

1) Is it the understanding that the specifications permit that the AKA procedure providing new keys to the UE may be performed significantly in advance of the corresponding Security/Ciphering Control procedures that activate these new keys? If so, in what proportion of cases does this currently occur?

2) Are the new keys that are not activated considered as new keys in the next signalling connection? (i.e. “Key Status” to RNC is indicated as ‘new’ in the security mode command.)

3) Could SA WG3 clarify what the intention of their specification is, especially with respect to the scenario described above?

A response LS explaining SA WG3 interpretation of the stage 2 was provided in TD S3-040644 which was reviewed and revised editorially in TD S3-040686 which was approved. If any problems are identified by RAN WG2 with this understanding, then CRs can be considered at the next SA WG3 meeting.

7.6 GERAN network access security

TD S3-040595 LS (from SA WG1) on removal of A5/2 algorithm in Release 6 MEs. This was introduced by Orange and acknowledged the request from SA WG3 to create CRs to remove support of A5/2 in Release 6 MEs. SA WG1 did not believe that any change is needed up to GSM Release 1998. SA WG1 reported that they thought the

selection of algorithms is outside the scope of SA WG1. The SA WG3 Chairman undertook to look into how to have the requirements implemented in the specifications.

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.

TD S3-040528 Analyse of the countermeasures to Barkan-Biham-Keller attack. This was introduced by Orange on behalf of Orange and Nokia and discussed the alternatives to protect against Barkan-Biham-Keller attack and proposed to select the Special RAND mechanism. ~~CRs to implement this were provided in TD S3-040xxx .~~ Comments to this proposal were provided in TD S3-040574.

TD S3-040574 Comments on Orange/Nokia contribution S3-040528 regarding domain separation. This was introduced by Vodafone and discussed the authenticated ciphering instruction mechanism to protect from these attacks. Vodafone believed that the claim in TD S3-040528 that the authenticated ciphering instruction mechanism does not provide any domain separation is misleading due to the fact that the authenticated ciphering instruction mechanism protects against the spread of the Barkan-Biham-Keller attack and that special RAND does not offer any significant advantages over the authenticated ciphering instruction mechanism with regard to domain separation. Vodafone believed that the conclusion of the analysis in TD S3-040263 is still valid and proposed that the authenticated cipher instruction mechanism should be adopted in preference to the special RAND mechanism.

Qualcomm and Ericsson expressed a preference for the authenticated cipher instruction mechanism. Siemens suggested that more time is given to consider this problem more thoroughly before making the decision and to postpone this to Rel-7.

Nokia commented that this has been discussed in SA WG3 for a long time now and further discussion time should not be necessary. The Special-RAND mechanism has been proposed in CRs, whereas there are no proposals for the implementation of the authenticated cipher instruction mechanism. Vodafone responded that the discussions in other groups has not been too great and the impact of these late Rel-6 CRs could cause problems.

It was agreed to postpone this work and not include it in Rel-6 and further contribution on this was encouraged in order to finalise the work as soon as possible for Rel-7.

TD S3-040572 An observation about Special RAND in GSM. This was superseded by the decision above and was noted.

TD S3-040534 On the introduction and use of UMTS AKA in GSM. This was introduced by Ericsson and discussed an inexpensive way to introduce UMTS AKA in GSM without the need for SIM replacements and proposed that this promising approach should be studied further. It was commented that this adds another implementation option which should be avoided wherever possible. Members were asked to consider this proposal and provide comments and discuss over the e-mail list.

7.7 Immediate service termination (IST)

The GSMA Security Group had discussed the IST issue (see TD S3-040492) and encouraged SA WG3 to again take forward the work item on IST. GSMA is looking for support at SA WG3 for this issue. Companies (particularly those listed as supporting the work) were asked to consider this and provide contribution.

7.8 Fraud information gathering system (FIGS)

There were no specific contributions under this agenda item.

7.9 GAA and support for subscriber certificates

7.9.1 TR 33.919 GAA

TD S3-040530 Pseudo-CR: Application guidelines to use GAA. This was introduced by BT on behalf of Alcatel, BT and Nokia. Some changes were made to the figure and text in section 7.1 and the Pseudo CR was revised in TD S3-040640 and this Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040513 Pseudo-CR: key safety with usage. This was introduced by Huawei. This was discussed and it was recognised that there is no corresponding text in the current TS and it was considered premature to add it at this time. Huawei were asked to propose this at a later time and delegates were asked to consider the proposals.

TD S3-040454 LS (from CN WG4) on Requirement for presence of the GAA-Application-Type AVP. This was introduced by Vodafone and asked SA WG3 to provide guidance to CN WG4 on which of the two understandings of the intent of GAA is correct. A response LS was prepared in TD S3-040649 which was reviewed and approved.

It was agreed to forward the GAA TR (33.919) to TSG SA for approval.

7.9.2 TS 33.220 GBA

The LS received at the previous meeting, TD S3-040373 "Reply (from SA WG2) to Liaison on Service Discovery of BSF and PKI portal" was considered. No problems had been identified with the proposal but no CRs had been contributed to this meeting. Nokia were asked to provide CRs to include this in the specifications for the next meeting.

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

TD S3-040487 GBA: Using IPsec or TLS to secure the Zn-reference Point. This was introduced by Siemens on behalf of Siemens and Nokia and studied further the advantages and disadvantages of IPsec and TLS for protecting the Zn reference point. The proposals were acceptable and related CR was provided in TD S3-040647.

TD S3-040647 CR: Securing Zn reference point. This was introduced by Nokia on behalf of Siemens and Nokia and was approved.

TD S3-040465 CR: Generic Ua interface requirements. This was introduced by Nokia and was approved. It was noted that the Core Network is also affected and this will be ticked for presentation to TSG SA.

TD S3-040504 CR: Detailing of key lifetime. This was introduced by Siemens and provided a justification and attached CR to better specify the key lifetime requirements. The attached CR was approved.

TD S3-040539 CR: B-TID generation. This was introduced by Nokia and was approved. It was noted that the ME is also affected and this will be ticked for presentation to TSG SA.

TD S3-040466 Transfer of application-specific user profiles in GAA. This was introduced by Nortel Networks and described a flexible and scalable alternative solution to obtain the identities and other profile information needed by the NAFs from the HSS by extending the Sh interface using pseudonyms.

> **Proposal 1:** SA WG3 agree that storage and retrieval of application-specific information (user profile information) is out of scope of the Generic Authentication Architecture.
> **Proposal 2:** SA WG3 agree to the alternative solution described in this paper for communicating the authenticated identity to the NAF in GAA.
> **Proposal 3:** Send LS to other relevant 3GPP groups requesting their views on non-IMS applications using the Sh interface from Rel-6 onwards.
> **Proposal 4:** Send LS to CN WG1/CN WG4, informing them of SA WG3's decision and requesting them to start the work on extending the Sh interface for Rel-6.

If the proposals are accepted, Nortel Networks volunteered to provide the necessary change requests to implement these proposals to the GAA specifications.

Comments were provided by Nokia and Siemens in TD S3-040500 *Solutions for transfer of User Security Settings - (User-Profile)* which argued that the Sh interface is not appropriate for User Security Settings transfer between Networks (inter-Domain), which will be needed for some services (e.g. MBMS). Siemens and Nokia recommended the use of Zh and Zn for the USS transfer.

It was agreed that the Zh and Zn approach should be used for Rel-6 but other mechanisms should be further considered for Rel-7 taking into account the amount of information that is needed for Rel-7 services.

TD S3-040514 BSF control of VPLMN services can be used by the UE. This was introduced by Huawei and discussed the necessity that BSF control of the services that can be visited by UE in the visited network and proposed that SA WG3 endorse the following:

> *When the Transaction Identity retrieve request is from D-proxy in the Visited Network, the BSF should check whether the UE can use the service in the Visited Network.*

The proposal was supported but it was recognised that the implementation of such a requirement in the BSF needs to be studied. The principle was therefore endorsed and discussions should continue over e-mail in order to provide a CR to the next meeting.

TD S3-040501 CR: GBA User Security Settings. This was introduced by Siemens on behalf of Nokia and Siemens. The CR was modified to clarify the definitions and an editors note in TD S3-040650 and was approved.

TD S3-040502 CR: User security settings. This was introduced by Siemens on behalf of Nokia and Siemens and was approved.

TD S3-040503 CR: GBA User Security Settings. This was introduced by Siemens on behalf of Nokia and Siemens and was approved.

TD S3-040648 Use of USIM and ISIM in GBA. This was introduced by Nokia on behalf of Nokia, Siemens, Gemplus and Motorola and presented the results of off-line discussions of TD S3-040508, TD S3-040591, TD S3-040592 and TD S3-040593 which were replaced by this contribution. 2 CRs were attached to implement the proposals and it was also proposed to write an LS to SA WG1, SA WG2 and T WG2 (CC: T WG3) to ask them their view on user involvement during UICC application selection. TIM commented that they preferred the simple solution to have USIM-based GBA, rather than ISIM-based. The attached CR to 33.220 was reviewed and approved. The attached CR to 33.141 was reviewed and approved. An LS was provided to inform SA WG1, SA WG2 and T WG2 (CC: T WG3) and the CRs attached in TD S3-040651 which was approved.

TD S3-040655 GBA_U Evening session report (Thursday, July 8th). An evening session was held to deal with the large number of GBA_U-related contributions and this report provided to the group to explain the discussions and agreements made at the session. The report was noted and the session chairman and participants were thanked for their co-operation at this late session.

TD S3-040654 CR: Introduction of GBA_U AUTN generation in the BSF. This was introduced by Axalto after discussion at the evening session. and was approved.

TD S3-040653 UICC-ME interface for GBA-U. This was introduced by Axalto and was created after the evening session. Three CR proposals were attached offering slightly different solutions for the mechanisms. There was a comment that perhaps the Ks_int and Ks_ext could be replaced with a single Ks Key but this would need further investigation. No consensus on which option to choose could be reached and it was agreed to send an LS to T WG3 with this issue for their opinion. This LS was provided in TD S3-040664 which was approved.

TD S3-040564 This was split into two documents TD S3-040662 and TD S3-040663 as a result of the evening session discussions.

TD S3-040662 Proposed CR to 33.220: Removal of the definition of a default type of NAF-specific key (Rel-6). This was introduced by Gemplus. The removal of the default NAF_ext was objected to, and the CR was revised in TD S3-040665 which was updated to remove the double revision marks in TD S3-040687 which was approved.

TD S3-040663 Proposed CR to 33.222: Precision on the NAF-specific key to use to secure Ua interface in case of GBA_U (Rel-6). This was withdrawn as it was not agreed to remove the default NAF_ext (see TD S3-040662).

TD S3-040540 CR: GBA_U: generic functions for Ks_int_NAF usage. This was rejected based on the discussions at the evening session.

The following contributions were covered by discussions in the evening session and were not dealt with in the SA WG3 Plenary:

TD S3-040475 Alternative to Special Random or AMF indication for GBA_U: MAC indication.
TD S3-040580 Comments to S3-040475 (Alternative to Special Random or AMF indication for GBA_U: MAC indication).
TD S3-040585 Comments to S3-040580.
TD S3-040490 CR: Introducing the Special-RAND mechanism for GBA_U.
TD S3-040477 GBA_U Scenarios and Rel 6 MEs capabilities.
TD S3-040491 GBA: The support of GBA features within a Rel-6 ME.
TD S3-040576 GBA: The support of GBA features within a Rel-6 ME.
TD S3-040478 CR: Requirement on ME capabilities for GBA_U.
TD S3-040488 CR: Unaware GBA_U MEs, which are GBA_ME aware only shall be allowed.
TD S3-040515 Clarification of Ks_ext.
TD S3-040498 GBA: GBA_U derivations.
TD S3-040533 CR: GBA_U: storage of Ks_ext in the UICC.
TD S3-040537 CR: GBA_U: Ks_ext not stored on UICC.
TD S3-040536 CR: GBA_U: key derivation procedure modified; Nokia, Siemens (CR+ppt-slides).
TD S3-040575 GBA_ME/GBA_U scenarios in UE att S3-040536 commented/revised by Axalto.

The SA WG3 Chairman reported that he would highlight to TSG SA the need for further functional changes in the GBA_U work after September 2004.

7.9.3 TS 33.221 Subscriber certificates

TD S3-040505 CR: Editorial cleanup. This was introduced by Nokia and was approved.

TD S3-040506 CR: Cleanup of procedure description. This was introduced by Nokia and was approved.

TD S3-040507 CR: Removal of unnecessary editor's notes. This was introduced by Nokia and was approved.

7.9.4 TS 33.222 HTTPS-based services

TD S3-040472 LS (from CN WG1) on Authentication Proxy. This was introduced by Lucent technologies. CN WG1 asked SA WG3 for clarification on where in the IMS architecture a separate authentication proxy exists and whether such a separate authentication proxy can be discovered by the UE. It was considered that the Proxy can exist in all those places and as it is a reverse-Proxy, no UE discovery is needed and the UE is unaware of it. A response LS was provided in TD S3-040652 which was approved.

TD S3-040473 LS from OMA SEC WG: Reply to LS on Presence Security. This was introduced by **3** and in response to the LS from SA WG3 in TD S3-040194, informed SA WG3 that OMA SEC WG are not working on updating WAP-219. According to the OMA rules, there will not be any changes made to WAP interoperability specifications. OMA Security would have to issue an OMA enabler with the changes in a new format suggested by SA WG3. This was not anticipated in the Rel-6 time frame. It was noted that WAP-219 allows for other cipher suites, e.g. AES. This was noted and delegates were asked to keep this in mind for Presence Security issues.

TD S3-040538 CR: GBA supported indication and NAF hostname transfer in HTTP and in PSK TLS. This was introduced by Nokia on behalf of Nokia and Siemens. This was updated to clarify the NOTE 2 and revised in TD S3-040656 which was approved.

TD S3-040551 CR: Further modifications to the division of TLS profile related text in 33.141 and 33.222. This was introduced by Ericsson on behalf of Ericsson and Siemens. The cover pages of the attached CRs needed completing and this was done for the CR to 33.141 in TD S3-040657 , which was approved, ~~and~~ the CR to 33.222 was amalgamated with the change in TD S3-040547 into TD S3-040658 which ~~were~~ was approved.

7.10 WLAN interworking

TD S3-040456 LS from SA WG1: Current UICC for W-LAN interworking. This was introduced by Telecom Italia and was provided for information. The LS was noted.

TD S3-040457 LS reply (from SA WG1) on multiple connections to VPLMNs simultaneously. This was introduced by the WLAN Rapporteur and asked SA WG3 to provide comment on whether simultaneous UE connections to

multiple VPLMNs can be provided without reducing the security provided by 3GPP. it was considered best to wait until discussion of TD S3-040494 before responding to this LS. It was agreed that TD S3-040668~~00~~ should be attached to a response LS which was provided in TD S3-040667 which was revised in TD S3-040688 and approved.

Secretary's note: As the attachment was not mentioned in the LS, it was again revised after the meeting in TD S3-040689 including attachments TD S3-040352, TD S3-040440 and TD S3-040668.

TD S3-040453 LS (from CN WG1) on Storage of temporary identities for EAP authentication. This was introduced by Ericsson and informed T WG3 of CN WG1's decision for storage of temporary identities for EAP authentication. CN WG1 had decided that the WLAN UE has to store all temporary identities for EAP authentication in the USIM, if appropriate Elementary Files (EF) are available in the USIM cards issued by the operator. If appropriate EFs are not available, then they are to be stored in the ME. It was commented that this was against the SA WG3 advice to CN WG1 in TD S3-040196 (from meeting #32). It was not clear whether these parameters should be available on the ME after power-off, and it should be clarified to CN WG1 that they should not be available after power-off, as indicated in the original LS from SA WG3. A response LS was provided in TD S3-040589 which was revised in TD S3-040666 and approved.

TD S3-040464 Reply LS on Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0. This had been approved by e-mail and sent after the SA WG3 meeting #33 and was noted.

TD S3-040467 WLAN: Justification for the introduction of a WLAN application. This was introduced by Gemplus and analysed the use of WLAN application and concluded that the use of a WLAN application offers a higher security level and the standardization of this application is not an issue. Gemplus recommended that SA WG3 adopt the WLAN application and send an LS to SA WG1 for consultation and to T WG3 to ask them to work on WLAN application. Comments from Nokia to this were provided in TD S3-040571 and were then considered.

> TD S3-040571 Comments to S3-040467: WLAN: Justification for the introduction of a WLAN application (Gemplus). This was introduced by Nokia and asks the following questions related to the Gemplus contribution:
> - It is already a clear requirement to use an old UICC, meaning the ME needs to support EAP anyway.
> - Do we need to duplicate the function in UICC?
> - What is Gemplus' proposal to ME based EAP function? Replace it or as another option?
>
> It was clarified that in the WLAN pre- (or re-) authentication procedure is not yet included in 3GPP specifications, but it exists in IEEE specifications and is likely to be an issue later.

It was questioned how the Gemplus solution related to TD S3-040456 where an early UICC was assumed to support WLAN interworking. Gemplus clarified that both solutions would be possible but a UICC would be the preferred use for the UICC with this WLAN application installed.

It was commented that it was not clear whether the proposal would imply a separate WLAN application (i.e. independent Keys) and this issue should be clarified to ease discussion of whether the benefits of putting EAP on the UICC are sufficient to justify the changes required to the specifications. More information was considered necessary to convince operators that such a change to the UICC specification was really necessary, providing the advantages gained over the ME-solution, which would be supported anyhow.

It was decided that discussion would be necessary in order that SA WG3 can provide TSG SA with the decision on UICC support for Release 6 or for a future Release. It was decided to have an evening session to discuss this and report back to SA WG3 in order to have a clear message to TSG SA and other groups on the SA WG3 assumptions for this. Gemplus provided a contribution after the evening session in TD S3-040590 which was presented. It was agreed the outcome of these discussions should be brought to the attention of TSG SA.

AP 34/03: Chairman to bring outcome of WLAN/UICC discussions to attention of TSG SA (see TD S3-040590).

TD S3-040574 Comments on Orange/Nokia contribution S3-040528 regarding domain separation. This was introduced by Vodafone and was taken as background for discussions and returned to~~.~~ for discussions. The full document was presented under agenda item 7.6.

TD S3-040526 Proposed CR to 33.234: References update (Rel-6). This was introduced by Ericsson and was modified to remove changes to references 3 and 29 in TD S3-040599, which was then approved.

TD S3-040494 Proposed CR to 33.234: Correction to restriction on simultaneous WLAN sessions (Rel-6). This was introduced by Huawei and was discussed. It was decided that this needed further off-line discussion and a new version produced. This was provided in TD S3-040600 and reviewed. It was updated editorially in TD S3-040668 which was approved.

TD S3-040512 Proposed CR to 33.234: Sending of temporary identities from WLAN UE (Rel-6). This was introduced by Huawei on behalf of Samsung and Huawei. Some editorial changes were made and the CR revised in TD S3-040601, which was approved.

TD S3-040525 Proposed CR to 33.234: Introduction of protected result indications (Rel-6). This was introduced by Ericsson and was discussed. The optional use by both sides was questioned and the value of the mechanism as a security mechanism was questioned. The CR was updated in TD S3-040602 to more clearly express the requirements which was revised to remove the double revision marks in TD S3-040670 and was approved.

TD S3-040524 Proposed CR to 33.234: Clarification on fast re-authentication procedure (Rel-6). This was introduced by Ericsson. The revision marks did not show in the CR so it was re-produced in TD S3-040603, which was approved.

TD S3-040555: Proposed CR to 33.234: Update reference to RFC3748 "Extensible Authentication Protocol (EAP)" (Rel-6). This was introduced by Lucent Technologies and was approved.

TD S3-040522: Security threats in Wa interface. This was introduced by Ericsson and analysed the potential risks associated with the sending of the Pairwise Master Key (PMK) from the 3GPP AAA server to the WLAN AN (over the Wa interface) and did not identify any attack and suggested that the encryption of the AVP containing the PMK with integrity protection secures the interface adequately and proposed that the editors note in section 4.2.2 of 33.234 should therefore be removed. It was proposed to replace the editors' note with text mandating the use of IPsec for DIAMETER unless the interface is physically protected, in which case IPsec is recommended. SA WG3 decided that this needed further consideration before mandating the protection mechanism to use for RADIUS and the issue was left for further discussion until the next meeting and e-mail discussion and contribution was encouraged. The CR to implement these changes, in TD S3-040523 was revised in TD S3-040604 to include these agreements. The CR was revised to remove the double revision marks in TD S3-040669 which was approved.

TD S3-040521: IPsec tunnels and W-APNs. This was introduced by Ericsson and analysed the need for singular or multiple IPsec ESP tunnels in scenario 3 and showed that, from a security point of view, both solutions are feasible. The other aspects (performance, complexity) should be studied more in detail in order to take a correct decision. Ericsson recommended that other groups are contacted in order to assess these aspects and suggested an LS be sent to SA WG2. There were some comments on this and it was agreed that an LS should be drafted to SA WG2 containing the agreements and questions of SA WG3 which was provided in TD S3-040605 which was reviewed and approved.

TD S3-040459: Clarification on Addresses used for Tunnel Establishment. A response to this LS was provided by Siemens in TD S3-040510 which was considered with this LS. The response was considered and updated editorially in TD S3-040606 and was approved.

TD S3-040527: Proposed CR to 33.234: Wm interface description (Rel-6). This was introduced by Ericsson. TD S3-040493 proposed changes for the same text and was also considered.

TD S3-040493: Proposed CR to 33.234: IPsec tunnelling establishment procedures (Rel-6). This was introduced by NTT DoCoMo. A comparison of these two proposals was provided by Ericsson in TD S3-040577:

TD S3-040577: Comparison of two CRs about tunnel authentication. This was introduced by Ericsson and analysed the two proposals for the Wm interface in TD S3-040527 and TD S3-040493. Ericsson proposed to adopt Ericsson's CR for Wm interface description. However, there are still some open issues to be addressed:

- Simultaneous access control when authenticating in scenario 3. Covered in NTT's CR but still needs to be studied in detail.

- Re-authentication procedure for scenario 3 has to be added to TS 33.234. Covered in NTT's CR but some corrections have to be performed, as indicated in the analysis above.

Ericsson also suggested that the Wg interface is not security-related and should be left for other groups.

It was decided to produce a combination CR to take the issues raised by Ericsson and NTT DoCoMo into account and this was provided in TD S3-040607 which was revised to remove the double revision marks in TD S3-040671 which was approved.

TD S3-040562: Binding Scenario Information to Mutual EAP Authentication. This was introduced by Nokia and discussed two mechanisms to prevent MITM attacks, when the EAP-IKEv2 is used in the WLAN interworking. Nokia proposed that the EAP-IKEv2 with the EAP-SIM/AKA is used to provide mutual authentication and either NAI or special RAND is used to provide protection against the MITM attacks. Siemens reported that the draft mentioned in section 3 (EAP-IKEv2) did not address the issue, and it had been confused with another draft not so well progressed in the IETF. The NAI proposal for short-term was considered a candidate for further study. It was greed to ask SA WG2 about these proposals and restrictions on the NAI and this was provided in TD S3-040608 which was revised in TD S3-040672 and approved.

TD S3-040511: Example of using EAP-AKA/EAP-SIM within IKEv2 for Mutual Authentication between UE and PDG. This was introduced by Huawei on behalf of Samsung and Huawei. It was not considered appropriate to introduce an Annex into the document which contains an editors' note about it being removed when the decision is made. The CR was therefore not approved, but SA WG3 were asked to keep this decision on choices in mind.

TD S3-040486: Proposed CR to 33.234: Conditional support of NAT (Rel-6). This was introduced by Nokia. Siemens objected that this could lead to incompatible products on the market. It was clarified that NAT support was intended to be mandatory for implementation, but not always used. This was clarified in the CR, which was updated in TD S3-040609. As a result of evening discussions, this was then withdrawn.

TD S3-040495: Proposed CR to 33.234: Correction for authentication procedure of WLAN UE split (Rel-6). This was introduced by Huawei. The CR was updated in TD S3-040610 with a corrected specification number and was approved.

TD S3-040594: Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces). Bluetooth security and configuration considerations for Annex A4 of TS 33.234 (Wireless Local Area Network (WLAN) interworking security). This was introduced by Toshiba on behalf of Toshiba, BT, Intel Corporation and supporting companies. The CR proposes to add text to 33.234 in order to give information on the Bluetooth interworking as studied in the internal 3GPP TR 33.817. Comments on this proposal were provided in TD S3-040578.

TD S3-040578: Open issues on (U)SIM security re-use. This was introduced by Ericsson on behalf of Ericsson and Nokia and provided arguments against the proposals provided in TD S3-040594.

TD S3-040587: Response to Comments on "Open issues on (U)SIM security re-use (S3-040578). This was introduced by Toshiba and provided arguments against the comments in TD S3-040578.

The large amount of changes were considered rather late to be included in Release 6, as many problems with references to URLs, requirements lists with no reference to the Stage 3 details (many of which were considered by some companies as implementation-dependent rather than standardisation issues), etc. Toshiba pointed out that the draft CR was made available on the server and an opportunity for participation in conference calls was made (the conference calls were cancelled due to lack of participation).

It was considered a useful idea to split this large CR up into separate smaller ones so that discussions could focus on individual issues and to arrange conference calls to resolve the comments received on these issues.

Raziq Yaqub (Toshiba) agreed 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 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. Updated proposals to be provided to the next SA WG3 meeting including a minimum security level for Security Re-Use scenarios.

Interested Members were asked to clarify exactly the most contentious issues they have with the proposals. It was decided to start this off with an evening off-line session during the meeting, to clarify the problematic parts in the proposals.

TD S3-040611 Results of the off-line meeting on "CR on (U)SIM Security re-use. This was introduced by Toshiba and reported the results of an off-line evening discussion held during the meeting. It was noted that SA WG3 had not *reversed* any decisions as mentioned in the report concerning the structure of the proposed CR, but the proposed split into more consistent topics was requested to allow the issues to be considered in isolation in order to clarify the proposals for change to the specifications. Toshiba also requested an additional conference call on 26 July 2004 08.30 Eastern USA Time, delegates who were available should try to participate in this call. Participation especially in the other 2 conference calls was expected from interested parties in order to progress these discussions. The draft CRs provided in TD S3-040627 TD S3-040628 and TD S3-040629 were noted and should be used as a basis for the discussions in the first conference call.

AP 34/04: Raziq Yaqub to arrange 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.

TD S3-040474: LS from Terry Bourk, Chair of Bluetooth Architecture Review Board: Response to S3-040197. This LS was introduced by Selim Aissi (Intel Corporation, Member of both SA WG3 and Bluetooth SEG). This LS requested SA WG3 to provide feedback and advice on the requirements for new commands needed to support the EAP-SIM Split scenario 2 (see TD S3-040197). It was clarified that the timescales for the specification work should be about 1 year to approve recommendations and another 6 months to 1 year to have it finally approved by Bluetooth SIG. This does not preclude pre-implementation by the chip manufacturers and the interworking test prototype work.

No issues were raised about the new Bluetooth security proposal by the Members at the meeting, and It was decided that this should be a subject of the conference calls in AP 34/04 and a draft response provided based on these discussions.

TD S3-040481: Proposal for Enhancing Bluetooth Security Using an Improved Pairing Mechanism. This was provided by Intel Corporation, Ericsson Mobile Platforms AB and Nokia Research and was presented by Intel

Corporation. Intel and the supporting companies requested SA WG3 to provide feedback and advice on the requirements on this new security algorithm which was already approved by the BARB. The new solution enhances Link Key strength while maintaining short PINs, therefore natively enhancing Bluetooth security. Any comments on the issues should be sent to Selim Aissi by 16 July 2004. The presentation was then noted.

TD S3-040480: Trust Requirements for Open Platforms in WLAN-WWAN Interworking. This was introduced by Intel Corporation (Selim Aissi) and addressed the appropriate 3GPP trust requirements for an Open Platform, based on a platform architecture comprised of hardware and software with security features that can be used as a basis for establishing trust in the entire OP. With the enhanced trust, a 3GPP infrastructure that includes OP's can support various mobile business applications and enable emerging data service businesses (e.g. DRM, Web Services) and asked SA WG3 to take into account this proposal for further security discussions. Intel was thanked for the presentation and it was recognised that if any work is needed in 3GPP, a WID will be needed at a future SA WG3 meeting while care should be taken that the work does not overlap with work being done elsewhere (e.g. TCG). It was clarified by Intel that that TD S3-040481 is more specific to 3GPP security requirements (no such work is being done in TCG or any other group) and that the document provides a security proposal solutions beyond the current scope of TCG. It was decided that off-line discussions should take place between interested Members and the WID be proposed if work on this in SA WG3 is considered necessary, based on these discussions.

TD S3-040567: Comment (in form of CR to S3-040272): Session Key Exchange Algorithm (SKEA) for Local Interface Trusted Tunnel Establishment. This was introduced by Intel and provided changes to their previous contribution in TD S3-040272 (which was provided at SA WG3 meeting #33 and was noted for use in future proposals). It was clarified that this showed how shared secrets can be used for the proposal instead of certificates. It was commented that this needs to be considered in more detail before adopting the proposed protocols in SA WG3. It was also pointed out that this would require algorithm work, which may then bypass the Bluetooth Security solutions and that WID(s) would be needed in SA WG3 if it is decided to continue with this proposal. It was recommended that this work should start with a supported WID and the type of deliverable (TR, TS, Study) decided and proposed to SA WG3 for discussion and agreement.

TD S3-040597 Reply (from SA WG1) to LS on Correlation of I-WLAN Access and Service Authorization (S2-042347/S1-040562). This was noted and delegates were asked to consider this off line and provide any comments if considered necessary.

TD S3-040625 LS from IETF LEMONADE: LEMONADE for MMS over 3GPP Interworking WLANs. This was provided for information and was noted. Delegates were asked to check the impacts of this off-line.

7.11 Visibility and configurability of security

There were no specific contributions under this agenda item.

7.12 Push

There were no specific contributions under this agenda item.

7.13 Priority

There were no specific contributions under this agenda item.

7.14 Location services (LCS)

There were no specific contributions under this agenda item.

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

There were no specific contributions under this agenda item. The contributions on this subject were related to WLAN interworking and were handled under agenda item 7.10.

7.16 Open service architecture (OSA)

There were no specific contributions under this agenda item.

7.17 Generic user profile (GUP)

TD S3-040458 Reply LS (from SA WG2) on GUP security status in SA3 and on collaboration of 3GPP and Liberty Alliance Project. This was introduced by Nokia and asked SA WG3 to inform SA WG2 about the completion of the GUP Security-related issues and any changes needed. TD S3-040521 contained some information which could be used to fulfil this request.

TD S3-040561 GUP Security Open Issues. This was presented by Ericsson on behalf of Ericsson, Nokia and Intel. The presentation described how the GUP issues are dealt with by the Liberty Alliance work and provided references to their documents for further study by delegates. The source companies proposed that this contribution and the attached presentation should provide enough arguments to SA WG3 in order to be able to close the remaining open items around GUP Security and in order to be able to endorse LAP-WSF specifications as the security and privacy solution to be used in GUP. If agreed, other impacted WGs (i.e. SA WG2 and CN WG4) should be informed to proceed to include references to relevant LAP-WSF security and privacy specifications as previously suggested in TD S3-040338. This was agreed and a Liaison to this effect was provided in TD S3-040623 which was reviewed and updated in TD S3-040673 which was approved.

7.18 Presence

TD S3-040616 Proposed CR to 33.141: Editorial cleanup of TS 33.141 (Rel-6). This was introduced by Siemens. The cover page was corrected in TD S3-040659 which was approved.

TD S3-040617 Editorial clean-up of 33.222. This was introduced by Ericsson. The cover page was corrected in TD S3-040660 which was approved.

TD S3-040546 Proposed CR to 33.141: Clarification on Ut interface (Rel-6). This was introduced by Vodafone on behalf of Vodafone and Ericsson. The cover page was corrected in TD S3-040661 which was approved

TD S3-040556 Proposed CR to 33.141: PSK TLS and SSC support (Rel-6) This was covered by the CR in TD S3-040616 and so was withdrawn.

7.19 User equipment management (UEM)

There were no specific contributions under this agenda item.

7.20 Multimedia broadcast/multicast service (MBMS)

TD S3-040460 Liaison statement (from SA WG4) on DRM protection for PSS. This was introduced by Ericsson. SA WG1 asked SA WG3 to review the working assumption for DRM protection of PSS and provide any comments. It was decided to review this off line and a response draft LS to SA WG4 was provided in TD S3-040613 which was updated to remove the CC: in TD S3-040674 which was approved.

TD S3-040461 Reply LS (from SA WG4) on MBMS security issues. This was introduced by Nokia and responds to the questions asked in the LSs from SA WG3 (TD S3-040443 and TD S3-040444). SA WG4 asked SA WG3 delegates interested in these MBMS Security issues to join the SA WG4 ad-hoc meeting, possibly 23rd August 2004 (to be confirmed). Only around 4 delegates indicated their willingness to attend this joint session in Prague and it was decided to send a response LS which was provided in TD S3-040614 which was updated in TD S3-040675 and approved. **It was noted that the introduction of the SRTP proposal was dependent on the agreements at the joint meeting and if no agreement is reached then it may be too late to introduce any new solutions into Rel-6.**

TD S3-040598 LS (from SA WG1) on MBMS key Management. This was introduced by Vodafone and reported that SA WG1 have taken into account the considerations reported by SA WG3 in TD S3-040445 and agreed that a combined ME/UICC solution is the best way forward. The attached CR was considered which stated that the ME key management support can be optionally supported, which appeared in contradiction to the LS (should be mandatory to support it on the ME). It did not seem to take into account that the BSF may not support GBA_U and even if UICC support is available, it may be necessary to use the ME mechanism. **It was noted that TD S3-040598 will probably need to be reviewed again at the next SA WG3 meeting.**

TD S3-040470 Proposed editorial changes to main body of TS 33.246. This was introduced by Siemens on behalf of Siemens and Ericsson. This Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040469 Proposed changes to Annex C of TS 33.246. This was introduced by Siemens. The notes to C.2 and C.3 were considered as misleading, as the Bearer confidentiality protection is not provided and so can not be disabled in these cases. The editor was asked to correct the notes to make them more factual. With this, the Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040535 Proposed CR to 33.246: User authentication in MBMS (Rel-6). This was introduced by Ericsson. The last editors note in 6.2.4 should be moved to become the 3rd editors note of 6.2 and the proposed editors note in 6.2.1 was rejected. With these changes the Pseudo-CR was agreed for inclusion by the editor in the draft TS.

TD S3-040489 N to N relationship between User Services and Transport Services. This was introduced by Siemens and proposed changes (Pseudo-CR) to the MBMS draft. It was commented that the use of the same MSK over different protocols is not allowed (re-use of a single MTK). It was decided to include this in the changes. The Pseudo-CR was updated to include the changes in TD S3-040615. These changes were combined into TD S3-040621 and was therefore withdrawn.

TD S3-040543 Feasibility of Subscription based key management. This was introduced by Ericsson and analysed the feasibility of subscription-based management using a GBA and MIKEY approach for MBMS key management. It concluded that this was feasible if some requirements are met, the benefit of the approach would however depend on SA WG4 decisions (i.e. there is questionable benefit if SA WG4 define an application layer joining procedure). This contribution was noted and should be taken into account when the SA WG4 decisions are known.

TD S3-040554 Push and pull key management. This was introduced by Ericsson and investigated Push and Pull issues using MIKEY. The proposals conclusions were contained in a Pseudo-CR in TD S3-040565.

TD S3-040565 Pseudo-CR to 33.246: Push and pull key management for MBMS (Rel-6). This was introduced by Ericsson and detailed the changes needed if the proposal in TD S3-040554 is agreed. Some comments had been made off line which would need to be included if the principle is agreed. It was also commented that a solution which avoids redundant message duplication could be devised. There was general support for the efficiency of the proposal but it was recognised that the changes may be effected by other agreements made on these sections as a result of other contributions. The principles of the Pseudo-CR were therefore agreed for inclusion in the draft TS.

TD S3-040542 Combined vs. Separate Key Delivery. This was introduced by Ericsson and discussed two approaches of using separate delivery of encryption and integrity keys in contrast to deriving the two keys from one master key and concluded that there should be only one "master key" delivered to the terminal, and this key should then be split into as many keys as required to satisfy the security protocols. A related Pseudo-CR had been provided by Nokia in TD S3-040520 which was also considered.

TD S3-040520 Pseudo-CR to 33.246: Concatenated MSK delivery in MBMS (Rel-6). This was introduced by Nokia and proposed the concatenation of the encryption and integrity Keys to transfer in a single MIKEY payload. A conflicting Pseudo-CR proposal for section 6.4 was provided in TD S3-040582.

TD S3-040582 Updated S3-040544 as comments to S3-040479 and S3-040563. Pseudo-CR to 33.246: Key management mechanism (Rel-6) (section 6.4 changes). This was presented by Ericsson and used in discussions.

Comments from other Members was requested in order to help decide which solution to adopt. Siemens stated that the use of MIKEY protocols appeared to push the balance in favour of the Ericsson proposal in TD S3-040582. Due to the time pressure for completion of the MBMS draft, Nokia agreed to adopt the Ericsson approach and keep their solution as backup in case of problems found in the future.

TD S3-040479 UICC-ME interface for MBMS. This was introduced by Gemplus on behalf of Axalto, Gemplus and OCS. Taking into account the schedule constraints for Rel-6, the source companies asked SA WG3 to complete the necessary SA WG3 CRs at this meeting and to inform the impacted WGs of the final result of the ME-UICC interface for MBMS. It was clarified that the request was to solve as many of the open issues as possible in the TS and to include the remaining issues as editors' notes in the draft to be presented to TSG SA for approval. The Pseudo-CR for an annex specifying the UICC-ME interface was considered and it was agreed that it should be revised in light of other agreements made at this meeting. The Pseudo-CR was revised in TD S3-040618 and updated again in TD S3-040676 which was agreed for inclusion by the editor in the draft TS.

TD S3-040541 Harmonized Key Management for Streaming and Download. This was introduced by Ericsson and discussed in more detail how key management in MBMS can be performed using MIKEY. A Pseudo-CR to implement this proposal was provided in TD S3-040582. It was asked how dependent upon the use of SRTP this proposal was. It was clarified that MIKEY is independent of the security protocol, although as MIKEY was developed along with SRTP, some common values are used and these may need to be redefined if another protocol is used. It was commented that the protocol part should be separated from the mechanism (MIKEY) part in the TS.

TD S3-040582 Updated S3-040544 as comments to S3-040479 and S3-040563. Pseudo-CR to 33.246: Key management mechanism (Rel-6) (section 6.4 changes). Comments from Axalto were provided in TD S3-040584 which was reviewed. These comments and other comments made were incorporated into an updated Pseudo-CR in TD S3-040619 and updated again in TD S3-040677 which was agreed for inclusion by the editor in the draft TS.

TD S3-040573 (updated 563) Handling MSKs and decrypting download data in MBMS. This was introduced by **3**. and proposed the format of an MSK identifier and a method of handling MSKs for certain services. A Pseudo-CR was attached to implement these proposals into the draft TS. It was recognised that the changes in 6.3 would need to be incorporated into the Ericsson changes and it was agreed to include these changes into the revised Pseudo-CR in TD S3-040619. The other changes were agreed for inclusion in the draft TS.

TD S3-040557 MBMS Download Protection. This was introduced by Ericsson and discussed protection of download objects in MBMS and shows that S/MIME does not provide integrity protection using symmetric keys, and that the public key based signatures that are provided do not cover the FDT. Other methods are also discussed. Ericsson therefore proposed to not consider the use of S/MIME but to study the use of XML-encryption for integrity protection. Delegates were invited to study this issue and provide contribution to the next meeting. **The current working assumption on use of S/MIME should therefore also be reviewed.**

TD S3-040552 SRTP for protecting of MBMS streaming data. This was introduced by Ericsson and proposed to choose SRTP for protection of MBMS streaming. A Pseudo-CR implementing this proposal was attached. It was noted that SA WG4 had indicated that there were other protection mechanisms available and that they should be asked to elaborate on this in the joint meeting. This proposal was therefore agreed conditionally upon further details from SA WG4. **The editor was asked to include this proposal along with an editors note in 6.5.1 indicating that the other solutions hinted at by SA WG4 are to be investigated and may be changed at the next SA WG3 meeting.** The editor pointed out that the Download text in section 7 would need restructuring to make the final text consistent. This was provided in TD S3-040620 which was agreed for inclusion in the draft TS.

TD S3-040553 Source Origin Authentication in MBMS. This was introduced by Ericsson and discussed the status of a mechanism which could provide Source Of Origin authentication. Ericsson concluded that threats involved due to lack of integrity protection and SOA need to be studied further. Attack on key identifiers seems to be one threat requiring SOA. Ericsson concluded that, in the meantime, it should be ensured that SOA is a possible way forward in the future Releases and noted that work is under way to add SOA support in SRTP (as mentioned in TD S3-040552). A Pseudo-CR introducing this threat and corresponding requirement in TS 33.246 was attached. It was commented that this could introduce requirements into Rel-6 which cannot be mitigated in the Rel-6 timescale. It was therefore suggested that these requirements be added for Rel-7. The threats were therefore accepted for inclusion in Rel-6 in order to allow mitigation measures to be developed by operators. The requirements should be kept for Rel-7. The Pseudo-CR was revised in TD S3-040621 including the changes for TD S3-040615 and was reviewed and agreed for inclusion in the draft TS.

It was agreed to create an LS to impacted groups to inform them of the updated MBMS TS (after the Editor has included all the agreed changes) which is to be presented to TSG SA for approval. The finalised TS was allocated to TD S3-040678. This LS was provided in TD S3-040622 and reviewed and updated in TD S3-040679 and was approved (to be sent when the final draft of TS 33.246 is ready in TD S3-040678).

7.21 Key Management of group keys for Voice Group Call Services

TD S3-040596 LS from SA WG1: SA WG1's answer to LS on VGCS and VBS security. This was introduced by Siemens. SA WG1 provided two CRs to the stage 1 specifications TS 42.068 and TS 42.069 which had been agreed in SA WG1. The CRs were briefly reviewed and no problems noted. Delegates were asked to forward any comments to their SA WG1 colleagues. The LS was then noted.

TD S3-040471 LS from ETSI SAGE: Responses on cryptographic aspects of VGCS. SAGE provided responses to the questions asked in TD S3-040446 "*Liaison Statement on VGCS and VBS security*". SAGE analysed the counter length verses random part (recommended at least 24 bit random part) and suggested that a VSTK_RAND of 38 to 40 bits allows many more calls than a VSTK_RAND of 32 bits. For the second question, SAGE recommended that the KMF should have the (roughly defined) property that, for a fixed but unknown VSTK, no significant statistical relationship can be predicted between the members of a given set of outputs {(V_Kci)} for a chosen set of inputs {(CGIi, CELL_GLOBAL_COUNTi)}. A discussion paper based on this was provided in TD S3-040496.

TD S3-040496 VGCS: Considerations on key generation and key modification. This was introduced by Siemens and proposed that SA WG3 approves following parameter lengths and KMF:

a) The length of CELL_GLOBAL_COUNT is 2 bits
b) VSTK_RAND has a length of 38 bit. If GERAN prefers or can accommodate only 36 bits (+2 bits for CELL_GLOBAL_COUNT), the length of VSTK_RAND is 36 bits.
c) An informal section on how to avoid colliding VSTK_RAND during the lifetime of V_Ki is included in the specification.
d) The key modification function KMF is based on SHA-1.

SA WG3 discussed these proposals and agreed that they were acceptable, noting that the call duration should not exceed 12 hours in order to avoid key repetition. These proposals were therefore endorsed.

e) SA3 discusses and conditionally approves the companion CR to 43.020, in order not to delay its approval as a Rel-6 feature at SA#24. If it is found desirable a CR-version with a VSTK_RAND of 36-bits could be made during SA3#34.
f) if GERAN2 response would indicate that SA3's CR is not inline with the GERAN2's decision on major points, the CR-presentation would not be done at SA#24 (September). Minor inconsistencies and errors could still be corrected at SA3#35 (November).
g) to inform GERAN2 of the latest CR version and status in SA3.
h) to tell GERAN2 that SA3 wishes to have (38+2)-bits available if possible but can live with 36+2 bits.

The final choice would be dependent upon GERAN WG2 decisions and Siemens provided 2 CRs for 36-bit and 38-bit versions in TD S3-040624 and proposed to conditionally approve the CRs depending upon GERAN WG2 decisions.

SA WG3 endorsed the principles in e) to h) and the CRs reviewed.

TD S3-040624 Proposed CR to 43.020: Introducing VGCS/VBS ciphering (Rel-6). This was introduced by Siemens and provided 2 CRs, 36-bit and 38-bit alternatives. These CRs were endorsed conditionally upon the GERAN WG2 decisions. The 36-bit version of the CR was approved and provided in TD S3-040638.

- An LS to GERAN WG2 was provided in TD S3-040630 which was reviewed and revised in TD S3-040680 and approved.

- An LS to ETSI SAGE was provided in TD S3-040631 which was reviewed and revised in TD S3-040681 and approved.

7.22 Guide to 3G security (TR 33.900)

There were no specific contributions under this agenda item.

7.23 Other areas

TD S3-040583 Selective Disabling of UE Capabilities; updated S3-040566 based on the comments on SA3 mailing list. This was introduced by Nokia and proposed some initial text for the study on threats and protection mechanisms that could exist from malicious programs on terminals. The final bullet in the document should highlight that there is a risk that even uninfected terminals may be denied access to certain services. It was agreed to highlight this and develop this document further for liaison to SA WG1 to add to the study work item. It was suggested that the document does not tackle prevention and detection of attacks. Members were asked to consider this in order to update the document and provide material to the author (T. Koskinen). The updated version was provided in TD S3-040632 and revised to include comments in TD S3-040682 and was agreed. The LS to SA WG1 was provided in TD S3-040633 which was reviewed and updated in TD S3-040683 and approved.

8 Review and update of work programme

Rapporteurs were asked to provide updates to the work programme to the Secretary, M. Pope in order for the Work Plan to be kept accurate and up-to-date.

9 Future meeting dates and venues

China meeting : Huawei ~~Hauwei~~ asked when we want to start meeting - agreed to try 4 days in October but 2 big WIs handled in Parallel (WLAN-IW and MBMS or GAA) It was considered necessary to identify documents which can be handled in parallel and those which need to be handled in main plenary. This was discussed and it was concluded that too many delegates would need to be present in the agenda items concerned, so it was decided not to hold parallel sessions at this meeting. It was also agreed that no changes were needed for the schedule of this meeting and it will start on Tuesday 23 November, 09.00 and end, at latest, Friday 26 November, 16.00.

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)

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#35	5-8 October 2004	Malta	EF3
S3#36	23-26 November 2004	Shenzhen, China	HuaWei Technologies
S3#37	21-25 February 2005	Australia (TBC)	Qualcomm (TBC)

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#14	19-21 July 2004	Povoa de Varzim, Portugal. Combined with ETSI TC LI	"European Friends of 3GPP"
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#25	8-10 & 13-16 September 2004	Palm Springs, USA	"NA Friends of 3GPP"
TSGs#26	8-10 & 13-16 December 2004	Athens, Greece	"European Friends of 3GPP"
Meeting	**2005**	**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

10 Any other business

The Release 6 Functional Freezing, expected for September 2004, was discussed with respect to the stability of SA WG3 specifications for Functional freezing at this time (i.e. only corrective CRs will be made to the specifications). The following estimation of the specifications was made:

- 33.246 (MBMS): Not considered ready, some functional changes may be necessary.
- 33.234 (WLAN-IW): Not considered ready, some functional changes may be necessary.
- 33.220 (GBA): Not considered ready, some functional changes may be necessary.
- 33.221 (Subscriber Certificates): It was generally agreed that this should be ready for functional freezing in September 2004.
- 33.222 (HTTPS-based services): It was generally agreed that this should be ready for functional freezing in September 2004.
- 33.141 (Presence): It was generally agreed that this should be ready for functional freezing in September 2004.
- 33.310 (NDS/AF): It was generally agreed that this should be ready for functional freezing in September 2004. The possible use of TLS will have no impact as it is not part of the 3GPP specifications.
- 33.203 (IMS): It was generally agreed that this should be ready for functional freezing in September 2004.

Close

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, North American Friends of 3GPP, for the facilities in Acapulco, Mexico. He then closed the meeting.

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

A.1 List of attendees

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Jorge Abellan Sevilla	Axalto S.A.	jsevilla@axalto.com		+33 1 46 00 59 33	+33 1 46 00 59 31	FR	ETSI
Dr. Selim Aissi	INTEL CORPORATION SARL	selim.aissi@intel.com		+01-503 264-3349	+01-503 264-1578	FR	ETSI
Mr. Hiroshi Aono	NTT DOCOMO INC.	aono@mml.yrp.nttdocomo.co.jp		+81 468 40 3509	+81 468 40 3788	JP	ARIB
Mr. Sundeep Bajikar	INTEL CORPORATION SARL	sundeep.bajikar@intel.com		+1 408-765-3705	+1 408-765-4614	FR	ETSI
Mr. Colin Blanchard	BT GROUP PLC	colin.blanchard@bt.com	+44 7711 191835	+44 1473 605353	+44 1473 623910	GB	ETSI
Mr. Marc Blommaert	SIEMENS NV/SA	marc.blommaert@siemens.com		+32 14 25 34 11	+32 14 25 33 39	BE	ETSI
Mr. Charles Brookson	DTI	cbrookson@iee.org	+44 20 7215 3691	+44 20 7215 3691	+44 20 7215 1814	GB	ETSI
Mr. Holger Butscheidt	BMWI	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. Hubert Ertl	GIESECKE & DEVRIENT GMBH	hubert.ertl@de.gi-de.com	+49 172 8691159	+49 89 4119 2796	+49 89 4119 2921	DE	ETSI
Dr. Adrian Escott	3	adrian.escott@three.co.uk		+44 7782 325254	+44 1628 766012	GB	ETSI
Mr. Louis Finkelstein	MOTOROLA LTD	louis.finkelstein@motorola.com		+1 847 576 4441	+1 847 538 4593	GB	ETSI
Miss Sylvie Fouquet	ORANGE SA	sylvie.fouquet@francetelecom.com		+33 145 29 49 19	+33 145 29 65 19	FR	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@siemens.com		+49 8963 641494	+49 8963 648000	DE	ETSI
Mr. Peter Howard	VODAFONE GROUP PLC	peter.howard@vodafone.com	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB	ETSI
Ms. Yingxin Huang	HUAWEI TECHNOLOGIES CO., LTD	huangyx@huawei.com		+86-10-82882752	+86-10-82882940	CN	CCSA
Mr. Bradley Kenyon	HEWLETT-PACKARD	brad.kenyon@hp.com		+1 402 384 7265	+1 402 384 7030	FR	ETSI
Ms. Tiina Koskinen	NOKIA CORPORATION	tiina.s.koskinen@nokia.com		+358504821347	+358718075300	FI	ETSI
Mr. Pekka Laitinen	NOKIA CORPORATION	pekka.laitinen@nokia.com		+358 5 0483 7438	+358 7 1803 6852	FI	ETSI
Mr. Bernd Lamparter	NEC EUROPE LTD	bernd.lamparter@netlab.nec.de		+49 6221 905 11 50	+49 6221 905 11 55	GB	ETSI
Mr. Alex Leadbeater	BT GROUP PLC	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. Vesa Lehtovirta	ERICSSON INC.	vesa.lehtovirta@ericsson.com		+358405093314	+	US	ATIS
Mr. Michael Marcovici	ATIS	marcovici@lucent.com		+1 630 979 4062	+1 630 224 9955	US	ATIS
Mr. David Mariblanca	ERICSSON LM	david.mariblanca@ericsson.com		+34 646004736	+34 913392538	SE	ETSI
Mr. Semyon Mizikovsky	LUCENT TECHNOLOGIES N. S. UK	smizikovsky@lucent.com		+1-973-386-6348	+1-973-386-4555	GB	ETSI
Dr. Valtteri Niemi	NOKIA CORPORATION	valtteri.niemi@nokia.com		+358504837327	+358718036850	FI	ETSI
Mr. Anand Palanigounder	NORTEL NETWORKS	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. Frank Quick	QUALCOMM EUROPE S.A.R.L.			+1 619 658 3608	+1 619 658 2113	FR	ETSI
Mr. Bengt Sahlin	ERICSSON LM	Bengt.Sahlin@ericsson.com		+358 40 778 4580	+358 9 299 3401	SE	ETSI
Mr. Stefan Schroeder	T-MOBILE DEUTSCHLAND	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
Mr. Willy Verbestel	RESEARCH IN MOTION LIMITED	wverbestel@rim.com	+1 760 580 0200	+1 760 737 8428	+1 760 294 2125	CA	ETSI
Mr. Berthold Wilhelm	BMWI	berthold.wilhelm@regtp.de		+49 681 9330 562	+49 681 9330 725	DE	ETSI
Mr. Dajiang Zhang	NOKIA JAPAN CO, LTD	dajiang.zhang@nokia.com		+86-13901168924	+86-010-84210576	JP	ARIB
Mr. Wenlin Zhang	HUAWEI TECHNOLOGIES CO., LTD	zhangwenlin@huawei.com		+86 82882753	+86 82882940	CN	CCSA

39 attendees

A.2 SA WG3 Voting list

Based on the attendees lists for meetings- #32, #33, and #34, the following companies are eligible to vote at SA WG3 meeting #35:

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	ETSI
HuaWei Technologies Co., Ltd	CN	3GPPMEMBER	CCSA
Hutchison 3G UK Ltd (3)	GB	3GPPMEMBER	ETSI
INTEL CORPORATION SARL	FR	3GPPMEMBER	ETSI
Lucent Technologies	US	3GPPMEMBER	ATIS
Lucent Technologies Network Systems UK	GB	3GPPMEMBER	ETSI
Mitsubishi Electric Co.	JP	3GPPMEMBER	ARIB
mmO2 plc	GB	3GPPMEMBER	ETSI
MOTORAOLA SEMICONDUCTOR ISRAEL LTD	IL	3GPPMEMBER	ETSI
MOTOROLA A/S	DK	3GPPMEMBER	ETSI
MOTOROLA Ltd	GB	3GPPMEMBER	ETSI
NEC EUROPE LTD	GB	3GPPMEMBER	ETSI
NEC Technologies (UK) Ltd	GB	3GPPMEMBER	ETSI
Nippon Ericsson K.K.	JP	3GPPMEMBER	ARIB
NOKIA Corporation	FI	3GPPMEMBER	ETSI
Nokia Japan Co, Ltd	JP	3GPPMEMBER	ARIB
Nokia Telecommunications Inc.	US	3GPPMEMBER	ATIS
NORTEL NETWORKS (EUROPE)	GB	3GPPMEMBER	ETSI
Nortel Networks (USA)	US	3GPPMEMBER	ATIS
NTT DoCoMo Inc.	JP	3GPPMEMBER	ETSI
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
OBERTHUR CARD SYSTEMS S.A.	FR	3GPPMEMBER	ETSI
ORANGE SA	FR	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
Research In Motion Limited	CA	3GPPMEMBER	ETSI
Samsung Electronics Ind. Co., Ltd.	KR	3GPPMEMBER	TTA
SAMSUNG Electronics Research Institute	GB	3GPPMEMBER	ETSI
SIEMENS AG	DE	3GPPMEMBER	ETSI
Siemens nv/sa	BE	3GPPMEMBER	ETSI
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
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

51 Voting Members

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040450	Draft Agenda for SA WG3 meeting #34	SA WG3 Chairman	2	Approval		Approved
S3-040451	Draft report of SA3#33 - version 0.0.6 (with revision marks)	SA WG3 Secretary	4.1	Approval		Approved with minor change. V1.0.0 to be placed on FTP server
S3-040452	Chairmans Report from SA#24 plenary	SA WG3 Chairman	4.2	Information		Noted
S3-040453	LS (from CN WG1) on Storage of temporary identities for EAP authentication	CN WG1	7.10	Information		Response LS to clarify power-off deletion of parameters in S3-040666
S3-040454	LS (from CN WG4) on Requirement for presence of the GAA-Application-Type AVP	CN WG4	7.9.1	Action		Response in S3-040649
S3-040455	Reply LS (from RAN WG3) on LS on Re-authentication and key set change during inter-system handover	RAN WG3	7.5	Information		Noted
S3-040456	LS from SA WG1: Current UICC for W-LAN interworking	SA WG1	7.10	Information		Noted
S3-040457	LS reply (from SA WG1) on multiple connections to VPLMNs simultaneously	SA WG1	7.10	Action		Response LS in S3-040612
S3-040458	Reply LS (from SA WG2) on GUP security status in SA3 and on collaboration of 3GPP and Liberty Alliance Project	SA WG2	7.17	Action		Response LS in S3-040623 based on S3-040561
S3-040459	LS from SA WG2: Clarification on Addresses used for Tunnel Establishment	SA WG2	7.10	Action		Draft response in S3-040510 considered.
S3-040460	Liaison statement (from SA WG4) on DRM protection for PSS	SA WG4	7.20	Action		Response LS in S3-040613
S3-040461	Reply LS (from SA WG4) on MBMS security issues	SA WG4	7.20	Action		Response LS in S3-040614
S3-040462	Response LS to N1-040501 (from RAN WG2) on Re-authentication and key set change during inter-system handover	RAN WG2	7.5	Action		Response LS in S3-040644
S3-040463	LS (from SA WG2) on interim IMS security	SA WG2	7.1	Action		TSG SA asked SA3 to clarify. Noted
S3-040464	Reply LS on Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0	SA WG3	7.10	Information		Was approved by e-mail 7 June 2004 (after S3#33 meeting). Noted
S3-040465	Proposed CR to 33.220: Generic Ua interface requirements (Rel-6)	Nokia	7.9.2	Approval		Approved
S3-040466	Transfer of application-specific user profiles in GAA	Nortel Networks	7.9.2	Discussion / Decision		Not agreed for Rel-6. To be reconsidered for Rel-7
S3-040467	WLAN: Justification for the introduction of a WLAN application	GemPlus	7.10	Discussion / Decision		Nokia comments in S3-040571
S3-040468	Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces). Bluetooth security and configuration considerations for Annex A4 of TS 33.234 (Wireless Local Area Network (WLAN) interworking security)	Toshiba, BT and supporting Companies	7.15	Approval	S3-040594	Revised in S3-040594
S3-040469	Proposed changes to Annex C of TS 33.246	Siemens, 3	7.20	Discussion / Decision		Agreed. Editor to include changes to draft TS (some modification to notes agreed)
S3-040470	Proposed editorial changes to main body of TS 33.246	Siemens, 3	7.20	Discussion / Decision		Agreed. Editor to include changes to draft TS
S3-040471	LS from ETSI SAGE: Responses on cryptographic aspects of VGCS	ETSI SAGE	7.21	Discussion		Discussion paper in S3-040496
S3-040472	LS (from CN WG1) on Authentication Proxy	CN WG1	7.9.4	Action		Response in S3-040652
S3-040473	LS from OMA SEC WG: Reply to LS on Presence Security	OMA SEC WG	7.18	Information		Noted
S3-040474	LS from Terry Bourk, Chair of Bluetooth Architecture Review Board: Response to S3-040197	Terry Bourk, Chair of Bluetooth Architecture Review Board	7.10	Action		To be discussed as part of conference calls for response at next meeting

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040475	Alternative to Special Random or AMF indication for GBA_U: MAC indication	Axalto, Genplus, Oburther	7.9.2			Covered at GBA_U evening session (see S3-040655)
S3-040476	Proposed CR: Introduction of GBA_U AUTN generation in the BSF	Axalto	7.9.2	Discussion	S3-040654	New version based on evening session in S3-040654
S3-040477	GBA_U Scenarios and Rel 6 MEs capabilities	Axalto, Genplus, OCS	7.9.2	Discussion		Covered at GBA_U evening session (see S3-040655)
S3-040478	Proposed CR to 33.220: Requirements on ME capabilities for GBA_U (Rel-6)	Axalto, Genplus, OCS	7.9.2	Discussion		Covered at GBA_U evening session (see S3-040655)
S3-040479	UICC-ME interface for MBMS	Axalto, Gemplus, OCS	7.20	Discussion		Open issues to be reviewed after other contributions handled. Pseudo-CR for annex D revised in S3-040618
S3-040480	Trust Requirements for Open Platforms in WLAN-WWAN Interworking	Intel Corporation	7.10	Discussion		Noted. Interested members to discuss off-line and WID provided if necessary
S3-040481	Proposal for Enhancing Bluetooth Security Using an Improved Pairing Mechanism	Intel Corporation, Ericsson Mobile Platforms AB, Nokia Research	7.10	Information		Noted. Comments to Intel by 16 July.
S3-040482	Proposed CR to 33.203: Deletion of old authentication vectors in S-CSCF after re-synchronization (Rel-5)	Nokia	7.1	Approval	S3-040634	Revised in S3-040634
S3-040483	Proposed CR to 33.203: Deletion of old authentication vectors in S-CSCF after re-synchronization (Rel-6)	Nokia	7.1	Approval	S3-040635	Revised in S3-040635
S3-040484	Proposed CR to 33.203: IMS Service Profile is independent from Implicit Registration Set (Rel-6)	Nokia	7.1	Approval	S3-040636	Revised in S3-040636
S3-040485	Interim security solution for early IMS implementations (S3-040265 commented by Nokia)	Nokia	7.1	Discussion		Comments to S3-040265
S3-040486	Proposed CR to 33.234: Conditional support of NAT (Rel-6)	Nokia	7.10	Approval	S3-040609	Revised in S3-040609
S3-040487	GBA: Using IPsec or TLS to secure the Zn-reference Point	Siemens, Nokia	7.9.2	Discussion / Decision		Pronciples agreed. CR in S3-040647
S3-040488	Proposed CR to 33.220: Unaware GBA_U MEs, which are GBA_ME aware only shall be allowed (Rel-6)	Siemens	7.9.2	Approval		Covered at GBA_U evening session (see S3-040655)
S3-040489	N to N relationship between User Services and Transport Services	Siemens	7.20	Discussion / Decision	S3-040615	Pseudo-CR attached. Revised in S3-040615
S3-040490	Proposed CR to 33.220: Introducing the Special-RAND mechanism for GBA_U (Rel-6)	Siemens	7.9.2	Approval		Covered at GBA_U evening session (see S3-040655)
S3-040491	GBA: The support of GBA features within a Rel-6 ME	Siemens	7.9.2	Discussion / Decision		Covered at GBA_U evening session (see S3-040655)
S3-040492	LS from GSMA Security Group: Report and request for work item on IST	GSMA -SEC	7.7	Action		Noted. Delegates encouraged to consider the request to create an IMS WI
S3-040493	Proposed CR to 33.234: IPsec tunneling establishment procedures (Rel-6)	NTT DoCoMo	7.10	Approval		Combined CR in S3-040607
S3-040494	Proposed CR to 33.234: Correction to restriction on simultaneous WLAN sessions (Rel-6)	Huawei	7.10	Approval	S3-040600	Further work needed to complete CR. Updated in S3-040600
S3-040495	Proposed CR to 33.234: Correction for authentication procedure of WLAN UE split (Rel-6)	Huawei	7.10	Approval	S3-040610	revised in S3-040610
S3-040496	VGCS: Considerations on key generation and key modification	Siemens, Vodafone	7.21	Discussion / Decision		Discussed
S3-040497	Proposed CR to 43.020: Introducing VGCS/VBS ciphering (Rel-6)	Siemens, Vodafone	7.21	Approval		Covered by discussions and other CRs
S3-040498	GBA: GBA_U derivations	Gemplus, Axalto, Oberthur	7.9.2	Discussion / Decision		Covered at GBA_U evening session (see S3-040655)

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040499	UICC-ME interface for GBA-U	Gemplus, Axalto, Oberthur	7.9.2	Discussion / Decision	S3-040653	New version based on evening session in S3-040653
S3-040500	Solutions for transfer of User Security Settings -(User-Profile)	Nokia, Siemens	7.9.2	Discussion / Approval		Zh, Zn interface use preferred for Rel-6
S3-040501	Proposed CR to 33.220: GBA User Security Settings (Rel-6)	Nokia, Siemens	7.9.2	Approval	S3-040650	Revised in S3-040650
S3-040502	Proposed CR to 33.221: User security settings (Rel-6)	Nokia, Siemens	7.9.3	Approval		Approved
S3-040503	Proposed CR to 33.222: GBA User Security Settings (Rel-6)	Nokia, Siemens	7.9.4	Approval		
S3-040504	Detailing of key lifetime	Siemens	7.9.2	Discussion / Approval		CR Attached. CR Approved
S3-040505	Proposed CR to 33.221: Editorial cleanup (Rel-6)	Nokia	7.9.3	Approval		Approved
S3-040506	Proposed CR to 33.221: Cleanup of procedure descriptions (Rel-6)	Nokia	7.9.3	Approval		Approved
S3-040507	Proposed CR to 33.221: Removal of unnecessary editor's notes (Rel-6)	Nokia	7.9.3	Approval	S3-040656	Revised in S3-040656
S3-040508	Use of USIM and ISIM in GBA	Siemens	7.9.2	Discussion / Approval		CR Attached. Contained in S3-040648
S3-040509	Proposed CR to 33.141: Editorial cleanup of TS 33.141 (Rel-6)	Siemens	7.18	Approval	S3-040616	Replaced by S3-040616
S3-040510	Draft LS to SA WG2: "Clarification on Addresses used for Tunnel Establishment"	Siemens	7.10	Discussion / Approval	S3-040606	Updated in S3-040606
S3-040511	Proposed CR to 33.234: Example of using EAP-AKA/EAP-SIM within IKEv2 for Mutual Authentication between UE and PDG (Rel-6)	Samsung, Huawei	7.10	Approval		Not approved, this decision on choice to be kept in mind by delegates
S3-040512	Proposed CR to 33.234: Sending of temporary identities from WLAN UE (Rel-6)	Samsung, Huawei	7.10	Approval	S3-040601	Revised in S3-040601
S3-040513	key safety with usage	Huawei	7.9.1	Discussion / Decision		No area for this in current spec. To be considered for future work.
S3-040514	BSF control of VPLMN services can be used by the UE	Huawei	7.9.2	Discussion / Decision		Principle endorsed. E-mail discussion and CR to next meeting to implement in BSF
S3-040515	Clarification of Ks_ext	Huawei	7.9.2	Discussion / Decision		Covered at GBA_U evening session (see S3-040655)
S3-040516	TISPAN-3GPP June 04 joint meeting notes	BT Group	5.7	Information	S3-040569	Revised by S3-040569
S3-040517	ISIM usage in GAA:	Nokia, Gemplus, Alcatel	7.9.2	Discussion / Approval	S3-040591	Revised by S3-040591
S3-040518	Proposed CR to 33.220: ISIM support	Nokia, Gemplus, Alcatel	7.9.2	Approval	S3-040592	Revised by S3-040592
S3-040519	Proposed CR to 33.141: ISIM support (Rel-6)	Nokia, Gemplus, Alcatel	7.18	Approval	S3-040593	Revised by S3-040593
S3-040520	Pseudo-CR to 33.246: Concatenated MSK delivery in MBMS (Rel-6)	Nokia	7.20	Approval		Not agreed in favour of Ericsson MIKEY proposal in S3-040582. To be kept as back-up in case of future problems
S3-040521	IPsec tunnels and W-APNs	Ericsson	7.10	Discussion / Decision		LS to S2 in S3-040605
S3-040522	Security threats in Wa interface	Ericsson	7.10	Discussion / Decision		IPSec mandatory for DIAMETER, RADIUS for further discussion
S3-040523	Proposed CR to 33.234: Deletion of editor's note (Rel-6)	Ericsson	7.10	Approval	S3-040604	Revised in S3-040604
S3-040524	Proposed CR to 33.234: Clarification on fast re-authentication procedure (Rel-6)	Ericsson	7.10	Approval	S3-040603	Revised in S3-040603
S3-040525	Proposed CR to 33.234: Introduction of protected result indications (Rel-6)	Ericsson	7.10	Approval	S3-040602	Revised in S3-040602
S3-040526	Proposed CR to 33.234: References update (Rel-6)	Ericsson	7.10	Approval	S3-040599	Revised in S3-040599

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040527	Proposed CR to 33.234: Wm interface description (Rel-6)	Ericsson	7.10	Approval		Combined CR in S3-040607
S3-040528	Analyse of the countermeasures to Barkan-Biham-Keller attack	Orange, Nokia	7.6	Discussion / Decision		Comments in S3-040574. Further contribution requested. Not for Rel-6
S3-040529	Proposed CR to 43.020: Introducing the special RAND mechanism as a principle for GSM/GPRS (Rel-6)	Orange, Nokia	7.6	Approval		Similar CR for 33.102 in S3-040570
S3-040530	Pseudo-CR to 33.919: Application guidelines to use GAA (Rel-6)	Alcatel , BT , Nokia	7.9.1	Approval	S3-040640	Revised in S3-040640
S3-040531	Forwards compatibility to TLS based access security	Ericsson	7.1	Discussion / Decision		CRs Attached. Proposed LS in S3-040532. Rel-6 CR revised in S3-040639
S3-040532	Draft LS to CN WG1 and CN WG4: Forwards compatibility to TLS based access security in IMS	Ericsson	7.1	Approval	S3-040646	Revised in S3-040646
S3-040533	Proposed CR to 33.220: GBA_U: storage of Ks_ext in the UICC (Rel-6)	Axalto, Gemplus, Oberthur	7.9.2	Approval		Covered at GBA_U evening session (see S3-040655)
S3-040534	On the introduction and use of UMTS AKA in GSM	Ericsson	7.6	Discussion		Noted. E-mail discussion expected
S3-040535	Proposed CR to 33.246: User authentication in MBMS (Rel-6)	Ericsson, Nokia	7.20	Approval		Agreed with mods for inclusion in draft TS
S3-040536	Proposed CR to 33.220: GBA_U: key derivation procedure modified (Rel-6)	Nokia, Siemens	7.9.2	Approval		Covered at GBA_U evening session (see S3-040655)
S3-040537	Proposed CR to 33.220: GBA_U: Ks_ext not stored on UICC (Rel-6)	Nokia, Siemens	7.9.2	Approval		Covered at GBA_U evening session (see S3-040655)
S3-040538	Proposed CR to 33.222: GBA supported indication and NAF hostname transfer in HTTP and in PSK TLS (Rel-6)	Nokia, Siemens	7.9.4	Approval	S3-040656	revised in S3-040656
S3-040539	Proposed CR to 33.220: B-TID generation (Rel-6)	Nokia	7.9.2	Approval		Approved
S3-040540	Proposed CR to 33.220: GBA_U: generic functions for Ks_int_NAF usage (Rel-6)	Nokia	7.9.2	Approval		Rejected at evening GBA_U session
S3-040541	Harmonized Key Management for Streaming and Download	Ericsson	7.20	Discussion / Decision		
S3-040542	Combined vs Separate Key Delivery	Ericsson	7.20	Discussion / Decision		Principles noted in context with other contributions
S3-040543	Feasibility of Subscription based key management	Ericsson	7.20	Discussion / Decision		Noted. SA4 decision awaited
S3-040544	Pseudo-CR to 33.246: Key management mechanism (Rel-6)	Ericsson	7.20	Approval		Comments in S3-040584. Used in discussions
S3-040545	Proposed CR to 33.310: Splitting the Roaming CA into a SEG CA and an Interconnection CA (Rel-6)	Vodafone, T-Mobile, Siemens	7.4	Approval	S3-040643	S3-040643
S3-040546	Proposed CR to 33.141: Clarification on Ut interface (Rel-6)	Vodafone, Ericsson	7.18	Approval	S3-040661	Revised in S3-040661
S3-040547	Proposed CR to 33.222: Editorial change to section 5.3 (Rel-6)	Vodafone	7.9.4	Approval		change incorporated in S3-040658
S3-040548	Proposed WID: Security for early IMS	Vodafone	7.1	Approval	S3-040637	Revised in S3-040637
S3-040549	New TR on early IMS security	Vodafone	7.1	Discussion / Decision		For evening discussion
S3-040550	MAPsec contributions from SA plenary	Vodafone	7.2	Information		Noted
S3-040551	Further modifications to the division of TLS profile related text in 33.141 and 33.222	Ericsson, Siemens	7.9.4	Discussion / Approval		CRs Attached. CR to 33.141 revised in S3-040657, 33.222 in S3-040658
S3-040552	SRTP for protecting of MBMS streaming data	Ericsson	7.20	Discussion / Approval		CR Attached. Revised to include re-structuring with Download text in S3-040620
S3-040553	Source Origin Authentication in MBMS	Ericsson	7.20	Discussion / Approval		CR Attached. Threats of Pseudo-CR included in S3-040621. Requirements for future Release

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040554	Push and pull key management	Ericsson	7.20	Discussion / Decision		Pseudo-CR in S3-040565.
S3-040555	Proposed CR to 33.234: Update reference to RFC3748 "Extensible Authentication Protocol (EAP)" (Rel-6)	Lucent Technologies	7.10	Approval		Approved
S3-040556	Proposed CR to 33.141: PSK TLS and SSC support (Rel-6)	Nokia, Nortel	7.18	Approval		Withdrawn. Covered by S3-040616
S3-040557	MBMS Download Protection	Ericsson	7.20	Discussion / Decision		
S3-040558	Authenticating the CSCF peer in a hybrid network (IMS and non-IMS interworking)	Nokia	7.1	Discussion / Decision		Some changes agreed in S3-040641
S3-040559	Proposed CR to 33.203: SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network (Rel-6)	Nokia	7.1	Approval	S3-040641	
S3-040560	Proposed CR to 33.210: SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network (Rel-6)	Nokia	7.3	Approval		Withdrawn as TLS not accepted
S3-040561	GUP Security Open Issues	Ericsson, Nokia, Intel	7.17	Discussion / Decision		Presentation attached
S3-040562	Binding Scenario Information to Mutual EAP Authentication	Nokia	7.10	Discussion / Decision		LS to SA2 on this in S3-040608
S3-040563	Handling MSKs and decrypting download data in MBMS	**3**	7.20	Discussion / Decision	S3-040573	Replacement in S3-040573
S3-040564	Proposed CR to 33.220: Removal of the definition of a default type of NAF-specific key. (Rel-6)	Gemplus	7.9.2	Approval	S3-040662 S3-040663	Revised in S3-040662 and S3-040663
S3-040565	Pseudo-CR to 33.246: Push and pull key management for MBMS (Rel-6)	Ericsson	7.20	Approval		Principles agreed to be included in the draft TS
S3-040566	Selective Disabling of UE Capabilities	Nokia	7.23	Discussion	S3-040583	Revised in S3-040583
S3-040567	Comment (in form of CR to S3-040272): Session Key Exchange Algorithm (SKEA) for Local Interface Trusted Tunnel Establishment	Intel	7.10	Discussion		Interested members to discuss and propose WID if appropriate
S3-040568	New CR Cover sheet, version 7.1	SA WG3 Secretary (M. Pope, MCC)	10	Information		
S3-040569	TISPAN-3GPP June 04 joint meeting notes	BT Group	5.7	Information		Noted. Delegates to take into account in IMS discussions
S3-040570	Proposed CR to 33.102: Introducing the special RAND mechanism as a principle for GSM/GPRS (Rel-6)	Orange, Nokia	7.6	Approval		Withdrawn
S3-040571	Comments to S3-040467: WLAN: Justification for the introduction of a WLAN application (Gemplus)	Nokia	7.10	Discussion / Decision		
S3-040572	An observation about Special RAND in GSM	QUALCOMM Europe	7.6	Discussion / Decision		LATE DOC. Noted. Further contribution requested. Not for Rel-6
S3-040573	Handling MSKs and decrypting download data in MBMS	**3**	7.20	Discussion / Decision	S3-040619	LATE DOC. 6.3 changes included in S3-040619. Other changes agreed for inclusion in draft TS
S3-040574	Comments on Orange/Nokia contribution S3-040528 regarding domain separation	Vodafone	7.6	Discussion		comment to S3-040528. Further contribution requested. Not for Rel-6
S3-040575	GBA_ME/GBA_U scenarios in UE att S3-040536 COMMENTED/REVISED BY AXALTO	Axalto	7.9.2	Discussion		comment to attachment to S3-040536. Covered at GBA_U evening session (see S3-040655)
S3-040576	GBA: The support of GBA features within a Rel-6 ME	Axalto	7.9.2	Discussion / Decision		comment to S3-040491. Covered at GBA_U evening session (see S3-040655)
S3-040577	Comparison of two CRs about tunnel authentication	Ericsson	7.10	Discussion / Decision		comment to S3-040493 and S3-040527. Combined CR in S3-040607

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040578	Open issues on (U)SIM security re-use	Ericsson, Nokia	7.15	Discussion / Decision		comment to S3-040468. More comments in S3-040587. Conference Calls to be arranged. Evening session to clarify main problems
S3-040579	comments to S3-040549: New TR on early IMS security	Ericsson	7.1	Discussion / Decision		comment to S3-040549
S3-040580	Comments to S3-040475 (Alternative to Special Random or AMF indication for GBA_U: MAC indication)	Siemens	7.9.2	Discussion / Decision		comment to S3-040475. More comment in S3-040585. Covered at GBA_U evening session (see S3-040655)
S3-040581	Comments to S3-040550: SMS Fraud countermeasure	Siemens, Vodafone	7.2	Discussion / Decision		comment to S3-040550. LS for comments in S3-040642
S3-040582	Updated S3-040544 as comments to S3-040479 and S3-040563. Pseudo-CR to 33.246: Key management mechanism (Rel-6) (section 6.4 changes).	Ericsson	7.20	Discussion / Decision	S3-040619	Updated S3-040544: comments to S3-040479 and S3-040563. Revised in S3-040619
S3-040583	Selective Disabling of UE Capabilities; updated S3-040566 based on the comments on SA3 mailing list	Nokia	7.23	Discussion		
S3-040584	Comments to S3-040544	Axalto	7.20	Discussion		Comments to S3-040544. Updated Pseudo-CR in S3-040619
S3-040585	comments to(Comments to (Alternative to Special Random or AMF indication for GBA_U:)	Axalto	7.9.2	Discussion		Comments to S3-040580. Covered at GBA_U evening session (see S3-040655)
S3-040586	Draft Presentation of AKA useage from 3GPP side	SA WG3 Chairman	6.2	Comment and update	S3-040645	Revised in S3-040645
S3-040587	Response to Comments on “Open issues on (U)SIM security re-use (S3-040578)	Toshiba et al	7.15	Discussion		Comments to S3-040578. Conference Calls to be arranged. Evening session to clarify main problems
S3-040588	Report of 3GPP2 security group to 3GPP2 plenary	3GPP2 Sec Liaison Officer	5.5	Information		Noted
S3-040589	LS to CN1: Clarification on deletion of MS-stored parameters on power-off	SA WG3	7.10	Approval	S3-040666	Revised in S3-040666
S3-040590	WLAN: ad-hoc session on WLAN application	Gemplus	7.10	Discussion / Decision		Chairman to report this to TSG SA
S3-040591	ISIM usage in GAA:	Nokia, Gemplus, Alcatel, Motorola	7.9.2	Discussion / Approval		Contained in S3-040648
S3-040592	Proposed CR to 33.220: ISIM support	Nokia, Gemplus, Alcatel	7.9.2	Approval		Contained in S3-040648
S3-040593	Proposed CR to 33.141: ISIM support (Rel-6)	Nokia, Gemplus, Alcatel	7.18	Approval		Contained in S3-040648
S3-040594	Proposed CR to 33.234: Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces). Bluetooth security and configuration considerations for Annex A4 of TS 33.234 (Wireless Local Area Network (WLAN) interworking security)	Toshiba, BT and supporting Companies	7.15	Approval		Conference Calls to be arranged. Evening session to clarify main problems
S3-040595	LS (from SA WG1) on removal of A5/2 algorithm in Release 6 MEs	SA WG1	7.5	Information		Noted. Chairman and Secretary to check best way to include reqs in specs
S3-040596	LS from SA WG1: SA WG1's answer to LS on VGCS and VBS security	SA WG1	7.21	Information		CRs attached for info. Noted
S3-040597	Reply (from SA WG1) to LS on Correlation of I-WLAN Access and Service Authorization (S2-042347/S1-040562)	SA WG1	7.10	Information		Noted. Delegates to check off-line

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040598	LS (from SA WG1) on MBMS key Management	SA WG1	7.20	Information		Check impacts on S3 Tss
S3-040599	Proposed CR to 33.234: References update (Rel-6)	Ericsson	7.10	Approval		Approved
S3-040600	Proposed CR to 33.234: Modification of mechanism to restrict simultaneous WLAN sessions (Rel-6)	Huawei	7.10	Approval	S3-040668	Revised in S3-040668
S3-040601	Proposed CR to 33.234: Sending of temporary identities from WLAN UE (Rel-6)	Samsung, Huawei	7.10	Approval		Approved
S3-040602	Proposed CR to 33.234: Introduction of protected result indications (Rel-6)	Ericsson	7.10	Approval	S3-040670	Revised in S3-040670
S3-040603	Proposed CR to 33.234: Clarification on fast re-authentication procedure (Rel-6)	Ericsson	7.10	Approval		Approved
S3-040604	Proposed CR to 33.234: Deletion of editor's note (Rel-6)	Ericsson	7.10	Approval	S3-040669	Revised in S3-040669
S3-040605	LS to SA WG2: LS on IPsec tunnels and W-APNs	SA WG3	7.10	Approval		Approved
S3-040606	Draft LS to SA WG2: "Clarification on Addresses used for Tunnel Establishment"	SA WG3	7.10	Approval		Approved
S3-040607	CR combining S3-040493 and S3-040527	David	7.10	Approval	S3-040671	Revised in S3-040671
S3-040608	LS on Binding Scenario Information to Mutual EAP Authentication	SA WG3	7.10	Approval	S3-040672	Revised in S3-040672
S3-040609	Proposed CR to 33.234: Conditional support of NAT (Rel-6)	Nokia	7.10	Approval		Withdrawn. Superseded by discussions
S3-040610	Proposed CR to 33.234: Correction for authentication procedure of WLAN UE split (Rel-6)	Huawei	7.10	Approval		Approved
S3-040611	Results of the off-line meeting on " CR on (U)SIM Security re-use	Toshiba, Intel, BT, T-Mobile, Nokia, Ericsson	7.10	Information		Noted. Additional conf call 26 July
S3-040612	Reply LS on multiple connections to VPLMNs simultaneously Response to: S3-040457 (S1-040389) Reply LS on multiple connections to VPLMNs simultaneously	SA WG3	7.20	Approval	S3-040667	Revised in S3-040667
S3-040613	Reply LS on DRM protection for PSS	SA WG3	7.20	Approval	S3-040674	Revised in S3-040674
S3-040614	Reply LS on MBMS security issues	SA WG3	7.20	Approval	S3-040675	Revised in S3-040675
S3-040615	N to N relationship between User Services and Transport Services	Siemens	7.20	Approval		Incorporated in S3-040621
S3-040616	Proposed CR to 33.141: Editorial cleanup of TS 33.141 (Rel-6)	Siemens, Ericsson, Nokia	7.18	Approval	S3-040659	Revised in S3-040659
S3-040617	Proposed CR to 33.222: Editorial clean-up of TS 33.222 (Rel-6)	Siemens, Ericsson, Nokia	7.18	Approval	S3-040660	Revised in S3-040660
S3-040618	Pseudo-CR to 33.234: UICC-ME interface for MBMS	Axalto, Gemplus, OCS	7.20	Approval	S3-040676	Revised in S3-040676
S3-040619	Handling MSKs and decrypting download data in MBMS	**3**	7.20	Approval	S3-040677	Revised in S3-040677
S3-040620	Pseudo-CR to 33.234: SRTP for protecting of MBMS streaming data	Adrian & Vesa	7.20	Approval		Agreed for inclusion in draft TS
S3-040621	Pseudo-CR to 33.234: Identified threats	Adrian & Vesa	7.20	Approval		Agreed for inclusion in draft TS
S3-040622	LS informing groups of completion of MBMS Security TS	Vesa	7.20	Approval	S3-040679	Revised in S3-040679
S3-040623	LS on GUP security status in SA3 and on collaboration of 3GPP and Liberty Alliance Project	Bengt	7.17	Approval	S3-040673	Revised in S3-040673
S3-040624	Proposed CR to 43.020: Introducing VGCS/VBS ciphering (Rel-6)	Siemens, Vodafone	7.21	Approval		36-bit revised in S3-040638
S3-040625	LS from IETF LEMONADE: LEMONADE for MMS over 3GPP Interworking WLANs	IETF LEMONADE	7.10	Information		Noted
S3-040626	Presentation of Status of AKA in TIA Standards	AHAG Chairman (F. Quick)	6.1	Information		Presented and noted
S3-040627	Draft 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	7.10	Information		Noted for conf calls
S3-040628	Draft CR to 33.234: Additional requirements for Communication over local interface via a Bluetooth link (Rel-6)	Toshiba, BT and supporting Companies	7.10	Information		Noted for conf calls

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040629	Draft 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	7.10	Information		Noted for conf calls
S3-040630	Draft LS on VGCS: length of VSTK_RAND	SA WG3	7.21	Approval	S3-040680	Revised in S3-040680
S3-040631	Draft LS on VGCS: Example algorithm A8_V	SA WG3	7.21	Approval	S3-040681	Revised in S3-040681
S3-040632	Selective Disabling of UE Capabilities; updated S3-040583 based on the comments in SA3#34 meeting	Nokia	7.23	Discussion	S3-040682	Revised in S3-040682
S3-040633	Draft LS on Security Aspects in Selective Disabling of UE Capabilities WI	SA WG3	7.23	Approval	S3-040683	Revised in S3-040683
S3-040634	Proposed CR to 33.203: Deletion of old authentication vectors in S-CSCF after re-synchronization (Rel-5)	Nokia	7.1	Approval		Approved
S3-040635	Proposed CR to 33.203: Deletion of old authentication vectors in S-CSCF after re-synchronization (Rel-6)	Nokia	7.1	Approval		Approved
S3-040636	Proposed CR to 33.203: IMS Service Profile is independent from Implicit Registration Set (Rel-6)	Nokia	7.1	Approval		Approved
S3-040637	Proposed WID: Security for early IMS	Vodafone	7.1	Approval		Approved
S3-040638	Proposed CR to 43.020: Introducing VGCS/VBS ciphering (Rel-6)	Siemens, Vodafone	7.1	Approval		Approved
S3-040639	Proposed CR to : Forwards compatibility to TLS based access security in IMS (Rel-6)	Ericsson	7.1	Approval		Approved
S3-040640	Pseudo-CR to 33.919: Application guidelines to use GAA (Rel-6)	Alcatel , BT , Nokia	7.9.1	Approval		Agreed for inclusion in draft TS
S3-040641	Proposed CR to : Authenticating the CSCF peer in a hybrid network (IMS and non-IMS interworking)	Nokia	7.1	Approval		Approved
S3-040642	LS on SMS Fraud countermeasure	SA WG3	7.2			Approved
S3-040643	Proposed CR to 33.310: Splitting the Roaming CA into a SEG CA and an Interconnection CA (Rel-6)	Vodafone, T-Mobile, Siemens	7.4	Approval		Approved
S3-040644	Response LS (to R2-041261) on Re-authentication and key set change during inter-system handover	SA WG3	7.5	Approval	S3-040686	Revised in S3-040686
S3-040645	Presentation of AKA usage in 3GPP	SA WG3 Vice Chairman (P. Howard)	6.2	Presentation		Presented and noted
S3-040646	LS to CN WG1 and CN WG4: Forwards compatibility to TLS based access security in IMS	Ericsson	7.1	Approval	S3-040684	Revised in S3-040684
S3-040647	Proposed CR to 33.220: Securing Zn reference point (Rel-6)	Siemens, Nokia	7.9.2	Approval		
S3-040648	USIM and ISIM selection in GAA	Nokia, Siemens, Gemplus, Motorola	7.9.2	Discussion / Approval		CRs attached.
S3-040649	LS on Requirement for presence of the GAA-Application-Type AVP	Peter	7.9.2	Approval		Approved
S3-040650	Proposed CR to 33.220: GBA User Security Settings (Rel-6)	Nokia, Siemens	7.9.2	Approval		Approved
S3-040651	LS to S1, S2, T2 on USIM and ISIM selection in GAA	Pekka	7.9.2	Approval		Approved
S3-040652	LS on Authentication Proxy	SA WG3	7.9.4	Approval		Approved
S3-040653	GBA_U ME-UICC interface and Ks_ext storage and 3 CR options	Axalto	7.9.2	Approval		Alternative mechanisms in each CR. No agreement on which CR to choose, to be added to LS in S3-040664
S3-040654	Proposed CR 33.220: GBA_U-MAC AV	Axalto	7.9.2	Approval		Approved
S3-040655	GBA_U Evening session report (Thursday, July 8th)	Session Chairman	7.9.2	Information		Noted
S3-040656	Proposed CR to 33.221: Removal of unnecessary editor's notes (Rel-6)	Nokia	7.9.3	Approval		Approved
S3-040657	CR to 33.141	SA WG3				Approved
S3-040658	CR to 33.222:	SA WG3				Approved
S3-040659	Proposed CR to 33.141: Editorial cleanup of TS 33.141 (Rel-6)	Siemens, Ericsson, Nokia	7.18	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040660	Proposed CR to 33.222: Editorial clean-up of TS 33.222 (Rel-6)	Siemens, Ericsson, Nokia	7.18	Approval		Approved
S3-040661	Proposed CR to 33.141: Clarification on Ut interface (Rel-6)	Vodafone, Ericsson	7.18	Approval		Approved
S3-040662	Proposed CR to 33.220: Removal of the definition of a default type of NAF-specific key (Rel-6)	Gemplus	7.9.2	Approval	S3-040665	Revised in S3-040665
S3-040663	Proposed CR to 33.222: Precision on the NAF-specific key to use to secure Ua interface in case of GBA_U (Rel-6)	Gemplus	7.9.2	Approval		Withdrawn due to no default NAF_ext in S3-040662
S3-040664	LS on Removal of the definition of a default type of NAF-specific key alternatives	Holger	7.9.2	Approval		Approved
S3-040665	Proposed CR to 33.220: Removal of the definition of a default type of NAF-specific key (Rel-6)	Gemplus	7.9.2	Approval	S3-040687	Revised in S3-040687
S3-040666	LS to CN1: Clarification on deletion of MS-stored parameters on power-off	SA WG3	7.10	Approval		Approved
S3-040667	Reply LS on multiple connections to VPLMNs simultaneously Response to: S3-040457 (S1-040389) Reply LS on multiple connections to VPLMNs simultaneously	SA WG3	7.20	Approval	S3-040688	Revised in S3-040688
S3-040668	Proposed CR to 33.234: Modification of mechanism to restrict simultaneous WLAN sessions (Rel-6)	Huawei	7.10	Approval		Approved
S3-040669	Proposed CR to 33.234: Deletion of editor's note (Rel-6)	Ericsson	7.10	Approval		Approved
S3-040670	Proposed CR to 33.234: Introduction of protected result indications (Rel-6)	Ericsson	7.10	Approval		Approved
S3-040671	CR combining S3-040493 and S3-040527	David	7.10	Approval		Approved
S3-040672	LS on Binding Scenario Information to Mutual EAP Authentication	SA WG3	7.10	Approval		Approved. 3 attachements
S3-040673	LS on GUP Security Progress in SA3	SA WG3	7.17	Approval		Approved. 2 attachments
S3-040674	Reply LS on DRM protection for PSS	SA WG3	7.20	Approval		Approved
S3-040675	Reply LS on MBMS security issues	SA WG3	7.20	Approval		Approved
S3-040676	Pseudo-CR to 33.234: UICC-ME interface for MBMS	Axalto, Gemplus, OCS	7.20	Approval		Agreed for inclusion in draft TS
S3-040677	Handling MSKs and decrypting download data in MBMS	**3**	7.20	Approval		Agreed for inclusion in draft TS
S3-040678	Updated version of TS 33.246 (MBMS) after all agreed changes are included	Editor (A. Escott)	7.20	Information		To be added to LS in S3-040622
S3-040679	LS informing groups of completion of MBMS Security TS	Vesa	7.20	Approval		Attach Updated MBMS draft when available (S3-040678)
S3-040680	LS on VGCS: length of VSTK_RAND	SA WG3	7.21	Approval		Approved
S3-040681	LS on VGCS: Example algorithm A8_V	SA WG3	7.21	Approval		Approved
S3-040682	Selective Disabling of UE Capabilities; updated S3-040583 based on the comments in SA3#34 meeting	Nokia	7.23	Discussion		Agreed
S3-040683	LS on Security Aspects in Selective Disabling of UE Capabilities WI	SA WG3	7.23	Approval		Approved
S3-040684	LS to CN WG1 and CN WG4: Forwards compatibility to TLS based access security in IMS	Ericsson	7.1	Approval		Approved
S3-040685	Draft TR on Early IMS Security v0.0.2	Vodafone	7.1	Information		Agreed to copy to TSG SA for info
S3-040686	Response LS (to R2-041261) on Re-authentication and key set change during inter-system handover	SA WG3	7.5	Approval		Approved
S3-040687	Proposed CR to 33.220: Removal of the definition of a default type of NAF-specific key (Rel-6)	Gemplus	7.9.2	Approval		Approved
S3-040688	Reply LS on multiple connections to VPLMNs simultaneously Response to: S3-040457 (S1-040389) Reply LS on multiple connections to VPLMNs simultaneously	SA WG3	7.20	Approval	S3-040689	Approved (but revised after meeting to add attachments, in S3-040689)

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-040689	Reply LS on multiple connections to VPLMNs simultaneously Response to: S3-040457 (S1-040389) Reply LS on multiple connections to VPLMNs simultaneously	SA WG3	7.20	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	5.4.0	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	5.8.0	Rel-5	S3	BOMAN, Krister	
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	5.5.0	Rel-5	S3	KOIEN, Geir	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210).
TR	33.900	Guide to 3G security	0.4.1	Rel-5	S3	BROOKSON, Charles	.
TR	33.903	Access Security for IP based services	none	Rel-5	S3	VACANT,	.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .

Type	Number	Title	Ver at SA3#33	Rel	TSG/ WG	Editor	Comment
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence .
TS	35.205	3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE. 2002-06: clarified that deliverable is TS not TR. .
TS	35.206	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification	5.1.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TS	35.207	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE .
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	5.0.0	Rel-5	S3	WRIGHT, Tim	.
TR	41.033	Lawful Interception requirements for GSM	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
TS	42.033	Lawful Interception; Stage 1	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
TS	43.020	Security-related network functions	5.0.0	Rel-5	S3	GILBERT, Henri	.
TS	43.033	Lawful Interception; Stage 2	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	.
Release 6 3GPP Specifications and Reports							
TS	33.102	3G security; Security architecture	6.1.0	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	6.2.0	Rel-6	S3	WILHELM, Berthold	.
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	6.6.0	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	6.0.0	Rel-6	S3	BOMAN, Krister	.
TS	33.203	3G security; Access security for IP-based services	6.3.0	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	6.1.0	Rel-6	S3	HAUKKA, Tao	WI = SEC1-SC (UID 33002) Based on 33.109 §4. .
TS	33.221	Generic Authentication Architecture (GAA); Support for subscriber certificates	6.0.0	Rel-6	S3	HAUKKA, Tao	WI = SEC1-SC (UID 33002) Based on 33.109 §5 & annex A. .
TS	33.222	Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)	6.0.0	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	6.1.0	Rel-6	S3	LOPEZ SORIA, Luis	.
TS	33.310	Network domain security; Authentication framework (NDS/AF)	6.1.0	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. .
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. .
Specifications and Reports identified (or to be allocated to)Release 6							
TS	33.246	3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)	1.2.1	Rel-6	S3	ESCOTT, Adrian	SP-22: target for v2.0.0 is SP-23, but this will be challenging.
TR	33.919	Generic Authentication Architecture (GAA); System description	1.2.1	Rel-6	S3	VAN MOFFAERT, Annelies	WI = SEC1-SC (UID 33002) .
TR	33.941	Presence service; Security	0.6.0	Rel-6	S3	BOMAN, Krister	.
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	010	-	Rel-6	Detailing of key lifetime	F	6.1.0	S3-34	S3-040504	SEC1-SC
33.220	011	-	Rel-6	Details of USIM/ISIM usage in GAA	C	6.1.0	S3-34	S3-040648	SEC1-SC
33.220	012	-	Rel-6	Generic Ua interface requirements	C	6.1.0	S3-34	S3-040465	SEC1-SC
33.220	013	-	Rel-6	B-TID generation	C	6.1.0	S3-34	S3-040539	SEC1-SC
33.220	014	-	Rel-6	Securing Zn reference point	C	6.1.0	S3-34	S3-040647	SEC1-SC
33.220	015	-	Rel-6	GBA User Security Settings	F	6.1.0	S3-34	S3-040650	SEC1-SC
33.220	016	-	Rel-6	Creation of GBA_U AV in the BSF	B	6.1.0	S3-34	S3-040654	SEC1-SC
33.220	017	-	Rel-6	Clarification of the definition of a default type of NAF-specific key	D	6.1.0	S3-34	S3-040687	SEC1-SC
33.141	001	-	Rel-6	ISIM used in GBA	C	6.0.0	S3-34	S3-040648	PRESNC
33.141	002	-	Rel-6	Further modifications to TLS profile related text in 33.141	F	6.0.0	S3-34	S3-040657	PRESNC
33.141	003	-	Rel-6	Editorial cleanup of TS 33.141	D	6.0.0	S3-34	S3-040659	PRESNC
33.141	004	-	Rel-6	Clarification on Ut interface	F	6.0.0	S3-34	S3-040661	PRESNC
33.221	001	-	Rel-6	User security settings	D	6.0.0	S3-34	S3-040502	SEC1-SC
33.221	002	-	Rel-6	Editorial cleanup	D	6.0.0	S3-34	S3-040505	SEC1-SC
33.221	003	-	Rel-6	Cleanup of procedure descriptions	F	6.0.0	S3-34	S3-040506	SEC1-SC
33.221	004	-	Rel-6	Removal of unnecessary editor's notes	F	6.0.0	S3-34	S3-040507	SEC1-SC
33.222	001	-	Rel-6	GBA User Security Settings	D	6.0.0	S3-34	S3-040503	SEC1-SC
33.222	002	-	Rel-6	GBA supported indication and NAF hostname transfer in HTTP and in PSK TLS	C	6.0.0	S3-34	S3-040656	SEC1-SC
33.222	003	-	Rel-6	Editorial clean-up of TS 33.222	D	6.0.0	S3-34	S3-040660	SEC1-SC
33.234	010	-	Rel-6	Update referece to RFC3748 "Extensible Authentication Protocol (EAP)"	F	6.1.0	S3-34	S3-040555	WLAN
33.234	011	-	Rel-6	References update	F	6.1.0	S3-34	S3-040599	WLAN
33.234	012	-	Rel-6	Sending of temporary identities from WLAN UE	F	6.1.0	S3-34	S3-040601	WLAN
33.234	013	-	Rel-6	Clarification on fast re-authentication procedure	F	6.1.0	S3-34	S3-040603	WLAN
33.234	014	-	Rel-6	Correction of authentication procedure for WLAN UE split	F	6.1.0	S3-34	S3-040610	WLAN
33.234	015	-	Rel-6	Modification of mechanism to restrict simultaneous WLAN sessions	C	6.1.0	S3-34	S3-040668	WLAN
33.234	016	-	Rel-6	Wa interface security	C	6.1.0	S3-34	S3-040669	WLAN
33.234	017	-	Rel-6	Introduction of protected result indications	F	6.1.0	S3-34	S3-040670	WLAN
33.234	018	-	Rel-6	Tunnel authentication procedure in Wm interface	F	6.1.0	S3-34	S3-040671	WLAN
33.222	004	-	Rel-6	Further modifications to TLS profile related text in 33.222	F	6.0.0	S3-34	S3-040658	SEC1-SC
33.203	068	-	Rel-5	Deletion of old authentication vectors in S-CSCF after re-synchronization	F	5.8.0	S3-34	S3-040634	IMS-ASEC
33.203	072	-	Rel-6	IMS Service Profile is independent from Implicit Registration Set	F	6.3.0	S3-34	S3-040636	IMS-ASEC
33.203	070	-	Rel-6	Forwards compatibility to TLS based access security	F	6.3.0	S3-34	S3-040639	IMS-ASEC
33.203	071	-	Rel-6	SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network	F	6.3.0	S3-34	S3-040641	IMS-ASEC
33.203	069	-	Rel-6	Deletion of old authentication vectors in S-CSCF after re-synchronization	A	6.3.0	S3-34	S3-040641	IMS-ASEC
33.310	004	-	Rel-6	Splitting the Roaming CA into a SEG CA and an Interconnection CA	C	6.1.0	S3-34	S3-040643	SEC1-NDS-AF
43.020	001	-	Rel-6	Introducing VGCS/VBS ciphering	B	5.0.0	S3-34	S3-040638	SECGKYV

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	From	Source TD	Comment/Status
S3-040453	LS (from CN WG1) on Storage of temporary identities for EAP authentication	CN WG1	N1-041045	Response LS to clarify power-off deletion of parameters in S3-040666
S3-040454	LS (from CN WG4) on Requirement for presence of the GAA-Application-Type AVP	CN WG4	N4-040748	Response in S3-040649
S3-040455	Reply LS (from RAN WG3) on LS on Re-authentication and key set change during inter-system handover	RAN WG3	R3-040944	Noted
S3-040456	LS from SA WG1: Current UICC for W-LAN interworking	SA WG1	S1-040532	Noted
S3-040457	LS reply (from SA WG1) on multiple connections to VPLMNs simultaneously	SA WG1	S1-040533	Response LS in S3-040612
S3-040458	Reply LS (from SA WG2) on GUP security status in SA3 and on collaboration of 3GPP and Liberty Alliance Project	SA WG2	S2-042208	Response LS in S3-040623 based on S3-040561
S3-040459	LS from SA WG2: Clarification on Addresses used for Tunnel Establishment	SA WG2	S2-042316	Draft response in S3-040510 considered.
S3-040460	Liaison statement (from SA WG4) on DRM protection for PSS	SA WG4	S4-040309	Response LS in S3-040613
S3-040461	Reply LS (from SA WG4) on MBMS security issues	SA WG4	S4-040322	Response LS in S3-040614
S3-040462	Response LS to N1-040501 (from RAN WG2) on Re-authentication and key set change during inter-system handover	RAN WG2	R2-041261	Response LS in S3-040644
S3-040463	LS (from SA WG2) on interim IMS security	SA WG2	S2-042346	TSG SA asked SA3 to clarify. Noted
S3-040471	LS from ETSI SAGE: Responses on cryptographic aspects of VGCS	ETSI SAGE	SAGE (04) 02	Discussion paper in S3-040496
S3-040472	LS (from CN WG1) on Authentication Proxy	CN WG1	N1-041313	Response in S3-040652
S3-040473	LS from OMA SEC WG: Reply to LS on Presence Security	OMA SEC WG	OMA-SEC-2004-0053	Noted
S3-040474	LS from Terry Bourk, Chair of Bluetooth Architecture Review Board: Response to S3-040197	Terry Bourk, Chair of Bluetooth Architecture Review Board	-	To be discussed as part of conference calls for response at next meeting
S3-040492	LS from GSMA Security Group: Report and request for work item on IST	GSMA -SEC	-	Noted. Delegates encouraged to consider the request to create an IMS WI
S3-040595	LS (from SA WG1) on removal of A5/2 algorithm in Release 6 MEs	SA WG1	S1-040627	Noted. Chairman and Secretary to check best way to include reqs in specs
S3-040596	LS from SA WG1: SA WG1's answer to LS on VGCS and VBS security	SA WG1	S1-040645	CRs attached for info. Noted
S3-040597	Reply (from SA WG1) to LS on Correlation of I-WLAN Access and Service Authorization (S2-042347/S1-040562)	SA WG1	S1-040716	Noted. Delegates to check off-line
S3-040598	LS (from SA WG1) on MBMS key Management	SA WG1	S1-040729	Check impacts on S3 Tss
S3-040625	LS from IETF LEMONADE: LEMONADE for MMS over 3GPP Interworking WLANs	IETF LEMONADE	-	Noted

E.2 Liaisons from the meeting

TD number	Title	TO	CC
S3-040605	LS to SA WG2: LS on IPsec tunnels and W-APNs	**SA WG2**	**-**
S3-040606	Draft LS to SA WG2: "Clarification on Addresses used for Tunnel Establishment"	**SA WG2**	**-**
S3-040642	LS on SMS Fraud countermeasure	**CN WG4, T WG2**	**SA WG2**

TD number	Title	TO	CC
S3-040649	LS on Requirement for presence of the GAA-Application-Type AVP	**CN WG4**	
S3-040651	LS to S1, S2, T2 on USIM and ISIM selection in GAA	**SA WG1, SA WG2, T WG2**	**T WG3**
S3-040652	LS on Authentication Proxy	**CN WG1**	**-**
S3-040664	LS on Removal of the definition of a default type of NAF-specific key alternatives	**T WG3**	**-**
S3-040666	LS to CN1: Clarification on deletion of MS-stored parameters on power-off	**CN WG1**	**T WG3**
S3-040672	LS on Binding Scenario Information to Mutual EAP Authentication	**SA WG2**	**CN WG4**
S3-040673	LS on GUP Security Progress in SA3	**SA WG2, CN WG4**	**-**
S3-040674	Reply LS on DRM protection for PSS	**SA WG4**	**-**
S3-040675	Reply LS on MBMS security issues	**SA WG4**	**-**
S3-040679	LS informing groups of completion of MBMS Security TS (Updated TS to be attached when available)	**SA WG4, SA WG2, CN WG1, T WG3, CN WG4**	**-**
S3-040680	LS on VGCS: length of VSTK_RAND	**GERAN WG2**	**-**
S3-040681	LS on VGCS: Example algorithm A8_V	**ETSI SAGE**	**-**
S3-040683	LS on Security Aspects in Selective Disabling of UE Capabilities WI	**SA WG1**	**-**
S3-040684	LS to CN WG1 and CN WG4: Forwards compatibility to TLS based access security in IMS	**CN WG1, CN WG4, SA WG2**	**-**
S3-040686	Response LS (to R2-041261) on Re-authentication and key set change during inter-system handover	**RAN WG2**	**CN WG1, RAN WG3**
S3-040689~~8~~	Reply LS on multiple connections to VPLMNs simultaneously. Response to: S3-040457 (S1-040389) Reply LS on multiple connections to VPLMNs simultaneously	**SA WG1**	**SA WG2**

Annex F: Actions from the meeting

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.

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

AP 34/03: Chairman to bring outcome of WLAN/UICC discussions to attention of TSG SA (see TD S3-040590).

AP 34/04: Raziq Yaqub to arrange 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.

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)