Technical Specification Group Services and System Aspects **TSGS#27(05) 0236**
Meeting #28, Quebec, Canada, 6-8 June 2005

Source:	**SA3**
Title:	**Draft Report of SA3 #38**
Document for:	**Information**
Agenda Item:	**7.3.1**

TSG-SA WG3 #38 **Draft S3-050322**
Geneva, Switzerland, 26th to 29th April 2005 **Agenda Item:**

Source: Secretary of 3GPP TSG-SA WG3

Title: Draft Report of SA3 meeting #38

Document for: Comment

Status: Draft Version 0.0.8

Contents

1 Opening of the meeting

The SA WG3 Chairman, Mr. V. Niemi opened the meeting which was hosted by EF3 in Geneva, Switzerland.

2 Agreement of the agenda and meeting objectives

TD S3-050184 Draft Agenda for SA WG3 meeting #38. This was introduced by the SA WG3 Chairman and was reviewed. The objectives for the meeting were also introduced as follows:

Meeting objectives:

- *One major objective is to solve the identified open issues related to (Release 6) https security and (Release 6) MBMS security.*
- *Another major objective is to get work in Release 7 into full speed.*

Preliminary schedule of the meeting:

- *Because we have agreed an early deadline for UICC-related issues in 6.9.4, it seems natural to start with 6.9 in technical work areas. Also, we still have a lot to to check in MBMS. Therefore, it may be good to take 6.20 as the second work area. This order would also enable us communicate our conclusions to CT groups (relatively) early in the week. Note that the CT working groups (incl. CT6) have a meeting in Mexico during the same week.*
- *Then, the planned milestones for each day of the meeting are as follows:*
- *Tuesday: completion of items 1-5 and technical items in 6.9 (GAA) and 6.18 (Presence). Hopefully a start in 6.20 (MBMS);*
- *Wednesday: Completion of 6.20 and also items 6.1-6.8.*
- *Thursday: items 6.10-6.17, 6.19 and 6.21-6.26;*
- *Friday: handling of output documents and agenda items 7-10.*
- *These milestones are based on the experience from previous meetings. The schedules have to be adjusted to the number of contributions submitted to each agenda item.*
- *Additional break-out sessions are probably arranged in some evenings.*

The draft agenda was then approved.

2.1 3GPP IPR Declaration

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

IPR Declaration:

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

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

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

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

3 Assignment of input documents

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

4 Meeting reports

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

TD S3-050185 Draft Report of SA WG3 meeting #36. The draft report was reviewed. Some text was provided for section 5.5 from Nortel. In section 6.2 there was a comment from the secretary; there was no impact on the CRs, and there were three separate CRs. The note was deleted.

Action points from meeting #36:

AP 37/01: Chairman to ask the Specifications Manager for the best way to handle the UE2 / UIA2 work in the specifications set (numbering etc.)
It was not certain what was intended with this action. It was assumed that a similar set of TSs for the Kasumi based solution. There is a problem with the names F8 and F9, but these are generic names for the algorithm and UEA1 and UIA1 are the specific names for the Kasumi algorithms. Hence the names of the existing TSs will need to be changed. A proposal for a solution to the naming issue will be provided by Telia Sonera. This action remains open for the time being.

AP 37/02: Qiuling Pan, (ZTE to lead an e-mail discussion on the LS in TD S3-050005 and provide a draft answer to the LS to the next SA WG3 meeting.
Closed, see TD S3-050227.

AP 37/03: B. Sahlin to provide an updated WID, based on TD S3-050060 for next SA WG3 meeting, taking into account the outcome of the TISPAN NGN Workshop.
Closed, see TD S3-050283.

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

AP 37/05: G. Horn to run an e-mail discussion based on TD S3-050101 (Review of recently published papers on GSM and UMTS security) and provide a contribution to the next SA WG3 meeting.
Closed, see TD S3-050236.

AP 37/06: S. Holtmanns to discuss GAA Enhancements WID and develop the scope and need for the work, and present the WID again with enough supporting companies (re: TD S3-050055).
Closed, see TD S3-050263; this is not the WID, but explains the issues.

AP 37/07: Nokia to check the termination part of TD S3-050181 and the impact and need for CRs for other specifications
Closed, see TD S3-050264 and TD S3-050265.

4.2 Report from SA#27

TD S3-050186 Report from SA#27 plenary. This was introduced by the SA WG3 Chairman and had been sent to the SA WG3 e-mail list after TSG SA meeting #27. The report was reviewed and noted.

4.3 Report from SA3-LI#17

TD S3-050196 contained the report of the last meeting of LI. This is the same as TD S3-050187 (which was withdrawn).

TD S3-050204 contained the WID for the Rel-7 architecture for Lawful Interception. It was noted that the scope of this covers Rel-6 features such as MBMS and there was some concern that this will only cover Rel-7. It was answered that LI can only be covered one the Rel-6 stuff is completed. It was also noted that the Generic Access in the context of IMS enhancements could cause the LI to suffer and so there was some concern that the LI work should be part of this WI. It was asked if Rogers Wireless were added and it was turned into a feature. The revsions was provided in TD S3-050315 and It was agreed to be sent to SA for approval.

TD S3-050199 contained a CR to 33.107 with a correction on the Use of Identities for I_WLAN lawful interception. It was agreed to be sent to SA for approval as CR 052.

TD S3-050197 contained a CR to 33.107 on Clarification for the usage of the Notion of a Service in Distributed IP Networks.

It was noted that MSISDN in the WLAN TS and it was questioned if a packet network gateway has all the information it needs from the Radius parameters. There have been a few debates on this in LI and the MSISDN is sent to the PDG at tunnel establishment. There have also been discussions as to whether it is valid, but SA2 have confirmed that it is there. It was noted that the abbreviation for BM-SC is not correct (currently it is BM-CS). It was revised to TD S3-050316 and It was agreed to be sent to SA for approval as CR 51r1.

TD S3-050201 contained a CR to 33.107 IMS Correclation. It was agreed to be sent to SA for approval as CR 053.

TD S3-050202 contained a CR to 33.108 on Correction to IMS Correlation. It was asked if this LI work item is for IMS. It was answered that there is one section in the TS that is IMS. It is noted that IMS is bearer independent, but here it appears to be specific for GPRS. It was answered that this is an old problem and this message needs to be sent back to the LI group. It was agreed to be sent to SA for approval as CR 072.

TD S3-050205 contained a CR to 33.108 on Inconsistency in Annex B.5. It was agreed to be sent to SA for approval as CR 074. TD S3-050206 contained a mirror of S3-050205 for Rel-6. It was agreed to be sent to SA for approval as CR 075.

TD S3-050198 contained a CR to 33.108 on Clarification to the Timing Issue. This contains some re-numbering of clauses which is not strictly allowed. It was explained that with this, aligns the section 7 with that of section 6. It was noted that this should not happen again in the LI group. However, for this CR, it will be tried in SA. It was revised to TD S3-050317 to put a some comments into the front sheet to explain why the clauses are re-numbered and it was agreed to be sent to SA for approval as CR 070r1.

TD S3-050200 contained a CR to 33.108 on Clarification Pertaining to the Filtering of SDP for IRI Only Cases. It was asked what is meant by the whole of the SIP message and do all the headers need to be maintained. The answer is that in general yes. It was agreed to be sent to SA for approval as CR 071.

TD S3-050203 contained CR to on 33.108 with an IMS Correlation. It was noted that section 7.3 indicates that the section is informative. Also, there is a contradiction with S3-050198. The CR was sent back to the LI with a recommendation that it should be in a separate informative annex. It was rejected.

TD S3-050207 contained a CR to 33.108 regarding an obsolete Import Statement in Annex B.6. It was agreed to be sent to SA for approval as CR 076.

4.4 Report from 3GPP/TISPAN workshop

TD S3-050211 contained an unofficial report from SA3 delegates who attended the workshop.

IMS Extension WID (TD-22)

> TISPAN WG7 Interim meeting should send a LS to SA3 WG7 to send a summary of NGN/IMS R1 working assumptions and requirements (covering requirements from all TISPAN WGs, e.g. WG1 and WG2) and ask them to start working on IMS security extensions.
>
> The discussion proosed to keep the mainenance of IMS core security specifications in 3GPP.

Work Split between 3GPP and SA3 (TD-21r)

> This item did not cause larger discussion, it was advised to carry work on a reply to SA3 in the WG7 mailing list. This was started on the 6. April.

Usage of UICC in TISPAN (TD-25, TD-26)

> These items caused larger discussion. Several opinions pointed out the need to support a large range of services and devices and that TISPAN deliberation is required.

Resulting from the workshop was a liaison statement in TD S3-050232 which was moved to agenda item 6.1.1.

5 Reports and Liaisons from other groups

5.1 3GPP working groups

There were no specific contributions under this agenda item.

5.2 IETF

There were no specific contributions under this agenda item.

5.3 ETSI SAGE

TD S3-050229 contained a Progress and information report on UEA2 and UIA2 development. This is the same as TD S3-050233 which was noted.

Per Christoffersson gave a report on ETSI SAGE: SAGE is on schedule to deliver a “provisionally final” specification of the algorithms by the end of June. Formal conclusion of the project will take place either one or four months after that, depending on whether a three month public evaluation phase is included.

The confidentiality algorithm will be based on the well known public domain stream cipher SNOW 2.0 [EJ]. However, it is expect that a slight modification to the algorithm will be made to increase resistance against algebraic attacks (which we believe to be the type of cryptanalytic attack most likely to threaten KASUMI). There is a liaison with the SNOW designers to deal with this.

There are two options:

a) The first option is a polynomial evaluation MAC, similar to the one used in the Galois Counter Mode of operation proposed for AES [MV], using the UEA2 function as the required source of one-time secret data.
b) The second option is something like HMAC-SHA-256.

It was asked if the original Kasumi-based design will be available publicly. It was replied that it is not on the 3GPP website and the reason for this is that an export licence is not yet available. There is a licence, however, for the GSMA website and it is publicly available from there (www.GSMworld.com).

Regarding the public evaluation, having SAGE organise for this work to be done is acceptable, although there is no budget yet. Mr Bookson indicated that cleary there are some peole who may evaluate it for free, but if SAGE were to indicate how much is required to evaluate it, then perhaps this could be asked of the GSMA. It was estimated in the meeting that this could be about 20-30kEuros.

The meeting agreed that a public evaluation is required for the algorithms should be done. The next problem would be to find out how much it may cost to do this, and who might do it.

AP 38/01: Per Christoffersson to ask SAGE for a budget estimate for the evaluation of the algorithms, and an outline proposal on how it would be done..

AP 38/02: Once this is done, then funding, if required, chairman to organise some arrangements so that evaluation can be organised.

On the question of using a polynomial evaluation MAC or HMAC-SHA-256 it was noted that SHA is used in key derivation currently. However, other than this, the algorithm is not really tried and tested in 3GPP.

The delegates were invited to discuss this with their development departments regarding the re-using of SHA-256 for the integrity algorithm. It should be noted that there were some collisions regarding SHA-1, but there has not been an urgent call for a replacement of SHA-1. It is not understood that the same problems apply to SHA-256 or, indeed, it matters for the integrity algorithm.

Regarding option (a), it was noted that if option (a) is selected it will be very important to ensure that the same value of COUNT||FRESH||DIRECTION is not used more than once with the same value of IK. If it were, then the algorithm would become seriously insecure. It was commented that there is a possibility that for two handovers, the same same value of COUNT||FRESH||DIRECTION could be used. In addition, if something changes in the future

RLC layers, that could introduce a major vulnerability. If there is a concern on this, then option (b) would be more appropriate.

The delegates were again invited to discuss this with their development departments on the choice of option (a) or (b). Any comments regarding the choice shall be passed back to Per before the 17th May. If there are no comments, then this decision will be left up to SAGE.

5.4 GSMA

Charles Brookson gave a brief report on GSMA SG. There have been no meetings since the last SA3. The Security Group was working on countering Trojan Horses and Virus threats to mobile terminals. This was seen to be an important item for this year, as there was increasing evidence that executable code on smart phones was capable of being compromised. This could lead to an increase in fraud.

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

The next meeting will on the 6/7 June in Paris. An invitation was extended to anyone who might want to intend the meeting (and who were not GSMA members) to contact Charles Brookson to discuss attendance.

The new CEIR is being rolled-out and is based in CANADA. A six monthly report for the EU is available for EU members.

GSMA SG Report for SA3 April 2005

The next meet of the GSMA SG will be in Paris on the 6/7th June.

As well as Trojans and Viruses, which are proving to be an increasing issue with smart phones, the items for the SG are:

1. Withdrawal of A5/2 cipher algorithm from GSM handsets and networks
   Proceeding well.

2. Development of New UMTS Cipher Algorithm
   As described in the SAGE report.

3. Anti-SMS/MMS Spam Handset Functionality

4. Automatic uploading of critical updates in handsets
   We think this may an issue if it is not done securely.

5. Develop Wireless Emergency Response Service (WERS)
   Something we have been working on for some time.

6. Guide to migrate from 2G to 3G
   To help operators.

7. Monitor Manufacturer Compliance with IMEI Integrity Principles
   The new CEIR was introduced this month, and is being rolled out to other operators. We produce the regular report to TCAM so that the EU can be updated on our progress as an industry.

8. Define functional requirements for secure terminal platforms

9. Define generic functional tests for Data Networks and Service Providers

10. Security risk analysis of emerging services

It was asked if ENUM was an item in GSMA SG. The answer was “no” at this time.

5.5 3GPP2

The report of 3GPP2 security work was provided by Anand Palanigounder. A meeting was held last week in Dallas.

LCS security framework document (S.P0110) is baselined in the 3GPP2 April 2005 meeting and is expected to be recommended for publication process in the May 2005 meeting.

Discussions on the appropriate bootstrapping method for 3GPP2 GBA is on-going and is likely to be based on HTTP (e.g., variant of DIGEST and/or password protected Diffie-Hellman). This is mainly being driven by the need to support different authentication methods (e.g. CAVE, CHAP, AKA) that are implemented in the 3GPP2 terminals

5.6 OMA

James Semple gave a report about OMA SEC activities at the recent meeting in Singapore 11-13 April. The main activity was completion of the Architecture document and Technical Specifications for Location Based Services (SUPL). In the 3GPP scenario the security solution is based on GBA and PSK-TLS, with options for MSISDN-IP address binding for authentication in early terminals. 3GPP2 is also based on PSK-TLS but does not discuss provisioning of the ‘top’ key, though the aim will be to support GBA as that work item progresses in 3GPP2.

Another WI of interest is Security Common Functions. Qualcomm suggested that it would be useful for SA3 to report any decisions made about 2G GBA to OMA SEC, as it may be of interest to the Common Functions work, and member companies should try to take a consistent approach between OMA and 3GPP about the need to deploy new services based on SIM.

An incoming LS (TD S3-050004) was dealt with under agenda item 6.20.

5.7 TR-45 AHAG

There has been some correspondence between the chairmen of SA3 and AHAG with the result that there will be joint session with SA WG3 during the Montreal meeting.

5.8 Other groups

TD S3-050227 contained a Reply LS to ITU on general security policy. This is the same as TD S3-050231 (which was withdrawn). This is the outcome of the email discussion on the subject. Some comments were made on line.

It was noted that there are some specifications which appear to be endorsed by SA3 in this liaison statement and these have not been discussed in SA3,

A revision was provided in TD S3-050285 and it was agreed to send this liaison statement.

TD S3-050240 contained a draft contribution from ITU-R WP8F on current 3GPP activities toward IP applications over mobile systems. ITU-R Ad Hoc has prepared the draft contribution contained in Annex 2 with the goal to provide to ITU-R WP8F information on what is already available in 3GPP and a view on the activities currently ongoing toward the future development of UTRAN.

It was noted that SA3 is being asked to review the annex 2.

The meeting decided that there is sufficient information in annex 2 and so it was noted.

6 Work areas

6.1 IP multimedia subsystem (IMS)

6.1.1 TS 33.203 issues

TD S3-050267 conatained a CR to 33.203 on Description of 2xx Auth_Ok message. It would appear that a description of 2xx Auth_Ok message is missing in the IMS registration flow. It was revised to TD S3-050302 and It was agreed to be sent to SA for approval as CR 080r1.

TD S3-050232 contained a liaison statement from TISPAN on cooperation related to IMS security extensions for fixed broadband access. From WG7 point of view, the highest priority is given to IMS signalling protection solution that traverse NA(P)T and firewall devices in the customer environment. Without this solution, TISPAN NGN/IMS Release 1 cannot be completed. It was noted that one deadline is September and so it would be good to have the joint meeting as soon as possible. Probably the June TISPAN #06bis meeting would be appropriate. Alternatively, the September TISPAN #08 is concurrent with an SA3 meeting, though sadly their only meeting which is not in Sophia Antipolis coincides with the SA3 meeting expected to be Sophia Antipolis (although this is not on the 3GPP site). This would be an excellent opportunity to co-location the meeting.

It was reported that the TISPAN work is still fluid and the assumptions could change. Nonetheless, some start could be made, but SA3 should be flexible if the assumptions change. A proposed response was provided in TD S3-050303. It was agreed to send this liaison statement.

AP 38/06: Chairman and Secretary to agree arrangements with TISPAN for co-locating a meeting with TISPAN on the 12-16th September in Slovenia and organise hosting.

TD S3-050283 contained a proposed Updated WID proposal for IMS security extensions (this is a revision of TD S3-050271 which was noted). Certainly some indicationg of timing for output is required, but there were some papers commenting on it and so these were taken before making a decision.

The first comment came from Ericsson in TD S3-050243 contained an Analysis of GBA based IMS signalling protection proposals. There are many major changes to current IMS specifications and the proposed change is too big for SA3 to make any decisions on it alone. Other working groups, e.g. SA1 and SA2, should be consulted before making any decisions related to this idea. From security point of view, SA3 should carefully analyze what is actually gained by GBA in this context, and is this new security service important enough to motivate such a major change to IMS. This document was noted in light of the revision of the WI in S3-050304.

TD S3-050242 contained a Proposal for SA3 working assumptions on IMS security extensions. It is understood that SA3 will initiate Release 7 work on IMS security extensions in SA3#38. Therefore, this input provides an overview of current TISPAN NGN/IMS Release 1 requirements, and identifies an initial list of working assumptions for future work. This document was noted in light of the revision of the WI in S3-050304.

TD S3-050244 contained some Nokia comments on Ericsson contributions: "Analysis of GBA based IMS signalling protection proposals" (TD S3-050243) and to "Proposal for SA3 working assumptions on IMS security extensions" (TD S3-050242). There would appear to be a bit of a misunderstanding in that the intention of "IMS GBA" is not to replace IMS AKA but have it as an optional method for authentication in IMS. An operator using GBA for a large range of services, might wish to deploy it also for IMS.

TD S3-050255 also contained some Comments on two IMS-related contributions (Working assumptions and WID). The general proposal is to include Generic Access Security (GAS) into the work item.

Regarding the use of WLAN for this GBA, it was commented that IMS Rel-5 architectures are due to be deployed soon and this also needs to be taken into account. Some operators may wish to implement IMS and not GBA as per the approach for WLAN. So it is not sure that including GAS as part of IMS is not such a good idea. Another comment was that the approach in S3-050255 could well be a stop-gap approach to security in IMS, but also there should be a more in-depth approach as suggested by S3-050244.

There was a great deal of discussion as to which is the correct approach to take. The options are GBA, TLS, GAS, etc.. There was as proposal to have the Generic Access Security into the WI, but this notwithstanding, there were no real objections to the WI. The question is if the GAS could be included into the WI. There was a comment that it is not clear what it really is, although there was a proposal to describe it. In the end, SA3 should study all options.

Another comment was that TISPAN has stated they cannot necessarily rely on having a physical UICC to implement the security mechanisms. This could be a problem for SA3. It was clarified, however, that the words in the WI were carefully chosen to indicate it is a reality that there may not be a UICC in the end terminal, but that in this situation, there will be some access to an UICC in some form (i.e.functional split case). The the words were chosen to allow for some compromise, whilst still maintaining the security.

This was revised off-line and was presented in draft form. There were some comments regarding the output expected. The revision of the WI for this was provided in TD S3-050304. The revision marks were accepted and the clean version was provided in TD S3-050320. It was agreed to be sent to SA for approval.

TD S3-050239 contained a Scalability of IMS/TLS server certificate deployment in which IMS related TLS server side certificate deployment is discussed with some clarification of the potential scalability problem. There are also two alternative solutions for the problem. It should be noted that the document assumes IMS roaming is a strong requirement also in fixed broadband access.

It was noted by the chairman that this document, which was presented to TISPAN, would be relevant to SA3 also if the WID is approved. It was asked what the transport protocol would be; e.g. UDP SCTP or TCP. It was answered that in IETF Datagram TLS seems to be gaining support.

The meeting was invited to provide further comments to the author. It was noted.

6.1.2 Security for early IMS

TD S3-050237 contained a discussion paper on the use of 401 Unauthorized and 399 Warning in Early IMS. The current text in clause 6.2.6 of TR 33.978 v200 (Early IMS security) does not conform with RFCs 2616, 2617 and 3261, because the 401 message and the 399 warning header are not used as they must. The new proposal is to use the algorithm field in the www-authenticate header to indicate early IMS to the UE which started communication with IMS AKA.

The CR to implement this was provided in TD S3-050238. In interworking case 5 of section 6.2.6, it is proposed to use 401 Unauthorized with a www-authenticate header with algorithm identifier “3GPP-early-IMS”, the warning header 399 is omitted.

Another proposal was another proposal was to remove all the text. There was some concern with this since there were no representatives from the oringator of the text at the meeting. Subsequently, it was discovered that this was done some time before.

It was revised and provided in TD S3-050305. It was agreed to be sent to SA for approval as CR 001.

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

TD S3-050228 contained a discussion document on Evaluation of ‘Fallback to unprotected mode’-parameter.. This specifically deals with the Sending Direction. It was agreed that the work on the MAP-sec gateway solution could be based on the assumption that *A Fallback indicator in the sending direction is not needed in this two phase approach but the fallback indicator in the receiving direction can only be reset if all partner PLMN’s use gateways*.

The document was noted.

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

There were no specific contributions under this agenda item.

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

6.5 UTRAN network access security

TD S3-050236 contained a draft LS to GSMA SG on recommendations resulting from a review of recently published papers on GSM and UMTS security. This was a result of an action 37/05 based on a discussion of S3-050101 on GSM and UMTS security. The email discussion after the meeting did not result in any comments.

In order to counteract the particular threats described in this paper, then the action needed is to have a new authentication when a mobile in Idle mode moves from a 2G MSC to a 3G MSC. In the GSMA SG, there is a guideline which is referred-to in the roaming agreements.

The liaison statement was provided in TD S3-050306 and It was agreed to send this liaison statement.

TD S3-050245 contained CR to 33.102 on Keystatus sent by CN node in Security Mode Command for Rel-5. RAN2 has clarified in CR R2-041837 on TS 25.331 (Rel-5) in which cases the UE shall expect keystatus 'new' in Security Mode Command message. GERAN specifications (A/Gb mode) currently do not specify handling of 'keystatus'. Also TS 33.102 does not specify explicitly in which traffic cases a CN node shall send keystatus 'new' in Security Mode Command message. It is proposed to add one sentence to TS 33.102 clarifying the traffic cases where CN node shall send keystatus 'new'.

It was commented that in 25.413 there are some Key staus settings and it is was not really know if all the cases are covered by this CR and or if it contradicts. Key status is also used by CT1 in their specifications. So it may be it may be prudent to sent this to RAN3 and CT1 in a liaison statement to make sure all is OK.

The liaison statement to do this was provided in TD S3-050308 and the revised CR was provided in TD S3-050307. This will be attached to the liaison statement in TD S3-050308. It was agreed to send this liaison statement.

TD S3-050246 contained the equivalent CR to 33.102 on Keystatus sent by CN node in Security Mode Command for Rel-6. With the decision to send this to RAN3 and CT1, this document was noted.

6.6 GERAN network access security

TD S3-050189 contained a liaison statement on providing IMSI and IMEI to the SMLC in positioning procedures. GERAN WG2 are in the process to allow IMSI and IMEI identities to be provided to the SMLC for the purposes described in GP-051013 which was attached. GERAN WG2 did not see any issue or security threat in approving the proposed enhancement but is sending it to SA3 for confirmation.

A discussion document on this was provided in TD S3-050226. The conclusion of the document was that there is no threat and a proposed liaison statement indicating this was provided in the zip-pack.

It was questioned if there may be an impact to the WI on Generic Access to A/Gb interface. It was answered that Generic Access to A/Gb interface has a separate gateway and does not enter the picture. There is another issue in that the SMLC now stores context information about subscribers; previously there would not have been any context information. This is probably not a great threat, but perhaps should have been included in the study. Also applications for LCS is normally buried deep in the core network, but typically the SMLC could be co-located with the BSC and could be vulnerable. Therefore, the motivation to break in to the SMLC may be higher with this change. This should be noted in the liaison statement and put an action on GERAN 2 such that SA3 need to be kept in the loop to ensure the identity

The liaison statement was provided in TD S3-050309. It was agreed to send this liaison statement.

TD S3-050213 contained a Access Security Review TR v 0.0.1 from the last meeting. A number of comments have been provided to this and so this document was noted as a starting point for this meeting.

TD S3-050221 contained a Comments on TD S3-050213: Access Security Review TR v 0.0.1. There were some comments on the comments (phew!). It was noted that the persistent attacks should be included in the study. It was decided to modify the TR in line with this document. It was noted. It is not yet ready to be sent to SA for information.

TD S3-050214 contained a Progress of Access Security Review. This was a continuation of the threat analysis is has been made, and the results thereof are proposed to enhance the report and it is proposed to add this to the TR. It was agreed to be included in the next version of the TR.

TD S3-050222 contained a Feature dependencies evaluation and it provides six new proposals for security enhancements. It was not sure where best to put this, perhaps section 10 or 11. It was commented that one aspect is missing and that is the Generic access to A/Gb. The answer was that this issue is missing from the whole TR and may need to be included throughout the document.

It was asked if the protection against algorithm negotiation bidding down attacts is for false base station eavesdropping. The answer was that it is not and this could well be a new element. Also, on the conclusion the usefulness seems to be based on the threat without an analysis. For instance (5) does not appear to give a significant increase in security, but it is a less costly feature to deploy and maybe this would cause it to be raised in profile. Hence, the analysis needs to take place in respect of several parameters. It was agreed to be included in the next version of the TR but the priorities are left open for the moment.

6.7 Immediate service termination (IST)

There were no specific contributions under this agenda item.

6.8 Fraud information gathering system (FIGS)

There were no specific contributions under this agenda item.

6.9 GAA and support for subscriber certificates

6.9.1 TR 33.919 GAA

TD S3-050253 contained a Draft LS out on on the usage of 2G SIM cards in GBA (this is the same as TD S3-050282 which was withdrawn). This was based on a document from Nokia that did not quite make it as an input document. The meeting schedule for SA1 does not really align with that of SA3 and so the final paragraph was added by Vodafone to allow the work to continue and let SA1 ratify the assumptions prior to SA in September.

It was also commented that using a 3G SIM card to access 3G GBA-based services, could be included in a TS rather than a TR. It was also commented that this decision could be made independently of SA1; particularly since this could open the dabate about the limited security of early 3G. At the last meeting, it was decided to get SA1 involved. This was because currently there is no specific requirement for this.

Fortuitously, the Vice Chairman of SA1 was present and was asked if the requirement already existing for the use of GBA. It was answered, and confirmed by the secretary of SA1 (who fortuitously was also present) that there are no requirements specifically for GBA. The chairman confirmed that the use of subscriber certificates would be implemented by GBA.

It was noted that if SA1 is being asked if this is required on a per-service basis, then this could cause some conflicting requirements. This was subsequently refuted. It was asked how this relates to section 7.2.1 in 22.228? The answer is that this was thought to be useful requirements to base the work on. It should be noted that this solution will provide a weaker security than what is available in 3G, but will allow the services to be started early.

The key here is to ask the right question of SA1. For example, SA1 could be asked if there is a plan to allow access to 3G with 2G SIMs since there are so many 2G cards in the market. It could be indicated that there are certain applications that GBA is intended to be used for in 3G and would SA1 like this to be extended to 2G SIMs? After all, it would be a pity to do all the work and have SA1 indicate that there is no requirement.

However, bearing in mind the time, it probably be better to do the work and then ask SA1 if it is required.

It was agreed that the work will continue tentatively with some CRs at the next meeting and send all this to SA1 from the next meeting.

AP 38/03: S. Holtmanns to draft an liaison statement to SA1 indicating why 2-GBA may be advantageous to SA1 and ask SA1 if this is required.

TD S3-050263 Status of evolvement of GAA Enhancement WID During the last meeting a WI was provided on possible GAA enhancements. In it some examples were mentioned. Several companies expressed interest in supporting the WID, but would like to see the further development on the mentioned topics first. Therefore the clear need and details for such a WID is still under discussion and should be continued.

It was noted that the OMA BCAST workshop with 3GPP, 3GPP2 and DVB-H is on the 23rd May and not on the 24th May. It was decided to continue on the items independantly with a view to creating a WI in September. It is too early to agree on this WI.

6.9.2 TS 33.220 GBA

TD S3-050234 contained a discussion document on GBA User Security Settings (GUSS) transfer optimisation. This paper discusses the methods to transfer GUSS from the HSS to the BSF, and how to minimize the traffic load related to the GUSS transfer procedure. The document was noted.

TD S3-050235 contained the CR to implement the changes. A GUSS timestamp is added to each GUSS indicating when the GUSS was last changed by the HSS. This timestamp is used to optimise the GUSS transfer policy between the HSS and the BSF: If the BSF has subscriber's GUSS in memory when it needs to fetch a new authentication vector (AV) for the subscriber, it will also include the GUSS timestamp to the request. Upon receiving the GUSS timestamp, the HSS will compare it to the time of the GUSS it has in its databases. If the timestamps are equal, the HSS does not send the GUSS to the BSF as the BSF already has a copy of the GUSS. If the timestamps are not equal, the HSS sends the GUSS as the BSF has an invalid GUSS, which needs to be updated. If the HSS has no GUSS, then it will send a no GUSS message to the BSF and the BSF will delete the old GUSS.

It was revised to TD S3-050286 and it was agreed to be sent to SA for approval as CR 052.

TD S3-050270 contained a CR to 33.220 on Correcting figure 4.4. Figure 4.4 indicates that the first message would be protected by a MAC. The use of the term MAC in the figure might be confusing and no corresponding text explaining the MAC is included in the body. It might not even be possible to protect the first message using a MAC with all Ua protocols.

It was revised to TD S3-050287 to tick the boxes and It was agreed to be sent to SA for approval as CR 51r1.

TD S3-050247 contained a discussion document on Usage of USS. The current TS 33.220 is ambiguous in the usage of User Security Settings (USS). This document indicated that ambiguity in the usage of USS can lead to possible security and interoperability problems. To overcome these problems it is proposed that it should be specified per application if USS is used or not. The CR to implement this was provided in TD S3-050248.

TD S3-050254 contained some comments on this discussion document. The contribution “Usage of USS” points out that there is some room for misunderstandings how the local policy enforcement in the BSF in done. However, this contribution dispels some of the misunderstandings and explains how operator local policy enforcement actually works in the BSF using GUSS/USS for the four cases that BSF has (not) a local policy and the NAF does (not) require a USS. In the end, there might be some need to clarify this, but the Ericsson way implies too much complexity.

TD S3-050249 was revised to TD S3-050281 prior to presentation, but also included some comments to the CR and discussion document. The Siemens view is that there is not an ambiguity, but that it is a deliberate decision. GBA is a generic feature with multiple use cases, Thus TS 33.220 cannot specify USS usage as mandatory, As mentioned, for the sake of interoperability, for some applications USS flags are specified, but in the TS specifying the application.

It was requested that the three parties should get together and determine a way forward and a joint contribution. This was provided in TD S3-050288. It was agreed to be sent to SA for approval as CR 050r1.

6.9.3 TS 33.221 Subscriber certificates

There were no specific contributions under this agenda item.

6.9.4 TS 33.222 HTTPS-based services

TD S3-050188 contained a discussion paper on HTTPS connection between an UICC and a NAF. During SA3#37, SA3 has agreed upon the working assumption that the HTTPS connection between a UICC-based application and a Network Application Function (NAF) is an option for TS 33.222 [1]. This contribution analyses the impacts of the use of HTTPS to secure the communication between a UICC-based application and a NAF, on the UE and the NAF.

TD S3-050275 contained Comments to HTTPS connection between an UICC and a NAF. It was questioned what are really the specific requirements from the OMA? There were a number of other impacts on the Axalto and Gemplus approach.

It was commented that to have one FQDN per NAF is not a restriction since it is rare to have more than one service on one machine, but rather it is normal to have one service on more than one machine. This was refuted with the information about virtual hosting which would mean that more than one service/application (or part thereof) could be hosted on one machine.

Another comment would appear to be specific to one type of implementation and so, once again, it was requested to understand more what the OMA is intending.

There is an agreement that a change is required to some TSs, but TD S3-050275 indicates that CT6 should be involved with regard to the Refresh command. It was further noted that there is already a Refresh command.

An overall point made was that a threat analysis should really be conducted before going forward with putting a browser (et al) on a USIM. The risks need to be known. An opposing view was that these applications will be from trusted sources and the risk is low. Also, the whole concept is being designed in conjunction with the OMA security group.

It was agreed that essentially there should be CRs for 24.109, 29.109 and 33.222. The CR to 33.222 is expected at the next meeting.

TD S3-050276 contained some comments on S3-050216 and S3-050219. The objective it to stimulate what issue that need to be discussed further and to indicate that this will not make Rel-6.

There was some debate regarding the CRs and that they were for Rel-6 and not for Rel-7. A possible solution would be to have a restricted function for Rel-6. Of course, there is an issue of backwards compatibility if a solution is provided in Rel-6. Another issue is the failure cases when incompatible keys are used.

It was noted that the work is being done quickly and during the meeting. Whilst this is not a problem per se, there is a danger that this could be done too hastily and mistakes could be made. Another approach would be to have this as a candidate for Rel-7 but for early implementation. It was agreed to finish all the work at the next meeting in June and try to propose this as a candidate for early implementation.

There was a question indicating if HTTP header to indicate the type of keys to be used? This is in reation to S3-050276 and section 3.2. It was noted that CT1 is already using the UA Header already, so perhaps it is possible.

It was agreed that the deadline for contributions on this topic, in order to give time for discussion and response will be Tuesday 7th June 2005, 16.00 CET, comment deadline remains the usual document Tuesday xx June 2005, 16.00 CET.

TD S3-050209, TD S3-050210, TD S3-050212, TD S3-050216, TD S3-050217, TD S3-050218, TD S3-050219, TD S3-050220, and TD S3-050262, were noted in conjunction with the discussion on S3-050276. They should be used as the basis for email discussion.

AP 38/04 Mauro to build on TD S3-050210 to remove the inconsistencies in 33.222 over an email discussion.

In the meantime, there is a mis-alignment between 33.220 and 24.109 for Rel-6. This needs to be corrected and so document TD S3-050289 was provided in draft form. It was agreed to send this liaison statement.

In the process of reviewing 33.222 it was noted that there was an editor’s note in the TS. It was decided to delete this and the CR to do this was provided in TD S3-050301. It was agreed to be sent to SA for approval as CR

6.10 WLAN interworking

TD S3-050278 contained a Reply LS on Mandating functionality in WLAN Ans. SA3 is being asked to consider the effects of making "immediate purging of a user from WLAN AN" a mandatory feature, and provide the necessary changes in their specifications. It is not clear if a periodic re-authentication will also purge a user from WLAN AN.

TD S3-050264 contained a discussion document on Terminating WLAN session by AAA server. The conclusion is that to be consistent with SA2 specification, SA3 needs to add RFC 3576 as reference in TS33.234. Also to add a NOTE at the end of the new section 6.1.6 on having RFC 3576 mandatory would be useful. The CR to do this was provided in TD S3-050265.

There appears to be two different approaches to the requirements. It was also questioned what is intended with on line billing. It is assumed that the RFC is secure in its own right and that SA3 has incorporated it in good faith. In the end, some analysis is required on this subject and could well end up on more CRs. In the meantime this CR fulfills the requirements of SA2. It was also noted that in section 5.5 there is immediate service termination and this could well be used instead. It was decided to check what the views of CT4 are.

Document TD S3-050264 was noted. TD S3-050265 was revised to TD S3-050312. There was confirmation from CT4 was received that the concept of SA2 has been accepted. It was agreed to be sent to SA for approval as CR 065r1.

A response to the LS from SA2 in S3-050278 was provided in a draft form TD S3-050313. It was noted that S3-050181 has been sent to SA #27 and has been approved and so this does not really need to be indicated to SA2. However, it should be noted that SA3 needs to highlight that this is relevant to SA2. It was revised on line and It was agreed to send this liaison statement.

TD S3-050311 was a proposed reply to S3-050265. This was not satisfactory and so a replacement was provided in TD S3-050313. TD S3-050311 was withdrawn.

TD S3-050277 contained a reply LS on Control of simultaneous accesses for WLAN 3GPP IP access. It would appear that SA2 is very pleased with the CR that was provided to SA2 in S3-050179 and S3-050151. Now the CR was produced at SA3 #37 and it went to SP #27 where it was approved. TD S3-050277 was noted.

TD S3-050214 contained a discussion document with a proposal to improve efficiency in setting up UE-initiated tunnels (Scenario 3) in WLAN interworking. The conclusion of the document is that if a UE accesses WLAN via EAP-AKA, then it can generate a key as pre-shared secret between the UE and the PDG for IKEv2 mutual authentication. The document suggests to include the proposed method to 33.234 as an option for Release 7.

It was asked if this proposal would cause a change to the RFC. The answer was that this needs to be checked. Also, this process seems to link scenario 3 with scenario 2 and it is not clear if this will always be the case. It was clarified that in this case the old method is used. Also, it was noted that one of the requirements is that the authentication of scenario 3 should be independent of scenario 2. It was also noted that UMA has gone straight for scenario 3 and this would stop this solution and/or the standards will diverge.

The group had some concerns and so this cannot be approved at this meeting and some more checking needs to be done. It was noted.

TD S3-050256 was revised prior to presentation to TD S3-050310 and contained a CR to 33.234 on Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access. There are no security holes in using multiple IPSec SAs per IKE_SA, so release-6 specs should not carry text that suggests that it has some. Considering rekeying to avoid session interruption, at some point in time, two IPsec SAs need to coexist.

There was a number of emails regarding QoS and that this may need to be revisited for Rel-7. There was also some concern that the scope has changed. It is no longer seen as future-proofing. It was proposed to modified in a way that there is a maximum number of IPsec SAs by subscription. If this is the case, then the PDG should have the control. This is not a problem but there probably should be another parameter between the AAA server and PDG.

It was revised to TD S3-050314 and it was agreed to be sent to SA for approval as CR 064r2.

TD S3-050266 contained CR to 33.234 on Correction to the definition of the Wn Reference Point. It would appear that analysis by CT4 on the text in TS 29.234 related to Wn has led to the conclusion that it should be clarified that the specific method to implement this Reference Point is out of scope of 3GPP. CT4 have agreed a CR to 29.234 removing the description of the Wn reference point from Stage 3. The change proposed in this CR brings 33.234 in line with CT4's analysis and the changes made to 29.234. It was agreed to be sent to SA for approval as CR 066.

6.11 Visibility and configurability of security

6.12 Push

There were no specific contributions under this agenda item.

6.13 Priority

There were no specific contributions under this agenda item.

6.14 Location services (LCS)

There were no specific contributions under this agenda item.

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

TD S3-050230 contained a discussion document on a solution for (U)SIM security reuse by peripheral devices on wireless local interface.

It was asked why this work is required since UE Split functionality is already described (33.234). It was answered that this document shows how this could be implemented. Still there was a comment that it is not understood what this work may add. It was also not clear what exactly needs to be standardised, although there were some comments that this could make the SIM/USIM vulnerable.

It was suggested that the search functionality has been rejected. Without this, it was not clear what is added to the SA3 TSs. This should be done in the form of CRs. The document was noted.

The WI in TD S3-050280 was noted for this meeting.

6.16 Open service architecture (OSA)

There were no specific contributions under this agenda item.

6.17 Generic user profile (GUP)

There were no specific contributions under this agenda item.

6.18 Presence

There were no specific contributions under this agenda item.

6.19 User equipment management (UEM)

There were no specific contributions under this agenda item.

6.20 Multimedia broadcast/multicast service (MBMS)

TD S3-050192 contained a liaison statement MBMS User Service finalization. SA3 is being asked to review clause Annex C (IANA registrations) of the attached TS 26.346. It would appear that SA4 does not use MIME types from the vendor tree and SA3 is being asked to modify their SA3 MIME-Type proposals.

Also, SA4 is asking SA3 to review clause 5.2.2.3 “Service Protection Description” and provide definitions for the “confidentiality protection”, “integrity protection” and “UICC key management” xml attributes.

There is a proposal from Ericsson regarding the definitions in TD S3-050252 and TD S3-050258. These should be taken first.

This was done and a revision was provided in TD S3-050300. It was agreed to send this liaison statement.

Ericsson volunteered to provide a CR to 33.246 for the parameters in the MIME types. This was provided in TD S3-050290. It was agreed to be sent to SA for approval as CR 066.

TD S3-050279 contained a reply LS on MBMS User Service finalization from SA4. This is a communication between SA4 and SA2 on BM-SC Proxy and Transport function in MBMS. It was copied to SA3 and it was noted.

TD S3-050193 contained a liaison statement on a new basis for the 3GP file format. This is a communication between SA4 and external groups on a new and improved file format for MBMS. It was copied to SA3 and it was noted.

TD S3-050194 contained a reply to Liaison Statement on Status of OMA Mobile Broadcast Services. The reply from OMA was provided in document TD S3-050190. OMA BCAST has understood that there is significant overlap between MBMAS and BCAST scope and functionalities, and will consider that in their specification work. It was copied to SA3 and it was noted. Also noted was the invitation to the informal workshop on Mobile Broadcast Service Standardization.

The chairman asked if anyone will attend this workshop.

AP 38/05 Ericsson to provide some company contribution input to the the delegates from their company as briefing for the informal workshop on Mobile Broadcast Service Standardization. This should be sent out on the email list by 8th May for comments. Deadline for comments to be 15th May.

TD S3-050208 contained some comments to 33.246 with changes marked from Siemens. This was withdrawn since comments are included in TD S3-050272.

TD S3-050269 Consistency check: requirements, functions and mechanisms. According to the updated issue list to complete MBMS Security [S3-050183] from SA3#37 the consistency check has not been completed. In this document the results of mapping the MBMS security requirements into security functions and mechanism are provided. The security requirements and security functions/mechanisms the requirements R3b and R4b need to be clarified. Apart from these two requirements, the MBMS security requirements have been adequately met.

On R3b it was indicated that this is probably met already. In R4b, it is the identity of the content provider which is the point of issue. Hence, it is necessary to clarify the requirements a bit rather than do any specific work to close the gap. Furthermore, the communication is point to point and so the information is protected with the GSM bearer security. However, the point to multipoint is not protected; nonetheless, there does not appear to be a significant security risk.

So, in this particular situation, it seems that there is a match between the requirements and the mechanisms. It was suggested that since this work has been done, the result needs to be recorded somewhere either as notes in these minutes or as an annex to this TR.

An update of this document was provided in TD S3-050291. There was some discussion as to whether it should be an annex or a TR in its own right. It was proposed to add this as an informative annex and, if possible, for Rel-6. The CR was provided as a draft in TD S3-050319. It was agreed to be sent to SA for approval as CR 067.

TD S3-050259 contained a Status of MIKEY related IETF work. The IETF draft draft-ietf-msec-newtype-keyid-01.txt [1] introducing the necessary modifications to MIKEY required by 3GPP MBMS has passed working group last call without any major comments, and is now awaiting evaluation by Area Director (AD). The document was turned over to the AD 2005-04-01 and has been recognized. However, no further action from the AD has been taken. It was noted.

TD S3-050272 contained a CR to 33.246 on Editorial corrections to TS 33.246. It was noted figure 4.3 there is a box missing. It was noted that there is another CR that changes this figure and the issue will be corrected there. It was revised to TD S3-050318 and it was agreed to be sent to SA for approval as CR 062r1.

TD S3-050268 CR to 33.246 on Omitted MTK Update Error Message. At the moment, the RFC 3830 specifies that all errors SHOULD be reported to the peer(s) by an error message. The BM-SC is vulnerable to the denial of service attack, because the MTK update uses multicast and MSK_I is shared with a large number of UEs. An attacker may generate many erroneous MTK update messages with a valid message authentication code. In the result, the BM-SC may be exhausted by error messages, which were sent by genuine UEs.

It was commented that a more strict approach should be taken whereby the UE should never send a reply to MTK update messages. It was revised to TD S3-050292 and It was agreed to be sent to SA for approval as CR 061r1.

TD S3-050274 CR to 33.246 on Use of IMPI in MBMS. GBA TS 33.220 specifies that BSF *may* send the IMPI to the NAF. It has not been specified if IMPI is sent in case of MBMS. When the UE has run a new bootstrapping and contacts the BM-SC with a new B-TID, the BM-SC needs the IMPI to bind the old B-TID to the new B-TID (and continue the session over Ua with the UE with new GBA-keys). This CR proposes that IMPI is sent from BSF to the BM-SC when GBA-keys are received from the BSF.

It was commented that the membership function should be put into the reason for change. Also, in 6.2.1.3 the keys should be 'sent' and not 'received' and a reference to the definition of IMPI should be put in. A revision was provided in TD S3-050293. It was agreed to be sent to SA for approval as CR 064r1.

TD S3-050273 CR to 33.246 on Clarifications on MBMS key management. There are a number of changes, the reasons for which, are on the front sheet. On the last change in the annex, it is agreed that authorization is not necessarily needed, but authentication is needed and it was suggested that the change could reflect this. It was revised in TD S3-050294 and It was agreed to be sent to SA for approval as CR 063r1.

TD S3-050251 contained a dicussion document on Globally unique MSKs and MKIs. This introduced the CR that was provided in S3-050252.

There was a comment that the assumption is that the user is connected to two BM-SCs of two operators and it was questioned if this is possible. It was answered that this could occur in a roaming situation and besides, it was not known if this scenario is restricted. At the end of the day, there is no specific requirement in TS 23.246, but then it is not specifying that it is not possible. This CR covers the situation should it occur. This was agreed.

TD S3-050252 CR to 33.246 on Clarification of MSK ID in announcement (or Globally unique MSKs and MKIs). There are situations when a UE is connected to multiple BM-SCs that could lead to that the wrong MSK/MTK is used. This happens if two or more BM-SCs by accident use the same MSK ID.

Another point made was Key Domain ID and Key Group ID could be combined in MSK ID. Moreover, the problem is really only for streaming and does not apply to download. There was an off-line discussion and a revision was provided in TD S3-050295 and It was agreed to be sent to SA for approval as CR 059r1.

See liaison statement from SA4 in S3-050192.

TD S3-050257 contained a discussion document on MSK identification in SRTP streams to introduce the CR in S3-050258.

TD S3-050258 CR to 33.246 on MKI and authentication tag length in User Service Description (SK identification in SRTP streams). It was asked what was included for the parameters for integrity protection. The answer was that the in the download case the information is already available. Some checking was taken off line with regard to the download case. It was revised to TD S3-050296 and it was agreed to be sent to SA for approval as CR 058r1.

See liaison statement from SA4 in S3-050192.

TD S3-050223 contained a CR to 33.246 on Clarification on CSB ID and SP payload useage.There is some confusion about wording 'not used' of MIKEY header fields. Whilst this is not directly related to the change, there was some concern that the MIKEY header is becoming longer and longer and perhaps a random number could be used. It was answered that this solution makes the TS future proof. It was revised to TD S3-050297 to add the CR number and It was agreed to be sent to SA for approval as CR 065.

TD S3-050224 contained a CR to 33.246 on Using MTK within an RTP session and relation to FEC streams. The CR is intended to Clarify how MTK should be applied to (FEC) repair streams. It was noted that there is an overlap with S3-050261 and so it may be better to merge these.

TD S3-050260 contained a discussion document on Usage of Key Group in MBMS security. This document introdruces the CR in S1-050261.

TD S3-050261 contained a CR to 33.246 on Clarification of key management overview (Usage of Key Group in MBMS security). The granularity of MBMS security is not according to SA4 TS 26.346. Also the description of the relation of MBMS User Services and usage of keys is underspecified. It was asked how this relates to the point-to-multipoint and parallel sessions. The answer was that this is the simple case and the whole group is treated as one receiver. Another question was received on note 3 and the possibility to update MSK within an RTP media flow and if this was correct. It was answered that better terminology would be "during" and not "within".

It was revised to TD S3-050298 and also contained the changes in TD S3-050224.

TD S3-050298 was agreed to be sent to SA for approval as CR 060r1.

TD S3-050195 contained a liaison statement on stream bundling for MBMS from SA4, which has discussed a proposal for ‘stream bundling’ for MBMS Forward Error Correction. SA4 would like to receive feedback from SA1, SA2 and SA3 on whether there are any service, architectural or security issues, respectively, with this proposal. It was noted (see response in S3-050299.)

It was reported that SA1 is supportive of this action and the Chairman of SA1 was tasked to contact the chairman of SA4 to communicate this. SA1 had the opportunity to comment and did not.

TD S3-050191 contained a reply on stream bundling for MBMS from RAN2, which believes that the proposed bundling has drawbacks. Also RAN2 would like to clarify the functionalities available in the access stratum in order to allow a more accurate analysis of the advantages / disadvantages of stream bundling in SA4. It was noted (see response in S3-050299.)

TD S3-050225 contained a discussion document on Stream bundling for MBMS from Siemens in answer to the liaison statement from SA4. The document evaluates the security implications of ‘stream bundling’ for MBMS Forward Error Correction based on the received LS’s from respectively SA4: S4-050245 (S3-050195) and RAN2: R2-051199 (S3-050191). The overall conclusion that there is no security issue with the stream bundling proposal as received from the LS. Some enhancements to the SA3 specification (Section 4.2) would, however, be useful in order to describe the key management consequences:

It was suggested that S3-050225 should be sent as an attachment to a liaison statement to SA4 indicating that SA3 endorse the approach. It was provided as a draft form. There was some concern regarding the FEC and the integrity protection. If the message authentication is wrong and the FEC is applied to correct it, then the message authentication needs to be done again to ensure that FEC was correctly implemented. A revision was provided in TD S3-050299 and it was agreed to send this liaison statement.

TD S3-050250 Comments to S3-050192 (S4-050245), S4-AHP210 and S4-AHP245. It is concluded that the media security is not seriously decreased if the FEC is applied below SRTP. Hence it is proposed that SA3 sends an LS indicating this. to SA4 notifying them our view on their work described in S4-050245 [1] and S4-AHP210 [4]. It was commented that a decision has not yet been made by SA4. From the SA3 point of view, it does not matter if you FEC before SRTP or after. For integrity it is probably to FEC after, but there is not much in it. In the meantime, SA4 should be informed that there is no restriction from SA3. It was decided to add this answer to S1-050299.

TD S3-050208 was withdrawn prior to presenation.

6.21 Key Management of group keys for Voice Group Call Services

There were no specific contributions under this agenda item.

6.22 Guide to 3G security (TR 33.900)

There were no specific contributions under this agenda item.

6.23 Selective disabling of UE capabilities

There were no specific contributions under this agenda item.

6.24 Trust requirements for open platforms

Ms. Lily Chen provided a report on the Trusted Computing Group (TCG/Mobile Phone WG). TCG March Member Meeting was held March 28 to April 1 in San Diego. Mobile Phone WG held 3 sessions (two half day and one evening). The main documents TCG MPWG currently working on are:

1) Use Case Phase I, which was passed working group vote at the meeting and will be submitted to Marketing Group for editorial improvement before publishing. The Phase I Use Case includes Platform Integrity, Robust DRM Implementation, Secure Channel between UE and UICC, etc.
2) Use Case Phase II is planned to be completed the second quarter of 2005. The Phase II use case will include mobile payment, mobile ticketing, and other application use cases.
3) Requirements document will define mobile device special requirements for TPM functions. It is planned to be finished in June of 2005.

4) Specification document will define Mobile Device Platform specifications on TPM functions. The planned deadline is the end of 2005. The next TCG member meeting will be the week of June 20 in Amsterdam.

6.25 Liberty Alliance

Dr. Silke Holtmanns gave an overview of the work in the liberty alliance in TD S3-050215. It was presented for information and was noted.

TD S3-050284 contained a proposed TR on Interworking of Liberty ID-FF, ID-WSF and Generic Authentication Architecture (0.0.1). It was presented as a baseline for future work. Delegates were requested to pass comments to the author. And it was approved as a good start for pseudo CRs.

6.25 Other areas

There were no specific contributions under this agenda item.

7 Review and update of work programme

This will be formalised in the future.

8 Future meeting dates and venues

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

AP 38/06 Chairman to contact the chairman of SA2 to arrange for a joint session to allow for a better basis for the work on ALL IP and/or I-WLAN.

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#39	28 June - 1 July 2005	Montreal, Canada (possibly with SA WG2)	NAF
S3#40	13- 16 September 2005	ETSI or EF3 / TBD (possibly Slovenia co-located with TISPAN)	ETSI or EF3 / TBD
S3#41	15 - 18 November 2005	TBD	Qualcomm / TBD

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#18	28 June - 1 July 2005	Montreal, Canada	
SA3 LI-#19	12 -16 October 2005	TBD	TBD

TSGs RAN/CN/T and SA Plenary meeting schedule

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

9 Any other business

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

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

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

Annex A: List of attendees at the SA WG3#38 meeting and Voting List

A.1 List of attendees

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Hiroshi Aono	NTT DOCOMO INC.	aono@nim.yrp.nttdocomo.co.jp		+81 468 40 3809	+81 468 40 3788	JP	ARIB
Mr. George Babut	ROGERS WIRELESS INC.	gheorghe.babut@rci.rogers.com		+1 416 935 6027	+1 416 935 7502	CA	ATIS
Mr. Colin Blanchard	BT GROUP PLC	colin.blanchard@bt.com	+44 79170 24951	+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. Paul Carpenter	RESEARCH IN MOTION LIMITED	pcarpenter@rim.com	+44 7736 961131		+44 1784 477 455	CA	ETSI
Mr. Mauro Castagno	TELECOM ITALIA S.P.A.	mauro.castagno@telecomitalia.it		+39 0112285203	+39 0112287056	IT	ETSI
Ms. Lily Chen	MOTOROLA S.A.S	lchen1@email.mot.com		+1 847 632 3033	+1 847 435 2264	FR	ETSI
Mr. Takeshi Chikazawa	MITSUBISHI ELECTRIC CO.	chika@isl.melco.co.jp		+81 467 41 2181	+81 467 41 2185	JP	ARIB
Mr. Per Christoffersson	TELIASONERA AB	per.christoffersson@teliasonera.com	+46 70 5925100	+46 8 50452493		SE	ETSI
Dr. Hubert Ertl	GIESECKE & DEVRIENT GMBH	hubert.ertl@de.gi-de.com	+49 172 8691159	+49 89 4119 2796	+49 89 4119 2921	DE	ETSI
Miss Sylvie Fouquet	ORANGE SA	sylvie.fouquet@francetelecom.com		+33 145 29 49 19	+33 145 29 65 19	FR	ETSI
Dr. Silke Holtmanns	NOKIA UK LTD	Silke.Holtmanns@nokia.com		+358 50 4868571	+358 718036139	GB	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@siemens.com		+49 8963 641494	+49 8963 648000	DE	ETSI
Mr. Peter Howard	VODAFONE GROUP PLC	peter.howard@vodafone.com	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB	ETSI
Mr. Bradley Kenyon	HEWLETT-PACKARD	brad.kenyon@hp.com		+1 402 384 7265	+1 402 384 7030	FR	ETSI
Ms. Tiina Koskinen	NOKIA TELECOMMUNICATIONS INC.	tiina.s.koskinen@nokia.com		+358504821347	+358718075300	US	ATIS
Mr. Bernd Lamparter	NEC TECHNOLOGIES (UK) LTD	bernd.lamparter@netlab.nec.de		+49 6221 905 11 50	+49 6221 905 11 55	GB	ETSI
Mr. Alex Leadbeater	BT GROUP PLC	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. Vesa Lehtovirta	ERICSSON INC.	vesa.lehtovirta@ericsson.com		+358405093314	+	US	ATIS
Mr. Marcel Mampaey	ALCATEL S.A.	marcel.mampaey@alcatel.be		+32 32 40 98 03	+32 32 40 99 32	FR	ETSI
Dr. Valtteri Niemi	NOKIA CORPORATION	valtteri.niemi@nokia.com		+358504837327	+358718036850	FI	ETSI
Mr. Karl Norrman	ERICSSON LM	karl.norrman@ericsson.com		+46 8 4044502	+46 8 4047020	SE	ETSI
Mr. Petri Nyberg	TELIASONERA AB	petri.nyberg@teliasonera.com		+358 204066824	+358 2040 0 3168	SE	ETSI
Mr. Anand Palanigounder	NORTEL NETWORKS	anand@nortel.com		+1 972 684 4772	+1 972 684 3775	US	ATIS
Miss Mireille Pauliac	GEMPLUS S.A.	mireille.pauliac@GEMPLUS.COM		+33 4 42365441	+33 4 42365792	FR	ETSI
Mr. Anand Prasad	NTT DOCOMO INC.	prasad@docomolab-euro.com		+49-89-56824112	+49-89-56824300	JP	ARIB
Mr. Rajavelsamy Rajadurai	SAMSUNG ELECTRONICS CO.	rajvel@samsung.com		+91 08 5119 7777	+91 08 5114 8855	JP	ARIB
Mr. Bengt Sahlin	NIPPON ERICSSON K.K.	Bengt.Sahlin@ericsson.com		+358 40 778 4580	+358 9 299 3401	JP	ARIB
Mr. Stefan Schroeder	T-MOBILE INTERNATIONAL AG	STEFAN.SCHROEDER@T-MOBILE.DE		+49 228 9363 3312	+49 228 9363 3309	DE	ETSI
Mr. Jacques Seif	AXALTO SA	JSeif@axalto.com		+33146007228	+33146005931	FR	ETSI
Mr. James Semple	QUALCOMM EUROPE S.A.R.L.	jsemple@qualcomm.com		+447880791303		FR	ETSI
Dr. Rajesh Talpade	TELCORDIA TECHNOLOGIES	rtalpade@telcordia.com		+1 732 699 2832	+	US	ATIS
Mr. Benno Tietz	VODAFONE D2 GMBH	benno.tietz@vodafone.com		+49 211 533 2168	+49 211 533 1649	DE	ETSI
Mr. Berthold Wilhelm	BMWI	berthold.wilhelm@regtp.de		+49 681 9330 562	+49 681 9330 725	DE	ETSI
Dr. Raziq Yaqub	TOSHIBA CORPORATION	ryaqub@tari.toshiba.com	+1-908-319-8422	+1 973 829 2103	+1-973-829-5601	JP	ARIB
Mr. Dajiang Zhang	NOKIA JAPAN CO, LTD	dajiang.zhang@nokia.com		+86-13901168924	+86-010-84210576	JP	ARIB

38 attendees

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #36, #37, and #38, the following companies are eligible to vote at SA WG3 meeting #39:

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

48 Voting Members

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050184	Draft Agenda for SA WG3 meeting #37	SA WG3 Chairman	2	Approval	None	Approved as provided.
S3-050185	Draft Report of SA WG3 meeting #36	SA WG3 Secretary	4.1	Approval	None	New version 1.0.0 provided on line from comments given.
S3-050186	Report from SA#26 plenary	SA WG3 Chairman	4.2	Information	None	Noted
S3-050187	Draft report of SA WG3 -LI Group meeting (Barcelona)	SA WG3-LI Group	4.3	Approval	196	Withdrawn; see 196
S3-050188	HTTPS connection between an UICC and a NAF	Axalto, Gemplus	6.9.4	Discussion / Decision	275	See comments in 275
S3-050189	LS on providing IMSI and IMEI to the SMLC in positioning procedures	GERAN [WG2	6.6	Action	226	See proposed response in 226
S3-050190	LS on Mobile Broadcast Services from OMA BCAST to 3GPP SA4	BAC BCAST	6.20	Information	AP 38.05	It was copied to SA3 and it was noted.
S3-050191	Reply on stream bundling for MBMS	RAN2	6.20	Action	299	See response in 299
S3-050192	Liaison statement MBMS User Service finalization	SA4	6.20	Action	300	Response in 300
S3-050193	Liaison statement on a new basis for the 3GP file format	SA4	6.20	Information	None	It was copied to SA3 and it was noted.
S3-050194	Reply to Liaison Statement on Status of OMA Mobile Broadcast Services	SA4	6.20	Information	190	It was copied to SA3 and it was noted. A reply was provided in 190
S3-050195	Liaison Statement on stream bundling for MBMS	SA4	6.20	Action	299	See 191 and 225.; Response in 299
S3-050196	Draft Meeting Report for Sophia Antipolis	LI Chairman	4.3	Approval	None	Noted
S3-050197	Clarification for the usage of the Notion of a Service in Distributed IP Networks	LI SWG	4.3	Approval	316	Revised to 316
S3-050198	Clarification to the Timing Issue	LI SWG	4.3	Approval	317	Revised to 317
S3-050199	Correction on the Use of Identities for I_WLAN lawful interception	LI SWG	4.3	Approval	Out	Agreed to be sent to SA for approval
S3-050200	Clarification Pertaining to the Filtering of SDP for IRI Only Cases	LI SWG	4.3	Approval	Out	Agreed to be sent to SA for approval
S3-050201	CR 33.107 IMS Correclation	LI SWG	4.3	Approval	Out	Agreed to be sent to SA for approval
S3-050202	Correction on IMS Correlation	LI SWG	4.3	Approval	Out	Agreed to be sent to SA for approval
S3-050203	CR 33.108 IMS Correlation	LI SWG	4.3	Approval	None	Rejected; section 7.3 should be in an informative annex.
S3-050204	WI on Lawful Interception in the 3GPP Rel-7 architecture	LI SWG	4.3	Approval	315	Revised to 315
S3-050205	Inconsistency in Annex B.5	LI SWG	4.3	Approval	Out	Agreed to be sent to SA for approval
S3-050206	Inconsistency in Annex B.5	LI SWG	4.3	Approval	Out	Agreed to be sent to SA for approval
S3-050207	Obsolete Import Statement in Annex B.6	LI SWG	4.3	Approval	Out	Agreed to be sent to SA for approval
S3-050208	Comments to 33.246 with changes marked from Siemens	Siemens	6.20	Approval	None	Withdrawn since comments are included in 272
S3-050209	Open issues with applying TS 33.222 to https on the UICC	Siemens	6.9.4	Discussion / Decision	None	Noted in conjuction with the discussion on S3-050276
S3-050210	HTTPS terminated on UICC: possible impacts	Telecom Italia	6.9.4	Discussion / Decision	None	Noted in conjuction with the discussion on S3-050276
S3-050211	Feedback from joint workshop between TISPAN and 3GPP	Nokia, Gemplus	4.4	Discussion	None	Noted
S3-050212	Open issues and solution approaches to applications other than MBMS using Ks_int_NAF	Nokia	6.9.4	Discussion / Decision	None	Noted in conjuction with the discussion on S3-050276
S3-050213	Access Security Review TR v 0.0.1	Ericsson	6.6	Discussion	221	Noted as the status of the TR into the meeting and out of last meeting. See comments in 221
S3-050214	Progress of Access Security Review	Ericsson	6.6	Approval	None	It was agreed to be included in the next version of the TR

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050215	Update on Liberty Alliance Activities	Nokia	6.25	Information	None	Noted
S3-050216	Comments on S3-050209 - Open issues with applying TS 33.222 to https on the UICC	Axalto, Gemplus	6.9.4	Discussion / Decision	None	Noted in conjuction with the discussion on S3-050276
S3-050217	Comments on S3-050212 - Open issues and solution approaches to applications other than MBMS using Ks_int_NAF	Axalto, Gemplus	6.9.4	Discussion / Decision	None	Noted in conjuction with the discussion on S3-050276
S3-050218	Comments on S3-050210 - HTTPS terminated on UICC: possible impacts	Axalto, Gemplus	6.9.4	Discussion / Decision	None	Noted in conjuction with the discussion on S3-050276
S3-050219	CR to 33.222 rel-6: HTTPS connection between a UICC and a NAF	Axalto, Gemplus	6.9.4	Approval	None	Noted in conjuction with the discussion on S3-050276
S3-050220	HTTPS connection between a UICC and a NAF: impacts on CT groups	Axalto, Gemplus	6.9.4	Discussion / Decision	None	Noted in conjuction with the discussion on S3-050276
S3-050221	Comments on S3-050213: Access Security Review TR v 0.0.1	Siemens	6.6	Discussion / Decision	None	Noted, comments to be included in new version of TR
S3-050222	Feature dependencies evaluation	Siemens	6.6	Discussion / Decision	None	It was agreed to be included in the next version of the TR but the priorities are left open for the moment.
S3-050223	CR to 33.246: Clarification on CSB ID and SP payload use	Siemens	6.20	Approval	297	Revised to 297
S3-050224	CR to 33.246: Using MTK within an RTP session and relation to FEC streams	Siemens	6.20	Approval	298	To be merged with 261.
S3-050225	Stream bundling for MBMS	Siemens	6.20	Discussion / Decision	299	To be attached to response in 299
S3-050226	Sending Mobile Identity to SMLC	Nortel Networks	6.6	Discussion / Decision	309	See revision of LS in 309
S3-050227	Reply LS to ITU on general security policy	ZTE Corporation	5.8	Discussion / Decision	285	Same as 231.; Revised to 285
S3-050228	Gateway: Evaluation of ‘Fallback to unprotected mode’-parameter.	Siemens	6.2		None	The conclusion was agreed
S3-050229	Progress and information on UEA2 and UIA2 development	ETSI SAGE	5.3	Information	AP 38.01 & 02	Same as 233. See AP 38.01 and 38.02
S3-050230	Solution for (U)SIM Security Ruse by Peripheral on Wireless Local Interface	Toshiba, Telcordia	6.15	Discussion	None	Noted, search function is rejected, but whatever is left should be brought to next meeting as CRs
S3-050231	Proposed Reply LS on General Security Policy for Secure Mobile End-to-End Data Communication	ZTE Corporation	5.8	Discussion / Decision	None	Same as 227. Withdrawn
S3-050232	cooperation related to IMS security extensions for fixed broadband access	ETSI TISPAN WG7	6.1.1	Action	303	Response in 303
S3-050233	Progress and information on UEA2 and UIA2 development	ETSI SAGE	5.3	Information	None	Same as 229; noted
S3-050234	GBA User Security Settings (GUSS) transfer optimisation	Nokia, Siemens	6.9.2	Discussion / Decision	None	Noted; See CR in 235.
S3-050235	CR to 33.220 on GBA User Security Settings (GUSS) transfer optimisation	Nokia, Siemens	6.9.2	Approval	286	Revised to 286
S3-050236	Cover sheet to draft LS to GSMA SG on recommendations resulting from a review of recently published papers on GSM and UMTS security	Vodafone, Siemens	6.5	Discussion / Decision	306	Revised to 306
S3-050237	Comments on use of 401 Unauthorized and 399 Warning in Early IMS	Siemens	6.1.2	Discussion / Decision	238	Noted; see CR in 238
S3-050238	CR to 33.978 on Correction of use of 401 Unauthorized and 399 Warning headers	Siemens	6.1.2	Approval	305	Revised to 305
S3-050239	Scalability of IMS/TLS server certificate deployment	Ericsson	6.1.1	Discussion	None	Further comments are invited to the author
S3-050240	Draft contribution for ITU-R WP8F on current 3GPP activities toward IP applications over mobile systems	Telecomitalia	5.8	Discussion / Decision	None	SA3 indicated that there is sufficient information already in annex 2. It was noted.
S3-050241	A proposal to improve efficiency in setting up UE-initiated tunnels (Scenario 3) in WLAN interworking	Motorola Inc.	6.10	Discussion / Decision	None	Noted; some concerns and some checking needs to be done.

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050242	Proposal for SA3 working assumptions on IMS security extensions	Ericsson	6.1.1	Discussion / Decision	304	This document was noted in light of the revision of the WI in S3-050304.
S3-050243	Analysis of GBA based IMS signalling protection proposals	Ericsson	6.1.1	Discussion / Decision	304	This document was noted in light of the revision of the WI in S3-050304.
S3-050244	Nokia comments on Ericsson contributions: "Analysis of GBA based IMS signalling protection proposals" (S3-050243) and to "Proposal for SA3 working assumptions on IMS security extensions" (S3-050242)	Nokia	6.1.1	Discussion / Decision	304	This document was noted in light of the revision of the WI in S3-050304.
S3-050245	CR to 33.102 on Keystatus sent by CN node in Security Mode Command (Rel-5)	Ericsson	6.5	Approval	307	Revised to 307
S3-050246	CR to 33.102 on Keystatus sent by CN node in Security Mode Command (Rel-6)	Ericsson	6.5	Approval	None	With the decision to send this to RAN3 and CT1, this document was noted
S3-050247	Discussion document on Usage of USS	Ericsson	6.9.2	Discussion / Decision	248, 254, 281	Noted; See CR in 248 and comments in 254 and 281
S3-050248	CR to 33.220 on Specifying USS per GAA application (or Usage of USS)	Ericsson	6.9.2	Action	288	Revised to 288
S3-050249	Comments on Usage of USS in S3-050247	Siemens	6.9.2	Discussion / Decision	281	Revised to 281
S3-050250	Comments to S4-50245, S4-AHP210 and S4-AHP245	Ericsson	6.20	Discussion / Decision	299	Makes no difference to SA3; see 299
S3-050251	Globally unique MSKs and MKIs	Ericsson	6.20	Discussion / Decision	252	Noted, see CR in 252
S3-050252	CR to 33.246 on Clarification of MSK ID in anouncement (or Globally unique MSKs and MKIs)	Ericsson	6.20	Approval	295	Revised to 295
S3-050253	Draft LS out on on the usage of 2G SIM cards in GBA	Vodafone	6.9.1	Approval	AP 38.03	Noted, resulted in AP to rephrase the LS to ask SA1 a different question on access to 3G services with 2G SIMs
S3-050254	Commenting paper to the "Usage of USS" of Ericsson (S3-050247)	Nokia	6.9.2	Discussion / Decision	288	See the end result of offline discussion in 288
S3-050255	Comments on two IMS-related contributions (Working assumptions and WID)	Siemens	6.1.1	Discussion / Decision	304	This document was noted in light of the revision of the WI in S3-050304.
S3-050256	CR to 33.234 on Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access	NOKIA, T-mobile	6.10	Approval	310	Revised to 310
S3-050257	MSK identification in SRTP streams	Ericsson	6.20	Discussion / Decision	258	Noted, see CR in 258
S3-050258	CR to 33.246 on MKI and authentication tag length in User Service Description (SK identification in SRTP streams)	Ericsson	6.20	Approval	296	Revised to 296
S3-050259	Status of MIKEY related IETF work	Ericsson	6.20	Discussion / Decision	None	Noted
S3-050260	Usage of Key Group in MBMS security	Ericsson	6.20	Discussion / Decision	261	Noted, see CR in 261
S3-050261	CR to 33.246 on Clarification of key management overview (Usage of Key Group in MBMS security)	Ericsson	6.20	Approval	298	Revised to 298
S3-050262	Comments to HTTPS terminated on UICC: possible impacts (210)	Nokia	6.9.4	Discussion / Decision	None	Noted in conjuction with the discussion on S3-050276
S3-050263	Status of evolvement of GAA Enhancement WID	Nokia, Vodafone	6.9.1	Discussion	None	Decided to continue on the items independantly with a view to creating a WI in September
S3-050264	Terminating WLAN session by AAA server	Nokia	6.10	Discussion / Decision	265	Noted; See CR in 265

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050265	CR to 33.234 on Terminate WLAN session by AAA server	Nokia	6.10	Approval	312	Revised to 312
S3-050266	CR to 33.234 on Correction to the definition of the Wn Reference Point	Nokia	6.10	Approval	Out	Agreed to be sent to SA for approval
S3-050267	CR to 33.203 on Description of 2xx Auth_Ok message	Samsung	6.1.1	Approval	302	Revised to 302
S3-050268	CR to 33.246 on Omitted MTK Update Error Message	Nokia	6.20	Approval	292	Revised to 292
S3-050269	Consistency check: requirements->functions and mechanisms	Nokia	6.20	Discussion	291	Revised to 291
S3-050270	CR to 33.220 on Correcting figure 4.4	Ericsson	6.9.2	Approval	287	Revised to 287
S3-050271	Updated WID proposal: IMS security extensions	Ericsson, Nokia, Nortel, Huawei	6.1.1	Discussion / Decision	283	Revised to 283
S3-050272	CR to 33.246 on Editorial corrections to TS 33.246	Ericsson, Siemens	6.20	Approval	318	Agreed to be sent to SA for approval; Revised to 318
S3-050273	CR to 33.246 on Clarifications on MBMS key management	Ericsson	6.20	Approval	294	Revised to 294
S3-050274	CR to 33.246 on Use of IMPI in MBMS	Ericsson	6.20	Approval	293	Revised to 293
S3-050275	Comments to HTTPS connection between an UICC and a NAF	Nokia	6.9.4	Discussion / Decision	None	Noted: It was agreed that essentially there should be CRs for 24.109, 29.109 and 33.222
S3-050276	Open issues with applying TS 33.222 to https on the UICC	Siemens	6.9.4	Discussion / Decision	None	Noted, It was agreed to finish all the work at the next meeting in June and try to propose this as a candidate for early implementation
S3-050277	Reply LS on Control of simultaneous accesses for WLAN 3GPP IP access	SA2	6.10	Action	None	Noted; SA2 is happy with the CR in 151 that went to SA #27 and was approved.
S3-050278	Reply LS on Mandating functionality in WLAN Ans	SA2	6.10	Action	313	Response in 313
S3-050279	Reply LS on MBMS User Service finalization from SA4	SA2	6.20	Information	None	It was copied to SA3 and it was noted
S3-050280	Work Item Description for Defining Solution/Architecture for (U)SIM Security Ruse by Multiple Peripheral Devices on Wireless Local Interface to Access Multiple Networks	Toshiba, Telcordia	6.15	Information	None	Supporting document to previously submitted contribution No. S3-050230; Noted
S3-050281	Comments on Usage of USS in S3-050247	Siemens	6.9.2	Discussion / Decision	288	See the end result of offline discussion in 288
S3-050282	LS on the usage of 2G SIM cards in GBA Commented on by Vodafone	Vodafone	6.9.1	Discussion / Decision	None	Withdrawn; Same as 253
S3-050283	Updated WID proposal: IMS security extensions	Ericsson, Nokia, Nortel, Huawei	6.1.1	Discussion / Decision	304	See comments in 243,; Revised to 304
S3-050284	Interworking of Liberty ID-FF, ID-WSF and Generic Authentication Architecture TR v 0.0.1	Nokia, Siemens	6.25	Discussion / Decision	None	Approved as a good start for pseudo CRs
S3-050285	Reply LS to ITU on general security policy	ZTE Corporation	5.8	Discussion / Decision	Out	Agreed to be sent
S3-050286	CR to 33.220 on GBA User Security Settings (GUSS) transfer optimisation	Nokia, Siemens	6.9.2	Approval	Out	Agreed to be sent to SA for approval
S3-050287	CR to 33.220 on Correcting figure 4.4	Ericsson	6.9.2	Approval	Out	Agreed to be sent to SA for approval
S3-050288	CR to 33.220 on Specifying USS per GAA application (or Usage of USS)	Ericsson	6.9.2	Approval	Out	Agreed to be sent to SA for approval
S3-050289	LS to CT1 on Alignment between 33.220 and 34.109	Orange	6.9.4	Discussion / Decision	Out	; Agreed to be sent
S3-050290	CR to 33.246 to Correct parameters in the examples	Ericsson	6.20	Approval	Out	Agreed to be sent to SA for approval
S3-050291	Consistency check: requirements->functions and mechanisms	Nokia	6.20	Discussion	319	Revised to 319
S3-050292	CR to 33.246 on Omitted MTK Update Error Message	Nokia	6.20	Approval	Out	Agreed to be sent to SA for approval
S3-050293	CR to 33.246 on Use of IMPI in MBMS	Ericsson	6.20	Approval	Out	Agreed to be sent to SA for approval

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-050294	CR to 33.246 on Clarifications on MBMS key management	Ericsson	6.20	Approval	Out	Agreed to be sent to SA for approval
S3-050295	CR to 33.246 on Clarification of MSK ID in anouncement (or Globally unique MSKs and MKIs)	Ericsson	6.20	Approval	Out	Agreed to be sent to SA for approval
S3-050296	CR to 33.246 on MKI and authentication tag length in User Service Description (SK identification in SRTP streams)	Ericsson	6.20	Approval	Out	Agreed to be sent to SA for approval
S3-050297	CR to 33.246: Clarification on CSB ID and SP payload use	Siemens	6.20	Approval	Out	Agreed to be sent to SA for approval
S3-050298	CR to 33.246 on Clarification of key management overview (Usage of Key Group in MBMS security)	Ericsson	6.20	Approval	Out	Agreed to be sent to SA for approval
S3-050299	Liaison Statement on stream bundling for MBMS	SA3	6.20	Approval	Out	Agreed to be sent
S3-050300	Liaison statement MBMS User Service finalization	SA3	6.20	Approval	Out	Agreed to be sent
S3-050301	CR to 33.222 on Removal of editor's note	Nokia & Ericsson	6.9.4	Approval	Out	Agreed to be sent to SA for approval
S3-050302	CR to 33.203 on Description of 2xx Auth_Ok message	SA3 (Samsung)	6.1.1	Approval	Out	Agreed to be sent to SA for approval
S3-050303	Reply to Cooperation related to IMS security extensions for fixed broadband access	SA3	6.1.1	Action	Out	Agreed to be sent
S3-050304	Updated WID proposal: IMS security extensions	Ericsson, Nokia, Nortel, Huawei	6.1.1	Discussion / Decision	320	Revised to 320
S3-050305	CR to 33.978 on Correction of use of 401 Unauthorized and 399 Warning headers	Siemens	6.1.2	Approval	Out	Agreed to be sent to SA for approval
S3-050306	Cover sheet to draft LS to GSMA SG on recommendations resulting from a review of recently published papers on GSM and UMTS security	Vodafone, Siemens	6.5	Approval	Out	Agreed to be sent
S3-050307	CR to 33.102 on Keystatus sent by CN node in Security Mode Command (Rel-5)	Ericsson	6.5	Approval	308	Agreed in principle. To be attached to 308 and not to be sent to SA #28 for approval.
S3-050308	LS on Keystatus sent by CN node in Security Mode Command (Rel-5)	Ericsson	6.5		Out	Agreed to be sent
S3-050309	Reply LS on providing IMSI and IMEI to the SMLC in positioning procedures	Nortel Networks	6.6	Approval	Out	Agreed to be sent
S3-050310	CR to 33.234 on Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access	NOKIA, T-mobile	6.10	Approval	314	Revised to 314
S3-050311	Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages	NOKIA	6.10	Approval	313	Withdrawn: Replaced by 313
S3-050312	CR to 33.234 on Terminate WLAN session by AAA server	Nokia	6.10	Approval	Out	Agreed to be sent to SA for approval
S3-050313	Reply LS on Mandating functionality in WLAN Ans	SA3	6.10	Approval	Out	Agreed to be sent
S3-050314	CR to 33.234 on Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access	NOKIA, T-mobile	6.10	Approval	Out	Agreed to be sent to SA for approval
S3-050315	WI on Lawful Interception in the 3GPP Rel-7 architecture	LI SWG	4.3	Approval	Out	Agreed to be sent to SA for approval
S3-050316	Clarification for the usage of the Notion of a Service in Distributed IP Networks	LI SWG	4.3	Approval	Out	Agreed to be sent to SA for approval
S3-050317	Clarification to the Timing Issue	LI SWG	4.3	Approval	Out	Agreed to be sent to SA for approval
S3-050318	CR to 33.246 on Editorial corrections to TS 33.246	Ericsson, Siemens	6.20	Approval	Out	Agreed to be sent to SA for approval
S3-050319	Consistency check: requirements->functions and mechanisms	MCC	6.20	Discussion	Out	Agreed to be sent to SA for approval
S3-050320	Updated WID proposal: IMS security extensions	Ericsson, Nokia, Nortel, Huawei	6.1.1	Discussion / Decision	Out	Agreed to be sent to SA for approval

Annex C: Status of specifications under SA WG3 responsibility

Spec Number	Title	PH1-Vers	PH2-Vers	R96-vers	R97-vers	R98-vers	R99-vers	Rel4-vers	Rel5-vers	Rel6-vers	Rel7-vers
01.31	Fraud Information Gathering System (FIGS); Service requirements; Stage 0					7.0.1	8.0.0				
01.33	Lawful Interception requirements for GSM					7.0.0	8.0.0				
01.61	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements				6.0.1	7.0.0	8.0.0				
02.09	Security aspects	3.1.0	4.5.1	5.2.1	6.1.1	7.1.1	8.0.1				
02.31	Fraud Information Gathering System (FIGS); Service description; Stage 1					7.1.1					
02.32	Immediate Service Termination (IST); Service description; Stage 1					7.1.1					
02.33	Lawful Interception (LI); Stage 1					7.3.0	8.0.1				
03.20	Security-related network functions	3.3.2	4.4.1	5.2.1	6.1.0	7.2.0	8.1.0				
03.31	Fraud Information Gathering System (FIGS); Service description; Stage 2					7.0.0					
03.33	Lawful Interception; Stage 2					7.2.0	8.1.0				
03.35	Immediate Service Termination (IST); Stage 2					7.0.1					
10.20	Lawful Interception requirements for GSM			5.0.1							
21.133	3G security; Security threats and requirements						3.2.0	4.1.0			
22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification						3.2.1	4.1.0	5.0.0	6.0.0	
22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1						3.0.0	4.0.0	5.0.0	6.0.0	
22.032	Immediate Service Termination (IST); Service description; Stage 1						3.0.0	4.0.0	5.0.0	6.0.0	
23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2						3.0.0	4.0.0	5.0.0	6.0.0	
23.035	Immediate Service Termination (IST); Stage 2						3.1.0	4.1.0	5.1.0	6.0.0	
33.102	3G security; Security architecture						3.13.0	4.5.0	5.5.0	6.3.0	
33.103	3G security; Integration guidelines						3.7.0	4.2.0			
33.105	Cryptographic algorithm requirements						3.8.0	4.2.0	5.0.0	6.0.0	
33.106	Lawful interception requirements						3.1.0	4.0.0	5.1.0	6.1.0	
33.107	3G security; Lawful interception architecture and functions						3.5.0	4.3.0	5.6.0	6.4.0	
33.108	3G security; Handover interface for Lawful Interception (LI)								5.9.1	6.8.2	7.0.0

33.120	Security Objectives and Principles						3.0.0	4.0.0			
33.141	Presence service; Security									6.1.0	
33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security							4.3.0	5.1.0	6.1.0	
33.203	3G security; Access security for IP-based services								5.9.0	6.6.0	
33.210	3G security; Network Domain Security (NDS); IP network layer security								5.5.0	6.5.0	
33.220	Generic Authentication Architecture (GAA); Generic bootstrapping architecture									6.4.0	
33.221	Generic Authentication Architecture (GAA); Support for subscriber certificates									6.2.0	
33.222	Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)									6.3.0	
33.234	3G security; Wireless Local Area Network (WLAN) interworking security									6.4.0	
33.246	3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)									6.2.0	
33.310	Network domain security; Authentication framework (NDS/AF)									6.2.0	
33.810	3G Security; Network Domain Security / Authentication Framework (NDS/AF); Feasibility Study to support NDS/IP evolution									6.0.0	
33.817	Feasibility study on (Universal) Subscriber Interface Module (U)SIM security reuse by peripheral devices on local interfaces									6.1.0	
33.900	Guide to 3G security								0.4.1		
33.901	Criteria for cryptographic Algorithm design process						3.0.0	4.0.0			
33.902	Formal Analysis of the 3G Authentication Protocol						3.1.0	4.0.0			
33.908	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms						3.0.0	4.0.0			
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			
33.919	Generic Authentication Architecture (GAA); System description									6.2.0	

33.941	Presence service; Security									0.6.0	
33.978	Security aspects of early IMS									6.0.0	
35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications						3.2.0	4.1.0	5.0.0	6.0.0	
35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification						3.1.2	4.0.0	5.0.0	6.0.0	
35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data						3.1.2	4.0.0	5.0.0	6.0.0	
35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data						3.1.2	4.0.0	5.0.0	6.0.0	
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	5.0.0	6.0.0	
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	5.1.0	6.0.0	
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	5.0.0	6.0.0	
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	5.0.0	6.0.0	
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	5.0.0	6.0.0	
41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0							4.0.1	5.0.0	6.0.0	
41.033	Lawful Interception requirements for GSM							4.0.1	5.0.0	6.0.0	
41.061	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements							4.0.0			

42.009	Security aspects							4.0.0			
42.033	Lawful Interception; Stage 1							4.0.0	5.0.0	6.0.0	
43.020	Security-related network functions							4.0.0	5.0.0	6.1.0	
43.033	3G security; Lawful Interception; Stage 2							4.0.0	5.0.0	6.0.0	
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	
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	
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	
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	
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	

Annex D: List of CRs to specifications under SA WG3 responsibility agreed at meeting #38

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	Doc No.	WG TD	Status	WI
33.107	052	-	Rel-6	Correction on the Use of Identities for I_WLAN lawful interception	F	6.4.0	S3-050199	S3LI05_35r1	agreed	SEC1-LI
33.107	053	-	Rel-7	CR 33.107 IMS Correclation	C	6.4.0	S3-050201	S3LI05_45r3	agreed	SEC1-LI
33.107	051	1	Rel-7	Clarification for the usage of the Notion of a Service in Distributed IP Networks	F	6.4.0	S3-050316		agreed	SEC-LI
33.108	071	-	Rel-7	Clarification Pertaining to the Filtering of SDP for IRI Only Cases	B	7.0.0	S3-050200	S3LI05_39r2	agreed	SEC1-LI
33.108	072	-	Rel-6	Correction on IMS Correlation	F	6.8.2	S3-050202	S3LI05_50r2	agreed	SEC1-LI
33.108	074	-	Rel-6	Inconsistency in Annex B.5	F	6.8.2	S3-050205	S3LI05_025r1	agreed	SEC1-LI
33.108	075	-	Rel-7	Inconsistency in Annex B.5	A	7.0.0	S3-050206	S3LI05_025r1	agreed	SEC1-LI
33.108	076	-	Rel-7	Obsolete Import Statement in Annex B.6	D	7.0.0	S3-050207	S3LI05_026r1	agreed	SEC1-LI
33.108	070	1	Rel-7	Clarification to the Timing Issue	B	7.0.0	S3-050317		agreed	SEC-LI
33.203	080	1	Rel-6	CR to 33.203 on Description of 2xx Auth_Ok message	F	6.6.0	S3-050302		agreed	IMS-ASEC
33.220	052	-	Rel-7	CR to 33.220 on GBA User Security Settings (GUSS) transfer optimisation	B	6.4.0	S3-050286		agreed	SEC1-SC
33.220	051	1	Rel-6	CR to 33.220 on Correcting figure 4.4	F	6.4.0	S3-050287		agreed	SEC1-SC
33.220	050	1	Rel-6	CR to 33.220 on Specifying USS per GAA application (or Usage of USS)	F	6.4.0	S3-050288		agreed	SEC1-SC
33.222	019	-	Rel-6	CR to 33.222 on Removal of editor's note	F	6.3.0	S3-050301		agreed	SEC1-SC
33.234	66	-	Rel-6	CR to 33.234 on Correction to the definition of the Wn Reference Point	F	6.4.0	S3-050266		agreed	WLAN
33.234	065	1	Rel-6	CR to 33.234 on Terminate WLAN session by AAA server	F	6.4.0	S3-050312		agreed	WLAN
33.234	64	2	Rel-6	CR to 33.234 on Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access	F	6.4.0	S3-050314		agreed	WLAN
33.246	066	-	Rel-6	CR to 33.246 to Correct parameters in the examples	F	6.2.0	S3-050290		agreed	MBMS
33.246	061	1	Rel-6	CR to 33.246 on Omitted MTK Update Error Message	C	6.2.0	S3-050292		agreed	MBMS
33.246	64	1	Rel-6	CR to 33.246 on Use of IMPI in MBMS	F	6.2.0	S3-050293		agreed	MBMS
33.246	063	1	Rel-6	CR to 33.246 on Clarifications on MBMS key management	C	6.2.0	S3-050294		agreed	MBMS
33.246	059	1	Rel-6	CR to 33.246 on Clarification of MSK ID in anouncement (or Globally unique MSKs and MKIs)	C	6.2.0	S3-050295		agreed	MBMS
33.246	058	1	Rel-6	CR to 33.246 on MKI and authentication tag length in User Service Description (SK identification in SRTP streams)	C	6.2.0	S3-050296		agreed	MBMS
33.246	065	-	Rel-6	CR to 33.246: Clarification on CSB ID and SP payload use	F	6.2.0	S3-050297		agreed	MBMS
33.246	060	1	Rel-6	CR to 33.246 on Clarification of key management overview (Usage of Key Group in MBMS security)	F	6.2.0	S3-050298		agreed	MBMS
33.246	062	1	Rel-6	CR to 33.246 on Editorial corrections to TS 33.246	D	6.2.0	S3-050318		agreed	MBMS
33.246	067	-	Rel-6	Consistency check: requirements->functions and mechanisms	F	6.2.0	S3-050319		agreed	MBMS
33.978	001	-	Rel-6	CR to 33.978 on Correction of use of 401 Unauthorized and 399 Warning headers	F	6.0.1	S3-050305		agreed	SEC-IMS

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	From	Source TD	Comment/Status
S3-050189	LS on providing IMSI and IMEI to the SMLC in positioning procedures	GERAN [WG2	GP-051170	See proposed response in 226
S3-050190	LS on Mobile Broadcast Services from OMA BCAST to 3GPP SA4	BAC BCAST	2005-0127R01	It was copied to SA3 and it was noted.
S3-050191	Reply on stream bundling for MBMS	RAN2	R2-051199	See response in 299
S3-050192	Liaison statement MBMS User Service finalization	SA4	S4-050141	Response in 300
S3-050193	Liaison statement on a new basis for the 3GP file format	SA4	S4-050218	It was copied to SA3 and it was noted.
S3-050194	Reply to Liaison Statement on Status of OMA Mobile Broadcast Services	SA4	S4-050237	It was copied to SA3 and it was noted. A reply was provided in 190
S3-050195	Liaison Statement on stream bundling for MBMS	SA4	S4-050245	See 191 and 225.; Response in 299
S3-050232	cooperation related to IMS security extensions for fixed broadband access	ETSI TISPAN WG7		Response in 303
S3-050233	Progress and information on UEA2 and UIA2 development	ETSI SAGE		Same as 229; noted
S3-050240	Draft contribution for ITU-R WP8F on current 3GPP activities toward IP applications over mobile systems	Telecomitalia		SA3 indicated that there is sufficient information already in annex 2. It was noted.
S3-050277	Reply LS on Control of simultaneous accesses for WLAN 3GPP IP access	SA2	S2-050941	Noted; SA2 is happy with the CR in 151 that went to SA #27 and was approved.
S3-050278	Reply LS on Mandating functionality in WLAN Ans	SA2	S2-050945	Response in 313
S3-050279	Reply LS on MBMS User Service finalization from SA4	SA2	S2-050948	It was copied to SA3 and it was noted

E.2 Liaisons from the meeting

TD number	Title	TO	CC	Date Sent
S3-050285	Reply LS to ITU on general security policy	ITU-T SG17		29/04/2005
S3-050289	LS to CT1 on Alignment between 33.220 and 34.109	CT1		27/04/2005
S3-050299	Liaison Statement on stream bundling for MBMS	SA4		29/04/2005
S3-050300	Liaison statement MBMS User Service finalization	SA4		29/04/2005
S3-050303	Reply to Cooperation related to IMS security extensions for fixed broadband access	TISPAN WG7		29/04/2005
S3-050306	Cover sheet to draft LS to GSMA SG on recommendations resulting from a review of recently published papers on GSM and UMTS security	GSMA SG		29/04/2005
S3-050308	LS on Keystatus sent by CN node in Security Mode Command (Rel-5)	RAN3, CT1	RAN2	29/04/2005
S3-050309	Reply LS on providing IMSI and IMEI to the SMLC in positioning procedures	GERAN WG2		29/04/2005
S3-050313	Reply LS on Mandating functionality in WLAN Ans	SA2		29/04/2005

Annex F: Actions from the meeting

AP 37/01: Chairman to ask the Specifications Manager for the best way to handle the UE2 / UIA2 work in the specifications set (numbering etc.)
It was not certain what was intended with this action. It was assumed that a similar set of TSs for the Kasumi based solution. There is a problem with the names F8 and F9, but these are generic names for the algorithm and UEA1 and UIA1 are the specific names for the Kasumi algorithms. Hence the names of the existing TSs will need to be changed. A proposal for a solution to the naming issue will be provided by Telia Sonera. This action remains open for the time being.

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

AP 38/01: Per Christoffersson to ask SAGE for a budget estimate for the evaluation of the algorithms, and an outline proposal on how it would be done..

AP 38/02: Once this is done, then funding, if required, chairman to organise some arrangements so that evaluation can be organised.

AP 38/03: S. Holtmanns to draft an liaison statement to SA1 indicating why 2-GBA may be advantageous to SA1 and ask SA1 if this is required.

AP 38/04 Mauro to build on TD S3-050210 to remove the inconsistencies in 33.222 over an email discussion.

AP 38/05 Ericsson to provide some company contribution input to the the delegates from their company as briefing for the informal workshop on Mobile Broadcast Service Standardization. This should be sent out on the email list by 8th May for comments. Deadline for comments to be 15th May.

AP 38/06: Chairman and Secretary to agree arrangements with TISPAN for co-locating a meeting with TISPAN on the 12-16th September in Slovenia and organise hosting.