3GPP TSG SA WG3 (Security) meeting #29 **Report v1.0.0**

15-18 July 2003

San Francisco, USA

Source:	**Secretary SA WG3 (Maurice Pope)**
Title:	**Report of SA WG3 meeting #29. Version 1.0.0**
Status:	**Approved at SA WG3 meeting #30**

Cable Car in San Francisco

Contents

1 Opening of the meeting

The Vice Chairman, V. Niemi, opened the meeting and welcomed delegates on behalf of the hosts "*3GPP2*".

2 Agreement of the agenda and meeting objectives

TD S3-030310 Draft Agenda for SA WG3 meeting #29. The draft agenda was reviewed.

Priorities for this meeting:

Priority 1: It was noted that the Rel-5 issues need to be fixed at this meeting and is the top priority for this meeting. Therefore agenda Item 7.1 will be dealt with first, followed by other Rel-5 CRs and the other items under agenda item 7.x, in reverse order (7.21, 7.20, ...). It was also recognised that the handling of MBMS would be useful before the joint session with 3GPP2 on these issues. Presence was also recognised as an important issue to resolve.

Priority 2 : To process Rel-6 specifications for delivery to TSG SA.

The draft agenda was then approved with agreed changes, as reflected in the numbering of this report.

2.1 3GPP IPR Declaration

The chairman made the following call for IPRs, and asked ETSI members to check the latest version of ETSI's policy available on the web server:

> The attention of the members of this Technical Specification Group is 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 members take note that they are hereby invited:
>
> - to investigate in their company whether their company does own IPRs which are, or are likely to become Essential in respect of the work of the Technical Specification Group.
> - to notify the Director-General, or the Chairman of their **respective** Organizational Partners, of all potential IPRs that their company may own, by means of the IPR Statement and the Licensing declaration forms (e.g. see the ETSI IPR forms http://webapp.etsi.org/Ipr/).

3 Assignment of input documents

The available documents were assigned to their respective agenda items.

4 Meeting reports

4.1 Approval of the report of SA3#28, Berlin, Germany, 6-9 May, 2003

TD S3-030311 Draft Report of SA WG3 meeting #28 v0.0.6.

It was confirmed that the deadline for contributions to SA WG3 meetings is 17.00 CET, 1 week (7 days) before the start date of the meeting. For Ad-hoc meetings, the deadline was confirmed as 17.00 CET, 2 working days before the start of the meeting.

Action Points from the meeting:

AP 28/01: T. Viitanen to lead an e-mail discussion on Openness of Rel-6 IMS Network. Completed. Related contributions after e-mail discussion were provided to this meeting.

AP 28/02: B. Owen to lead an e-mail discussion on SA set-up procedure in Rel-5. Completed.

AP 28/03: SA set-up procedure in Rel-5 problem to be reported to TSG SA by SA WG3 Chairman. Completed.

AP 28/04: B. Sahlin to lead e-mail discussion based on TD S3-030243 on impacts of SIGTRAN on TS 33.210 for input to SA WG3 meeting #29. Completed. Little activity in the discussion and work still to be done in the IETF. This may be revisited in later meetings if necessary.

AP 28/05: *A. Escott to lead e-mail discussion on "potential Man-In-The-Middle threat providing IMEISV in clear", related to TD S3-030225, for contribution to SA WG3 meeting #29.* Completed. **To be continued during the discussion of LSs at this meeting**.

AP 28/06: *SSH to provide suggestions for profiling CMPv2 for 3GPP use and provide contributions on this at the next SA WG3 meeting.* Completed. Related contribution in TD S3-030347.

AP 28/07: *A. Van Moffaert to lead an e-mail discussion on structure and scope of the draft TS on bootstrapping of application security.* Completed.

AP 28/08: *D. Mariblanca to lead an e-mail discussion on Implications of the trust relation between the Cellular Operator and the WLAN Access Provider based on TD S3-030261 for conclusion at the next meeting.* Completed. Contribution summarising the discussion conclusions provided to e-mail list and several contributions were provided to this meeting.

AP 28/09: *M. Wivfesson to lead an e-mail discussion based on SA WG2 and SA WG4 responses to MBMS and DRM issues based on TD S3-030293 to create a new proposed LS to these groups.* Not complete. It was considered premature to provide the LS off-line and this will be reconsidered during this meeting. It was later considered too soon to send this LS and so the Action was withdrawn.

AP 28/xx: *(un-numbered, under TD S3-030238): T. Viitanen agreed to create the draft LS by 16 May, comments by 23 May and approval by 30 May 2003. (a document number will be given when the document is approved).* Completed, but no consensus on the content of an LS over e-mail. This will be continued at this meeting. T. Viitanen provided a draft of the LS developed during the discussions in TD S3-030437.

It was agreed that P. Howard would take over the rapporteurship for T. Wrights' documents, P. Christoffersson the algorithm specifications, and V. Niemi the remaining specifications where M. Walker is listed as Rapporteur. Delegates were asked to check other Rapporteurs of SA WG3 documents in order to update the list to Active participants to the meeting (preferable based on the same company replacing old Rapporteurs).

Some minor modifications were made to the attendees list in the report, which was then approved and will be placed on the 3GPP FTP server as version 1.0.0.

4.2 Report from SA#20, Hämeenlinna, Finland, 9-12 June, 2003

TD S3-030331 Report from SA#20 plenary. This was introduced by the SA WG3 Chairman and provided information on decisions and advice made at the previous TSG SA Plenary. Delegates were asked to take note of the advice given in respect to working procedures and CR preparation and e-mail approval. The report was then noted.

4.3 SA WG3 LI Issues

TD S3-030353 DRAFT Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #2/03 on lawful interception. The draft report of the Vienna meeting of the LI Group was introduced by B. Wilhelm. The report was provided for information and was noted. The possibility of a co-located meeting in November with the LI group was still under investigation and it may be possible to locate SA WG3 in a nearby hotel to the DTI in London, UK. **C. Brookson undertook to look into the possibilities of this**.

TD S3-030352 SA WG3 LI Group CRs Approved by e-mail. This was provided for information, as the attached CRs had already been approved by SA WG3 over e-mail. The document was then noted.

TD S3-030394 Proposed CR to 33.108: Reference errors in Annex G (Rel-5) and TD S3-030395 Proposed CR to 33.108: Reference errors in Annex G (Rel-6). This CR were provided directly to SA WG3 as the errors were noted after the LI Group meeting. The LI Group were consulted and happy for these CRs to go to SA WG3. The CRs were then approved.

5 Reports and liaisons from other groups

5.1 3GPP working groups

The LSs from other groups were handled under agenda items relevant to their topics.

5.2 IETF

TD S3-030370 HTTP Digest AKAv2 status and SQN issues. This was introduced by Ericsson and reported the progress of HTTP Digest AKAv2 in the IETF. It was clarified that the draft had been submitted to the IETF already. The IETF draft was attached and was briefly reviewed. Ericsson reported that there was good confidence for the Expert review to be done and for completion of the draft by the end of 2003. It was clarified that this should not need any related changes to the 3GPP IMS specifications. It was noted that the use of both AKA versions may lead to a contradiction between 3GPP and IETF implementation of the HTTP Digest AKA. **It was agreed that the content of section 5.1 in the draft and the impact on 3GPP specifications and implementations should be studied in depth.**

5.3 ETSI SAGE

TD S3-030389 Proposed CR to 55.216: Clarification on the usage of the Key length (Rel-6). This was introduced by Siemens and proposed to remove the unnecessary KLEN flexibility in the Algorithms. It was questioned whether this change should be done before the proposed Delta specifications for A5/4 and GEA4 were provided. The principle of creating a "Delta Specification" for A5/4 and GEA4, referencing A5/3 and GEA3 specification with the changes for the 128 bit key lengths was discussed. It was agreed as a working assumption that the A5/4 and GEA4 specification will be produced as a new TS. The CR was then updated slightly in TD S3-030438 and approved.

AP 29/01: M Pope to get a new TS number for use to provide the draft A5/4 and GEA4 document.

5.4 GSMA SG

Mr. C. Brookson provided a verbal report of activities within the GSM Association Security Group:

IMEI issues were still an important work item, as countries and the EU are looking at ways of making them more secure. The GSM Association supports the central identity register and the process.

There were still various issues to address, and further work was required on the over billing attack. This would be presented at the next SA WG3 meeting, and contributions are still welcome from SA WG3 Members.

Some recent work had been taking place on the security of algorithms and supporting protocols. This may result in some change requests being submitted to SA WG3 in the near future.

The next meeting of GSMA SG will be 22-23 September 2003 in Warsaw.

5.5 3GPP2

A joint session had been arranged between 3GPP SA WG3 and 3GPP2 S4 (Security Group) for the afternoon of 16 July (see Agenda Item 6).

5.6 TIA TR-45

There were no specific contributions under this agenda item.

5.7 OMA

TD S3-030338 Extract of OMA Discussion Part of TSG SA #20 Draft Report (v.0.0.4). This was introduced by the SA WG3 Chairman and provided the agreements from the discussions at TSG SA#20 following the discussions on the OMA work. It was noted that 3GPP is not a legal entity and it's work is released for use by the Standards Organisations, whereas the OMA is a legal entity and takes responsibility for the IPR and Liability of its' work. It was considered that this issue should be discussed at the TSG SA level. The document was then noted.

TD S3-030339 Cover Note to “3GPP Dependencies on OMA Deliverables”. This was introduced by the SA WG3 Chairman and asked SA WG3 to review the dependencies list and provide comments back to I. Sharp. It was commented that OSA Security dependencies did not appear on the list, whereas it was on the list sent to TSG SA. A response LS was provided in TD S3-030439 which was approved.

TD S3-030435 LS from OMA: Mobile PKI service enabler. This was introduced by Gemplus. The level of approval status of this LS was not known, and so it was taken for information only at this time. It reported that the OMA SEC group has released a complete set of specifications to enable mobile PKI based services and applications covering:

1. Mobile device security element
2. Security element bootstrapping
3. User enrolment mechanisms
4. Certificate profile
5. CRL profile and OCSP mobile profile
6. End-to-end transport layer security
7. Application layer digital signature

OMA SEC proposed that 3GPP, 3GPP2 and OMA collaborate to progress this work item. As an initial step, OMA SEC proposed that progress reports and development plans are shared in order to identify areas of potential overlap and/or reuse. OMA SEC would also appreciate if 3GPP SA WG3 can elaborate on their current plans to address topics (1), (5), (6) and (7). These issues were covered by the LS in TD S3-030459 (see agenda item 7.9).

5.8 Other groups

There were no specific contributions under this agenda item.

6 Joint session with 3GPP2 TSG-S WG4 (security) group (probably on Wednesday 16th)

The meeting was opened by V. Niemi, 3GPP SA WG3 Chairman and delegates introduced themselves. M. Marcovici, 3GPP2 S4 Chairman welcomed delegates to the joint session.

TD S3-030450 Slides for joint Meeting 3GPP / 3GPP2. This was prepared and presented by M Marcovici, Chairman of 3GPP2 S4. The following topics were introduced, providing an overview of the status of work in 3GPP2 for the following documents:

-	**WLAN-3GPP2 Interworking**	**3GPP2 S.P0087 (Draft)**
-	**Broadcast/Multicast**	**3GPP2 S.P0083 Broadcast-Multicast Service Security Framework**
-	**IMS Security Framework**	**3GPP2 S.P0086**
-	**AKA in 3GPP2**	**3GPP2 X.P0006**
-	**Security Algorithm**	**3GPP2 S.S0053, S.S0054, S.S0055 and S.S0078**

There were some questions and clarifications after the presentation and the 3GPP2 S4 Chairman was thanked for his presentation, which was noted.

6.1 3GPP2 IMS security framework

TD S3-030452 3GPP2 S.P0083 v0.6: Broadcast-Multicast Service Security Framework. This was provided for information and was noted (without presentation).

6.2 WLAN interworking - security framework

TD S3-030410 Loose Coupling Interworking Issues. this was presented by S. McCann, Siemens. It was clarified that "loose coupling" referred to Scenario 2 of the 3GPP WLAN interworking scenarios. It was reported that IEEE 802.11 will possibly produce an interworking Recommended Practice (RP) and any thoughts, comments and technical input on this would be welcomed by IEEE 802.11 WGs. It was mentioned that there exists a practice for accounting records between roaming partners, which may be of use to IEEE 802.11. The presentation was then noted.

6.3 BCMCS security framework

TD S3-030356 MBMS Security Framework. This was presented by Qualcomm Europe and was noted.

TD S3-030451 Presentation Slides: BCMCS Security Framework. This was presented by Qualcomm and was presented for information to the joint session. The security goal is (dissuasion) to make it infeasible for re-distribution of keys by unauthorised users rather than prevention, such that it is too costly or too slow (e.g. for time critical applications) to be worthwhile. It was noted that there was a proposal for a scheme and security requirements for 3GPP MBMS in TD S3-030335, which was fairly similar to this 3GPP2 scheme. The presentation was discussed for clarification and noted.

6.4 Proposed use of UAK in 3GPP2

There were no specific contributions under this agenda item.

6.5 3GPP2 Network security – use of TLS or IPsec

There were no specific contributions under this agenda item.

7 Work areas

7.1 IP multimedia subsystem (IMS)

TD S3-030319 Response LS from T WG3: Re: LS on clarification of USIM-based access to IMS. This was introduced by the T WG3 Chairman (N. Barnes, Motorola) and was provided to SA WG3 for information. The LS was noted.

TD S3-030323 LS (from CN WG1) on transport of unknown SIP signalling elements. This was introduced by Nokia and asked SA WG3 to take the transport of "unknown" SIP signalling elements into consideration in their work and to provide a reply if any problems were foreseen from the security point of view. There was a potential problem with the firewall filtering of undefined messages to protect NEs in 3GPP Networks. It was explained that the firewalls should know which messages to pass and the equivalent application to both known and unknown SIP messages should allow transparent passing of the SIP messages and the S-CSCF is responsible for applying filtering on SIP messages that it receives.

It was decided that a LS should be produced to clarify the correct understanding of SA WG3, indicating that firewalls should still need to be put in place in the Network. The LS was provided in TD S3-030440 which was reviewed and revised in TD S3-030466 which was revised in TD S3-030470 and approved.

TD S3-030330 LS (from CN WG1) on Security Association Lifetimes. This was introduced by "3" and asked SA WG3 to modify 33.203 to align with the agreements in CN WG1 on SA Lifetimes. A related LS was provided from TSG CN in TD S3-030336 which was also introduced by "3" and provided some questions about the mechanisms for SA Lifetimes. A discussion contribution and proposed response to this was provided by "3", Ericsson and Lucent in TD S3-030399 which was introduced by "3" and discussed. The related CR was considered and it was decided to have an evening drafting meeting to get agreement on the text in order to have a clear response to CN WG1. A drafting session was held and the attached LS was revised in TD S3-030441 which was approved. The attached CR was revised in TD S3-030442 which was approved and attached to the LS.

TD S3-030429 LS from SA WG2: Response to LS on clarification of USIM-based access to IMS. This was introduced by Ericsson and asks SA WG3 to clarify their IMS specification on Release 1999 and Rel-4 USIM application, i.e. "Use of a USIM application on a UICC **without ISIM**". It was reported that this is already clarified in the specification after the highlighted change. A response LS to SA WG2 was provided in TD S3-030443 which was revised in TD S3-030467 and approved.

TD S3-030431 Liaison (from SA WG2) on SIP signalling interworking. This was introduced by Siemens and reported that SA WG2 had agreed to adopt the "end-to-end modified flow as the basis for SIP interworking" and asked SA WG3 to update their specifications as necessary when this has been completed in SA WG2. The LS was noted and the specifications will be updated when TS 23.228 has been updated by SA WG2.

TD S3-030432 LS (from SA WG2) on Security Implications of Gq interface. This was introduced by Ericsson and asked SA WG3 to consider the security implications of a new Gq interface and to provide information on Security mechanisms to be used to protect this interface. **Delegates were asked to consider the draft TR 23.917 attached to the LS and to provide contributions for the next SA WG3 meeting**. A response LS to report that the NDS mechanisms would be considered for use by SA WG3 was provided in TD S3-030444 which was approved.

Release 5 Issues:

TD S3-030415 Discussion paper on solutions regarding the behaviour of SIP over TCP and SA handling in re-authentications. This was introduced by Siemens and discussed the reasons for the proposed CRs in TD S3-030416 and TD S3-030418 following some e-mail discussion on this topic. It was clarified that only TCP and UDP protocols had been analysed and the use for other protocols would need further study.

TD S3-030416 Proposed CR to 33.203: Alignment of security association handling and behaviour of SIP over TCP (Rel-5).
(Note: The cover page had the wrong Release indicated and the proposed CR was intended for Rel-5).
This was introduced by Siemens and considered with TD S3-030421. The principles of this CR were agreed and were included in the updated CRs in TD S3-030445 and TD S3-030461 (see below).

TD S3-030421 Proposed CR to 33.203: Annex H in 33.203 (Rel-5).
(Note: The cover page had the wrong Release indicated and the proposed CR was intended for Rel-5 and that although this was technically a late document, this had been due to a change in the e-mail address of the sender and the distribution had been rejected by the e-mail list server).
This was introduced by Ericsson. There was some objection against the specification of additional parameters which would not be in line with the IETF sip-sec-agree draft and would introduce a lot of changes at stage 3. It was clarified that this would provide an extension to the IETF draft for 3GPP use and that CN WG1 colleagues considered this approach better in terms of Protocol design. It was also argued that an alternative solution based on the request for consecutive SPIs numbers (Ports) would also be an extension to the principles of the IETF draft. The principles of this CR were agreed and were included in the updated CRs in TD S3-030445 and TD S3-030461 (see below).

TD S3-030461 Proposed CR to 33.203: Security association handling, behaviour of SIP over TCP and re-authentication (Rel-5). This was produced by re-drafting TD S3-030416 and TD S3-030421 in a drafting group. The CR was reviewed and approved.

> **Members were asked to inform their CN WG1 delegates that the statement "all pending transactions are timed out" in the CR (S3-030461) does not aim to introduce a new timer. Rather, it is up to CN WG1 to implement the statement based on their knowledge of SIP.**

TD S3-030445 Proposed CR to 33.203: Annex H in 33.203 (Rel-5). This was produced by re-drafting TD S3-030416 and TD S3-030421 in a drafting group. This CR was approved.

TD S3-030417 Delta Changes to TS 33.203 on Security Association Handling in Re-authentications. This was introduced by Siemens and provided a proposal for implementing the problem identified by Lucent at SA WG3 meeting #28 (TD S3-030258) of not changing the server port, as this would result in a lot of extra signalling overhead. The solution to fix the server port and change the client port was agreed in principle, but that the handling of old SA use should be further studied off-line. This was covered under the CR in TD S3-030461.

TD S3-030418 Proposed CR to 33.203: Security association handling, behaviour of SIP over TCP and re-authentication (Rel-6). This was covered under the CR in TD S3-030461.

Release 6 Issues:

TD S3-030376 Make a split between TS33.203 and Presence. This was introduced by Ericsson and proposed that:

1) SA WG3 define a new TS for Presence and require a number from MCC and initiate the work to move relevant parts from the TR to this new TS;

2) SA WG3 endorses the working principle that future services on top of IMS are candidates for creating an individual TS rather than updating the TS33.203 for each new application;

3) that parts of the current Presence TR are moved into this TS and parts moved to TS33.203. CRs are brought to this meeting (TD S3-030377 and TD S3-030378).

It was agreed that the principle to produce a new TS for Presence using the service parts of the draft TR. Ericsson offered to be Rapporteur for this new TS.

TD S3-030377 Proposed CR to 33.203: Introducing the Privacy mechanism (Rel-6). This was provided by Ericsson. Ericsson reported that this CR was in line with current CN WG1 work, although there are some editors notes where items are left for further study in SA WG3 which CN WG1 also need to study. **It was decided that this CR should be sent to CN WG1 and SA WG2, cc: SA WG1**. A LS was drafted for this in TD S3-030454 which was reviewed and updated in TD S3-030468 which was approved.

TD S3-030378 Proposed CR to 33.203: Introducing Confidentiality Protection for IMS (Rel-6). This was provided by Ericsson. (This CR, if approved at TSG SA, will produce the Rel-6 version of TS 33.203). It was proposed to wait for further Rel-5 CRs to be dealt with and to re-draft this CR if necessary, taking the changes into account for consistency of the Rel-6 text after Rel-5 changes are made. A replacement CR was provided in TD S3-030455 which was approved.

TD S3-030374 Key Expansion function for IMS/Presence. This was introduced by Ericsson and proposes using triple-DES Key Expansion and include this in TS 33.203 (Rel-6) (a CR was provided for this in TD S3-030375). The proposal was agreed.

TD S3-030375 Proposed CR to 33.203: Introducing Cipher key Expansion for IMS (Rel-6). This was provided by Ericsson. (This CR, if approved at TSG SA, will produce the Rel-6 version of TS 33.203). This CR was approved.

TD S3-030372 Profiling of RFC3325. This was introduced by Ericsson and discusses the principles to be adopted for Trust Domain security management. Ericsson reported that this was intended to be an informative annex to provide important information. It was also noted that the whole text was new, and this should be shown in the final CR. It was agreed that this discussion paper and the related CR in TD S3-030373 should be added to the LS in TD S3-030454.

TD S3-030373 Proposed CR to 33.203: Trust Domain and the definition of SPEC(T) (Rel-6). This was provided by Ericsson. (This CR, if approved at TSG SA, will produce the Rel-6 version of TS 33.203). This was updated in TD S3-030456 to show all changes and added to the LS in TD S3-030453. The CR was not approved at this time, but will be re-considered after comments are received from the addressed groups.

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

There were no specific contributions under this agenda item.

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

TD S3-030350 Proposed CR to 33.210: Change of IKE profiling (Rel-5). This was provided by T-Mobile and Siemens. This CR was approved.

TD S3-030354 Proposed CR to 33.210: Change of IKE profiling (Rel-6). It was noted that the category should be "A". This CR was approved as Category "A".

TD S3-030404 Proposed CR to 33.210: Update draft-ietf-ipsec-sctp-03.txt reference to new standard RFC: RFC3554 (Rel-5). It was noted that this type of change may not be accepted for Rel-5, as TSG SA Plenary only accepts changes that are system impact for Rel-5. However, this CR was approved.

TD S3-030405 Proposed CR to 33.210: Update draft-ietf-ipsec-sctp-03.txt reference to new standard RFC: RFC3554 (Rel-6). This CR was approved.

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

Due to lack of time, it was decided to do e-mail approval for the Pseudo-CRs contained in TDs S3-030380, S3-030381, S3-030384, S3-030385, S3-030386, S3-030387 and S3-030388.

TD S3-030379 NDS/AF – Fetching Cross-Certificates. Noted.

7.5 UTRAN network access security

TD S3-030312 LS (from SA WG2) on unciphered IMEISV transfer. This was introduced by the SA WG3 Chairman. SA WG2 asked SA WG3 to note their response to questions and make necessary changes to Release 1999 TS 33.102 to align with CN WG1 specifications. The reply LS in TD S3-030321 was considered (see below) and the resulting CRs for e-mail discussion

TD S3-030321 Reply LS (from CN WG1) on unciphered IMEISV transfer. This was introduced by Siemens and informed SA WG3 that CN WG1 had checked TS 24.008 and confirmed that there are no timing restrictions for MSC/VLR, SGSN or UE on the handling of an IMEISV request. It was recognised that this would need to be handled over an e-mail discussion in order to have necessary CRs available for the September 2003 TSG Plenary, otherwise it could only be available for December 2003. It was agreed to try to do this by e-mail Comments by 29 August, Approval by 5 September 2003.

AP 29/02: M Blommaert and P Howard to chair e-mail discussions on Early release IMEISV transfer and produce CRs for comment by 29 August, Approval 5 September 2003.

7.6 GERAN network access security

TD S3-030322 LS (From CN WG1 re: S3-030308) on increasing the key length for GEA3. This was introduced by the SA WG3 Chairman and asked SA WG3 to take the change of key length into account in their work. The LS was then noted.

TD S3-030361 Enhanced Security for A/Gb. This was introduced by Ericsson and proposed that SA WG3 endorses the principles outlined in the contribution as the working assumption for secure negotiation for the Gb interface and that liaison statements are sent to CN WG1 and T WG3 to study the feasibility from a Protocol point of view as well as USIM point of view. There was some discussion and some concerns raised over some of the proposals. There was some objection to sending an LS at the moment because it is not known which mechanisms and solutions will be chosen. As there were no other proposals available, it was therefore decided that the principles given in the contribution could be used as a working assumption until the next SA WG3 meeting where any alternative proposals can be discussed and a solution chosen. One alternative solution was submitted in TD S3-030463 during the meeting. As there was no time to discuss it in the meeting, **delegates were asked to study it for next meeting**.

TD S3-030390 Proposed CR to 33.102: Clarification on the usage of the c3 conversion function (Rel-6). This was introduced by Siemens and specified that the c3 function shall not be implemented in the UE. The CR was updated in TD S3-030465 which was approved.

TD S3-030402 Effects of service 27/38 on 2G/3G Interworking and emergency call. This was introduced by Siemens. It was agreed that the contribution contained valuable information and an e-mail discussion was set up to agree what should be done with the document (i.e. who it should be sent to). M. Blommaert agreed to run this e-mail discussion.

AP 29/03: M. Blommaert to run e-mail discussion to discuss what should be done with the information in TD S3-030402.

7.7 Immediate service termination (IST)

There were no specific contributions under this agenda item.

7.8 Fraud information gathering system (FIGS)

There were no specific contributions under this agenda item.

7.9 Support for subscriber certificates

TD S3-030317 Draft TS ab.cde version 0.2.0: Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description (Release 6). This was noted.

TD S3-030407 Bootstrapping and subscriber certificate use cases. This was introduced by Nokia and described several use cases for subscriber certificates enrolled using AKA and a bootstrapping procedure. The document concludes that all of the mentioned use cases are possible to support with subscriber certificates, many of them are also possible to support with bootstrapped shared keys. This would require that application server implements NAF to obtain shared keys from the BS. It was commented that the Key Generation in the terminal needs to be guaranteed to be of good quality. The contribution was then noted.

TD S3-030317 Draft TS ab.cde version 0.2.0: Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description (Release 6). This was provided by the Rapporteur (T Haukka, Nokia) for information and was noted.

TD S3-030348 Interface Naming in Bootstrapping System. This was introduced by Nokia and provided a scheme for naming of interfaces for bootstrapping systems. The interface naming was agreed and a LS to SA WG2 was provided in TD S3-030457 which was revised in TD S3-030471 and approved.

TD S3-030340 3GPP Specifications upgrading for Bootstrapping and Subscriber Certificates. This was introduced by Nokia and provided for information. It summarised the current understanding about the possible updates needed in the 3GPP specifications for implementation of the Bootstrapping and Subscriber Certificate procedures in their C and D interfaces. It proposed to include detailed procedural descriptions to corresponding interface parts of the current draft TS. It was decided to send this document to CN WG4 for their recommendation on which option to choose for inclusion of the detailed description of the interfaces. An LS to CN WG4, and CN WG1, was provided in TD S3-030458 and was revised in TD S3-030469 which was approved.

TD S3-030341 Transaction identifier location in protocol A. This was provided by Nokia and concerned an issue on how the transaction identifier (TID) is transferred from BSF to UE in protocol A. A Pseudo-CR was attached providing the message definitions. It was agreed to attach the contents of the Pseudo-CR to the LS in TD S3-030469. The document was therefore noted at this time awaiting a response from the LS.

TD S3-030411 Key provision in bootstrapping of application security. This was introduced by Siemens and proposed two improvements to the currently specified provision of the keys shared between a UE and a NAF, namely a reduced involvement of the HSS and a means for the NAF to request a key change. The changes were presented in the form of pseudo-CRs:

> **For section 1.1 of the contribution:** there was some discussion on the need for and use-cases for accepting this proposal. There was also some support for introducing the flexible approach described in the proposal. It was noted that if found later to be not useful, it could be removed again as the TS is not yet under change control. It was decided that more contribution supporting and objecting to this scheme should be made off-line and, if necessary, to the next SA WG3 meeting so that a new review can be made. Section 3.1 (related Pseudo-CR) was then not accepted at this time.
>
> **For section 1.2 of the contribution:** The ability of both sides to trigger the generation of the new shared key was proposed to be clarified how a NAF can trigger a key update. It was agreed that the NAF needs to be able to trigger a key update. Section 3.2 (related Pseudo-CR) was reviewed and approved for inclusion in the draft TS.

TD S3-030342 Pseudo-CR to Support for Subscriber Certificates: Protocol C in stage 3 detail. This was noted and attached to the LS in TD S3-030458.

TD S3-030343 Pseudo-CR to Support for Subscriber Certificates: Protocol D in stage 3 detail. This was noted and attached to the LS in TD S3-030458

TD S3-030344 Pseudo-CR to Support for Subscriber Certificates: Support of operator control for certificate issuing. This was provided by Nokia and was approved for inclusion in the draft TS.

TD S3-030345 Pseudo-CR to Support for Subscriber Certificates: Clarification of the authentication mechanism of the TS. This was provided by Nokia and was approved for inclusion in the draft TS. It was recognised that the Scope will also need to be updated to reflect the pre-certified key pair specified independently by OMA.

TD S3-030347 CMPv2 profile for 3GPP subscriber certificate enrolment. This was provided by SSH Communications Security and proposed that CMPv2 with the profile described is selected as the recommendation, or the only protocol B and that a pseudo-CR stating such selection should be created at the next SA WG3 meeting. There was some objection to the proposal it was therefore noted.

TD S3-030357 Generic secure message exchange using HTTP Digest Authentication. This was introduced by Nokia and proposed to add the description of this generic secure message exchange using HTTP Digest Authentication (section 2 of the contribution, and an introduction based on section 1) to the draft TS as an informative annex. This was approved for inclusion in the draft TS. It was noted that the Protocol B may depend upon the final choice of scheme made by SA WG3 and this will need to be reviewed later by SA WG3. An editors' note will be added to say this.

TD S3-030355 Support for Subscriber Certificates. This was introduced by SchlumbergerSema and proposed that the SA WG3 send a LS to the OMA Security group for the exchange of documents and relevant information. An ad-hoc joint meeting could also be arranged in order to check the possibility to collaborate for advancing a coherent solution that take advantage of existing specifications. It was agreed to send a liaison to the OMA SG. The SA WG3 Chairman undertook to withhold the transmission of the LS until agreement for a joint meeting had been received from TSG SA. It was considered that this may be proposed during the SA WG3 meeting with the LI Group in London. The LS was provided in TD S3-030459 which was approved **but will not be transmitted until after the SA WG3 Chairman confirms that a joint meeting with OMA SG is allowed**.

TD S3-030382 Generation and storage of the UE's public/private key pair associated to the requested certificate. This was introduced by Gemplus and proposed adding some security requirements on the generation and the storage of the UE's public/private key pair associated to the requested certificate in the draft TS. It was agreed that some discussion of the key pair storage use cases and their related security risk analyses in different scenarios could be included in an informative Annex to the draft TS, or as a separate TR. Contribution on this was invited for the next SA WG3 meeting.

7.10 WLAN Interworking

TD S3-030428 LS (from SA WG2) on Denial of Service attacks against the 3GPP WLAN Interworking system. This was introduced by Nortel Networks. SA WG2 asked SA WG3 to comment on the validity of the attached document (S2-032483: "Security analysis for Tunnel Establishment") and any other security issues that SA WG3 believe should be considered in SA WG2's ongoing architecture work. It was decided to hold an e-mail discussion in order to elaborate a response for the August 18 meeting of SA WG2. A. Palanigounder agreed to lead an e-mail discussion and draft a response LS.

AP 29/04: A. Palanigounder to lead an e-mail discussion and draft an LS in response to TD S3-030428 (Denial of Service attacks against the 3GPP WLAN Interworking system). Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003.

TD S3-030433 LS (from SA WG2) on the recommendation from IREG of non publicly routable IP addresses for the GPRS nodes. This was introduced by BT Group. SA WG2 asked to comment on and provide any solutions if any security issues when a PDG address on GRX is made visible and accessible to specific authorised UEs.It was decided to deal with this over an e-mail discussion and S Nguyen Ngoc was asked to lead this.

AP 29/05: S. Nguyen Ngoc was asked to lead an e-mail discussion over LSs in TD S3-030433 and to produce a response LS. Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003.

TD S3-030427 LS (from SA WG2) on PDG IP address discovery using public DNS for WLAN interworking. This was introduced by Ericsson and asked SA WG3 to answer the following questions:

> Is allowing IP address of the WAG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking?
>
> Is allowing IP address of the PDG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking?

It was decided to deal with this over an e-mail discussion and C Blanchard agreed to lead this.

AP 29/06: C. Blanchard to lead an e-mail discussion over LSs in TD S3-030427 and to produce a response LS. Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003.

TD S3-030320 Reply LS (from CN WG1) on Impacts on the UE of UE-Initiated Tunnelling. This was introduced by Nokia and informed SA WG2 that CN WG1 has started WLAN related Stage 3 work and is focusing on WLAN authentication between UE and 3GPP AAA server using EAP/AKA and EAP/SIM procedures. The LS was noted.

TD S3-030425 LS (from SA WG2) on Security issues regarding multiple PDP contexts in GPRS. This was introduced by Vodafone and had been copied to SA WG3 for information. A response from SA WG1 was provided in TD S3-030448. The LS was noted.

TD S3-030448 Reply LS (from SA WG1) on Security issues regarding multiple PDP contexts in GPRS. This was introduced by Nokia and asked SA WG3 to take the stage 1 simultaneous access requirements into account in their work and to mitigate security threats to an acceptable level. This LS was noted and contributions were invited on methods to address any security threats.

TD S3-030326 LS (from CN WG4) on Security Issues regarding multiple access connections. This was introduced by Nortel Networks and asked SA WG3 group to take note of the two solutions identified for the dual GPRS connection scenario (either network based or a UE based solution), noting that the UE based solution would require no changes to 3GPP specifications and would be applicable to all six of the scenarios described and would in some situations allow both of the connections to remain in place. SA WG2 had noted that the detailed analysis is too early to be considered in the current work in SA WG2 and the analysis is forwarded to CN WG4 to be considered in their work on WLAN interworking. It was decided that there would be nothing done in the network for this at present. The LS was then noted.

TD S3-030426 LS (from SA WG2) on 802.11i / WPA and RADIUS to Diameter co-existence analysis and recommendations for WLAN interworking. This was introduced by Ericsson was copied to SA WG3 and was noted.

TD S3-030318 LS (from T WG3) on WLAN interworking. This was introduced by Gemplus and was copied to SA WG3 for information. The LS was noted. A response LS was provided in TD S3-030449.

TD S3-030449 Reply LS (from SA WG1) on WLAN Interworking requirements for SIM and USIM. This was introduced by BT Group and informed SA WG3 of SA WG1 position on each of the technical solutions fully articulates the service requirements to SA3 and T3 for SIM and USIM WLAN Interworking. This LS was noted.

TD S3-030333 Draft TS 33.234 V0.5.0: WLAN Interworking Security. This was introduced by the Rapporteur (C. Blanchard, BT Group). The draft included the changes agreed at SA WG3 meeting #28. this was provided for information and was noted.

TD S3-030364 Pseudo-CR to 33.234: Clarification on pseudonyms (WLAN Security). This was provided by Ericsson and was approved for inclusion in the draft TS.

TD S3-030363 Pseudo-CR to 33.234: Co-Existence of RADIUS and Diameter (WLAN Security). This was provided by Ericsson. It was clarified that the Annex was intended to be informative. It was reported that CN WG4 had acknowledged that this was allowed in their specifications. This was approved for inclusion in the draft TS.

TD S3-030365 Pseudo-CR to 33.234: WLAN UE Functional Split (WLAN Security). This was provided by Ericsson. There was some objection to the inclusion of the bullet "EAP-AKA and EAP-SIM shall terminate in the TE (e.g. laptop computer)". It was agreed to include this bullet as an editors note "termination point of EAP-AKA and EAP-SIM is for further study". It was noted that the first bullet point may be a duplication. This needed further investigation but can be removed before approval of the Draft TS. With this change to the second bullet, the Pseudo-CR was then approved for inclusion in the draft TS.

TD S3-030334 Pseudo CR to 33.234 v0.5.0: Support for interleaving authentication. This was introduced by BT Group. There was no support for this and the Pseudo-CR was rejected. It was noted, however, that there is an issue on interleaving which requires further study and delegates were asked to contribute on this.

TD S3-030383 Pseudo-CR to 33.234: Support for interleaving authentication (WLAN Security). This was introduced by Siemens and introduced an informative annex on Management of sequence numbers, copied from TS 33.203 with minor editing for WLAN applicability. It was agreed that the handling of the INDEX value was only an example and the Pseudo-CR was approved for inclusion in the draft TS with additional text to clarify this.

TD S3-030362 Pseudo-CR to 33.234: Alignment with WLAN architecture definition (WLAN Security). This was introduced by Ericsson. It was agreed that an editors' note should be added to 4.1.1 mentioning that the section is dependant upon the final SA WG2 architecture. The Pseudo-CR was then approved for inclusion in the draft TS. The attached proposal for an LS to SA WG2 was not agreed, as SA WG3 should discuss and specify what is to be protected.

The contributions on WLAN trust model were considered together:

> TD S3-030369 WLAN – Implications of the trust relation between the Cellular Operator and the WLAN Access Provider. This was introduced by Ericsson and provided an analysis of the trust relationships. Ericsson suggested to incorporate this analysis into Annex B of TS 33.234 and proposed that SA WG3 inform SA WG1 and SA WG2 about the implications that the trust relation between the Cellular Operator and the WLAN Access Provider has on the WLAN-3GPP interworking solution.
>
> TD S3-030332 Alternative WLAN Interworking Trust Model. This was introduced by BT Group and purposed some modifications to the trust model suggested by Ericsson in S3-030261 to reflect the comments made on the SA WG3 e-mail list since SA WG3 meeting #28. This was noted and to be taken into account during the Trust Model discussions (see AP 29/07).
>
> TD S3-030414 Consequences of the WLAN trust model?. This was introduced by Siemens who had analysed the content of contributions from Ericsson and BT Group and proposed:
>
> - *Clarify the purpose of the inclusion of a trust model in TS 33.234. One purpose could be to motivate the selection of security mechanisms in the main body.*
> - *If the purpose of the trust model is to motivate the selection of security mechanisms in the main body then restrict the trust model to those aspects impacting security mechanisms specified in TS 33.234. This implies to remove the considerations on access to services provided by the WLAN Access Provider. (This is mostly about charging which is not in the responsibility of SA WG3. The charging related aspects could be communicated to SA WG5 in an LS.)*

- *Make the consequences from the trust model explicit. The proposed consequence is that:*
  - *SA WG3 needs to specify the confidentiality, integrity and key management for a tunnel between UE and PLMN (home or visited), and that*
  - *the security for the tunnel is optional as it may not be needed in cases of high trust.*

It was agreed to include the table from TD S3-030369 with an editors note that this is for further elaboration in the draft TS. P. Howard agreed to lead an e-mail discussion on this and provide a contribution to SA WG3 meeting#30.

AP 29/07: P. Howard to lead an e-mail discussion on Trust Model and provide a contribution to SA WG3 meeting#30.

TD S3-030398 Pseudo-CR to 33.234: Clarification to Annex B.2 Trust Relation Editor's Note (WLAN Security). This was introduced by AT&T Wireless Services. It was agreed to include in the main body of the draft TS.

7.11 Visibility and configurability of security

There were no specific contributions under this agenda item.

7.12 Push

There were no specific contributions under this agenda item.

7.13 Priority

There were no specific contributions under this agenda item.

7.14 Location services (LCS)

There were no specific contributions under this agenda item.

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

TD S3-030420 Technical Report on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6). This was provided by the following companies: Toshiba, Intel, T-Mobile, Nokia, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel. It was provided for information and was noted. The document had been produced via telephone conference calls between the involved companies and it was requested that at least 1 telephone conference is opened up and SA WG3 are invited to join it, before the October meeting. It was also requested that the draft is distributed to SA WG3 after each update so that Members can track the evolution of the work.

It was proposed to add this to the topics covered by the ad-hoc meeting 3-4 September 2003, but it was decided that priority is given to the Generic Authentication Architecture and MBMS discussions. Order of discussions: GAA, MBMS.

7.16 Open service architecture (OSA)

There were no specific contributions under this agenda item.

7.17 Generic user profile (GUP)

TD S3-030316 LS from T WG2: UE security aspects of the GUP architecture. This was introduced by the SA WG3 Chairman. Due to lack of time, it was necessary to deal with a discussion and response over e-mail. The GUP Rapporteur (B. Owen) will be asked to lead the e-mail discussion using the same deadlines that were agreed also for WLAN related LSs to SA2, see AP 29/04.

AP 29/08: B. Owen to lead an e-mail discussion on TD S3-030316 (UE security aspects of the GUP architecture). Comments before 6 August, draft response LS: 8 August and Approval for transmission 15 August 2003.

TD S3-030404 LS (from SA WG2) on usage of GUP reference points. This was introduced by the SA WG3 Chairman. Due to lack of time, it was necessary to deal with a discussion and response over e-mail. The GUP Rapporteur (B. Owen) will be asked to lead the e-mail discussion using the same deadlines that were agreed also for WLAN related LSs to SA2, see AP 29/04.

TD S3-030329 LS (from SA WG5) on usage of GUP reference points. This was provided for information and was noted.

7.18 Presence

TD S3-030351 Draft TS 33.abc: Presence Service; Security. Version 0.5.0. This was provided for information and included updates from agreements from SA WG3 meeting #28. The draft TS was noted.

TD S3-030325 LS (from CN WG1) on security solutions for the Ut reference point. This was introduced by Siemens CN WG1 informed SA WG3 that the solutions proposed by SA Wg3 were feasible, but had a number of drawbacks:

This would be the first case where a Rel-6 service in an Application Server requires the S-CSCF to be updated to Rel-6 which causes backward compatibility problems.

- *It is anticipated that the key derivation in the S-CSCF puts additional processing load on the S-CSCF which is multiplied by the number of application servers involved.*
- *CN WG1 thinks that registration should be used exclusively for authentication of the UE to the IMS.*

The LS was then noted.

TD S3-030430 Liaison (from SA WG2) on Security Solutions for the Ut Reference Point. This was introduced by Siemens and was provided for information. The LS was noted.

TD S3-030447 LS (from SA WG1) on requirements on security for the Mt reference point. SA WG1 informed SA WG3 that in their understanding, the Mt (Ut) Reference point is meant to allow IMS subscribers to manage their data on application servers, so it is required that the IMS subscriber is unambiguously identified prior to usage. The LS was noted.

TDs S3-030413, TD S3-030391, TD S3-030359, TD S3-030371 and TD S3-030400 were presented and discussed in order to arrive at a common understanding of the issues and proposed solutions for Presence security.

TD S3-030413 Evaluation of proposals for security at the Ut (formerly: Mt) reference point. This was provided by Siemens and summarised the proposals received in SA WG3 meeting #28 and concluded that the IMS-based solution was preferred, or as a second choice, the BSF-based solution should be adopted. Siemens proposed that SA WG3 should be careful not to develop two or more similar solutions for the different Applications (i.e. there should be a single bootstrapping architecture). **SA WG3 agreed that the proxy functionality providing the termination point for TLS should be used**.

The contribution also analysed the comments received from CN WG1 in TD S3-030325 (the drawbacks with the proposals) which were discussed. (see TD S3-030325 above)

TD S3-030391 Comparison of different approaches in the Presence/Ut interface. This was provided by Nokia and Ericsson and compared the two approaches, based on HTTP authentication proxy, and based on IMS registration. It also suggested that SA WG3 decides which of the two approaches is preferred for further study.

TD S3-030359 Rationale of Presence service and Authentication Proxy functionality in detail. This was provided by Nokia and discussed the design preference based on the description of the service. It compared the solution proposals and concluded to use Authentication proxy as an optimised solution.

TD S3-030371 Access to Application Servers using HTTP in Presence/Ut interface. This was provided by Ericsson and proposed architectural means to solve the problem. It suggested that SA WG3 should take a working assumption that access to all such applications can be implemented using HTTP proxy as a centralized access point. Ericsson highlighted that AKA standardisation and update in IETF is much faster then the usual adoption process in IETF. AKAv2 had already been designed for re-use of passwords.

It was decided to collect together the open issues related to key management of HTTP-based services into a list in order to concentrate them between meetings. It was decided to arrange an email collection of the issues. **Deadline for submission of issues was decided to be 27th August**.

AP 29/09: G. Horn to lead an e-mail discussion on open issues related to Key Management of HTTP-based services. Deadline for collection of issues: 27 August 2003.

A resulting contribution was provided in TD S3-030460.

TD S3-030400 IMS watcher authentication. This was introduced by Nokia and proposed the presentity issued password-based authentication as optional to the IMS, and may be adopted for non-IMS watcher authentication. Nokia also suggested that LSs to SA WG1should be generated on whether this new requirement makes sense to the IMS user and to SA WG2 and CN WG1 requesting their views on adding this new feature for IMS user; and finally to all groups, the solution for non-IMS watcher authentication. It was agreed that this feature of security based on passwords should be optional. It was also agreed to provide an LS informing SA WG1, copied to SA WG2 and CN WG1, informing them of this and asking if there are any comments or concerns on the need for this. It was agreed to do this after more discussion at SA WG3 meeting #30 meeting.

AP 29/10: Tao Haukka to provide draft LS to SA WG1 on IMS watcher authentication for discussion at SA WG3 meeting #30.

7.19 User equipment management (UEM)

There were no specific contributions under this agenda item.

7.20 Multimedia broadcast/multicast service (MBMS)

TD S3-030313 LS (from SA WG4) on DRM Content Format. This was introduced by the SA WG3 Chairman and was copied to SA WG3 for information. SA WG4 informed OMA DRM DL that they were looking forward to good cooperation on DRM. The LS was noted.

TD S3-030314 Reply LS (from SA WG4) to “Reply to Liaison Statement on MBMS Codec Requirements”. This was introduced by Nokia and was provided to SA WG3 for information. The LS was noted.

TD S3-030315 Liaison response (from SA WG4) on LS on Protocols, Codecs and Media formats for MBMS. This LS was provided to SA WG3 for information and was noted.

TD S3-030328 Response (from RAN WG2) to LS on double ciphering for MBMS multicast data. This was introduced by Siemens and was provided to SA WG3 for information. It was agreed that there was no need to consider the issue of avoidance of double ciphering any further in SA WG3. The LS was noted.

TD S3-030337 LS (from CN WG4 on adapting Cx interface protocols for security purposes. This was introduced by Nokia and asked SA WG3 to consider the synchronisation problem of AVs and security requirements for inter-domain Cx interface usage and to provide guidance to CN WG4. The issues described will be considered by SA WG3 at the ad-hoc meeting. SA WG3 do not consider the case of inter-domain use of the Cx protocol and is restricted to intra-domain usage for Rel-6 work. A response LS will be prepared by G. Horn in TD S3-030473 for distribution for comments and approval by e-mail after the meeting. Comments by 25 July 2003, Approval by 1 August 2003.

TD S3-030434 LS (from SA WG4) on DRM for Progressive Download. This was introduced by the SA WG3 Chairman and was provided to SA WG3 for information. It was agreed that this should be monitored by SA WG3 as the DRM work is now handled in OMA. The LS was then noted.

TD S3-030446 Reply (from SA WG1) to Liaison Statement on “MBMS Codec Requirements. This was introduced by Nortel Networks and was provided to SA WG3 for information. SA WG1 informed groups that they will define a new "MBMS **Teleservice**" and keep SA WG4 informed on progress of the work. It was noted that there may be some impact on SA WG3 (a contribution on this was provided in TD S3-030401). The LS was noted.

MBMS Security contributions:

TD S3-030397 User authentication by Service Platforms. This was introduced by Nortel Networks and considered the relationship between "User authentication by a service platform" and the Support for Subscriber Certificates work ongoing in SA WG3. It was recognised that the use of Proxy CAs and BSF needed further analysis. It was also clarified that it was envisaged that a single, long-lived certificate could be used for user access to many operator services. There was some support that a general-purpose approach should be taken in the chosen scheme. Some further work on Architecture was considered necessary. Other related contributions were then considered.

TD S3-030412 HSS/HLR-related security architecture issues and implications for presence, MBMS and support for subscriber certificates. This was introduced by Siemens and proposes architectural design rules/guidelines for the development of security solutions. It was noted that guideline 6 was not really HSS-related (although the HSS may be impacted if the guideline was not followed). It was generally accepted that such guidelines were useful and it was recognised that some further editing should be done to make a fully acceptable set for adoption by SA WG3 for use in security work. A drafting session was arranged for the evening to update the guidelines.

TD S3-030460 HSS/HLR-related security architecture guidelines. The guidelines were presented by the drafting group chairman (G. Horn) and were approved. The guidelines are recorded in this report below:

HSS-related design guidelines for a security architecture:

It is recommended that these guidelines are taken into account for all features currently being specified for 3GPP Release 6, and features in future releases. It is certainly not possible nor desirable to make any changes to earlier Releases. It is also clear that often a trade-off has to be made between these guidelines and other criteria, e.g. regarding service provision or the impact on other entities. However, it should be noted that the HSS is arguably one of the most valuable assets of an operator.

1. The number of different types of interfaces to the HSS should be minimised in order to keep the complexity of the HSS low. This applies in particular to interfaces over which authentication vectors are retrieved from the HSS as they are highly security-critical.
2. For reasons of HSS and AuC-performance, the overall number of authentication vectors requested from the authentication centre as well as the number of requests should be kept low. Mechanisms, which make economical use of authentication vectors, should be preferred. In particular, mechanisms, which avoid bursts in authentication vector requests, should be preferred.
3. The number of nodes with access to authentication vectors should be limited in order to reduce the possibility of illegitimate access to authentication vectors.
4. The number of authentication domains (e.g. CS and the PS domain, the IMS, 3G-WLAN interworking, presence and MBMS) as well as the number of nodes within a domain for which authentication vectors for one user are stored (e.g. 3GPP AAA servers) should be kept small. This is to avoid frequent re-synchronisation. Re-synchronisation problems do not occur if unused AVs are forwarded to other nodes where they are needed, as is the case e.g. with VLRs in the same PLMN.
5. Mechanisms should be designed in such a way that the effect of a compromise of authentication information in one authentication domain on other domains is minimised.
6. Authentication information should be securely stored in nodes and securely transported between nodes.

Terminology: The notion of “authentication domain” is used here to denote a subsystem of a 3G network, which uses authentication vectors.

TD S3-030367 Access to Application Servers using HTTP in MBMS. This was introduced by Ericsson and discussed some problems and solutions for potential SQN synchronisation failure related to re-use of AKA with HTTP-based applications. Ericsson proposed that SA WG3 make a working assumption that access to all applications that use HTTP for transport and AKA for authentication can be implemented using a reverse HTTPS proxy in order to solve potential synchronization problems and to inform SA2 and CN4 that architectural means would play an important role when solving the problems related to potential SQN synchronization failures.

TD S3-030393 Authentication in MBMS. This contribution was provided by Alcatel and proposed the use of generic bootstrapping application security mechanism described in the draft TS "Bootstrapping of Application Security using AKA and Support for Subscriber Certificates".

TD S3-030403 MBMS authentication architectures evaluation. This was introduced by Siemens and provided an evaluation of possible authentication architectures for MBMS: direct AKA based and BSF-based. It concluded is that further study is needed before deciding on this issue. Siemens proposed to further study the different authentication alternatives taking into account the suggestions made by this contribution.

It was generally agreed that not enough information was available to make a decision in SA WG3 and the proxy scenario also needs analysis. The received contributions on this were considered very useful as a basis for further study and delegates were asked to do this, possibly for further development in an MBMS ad-hoc meeting.

TD S3-030358 DRAFT 3GPP TS 33.246 V0.1.1 (MBMS Security). This was provided by the Editor for information and included changes agreed at the previous meeting. A clean version will be used for any changes agreed at this meeting. The TS was then noted.

TD S3-030401 MBMS Security Requirements Clarification. This was introduced by Nortel Networks and discussed their understanding of the MBMS Service requirements in TS 22.146. It proposed two working assumptions for SA WG3 to adopt and the changes to the TS required to reflect the clarifications in order to further progress the MBMS work item by means of a Pseudo-CR attached to the contribution. Conclusion 1 was not agreed as a working assumption that could be made at this time by SA WG3, and Conclusion 2 was agreed under the understanding that the ongoing work is not stopped. The Pseudo-CR was discussed and it was agreed that the proposed changes should be re-edited and captured in an Editors' Note rather than a change to the specification, as it is more related to further development of the MBMS specification. It was decided to do this over e-mail after the meeting.

TD S3-030366 Pseudo-CR to 33.246: Confidentiality protection of MBMS multicast data (MBMS Security). It was clarified that the prevention of a valid subscriber retransmitting the received data could not be protected against, as this is a DRM issue. Ericsson proposed that it would be a good idea to capture these requirements in the draft TS at this stage, and if considered unnecessary in the future, they could be removed again. It was agreed that this should be included by the editor with some re-wording of the text.

TD S3-030335 Hybrid MBMS Key Management Scheme. This was introduced by BT Group. BT Group had analysed some contributions discussed at SA WG3 meeting #28 and supported the view that efficient use of the radio and network resources is important, and proposed that by making use of the uplink messages, a hybrid scheme may be designed which retains the multipoint principle of the LKH scheme, but is more in line with the hierarchy of the BAK scheme. This hybrid scheme more closely matches the needs of network operators, in terms of complexity, operational efficiency and perhaps most importantly, in minimising potential complaints from users that they have missed the start of a broadcast event that they have paid for, due to keying errors. After some discussion it was decided that the requirements need to be analysed to put them into the current SA WG3 terminology and to check which requirements are really necessary. The resulting requirements should be inserted in the draft TS where they are clear, and SA WG1 should be consulted if necessary on any items which need clarification. This was agreed to be done over e-mail for presentation to the ad-hoc meeting in September 2003. C. Blanchard agreed to organise and chair the discussion group on this.

AP 29/11: C. Blanchard to set up a discussion group and elaborate the MBMS Key Management requirements based on TD S3-030335.

Available contributions on MBMS Keying were presented and used for a joint discussion on the proposed mechanisms:

TD S3-030360 Levels of Key Hierarchy for MBMS. This was covered by the presentation in TD S3-030451 and was noted.

TD S3-030349 MBMS re-keying: PTP with periodic re-keying. This was introduced by Huawei Technologies and proposed some "*simple yet effective*" re-keying schemes for initial MBMS services and proposed adopting the point-to-point re-keying with periodic re-keying as described in the document. Furthermore, Huawei Technologies suggested studying more complex techniques, such as LKH, for subsequent Releases. The contribution was noted.

TD S3-030368 Introducing SRTP and MIKEY in TS 33.246 (MBMS Security). This was introduced by Ericsson and provided information regarding the relation between the MSEC architecture and MBMS architecture. It also provided some reasoning for choosing SRTP and MIKEY as security and key management protocols and introducing them into TS 33.246. An attached Pseudo-CR described the proposed changes to draft TS 33.246. Ericsson also proposed that SA WG3 should follow and re-use the work done in IETF MSEC WG. It was acknowledged that this proposal was a diversion from the scheme adopted by 3GPP2, which should also be taken into account.

TD S3-030396 Key distribution and billing in PayTV model. This was introduced by Oberthur and Gemplus and provided more information on the key distribution and billing offered by the PayTV model. It was reported that the DVB-3GPP convergence scenario had been presented to SA WG1 and it would be further studied at their next ad-hoc meeting.

TD S3-030408 Reliable key distribution mechanism. This was introduced by Samsung Electronics. It was similar to the contribution from BT Group in TD S3-030335 and concluded with some requirements to be included in the draft TS:

- BMSC shall be able to page users for the coming key distribution via MBMS notification;
- UEs who miss the key distribution shall be able to ask for one separate key distribution over one dedicated channel;
- BMSC shall be able to support the point-to-point key distribution as one supplemental mechanism to the multicast based key distribution.

There was much discussion on the issues and proposals raised by the contributions and no agreement could be achieved on inclusion of the key management scenarios in the draft TS at this stage. It was agreed that this should be further debated in the ad-hoc meeting (early September 2003) in order to get a firm proposal to be confirmed by SA WG3 in October 2003.

AP 29/12: M. Pope to check if an ad-hoc meeting can be held at ETSI premises 3-4 September 2003 (20 delegates).

TD S3-030409 Some consideration about Ciphering Key usage timing. This was introduced by Samsung Electronics and analysed several scenarios related to CK usage timing for MBMS and concluded that the autonomous method for new CK indication is not feasible for MBMS and proposed that SA WG3 start studying a method for new CK usage indication. SA WG3 agreed with the conclusions from the analysis and thanked Samsung Electronics for performing this study. SA WG3 need to study this issue further.

TD S3-030437 draft LS (to SA WG1) on clarification of MBMS charging issues. This was introduced by T. Viitanen and was the status of the LS which failed completion and agreement over e-mail. It was considered that SA WG1 shouldn't be misled in thinking that all the detailed charging issues could be solved by SA WG3 in the Rel-6 time frame. It was decided to update the LS to clarify this in TD S3-030453 which was revised in TD S3-030472 and approved.

7.21 Guide to 3G security (TR 33.900)

There were no specific contributions under this agenda item.

8 Review and update of work programme

TD S3-030392 Proposed WID: Key Management of group keys for Voice Group Call Services. This was provided by Vodafone D2. The timescales were considered ambitious and the possibility to complete the work in time for Rel-6 was questioned. It was agreed that the time plan should be updated to give 1 more TSG Plenary time for completion. An updated WID was provided in TD S3-030464 which was approved.

9 Future meeting dates and venues

The planned meetings were as follows:

Meeting	Date	Location	Host
S3-Ad-Hoc	3-4 September 2003	TBD	Host required
S3#30	6 (13.00) - 10 October 2003	Povoa De Varzim, Portugal	European 'Friends of 3GPP'
S3#31	18-21 November 2003	London co-located with S3-LI (TBC)	DTI (TBC)
S3#32	09-13 February 2004	TBD	TBD
S3#33	10-14May 2004	Korea (TBC)	Samsung (TBC)

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#10	23 - 25 September 2003	US	TBA
SA3 LI-#11	18-20 November 2003	London	DTI

TSGs RAN/CN/T and SA Plenary meeting schedule

Meeting	2003	Location	Primary Host
TSG RAN/CN/T #21	16-19 September 2003	Berlin, Germany	European Friends of 3GPP
TSG SA #21	22-25 September 2003	Berlin, Germany	European Friends of 3GPP
TSG RAN/CN/T #22	9-12 December 2003	Hawaii, USA	NA Friends of 3GPP
TSG SA #22	15-18 December 2003	Hawaii, USA	NA Friends of 3GPP
Meeting	**2004 DRAFT TBD**	**Location**	**Primary Host**
TSG#23	March 9-12 & 15-18 2004	China	
TSG#24	June 1-4 & 7-10 2004	Korea	
TSG#25	7-10 & 13-16 September 2004	USA	
TSG#26	7-10 & 13-16 December 2004	To Be Decided	

Invitations to the next meeting should be transmitted the week after this meeting. M Pope to contact hosts.

10 Any other business

Late Contributions (received after 17.00 CET, Thursday 10 July):

TD S3-030422 SA handling regarding to the lifetime of SA. This was handled with other contributions in an off-line drafting group.

TD S3-030423 Proposed CR to 33.203: Removal of SA lifetime (Rel-5). This was not handled with other contributions, but it was discussed in an off-line drafting group.

11 Close

The Chairman, V. Niemi, thanked delegates for their hard work during the meeting and the Hosts for the facilities. He then closed the meeting.

Annex A: List of attendees at the SA WG3#28 meeting and Voting List

A.1 List of attendees

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Jorge Abellan Sevilla	SchlumbergerSema	jorge.abellan@slb.com		+33 1 46 00 59 33	+33 1 46 00 59 31	FR	ETSI
Mr. Hiroshi Aono	NTT DoCoMo Inc.	aono@mml.yrp.nttdocomo.co.jp		+81 468 40 3509	+81 468 40 3788	JP	ARIB
Mr. Nigel Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	+44 7785 31 86 31	+44 1 256 790 169	+44 1 256 790 190	GB	ETSI
Mr. Colin Blanchard	BT Group Plc	colin.blanchard@bt.com	+44 7711 191835	+44 1473 605353	+44 1473 623910	GB	ETSI
Mr. Marc Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.com		+32 14 25 34 11	+32 14 25 33 39	BE	ETSI
Mr. Krister Boman	ERICSSON LM	krister.boman@ericsson.com	+46 70 246 9095	+46 31 747 4055		SE	ETSI
Mr. Charles Brookson	DTI	cbrookson@iee.org	+44 7956 567 102	+44 20 7215 3691	+44 20 7931 7194	GB	ETSI
Mr. Holger Butscheidt	BMWi	Holger.Butscheidt@RegTP.de		+49 6131 18 2224	+49 6131 18 5613	DE	ETSI
Mr. Mauro Castagno	TELECOM ITALIA S.p.A.	mauro.castagno@telecomitalia.it		+39 0112285203	+39 0112287056	IT	ETSI
Mr. Sharat Chander	AT&T Wireless Services, Inc.	sharat.chander@attws.com	+1 435 894 7756	+1 425 580 6596	+1 425 580 6811	US	T1
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp		+81 467 41 2181	+81 467 41 2185	JP	ARIB
Mr. Per Christoffersson	TeliaSonera AB	per.christoffersson@teliasonera.com		+46 705 925100		SE	ETSI
Mr. Kevin England	mmO2 plc	kevin.england@o2.com	+447710016799	+447710016799		GB	ETSI
Mr. Hubert Ertl	GIESECKE & DEVRIENT GmbH	hubert.ertl@de.gi-de.com	+49 172 8691159	+49 89 4119 2796	+49 89 4119 2921	DE	ETSI
Dr. Adrian Escott	3	adrian.escott@three.co.uk		+44 7782 325254	+44 1628 766012	GB	ETSI
Mr. John B Fenn	SAMSUNG Electronics	johnbfenn@aol.com	+44 78 02 339070	+44 1784 428 600	+44 1784 428 629	GB	ETSI
Mr. Louis Finkelstein	MOTOROLA JAPAN LTD	louis.finkelstein@motorola.com		+1 847 576 4441	+1 847 538 4593	JP	ARIB
Mr. Jean-Bernard Fischer	OBERTHUR CARD SYSTEMS S.A.	jb.fischer@oberthurcs.com		+33 141 38 18 93	+33 141 38 48 23	FR	ETSI
Mr. Philip Ginzboorg	NOKIA Corporation	philip.ginzboorg@nokia.com		+358 5 0483 6224	+358 9 4376 6852	FI	ETSI
Ms. Tao Haukka	Nokia Korea	tao.haukka@nokia.com		+358 40 5170079		KR	TTA
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. Robert Jaksa	HUAWEI TECHNOLOGIES Co. Ltd.	rjaksa@futurewei.com		+1 972 509 5599	+1 972 509 0309	CN	ETSI
Mr. Geir Koien	TELENOR AS	geir-myrdahl.koien@telenor.com		+47 90752914	+47 37 04 52 84	NO	ETSI
Mr. Pekka Laitinen	NOKIA Corporation	pekka.laitinen@nokia.com		+358 5 0483 7438	+358 7 1803 6852	FI	ETSI
Mr. Alex Leadbeater	BT Group Plc	alex.leadbeater@bt.com		+441473608440	+44 1473 608649	GB	ETSI
Mr. David Mariblanca	ERICSSON LM	david.mariblanca@ericsson.com		+34 646004736	+34 913392538	SE	ETSI
Mr. Stephen McCann	SIEMENS AG	stephen.mccann@roke.co.uk		+44 1794 833341	+44 1794 833434	DE	ETSI
Mr. Sebastien Nguyen Ngoc	ORANGE FRANCE	sebastien.nguyenngoc@francetelecom.com		+33 1 45 29 47 31	+33 1 45 29 65 19	FR	ETSI
Mr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com		+358 50 4837 327	+358 9 437 66850	FI	ETSI
Mr. Bradley Owen	Lucent Technologies N. S. UK	bvowen@lucent.com		+44 1793 897312	+44 1793 897414	GB	ETSI
Mr. Anand Palanigounder	NORTEL NETWORKS (EUROPE)	anand@nortelnetworks.com		+1 972 684 4772	+1 972 685 3123	GB	ETSI
Miss Mireille Pauliac	GEMPLUS Card International	mireille.pauliac@GEMPLUS.COM		+33 4 42365441	+33 4 42365792	FR	ETSI
Mr. Maurice Pope	ETSI Secretariat	maurice.pope@etsi.org	+33 (0)6 07 59 08 49	+33 4 92 94 42 59	+33 4 92 38 52 59	FR	ETSI
Mr. Greg Rose	QUALCOMM EUROPE S.A.R.L.	ggr@qualcomm.com	+61 2 8701 4052	+61 2 9817 4188	+61 2 9817 5199	FR	ETSI
Mr. Bengt Sahlin	ERICSSON LM	Bengt.Sahlin@lmf.ericsson.se		+358 40 778 4580	+358 9 299 3401	SE	ETSI
Mr. Stefan Schroeder	T-MOBILE DEUTSCHLAND	stefan.schroeder@t-mobile.de		+49 228 9363 3312	+49 228 9363 3309	DE	ETSI
Mr. James Semple	QUALCOMM EUROPE S.A.R.L.	c_jsemple@qualcomm.com		+447880791303		FR	ETSI

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG	
Mr. Benno Tietz	Vodafone D2 GmbH	benno.tietz@vodafone.com		+49 211 533 2168	+49 211 533 1649	DE	ETSI
Mr. Willy Verbestel	RIM	wmjv@hotmail.com	+1 760 580 4585	+1 760 737 8428	+1 760 294 2125	CA	ETSI
Mr. Tommi Viitanen	Nokia Telecommunications Inc.	tommi.viitanen@nokia.com		+358405131090	+358718075300	US	T1
Ms. Monica Wifvesson	ERICSSON LM	monica.wifvesson@emp.ericsson.se		+46 46 193634	+46 46 231650	SE	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. Guanghai Zhang	China Mobile Com. Corporation	zhangguanghai@chinamobile.com		+86 1066506888-1311	+86 10 63600117	CN	CWTS
Mr. Yanmin Zhu	Samsung Electronics Co., Ltd	zym@samsung.co.kr		+861068427711	+861068481898	KR	TTA

46 attendees

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #27, #28 and #29, the following companies are eligible to vote at SA WG3 meeting #30:

Company	Country	Status	Partner Org
3	GB	3GPPMEMBER	ETSI
ALCATEL S.A.	FR	3GPPMEMBER	ETSI
AT&T Wireless Services, Inc.	US	3GPPMEMBER	T1
BT Group Plc	GB	3GPPMEMBER	ETSI
BUNDESMINISTERIUM FUR WIRTSCHAFT	DE	3GPPMEMBER	ETSI
Centre for Development of Telematics	IN	3GPPMEMBER	ETSI
China Mobile Communications Corporation (CMCC)	CN	3GPPMEMBER	CWTS
DTI - Department of Trade and Industry	GB	3GPPMEMBER	ETSI
GEMPLUS Card International	FR	3GPPMEMBER	ETSI
GIESECKE & DEVRIENT GmbH	DE	3GPPMEMBER	ETSI
HEWLETT-PACKARD France	FR	3GPPMEMBER	ETSI
HUAWEI TECHNOLOGIES Co. Ltd.	CN	3GPPMEMBER	ETSI
INTEL CORPORATION SARL	FR	3GPPMEMBER	ETSI
Lucent Technologies	US	3GPPMEMBER	T1
Lucent Technologies Network Systems UK	GB	3GPPMEMBER	ETSI
Lucent Technologies Networks System GmbH	DE	3GPPMEMBER	ETSI
MICROSOFT EUROPE SARL	FR	3GPPMEMBER	ETSI
Mitsubishi Electric Co.	JP	3GPPMEMBER	ARIB
mmO2 plc	GB	3GPPMEMBER	ETSI
MOTOROLA JAPAN LTD	JP	3GPPMEMBER	ARIB
MOTOROLA Ltd	GB	3GPPMEMBER	ETSI
NOKIA Corporation	FI	3GPPMEMBER	ETSI
NOKIA KOREA	KR	3GPPMEMBER	TTA
Nokia Telecommunications Inc.	US	3GPPMEMBER	T1
NORTEL NETWORKS (EUROPE)	GB	3GPPMEMBER	ETSI
Nortel Networks (USA)	US	3GPPMEMBER	T1
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
OBERTHUR CARD SYSTEMS S.A.	FR	3GPPMEMBER	ETSI
ORANGE FRANCE	FR	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
Research In Motion Limited	CA	3GPPMEMBER	ETSI
Samsung Electronics Ind. Co., Ltd.	KR	3GPPMEMBER	TTA
SAMSUNG Electronics Research Institute	GB	3GPPMEMBER	ETSI
SchlumbergerSema - Schlumberger Systèmes S.A	FR	3GPPMEMBER	ETSI
SIEMENS AG	DE	3GPPMEMBER	ETSI
SIEMENS ATEA NV	BE	3GPPMEMBER	ETSI
SSH Communications Security Corp	FI	3GPPMEMBER	ETSI
T-MOBILE DEUTSCHLAND	DE	3GPPMEMBER	ETSI
TELECOM ITALIA S.p.A.	IT	3GPPMEMBER	ETSI
Telefon AB LM Ericsson	SE	3GPPMEMBER	ETSI
Telenor AS	NO	3GPPMEMBER	ETSI
TeliaSonera AB	SE	3GPPMEMBER	ETSI
Toshiba Corporation, Digital Media Network Company	JP	3GPPMEMBER	ARIB
TruePosition Inc.	US	3GPPMEMBER	ETSI
VeriSign Switzerland SA	CH	3GPPMEMBER	ETSI
Vodafone D2 GmbH	DE	3GPPMEMBER	ETSI
VODAFONE Group Plc	GB	3GPPMEMBER	ETSI

47 Individual Member Companies

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030310	Draft Agenda for SA WG3 meeting #29	SA WG3 Chairman	2	Approval		Approved with agreed modifications to scheduling
S3-030311	Draft Report of SA WG3 meeting #28 v0.0.6	SA WG3 Secretary	4.1	Approval		Minor update and approved as version 1.0.0
S3-030312	LS (from SA WG2) on unciphered IMEISV transfer	SA WG2	7.5	Action		E-mail discussions for CR production and approval (M Blommaert, P Howard)
S3-030313	LS (from SA WG4) on DRM Content Format	SA WG4	7.20	Information		Noted
S3-030314	Reply LS (from SA WG4) to “Reply to Liaison Statement on MBMS Codec Requirements”	SA WG4	5.1	Information		Noted
S3-030315	Liaison response (from SA WG4) on LS on Protocols, Codecs and Media formats for MBMS	SA WG4	5.1	Information		Noted
S3-030316	LS from T WG2: UE security aspects of the GUP architecture	T WG2	5.1	Action		Response via e-mail (B Owen to lead)
S3-030317	Draft TS ab.cde version 0.2.0: Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description (Release 6)	Rapporteur (T Haukka)	7.9	Information		Noted
S3-030318	LS (from T WG3) on WLAN interworking	T WG3	7.10	Information		Noted
S3-030319	Response LS from T WG3: Re: LS on clarification of USIM-based access to IMS	T WG3	7.1	Information		Noted
S3-030320	Reply LS (from CN WG1) on ‘Impacts on the UE of UE-Initiated Tunnelling”	CN WG1	5.1	Information		Noted
S3-030321	Reply LS (from CN WG1) on unciphered IMEISV transfer	CN WG1	5.1	Information		E-mail discussions for CR production and approval (M Blommaert, P Howard)
S3-030322	LS (From CN WG1 re: S3-030308) on increasing the key length for GEA3	CN WG1	5.1	Action		Noted
S3-030323	LS (from CN WG1) on transport of unknown SIP signalling elements	CN WG1	7.1	Action		Reply LS in S3-030440
S3-030324	LS (from CN WG1) on Security Association Lifetimes	CN WG1		Action		Revised in S3-030330
S3-030325	LS (from CN WG1) on security solutions for the Ut reference point	CN WG1	7.18	Information		Noted
S3-030326	LS (from CN WG4) on Security Issues regarding multiple access connections	CN WG4	7.10; 7.6	Action		Noted. No standardisation in NW at present
S3-030327	WITHDRAWN - Response (from RAN WG2) to LS on double ciphering for MBMS multicast data.	RAN WG2	7.20	Information	S3-030328	WITHDRAWN - replaced by S3-030328
S3-030328	Response (from RAN WG2) to LS on double ciphering for MBMS multicast data	RAN WG2	7.20	Information		No need to pursue double ciphering any further. Noted
S3-030329	LS (from SA WG5) on usage of GUP reference points	SA WG5	5.1	Information		Noted
S3-030330	LS (from CN WG1) on Security Association Lifetimes	CN WG1	7.1	Action		Related to S3-030336
S3-030331	Report from SA#20 plenary	SA WG3 Chairman	4.2	Information		Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030332	Alternative WLAN Inter-working Trust Model	BT Group	7.10	Discussion / Decision		Noted. To be taken into account in Trust Model discussions (AP 29/07)
S3-030333	Draft TS 33.234 V0.5.0: WLAN Interworking Security	Rapporteur (C. Blanchard)	7.10	Information		Noted
S3-030334	Pseudo CR to 33.234 v0.5.0: Support for interleaving authentication	BT Group	7.10	Approval		Rejected
S3-030335	Hybrid MBMS Key Management Scheme	BT Group	7.20	Discussion / Decision		e-mail elaboration of requirements to be set up by C. Blanchard
S3-030336	LS (from TSG CN) on Security Association Lifetime Management	TSG CN	5.1	Action		Used in Drafting meeting Output CR in S3-030442
S3-030337	LS (from CN WG4 on adapting Cx interface protocols for security purposes	CN WG4	7.20	Action		Reply in S3-030473
S3-030338	Extract of OMA Discussion Part of TSG SA #20 Draft Report (v.0.0.4)	SA WG3 Secretary	5.7	Information		Noted
S3-030339	Cover Note to “3GPP Dependencies on OMA Deliverables”	Ian Sharp (for TSG SA)	5.7	Discussion		Response LS in S3-030439
S3-030340	3GPP Specifications upgrading for Bootstrapping and Subscriber Certificates	Nokia	7.9	Information		LS to CN4, CN1 in S3-030458
S3-030341	Transaction identifier location in protocol A	Nokia	7.9	Discussion / Decision		Attached Pseudo-CR content to be included in LS (S3-030458)
S3-030342	Pseudo-CR to Support for Subscriber Certificates: Protocol C in stage 3 detail	Nokia	7.9	Approval		Noted and attached to LS in S3-030458
S3-030343	Pseudo-CR to Support for Subscriber Certificates: Protocol D in stage 3 detail	Nokia	7.9	Approval		Noted and attached to LS in S3-030458
S3-030344	Pseudo-CR to Support for Subscriber Certificates: Support of operator control for certificate issuing	Nokia	7.9	Approval		Approved for inclusion in draft TS
S3-030345	Pseudo-CR to Support for Subscriber Certificates: Clarification of the authentication mechanism of the TS	Nokia	7.9	Approval		Approved for inclusion in draft TS
S3-030346	WITHDRAWN - WLAN – Implications of the trust relation between the Cellular Operator and the WLAN Access Provider	Ericsson	7.10	Discussion / Decision	S3-030369	Withdrawn and replaced by S3-030369
S3-030347	CMPv2 profile for 3GPP subscriber certificate enrolment	SSH Communications Security	7.9	Discussion / Decision		Noted (objections receieved)
S3-030348	Interface Naming in Bootstrapping System	Nokia	7.9	Discussion / Decision		I/F Names agreed. LS to SA2 in S3-030457
S3-030349	MBMS re-keying: PTP with periodic re-keying	Huawei Technologies	7.20	Discussion / Decision		Noted
S3-030350	Proposed CR to 33.210: Change of IKE profiling (Rel-5)	T-Mobile, Siemens	7.3	Approval		Approved
S3-030351	Draft TS 33.abc: Presence Service; Security. Version 0.5.0	Ericsson	7.18	Information		Noted. Includes agreements from last meeting
S3-030352	SA WG3 LI Group CRs Approved by e-mail	SA WG3 LI Group	5.1	Information		Noted (CR already approved by e-mail)
S3-030353	DRAFT Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #2/03 on lawful interception	SA WG3 LI Group	5.1	Information		Noted
S3-030354	Proposed CR to 33.210: Change of IKE profiling (Rel-6)	T-Mobile, Siemens	7.3	Approval		Approved as Cat "A"

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030355	Support for Subscriber Certificates	SchlumbergerSema	7.9	Discussion / Decision		Agreed to send LS to OMA SG in S3-030459
S3-030356	MBMS Security Framework	Qualcomm Europe	Joint Session	Discussion		Presented and noted
S3-030357	Generic secure message exchange using HTTP Digest Authentication	Nokia	7.9	Discussion / Decision		Agreed for inclusion in inf annex
S3-030358	DRAFT 3GPP TS 33.246 V0.1.1 (MBMS Security)	Editor	7.20	Information		Noted
S3-030359	Rationale of Presence service and Authentication Proxy functionality in detail	Nokia	7.18	Discussion / Decision		Discussed. LS to be drafted for next meeting (T. Haukka)
S3-030360	Levels of Key Hierarchy for MBMS	Qualcomm Europe	7.20	Discussion		Noted
S3-030361	Enhanced Security for A/Gb	Ericsson	7.6	Discussion / Decision		Proposals expected S3#29
S3-030362	Pseudo-CR to 33.234: Alignment with WLAN architecture definition (WLAN Security)	Ericsson	7.10	Approval		Approved for inclusion in draft TS. Sect 4.1.1 depends on SA2 output
S3-030363	Pseudo-CR to 33.234: Co-Existence of RADIUS and Diameter (WLAN Security)	Ericsson	7.10	Approval		Approved for inclusion in draft TS
S3-030364	Pseudo-CR to 33.234: Clarification on pseudonyms (WLAN Security)	Ericsson	7.10	Approval		Approved for inclusion in draft TS
S3-030365	Pseudo-CR to 33.234: WLAN UE Functional Split (WLAN Security)	Ericsson	7.10	Approval		Approved for inclusion in TS (change to 2nd bullet)
S3-030366	Pseudo-CR to 33.246: Confidentiality protection of MBMS multicast data (MBMS Security)	Ericsson	7.20	Approval		Approved for inclusion in draft (with modifications)
S3-030367	Access to Application Servers using HTTP in MBMS	Ericsson	7.20	Discussion / Decision		For further study and discussion in MBMS Ad-hoc
S3-030368	Introducing SRTP and MIKEY in TS 33.246 (MBMS Security)	Ericsson	7.20	Discussion / Decision		Pseudo-CR attached. Divergent from 3GPP2 scheme. To be discussed in MBMS ad-hoc
S3-030369	WLAN – Implications of the trust relation between the Cellular Operator and the WLAN Access Provider	Ericsson	7.10	Discussion / Decision		To be used in Trust Model e-mail discussion
S3-030370	HTTP Digest AKAv2 status and SQN issues	Ericsson	5.2	Information		Good confidence for completion by end of year. Section 5.3 to be studied for impacts on 3GPP.
S3-030371	Access to Application Servers using HTTP in Presence/Ut interface	Ericsson	7.18	Discussion / Decision		Discussed. LS to be drafted for next meeting (T. Haukka)
S3-030372	Profiling of RFC3325	Ericsson	7.1	Discussion / Decision		To be added to LS in S3-030454
S3-030373	Proposed CR to 33.203: Trust Domain and the definition of SPEC(T) (Rel-6)	Ericsson	7.1	Approval		Revised in S3-030456
S3-030374	Key Expansion function for IMS/Presence	Ericsson	7.1	Discussion / Decision		Proposal to use triple-DES key expansion agreed
S3-030375	Proposed CR to 33.203: Introducing Cipher key Expansion for IMS (Rel-6)	Ericsson	7.1	Approval		Approved (Rel-6)

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030376	Make a split between TS33.203 and Presence	Ericsson	7.1	Discussion / Decision		Proposal to create TS for Presence Security agreed. CRs in S3-030377 and S3-030378
S3-030377	Proposed CR to 33.203: Introducing the Privacy mechanism (Rel-6)	Ericsson	7.1	Approval		CR to be forwarded to CN1, SA2 cc SA1 for comment. LS in S3-0303454
S3-030378	Proposed CR to 33.203: Introducing Confidentiality Protection for IMS (Rel-6)	Ericsson	7.1	Approval	S3-030455	Revised in S3-030455
S3-030379	NDS/AF – Fetching Cross-Certificates	Nokia, Siemens, SSH, T-Mobile	7.4	Discussion		Pseudo-CR in S3-030380. Noted
S3-030380	Pseudo-CR to NDS/AF: Fetching cross-certificates	Nokia, Siemens, SSH, T-Mobile	7.4	Approval		e-mail approval
S3-030381	Proposal for NDS/AF draft TS v0.4.0	Nokia, Siemens, SSH, T-Mobile	7.4	Discussion / Decision		e-mail approval
S3-030382	Generation and storage of the UE's public/private key pair associated to the requested certificate	GemPlus	7.9	Discussion / Decision		Contribution on risk analysis invited to next meeting
S3-030383	Pseudo-CR to 33.234: Support for interleaving authentication (WLAN Security)	Siemens	7.10	Approval		Approved with clarification of index value is an example
S3-030384	Pseudo-CR to ab.cde (NDS/AF): Addition of a Clause on backward compatibility to NDS/IP	Siemens, Nokia, SSH, T-Mobile	7.4	Approval		e-mail approval
S3-030385	Pseudo-CR to NDF/AF: Addition of a Clause on CRL Management within the SEG	Nokia, Siemens, SSH, T-Mobile	7.4	Approval		e-mail approval
S3-030386	Pseudo-CR to NDF/AF: Handling critical and non critical certificate extensions	Nokia, Siemens, SSH, T-Mobile	7.4	Approval		e-mail approval
S3-030387	Pseudo-CR to NDF/AF: Additions to the clause 5.3 on profiling of certificates	Nokia, Siemens, SSH, T-Mobile	7.4	Approval		e-mail approval
S3-030388	Pseudo-CR to NDF/AF: Addition of text on usecases	Nokia, Siemens, SSH, T-Mobile	7.4	Approval		e-mail approval
S3-030389	Proposed CR to 55.216: Clarification on the usage of the Key length (Rel-6)	Siemens	5.3	Approval	S3-030438	Agreed that new TS will be provided for A5/4 and GEA4. CR updated in S3-030438
S3-030390	Proposed CR to 33.102: Clarification on the usage of the c3 conversion function	Siemens, Nokia, T-Mobile	7.5	Approval	S3-030465	Revised in S3-030465
S3-030391	Comparison of different approaches in the Presence/Ut interface	Nokia, Ericsson	7.18	Discussion / Decision		Discussed. LS to be drafted for next meeting (T. Haukka)
S3-030392	Proposed WID: Key Management of group keys for Voice Group Call Services	Vodafone D2	8	Approval	S3-030464	Revised time plan in S3-030464
S3-030393	Authentication in MBMS	Alcatel	7.20	Discussion / Decision		To be discussed further in MBMS ad-hoc
S3-030394	Proposed CR to 33.108: Reference errors in Annex G (Rel-5)	Lucent Technologies	4.3	Approval		Approved
S3-030395	Proposed CR to 33.108: Reference errors in Annex G (Rel-6)	Lucent Technologies	4.3	Approval		Approved
S3-030396	Key distribution and billing in PayTV model	Gemplus, Oberthur	7.20	Discussion / Decision		To be discussed further in ad-hoc
S3-030397	User authentication by Service Platforms	Nortel Networks	7.9	Discussion / Decision		More architecture work needed

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030398	Pseudo-CR to 33.234: Clarification to Annex B.2 Trust Relation Editor's Note (WLAN Security)	AT&T Wireless Services	7.10	Approval		Approved for inclusion in main body of TS
S3-030399	SA Lifetimes	3, Ericsson, Lucent	7.1	Discussion / Decision		Proposed replies to LSs and proposals for CR to 33.203
S3-030400	IMS watcher authentication	Nokia	7.18	Discussion / Decision		Discussed. LS to be drafted for next meeting (T. Haukka)
S3-030401	MBMS Security Requirements Clarification	Nortel Networks	7.20	Discussion / Decision		Conclusion 2 agreed if ongoing work not stopped. Pseudo-CR to be re-edited into editors note
S3-030402	Effects of service 27/38 on 2G/3G Interworking and emergency call	Siemens	7.5	Discussion / Decision		e-mail discussion to decide what to do with info
S3-030403	MBMS authentication architectures evaluation	Siemens	7.20	Discussion / Decision		To be discussed further in MBMS ad-hoc
S3-030404	Proposed CR to 33.210: Update draft-ietf-ipsec-sctp-03.txt reference to new standard RFC: RFC3554 (Rel-5)	Siemens	7.3	Approval		Approved
S3-030405	Proposed CR to 33.210: Update draft-ietf-ipsec-sctp-03.txt reference to new standard RFC: RFC3554 (Rel-6)	Siemens	7.3	Approval		Approved
S3-030406	Pseudo CR to Presence Security Draft: Authentication of IMS subscriptions for Presence Service	Nokia	7.18			
S3-030407	Bootstrapping and subscriber certificate use cases	Nokia	7.9	Discussion		Noted
S3-030408	Reliable key distribution mechanism	Samsung Electronics	7.20	Discussion / Decision		To be discussed further in ad-hoc
S3-030409	Some consideration about Ciphering Key usage timing	Samsung Electronics	7.20	Discussion / Decision		Conclusions of analysis agreed. S3 neeed further study of mechanism
S3-030410	Loose Coupling Interworking Issues	Siemens	6 (Joint Session)	Information		Presented and noted
S3-030411	Key provision in bootstrapping of application security	Siemens	7.9	Discussion / Decision		Pseudo CR in 3.1 postponed for more contribution. Pseudo-CR in 3.2 accepted
S3-030412	HSS/HLR-related security architecture issues and implications for presence, MBMS and support for subscriber certificates	Siemens	7.20	Discussion / Decision		Drafting session to elaborate guidelines
S3-030413	Evaluation of proposals for security at the Ut (formerly: Mt) reference point	Siemens	7.18	Discussion / Decision		Discussed. LS to be drafted for next meeting (T. Haukka)
S3-030414	Consequences of the WLAN trust model?	Siemens	7.10	Discussion / Decision		To be used in Trust Model e-mail discussion
S3-030415	Discussion paper on solutions regarding the behaviour of SIP over TCP and SA handling in re-authentications	Siemens	7.1	Discussion		Further study required
S3-030416	Proposed CR to 33.203: Alignment of security association handling and behaviour of SIP over TCP (Rel-5)	Ericsson / Lucent / Siemens	7.1	Approval		Cover page error: Intended Rel-5. Principles agreed and included in updated version in S3-030445 and S3-030461

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030417	Delta Changes to TS 33.203 on Security Association Handling in Re-authentications	Siemens	7.1	Discussion		CR in S3-030461
S3-030418	Proposed CR to 33.203: Security association handling, behaviour of SIP over TCP and re-authentication (Rel-6)	Lucent / Siemens	7.1	Approval		Covered by CR in S3-030461
S3-030419	Technical Report on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6)	Toshiba, Intel, T-Mobile, Nokia, Telcordia, Thomson, Fujitsue, HP, RIM, SmartTrust, BT Group PLC, Alcatel	7.15	Information	S3-030420	(Late document): Replaced by S3-030420 due to error in Company name spelling (Fujitsu)
S3-030420	Technical Report on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6)	Toshiba, Intel, T-Mobile, Nokia, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel	7.15	Information		(Late document due to transmission delays by list server): To be discussed in ad-hoc if time
S3-030421	Proposed CR to 33.203: Annex H in 33.203 (Rel-5)	Ericsson	7.1	Approval	S3-030445	(Late document due to rejected posting by e-mail exploder): Cover sheet wrong Rel = Rel-5. Principles of CR agreed. Updated and included in S3-030445 and S3-030461
S3-030422	SA handling regarding to the lifetime of SA	Nokia	7.1	Discussion / Decision		(Late document): Dealt with in Drafting meeting.
S3-030423	Proposed CR to 33.203: Removal of SA lifetime (Rel-5)	Nokia	7.1	Approval		(Late document): Dealt with in Drafting meeting.
S3-030424	LS (from SA WG2) on usage of GUP reference points	SA WG2	7.17	Information		Response via e-mail (B Owen to lead)
S3-030425	LS (from SA WG2) on Security issues regarding multiple PDP contexts in GPRS	SA WG2	7.10; 7.6	Information		Noted
S3-030426	LS (from SA WG2) on 802.11i / WPA and RADIUS to Diameter co-existence analysis and recommendations for WLAN interworking	SA WG2	7.10	Information		Noted
S3-030427	LS (from SA WG2) on PDG IP address discovery using public DNS for WLAN interworking	SA WG2	7.10	Action		C Blanchard to lead e-mail discussion and provide response LS
S3-030428	LS (from SA WG2) on Denial of Service attacks against the 3GPP WLAN Interworking system	SA WG2	7.10	Action		LS to be provided over e-mail (A Palanigounder) by 15 August
S3-030429	LS from SA WG2: Response to LS on clarification of USIM-based access to IMS	SA WG2	7.1	Action		Reply in S3-0304443
S3-030430	Liaison (from SA WG2) on Security Solutions for the Ut Reference Point	SA WG2	7.18	Information		Noted
S3-030431	Liaison (from SA WG2) on SIP signalling interworking	SA WG2	7.1	Action		Noted. SA WG3 specs to be updated when 23.228 is updated.
S3-030432	LS (from SA WG2) on Security Implications of Gq interface	SA WG2	7.1	Action		Contribution invited to next meeting for security mechanisms needed for the Gq interface (e.g. NDS). Response LS in S3-030444

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030433	LS (from SA WG2) on the recommendation from IREG of non publicly routable IP addresses for the GPRS nodes	SA WG2	7.10	Action		S. Nguyen Ngoc to lead e-mail discussion and provide response LS
S3-030434	LS (from SA WG4) on DRM for Progressive Download	SA WG4	7.20	Information		SA WG3 to monitor work. Noted
S3-030435	LS from OMA: Mobile PKI service enabler	OMA SEC / SCT WG	5.7	Action		Reply LS in S3-030459
S3-030436	SIM access via 'SIM Access Profile' and Bluetooth link	Ericsson		Discussion		Re-submitted for discussion from meeeting#28
S3-030437	draft LS on clarification of MBMS charging issues (T Viitanen)	SA WG3	7.20	Approval	S3-030453	Not agreed during e-mail discussions - (further discussed at meeting). Revised in S3-030453
S3-030438	Proposed CR to 55.216: Clarification on the usage of the Key length (Rel-6)	Siemens	5.3	Approval		Approved
S3-030439	Reply to Letter "3GPP Dependencies on OMA Deliverables" (S3-030339)	SA WG3	5.7	Approval		Approved
S3-030440	Reply LS to S3-030323 on "known and unknown" SIP message handling (Shirat)	SA WG3	7.1	Approval	S3-030466	Revised in S3-030466
S3-030441	Response LS on Security Association Lifetime Management	SA WG3	6.1	Approval		Approved
S3-030442	Proposed CR to 33.203: Modification of the security association lifetime management (Rel-5)	SA WG3	6.1	Approval		Approved
S3-030443	Draft Response to LS on clarification of USIM-based access to IMS	SA WG3	7.1	Approval	S3-030467	Revised in S3-030467
S3-030444	Reply LS to SA WG2 on Gq interface (Geir)	SA WG3	7.1	Approval		Approved
S3-030445	Proposed CR to 33.203: Annex H in 33.203 (Rel-5)	SA WG3	7.1	Approval		Approved
S3-030446	Reply (from SA WG1) to Liaison Statement on "MBMS Codec Requirements	SA WG1	7.20	Information		Noted
S3-030447	LS (from SA WG1) on requirements on security for the Mt reference point	SA WG1	7.18			Noted
S3-030448	Reply LS (from SA WG1) on "Security issues regarding multiple PDP contexts in GPRS"	SA WG1	7.10	Action		Noted. Contribution invited on threats
S3-030449	Reply LS (from SA WG1) on WLAN Interworking requirements for SIM and USIM	SA WG1	7.10	Information		Noted
S3-030450	Slides for joint Meeting 3GPP / 3GPP2	3GPP2 S4 Chairman (M Marcovici)	5.5	Information		Noted
S3-030451	Presentation Slides: BCMCS Security Framework	Qualcomm	5.5	Information		Noted
S3-030452	3GPP2 S.P0083 v0.7: Broadcast-Multicast Service Security Framework	Qualcomm	5.5	Information		Not discussed, for info only
S3-030453	draft LS on clarification of MBMS charging issues (P Howard)	SA WG3	7.20	Approval	S3-030472	Revised in S3-030472
S3-030454	DRAFT LS on Profiling of RFC3325 for IMS	SA WG3	7.1	Approval	S3-030468	Revised in S3-030468
S3-030455	Proposed CR to 33.203: Introducing Confidentiality Protection for IMS (Rel-6)	Ericsson	7.1	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-030456	Proposed CR to 33.203: Trust Domain and the definition of SPEC(T) (Rel-6)	Ericsson	7.1	Approval		Cleaned up version of S3-030373. For adding to LS in S3-030454
S3-030457	[DRAFT] LS on new interface names	SA WG3	7.9	Approval	S3-030471	Revised in S3-030471
S3-030458	[DRAFT] Stage 3 level specification directions for support for subscriber certificate work item	SA WG3	7.9	Approval	S3-030469	Revised in S3-030469
S3-030459	LS on “Mobile PKI service enabler”	SA WG3	7.9	Approval		Approved <DELAY transmission UNTIL SA permission>
S3-030460	HSS/HLR-related security architecture guidelines	Ericsson, Nokia, Nortel Networks, Siemens, T-Mobile, Vodafone	7.9	Discussion / Decision		Approved
S3-030461	Proposed CR to 33.203: Security association handling, behaviour of SIP over TCP and re-authentication (Rel-5)	3, Ericsson, Lucent, Siemens	7.1	Approval		Approved
S3-030462	WITHDRAWN Proposed CR to 33.203: Clarification to USIM based access to IMS (Rel-5)					WITHDRAWN
S3-030463	Cipher key separation for A/Gb security enhancements	Vodafone	7.5	Discussion / Decision		Delegates to study for next meeting
S3-030464	Proposed WID: Key Management of group keys for Voice Group Call Services	Vodafone D2	8	Approval		Approved
S3-030465	Proposed CR to 33.102: Clarification on the usage of the c3 conversion function	Siemens, Nokia, T-Mobile	7.5	Approval		Approved
S3-030466	[DRAFT] Response to LS on transport of unknown SIP signalling elements	SA WG3	7.1	Approval	S3-030470	Revised in S3-030470
S3-030467	Draft Response to LS on clarification of USIM-based access to IMS	SA WG3	7.1	Approval		Approved
S3-030468	DRAFT LS on Profiling of RFC3325 for IMS	SA WG3	7.1	Approval		Approved
S3-030469	LS on Stage 3 level specification directions for support for subscriber certificate work item	SA WG3	7.9	Approval		Approved
S3-030470	Response to LS on transport of unknown SIP signalling elements	SA WG3	7.1	Approval		Approved
S3-030471	LS on new interface names	SA WG3	7.9	Approval		Approved
S3-030472	LS on clarification of MBMS charging issues (P Howard)	SA WG3	7.20	Approval		Approved
S3-030473	Response to LS in S3-030337 (G Horn)	SA WG3	7.20	Approval		Approved by e-mail 28 July 2003

Annex C: Status of specifications under SA WG3 responsibility

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

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	3.2.0	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	3.1.2	R99	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
Release 4 3GPP Specifications and Reports							
TS	21.133	3G security; Security threats and requirements	4.1.0	Rel-4	S3	CHRISTOFFERSSON, Per	
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	4.1.0	Rel-4	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards).
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	4.0.0	Rel-4	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031.
TS	23.035	Immediate Service Termination (IST); Stage 2	4.1.0	Rel-4	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards).
TS	33.102	3G security; Security architecture	4.5.0	Rel-4	S3	BLOMMAERT, Marc	
TS	33.103	3G security; Integration guidelines	4.2.0	Rel-4	S3	BLANCHARD, Colin	
TS	33.105	Cryptographic Algorithm requirements	4.1.0	Rel-4	S3	CHIKAZAWA, Takeshi	
TS	33.106	Lawful interception requirements	4.0.0	Rel-4	S3	WILHELM, Berthold	
TS	33.107	3G security; Lawful interception architecture and functions	4.3.0	Rel-4	S3	WILHELM, Berthold	
TS	33.120	Security Objectives and Principles	4.0.0	Rel-4	S3	WRIGHT, Tim	
TS	33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	4.3.0	Rel-4	S3	ESCOTT, Adrian	2001-05-24: title grows MAP; see 33.210 for IP equivalent.
TR	33.901	Criteria for cryptographic Algorithm design process	4.0.0	Rel-4	S3	BLOM, Rolf	
TR	33.902	Formal Analysis of the 3G Authentication Protocol	4.0.0	Rel-4	S3	HORN, Guenther	
TR	33.903	Access Security for IP based services	none	Rel-4	S3	VACANT,	
TR	33.908	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	4.0.0	Rel-4	S3	WALKER, Michael	TSG#7: S3-000105=NP-000049

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
TR	33.909	3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions	4.0.1	Rel-4	S3	WALKER, Michael	TSG#7: Is a reference in 33.908. Was withdrawn, but reinstated at TSG#10.
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	4.1.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.205	3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE. 2002-06: clarified that deliverable is TS not TR.
TS	35.206	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TS	35.207	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	4.0.0	Rel-4	S3	WALKER, Michael	ex SAGE
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	4.0.1	Rel-4	S3	WRIGHT, Tim	
TR	41.033	Lawful Interception requirements for GSM	4.0.1	Rel-4	S3	MCKIBBEN, Bernie	
TS	41.061	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	4.0.0	Rel-4	S3	WALKER, Michael	
TS	42.009	Security Aspects	4.0.0	Rel-4	S3	CHRISTOFFERSSON, Per	
TS	42.033	Lawful Interception; Stage 1	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
TS	43.020	Security-related network functions	4.0.0	Rel-4	S3	GILBERT, Henri	

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
TS	43.033	Lawful Interception; Stage 2	4.0.0	Rel-4	S3	MCKIBBEN, Bernie	
Release 5 3GPP Specifications and Reports							
TS	22.022	Personalisation of Mobile Equipment (ME); Mobile functionality specification	5.0.0	Rel-5	S3	NGUYEN NGOC, Sebastien	Transfer>TSG#4
TS	22.031	Fraud Information Gathering System (FIGS); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 02.31 R99 and 42.031 Rel-4 & Rel-5 -> 22.031.
TS	22.032	Immediate Service Termination (IST); Service description; Stage 1	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 02.32 (R99) and 42.032 (Rel-4 onwards).
TS	23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	5.0.0	Rel-5	S3	WRIGHT, Tim	SP-18: decided FIGS is joint GERAN/UTRAN so 03.31 R99 and 43.031 Rel-4 & Rel-5 -> 23.031.
TS	23.035	Immediate Service Termination (IST); Stage 2	5.1.0	Rel-5	S3	WRIGHT, Tim	SP-16: created to take over from 03.35 (R99) and 43.035 (Rel-4 onwards).
TS	33.102	3G security; Security architecture	5.2.0	Rel-5	S3	BLOMMAERT, Marc	
TS	33.106	Lawful interception requirements	5.1.0	Rel-5	S3	WILHELM, Berthold	
TS	33.107	3G security; Lawful interception architecture and functions	5.5.0	Rel-5	S3	WILHELM, Berthold	
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	5.4.0	Rel-5	S3	WILHELM, Berthold	2001-12-04 Title changed from "Lawful Interception; Interface between core network and law agency equipment" (Berthold.Wilhelm@RegTP.de).
TS	33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	5.1.0	Rel-5	S3	ESCOTT, Adrian	2001-05-24: title grows MAP; see 33.210 for IP equivalent.
TS	33.201	Access domain security	none	Rel-5	S3	POPE, Maurice	
TS	33.203	3G security; Access security for IP-based services	5.6.0	Rel-5	S3	BOMAN, Krister	
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	5.4.0	Rel-5	S3	KOIEN, Geir	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210).
TR	33.900	Guide to 3G security	0.4.1	Rel-5	S3	BROOKSON, Charles	
TR	33.903	Access Security for IP based services	none	Rel-5	S3	VACANT,	
TS	35.201	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.202	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.203	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.204	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE; supplied by ETSI under licence
TS	35.205	3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE. 2002-06: clarified that deliverable is TS not TR.

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
TS	35.206	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification	5.1.0	Rel-5	S3	WALKER, Michael	ex SAGE
TS	35.207	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE
TS	35.208	3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE
TR	35.909	3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation	5.0.0	Rel-5	S3	WALKER, Michael	ex SAGE
TR	41.031	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	5.0.0	Rel-5	S3	WRIGHT, Tim	
TR	41.033	Lawful Interception requirements for GSM	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	
TS	42.033	Lawful Interception; Stage 1	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	
TS	43.020	Security-related network functions	5.0.0	Rel-5	S3	GILBERT, Henri	
TS	43.033	Lawful Interception; Stage 2	5.0.0	Rel-5	S3	MCKIBBEN, Bernie	
Release 6 3GPP Specifications and Reports							
TS	33.108	3G security; Handover interface for Lawful Interception (LI)	6.2.0	Rel-6	S3	WILHELM, Berthold	2001-12-04 Title changed from "Lawful Interception; Interface between core network and law agency equipment" (Berthold.Wilhelm@RegTP.de).
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security	6.2.0	Rel-6	S3	KOIEN, Geir	2001-05-24: 33.200 split into MAP (33.200) and IP (33.210).
TR	33.810	3G Security; Network Domain Security / Authentication Framework (NDS/AF); Feasibility Study to support NDS/IP evolution	6.0.0	Rel-6	S3	N, A	2002-07-22: was formerly 33.910.
TS	55.205	Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8	6.0.0	Rel-6	S3	WALKER, Michael	Not subject to export control.
TS	55.216	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 1: A5/3 and GEA3 specification	6.1.0	Rel-6	S3	N, A	
TS	55.217	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data	6.1.0	Rel-6	S3	N, A	

Type	Number	Title	Ver at TSG#18	Rel	TSG/ WG	Editor	Comment
TS	55.218	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 3: Design and conformance test data	6.1.0	Rel-6	S3	N, A	
TR	55.919	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report	6.1.0	Rel-6	S3	N, A	

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

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WI
33.102	180	-	Rel-6	Clarification on the usage of the c3 conversion function	F	5.2.0	S3-29	S3-030465	SEC1
33.102	181	-	Rel-5	IMEISV retrieval before completion of security mode setup procedure	F	5.2.0	S3-29	S3-030478	LATE_UE
33.106	005	-	Rel-6	References	D	5.1.0	S3-29	S3-030352	SEC1-LI
33.107	031	-	Rel-5	Missing QoS Parameter in IRI	F	5.5.0	S3-29	S3-030352	SEC1-LI
33.107	032	-	Rel-6	TEL URL for IMS interception identity	B	5.5.0	S3-29	S3-030352	SEC1-LI
33.107	033	-	Rel-6	Stereo delivery to LEMF	D	5.5.0	S3-29	S3-030352	SEC1-LI
33.108	017	-	Rel-6	Correct Abbreviations in TS 33.108	D	6.2.0	S3-29	S3-030352	SEC1-LI
33.108	018	-	Rel-5	Syntax error in Annex B.3	F	5.4.0	S3-29	S3-030352	SEC1-LI
33.108	019	-	Rel-6	Syntax error in Annex B.3	A	6.2.0	S3-29	S3-030352	SEC1-LI
33.108	020	-	Rel-6	Inconsistency in Annex B.3	D	6.2.0	S3-29	S3-030352	SEC1-LI
33.108	021	-	Rel-6	Data Link Establishment and Sending part for ROSE operation	F	6.2.0	S3-29	S3-030352	SEC1-LI
33.108	022	-	Rel-6	Correction on the usage of Lawful Interception identifiers	F	6.2.0	S3-29	S3-030352	SEC1-LI
33.108	023	-	Rel-6	Subscriber controlled input clarification	F	6.2.0	S3-29	S3-030352	SEC1-LI
33.108	024	-	Rel-6	Field separator in subaddress	D	6.2.0	S3-29	S3-030352	SEC1-LI
33.108	025	-	Rel-5	Reference errors in Annex G	F	5.4.0	S3-29	S3-030394	SEC1-LI
33.108	026	-	Rel-6	Reference errors in Annex G	A	6.2.0	S3-29	S3-030395	SEC1-LI
33.203	042	-	Rel-6	Introducing Cipher key Expansion for IMS	B	5.6.0	S3-29	S3-030375	IMS-ASEC
33.203	043	-	Rel-5	Modification of the security association lifetime management	F	5.6.0	S3-29	S3-030442	IMS-ASEC
33.203	044	-	Rel-5	Annex H in 33.203	F	5.6.0	S3-29	S3-030445	IMS-ASEC
33.203	045	-	Rel-5	Security association handling, behaviour of SIP over TCP and re-authentication	F	5.6.0	S3-29	S3-030461	IMS-ASEC
33.203	046	-	Rel-6	Introducing Confidentiality Protection for IMS	B	5.6.0	S3-29	S3-030455	IMS-ASEC
33.210	011	-	Rel-5	Change of IKE profiling	F	5.4.0	S3-29	S3-030350	SEC-NDS-IP
33.210	012	-	Rel-6	Change of IKE profiling	A	6.2.0	S3-29	S3-030354	SEC-NDS-IP
33.210	013	-	Rel-5	Update draft-ietf-ipsec-sctp-03.txt reference to new standard RFC: RFC3554	F	5.4.0	S3-29	S3-030404	SEC-NDS-IP
33.210	014	-	Rel-6	Update draft-ietf-ipsec-sctp-03.txt reference to new standard RFC: RFC3554	A	6.2.0	S3-29	S3-030405	SEC-NDS-IP
55.216	002	-	Rel-6	Clarification on the usage of the Key length	F	6.1.0	S3-29	S3-030438	SEC1-CSALGO1

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	Source TD	Comment/Status
S3-030312	LS (from SA WG2) on unciphered IMEISV transfer	S2-032156	E-mail discussions for CR production and approval (M Blommaert, P Howard)
S3-030313	LS (from SA WG4) on DRM Content Format	S4-030366	Noted
S3-030314	Reply LS (from SA WG4) to "Reply to Liaison Statement on MBMS Codec Requirements"	S4-030415	Noted
S3-030315	Liaison response (from SA WG4) on LS on Protocols, Codecs and Media formats for MBMS	S4-030419	Noted
S3-030316	LS from T WG2: UE security aspects of the GUP architecture	T2-030263	Response via e-mail (B Owen to lead)
S3-030317	Draft TS ab.cde version 0.2.0: Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description (Release 6)		Noted
S3-030318	LS (from T WG3) on WLAN interworking	T3-030411	Noted
S3-030319	Response LS from T WG3: Re: LS on clarification of USIM-based access to IMS	T3-030430	Noted
S3-030320	Reply LS (from CN WG1) on 'Impacts on the UE of UE-Initiated Tunnelling"	N1-030817	Noted
S3-030321	Reply LS (from CN WG1) on unciphered IMEISV transfer	N1-030818	E-mail discussions for CR production and approval (M Blommaert, P Howard)
S3-030322	LS (From CN WG1 re: S3-030308) on increasing the key length for GEA3	N1-030820	Noted
S3-030323	LS (from CN WG1) on transport of unknown SIP signalling elements	N1-030896	Reply LS in S3-030440
S3-030324	LS (from CN WG1) on Security Association Lifetimes	N1-030918	Revised in S3-030330
S3-030325	LS (from CN WG1) on security solutions for the Ut reference point	N1-030933	Noted
S3-030326	LS (from CN WG4) on Security Issues regarding multiple access connections	N4-030663	Noted. No standardisation in NW at present
S3-030328	Response (from RAN WG2) to LS on double ciphering for MBMS multicast data	R2-031460	No need to pursue double ciphering any further. Noted
S3-030329	LS (from SA WG5) on usage of GUP reference points	S5-032227r5	Noted
S3-030330	LS (from CN WG1) on Security Association Lifetimes	N1-030918rev1 (S3-030324)	Related to S3-030336
S3-030336	LS (from TSG CN) on Security Association Lifetime Management	NP-030308	Used in Drafting meeting Output CR in S3-030442
S3-030337	LS (from CN WG4 on adapting Cx interface protocols for security purposes	N4-030722	Reply in S3-030473
S3-030339	Cover Note to "3GPP Dependencies on OMA Deliverables"		Response LS in S3-030439
S3-030424	LS (from SA WG2) on usage of GUP reference points	S2-032679	Response via e-mail (B Owen to lead)
S3-030425	LS (from SA WG2) on Security issues regarding multiple PDP contexts in GPRS	S2-032680	Noted
S3-030426	LS (from SA WG2) on 802.11i / WPA and RADIUS to Diameter co-existence analysis and recommendations for WLAN interworking	S2-032727	Noted
S3-030427	LS (from SA WG2) on PDG IP address discovery using public DNS for WLAN interworking	S2-032729	C Blanchard to lead e-mail discussion and provide response LS
S3-030428	LS (from SA WG2) on Denial of Service attacks against the 3GPP WLAN Interworking system	S2-032730	LS to be provided over e-mail (A Palanigounder) by 15 August

TD number	Title	Source TD	Comment/Status
S3-030429	LS from SA WG2: Response to LS on clarification of USIM-based access to IMS	S2-032731	Reply in S3-0304443
S3-030430	Liaison (from SA WG2) on Security Solutions for the Ut Reference Point	S2-032735	Noted
S3-030431	Liaison (from SA WG2) on SIP signalling interworking	S2-032737	Noted. SA WG3 specs to be updated when 23.228 is updated.
S3-030432	LS (from SA WG2) on Security Implications of Gq interface	S2-032745	Contribution invited to next meeting for security mechanisms needed for the Gq interface (e.g. NDS). Response LS in S3-030444
S3-030433	LS (from SA WG2) on the recommendation from IREG of non publicly routable IP addresses for the GPRS nodes	S2-032746	S. Nguyen Ngoc to lead e-mail discussion and provide response LS
S3-030434	LS (from SA WG4) on DRM for Progressive Download	S4-030510	SA WG3 to monitor work. Noted
S3-030435	LS from OMA: Mobile PKI service enabler		Reply LS in S3-030459
S3-030446	Reply (from SA WG1) to Liaison Statement on “MBMS Codec Requirements	S1-030870	Noted
S3-030447	LS (from SA WG1) on requirements on security for the Mt reference point	S1-030912	Noted
S3-030448	Reply LS (from SA WG1) on "Security issues regarding multiple PDP contexts in GPRS"	S1-030958	Noted. Contribution invited on threats
S3-030449	Reply LS (from SA WG1) on WLAN Interworking requirements for SIM and USIM	S1-030966	Noted

E.2 Liaisons from the meeting

TD number	Title	Comment/Status	TO	CC
S3-030439	Reply to Letter “3GPP Dependencies on OMA Deliverables” (S3-030339)	Approved	**Mr. Iain Sharp**	
S3-030441	Response LS on Security Association Lifetime Management	Approved	**TSG CN, CN WG1**	
S3-030444	Reply LS to SA WG2 on Gq interface (Geir)	Approved	**SA WG2**	
S3-030467	Draft Response to LS on clarification of USIM-based access to IMS	Approved	**SA WG2**	**SA WG1, T WG3**
S3-030468	DRAFT LS on Profiling of RFC3325 for IMS	Approved	**SA WG2, CN WG1**	**SA WG1**
S3-030469	LS on Stage 3 level specification directions for support for subscriber certificate work item	Approved	**CN WG1, CN WG4**	
S3-030470	Response to LS on transport of unknown SIP signalling elements	Approved	**CN WG1**	**SA WG2, SA WG5**
S3-030471	LS on new interface names	Approved	**SA WG2**	**CN WG1, CN WG4**
S3-030472	LS on clarification of MBMS charging issues (P Howard)	Approved	**SA WG1**	
S3-030459	LS on “Mobile PKI service enabler”	Approved **<DELAY transmission UNTIL SA permission>**	**OMA SEC / SCT WG**	**3GPP2 TSG-S WG4**
S3-030473	Reply to LS N4-030722 (=S3-030337) on adapting Cx interface protocols for security purposes	Approved by e-mail 28 July 2003	**CN WG4**	
S3-030474	LS on ‘Effects of service 27/38 on 2G/3G Interworking and emergency call’	Approved by e-mail 13 August 2003	**T WG3 CN WG1**	
S3-030475	Reply to LS on the recommendation from IREG of non publicly routable IP addresses for the GPRS nodes	Approved by e-mail 14 August 2003	**SA WG2**	**IREG, IREG Packet Group, GSMA WLAN Task Force, GSMA Security Group**
S3-030476	Reply to LS S2-03279 (=S3-030427) Address discovery using public DNS for WLAN interworking	Approved by e-mail 14 August 2003	**SA WG2**	

TD number	Title	Comment/Status	TO	CC
S3-030477	Reply to LS on DoS attacks against the 3GPP WLAN Interworking system	Approved by e-mail 14 August 2003	**SA WG2**	

Annex F: Actions from the meeting

AP 29/01: M Pope to get a new TS number for use to provide the draft A5/4 and GEA4 document.

AP 29/02: M Blommaert and P Howard to chair e-mail discussions on Early release IMEISV transfer and produce CRs for comment by 29 August, Approval 5 September 2003.

AP 29/03: M. Blommaert to run e-mail discussion to discuss what should be done with the information in TD S3-030402.

AP 29/04: A. Palanigounder to lead an e-mail discussion and draft an LS in response to TD S3-030428 (Denial of Service attacks against the 3GPP WLAN Interworking system). Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003.

AP 29/05: S. Nguyen Ngoc was asked to lead an e-mail discussion over LSs in TD S3-030433 and to produce a response LS. Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003.

AP 29/06: C. Blanchard to lead an e-mail discussion over LSs in TD S3-030427 and to produce a response LS. Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003.

AP 29/07: P. Howard to lead an e-mail discussion on Trust Model and provide a contribution to SA WG3 meeting#30.

AP 29/08: B. Owen to lead an e-mail discussion on TD S3-030316 (UE security aspects of the GUP architecture). Comments before 6 August, draft response LS 8 August and Approval for transmission 15 August 2003.

AP 29/09: G. Horn to lead an e-mail discussion on open issues related to Key Management of HTTP-based services. Deadline for collection of issues: 27 August 2003.

AP 29/10: Tao Haukka to provide draft LS to SA WG1 on IMS watcher authentication for discussion at SA WG3 meeting #30.

AP 29/11: C. Blanchard to set up a discussion group and elaborate the MBMS Key Management requirements based on TD S3-030335.

AP 29/12: M. Pope to check if an ad-hoc meeting can be held at ETSI premises 3-4 September 2003 (20 delegates).