3GPP TSG SA WG3 (Security) meeting #24 **Draft Report**

9-12 June 2002

Helsinki, Finland

Source:	**Secretary 3GPP TSG SA WG3 (M. Pope, MCC)**
Title:	**Report version 1.0.0**
Status:	**Approved**

DRAFT REPORT

Suomenlinna, Helsinki's Island Fortress:

Contents

1 Opening of the meeting

Prof. M. Walker, the SA WG3 Chairman opened the meeting. Sonera welcomed delegates to Helsinki and provided the domestic arrangements. A social event had been arranged by SSH and Nokia, for Wednesday evening.

2 Agreement of the agenda and meeting objectives

TD S3-020325 The draft agenda was approved.

2.1 3GPP IPR Declaration

Delegates were reminded of their Member Companies responsibilities under the 3GPP IPR agreement.

3 Assignment of input documents

The available input documents were assigned to their respective agenda items. A large number of documents had been sent to the list on Friday afternoon, and the Secretary was unable to retrieve them in time for the meeting. Also delegates didn't have enough time to review the contributions properly in their companies and a deadline for contributions was called for. **It was decided that for the next meeting, the previous Thursday, 17.00 CET was the deadline for any documents for discussion - any documents received after this deadline may not be discussed if there is not enough time in the meeting.**

4 Reports from 3GPP SA3 meetings

4.1 SA3#23, 13-16 May 2002

TD S3-020326 Draft report of SA WG3 meeting #23 - v0.0.5. The report was reviewed and some minor corrections suggested: Host of this meeting to be corrected to Nokia and Sonera. TS 33.108 (Annex C) - The rapporteur should be corrected to Ron Ryan. Annex E to be completed by Secretary. The approved version 1.0.0 will be placed on the FTP server.

4.2 SA3 LI #3/02, 4-6 June 2002

TD S3-020345 Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #3/02 on lawful interception - Budapest 4-6 June 2002. This was presented by B. Wilhelm. It was reportewd that B. Adams had been elected as a Vice Chairman of the LI group. The report was then noted.

TD S3-020348 CR to 33.106: Changes to 33.106 to clarify interception capabilities (Rel-5). It was considered that the phrasing of the changed text should be changed to allow provision of keys according to national regulations. This was revised in TD S3-020396 which was reviewed and approved.

TD S3-020346 CR to 33.107: Essential clarification to the Timestamp IE (Rel-5). This CR was approved.

TD S3-020347 CR to 33.107: Additional X3-interface parameters (Rel-5). This CR was approved.

TD S3-020351 CR to 33.108: Corrections to TS 33.108 (Rel-5). This CR was approved.

TD S3-020349 LS concerning Rapporteur to ETSI TC LI (Response to: LS (32TD050) on LS to 3GPP SA3 LI on work coordination from ETSI TC LI #32). This LS was noted.

TD S3-020350 LS on implications of the IPv6 auroconfiguration on LI. It was noted that no problems were expected from this. The LS was noted.

5 Report from SA#16, 10-13 June 2002

TD S3-020397 Report of SA WG3 activities at TSG SA#16:

1. *The chairman of CN4 reported that CN4 couldn't give guarantees that the stage 3 work on Ze-interface for MAPSEC can be completed before SA#17 plenary in September (see also an LS S3-020329). The SA plenary had earlier decided that the (first) release of MAPSEC automatic key management is agreed once the specification work is done. Based on these facts the SA plenary decided to postpone MAPSEC automatic key management beyond Release 5. As an administrative consequence, SA3 was requested to prepare a "reverse CR" to exclude the automatic key management from TS 33.200 Release 5. I propose SA3 prepares at the same time another CR which re-introduces automatic key management for TS 33.200 Release 6.*
2. *SA#16 was extremely sensitive on all Rel.99/Rel.4 CRs. It was decided that in the future a Rel.99/Rel.4 CR could be accepted only if there would be a system malfunction as a consequence of not approving the CR. For instance, clarifying CRs that are introduced in order to decrease the possibility of misinterpretations of specs are not allowed. Based on this principle, SA#16 rejected our proposed R99/R4 CR pair on ciphering indicator (S3-020250 and S3-020251). However, nobody questioned the fact that the feature is indeed mandatory. Similarly, our proposed CR pair on sequence numbers (S3-020308 and S3-020309) was rejected. The good news here is that SA#16 created an identical CR for Release 5.*
3. *All other CRs, including three other R99/R4 CR pairs, were accepted, some with minor editorial modifications. It was commented, and I agreed, that the term "plastic roaming" is wrong wording in the cover sheet of the CR about ISIM parameters (S3-020314). However, the actual change in the spec was OK with SA#16.*
4. *The WID on DRM security was approved. However, a revised version of the WID was requested for the next SA plenary, since time scales were missing and, also, "Service aspects" and "Charging aspects" need to be reworded.*
5. *Only the Feasibility Study part of our proposed WID "Network Domain Security; Authentication Framework" was approved. The SA plenary wants to see the results of the FS before deciding whether the rest of the work should be carried out. I modified the WID accordingly and the revised version was approved (SP-020387). As a practical consequence, we have to prepare a separate WID for the rest of the work (in case the FS implies the work should continue).*
6. *The LI spec TS 33.108 was approved in Release 5 and it is now under change control.*
7. *A strong role of SA3 was specifically requested for the work items of Presence and MBMS.*
8. *IST specs were renumbered as we requested (see SP-020403).*
9. *A new CR cover sheet template was created. The ISIM is now included in the boxes under "Proposed change affects" section as "UICC apps" replaces "(U)SIM" as the title of the first box. SA plenary expects that the new template (SP-020412) be taken into use at latest for all proposed CRs in SA#18.*

V Niemi was thanked for representing SA WG3 at the TSG SA plenary and the report was noted.

6 Reports and liaisons from other groups

6.1 3GPP working groups

TD S3-020327 SA WG1 Position Statement related to ITU-T request for information on activities related to Emergency Telecommunications Services (ETS). This was provided by SA WG1 for information and was reviewed and noted. **It was also noted that any security work identified for these Emergency Telecommunications Services would require contributions to the SA WG3 meeting, covering members' concerns**.

TD S3-020328 Response Liaison Statement on IMS Identities for R99/R4 UICC. this LS was noted.

TD S3-020329 LS from CN WG4 on Status of protocol work on Ze interface. The best way forward to remove the Ze interface work from the Rel-5 specifications was discussed. After some discussion on the way forward on this issue, it was agreed that CN WG4 should be asked for a enstination of timescales for the Ze interface specification work before agreeing on the best way forward. A LS was provided in TD S3-020398 which was approved. It was noted that 33.200 Rel-5 would need to be reverted back to the Rel-4 status for the Ze interface and this would be done when a response is available from CN WG4.

TD S3-020332 Answer from SA WG4 to "Liaison Statement on PSS Release 6 work programme". This LS was considered and noted.

TD S3-020334 LS from T WG3 on OFM and the IMS service. It was considered that the ciphering indicator is not a Feature within the IMS, but is applicable to the packet-bearer when the IMS service is used. It was agreed to draft a LS to T WG3 clarifying this distinction, which was provided in s3s applicable to the packet-bearer when the IMS service is used. It was agreed to draft a LS to T WG3 clarifying this distinction, which was provided in TD S3-020399 which was approved.

TD S3-020335 Response from T WG3 to "Liaison Statement on Access to IMS Services using 3GPP release 99 and release 4 UICCs" (S1-020577). This LS was considered and noted.

TD S3-020336 Liaison Statement from T WG3 on terminology regarding ISIM/USIM. This asked WGs to check their specifications to ensure they are in line with the current definition of ISIM, as agreed at TSG T#15. **K Boman agreed to check TS 33.203 and respond to the contact person for the LS (M. de Groot)**.

AP 24/01: K Boman agreed to check TS 33.203 for ISIM/USIM Terminology and respond to the contact person for the LS in TD S3-020336 (M. de Groot).

TD S3-020353 Reply to Liaison Statement on use of IP as transport for the Inter-GMLC Interface. This was provided by SA WG2 for information and was noted.

TD S3-020357 Answer to Liaison Statement regarding PSS Release 6 work programme. This was provided by SA WG2 for information and was noted.

TD S3-020438 LS from SA WG5: Reply on Packet Switched Streaming (PSS) in Rel-6 Work Programme. This was provided for information and noted.

TD S3-020439 LS from SA WG5 on Diameter security issues. SA WG5 asked SA WG3 whether DIAMETER base protocol is sufficient for a charging application. This had not been analysed yet by SA WG3 and so the TD was postponed to the next meeting.

6.2 IETF co-ordination

TD S3-020386 Status of SIP Security Agreement Draft in IETF. This was introduced by Ericsson and outlined the status of SIP-sec-agree draft in IETF. The document was noted.

G. Koien provided a verbal report on AES work still in pipe-line. Ciphering still under discussion. S-CTP has now been proposed as an RFC, (SA WG3 have already abandoned it's use in specifications as it was not thought likely to become an RFC). A major IPsec review has started in the IETF (beginning with a reveiew of IKE, which provided dual proposals, and they are trying to come to a convergent solution).

6.3 ETSI SAGE

TD S3-020388 Use of Kasumi-based functions for Group release security solution. This was introiduced by P Chrisoffersson, on behalf of ETSI SAGE. After an investigation, ETSI SAGE propose that f8 should be used for the Group Release mechanism. **SA WG3 considered the recommendations and would take them into account in the specification od the Group release mechanism**.

TD S3-020389 LS from ETSI SAGE: Advice on key expansion for HMAC-SHA-1-96. SAGE considered the expansion between the requirements of Key lengths and concluded that a simple key expansion scheme should be used if needed and proposed an alternative RFC that could be used, depending on conformance requirements. The advice from ETSI SAGE was then noted. A CR to include these recommendations in the standards was prepared by Ericsson in TD S3-020401 which was reviewed and updated in TD S3-020435 and approved.

TD S3-020360 SAGE deliverables A5/3. These were introduced as the output from the ETSI SAGE Task Force. The documents were approved for forwarding to TSG SA for approval at TSG SA meeting #17.

A press Release had appeared at the end of June 2002 from the A5/3 owners.

Concerning dates for implementation - some discussion was held on the formal way to specify these dates and who should mandate such dates. One way used sucessfully before is a guideline from the GSMA to operators. It was suggested that a date of 2 years from publication date. **Manufacturers were asked to check this suggestion and comment to C. Brookson (GSMA contact)**. C. Brookson agreed to write a letter to Manufacturers indicating the issues and suggested dates, requesting their views on this, provided in TD S3-020405 which was discussed and updated in TD S3-020440 which was approved.

6.4 GSMA SG

C. Brookson gave a verbal report on the GSMA SG. It was noted that 2 manufacturers had attended the previous meeting as invited and a further invitation to Manufacturers to attend was extended. Next meeting 18-19 September 2002 in Bristol, UK, hosted by Orange UK..

6.5 3GPP2

There were no specific contributions under this agenda item. It was reported that there had been a lot of discussion on the harmonisation issues for IMS in 3GPP2.

6.6 TIA TR-45

There were no specific contributions under this agenda item and no representation to provide a report to the meeting.

6.7 Other Groups

P. Howard provided a brief verbal report on the meeting with the European Commission. A Council resolution on Network Security was released this year and a group will be set up with 20 man-days' sponsorship to address the requirements. SA WG3 were identified as a group which may be impacted. A web site is available for more information:
http://www.etsi.org/frameset/home.htm?/public-interest/Network_Information_Security.htm.

7 Technical issues

7.1 IP multimedia subsystem (IMS)

TD S3-020400 Presentation on SA Handling (Ericsson). This was presented by Ericsson. A discussion paper and proposed CR to 33.102 on the subject was provided in TD S3-020361 which was then considered:

TD S3-020361: Many questions were raised over the introduction of this mechanism, which relies upon the use of Old SAs, in order to authenticate new SAs, and more time was needed to consider this. It was decided to return to this after other contributions and overnight study. This was combined with TD S3-020402 in TD S3-020443 (see below).

TD S3-020402 Proposed CR to 33.203: Update of SA handling procedures. This was introduced by Hutchison 3G UK. After discussion of this scheme, delegates were asked to also consider this overnight in order to come to a final decision at this meeting. This was combined with TD S3-020361 in TD S3-020443 (see below).

TD S3-020443 Proposed CR to 33.203: Update of SA handling procedures. This CR was introduced by Hutchison 3G UK. The CR was reviewed and many modifications were made to the wording of the proposals and the CR was updated in TD S3-020450 for use as a basis for further correction over e-mail after the meeting. **A. Escott agreed to update the document and send for approval. 2 weeks comments period (29 July) and 1 week to update (2 August) and send for approval. Approval deadline 16 August 2002.**

AP 24/02: A. Escott to update TD S3-020450 and send for approval. A 2 week comments period (29 July) and 1 week to update (2 August) and send for approval. Approval deadline 16 August 2002.

TD S3-020385 Profiling SIP Security Agreement for IMS Rel-5. This was introduced by Ericsson and proposes a new profiling scheme, allowing defaults to be used for ommitted parameters in the SIP messages (for increased efficiency potential). The principles of the scheme were accepted, and the associated CR considered in TD S3-020379.

TD S3-020379 Draft-ietf-sip-sec-agree syntax for manually keyed IPsec. This was introduced by Ericsson. Some problems were raised with the indication that a Null algorithm was default as this is specifically not allowed for IMS use. The CR was accepted in principle, recognising that other contributions may require revision to the wording if accepted, the CR was revised and provided in TD S3-020406 which was reviewed and updated in TD S3-020436 which was approved.

TD S3-020383 Proposed CR to 33.203: Removal of some editor notes in TS33.203. These changes were accepted in principle and related CRs also proposing to delete these notes were taken into account in order to prevent cross-over of CRs. This was done and the CR was then approved.

TD S3-020369 Proposed CR to 33.203: Correction to S-CSCF behaviour on Network Authentication Failure. This was re-introduced by Hutchison 3G UK, as it had been accepted at the previous meeting, and subsequently withdrawn from the set of agreed CRs as it was thought that it may be covered by other changes. The author explained that this had not been taken into account and re-wrote the CR to the updated version of 33.203. The editors note deletion was covered by TD S3-020383 and other clarifications were proposed, the CR was revised in TD S3-020407 which was approved.. A LS to CN WG1, to raise the point that an error message is missing, was drafted in TD S3-020408 which was approved.

TD S3-020370 Proposed CR top 33.203: Correcting the network behaviour in response to an incorrect AUT-S. This was re-introduced by Hutchison 3G UK, as it had been accepted at the previous meeting, and subsequently withdrawn from the set of agreed CRs as it was thought that it may be covered by other changes. The author explained that this had not been taken into account and re-wrote the CR to the updated version of 33.203. Editorial modifications and removal of the deletion of the editors note were needed and the CR was revised in TD S3-020409 which was approved.

TD S3-020371 Proposed CR to 33.203: Update of User Authentication Failure. This was re-introduced by Hutchison 3G UK, as it had been accepted at the previous meeting, and subsequently withdrawn from the set of agreed CRs as it was thought that it may be covered by other changes. The author explained that this had not been taken into account and re-wrote the CR to the updated version of 33.203. Editorial modifications and removal of the deletion of the editors note were needed and the CR was revised in TD S3-020410 which was modified again in TD S3-020442 and approved.

TD S3-020382 Proposed CR to 33.203: Mitigating reflection attacks in IMS. This was introduced by Nokia and proposes a simplification to the detection of reflection attacks at the P-CSCF instead of using direction bits which will non-compatible with de-facto IPSec solutions. There was some discussion on the reason for change and whether this is really wanted for 3GPP systems. It was agreed to update the reason for change with a clearer justification for making this change. An updated CR was provided in TD S3-020411 with a clearer definition of the *reasons for change* and *consequences if not approved*, and the CR was approved.

TD S3-020376 Proposed CR to 33.203: Protect port number to be assigned by UE in re-registration. This was introduced by Nokia. The reason for change was unclear and needed updating. The need for this which may be covered in 7.4 was questioned. It was clarified that the UE behaviour when it is not challenged is not specified and the UE needs to take a new port number for re-registration. The *reason for change* was updated in TD S3-020412 which was approved.

TD S3-020372 SA and registration lifetimes. This was introduced by Hutchison 3G UK. Two solutions for handling unauthenticated registrations were presented and after some consideration, the first was chosen (the expiry timer set to no longer than the longest remaining time of all registered IMPUs for that IMPI). It was decided to forwarded this with a LS to CN WG1, which was provided in TD S3-020415. After some discussion on the content of the LS, no agreement could be made in time, so the LS was **not approved**. **SA WG3 members were asked to talk to their CN WG1 colleagues in order to inform them of the current situation in SA WG3 and the need for a solution to this problem**. **Active discussion over the e-mail list was also encouraged in order to resolve this quickly at the next meeting.**

AP 24/03: A. Escott to initiate an e-mail discussion with SA WG3/CN WG1 on SA and registration lifetimes in order to have quick resolution of this issue at the next meeting.

TD S3-020374 Common IPsec SA for UDP and TCP sockets. This was introduced by Nokia and discussed the feasibility of sharing common IPsec SAs for UDP and TCP sockets. There was some discussion on the proposed change, from the proposed efficiency gain viewpoint, against the changes required to the Rel-5 specification.TD S3-020387 was considered for use in the justification of the proposed CR attached to the document. The CR was modified according to agreements and provided in TD S3-020416 which was approved. A LS to CN WG1 regarding these necessary changes was provided in TD S3-020417 which was approved (TD S3-020416 to be attached).

TD S3-020387 MitM attack for TCP Security Association negotiation. This was introduced by Ericsson and documents an attack for SA negotiation between UA and P-CSCF. The justification given here was accepted as useful for the CR provided by Nokia in TD S3-020374 and Ericsson were thanked for the analysis. The contribution was then noted.

TD S3-020375 Transport layer address in Via header. This was introduced by Nokia and corrects a mis-use of SIP header, and proposes the moving of the UE's IP address from the *Contact header* to the *Via header*. Siemens reported that a CN WG1 colleague had raised concerns over the use of the Via header, and suggested that the problem is reported to CN WG1 and ask them to find the appropriate solution for this protection. It was reported that a LS had been sent to CN WG1 on this at the previous meeting in TD S3-020316 which had not been dealt with yet by CN WG1.

TD S3-020380 Proposed CR to 33.203: Draft-ietf-sip-sec-agree syntax for manually keyed IPsec This was introduced by Ericsson. This issue had been discussed before and other solutions proposed and this CR was based on the agreed way forward. The CR was a clarification to prevent mis-implementation and was approved.

TD S3-020381 Proposed CR to 33.203: Attacker sends responses to requests intended for other parties. Other solutions were identified as possible, and evaluation of this was considered necessary. It was agreed to send this proposal to CN WG1 for evaluation and to re-consider it based upon comments received from CN WG1. A LS to CN WG3 requesting this was provided in TD S3-020418 which was modified slightly in TD S3-020441 and approved.

TD S3-020393 Proposed CR to 33.203: Correction of authentication vector distribution procedure. This was introduced by Vodafone and proposed a relaxation to the restriction on number of authentification vectors. The CR was updated to clarify it and to update the cover sheet and this was provided in TD S3-020419 which was approved. A LS to CN WG4 was required to whether this has any impact on their specifications, was provided in TD S3-020420 which was reviewed and modified slightly in TD S3-020437 which was approved.

TD S3-020404 Utilizing SIP parameter to handle SA database optimally in P-CSCF. This was introduced by Nokia. It was considered that Timer "F" could be better identified by reference to it's use in the CN WG1 specifications. Other definitions also needed updating. Nokia were asked to re-write the CR after consultation with CN WG1 colleagues and resubmit to SA WG3.

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

TD S3-020359 Security solution for UTRAN IP transport. This was introduced by Nokia and proposed the enhancement of NDS/IP specification to also cover the control plane of UTRAN IP transport (IP based Iu, Iur, Iub and Iupc interfaces) in Rel-6. There was some discussion over the use of IKE's successor protocol as there had been no analysis of the need for this change for Rel-6. It was agreed that SA WG3 needs to do this work, as already agreed with RAN WG3. It was decided that the WID should be updated and this was provided in TD S3-020422 which was reviewed and modified in TD S3-020444 which was approved.

TD S3-020368 COPS usage for IPSec policy management in NDS/IP. This was introduced by SSH Communications Security Corp. and proposes that SA WG3 take the usage of COPS as the working assumption for Rel-6 NDS/IP IPSec policy management. It was clarified that this is is not covered by existing (Rel-5) interfaces. After some discussion, it was agreed that the requirements for security management need to be collected and this would be further analysed once they are agreed.

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

There were no specific contributions under this agenda item.

7.4 UTRAN network access security

There were no specific contributions under this agenda item.

7.5 GERAN network access security

TD S3-020352 LS on A/Gb evolution. This LS from GERAN asked SA WG3 to consider their proposed solution to move ciphering from LLC to the radio access network when providing conversational services, and to review and provide comments on the A/Gb mode evolution feasibility study. It was thought that the Gb-Iu interface would need to be enhanced to provide the required security. The attached feasibility study was reviewed from a security point of view:

Should integrity protection be applied in Iu mode for GERAN? - The work done for UTRAN Iu-mode protection can be used as a basis for this. It was agreed that the level of protection needed for GERAN needs to be studied and agreed. (The WID for GERAN secutiry also needs to be updated for Rel-6 security enhancement work). It was agreed that an LS should be produced answering the open issues related to Security, where available, and informing GERAN where SA WG3 will study issues. It was noted that GERAN requested completion of this work by August, which was considered feasible and it was agreed to start the study and inform GERAN that the work is expected to be completed for their November meeting. Ane-mail discussion group was also set up to progress the study quickly, controlled by P. Howard. A LS to GERAN was prodiced informing them of the activities and asking for involvement in the e-mail exchange was provided in TD S3-020423 which was modified slightly in TD S3-020445 which was approved.

7.6 Immediate service termination (IST)

TD S3-020342 Proposed CR to 23.035: Correction of use IST Command message and Call Termination Indication parameter (R99). This was introduced by Ericsson and proposed an alignment between Stage 2 and Stage 3 for non-CAMEL IST. CN WG4 introduced an optimisation in 1999, which had not been taken account of in the stage 2 specification for IST (was GSM TS 03.35 - now 3GPP TS 23.035). This CR was approved.

TD S3-020343 Proposed CR to 23.035: Correction of use IST Command message and Call Termination Indication parameter (Rel-4). (Category A CR for Rel-4 version of IST Stage 2). This CR was approved.

TD S3-020344 Proposed CR to 23.035: Correction of use IST Command message and Call Termination Indication parameter (Rel-5). (Category A CR for Rel-5 version of IST Stage 2). This CR was approved.

TD S3-020394 Proposed CR to 22.032: Application of IST to PS services (Rel-5). Some concerns had been received by the author of this CR, which needed further study to address the issues. The current CR was reviewed to introduce the concepts for the required changes to the Stage 1 IST specification to include the specific PS requirements and clarify where items are particular to CS. The CR was **not approved,** as the issue needed further study and refinement. The Charging records should indicate that a call was terminated due to IST, but this is not reflected in SA WG5 specifications. It was agreed that a LS to SA WG5 should be produced to bring their attention to this. This LS was provided in TD S3-020424 which was modified in TD S3-020446 and approved.

An e-mail discussion group was set up to discuss IST issues, lead by P. Howard.

AP 24/04: P. Howard to lead an e-mail discussion group to discuss IST issues.

7.7 Support for subscriber certificates

TD S3-020333 LS from T WG2 on support for subscriber certificates. This was introduced by Nokia and asks SA WG3 to keep T WG2 informed of any documents and specifications dealing with the issue of subscriber certificates in the future. It was agreed to copy T WG2 on any communications. The LS was then noted.

TD S3-020356 LS on subscriber certificates (Response to S3-020322). This was introduced by Nokia and asks for more information on the issues for subscriber certificates, justification for using the link access instead of access independent, how roaming subscribers could be supported and the security requirements for issue and usage. Nokia had provided 2 contributions (TDs S3-020377, S3-020378) and Siemens 1 contribution (TD S3-020365), around this issue which were presented and discussed in order to form a basis for a reply to this LS in TD S3-020413 (reported below).

TD S3-020365 Analysis of Subscriber Certificates Concept. This was introduced by Siemens and outlined methods for dealing with subscriber certificates and outstanding issues to be considered (e.g. roaming). There were some ideas in common with the Nokia contributions, and some differences (e.g. requiremnet to include Proof Of Possession - POP, Nokia asked whether this will always be needed, and have not identified any currrent use-cases). Further study is needed to determine whether POP should be included to handle possible future use-cases.

TD S3-020377 Architecture alternatives for supporting subscriber certificates. This was introduced by Nokia and provided some potential solutions along with lists of their respective benefits and drawbacks. It was agreed that the proposed architctures need to be further reviewed and the advantages of the propsals over a "global" architecture needs to be determined. It was thought useful to provide this information to SA WG2 to indicate the sort of issues being studies by SA WG3.

TD S3-020378 Security and other requirements for subscriber certificates. This was introduced by Nokia and outlines the results of the study carried out by Nokia on the requirements for subscriber certificates and suggests these requirements are sent to SA WG2 and SA WG1.

During the discussion of contributions on this subject, the open issues were identified as more work on:

- **Requirements for POP and identification of use cases; (V. Niemi - lead e-mail discussion and report to next meeting)**
- **Compatibility with WAP; (S. Ward, included in next item discussion)**
- **Relationship and compatibility with m-commerce work and certificate work in other ETSI groups, IETF etc.; (S. Ward - lead e-mail discussion and report to next meeting)**
- **Involvement of SA WG1, particularly on roaming issues, Vistited Network issued certificates, resolution of disputes and user cases;**
- **access independence issues (advantages/drawbacks of different solutions - global PKI considerations); (P. Howard - lead e-mail discussion and report to next meeting)**
- **Lawful interception implications; (B. Wilhelm/C. Brookson - investigate and report to next meeting)**
- **Business relationships, Trust relationships, resolution of disputes (Trust issues). (P. Howard - lead e-mail discussion and report to next meeting)**

The above list may be added to as study progresses.

Delegates were asked to consider the above items and provide a summary of activities and issues to SA WG3. Volunteers for each item were found as indicated in the list.

AP 24/05: Various: People listed in Subscriber Certificates open issues list to progress discussions and report to next meeting.

TD S3-020413 LS to SA WG2, SA WG1, cc: T WG2 on Security activities and considerations for Subscriber Certificates. This was introduced by Nokia and discussed and modified in TD S3-020447 which was approved.

7.8 Digital rights management (DRM)

There were no specific contributions under this agenda item.

7.9 WLAN inter-working

TD S3-020392 Proposed WID draft 2: WLAN Interworking Security. This was introduced by BT Group. It was suggested that SA WG3 should aim for Access independent specifications in order to allow flexibility for future developments of access networks. It was recognised that full access independence was probably not possible, but it was agreed that this should be done as far as possible in the work. The WID was updated to reflect the comments made and provided in TD S3-020425 which was updated in TD S3-020451 which was approved.

TD S3-020354 Liaison statement on 3GPP System to WLAN Inter working. SA WG2 requested that SA WG3 review the draft of the TR on WLAN interworking and comment. The requirements were reviewed briefly, and some discussion about the requirements ensued. It was recognised that some modifications to the document would be desirable, and issues should be documented, e.g.:

- UE notation, Level of authentication / In principle, equivalent to UTRAN access security.
- Scenarios supported by architecture.
- Timescale of September 2002 is not possible for SA WG3 work.
- Can AP and Access Server be separate? - if so, what is the protocol to be used between them?
- Access to HIPERLAN2, Bluetooth, etc. to be clarified.
- EAP/AKA authentication: Are other methods ruled out intentionally?
- SA WG3 will create TS based on the TR.
- The protocol between the Access Point and Access Server was also considered in need of clarification as the security implications of this need to be identified.
- The WLAN UE - AAA Server Authentication needs further consideration. SA WG2 appear to have already specified the authentication methods to be used and this may require discussion.
- It was agreed that SA WG3 should help in further elaboration of the Stage 2 TR and produce a TS based upon the principles.

A Liason Statement to SA WG2 was provided in TD S3-020426 and was updated in TD S3-020452 and was approved.

TD S3-020390 Draft TR: Wireless Local Area Network (WLAN) Interworking Security. This was presented by the editor (Ericsson). A comment on 5.1.2 where implementation of the SIM/USIM application in software should be removed as no decision on allowing implementation other than on the UICC has not yet been made. The creation of a TR before the TS was questioned and it was agreed that it would be better to create the TS directly, focussing on the archtecture in the SA WG2 specification, due to timescales for the work. Mr. Luis Lopez Soria (Ericsson) agreed to be the editor for this work. Delegates were asked to review this TR and comment to the editor, who will update the TR (to become a TS) accordingly.

AP 24/06: L. Lopez Soriato update WLAN TS based on comments received for next meeting.

TD S3-020331 Reply from SA WG1 to the LS on WLAN Interworking. This was introduced by BT Group and asked SA WG3 to provide feedback on the understanding of SA WG1 outlined in the LS. The ownership and operations principles were accepted. For Internetworking Trust it was considered that the architecture proposed indicated a Radio Access rather than network interworking. Level of trust (1) was considered unreasonable, as a completely untrusted WLAN would not be connected to a 3GPP network. A trust model should be developed in SA WG3 to attach as an informative annex to the WLAN security TS. A reply LS to SA WG1 was provided in TD S3-020427 and was updated in TD S3-020453 and was approved.

TD S3-020337 Letter to SA WG3 Chairman: information about ongoing work on WLAN – 3G and other Public Access networks interworking. It was agreed to provide the draft WLAN security WID to inform the groups of work ongoing in SA WG3 and inviting representatives to the next SA WG3 meeting to discuss this work, and to copy the reply to SA WG2 for information. **This reply will be provided in TD S3-020428 by the SA WG3 Chairman after the meeting.**

AP 24/07: M. Walker to produce TD S3-020428 (response to letter to SA WG3 Chairman in TD S3-020337) and copy to SA WG3 list.

TD S3-020341 Introduction of IEEE 802.11 Security . This was covered by inclusion in TD S3-020390. It was noted that TKIP mechanism is being introduced to fix the known problems with WEP.

It was recognised that there will be a significant amount of work in SA WG3 on WLAN security and active contribution was invited on this to progress the work.

7.10 Visibility and configurability of security

There were no specific contributions under this agenda item.

7.11 Push

TD S3-020403 Reply LS on Push Security (response to LS S1-020541 on Push Security from SA1). This had been approved by e-mail before the meeting and was therefore noted.

7.12 Priority

TD S3-020330 Response from RAN WG2 to LS (S1-020642) on Priority Service Feasibility Study. This was introduced by Siemens and was noted.

7.13 Location services (LCS)

There were no specific contributions under this agenda item.

7.14 User equipment functionality split (UEFS)

There were no specific contributions under this agenda item.

7.15 Open service architecture (OSA)

TD S3-020421 LS from CN WG5 on OSA Security.This was introduced by Alcatel and had been provided to SA WG3 for information. Delegates were asked to review the attached CRs off-line and raise any implications to SA WG3 at the next meeting. The LS was then noted.

7.16 Generic user profile (GUP)

TD S3-020338 Proposed WID: 3GPP Generic User Profile Security. This was introduced by Lucent Technologies. Supporting companies and Rapporteur required completion. Access Control should also be added to the list of objectives. Mr. B. Owen agreed to be the Work Item rapporteur. The WID was updated to reflect agreed changes and provided in TD S3-020430 which was approved.

7.17 Presence

TD S3-020339 Proposed WID update: Support of the Presence Service Security Architecture. This was introduced by Ericsson. Proposals were distributed by e-mail and the WID produced taking comments into account. This was modified in TD S3-020429 and approved.

TD S3-020340 Firsat Draft TR: Presence security Architecture. This was briefly introduced by Ericsson and noted. Contribution was invited to the development of this TR.

7.18 User equipment management (UEM)

TD S3-020362 [DRAFT] Liaison Statement on Release 6 WID for User Equipment Management. This was introduced by Vodafone. SA WG5 asked for comments on their WID, which was reviewed. A response was provided in TD S3-020431 which was updated in TD S3-020448 and approved.

TD S3-020391 Draft WID: Release 6 User Equipment Management: Security aspects. This was introduced by Vodafone. The WI was updated with the list of supporting companies and editorially modified in TD S3-020432 which was approved.

7.19 Multimedia Broadcast/Multicast Service (MBMS)

TD S3-020373 Proposed WID: Security Aspects of Multimedia Broadcast/Multicast Service (MBMS). This was introduced by Hutchison 3G UK. Minor modifications were made and supporting companies added. The WID was updated in TD S3-020433 which was approved.

TD S3-020355 Liaison statement on the MBMS security. This was introduced by Alcatel and asked SA WG3 to answer some questions on MBMS security issues. Alcatel had reviewed the questions, and provided guidelines for response in TD S3-020363 which was considered.

TD S3-020363 MBMS security. This was introduced by Alcatel. Alcatel had reviewed the questions from SA WG2 in TD S3-020355 and provided these guidelines for an SA WG3 response, which were reviewed and discussed. A reply LS to SA WG2 was provided in TD S3-020434, which reported the activities in SA WG3 on MBMS (the WID to be attached) which was updated in TD S3-020449 and approved.

NOTE: TD S3-020307 from the previous meeting contains the drafts for MBMS. Delegates were invited to study these drafts.

7.20 PKI-based key management for network domain security

TD S3-020358 NDS/AF Feasibility Study to support the evolution of TS 33.210 NDS/IP. This was presented by Nokia and provided the results of their comprehensive study of the security requirements which need to be considered to support the evolution of NDS/IP.

It was clarified that some limitations on the scope of study for PKI had been made in order to make progress, although the full scope of PKI usage may be advantageous.

The question of reliability and Fallback procedures was raised. The FS has not taken this into account specifically, but would need to be considered during any standardisation activities.

Cross-certificates between operators, and the best methods to use for this was considered in need of study.

Although secret-key solutions are mentioned in the FS it was thought that this should be further investigated in the FS.

The supporting companies were thanked for the tremendous effort they had put into producing the feasibility study. There were some concerns that the whole approach was unnecessarily complex and off-the-shelf solutions may be used or adapted for use. PKI vs symetric architecture should be further discussed in the FS. It was thought that comments received should be taken into consideration and the FS could be submitted to TSG SA for information as an intrnal 3GPP TR. The FS would then be updated and used as justification for the WID, including realistic timescales. The updated document in TR format was provided in TD S3-020414 **which will be forwarded to TSG SA#17 for information**.

TD S3-020366 CMP and CMC Comparison. This was introduced by SSH Communications Security Corp. which concludes by suggesting SA WG3 will take CMPv2 as a working assumption for certificate lifecycle management for NDS/AF work. This contribution was noted.

8 Review and update of work programme

All rapporteurs were asked to check the latest version of the work plan on the ftp site and inform the Secretary of any changes and updates needed for the SA WG3 items.

9 Future meeting dates and venues

Siemens announced that the EU initiative for 4th Generation Security systems (PAMPAS) had arranged a Workshop on 16-17 September 2002 in London. A call for papers of approx 1-3 pages from interested members was requested. See http://www.pampas.eu.org for further details.

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#25	8 - 11 October 2002	Munich, Germany	Siemens
S3#26	19 - 22 November 2002	Sophia Antipolis (TBC) (Or co-located with T WG2 MeXE group, Korea)	ETSI (TBC)
S3#27	25 - 28 February 2003	TBC	European Friends' (TBC)
S3#28	06 - 09 May 2003	TBC	European Friends' (TBC)

LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#6	24 - 26 Sep 2002	Helsinki FI	
SA3 LI-#7	12 - 14 Nov 2002	San Diego US	
SA3 LI-#8	18 - 20 Feb 2003	Paris FR	
SA3 LI-#9	13 - 15 May 2003	Sophia Antipolis FR	
SA3 LI-#10	16 - 18 Sep 2003	US	

TSGs RAN/CN/T and SA Plenary meeting schedule

TSG RAN/CN/T #17	3 – 6 September	Biarritz, France	Alcatel
TSG SA #17	9 – 12 September	Biarritz, France	Alcatel
TSG RAN/CN/T #18	3 – 6 December	USA	NA 'Friends of 3GPP'
TSG SA #18	9 – 12 December	USA	NA 'Friends of 3GPP'
Meeting	**2003**	**Location**	**Primary Host**
TSG# RAN/CN/T 19	11-14 March (tba)	UK	UK 'Friends of 3GPP'
TSG SA #19	17-20 March (tba)	UK	UK 'Friends of 3GPP'
TSG#20	June (tba)	Finland	Nokia
TSG#21	September (tba)		
TSG#22	December (tba)		
Meeting	**2004 DRAFT SUGGESTION**	**Location**	**Primary Host**
TSG#23	March 9-12 & 15-18	UK	UK 'Friends of 3GPP'
TSG#24	June 1-4 & 7-10	Finland	Nokia
TSG#25	7-10 & 13-16 September		
TSG#26	7-10 & 13-16 December		

10 Any other business

There were no specific contributions under this agenda item.

11 Close

The Vice Chairman, V. Niemi Chaired the meeting for the last afternoon, he thanked the hosts, Sonera, Nokia and SSH, for the meeting arrangements and the delegates for their their hard work and cooperation and closed the meeting.

Annex A: List of attendees at the SA WG3#24 meeting and Voting List

A.1 List of attendees

Name	Company	e-mail	3GPP ORG	
Mr. Nigel Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	ETSI	GB
Mr. Colin Blanchard	BT Group Plc	colin.blanchard@bt.com	ETSI	GB
Mr. Marc Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	ETSI	BE
Mr. Krister Boman	ERICSSON L.M.	krister.boman@erv.ericsson.se	ETSI	SE
Mr. Charles Brookson	DTI	cbrookson@iee.org	ETSI	GB
Mr. Mauro Castagno	TELECOM ITALIA S.p.A.	mauro.castagno@tilab.com	ETSI	IT
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp	ARIB	JP
Mr. Per Christoffersson	TELIA AB	per.e.christoffersson@telia.se	ETSI	SE
Mr. KEVIN ENGLAND	mmO2 plc	kevin.england@o2.com	ETSI	GB
Dr. Adrian Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	GB
Mr. Louis Finkelstein	Motorola Inc.	louisf@labs.mot.com	T1	US
Mr. Giorgi Gulbani	NOKIA Corporation	giorgi.gulbani@nokia.com	ETSI	FI
Miss Jessica Gunnarsson	TELIA AB	jessica.l.gunnarsson@telia.se	ETSI	SE
Ms. Tao Haukka	NOKIA Corporation	tao.haukka@nokia.com	ETSI	FI
Mr. Veli-Pekka Heinonen	HotSip AB	Veli-Pekka.Heinonen@hotsip.com	ETSI	FI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@siemens.com	ETSI	DE
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vodafone.com	ETSI	GB
Mr. Geir Koien	TELENOR AS	geir-myrdahl.koien@telenor.com	ETSI	NO
Mr. Alexander Leadbeater	BT Group Plc	alex.leadbeater@bt.com	ETSI	GB
Mr. Luis Lopez Soria	Ericsson Inc.	luis.lopez-soria@ece.ericsson.se	T1	US
Mr. Tomi Mikkonen	SSH Communications Security	tomi.mikkonen@ssh.com	ETSI	FI
Mr. Sebastien Nguyen Ngoc	France Telecom	sebastien.nguyenngoc@rd.francetelecom.com	ETSI	FR
Mr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI	FI
Mr. Petri Nyberg	SONERA Corporation	petri.nyberg@sonera.com	ETSI	FI
Mr. Bradley Owen	Lucent Technologies N. S. UK	bvowen@lucent.com	ETSI	GB
Mr. Olivier Paridaens	ALCATEL S.A.	Olivier.Paridaens@ALCATEL.BE	ETSI	FR
Miss Mireille PAULIAC	GEMPLUS Card International	mireille.pauliac@GEMPLUS.COM	ETSI	FR
Mr. Maurice Pope	ETSI Secretariat	maurice.pope@etsi.fr	ETSI	FR
Mr. Petri Säkkinen	SSH Communications Security	petri.sakkinen@ssh.com	ETSI	FI
Mr. Stefan Schroeder	T-MOBILE DEUTSCHLAND	stefan.schroeder@t-mobile.de	ETSI	DE
Mr. Hugh Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	T1	US
Mr. Benno Tietz	Vodafone D2 GmbH	benno.tietz@vodafone.com	ETSI	DE
Mr. Vesa Torvinen	ERICSSON L.M.	vesa.torvinen@ericsson.fi	ETSI	SE
Mr. Tommi Viitanen	NOKIA Corporation	tommi.viitanen@nokia.com	ETSI	FI
Prof. Michael Walker	VODAFONE Group Plc	mike.walker@vodafone.com	ETSI	GB
Mr. Stuart Ward	ORANGE PCS LTD	stuart.ward@orange.co.uk	ETSI	GB
Ms. Monica Wifvesson	ERICSSON L.M.	monica.wifvesson@emp.ericsson.se	ETSI	SE
Mr. Berthold Wilhelm	BMWi	berthold.wilhelm@regtp.de	ETSI	DE

38 attendees

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #22, #23 and #24, the following companies are eligible to vote at SA WG3 meeting #25:

Company	Country	Status	Partner Org
ALCATEL BELL	BE	3GPPMEMBER	ETSI
ALCATEL S.A.	FR	3GPPMEMBER	ETSI
AT&T Wireless Services, Inc.	US	3GPPMEMBER	T1
BMWi	DE	3GPPMEMBER	ETSI
BT Group Plc	GB	3GPPMEMBER	ETSI
Cingular Wireless LLC	US	3GPPMEMBER	T1
Dansk MobilTelefon I/S	DK	3GPPMEMBER	ETSI
DTI	GB	3GPPMEMBER	ETSI
Ericsson Inc.	US	3GPPMEMBER	T1
ERICSSON L.M.	SE	3GPPMEMBER	ETSI
France Telecom	FR	3GPPMEMBER	ETSI
GEMPLUS Card International	FR	3GPPMEMBER	ETSI
HotSip AB	FI	3GPPMEMBER	ETSI
Hutchison 3G UK Limited	GB	3GPPMEMBER	ETSI
Lucent Technologies	US	3GPPMEMBER	T1
Lucent Technologies N. S. UK	GB	3GPPMEMBER	ETSI
Mitsubishi Electric Co.	JP	3GPPMEMBER	ARIB
mmO2 plc	GB	3GPPMEMBER	ETSI
Motorola Inc.	US	3GPPMEMBER	T1
MOTOROLA Ltd	GB	3GPPMEMBER	ETSI
NOKIA Corporation	FI	3GPPMEMBER	ETSI
NORTEL NETWORKS (EUROPE)	GB	3GPPMEMBER	ETSI
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
OBERTHUR CARD SYSTEMS S.A.	FR	3GPPMEMBER	ETSI
ORANGE FRANCE	FR	3GPPMEMBER	ETSI
ORANGE PCS LTD	GB	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
SAMSUNG Electronics	GB	3GPPMEMBER	ETSI
SchlumbergerSema	FR	3GPPMEMBER	ETSI
SIEMENS AG	DE	3GPPMEMBER	ETSI
SIEMENS ATEA NV	BE	3GPPMEMBER	ETSI
SONERA Corporation	FI	3GPPMEMBER	ETSI
SSH Communications Security	FI	3GPPMEMBER	ETSI
T-MOBILE DEUTSCHLAND	DE	3GPPMEMBER	ETSI
TELECOM ITALIA S.p.A.	IT	3GPPMEMBER	ETSI
TELENOR AS	NO	3GPPMEMBER	ETSI
TELIA AB	SE	3GPPMEMBER	ETSI
Vodafone D2 GmbH	DE	3GPPMEMBER	ETSI
VODAFONE Group Plc	GB	3GPPMEMBER	ETSI

39 Member companies

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020325	Draft agenda for meeting #24	SA WG3 Chairman	2	Approval		Approved
S3-020326	Draft report of SA WG3 meeting #23 - v0.0.5	SA WG3 Secretary	4.1	Approval		Approved (with minor modifications) new version 1.0.0 will be put on FTP server
S3-020327	SA1 Position Statement related to ITU-T request for information on activities related to Emergency Telecommunications Services (ETS)	SA WG1	6.1	Information		Noted. contributions to the SA WG3 meeting, covering members' concerns
S3-020328	Response Liaison Statement on IMS Identities for R99/R4 UICC	CN WG1	6.1	Information		Noted
S3-020329	LS from CN WG4 on Status of protocol work on Ze interface	CN WG4	6.1	Action		Reply in 398
S3-020330	Response from RAN WG2 to LS (S1-020642) on Priority Service Feasibility Study	RAN WG2	7.12	Information		Noted
S3-020331	Reply from SA WG1 to the LS on WLAN Interworking	SA WG1	7.9	Action		Reply in TD427
S3-020332	Answer from SA WG4 to “Liaison Statement on PSS Release 6 work programme”	SA WG4	6.1	Action		Noted
S3-020333	LS from T WG2 on support for subscriber certificates	T WG2	7.7	Action		Noted
S3-020334	LS from T WG3 on OFM and the IMS service	T WG3	6.1	Action		Reply in 399
S3-020335	Response from T WG3 to “Liaison Statement on Access to IMS Services using 3GPP release 99 and release 4 UICCs” (S1-020577)	T WG3	6.1	Information		Noted
S3-020336	Liaison Statement from T WG3 on terminology regarding ISIM/USIM	T WG3	6.1	Action		K Boman to check 33.203 and e-mail contact person if no problems
S3-020337	Letter to SA WG3 Chairman: information about ongoing work on WLAN – 3G and other Public Access networks interworking	Chairman ETSI EP BRAN & Chairman of High Speed Wireless Access Committee of MMAC-PC	7.9	Information		Reply to be drafted by Chairman in TD448
S3-020338	Proposed WID: 3GPP Generic User Profile Security	Lucent Technologies	7.16	Approval	S3-020430	Revised in TD430
S3-020339	Proposed WID update: Support of the Presence Service Security Architecture	Ericsson	7.17	Approval	S3-020429	Revised in TD429
S3-020340	Firsat Draft TR: Presence security Architecture	Ericsson	7.17	Discussion		Noted
S3-020341	Introduction of IEEE 802.11 Security	Ericsson	7.9	Discussion		Covered by TD390
S3-020342	Proposed CR to 23.035: Correction of use IST Command message and Call Termination Indication parameter (R99)	Ericsson	7.6	Approval		Approved
S3-020343	Proposed CR to 23.035: Correction of use IST Command message and Call Termination Indication parameter (Rel-4)	Ericsson	7.6	Approval		Approved
S3-020344	Proposed CR to 23.035: Correction of use IST Command message and Call Termination Indication parameter (Rel-5)	Ericsson	7.6	Approval		Approved
S3-020345	Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #3/02 on lawful interception - Budapest 4-6 June 2002	LI group	4.2	Information		Noted
S3-020346	CR to 33.107: Essential clarification to the Timestamp IE (Rel-5)	LI group	4.2	Approval		Approved
S3-020347	CR to 33.107: Additional X3-interface parameters (Rel-5)	LI group	4.2	Approval		Approved
S3-020348	CR to 33.106: Changes to 33.106 to clarify interception capabilities (Rel-5)	LI group	4.2	Approval	S3-020396	Revised in TD396
S3-020349	LS concerning Rapporteur to ETSI TC LI (Response to: LS (32TD050) on LS to 3GPP SA3 LI on work coordination from ETSI TC LI #32)	LI group	4.2	Information		Noted
S3-020350	LS on implications of the IPv6 auroconfiguration on LI	LI group	4.2	Information		Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020351	CR to 33.108: Corrections to TS 33.108 (Rel-5)	LI group	4.2	Approval		Approved
S3-020352	LS on A/Gb evolution	TSG GERAN	7.5	Action		Reply in TD445
S3-020353	Reply to Liaison Statement on use of IP as transport for the Inter-GMLC Interface	SA WG2	6.1	Information		Noted
S3-020354	Liaison statement on 3GPP System to WLAN Inter working	SA WG2	7.9	Action		Reply in TD426
S3-020355	Liaison statement on the MBMS security	SA WG2	7.19	Action		Reply in TD434
S3-020356	LS on subscriber certificates (Response to S3-020322)	SA WG2	7.7	Action		Reply in TD413
S3-020357	Answer to Liaison Statement regarding PSS Release 6 work programme	SA WG2	6.1	Information		Noted
S3-020358	NDS/AF Feasibility Study to support the evolution of TS 33.210 NDS/IP	Nokia, Siemens, SSH, Telenor, T-Mobile	7.20	Discussion and approval	S3-020414	Updated into TR format in TD414
S3-020359	Security solution for UTRAN IP transport	Nokia	7.2	Discussion and approval	S3-020422	WID updated in TD422
S3-020360	SAGE deliverables A5/3	SA WG3 Secretary (MCC)	6.3	Approval		Deliverables approved. Implementation letter to manufacturers in TD405
S3-020361	SA handling	Ericsson	7.1		S3-020443	Combined with TD402
S3-020362	[DRAFT] Liaison Statement on Release 6 WID for User Equipment Management	SA WG5	7.18			Response in TD448
S3-020363	MBMS security	Alcatel	7.19			Answers considered and used to produce reply LS in TD434
S3-020364	Encryption for MBMS Multicast	Lucent Technologies	7.19			WITHDRAWN
S3-020365	Analysis of Subscriber Certificates Concept	Siemens	7.7			Further study is needed to determine whether POP should be included to handle possible future use-cases
S3-020366	CMP and CMC Comparison	SSH Communications Security Corp	7.20			Noted
S3-020367	CMP and CMC Comparison (WITHDRAWN)	SSH Communications Security Corp				WITHDRAWN - Repeat of S3-020366
S3-020368	COPS usage for IPSec policy management in NDS/IP	SSH Communications Security Corp	7.2			Requirements for security management need to be collected
S3-020369	Proposed CR to 33.203: Correction to S-CSCF behaviour on Network Authentication Failure	Hutchison 3G UK	7.1	Approval	S3-020407	Revised in TD407
S3-020370	Proposed CR top 33.203: Correcting the network behaviour in response to an incorrect AUT-S	Hutchison 3G UK	7.1	Approval	S3-020409	Revised in TD409
S3-020371	Proposed CR to 33.203: Update of User Authentication Failure	Hutchison 3G UK	7.1	Approval	S3-020410	Revised in TD410
S3-020372	SA and registration lifetimes	Hutchison 3G UK	7.1			LS in TD415
S3-020373	Proposed WID: Security Aspects of Multimedia Broadcast/Multicast Service (MBMS)	Hutchison 3G UK	7.19		S3-020433	Revised in TD433
S3-020374	Common IPsec SA for UDP and TCP sockets	Nokia	7.1			Related CR and LS in TD416, TD417
S3-020375	Transport layer address in Via header	Nokia	7.1			Await reply from related LS in TD316
S3-020376	Proposed CR to 33.203: Protect port number to be assigned by UE in re-registration	Nokia	7.1		S3-020412	Revised in TD412
S3-020377	Architecture alternatives for supporting subscriber certificates	Nokia	7.7			Discussed and noted. List of open issues created

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020378	Security and other requirements for subscriber certificates	Nokia	7.7			Discussed and noted. List of open issues created
S3-020379	Proposed CR to 33.203: SA handling when the UE changes IP address	Ericsson	7.1		S3-020406	Revised in TD406
S3-020380	Proposed CR to 33.203: Draft-ietf-sip-sec-agree syntax for manually keyed IPsec	Ericsson	7.1			Approved
S3-020381	Proposed CR to 33.203: Attacker sends responses to requests intended for other parties	Ericsson, Nokia	7.1			Not approved. Related LS in TD441
S3-020382	Proposed CR to 33.203: Mitigating reflection attacks in IMS	Ericsson, Nokia	7.1		SP-020411	Revised in TD411
S3-020383	Proposed CR to 33.203: Removal of some editor notes in TS33.203	Ericsson	7.1			Approved
S3-020384	Proposed CR to 33.203: MITM attack for TCP SA negotiation	Ericsson	7.1			WITHDRAWN (covered by TDs 374, 387)
S3-020385	Profiling SIP Security Agreement for IMS R5	Ericsson	7.1			Principles accepted. CR in TD379
S3-020386	Status of SIP Security Agreement Draft in IETF	Ericsson	6.2			Noted
S3-020387	MitM attack for TCP Security Association negotiation	Ericsson	7.1		S3-020416	revised in TD416
S3-020388	Use of Kasumi-based functions for Group release security solution	ETSI SAGE	6.3			SA WG3 to take recommendations into account in the specification od the Group release mechanism
S3-020389	LS: Advice on key expansion for HMAC-SHA-1-96	ETSI SAGE	6.3	Action		Response LS in 401
S3-020390	Draft TR: Wireless Local Area Network (WLAN) Interworking Security	(Editor) Ericsson	7.9	Information		Noted. TS to be produced instead of TR first
S3-020391	Draft WID: Release 6 User Equipment Management: Security aspects	Vodafone	7.18	Approval	S3-020432	Revised in TD432
S3-020392	Proposed WID draft 2: WLAN Interworking Security WID	BT Group	7.9	Approval	S3-020425	Revised in TD425
S3-020393	Proposed CR to 33.203: Correction of authentication vector distribution procedure.	Vodafone	7.1	Approval	S3-020419	Revised in TD419
S3-020394	Proposed CR to 22.032: Application of IST to PS services	Vodafone	7.6	Approval		Not approved. Related LS in TD446
S3-020395	Proposed CR to 23.035: Application of IST to PS services	Vodafone	7.6	Approval		Not approved. Related LS in TD446
S3-020396	CR to 33.106: Changes to 33.106 to clarify interception capabilities (Rel-5)	LI group	4.2	Approval		Approved
S3-020397	Report to SA3 on SA#16	SA WG3 Vice Chairman	5	Information		Noted
S3-020398	Reply LS to CN WG4 on Status of protocol work on Ze interface (N4-020769)	SA WG3	6.1	Approval		Approved
S3-020399	LS to T WG3 on OFM and the IMS service	SA WG3	6.1	Approval		Approved
S3-020400	Presentation on SA Handling	Ericsson	7.1	Presentation		Presented. Related doc TD361
S3-020401	Response to ETSI SAGE (TD389)	SA WG3 (K Boman)		Approval	S3-020435	Revised in TD435
S3-020402	Proposed CR to 33.203: Update of SA handling procedures	Hutchison 3G UK	7.1	Approval	S3-020443	Combined with TD361
S3-020403	Reply LS on Push Security (response to LS S1-020541 on Push Security from SA1)	Vodafone	7.11	Information		Approved by e-mail before meeting
S3-020404	Utilizing SIP parameter to handle SA database optimally in P-CSCF	Nokia	7.1	Discussion / Approval		Nokia were asked to re-write the CR after consultation with CN WG4 colleagues and resubmit to SA WG3
S3-020405	[DRAFT] LS on introduction and adoption of A5/3	SA WG3		Approval	S3-020440	revised in TD440
S3-020406	Proposed CR to 33.203: SA handling when the UE changes IP address	Ericsson	7.1	Approval	S3-020436	revised in TD436

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020407	Proposed CR to 33.203: Correction to S-CSCF behaviour on Network Authentication Failure	Hutchison 3G UK	7.1	Approval		Approved
S3-020408	LS to CNWG1	SA WG3 (Monica)	7.1	Approval		Approved
S3-020409	Proposed CR top 33.203: Correcting the network behaviour in response to an incorrect AUT-S	Hutchison 3G UK	7.1	Approval		Approved
S3-020410	Proposed CR to 33.203: Update of User Authentication Failure	Hutchison 3G UK	7.1	Approval	S3-020442	revised in TD442
S3-020411	Proposed CR to 33.203: Mitigating reflection attacks in IMS	Ericsson, Nokia	7.1	Approval		Approved
S3-020412	Proposed CR to 33.203: Protect port number to be assigned by UE in re-registration	Nokia	7.1	Approval		Approved
S3-020413	LS to SA WG2, SA WG1 cc: T WG2 on architecture and requirements for subscriber certificates	SA WG3	7.7	Approval	S3-020447	revised in TD447
S3-020414	TR format: FS for NDS/IP evolution WID	Nokia	7.20	Information		Agreed to send to TSG SA#17 for information
S3-020415	LS on SA Lifetime	SA WG3	7.1	Approval		Not Approved. Delegates to inform CN1 colleagues of problem. To be resolved at next meeting
S3-020416	CR to 33.203: Common IPsec SA for UDP and TCP sockets	Nokia	7.1	Approval		Approved
S3-020417	LS to CN WG1: Same SA to be utilized for both UDP and TCP transport protocols	SA WG3	7.1	Approval		Approved (TD416 to attach)
S3-020418	LS to CN WG1 on Attacker sends responses to requests intended for other parties	SA WG3 (K Boman)	7.1	Approval	S3-020441	Replaced by TD441
S3-020419	Proposed CR to 33.203: Correction of authentication vector distribution procedure.	Vodafone	7.1	Approval		Approved
S3-020420	LS to CN WG4 on impacts to CR in 419	SA WG3	7.1	Approval	S3-020437	revised in TD437
S3-020421	LS from CN WG5 on OSA Security	CN WG5	7.15	Information		Noted
S3-020422	Updated WID on NDS/IP	SA WG3	7.2	Approval	S3-020444	Replaced by TD444
S3-020423	LS to GERAN : Reply to GP-022012	SA WG3 (P.Howard)	7.5	Approval	S3-020445	Replaced by TD445
S3-020424	LS to SA WG5: IST Charging records	SA WG3 (P.Howard)	7.6	Approval	S3-020446	Replaced by TD446
S3-020425	Proposed WID draft 2: WLAN Interworking Security WID	BT Group	7.9	Approval	S3-020451	Replaced by TD451
S3-020426	LS to SA WG2: Comments on WLAN draft TR	BT Group	7.9	Approval	S3-020452	Replaced by TD452
S3-020427	LS to SA WG1: WLAN interworking understandings	SA WG3	7.9	Approval	S3-020453	Replaced by TD453
S3-020428	LS Reply to TD337	SA WG3 (M.Walker)	7.9	Approval		To be provided by SA WG3 Chairman after meeting
S3-020429	Proposed WID update: Support of the Presence Service Security Architecture	Ericsson	7.17	Approval		Approved
S3-020430	Proposed WID: 3GPP Generic User Profile Security	Lucent Technologies	7.16	Approval		Approved
S3-020431	LS to SA WG5 response to TD362	SA WG3 (P.Howard)	7.18	Approval	S3-020448	Replaced by TD448
S3-020432	Draft WID: Release 6 User Equipment Management: Security aspects	Vodafone	7.18	Approval		Approved
S3-020433	Proposed WID: Security Aspects of Multimedia Broadcast/Multicast Service (MBMS)	Hutchison 3G UK	7.19	Approval		Approved
S3-020434	Response to Liaison statement on the MBMS security	SA WG3	7.19	Approval	S3-020449	Replaced by TD449
S3-020435	Response to ETSI SAGE (TD389)	SA WG3 (K Boman)		Approval		Approved
S3-020436	Proposed CR to 33.203: SA handling when the UE changes IP address	Ericsson	7.1	Approval		Approved
S3-020437	LS to CN WG4 on impacts to CR in 419	SA WG3	7.1	Approval		Approved
S3-020438	LS from SA WG5: Reply on Packet Switched Streaming (PSS) in Rel-6 Work Programme	SA WG5	6.1	Information		Noted
S3-020439	LS from SA WG5 on Diameter security issues	SA WG5	6.1	Action	xxx	POSTPONED to NEXT MEETING

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020440	[DRAFT] LS on introduction and adoption of A5/3	SA WG3		Approval		Approved
S3-020441	LS to CN WG1 on Attacker sends responses to requests intended for other parties	SA WG3 (K Boman)	7.1	Approval		Approved
S3-020442	Proposed CR to 33.203: Update of User Authentication Failure	Hutchison 3G UK	7.1	Approval		Approved
S3-020443	Proposed CR to 33.203: Update of SA handling procedures	Hutchison 3G UK	7.1	Approval	S3-020450	Replaced by TD450
S3-020444	Updated WID on NDS/IP	SA WG3	7.2	Approval		Approved
S3-020445	LS to GERAN : Reply to GP-022012	SA WG3 (P.Howard)	7.5	Approval		Approved
S3-020446	LS to SA WG5: IST Charging records	SA WG3 (P.Howard)	7.6	Approval		Approved
S3-020447	LS to SA WG2, SA WG1 cc: T WG2 on architecture and requirements for subscriber certificates	SA WG3	7.7	Approval		Approved
S3-020448	LS to SA WG5 response to TD362	SA WG3 (P.Howard)	7.18	Approval		Approved
S3-020449	Response to Liaison statement on the MBMS security	SA WG3	7.19	Approval		Approved
S3-020450	Proposed CR to 33.203: Update of SA handling procedures	Hutchison 3G UK	7.1	Approval		Finalise over e-mail (A. Escott)
S3-020451	Proposed WID draft 2: WLAN Interworking Security WID	BT Group	7.9	Approval		Approved
S3-020452	LS to SA WG2: Comments on WLAN draft TR	BT Group	7.9	Approval		Approved
S3-020453	LS to SA WG1: WLAN interworking understandings	SA WG3	7.9	Approval		Approved
S3-020454	CR to 33.107: Inclusion of Serving System IRI (Rel-5)	SA WG3 LI group	-	e-mail approval		For e-mail approval by 23 August 2002

Annex C: Status of specifications under SA WG3 responsibility

Specification			Title	Editor	Rel
TR	01.31	7.0.1	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	WRIGHT, Tim	R98
TR	01.31	8.0.0	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	WRIGHT, Tim	R99
TR	01.33	7.0.0	Lawful Interception requirements for GSM	BONNER, Brye	R98
TR	01.33	8.0.0	Lawful Interception requirements for GSM	BONNER, Brye	R99
TS	01.61	6.0.1	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	WALKER, Michael	R97
TS	01.61	7.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	WALKER, Michael	R98
TS	01.61	8.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	WALKER, Michael	R99
TS	02.09	3.1.0	Security aspects	CHRISTOFFERSSON, Per	Ph1
TS	02.09	4.5.1	Security aspects	CHRISTOFFERSSON, Per	Ph2
TS	02.09	5.2.1	Security aspects	CHRISTOFFERSSON, Per	R96
TS	02.09	6.1.1	Security aspects	CHRISTOFFERSSON, Per	R97
TS	02.09	7.1.1	Security aspects	CHRISTOFFERSSON, Per	R98
TS	02.09	8.0.1	Security aspects	CHRISTOFFERSSON, Per	R99
TS	02.31	7.1.1	Fraud Information Gathering System (FIGS); Service description; Stage 1	WRIGHT, Tim	R98
TS	02.31	8.0.1	Fraud Information Gathering System (FIGS); Service description; Stage 1	WRIGHT, Tim	R99
TS	02.32	7.1.1	Immediate Service Termination (IST); Service description; Stage 1	WRIGHT, Tim	R98
TS	02.33	7.3.0	Lawful Interception (LI); Stage 1	BONNER, Brye	R98
TS	02.33	8.0.1	Lawful Interception (LI); Stage 1	BONNER, Brye	R99
TS	03.20	3.3.2	Security-related Network Functions	NGUYEN NGOC, Sebastien	Ph1
TS	03.20	3.0.0	Security-related Network Functions	NGUYEN NGOC, Sebastien	Ph1-EXT
TS	03.20	4.4.1	Security-related Network Functions	NGUYEN NGOC, Sebastien	Ph2
TS	03.20	5.2.1	Security-related Network Functions	NGUYEN NGOC, Sebastien	R96
TS	03.20	6.1.0	Security-related Network Functions	NGUYEN NGOC, Sebastien	R97
TS	03.20	7.2.0	Security-related Network Functions	NGUYEN NGOC, Sebastien	R98
TS	03.20	8.1.0	Security-related Network Functions	NGUYEN NGOC, Sebastien	R99
TS	03.31	7.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 2	WRIGHT, Tim	R98
TS	03.31	8.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 2	WRIGHT, Tim	R99
TS	03.33	7.2.0	Lawful Interception; Stage 2	BONNER, Brye	R98
TS	03.33	8.1.0	Lawful Interception; Stage 2	BONNER, Brye	R99
TS	03.35	7.0.1	Immediate Service Termination (IST); Stage 2	WRIGHT, Tim	R98
TS	21.133	3.2.0	3G security; Security threats and requirements	CHRISTOFFERSSON, Per	R99
TS	21.133	4.1.0	3G security; Security threats and requirements	CHRISTOFFERSSON, Per	Rel-4
TS	22.022	3.2.1	Personalisation of Mobile Equipment (ME); Mobile functionality specification	NGUYEN NGOC, Sebastien	R99
TS	22.022	4.1.0	Personalisation of Mobile Equipment (ME); Mobile functionality specification	NGUYEN NGOC, Sebastien	Rel-4
TS	22.032	3.0.0	Immediate Service Termination (IST); Service description; Stage 1	HOWARD, Peter	R99

TS	22.032	4.0.0	Immediate Service Termination (IST); Service description; Stage 1	HOWARD, Peter	Rel-4
TS	22.032	5.0.0	Immediate Service Termination (IST); Service description; Stage 1	HOWARD, Peter	Rel-5
TS	23.035	3.0.0	Immediate Service Termination (IST); Stage 2	HOWARD, Peter	R99
TS	23.035	4.0.0	Immediate Service Termination (IST); Stage 2	HOWARD, Peter	Rel-4
TS	23.035	5.0.0	Immediate Service Termination (IST); Stage 2	HOWARD, Peter	Rel-5
TS	33.102	3.12.0	3G security; Security architecture	BLOMMAERT, Marc	R99
TS	33.102	4.4.0	3G security; Security architecture	BLOMMAERT, Marc	Rel-4
TS	33.102	5.0.0	3G security; Security architecture	BLOMMAERT, Marc	Rel-5
TS	33.103	3.7.0	3G security; Integration guidelines	BLANCHARD, Colin	R99
TS	33.103	4.2.0	3G security; Integration guidelines	BLANCHARD, Colin	Rel-4
TS	33.105	3.8.0	Cryptographic Algorithm requirements	CHIKAZAWA, Takeshi	R99
TS	33.105	4.1.0	Cryptographic Algorithm requirements	CHIKAZAWA, Takeshi	Rel-4
TS	33.106	3.1.0	Lawful interception requirements	WILHELM, Berthold	R99
TS	33.106	4.0.0	Lawful interception requirements	WILHELM, Berthold	Rel-4
TS	33.106	5.0.0	Lawful interception requirements	WILHELM, Berthold	Rel-5
TS	33.107	3.5.0	3G security; Lawful interception architecture and functions	WILHELM, Berthold	R99
TS	33.107	4.3.0	3G security; Lawful interception architecture and functions	WILHELM, Berthold	Rel-4
TS	33.107	5.3.0	3G security; Lawful interception architecture and functions	WILHELM, Berthold	Rel-5
TS	33.108	5.0.0	3G security; Handover interface for Lawful Interception (LI)	RYAN, Ron	Rel-5
TS	33.120	3.0.0	Security Objectives and Principles	WRIGHT, Tim	R99
TS	33.120	4.0.0	Security Objectives and Principles	WRIGHT, Tim	Rel-4
TS	33.200	4.3.0	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	ESCOTT, Adrian	Rel-4
TS	33.200	5.0.0	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security	ESCOTT, Adrian	Rel-5
TS	33.203	5.2.0	3G security; Access security for IP-based services	BOMAN, Krister	Rel-5
TS	33.210	5.1.0	3G security; Network Domain Security (NDS); IP network layer security	KOIEN, Geir	Rel-5
TR	33.900	0.4.1	Guide to 3G security	BROOKSON, Charles	Rel-6
TR	33.901	3.0.0	Criteria for cryptographic Algorithm design process	BLOM, Rolf	R99
TR	33.901	4.0.0	Criteria for cryptographic Algorithm design process	BLOM, Rolf	Rel-4
TR	33.902	3.1.0	Formal Analysis of the 3G Authentication Protocol	HORN, Guenther	R99
TR	33.902	4.0.0	Formal Analysis of the 3G Authentication Protocol	HORN, Guenther	Rel-4
TR	33.904	none	Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms	VACANT,	Rel-4
TR	33.908	3.0.0	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	WALKER, Michael	R99
TR	33.908	4.0.0	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	WALKER, Michael	Rel-4
TR	33.909	4.0.1	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	WALKER, Michael	Rel-4
TS	35.201	3.2.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	WALKER, Michael	R99
TS	35.201	4.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	WALKER, Michael	Rel-4
TS	35.201	5.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	WALKER, Michael	Rel-5
TS	35.202	3.1.2	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	WALKER, Michael	R99

TS	35.202	4.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	WALKER, Michael	Rel-4
TS	35.202	5.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	WALKER, Michael	Rel-5
TS	35.203	3.1.2	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	WALKER, Michael	R99
TS	35.203	4.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	WALKER, Michael	Rel-4
TS	35.203	5.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	WALKER, Michael	Rel-5
TS	35.204	3.1.2	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	WALKER, Michael	R99
TS	35.204	4.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	WALKER, Michael	Rel-4
TS	35.204	5.0.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	WALKER, Michael	Rel-5
TR	35.205	4.0.0	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	WALKER, Michael	Rel-4
TR	35.205	5.0.0	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	WALKER, Michael	Rel-5
TS	35.206	4.0.0	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	WALKER, Michael	Rel-4
TS	35.206	5.0.0	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	WALKER, Michael	Rel-5
TS	35.207	4.0.0	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	WALKER, Michael	Rel-4
TS	35.207	5.0.0	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	WALKER, Michael	Rel-5
TS	35.208	4.0.0	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	WALKER, Michael	Rel-4
TS	35.208	5.0.0	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	WALKER, Michael	Rel-5
TR	35.909	4.0.0	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	WALKER, Michael	Rel-4
TR	35.909	5.0.0	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	WALKER, Michael	Rel-5
TR	41.031	4.0.1	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	WRIGHT, Tim	Rel-4
TR	41.031	5.0.0	Fraud Information Gathering System (FIGS); Service requirements; Stage 0	WRIGHT, Tim	Rel-5
TR	41.033	4.0.1	Lawful Interception requirements for GSM	BONNER, Brye	Rel-4
TR	41.033	5.0.0	Lawful Interception requirements for GSM	BONNER, Brye	Rel-5
TS	41.061	4.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	WALKER, Michael	Rel-4
TS	42.009	4.0.0	Security Aspects	CHRISTOFFERSSON, Per	Rel-4
TS	42.031	4.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 1	WRIGHT, Tim	Rel-4
TS	42.031	5.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 1	WRIGHT, Tim	Rel-5
TS	42.033	4.0.0	Lawful Interception; Stage 1	BONNER, Brye	Rel-4
TS	42.033	5.0.0	Lawful Interception; Stage 1	BONNER, Brye	Rel-5
TS	43.020	4.0.0	Security-related network functions	GILBERT, Henri	Rel-4
TS	43.031	4.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 2	WRIGHT, Tim	Rel-4
TS	43.031	5.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 2	WRIGHT, Tim	Rel-5
TS	43.033	4.0.0	Lawful Interception; Stage 2	BONNER, Brye	Rel-4
TS	43.033	5.0.0	Lawful Interception; Stage 2	BONNER, Brye	Rel-5

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	WG status
23.035	001		R99	Correction of use IST Command message and Call Termination Indication parameter	F	3.0.0	S3-24	S3-020342	agreed
23.035	002		Rel-4	Correction of use IST Command message and Call Termination Indication parameter	A	4.0.0	S3-24	S3-020343	agreed
23.035	003		Rel-5	Correction of use IST Command message and Call Termination Indication parameter	A	5.0.0	S3-24	S3-020344	agreed
33.107	026		Rel-5	Essential clarification to the Timestamp IE	F	5.3.0	S3-24	S3-020346	agreed
33.107	027		Rel-5	Additional X3-interface parameters	F	5.3.0	S3-24	S3-020347	agreed
33.108	001		Rel-5	Corrections to TS 33.108	F	5.0.0	S3-24	S3-020351	agreed
33.203	012		Rel-5	SA handling when the UE changes IP address	F	5.2.0	S3-24	S3-020380	agreed
33.203	013		Rel-5	Removal of some editor notes in TS33.203	F	5.2.0	S3-24	S3-020383	agreed
33.106	004		Rel-5	Changes to 33.106 to clarify interception capabilities	F	5.0.0	S3-24	S3-020396	agreed
33.203	014		Rel-5	Correction to S-CSCF behaviour on Network Authentication Failure	F	5.2.0	S3-24	S3-020407	agreed
33.203	015		Rel-5	Correcting the network behaviour in response to an incorrect AUT-S	F	5.2.0	S3-24	S3-020409	agreed
33.203	016		Rel-5	Mitigating reflection attacks in IMS	F	5.2.0	S3-24	S3-020411	agreed
33.203	017		Rel-5	Protect port number to be assigned by UE in re-registration	F	5.2.0	S3-24	S3-020412	agreed
33.203	018		Rel-5	One SA for both TCP and UDP sockets	F	5.2.0	S3-24	S3-020416	agreed
33.203	019		Rel-5	Correction of authentication vector distribution procedure	F	5.2.0	S3-24	S3-020419	agreed
33.203	020		Rel-5	The definition of the key to be used for HMAC-SHA1-96 within ESP	F	5.2.0	S3-24	S3-020435	agreed
33.203	021		Rel-5	Draft-ietf-sip-sec-agree syntax for manually keyed Ipsec	F	5.2.0	S3-24	S3-020436	agreed
33.203	022		Rel-5	Update of User Authentication Failure	F	5.2.0	S3-24	S3-020442	agreed

One CR for e-mail approval after meeting (deadline 23 August 2002). CR number to be added if approved (will be CR 028).

33.107	xxx		Rel-5	Inclusion of Serving System IRI	F	5.3.0	S3-24	S3-020454	e-mail approval

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	Source TD	Comment/Status
S3-020327	SA1 Position Statement related to ITU-T request for information on activities related to Emergency Telecommunications Services (ETS)	S1-021190	Noted. contributions to the SA WG3 meeting, covering members' concerns
S3-020328	Response Liaison Statement on IMS Identities for R99/R4 UICC	N1-021427	Noted
S3-020329	LS from CN WG4 on Status of protocol work on Ze interface	N4-020769	Reply in 398
S3-020330	Response from RAN WG2 to LS (S1-020642) on Priority Service Feasibility Study	R2-020330	Noted
S3-020331	Reply from SA WG1 to the LS on WLAN Interworking	S1-021186	Reply in TD427
S3-020332	Answer from SA WG4 to “Liaison Statement on PSS Release 6 work programme”	S4-020332	Noted
S3-020333	LS from T WG2 on support for subscriber certificates	T2-020574	Noted
S3-020334	LS from T WG3 on OFM and the IMS service	T3-020379	Reply in 399
S3-020335	Response from T WG3 to “Liaison Statement on Access to IMS Services using 3GPP release 99 and release 4 UICCs” (S1-020577)	T3-020406	Noted
S3-020336	Liaison Statement from T WG3 on terminology regarding ISIM/USIM	T3-020409	K Boman to check 33.203 and e-mail contact person if no problems
S3-020337	Letter to SA WG3 Chairman: information about ongoing work on WLAN – 3G and other Public Access networks interworking	BRAN28td085r2	Reply to be drafted by Chairman in TD448
S3-020349	LS concerning Rapporteur to ETSI TC LI (Response to: LS (32TD050) on LS to 3GPP SA3 LI on work coordination from ETSI TC LI #32)	S3LI02_125r2	Noted
S3-020350	LS on implications of the IPv6 auroconfiguration on LI	S3LI02_127r1	Noted
S3-020352	LS on A/Gb evolution	GP-022012	Reply in TD445
S3-020353	Reply to Liaison Statement on use of IP as transport for the Inter-GMLC Interface	S2-021919	Noted
S3-020354	Liaison statement on 3GPP System to WLAN Inter working	S2-022022	Reply in TD426
S3-020355	Liaison statement on the MBMS security	S2-022040	Reply in TD434
S3-020356	LS on subscriber certificates (Response to S3-020322)	S2-022047	Reply in TD413
S3-020357	Answer to Liaison Statement regarding PSS Release 6 work programme	S2-022050	Noted
S3-020362	[DRAFT] Liaison Statement on Release 6 WID for User Equipment Management	S5-022110	Response in TD448
S3-020388	Use of Kasumi-based functions for Group release security solution	SAGE (02) 26	SA WG3 to take recommendations into account in the specification od the Group release mechanism
S3-020389	LS: Advice on key expansion for HMAC-SHA-1-96	SAGE (02) 27	Response LS in 401
S3-020421	LS from CN WG5 on OSA Security	N5-020569	Noted
S3-020438	LS from SA WG5: Reply on Packet Switched Streaming (PSS) in Rel-6 Work Programme	S5-024235	Noted
S3-020439	LS from SA WG5 on Diameter security issues	S5-024240	POSTPONED to NEXT MEETING

E.2 Liaisons from the meeting

TD number	Title	Comment/Status	TO	CC
S3-020398	Reply LS on Status of protocol work on Ze interface (N4-020769)	Approved	**CN WG4**	
S3-020399	LS on OFM and the IMS service (response to LS T3-020379 on OFM and the IMS service)	Approved	**T WG3**	
S3-020403	Reply LS on Push Security (response to LS *S1-020541* on Push Security from SA1)	Approved	**SA WG1**	**SA WG2**
S3-020408	LS on Network Authentication Failure in the UE	Approved	**CN WG1**	
S3-020417	Same SA to be utilized for both UDP and TCP transport protocols	Approved (attachment S3-020416)	**CN WG1**	
S3-020437	IMS authentication vector distribution on the Cx interface	Approved (attachment S3-020419)	**CN WG4**	
S3-020440	LS on introduction and adoption of A5/3 and GEA3	Approved (link to attachment S3-020360.zip)	**Manufacturers for Comment, GSM Association Security Group and TWG**	**TSG SA ETSI SAGE**
S3-020441	Bye and Response attacks in IMS	Approved (attachment S3-020381)	**CN WG1**	
S3-020445	Security aspects of A/Gb evolution	Approved	**GERAN**	**SA Wg2 CN WG1 CN WG3**
S3-020446	Indication of call termination as a result of IST operation	Approved	**SA WG5**	
S3-020447	LS on architecture and requirements for subscriber certificates (response to LS (S2-022047/S3-020356) on "LS on subscriber certificates" from SA2 and LS (T2-020574/S3-020333) on the same subject from T2)	Approved	**SA WG1 SA WG2**	**T WG2**
S3-020448	Release 6 WID on User Equipment Management – security aspects (response to LS *S5-022110* on Release 6 WID for User Equipment Management)	Approved (attachment S3-020432)	**SA WG5 SWG-A**	**T WG2 T WG3**
S3-020449	Response to Liaison statement on the MBMS security	Approved (attachment S3-020433)	**SA WG2**	**SA WG1 RAN WG2**
S3-020452	LS on 3GPP System to WLAN Inter working architecture (TR 23.934) (response to LS Tdoc S2-022022 (S3-020354) on 3GPP System to WLAN Inter working from SA2)	Approved (attachments: WLAN Interworking Security WID Draft TR Wireless Local Area Network (WLAN) Interworking Security)	**SA WG2**	
S3-020453	WLAN Ownership, Operations and Internetworking Trust (response to LS (S1-021186**)** on WLAN Interworking)	Approved (attachments: WLAN Interworking Security WID Draft TR Wireless Local Area Network (WLAN) Interworking Security)	**SA WG1**	

Annex F: Actions from the meeting

AP 24/01: K Boman agreed to check TS 33.203 for ISIM/USIM Terminology and respond to the contact person for the LS in TD S3-020336 (M. de Groot).

AP 24/02: A. Escott to update TD S3-020450 and send for approval. A 2 week comments period (29 July) and 1 week to update (2 August) and send for approval. Approval deadline 16 August 2002.

AP 24/03: A. Escott to initiate an e-mail discussion with SA WG3/CN WG1 on SA and registration lifetimes in order to have quick resolution of this issue at the next meeting.

AP 24/04: P. Howard to lead an e-mail discussion group to discuss IST issues.

AP 24/05: Various: Volunteers listed in Subscriber Certificates open issues list (see agenda item 7.7) to progress discussions and report to next meeting.

AP 24/06: L. Lopez Soriato update WLAN TS based on comments received for next meeting.

AP 24/07: M. Walker to produce TD S3-020428 (response to letter to SA WG3 Chairman in TD S3-020337) and copy to SA WG3 list.