

---

**Source:** SA WG3 Secretary (MCC)  
**Title:** Reports of SA WG3 meetings #25 and #26  
**Document for:** Information  
**Agenda Item:** 7.3.1

---

SA WG3 has held 2 meetings since TSG SA#17, as follows:

S3#25	8 - 11 October 2002	Munich, Germany	Siemens
S3#26	19 - 22 November 2002	Oxford, UK	European Friends of 3GPP

Attached are the approved report of meeting #25 and the draft report of meeting #26.

**3GPP TSG SA WG3 (Security) meeting #25**

**8-11 October 2002, Munich, Germany**

---

**Source: Secretary SA WG3**  
**Title: Draft Report of SA WG3 meeting #25 - version 1.0.0**  
**Status: Approved**

---

**Draft Report**



**Munich Clock Tower**

**Contents**

**1 Opening of the meeting ..... 3**

**2 Agreement of the agenda and meeting objectives ..... 3**

2.1 3GPP IPR Declaration ..... 3

**3 Assignment of input documents..... 3**

**4 Reports from 3GPP SA3 meetings..... 3**

4.1 SA3#24, 9-12 July 2002 ..... 3

4.2 SA3 LI #12, 24-26 September 2002 ..... 4

**5 Report from SA#17, 9-12 September 2002..... 4**

**6 Reports and liaisons from other groups ..... 5**

6.1 3GPP working groups..... 5

6.2 IETF co-ordination ..... 5

6.3 ETSI SAGE ..... 5

6.4 GSMA SG ..... 5

6.5 3GPP2 ..... 6

6.6 TIA TR-45 ..... 6

6.7 Other Groups ..... 6

**7 Technical issues ..... 6**

7.1 IP multimedia subsystem (IMS) ..... 6

7.2 Network domain security: IP layer (NDS/IP) ..... 7

7.3 Network domain security: MAP layer (NDS/MAP) ..... 7

7.4	UTRAN network access security .....	8
7.5	GERAN network access security.....	9
7.6	Immediate service termination (IST).....	9
7.7	Support for subscriber certificates .....	9
7.8	Digital rights management (DRM) .....	11
7.9	WLAN inter-working.....	11
7.10	Visibility and configurability of security .....	13
7.11	Push.....	14
7.12	Priority.....	14
7.13	Location services (LCS) .....	14
7.14	User equipment functionality split (UEFS).....	14
7.15	Open service architecture (OSA).....	14
7.16	Generic user profile (GUP) .....	14
7.17	Presence.....	14
7.18	User equipment management (UEM).....	15
7.19	Multimedia Broadcast/Multicast Service (MBMS) .....	15
7.20	PKI-based key management for network domain security .....	16
<b>8</b>	<b>Review and update of work programme.....</b>	<b>17</b>
<b>9</b>	<b>Future meeting dates and venues.....</b>	<b>17</b>
<b>10</b>	<b>Any other business.....</b>	<b>17</b>
<b>11</b>	<b>Close.....</b>	<b>18</b>
	<b>Annex A: List of attendees at the SA WG3#24 meeting and Voting List.....</b>	<b>19</b>
A.1	List of attendees.....	19
A.2	SA WG3 Voting list.....	20
	<b>Annex B: List of documents .....</b>	<b>21</b>
	<b>Annex C: Status of specifications under SA WG3 responsibility.....</b>	<b>28</b>
	<b>Annex D: List of CRs to specifications under SA WG3 responsibility agreed at this meeting .....</b>	<b>32</b>
	<b>Annex E: List of Liaisons .....</b>	<b>33</b>
E.1	Liaisons to the meeting .....	33
E.2	Liaisons from the meeting.....	34
	<b>Annex F: Actions from the meeting .....</b>	<b>35</b>

## 1 Opening of the meeting

The SA WG3 Vice Chairman, V. Niemi, opened the meeting and welcomed delegates to Munich. The meeting was hosted by Siemens. G. Horn welcomed everybody on behalf of Siemens and provided the domestic arrangements for the meeting.

## 2 Agreement of the agenda and meeting objectives

[TD S3-020455](#) Draft agenda for meeting #25. The agenda was **approved** without change.

### 2.1 3GPP IPR Declaration

The SA WG3 Vice Chairman reminded delegates of their responsibilities regarding the declaration of essential IPRs.

## 3 Assignment of input documents

The available documents were allocated to their respective agenda items. It was noted that the late documents (received after 17.00 CET, Thursday 3 October 2002) would be dealt with if possible, but priority would be given to dealing with documents that were already submitted before the deadline.

## 4 Reports from 3GPP SA3 meetings

### 4.1 SA3#24, 9-12 July 2002

[TD S3-020456](#) Draft Report of meeting #24 - vsn 0.0.3. The report was reviewed by the meeting.

Actions from meeting #24:

- 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).  
This had been completed. No changes were necessary from SA WG3.
- 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.  
Completed.
- AP 24/04:** P. Howard to lead an e-mail discussion group to discuss IST issues.  
Ongoing - e-mail discussion to be re-initiated for reporting to the next SA WG3 meeting.
- AP 25/01:** P. Howard to lead an e-mail discussion group to discuss IST issues and report to next SA WG3 meeting.
- AP 24/05:** Various: People listed in Subscriber Certificates open issues list to progress discussions and report to next meeting.  
Completed. Various e-mail discussions took place and inputs provided to the meeting. The Lawful Interception implications are still to be discussed in the LI group. It was noted that a WID has been created in the LI group.
- AP 25/02:** (B. Wilhelm / C. Brookson) LI group to consider implications of Subscriber Certificate work on LI.
- AP 24/06:** L. Lopez Soriato update WLAN TS based on comments received for next meeting.  
Completed.
- 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.  
Completed.

Changes as follows were requested: TS 33.201, TS 33.903 to be deleted. TR 33.900 to be Rel-6. The status of TS 42.009 should be checked (i.e. whether or not it should be continued into Rel-5). For the FIGS specifications, the FIGS WI is no longer supported. **C. Brookson agreed to ask operators whether any development on FIGS functionality was required. A decision whether or not to continue FIGS into Rel-6 will be taken at the next meeting.**

**AP 25/03: C. Brookson to circulate draft 33.900 to SA WG3 for update and approval at next meeting as a Rel-6 TR.**

**AP 25/04: C. Brookson to ask operators whether there is any support for FIGS in Release 6 and report to SA WG3 meeting #26.**

## 4.2 SA3 LI #12, 24-26 September 2002

**TD S3-020488** Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #3/02 on lawful interception. This was provided for information and was **noted**.

**TD S3-020489** Proposed CR to 33.107-5.4.0: Event Time (Rel-5). This CR was **approved**.

**TD S3-020490** Proposed CR to 33.107-5.4.0: Essential correction to the LI events generated during inter-SGSN RAU, when PDP context is active (Rel-5). The affected Specification was identified as 33.108, **it was reported that this CR was under e-mail discussion on the LI list and would be presented for approval after their next meeting.** The CR was **noted**.

**TD S3-020494** Proposed CR to 33.108-5.1.0: Essential correction to the LI events generated during RAU, when PDP context is active (Rel-5). "lease" will be changed to "least" in 6.5.1.2. The added-then-deleted text in the table title in Table 6.11a will be removed. The CR was updated and provided in **TD S3-020546. It was reported that this CR was under e-mail discussion on the LI list and would be presented for approval after their next meeting.** The CR was **noted**.

**TD S3-020491** Proposed CR to 33.108-5.1.0: Essential corrections to the Annex C.1 (ULIC) - (Rel-5). This CR was **approved**.

**TD S3-020492** Proposed CR to 33.108-5.1.0: Missing PDP Context Modification event (Rel-5). This CR was **approved**.

**TD S3-020493** Proposed CR to 33.108-5.1.0: Aggregation of IRI Records (**Rel-6**). This CR was **approved**.

**TD S3-020496** WI Description: Lawful Interception in the 3GPP Rel-6 architecture. This WI description was **approved**.

**TD S3-020497** LS on change to LI email subscription and access controlled SA3-LI document area. **It was thought that detailed arguments explaining why this change is needed should be provided before SA WG3 (or TSG SA) are likely to make a decision on this proposal.**

**AP 25/05: B. Wilhelm to ask the LI group to provide more information on the reasons for the restricted access to the LI FTP area, in order for a better understanding of the issues involved for SA WG3 and TSG SA to be gained in considering the request (re: TD S3-020497 / S3LI02\_155r1).**

## 5 Report from SA#17, 9-12 September 2002

**TD S3-020498** Report on SA#17 for SA3. This was introduced by the SA WG3 Vice Chairman and was reviewed.

- It was noted that 22.022 was a SA WG3 specification and it had now been upgraded to version 5.0.0 by the MCC Secretary.
- The A5/3 deadline had been proposed as October 2004 and was expected to be announced at the next GSMA meeting (October 2002). It was noted that this includes GEA3 as a mode of A5/3 working.
- Removal of MAPsec Automatic Key management from Release 5. **M. Pope agreed to try to find the necessary changes needed to remove the automatic Key management from Release 5, using the latest Release 4 and Release 5 versions.** (see agenda item 7.3, **TD S3-020568**).

- GERAN Security: Enhanced A/Gb mode. Status needs to be clarified at next TSG SA Plenary.

The Chairman's report from the TSG SA meeting #17 was then **noted**.

**TD S3-020543** Draft report of TSG SA meeting #17 - version 0.0.4. This was provided by the Secretary for information.

The GSA3 A5/3 Algorithm report was thought in need of clarification, in order not to mislead readers on the implications. The SA WG3 Chairman will provide a comment to the draft report on this and provide information to the next TSG SA meeting in the SA WG3 Chairman's report to TSG SA.

It was **noted** that **TD SP-020513** (WID NDS/IP) had been approved (not reported in the draft report).

The draft report of TSG SA meeting #17 was then **noted**.

## 6 Reports and liaisons from other groups

### 6.1 3GPP working groups

**TD S3-020462** LS reply on Packet Switched Streaming (PSS) in Rel-6 Work Programme. This was **noted**.

**TD S3-020464** LS reply on "Answer to "LS on PSS Release 6 work programme"". This was **noted**.

**TD S3-020467** New requirements about functionality to make subscription to different domains independent or linked based on operator decision. It was noted that the attached CR had been **rejected** at TSG SA#17. A related LS had been forwarded to SA WG3 in **TD S3-020468** "Response to T3-020406/S1-021427 (Response "Liaison Statement on Access to IMS Services using 3GPP release 99 and release 4 UICCs" (S1-020577))". This was provided for information and was **noted**. A response LS to **TD S3-020467** and **TD S3-020468**, noting the discussion at SA WG3 on ISIM and USIM security requirements being the same from a Security perspective, was provided in **TD S3-020561** which was modified and updated in **TD S3-020577** which was **approved**.

**TD S3-020469** LS on Speech Enabled Services. The attached TR 22.977 and TS 22.243 should be reviewed and contribution made to next meeting. L. Finklestein agreed to start an e-mail discussion on this and provide a response LS by 4 November 2002. Comments to be provided to L. Finklestein by 21 October 2002. Approval of resulting LS on 4<sup>th</sup> November 2002.

**TD S3-020470** Draft Working Item Description PSS Rel-6 and LS response to:

"Answer to Liaison Statement regarding PSS Release 6 work programme" (S2-022050/ S4 (02)0375) from SA2, and "LS reply on Packet Switched Streaming (PSS) in Rel-6 Work Programme" (S5-024235/S4(0)0376) from SA5. No comments were made on the attached WID and their next meeting had already been held. The LS was then **noted**.

### 6.2 IETF co-ordination

This was covered under specific areas in Agenda Item 7.

### 6.3 ETSI SAGE

P. Christoffersson provided a verbal report of the work in ETSI SAGE. The reported Attack from Crypto was not considered a real attack, but rather a demonstration of a theoretical method for attack of the algorithm and was considered of low impact. A study on Plaintext redundancy was identified as needed. **Resources were needed to help with this study and delegates were asked to forward any names to help with this.**

### 6.4 GSMA SG

C. Brookson provided a verbal report. Discussions on HS theft - government legislation and input of EIR needed. GSMA have put on a shared part of the CEIR, which can be fed by Operators. Data integrity is an issue, as old blacklist equipment is still on the system. A new PRD on Security policy between operators in order to help with roaming agreements. A Security Advice service is under consideration to provide advice on Network Security to Operators.

SA WG3 delegates were invited to the next meeting 27-28 November 2002 in Ireland. Interested people should contact C. Brookson.

MILENAGE 2G: The new name for this algorithm is under consideration (possibly "G-MILENAGE", or "GSM-MILENAGE"). The algorithm will be delivered by ETSI SAGE to SA WG3. Partners' agreements will be required and the Distribution agreements between 3GPP and GSMA will need to be agreed upon.

## 6.5 3GPP2

The TSG S Security group was reported to be known as "TSG-S WG4", which should be reflected in future agendas. Main items - common algorithms for 3GPP2; 3GPP2 documents S-0033, S-0055 and SP-0078.

## 6.6 TIA TR-45

The AHAG group was reported to be meeting only each 3 months, joint with the TR-45 Plenary and are currently only working on maintenance of TDMA algorithm work. Joint meetings with AHAG was thought unnecessary at present. The co-operation agreements may be reviewed.

## 6.7 Other Groups

There were no specific contributions under this agenda item. Inputs were dealt with under their topics in agenda item 7.

## 7 Technical issues

### 7.1 IP multimedia subsystem (IMS)

[TD S3-020495](#) Interception regarding IMS. This was a contribution to the LI group Helsinki meeting. The contribution was **noted** by SA WG3, and further discussion was requested within the LI group, based on this and additional contributions to their meeting.

[TD S3-020458](#) LS on Diameter security issues. A related LS was postponed from the previous meeting in [TD S3-020439](#) "LS from SA WG5 on Diameter security issues". A response to SA WG5 was produced, informing SA WG5 that SA WG3 agree with CN WG4 that NDS/IP can be used to secure the interfaces. SA WG3 still need to verify whether the latest DIAMETER draft includes the requirements in the NDS/IP specification. This LS was provided in [TD S3-020547](#) which was updated in [TD S3-020576](#) and **approved**.

[TD S3-020485](#) Response to IETF LS on Interoperability Issues and SIP in IMS. This was introduced by Ericsson. It was noted that as much work as possible would need to be done to finalise Rel-5 work by December 2002. The contribution was then **noted**.

[TD S3-020480](#) Liaison statement on Interoperability Issues and SIP in IMS. This was introduced by Nokia and provides an analysis of items needing work for completion of Release 5. Items 3 and 5 were thought necessary to consider immediately, and Item 2 should also be considered. For item 3, it was noted that end-to-end integrity cannot be provided if the headers are modified at intermediate nodes. For Item 5, CN WG1 view was considered OK. No changes to the security requirements were expected. A response was provided in [TD S3-020550](#) which was updated in [TD S3-020578](#) and **approved**.

[TD S3-020516](#) IETF status report: SIP security agreement. This was introduced by Ericsson and proposed that SA WG3 decide on a deadline for the completion of SIP-sec-agree for inclusion in Rel-5. It proposes the IETF meeting as a deadline and a backup plan to be sure of a fall-back solution for November 2002. The idea for a back-up plan, in case of no approval of the draft by the IETF, was **approved** by SA WG3. A solution is needed for December Plenary in order to complete this for Rel-5. Co-operation with CN WG1 is needed to ensure that any CRs needed for the December Plenary are prepared in good time. A LS informing CN WG1 of these proposals was provided in [TD S3-020551](#) which was modified slightly in [TD S3-020580](#) and **approved**.

[TD S3-020457](#) Secure registration of IP addresses. This was introduced by Nokia and asks SA WG3 to take into account the mechanism employed when setting up the SA in the P-CSCF. A CR related to this was provided at the last meeting in [TD S3-020375](#) which was again reviewed. A CR was produced in [TD S3-020553](#) which was **approved**.

[TD S3-020460](#) IMS authentication vector distribution on the Cx interface. This was introduced by Ericsson and was **noted**.



[TD S3-020499](#) Proposed CR to 33.203-5.3.0: Sending error response when P-CSCF receives unacceptable proposal (Rel-5). This was introduced by Nokia and aligns stage 2 and stage 3 specifications. It was reported that the *4xx\_Unacceptable\_Proposal* message had been introduced to keep the specification generic. This CR was updated slightly in [TD S3-020554](#) and was **approved**.

[TD S3-020513](#) Proposed CR to 33.203: Indication in the UE that the SA is no longer active in P-CSCF (Rel-5). This was introduced by Ericsson and attempted to clarify the procedure for detecting no longer active SAs. The CR was revised in [TD S3-020555](#) which was **approved**. A LS to CN WG1 was provided to check any impact of this CR to their specifications 24.228 and 24.229 was provided in [TD S3-020556](#) which was modified in [TD S3-020579](#) and **approved**.

[TD S3-020514](#) The use of SAs in IMS user authentication failures. This was introduced by Hutchison 3G UK and proposes that the P-CSCF should always rule out the case in which P-CSCF sends an error message in SM12 unprotected. A related CR was provided in [TD S3-020515](#) which was modified in [TD S3-020558](#) and **approved**.

[TD S3-020527](#) Registration and SA lifetimes. This was presented by Hutchison 3G and reviewed the discussion so far on the binding between SA and registration lifetimes, in order to help SA WG3 reach a consensus on one of the discussed solutions or to develop an alternative solution. After some discussion, an evening session was set up for interested parties to discuss and return with an agreed proposal. The evening session reported that more time was required and an e-mail discussion will be held, and A. Escott agreed to lead this and draft a new CR proposal.

**AP 25/06: A. Escott to lead e-mail discussion group on registration of SA lifetimes and provide a CR for SA WG3 meeting #26.**

[TD S3-020548](#) Proposed CR to 33.203: Re-use and re-transmission of RAND and AUTN (Rel-5). This was introduced by Ericsson and proposes the removal of an editors note as there is no longer any need for it. There was a request that the actions of the S-CSCF should be added to the specification if the editors note is removed - text from the conclusions in the *Reasons for Change* could be used for this purpose. It was agreed that this could be attempted overnight and a revised CR was presented in [TD S3-020560](#). The CR was discussed and modified in [TD S3-020590](#). It was agreed that these issues should be discussed and the CR updated and presented to the next SA WG3 meeting (CR **postponed**).

[TD S3-020567](#) Due to an error in document number allocation, this was provided with a new number after the meeting [TD S3-020591](#) will also be subject to this e-mail discussion for presentation to the next meeting.

[TD S3-020559](#) Proposed CR to 33.203: Clean up one Editor's note in 33.203 (Rel-5). This was introduced by AT&T Wireless and proposed the removal of an editors note as the Hiding mechanism for Rel-5 no longer depends upon the issues described by the editors note. This CR was **approved**.

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

[TD S3-020536](#) Security need evaluation of UTRAN and GERAN IP transport interfaces. This was introduced by Nokia and recommended to have encryption and integrity protection on Iu interface. A lower priority proposal was to use integrity checking for control plane interfaces that are IP based, which are namely Iur, Iub, Iupc, Iur-g and Iu-BC. As the Gb interface is already covered by encryption in SGSN, it does not need to be secured by the NDS/IP mechanism. After some discussion, it was **agreed** that as a working assumption, **protection of the RANAP protocol over the Iu interface would be given the highest priority**. CRs on this topic were requested, for the higher priority interfaces first and the lower priority interfaces will be dealt with after these.

[TD S3-020552](#) Proposed CR to 33.210: Adding requirement to provide mandatory support for 3DES encryption in NDS/IP. Remove AES references and dependencies (Rel-5). This was introduced by Telenor and proposed the removal of AES, which is not complete in the IETF, and mandating support of 3DES. This CR was modified slightly and revised in [TD S3-020562](#), updated again to include equivalent changes to section 5.4 in [TD S3-020563](#) which was **approved**.

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

[TD S3-020481](#) LS on Status of protocol work on Ze interface. This was introduced by Nokia and was provided by CN WG4 to SA WG3 for information. The LS was **noted**.



[TD S3-020568](#) Proposed CR to 33.200: Removal of Automatic Key Management from Rel-5 (Rel-5). This CR was **postponed** and **A. Escott agreed to check the necessary changes off line and represent the CR to the next meeting.**

## 7.4 UTRAN network access security

[TD S3-020482](#) LS on re-used of START value for ciphering of RB using RLC TM during SRNS relocation. This was introduced by Nortel Networks. RAN WG2 asked SA WG3:

- *whether SA WG3 consider that the R'99 handling of ciphering of RB using RLC TM during SRNS relocation by re-using COUNT-C values is a security problem that needs correction in further releases (Rel-4 onwards).*
- *If yes, RAN WG2 asks SA WG3 if the attached proposal is in line with the SA WG3 principles, is more secure compared to the solution adopted in Release 1999 and looks acceptable as far as SA WG3 are concerned.*

The attached document (R2-022550) discussed the proposal for consideration by SA WG3.

SA WG3 **agreed** that the described problem should be addressed in Rel-4 RAN specifications. Some issues with backward compatibility to Release 1999 mobiles and the specification of the value of "x" (needs to be positive and of a large enough value). A response LS was provided in [TD S3-020564](#) which was modified in [TD S3-020583](#) and **approved**.

[TD S3-020483](#) LS to SA WG3 on Group release security solution. This was introduced by Ericsson. RAN WG2 asked SA WG3 to answer the following questions:

- 1 *If group release functionality is introduced in RRC signalling is a security mechanism needed or not?*
- 2 *If the answer to question 1 is that it is needed, can SA WG3 guide RAN WG2 on possible ways to limit UE implementation impacts, e.g. on the possible reuse without modifications of one of the Release 1999 security blocks (F8 or F9).*

The following related contributions were considered:

[TD S3-020510](#) Group Release Authentication algorithm. This was introduced by Ericsson and requested support from SA WG3 to agree on that HMAC SHA-1 is used to create the Group Indicia and that the indicia as well as the key are 128 bits long. If so, Ericsson suggested that SA WG3 send an LS with the requirements to RAN WG 2. The LS should also inform RAN WG 2 that SA WG3 expects to approve a CR against TS 33.102 at SA WG3 meeting #26, if RAN WG2 adopt the Group Release function. [TD S3-020388](#) (from meeting #24) was a LS from ETSI SAGE on the suitability of the f9 and f8 functions for the Group Release function (this had been copied to RAN WG2). Although the LS indicates a variant of f8 would be best, it also indicated that f8 is adequate, and in order to meet timescales for RAN WG2, the use of f8 was considered the best choice.

[TD S3-020537](#) Group release security mechanism. This was presented by Lucent Technologies and discusses the need for protection of the Group Release mechanism, and the need for protection of individual Release messages.

It was agreed that the impact of not protecting against the cost of protecting the Group Release function required further study. Other existing similar attacks should also be analysed to determine the efficiency of protection and the need for protection of other mechanisms. B. Owen agreed to lead an e-mail discussion to conclude on this issue. A LS to RAN WG2 was provided in [TD S3-020565](#) which was modified slightly in [TD S3-020584](#) and **approved**.

**AP 25/07: B. Owen to lead an e-mail discussion to conclude on the need to secure the Group Release function.**

If it is agreed that a protection mechanism is needed, ETSI SAGE were asked to provide information of the use of f8 and Qualcomm agreed to produce a CR to 33.102 based on this for the next SA WG3 meeting. **P. Christoffersson agreed to co-ordinate this with G. Rose.**

**AP 25/08: P. Christoffersson (mechanism) and G. Rose (CR to 33.102) to co-ordinate the use of f8 to provide protection for Group Release mechanism, if the SA WG3 e-mail discussion on the need to have protection concludes that protection is desirable.**

[TD S3-020585](#) Proposed CR to 33.102 for information: USIM support in GERAN only terminals (Rel-5).

**NOTE:** The title on the CR sheet is incorrect and should read "Group Release Authentication Function".

This was provided for information and will be submitted if the need for Group Release protection is confirmed.

## 7.5 GERAN network access security

[TD S3-020474](#) Response LS on Security enhancements for GERAN. This was introduced by Ericsson. TSG GERAN asked SA WG3 whether there is a plan to create work items to enhance GERAN Security for A/Gb mode. This was in response to GERAN document GP-022491, which had been elaborated by Vodafone following SA WG3 e-mail discussions. **P. Howard agreed to develop a WID for GERAN Security enhancements. Contribution and indication of supporting companies were invited for this**, This will be submitted to the next SA WG3 meeting. A reply LS was provided in [TD S3-020566](#) which was modified slightly in [TD S3-020589](#) and **approved**.

**AP 25/09: P. Howard to develop WID for GERAN Security Enhancements (Rel-6).**

[TD S3-020477](#) Reply LS on "Gb evolution". This was introduced by Nokia and summarised the result of discussions in SA WG2. There were no actions on SA WG3, and delegates were asked to take the LS into account for SA WG3 work on Gb evolution. The LS was then **noted**.

[TD S3-020540](#) Reply LS on "Gb evolution". This was introduced by Vodafone. TSG GERAN informed SA WG2 on WIDs created related to Gb evolution. It was reported that the joint GERAN/SA WG2 meeting had been set for 21-22 October in Sweden. This LS was **noted** and it was decided to copy the LS in [TD S3-020589](#) (see above) to SA WG2 for information.

[TD S3-020503](#) Proposed CR to 33.102: USIM support in GERAN only terminals (Rel-5). This was introduced by Siemens and was revised in [TD S3-020567](#). **This will be subject to an e-mail discussion for re-presentation to the next meeting**.

[TD S3-020545](#) A5/3 and GEA3 and their relation with EGPRS. This was introduced by Ericsson and questions the use of A5/3 for EDGE and the data-rate for EGPRS and asks SA WG3 to discuss the issues raised in order to provide any necessary CRs to the next SA WG3 meeting. It was confirmed that A5/3 and GEA3 were suitable for both GSM/GPRS and EDGE variants, the algorithm specifications are unclear on this: **The modulation scheme used in the PS domain does not affect the GEA3 algorithm mechanism. A5/3 (CS domain) has 2 modes of use, GSM standard mode and GSM EDGE mode**. No CR to TS 43.020 was thought necessary, as implementers need to look at the algorithm specifications where the two modes of operation are clarified. It was agreed, however, to create a CR to the Technical Report TR 55.919 to clarify the use of the term "EDGE" in the specifications and the EGPRS bit-rates. **K. Boman agreed to do this for the next SA WG3 meeting**.

**AP 25/10: K. Boman to clarify the use of the term EDGE for CS and PS domains in TR 55.919 (CR to be drafted).**

## 7.6 Immediate service termination (IST)

There were no specific contributions under this agenda item.

## 7.7 Support for subscriber certificates

[TD S3-020463](#) Liaison Statement from SA WG1 on subscriber certificates. This was introduced by Nokia and informs SA WG2, SA WG3 and T WG2 that SA WG1 have added a new section to TS 22.105, in response to LSs received on subscriber certificates, which is copied in the LS. It was not clear whether SA WG1 allowed the visited network to issue service usage certificates, which was the question asked by SA WG3 in the LS to SA WG1. It was considered that SA WG1 do not need to specify who issues the certificates, and this should be specified by SA WG3. The LS was **noted**.

[TD S3-020471](#) LS from T WG3 on Subscriber Certificates. This was introduced by Motorola. T WG3 call the attention of SA WG3 to the Digital Identity Module (DIM) work item recently approved by ETSI SCP. One objective of this effort is to find common elements in the various identity modules (xIM's) and to centralize these elements in a general-purpose card service. It is expected that subscriber

certificate handling and public and private key operations will be part of this common core. This LS was **noted**. The developments of DIM work should be monitored by SA WG3.

**TD S3-020479** LS response from CN WG1 on subscriber certificates. This was introduced by Nokia. The LS was **noted**. SA WG3 should monitor progress and send details and requests for information to CN WG1 as and when needed.

**TD S3-020486** Architectural choices for Subscriber Certificates. This was briefly presented by Nokia and described a number of possibilities for the provision of subscriber certificates and discusses the advantages and disadvantages of each proposal. The presentation was related to the results of the e-mail discussions on subscriber certificates. The involvement of the IETF in the IMS option was clarified that it could be specified inside SIP. The 4 proposals were analysed and discussed. It was thought that the response from SA WG2 should be taken into account after they deal with the LS at their meeting. The presentation was **noted** and delegates were asked to keep these options in mind for further discussion at the next meeting with feedback from SA WG2.

**TD S3-020487** Digital Signatures: Who is doing what? This was introduced by Orange and collects together information on ongoing work on Digital Signatures. The document was **noted** and SA WG3 would continue to monitor the work ongoing in this area.

**TD S3-020541** Conclusions on Proof of Possession discussion. This was introduced by the SA WG3 Vice Chairman and provided the conclusions of the e-mail discussion on PoP. The comments received over the e-mail discussions were presented and the general conclusions were that there are three options for 3GPP:

1. *mandate PoP in all cases; This has the side effect that at least some use cases will be prevented.*
2. *mandate PoP at least when use of key includes anything other than the commitment type. This assumes that application developers will correctly check the `keyUsage` parameter and clearly indicate it to the user.*
3. *do not require PoP at all. This assumes that the certificates will be used with applications and application protocols which are well designed (3GPP specifications can clearly indicate what "well designed" means in this context).*

The concluding recommendation was for the option 3, for the following reasons:

- *trying to provide protection from badly designed applications or application protocols is not advisable: it might lead to the CA operator being liable for any design error made by arbitrary application developer.*
- *the specification should not have a feature that does not have a compelling reason; the only reasons we found so far in the above discussion is basically "protecting potential victims from badly designed applications or application protocols".*

The paper was discussed and **noted**.

**TD S3-020542** Trust and PKI email discussion input paper. This was briefly reviewed for information on the input paper for the e-mail discussion. This was **noted** and taken into account for the discussion of related input papers.

**TD S3-020500** Contribution to discussion on architecture and trust for subscriber certificates. This was introduced by Siemens and provided discussion material on architecture options for trust and subscriber certificates. It was agreed that some level of standardisation of certificates was required, but the exact level of standardisation required further study and discussion. The evolution paths for deployment and roaming issues were suggested to be similar to the evolution of GPRS service offering. This would need further discussion. Revocation of certificates was argued to be more efficient than the use of short-lived certificates. This would require connection for the revocation to complete. Short-lived certificates may remove the need for OCSB servers. Certificate management on the UE would require further analysis (space considerations for storage of certificates). The complexities of interfaces between CA\_S and HLR versus CS\_S and SGSN requires further investigation and discussion. Authentication vs. Authorisation: Value-added service permissions may need to be added to user profiles. Proposals for criteria for an evaluation of architectural choices was outlined in section 10 of the contribution, **it was agreed that this could be taken into account as criteria for future discussion.**

It was generally agreed that the choice of Architecture for Subscriber Certificates requires more study and discussion within SA WG3 (in conjunction with the work ongoing in SA WG2).

It was mentioned that with the large number of issues raised on Subscriber Certificates, that the original Work Item predicted timescales and scope of work may need reviewing.

**TD S3-020509** Issuing Subscriber Certificates at Application Layer. This was introduced by Ericsson and discussed an alternative approach for issuing subscriber certificates at application layer, Ericsson preferred Application layer (instead of some lower layer) in order to promote access independency.

It was suggested that SA WG3 takes the following as working assumptions in relation to subscriber certificates:

1. Application layer approach.
2. Home network controlled model.

It is also suggested that SA WG3 should study if IMS could be re-used for certificate management.

The points provided in this contribution were discussed in length. Further discussion was recognised to be necessary on the issues raised.

**TD S3-020512** Contribution to discussion on subscriber certificates. This was introduced by Orange and discussed the need for Home Control of certificates in order to limit the potential damage due to complaints from customers receiving services from third parties. *Most importantly, Orange would like to see the requirement for home control to be addressed in the solution that SA WG3 adopt for support of subscriber certificates. Secondly, Orange also believe that the possibility to build an inter-operator PKI for that support should be carefully examined because it provides a better solution for the purpose of the work item.*

It was agreed that Home control needs to be handled as it is a service requirement from SA WG1. The solution adopted for this needs further discussion.

## 7.8 Digital rights management (DRM)

There were no specific contributions under this agenda item.

## 7.9 WLAN inter-working

**TD S3-020570** Cellular – WLAN Interworking: Activities in ETSI/MMAC and WIG Status. Dr. Robert Hancock, Siemens / Roke Manor Research provided a presentation of an overview of the Activities on Wireless LAN and the status of the ETSI/MMAC and WIG work. A LS from WIG to TSG SA, which will be copied to SA WG3 is about to be forwarded which provides the scope of WIG and information on their work.

For information, the WIG e-mail reflector list is [WIG@list.etsi.fr](mailto:WIG@list.etsi.fr)

Conclusions (from slides):

- *based initially on ETSI work, WIG can serve to define a reference point and protocols which enable 3GPP “core” networks to exploit any WLAN technology;*
- *the W.2 interface can be used as a vehicle for defining concrete requirements on the WLAN part of the overall system:*
  - *Very important, especially for security.*

Dr. Hancock was thanked for the presentation which formed useful background on the work ongoing and security issues to be tackled for WLAN interworking. The presentation was then **noted**.

**TD S3-020476** LS (from SA WG2) on 3GPP System to WLAN Inter working architecture. This was introduced by Ericsson and provides comments on the feedback received from SA WG3 on TR 23.934 and asked SA WG3 to provide feedback on the work split proposal as well as on the issue of identity protection.

Work Split

- Security framework: SA WG3 would be responsible for the security framework, e.g. security features on relevant interfaces.
- EAP Methods: Though specific methods have been identified by SA WG2, i.e. EAP-SIM and EAP-AKA, SA WG2 doesn't not have the expertise to specify the methods to be used on top of EAP. Thus SA WG2 wishes that SA WG3 would design the authentication methods to be used on top of the EAP framework.

For EAP methods, it was thought that the use of the word "design" was misleading, and SA WG3 are only asked to specify suitable methods.

It was commented that the protection of handovers may be more difficult as handovers are likely to be more frequent than in normal 3GPP networks. The Allocation and storage of Temporary Identities also needs further study.

It was clarified that SA WG2 have now removed the detail of the internal WLAN structure from their specification.

It was agreed that the target is to have equivalent level of security for WLAN interworking as is available for 3GPP systems.

A LS to reply to the questions from SA WG2 was provided in [TD S3-020571](#) and updated in [TD S3-020586](#) which was **approved**.

[TD S3-020511](#) IETF and WLAN Authentication Methods. This was introduced by Nokia and documented the status of IETF documents used for WLAN Authentication and outlines the Recent Changes in EAP AKA and EAP SIM drafts. The document encouraged SA WG3 members to actively participate the IETF mailing list discussion about the open issues in the IETF drafts related to WLAN interworking.

Ericsson and Nokia were thanked for this investigation and report and SA WG3 members were asked to help ensure progress on WLAN drafts in the IETF in order to finalise the drafts in good time for use in Release 6. The contribution was then **noted**.

[TD S3-020517](#) Use of smart cards in WLAN interworking. This was introduced by GemPlus and provided reasons to use Smart Cards in WLAN. There was a lot of discussion on this and many companies did not see a great value in creating another application WSIM when the USIM should be used (and enhanced if it does not currently cover the security requirements).

**GemPlus were asked to re-develop the proposal and prepare more details on the e-mail list for further discussion at the next meeting.**

[TD S3-020518](#) Pseudo-CR to WLAN Interworking draft: Editorial changes concerning the term "SIM/USIM-based authentication" (Rel-6). This was introduced by GemPlus and tidies up the text of clause 6.1.1, removing the "SIM" part as the clause is dedicated to USIM authentication. It was pointed out that this had been added explicitly by the editor of the draft. **The Editors (L. Lopez, C. Blanchard) were asked to verify the reason for this and correct if appropriate.**

[TD S3-020519](#) Pseudo-CR to WLAN Interworking draft: Removal of the sentence related to a SIM/USIM software application (Rel-6). This had been agreed at meeting #24 and the change was **agreed** by SA WG3.

[TD S3-020520](#) Pseudo-CR to WLAN Interworking draft: Changes to UICC are allowed (Rel-6). The changes were **agreed**. It was noted that clause 4.2 does not contain Security Requirements and requires a full review. **The Editors were asked to propose updates to clause 4.2.**

[TD S3-020521](#) Pseudo-CR to WLAN Interworking draft: Editorial changes concerning abbreviations (Rel-6). This change was **agreed**. **The Editors were also asked to remove any abbreviations which are already provided in TR 21.905 and make a reference to the vocabulary document instead.**

[TD S3-020522](#) Draft TS 33.cde - 0.1.0: Wireless Local Area Network (WLAN) Interworking Security (Release 6). This was briefly introduced by Ericsson, in the absence of the Editors at the meeting. It was not known if any changes had been introduced without the revision marks. **The document editors were asked to use revision marks for future updates to help delegates to track the changes.** It was **noted** that the SA WG2 position was that authentication is done in the Home Network, and SA WG3 **endorsed** this.

[TD S3-020525](#) IEEE 802.11 and WECA Status Updates. this was introduced by Ericsson and provided an update to the status of IEEE 802.11 work. It was noted that *WECA* had now changed its' name to "*Wi-Fi Alliance*". It was noted that *TKIP* is "**Temporal Key Integrity Protocol**". The contribution was then **noted**.



[TD S3-020544](#) On the security of EAP/SIM and EAP/AKA and their use in WLAN-3G-interworking. This was introduced by Siemens.

*Conclusions (from contribution)*

1. *If it is the objective to reach a security level for WLAN-3G interworking which is comparable to GSM then the use of EAP/SIM without additional precautions seems fine. This objective would, however, contradict a security requirement in the WLAN draft TS that “ The user should have same security level for WLAN access as for 3GPP access”. But note, that the security requirements section in the WLAN draft TS may need some revision as there seem to be contradictory requirements.*
2. *Measures to increase the security level of EAP/SIM over that of GSM are technically possible, but the benefits have to be carefully weighed against the drawback that they seem to make it more difficult to leverage the existing authentication infrastructure. The use of EAP/AKA seems to make it possible to use the existing infrastructure.*
3. *The use of EAP/AKA seems preferable over the use of EAP/SIM.*

**The principles of this contribution were endorsed as a working assumption by SA WG3** (i.e. if only access to the WLAN with USIM is allowed, then use EAP-AKA, if access with SIM card is allowed, and no USIM is available then use EAP-SIM). **An analysis of any problems with allowing SIM access should be made.**

It was proposed that the WID for WLAN should explicitly include the SIM access (WID was approved in SA WG3 meeting #24, [TD S3-020451](#)). This should be considered by delegates and changes proposed if necessary.

[TD S3-020557](#) On the use of EAP/SIM in 3G-WLAN-interworking. This was introduced by Ericsson and addresses conflicting security requirements in the Draft WLAN security TS.. It was **agreed** that the 7<sup>th</sup> bullet should read:

"The subscriber should have at least the same security level for WLAN access as for his current cellular access subscription (i.e. GSM or UMTS)".

This bullet should be considered for improvement (as the level of security is not directly under 3GPP control) and contributions presented to the next SA WG3 meeting. The other changes in the contribution were then **approved**.

[TD S3-020523](#) 3G-WLAN – Trust Model. This was introduced by Ericsson and proposed a 3G-WLAN system model, describing the key players and their trust relationships. Ericsson proposed that the Trust Model described in section 2 of the contribution is adopted by SA WG3, and incorporated to Annex B of the Draft "WLAN Interworking Security". The Trust model described was considered in need of further study and it was decided to return to this at the next SA WG3 meeting. **The final paragraph of clause 2.2 was therefore transformed into an editors note, and it was agreed to insert this modified text into Annex B of the draft TS.**

[TD S3-020524](#) 3G-WLAN - Security Evaluation and Countermeasures Proposal. This was introduced by Ericsson and described potential threats and attacks, and proposes countermeasures for a 3G-WLAN interworking solution. Ericsson proposed that the Security Evaluation and Countermeasures proposal described in sections 2 and 3 are agreed by SA WG3 and incorporated to Annex C of the Draft "WLAN Interworking Security". It was **agreed** that the 2<sup>nd</sup> sentence of clause 2.1.2 should be removed. It was noted that the Access Server Node (ASN) functionality is assumed throughout the proposal, but the ASN has not been agreed in the document at present. It was decided that more time was needed for consideration of the issues. **Delegates were asked to consider and contribute to this at the next meeting.** The contribution was then **noted**.

[TD S3-020539](#) 3G-WLAN – Security Endpoint. This was introduced by Ericsson and argued that the security endpoint must be physically secure; and, hence lie "deeper" in the WLAN AN than the WLAN access point. Traffic protection alternatives were also discussed and a solution using IPsec was sketched out in the contribution. It was commented that the L2.5 solution would require unique driver software for each OS and WLAN access. It was agreed that further discussion is needed on these scenarios and solutions and delegates were asked to contribute via the e-mail list for re-consideration at the next SA WG3 meeting.

## 7.10 Visibility and configurability of security

There were no specific contributions under this agenda item.

## 7.11 Push

[TD S3-020466](#) Reply LS from SA WG1 on Push Security. SA WG1 requested more comments on the security aspects of the current draft of TS 22.174 (attached to the LS). The draft TS was briefly reviewed, but it was considered that members should review the draft off-line and P. Howard agreed to lead a review and would report if any further comments should be provided to SA WG1. P. Howard agreed to lead an e-mail discussion on any identified issues and co-ordinate comments to SA WG1.

**AP 25/11: P. Howard to lead e-mail discussion on Push Security issues (TS 22.174) and co-ordinate any comments to SA WG1.**

## 7.12 Priority

There were no specific contributions under this agenda item.

## 7.13 Location services (LCS)

[TD S3-020459](#) LS (from CN WG4) on use of IP as transport for the Inter-GMLC Interface. This was introduced by Ericsson and was copied to SA WG3 for information. The LS was **noted**.

[TD S3-020461](#) LS back to SA1 and SA2 (from CN WG5) on enhanced user privacy and new security requirements for LCS. This was introduced by Ericsson and was copied to SA WG3 for information. It was noted that CN WG5 had taken SA WG3 comments on Client Authentication into account in their specification. The LS was **noted**.

[TD S3-020465](#) (LS from SA WG1) Support of LCS enhanced user privacy in OSA. This was introduced by Lucent Technologies and was a response to the LS from CN WG5 in [TD S3-020461](#). The LS was copied to SA WG3 for information and was **noted**.

[TD S3-020478](#) LS (from LiF-SIG) to 3GPP TSG WG CN4, CN, SA3, SA2, and GSMA SERG on the protocol development for the GMLC Lr-interface. LiF-SIG Roaming ad-hoc asked SA WG3 to provide recommendations for an acceptable security protocol for the MLP-based Lr interface. An investigation was made off-line and a LS to LiF-SIG was provided in [TD S3-020581](#) which was modified slightly in [TD S3-020582](#) and **approved**.

## 7.14 User equipment functionality split (UEFS)

There were no specific contributions under this agenda item.

## 7.15 Open service architecture (OSA)

There were no specific contributions under this agenda item.

## 7.16 Generic user profile (GUP)

There were no specific contributions under this agenda item.

## 7.17 Presence

[TD S3-020475](#) Liaison (from SA WG2) on Security and Charging Issues with use of HTTP within IMS. This was introduced by Nokia. SA WG2 had not identified any particular use scenarios for HTTP at present, but do not rule out identifying scenarios in the future. SA WG2 asked SA WG3 to comment on and investigate potential security issues related to the use of HTTP within IMS for service related purposes. [TD S3-020528](#) (see below) was considered before finalising on this Liaison.

[TD S3-020528](#) HTTP Security. This was introduced by Nokia and reports a study of HTTP security under request from SA2 WG. One solution very much based on IETF existing protocol is presented. It also combines 3GPP Digest AKA for authentication as advantage. Nokia proposed to start the analysis based on knowledge investigated as a baseline (as provided in this contribution) and to query SA WG2 for the deployment detail of HTTP feature and its required security functions. It was clarified that this had been developed assuming many types of server, as well as Presence servers and that it would not be needed if SA WG2 decide not to use HTTP after all. It was agreed to send a LS to SA WG2 asking them for details of the expected use for HTTP and showing that there are potential solutions if it is required. The LS was provided in [TD S3-020572](#) and updated in [TD S3-020587](#) which was **approved**.



[TD S3-020502](#) Presence Security Proposal. This was introduced by Nortel Networks and proposed a solution for securing the information exchanged between the Presence Server and Watcher applications. This was covered by the discussions of [TD S3-020507](#) below.

[TD S3-020507](#) Presence Security Architecture. This was introduced by Ericsson and aimed to identify some security requirements that apply for the Presence Architecture. The contribution does not assume any particular architecture, e.g. IMS, and it is general in nature. Ericsson asked SA WG3 to discuss and endorse the proposed requirements as working assumptions and collect them where appropriate in the TR. It was **agreed** to input the material in the contribution in the draft TR and to liaise the information to SA WG2 for their comments on section 2. The LS was provided in [TD S3-020569](#) which was modified in [TD S3-020588](#) which was **approved**.

[TD S3-020508](#) Working Assumptions and Open Issues in Presence Security. This was introduced by Ericsson and compared the Presence Reference Architecture to existing UMTS security mechanisms. The goal of the paper was to identify working assumptions and open issues for SA WG3 and asked SA WG3 to endorse the working assumptions and to begin studies on the open issues.

The working assumptions were **endorsed** by SA WG3, noting that there are some other issues, e.g. Network-based Watcher applications, which are not fully covered.

It was **agreed** to attach the contribution to the LS to SA WG2 in [TD S3-020588](#), explaining the detail of this contribution as opposed to the general issues in [TD S3-020507](#).

## 7.18 User equipment management (UEM)

[TD S3-020472](#) LS (from T WG3) on User Equipment Management Feasibility Study (TR 32.802). This was introduced by AT&T Wireless. This was provided for information and was **noted**.

[TD S3-020473](#) LS (from T WG3) on Rel-6 WID for User Equipment Management. This was introduced by AT&T Wireless. This was provided for information and was **noted**. **It was recognised that the security aspects of the T WG3 WID on the remote management of UEs would need to be studied by SA WG3.**

## 7.19 Multimedia Broadcast/Multicast Service (MBMS)

[TD S3-020504](#) MBMS Fraud and countermeasures. This was introduced by Siemens and analysed the fraud issues that are an inherent property of sharing an MBMS key among MBMS users. Some measures were proposed that could be used to combat that type of fraud and should be taken into account when selecting the appropriate MBMS architecture. Siemens proposed that SA WG3 communicates these findings to SA WG2 as important criteria for selecting the appropriate architecture.

It was concluded that the techniques seem useful and further study of the fraud models and possible solutions need to be done. The solutions developed could be included as guidelines for implementation of the specified mechanisms. The document was then **noted**.

[TD S3-020501](#) Draft 3GPP2 Broadcast / Multicast Service security specifications. This presentation and associated documents were presented by Qualcomm. This was provided for information on the issues being studied in 3GPP2, which may be of use for the development of the MBMS Security architecture in 3GPP. The presentation was discussed and clarification provided on some points. It was noted that the stage 2 document attached was more up-to-date, as it had been updated as a result of the recent meeting of the 3GPP2 MBMS group. The presentation was **noted**.

[TD S3-020505](#) MBMS security functions. This was introduced by Siemens and described the needed security functions for MBMS and analysed the allocation of these security functions to the NE's from the viewpoint of security re-usability. The contribution concludes that:

- *It is preferred to allocate the MBMS security functions 1 and 2 not to the BM-SC at the application layer as it would give rise to additional authentication/encryption functionality and complexity.*
- *For security function 3, the SA WG2 view can be confirmed that there is no need for standardization (see TR 23.846 V1.2.0, clause 7.1.8).*
- *Siemens proposed to inform SA WG2 of the above conclusions such that the selection of the architectural options can proceed.*

Other proposals were provided in contributions which also need to be considered.

[TD S3-020526](#) Draft TS 33.cde - 0.0.1: Security of Multimedia Broadcast/Multicast Service (Release 6). This was provided by the editor for information and was **noted**. Comments were requested off-line for update at the next meeting.

[TD S3-020532](#) MBMS – Trust and Threats. This was introduced by Ericsson and shows the MBMS architecture, describing the roles and their trust relationships. The document also described some potential threats and attacks in order to help 3GPP identify security requirements for the MBMS system, and choose suitable security mechanisms which fulfil those requirements. Ericsson proposed that SA WG3 adopt the security requirements given in section 1.8 of the contribution and insert the text into the Draft TR in order to provide a basis for further elaboration.

It was **agreed** to add this to the TR, the Threat and Trust model parts should be inserted as Annexes in the TR. Some parts of the text needed editing, and the editor agreed to add some editors notes where clarification was needed. section 1.8.2, R3a should be included as an editors note indicating that the requirements are for further study. Contributions were requested to the next meeting to re-organize and develop the Draft TR after it is distributed by the Editor.

[TD S3-020573](#) MBMS Security: A Summary of three contributions S3-020533, 534 & 535. This was presented by Ericsson and summarised the proposals given in their contributions [TD S3-020533](#), [TD S3-020534](#) and [TD S3-020535](#).

Ericsson is proposed that SA WG3 endorses the following working assumptions for MBMS Security:

1. S3-020533 (Security protocol)
  - i Security protocol at application layer
  - ii IETF SRTP as security protocol for streaming
2. S3-020534 (Key Management)
  - i IETF MIKEY using pre-shared keys and symmetric crypto
3. S3-020535 (Push Re-keying)
  - i IETF MIKEY is potentially extended to support LKH (Logical Key Hierarchy)

The proposals were discussed and it was recognised that the other contribution in [TD S3-020538](#) should also be considered with document (see below).

[TD S3-020538](#) MBMS Security Architecture Proposal. This was introduced by Nortel Networks and proposed mechanisms for MBMS user authentication, authorisation and data encryption. This supported the application layer security as proposed by Ericsson in [TD S3-020573](#).

It was thought that a comparison of the solutions with respect to the impact on the business and threat models was required in order to select the most appropriate solutions.

**It was agreed that as a user could subscribe to service A, and not subscribe to service B, another user could subscribe to service B, and not subscribe to service A, then it follows that the keys need to be different for services A and B.**

It was recognised that there are many open issues and delegates were asked to consider the contributions and proposals for MBMS and to contribute to the next meeting of SA WG3 in order to progress the draft specification.

## 7.20 PKI-based key management for network domain security

[TD S3-020506](#) TR 33.810 v1.0.1\_2: NDS/AF Feasibility Study. The updates made to the draft TR were presented by Nokia. The version number of the document should be 1.1.0, as there are substantial additions to the previous version 1.0.1, and the editor was asked to put the text into passive prose (i.e. replacing the instances of "we ... "). It was noted that tamper proof storage of "secrets" is important, and the both symmetric and asymmetric key systems have secrets to be securely stored.

**The editor was thanked for his tremendous effort in updating the feasibility study and a new version and revised WID was requested for the next meeting for approval. Further comments should be provided to the editor.**

[TD S3-020575](#) TR 33.810 v1.1.0: NDS/AF Feasibility Study. This was introduced by the Editor who outlined the changes made to the draft. This TR was **approved** and will be forwarded to TSG SA meeting #18 for TSG Approval as a Release 6 Feasibility Study.

[TD S3-020574](#) Proposed WID: Network Domain Security; Authentication Framework (NDS/AF). This WID was created based upon the related WID for the Feasibility Study for this work. There was some concerns and confusion over the targeted Release for this work. It was agreed that an e-mail discussion would be held in order to try to achieve agreement and the WID would be re-presented at the next meeting if appropriate.

## 8 Review and update of work programme

There was no time to deal with this agenda item.

## 9 Future meeting dates and venues

Additional SA WG3 meeting dates were agreed, as shown in the following table.

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#26	19 - 22 November 2002	Oxford	European 'Friends of 3GPP'
S3#27	25 - 28 February 2003	Sophia Antipolis	ETSI
S3#28	06 - 09 May 2003	Berlin	European 'Friends of 3GPP'
S3#29	15-18 July 2003	San Francisco (tbc)	NA 'Friends of 3GPP' (tbc)
S3#30	7-10 October 2003	Italy (tbc) ??	tbd

### LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#7	12 - 14 November 2002	San Diego US	
SA3 LI-#8	19 - 21 February 2003	Paris FR	
SA3 LI-#9	13 - 15 May 2003	Sophia Antipolis FR	
SA3 LI-#10	16 - 18 September 2003	US	

### TSGs RAN/CN/T and SA Plenary meeting schedule

TSG RAN/CN/T #18	3 – 6 December	New Orleans USA	NA 'Friends of 3GPP'
TSG SA #18	9 – 12 December	New Orleans USA	NA 'Friends of 3GPP'
Meeting	2003	Location	Primary Host
TSG RAN/CN/T #19	11-14 March (tba)	UK	European 'Friends of 3GPP'
TSG SA #19	17-20 March	UK	European 'Friends of 3GPP'
TSG RAN/CN/T #20	3-6 June	Hämeenlinna, FIN	Nokia
TSG SA #20	9-12 June	Hämeenlinna, FIN	Nokia
TSG RAN/CN/T #21	16-19 September	Germany	
TSG SA #21	22-25 September	Germany	
TSG RAN/CN/T #22	9-12 December	US	
TSG SA #22	15-18 December	US	
Meeting	2004 DRAFT TBD	Location	Primary Host
TSG#23	March 9-12 & 15-18	China	
TSG#24	June 1-4 & 7-10	Korea	
TSG#25	7-10 & 13-16 September	USA	
TSG#26	7-10 & 13-16 December	TBD	

## 10 Any other business

There were no specific contributions under this agenda item.

## **11 Close**

The Chairman thanked the host, Siemens, for the meeting arrangements, and the delegates for their hard work and co-operation during the meeting, 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. Hiroshi Aono	NTT DoCoMo Inc.	<a href="mailto:aono@mml.yrp.nttdocomo.co.jp">aono@mml.yrp.nttdocomo.co.jp</a>	ARIB	JP
Mr. Nigel Barnes	MOTOROLA Ltd	<a href="mailto:Nigel.Barnes@motorola.com">Nigel.Barnes@motorola.com</a>	ETSI	GB
Mr. Marc Blommaert	SIEMENS ATEA NV	<a href="mailto:marc.blommaert@siemens.atea.be">marc.blommaert@siemens.atea.be</a>	ETSI	BE
Mr. Krister Boman	ERICSSON L.M.	<a href="mailto:krister.boman@erv.ericsson.se">krister.boman@erv.ericsson.se</a>	ETSI	SE
Mr. Charles Brookson	DTI	<a href="mailto:cbrookson@iee.org">cbrookson@iee.org</a>	ETSI	GB
Mr. Mauro Castagno	TELECOM ITALIA S.p.A.	<a href="mailto:mauro.castagno@tilab.com">mauro.castagno@tilab.com</a>	ETSI	IT
Mr. Per Christoffersson	TELIA AB	<a href="mailto:per.e.christoffersson@telia.se">per.e.christoffersson@telia.se</a>	ETSI	SE
Mr. KEVIN ENGLAND	mmO2 plc	<a href="mailto:kevin_england@o2.com">kevin_england@o2.com</a>	ETSI	GB
Dr. Adrian Escott	Hutchison 3G UK Limited	<a href="mailto:adrian.escott@hutchison3G.com">adrian.escott@hutchison3G.com</a>	ETSI	GB
Mr. John B Fenn	SAMSUNG Electronics	<a href="mailto:johnbfenn@aol.com">johnbfenn@aol.com</a>	ETSI	GB
Mr. Louis Finkelstein	Motorola Inc.	<a href="mailto:louisf@labs.mot.com">louisf@labs.mot.com</a>	T1	US
Dr. Mark Grayson	Cisco Systems France	<a href="mailto:mgrayson@cisco.com">mgrayson@cisco.com</a>	ETSI	FR
Dr. Robert Hancock	SIEMENS AG	<a href="mailto:robert.hancock@roke.co.uk">robert.hancock@roke.co.uk</a>	ETSI	GB
Ms. Tao Haukka	Nokia Korea	<a href="mailto:tao.haukka@nokia.com">tao.haukka@nokia.com</a>	TTA	FI
Mr. Henry Haverinen	NOKIA Corporation	<a href="mailto:henry.haverinen@nokia.com">henry.haverinen@nokia.com</a>	ETSI	FI
Mr. Guenther Horn	SIEMENS AG	<a href="mailto:guenther.horn@siemens.com">guenther.horn@siemens.com</a>	ETSI	DE
Mr. Peter Howard	VODAFONE Group Plc	<a href="mailto:peter.howard@vodafone.com">peter.howard@vodafone.com</a>	ETSI	GB
Mr. Geir Koien	TELENOR AS	<a href="mailto:geir-myrdahl.koien@telenor.com">geir-myrdahl.koien@telenor.com</a>	ETSI	NO
Mr. Alex Leadbeater	BT Group Plc	<a href="mailto:alex.leadbeater@bt.com">alex.leadbeater@bt.com</a>	ETSI	GB
Mr. Michael Marcovici	Lucent Technologies	<a href="mailto:marcovici@lucent.com">marcovici@lucent.com</a>	T1	US
Mr. Sebastien Nguyen Ngoc	ORANGE FRANCE	<a href="mailto:sebastien.nguyenngoc@rd.franceteleco">sebastien.nguyenngoc@rd.franceteleco</a>	ETSI	FR
Mr. Valtteri Niemi	NOKIA Corporation	<a href="mailto:valtteri.niemi@nokia.com">valtteri.niemi@nokia.com</a>	ETSI	FI
Mr. Gustavo Nieto	SIEMENS AG	<a href="mailto:gustavo.nieto-blanco@icn.siemens.de">gustavo.nieto-blanco@icn.siemens.de</a>	ETSI	DE
Mr. Petri Nyberg	SONERA Corporation	<a href="mailto:petri.nyberg@sonera.com">petri.nyberg@sonera.com</a>	ETSI	FI
Mr. Bradley Owen	Lucent Technologies N. S. UK	<a href="mailto:bvowen@lucent.com">bvowen@lucent.com</a>	ETSI	GB
Mr. Anand Palanigounder	NORTEL NETWORKS (EUROPE)	<a href="mailto:anand@nortelnetworks.com">anand@nortelnetworks.com</a>	ETSI	GB
Miss Mireille PAULIAC	GEMPLUS Card International	<a href="mailto:mireille.pauliac@GEMPLUS.COM">mireille.pauliac@GEMPLUS.COM</a>	ETSI	FR
Mr. Maurice Pope	Mobile Competence Centre	<a href="mailto:maurice.pope@etsi.fr">maurice.pope@etsi.fr</a>	(MCC)	FR
Mr. Greg Rose	QUALCOMM EUROPE S.A.R.L.	<a href="mailto:ggr@qualcomm.com">ggr@qualcomm.com</a>	ETSI	AU
Ms. Stephanie Salgado	Schlumberger Sema	<a href="mailto:salgado@montrouge.sema.slb.com">salgado@montrouge.sema.slb.com</a>	ETSI	FR
Mr. Stefan Schroeder	T-MOBILE DEUTSCHLAND	<a href="mailto:stefan.schroeder@t-mobile.de">stefan.schroeder@t-mobile.de</a>	ETSI	DE
Mr. Hugh Shieh	AT&T Wireless Services, Inc.	<a href="mailto:hugh.shieh@attws.com">hugh.shieh@attws.com</a>	T1	US
Mr. Ramachandran Subramanian	QUALCOMM EUROPE S.A.R.L.	<a href="mailto:rsubrama@qualcomm.com">rsubrama@qualcomm.com</a>	ETSI	US
Mr. Benno Tietz	Vodafone D2	<a href="mailto:benno.tietz@vodafone.com">benno.tietz@vodafone.com</a>	ETSI	DE
Mr. Vesa Torvinen	ERICSSON L.M.	<a href="mailto:vesa.torvinen@lmf.ericsson.se">vesa.torvinen@lmf.ericsson.se</a>	ETSI	SE
Mr. Lee Valerius	NORTEL NETWORKS (EUROPE)	<a href="mailto:valerius@nortelnetworks.com">valerius@nortelnetworks.com</a>	ETSI	US
Mr. Willy Verbestel	RIM	<a href="mailto:wmjv@hotmail.com">wmjv@hotmail.com</a>	ETSI	US
Mr. Tommi Viitanen	Nokia Telecommunications Inc.	<a href="mailto:tommi.viitanen@nokia.com">tommi.viitanen@nokia.com</a>	T1	FI
Mr. Stuart Ward	ORANGE PCS LTD	<a href="mailto:stuart.ward@orange.co.uk">stuart.ward@orange.co.uk</a>	ETSI	GB
Ms. Monica Wifvesson	ERICSSON L.M.	<a href="mailto:monica.wifvesson@emp.ericsson.se">monica.wifvesson@emp.ericsson.se</a>	ETSI	SE
Mr. Berthold Wilhelm	BMW	<a href="mailto:berthold.wilhelm@regtp.de">berthold.wilhelm@regtp.de</a>	ETSI	DE

41 attendees

## A.2 SA WG3 Voting list

Based on the attendees lists for meetings #23, #24 and #25, the following companies are eligible to vote at SA WG3 meeting #26:

Company	Country	Status	Partner Org
ALCATEL S.A.	FR	3GPPMEMBER	ETSI
AT&T Wireless Services, Inc.	US	3GPPMEMBER	T1
BUNDESMINISTERIUM FUR WIRTSCHAFT	DE	3GPPMEMBER	ETSI
BT Group Plc	GB	3GPPMEMBER	ETSI
Cisco Systems France	FR	3GPPMEMBER	ETSI
Dansk MobilTelefon I/S	DK	3GPPMEMBER	ETSI
DTI - Department of Trade and Industry	GB	3GPPMEMBER	ETSI
Ericsson Incorporated	US	3GPPMEMBER	T1
Telefon AB LM Ericsson	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 Network Systems 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
NOKIA KOREA	KR	3GPPMEMBER	TTA
Nokia Telecommunications Inc.	US	3GPPMEMBER	T1
NORTEL NETWORKS (EUROPE)	GB	3GPPMEMBER	ETSI
NTT DoCoMo Inc.	JP	3GPPMEMBER	ARIB
ORANGE FRANCE	FR	3GPPMEMBER	ETSI
ORANGE PCS LTD	GB	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
Research In Motion Limited	CA	3GPPMEMBER	ETSI
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
SONERA Corporation	FI	3GPPMEMBER	ETSI
SSH Communications Security Corp	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

40 Individual Member Companies

**Annex B: List of documents**

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020455	Draft agenda for meeting #25	Chairman	2	Approval		Approved
S3-020456	Draft Report of meeting #24 - vsn 0.0.3	Secretary	4.1	Approval		Approved with minor changes - updated v1.0.0 to be placed on FTP server
S3-020457	Secure registration of IP addresses	CN WG1	7.1	Action		Revised CR from S3-020375 in S3-020553
S3-020458	LS on on Diameter security issues	CN WG4	7.1	Information		Response in S3-020547
S3-020459	LS on use of IP as transport for the Inter-GMLC Interface	CN WG4	7.13	Information		Noted
S3-020460	IMS authentication vector distribution on the Cx interface	CN WG4	7.1	Information		Response to SA WG3 questions. Noted
S3-020461	LS back to SA1 and SA2 on enhanced user privacy and new security requirements for LCS	CN WG5	7.13	Information		Noted
S3-020462	LS reply on Packet Switched Streaming (PSS) in Rel-6 Work Programme	SA WG1	6.1	Information		Noted
S3-020463	Liaison Statement on subscriber certificates	SA WG1	7.7	Information		Response to SA WG3 on Subscriber Certificates. Noted.
S3-020464	LS reply on "Answer to "LS on PSS Release 6 work programme""	SA WG1	6.1	Information		Noted
S3-020465	Support of LCS enhanced user privacy in OSA	SA WG1	7.13	Information		Noted
S3-020466	Reply LS on Push Security	SA WG1	7.11	Action		P Howard to lead e-mail discussion if any issues are identified in the draft TS
S3-020467	New requirements about functionality to make subscription to different domains independent or linked based on operator decision	SA WG1	6.1	Action		Attached CR had been rejected in SA#17. Response LS in S3-020561
S3-020468	Response to T3-020406/S1-021427 (Response "Liaison Statement on Access to IMS Services using 3GPP release 99 and release 4 UICCs" (S1-020577))	SA WG1	6.1	Information		Noted. Response LS in S3-020561
S3-020469	LS on Speech Enabled Services	SA WG1	6.1	Information		TR 22.977 and TS 22.243 should be reviewed and contribution to e-mail group. L Finklestein to create response LS to SA WG1 by 4 November
S3-020470	Draft Working Item Description PSS Rel-6 and LS response to: "Answer to Liaison Statement regarding PSS Release 6 work programme" (S2-022050/ S4 (02)0375) from SA2, and "LS reply on Packet Switched Streaming (PSS) in Rel-6 Work Programme" (S5-024235/S4(0)0376) from SA5	SA WG4	6.1	Information		No comments on WID. Noted
S3-020471	LS on Subscriber Certificates	T WG3	7.7	Information		Response to SA WG3 on Subscriber Certificates. Noted.



TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020472	LS on User Equipment Management Feasibility Study (TR 32.802)	T WG3	7.18	Information		Noted
S3-020473	LS on Rel-6 WID for User Equipment Management	T WG3	7.18	Information		Noted
S3-020474	Response LS on Security enhancements for GERAN	TSG GERAN	7.5	Action		Reply LS in S3-020566. P Howard to develop WID for next meeting
S3-020475	Liaison on Security and Charging Issues with use of HTTP within IMS	SA WG2	7.17	Action		Reply LS in S3-020572
S3-020476	LS on 3GPP System to WLAN Inter working architecture	SA WG2	7.9	Action		LS response to SA WG2 in S3-020586
S3-020477	Reply LS on "Gb evolution"	SA WG2	7.5	Information		Noted
S3-020478	LS to 3GPP TSG WG CN4, CN, SA3, SA2, and GSMA SerG on the protocol development for the GMLC Lr-interface	Lf-SIG	7.13	Action		LS provided in S3-020582
S3-020479	LS response on subscriber certificates	CN WG1	7.7	Action		Noted
S3-020480	Liaison statement on Interoperability Issues and SIP in IMS	CN WG1	7.1	Action		Response in SP-020550
S3-020481	LS on Status of protocol work on Ze interface	CN WG4	7.3	Information		Noted
S3-020482	LS on re-used of START value for ciphering of RB using RLC TM during SRNS relocation	RAN WG2	7.4	Action		Agreed change needed in Rel-4. Response LS in S3-020564
S3-020483	LS to SA3 on Group release security solution	RAN WG2	7.4	Action		Other contributions considered. Need for protection to be discussed over e-mail. Response LS in S3-020565
S3-020484	WITHDRAWN - Duplicate of TD465: Support of LCS enhanced user privacy in OSA	SA WG1	7.13	Information		WITHDRAWN - Duplicated input
S3-020485	Response to IETF LS on Interoperability Issues and SIP in IMS	TSG SA	7.1	Information		Noted
S3-020486	Architectural choices for Subscriber Certificates	Nokia	7.7	Presentation		Noted. Feedback from SA WG2 awaited for further discussion
S3-020487	Digital Signatures: Who is doing what?	Orange	7.7	Information		Noted. SA WG3 to monitor ongoing work on DS
S3-020488	Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #3/02 on lawful interception	SA WG3-LI Group	4.2	Information		PDF Only. Noted
S3-020489	Proposed CR to 33.107-5.4.0: Event Time (Rel-5)	SA WG3-LI Group	4.2	Approval		Approved
S3-020490	Proposed CR to 33.107-5.4.0: Essential correction to the LI events generated during inter-SGSN RAU, when PDP context is active (Rel-5)	SA WG3-LI Group	4.2	Approval		Noted. E-mail discussion in LI group.
S3-020491	Proposed CR to 33.108-5.1.0: Essential corrections to the Annex C.1 (ULIC) - (Rel-5)	SA WG3-LI Group	4.2	Approval		Approved
S3-020492	Proposed CR to 33.108-5.1.0: Missing PDP Context Modification event (Rel-5)	SA WG3-LI Group	4.2	Approval		Approved
S3-020493	Proposed CR to 33.108-5.1.0: Aggregation of IRI Records (Rel-6)	SA WG3-LI Group	4.2	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020494	Proposed CR to 33.108-5.1.0: Essential correction to the LI events generated during RAU, when PDP context is active (Rel-5)	SA WG3-LI Group	4.2	Approval	S3-020546	Updated in S3-020546
S3-020495	Interception regarding IMS	Telcordia Technologies and Federal Bureau of Investigation	7.1	Discussion / Action		(Forwarded to SA WG3 by SA WG3-LI). Noted. Further discussion within the LI group
S3-020496	WI Description: Lawful Interception in the 3GPP Rel-6 architecture	SA WG3-LI Group	4.2	Approval		Approved
S3-020497	LS on change to LI email subscription and access controlled SA3-LI document area	SA WG3-LI Group	4.2	Action		Return to LI to clarify reasons for the closing of FTP site
S3-020498	Report on SA#17 for SA3	SA WG3 Chairman	5	Information		Noted
S3-020499	Proposed CR to 33.203-5.3.0: Sending error response when P-CSCF receives unacceptable proposal (Rel-5)	Nokia	7.1	Approval	S3-020554	Updated in S3-020554
S3-020500	Contribution to discussion on architecture and trust for subscriber certificates	Siemens	7.7	Discussion		Discussed. Many points raised that need further discussion before deciding on Architecture
S3-020501	Draft 3GPP2 Broadcast / Multicast Service security specifications	Qualcomm	7.19	Information / Review		Noted
S3-020502	Presence Security Proposal	Nortel Networks	7.17	Discussion		Covered by discussion of S3-020507
S3-020503	Proposed CR to 33.102: USIM support in GERAN only terminals (Rel-5)	Siemens	7.5	Approval	S3-020567	Revised in S3-020567
S3-020504	MBMS Fraud and countermeasures	Siemens	7.19	Discussion		Noted. More study of fraud scenarios and solutions needed
S3-020505	MBMS security functions	Siemens	7.19	Discussion		Discussed
S3-020506	TR 33.810 v1.0.1_2: NDS/AF Feasibility Study	Nokia, Siemens, SSH, Telenor, T-Mobile	7.20	Discussion / Approval		Further comments should be provided to the editor for approval at next meeting
S3-020507	Presence Security Architecture	Ericsson	7.17	Discussion / Decision		To be included in TR. LS to SA WG2 in S3-020569
S3-020508	Working Assumptions and Open Issues in Presence Security	Ericsson	7.17	Discussion / Decision		Working assumptions endorsed. Added to LS to SA WG2 in S3-020569
S3-020509	Issuing Subscriber Certificates at Application Layer	Ericsson	7.7	Discussion / Decision		Discussed
S3-020510	Group Release Authentication algorithm	Ericsson	7.4	Discussion / Decision		Use of f8 considered more appropriate for Rel-5, need for protection to be discussed over e-mail. Noted.
S3-020511	IETF and WLAN Authentication Methods	Ericsson and Nokia	7.9	Information		Noted. Members asked to help progress IETF WLAN drafts

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020512	Contribution to discussion on subscriber certificates	Orange	7.7	Discussion		Home Control is SA1 requirement. Solution needs developing
S3-020513	Proposed CR to 33.203: Indication in the UE that the SA is no longer active in P-CSCF (Rel-5)	Ericsson, Hutchison 3G	7.1	Approval	S3-020555	Revised in S3-020555. Related LS to CN1 in S3-020556
S3-020514	The use of SAs in IMS user authentication failures	Ericsson, Hutchison 3G	7.1	Discussion / Decision		Discussed as background to S3-020515
S3-020515	Proposed CR to 33.203: The use of SAs in user authentication failures (Rel-5)	Ericsson, Hutchison 3G	7.1	Approval	S3-020558	Revised in S3-020558. Added to LS in S3-020556
S3-020516	IETF status report: SIP security agreement	Ericsson & Nokia	7.1	Discussion / Decision		LS to CN1 in SP-020551
S3-020517	Use of smart cards in WLAN interworking	GEMPLUS Card International	7.9	Discussion		GemPlus to develop proposals further by e-mail and next meeting
S3-020518	Pseudo-CR to WLAN Interworking draft: Editorial changes concerning the term "SIM/USIM-based authentication" (Rel-6)	GEMPLUS Card International	7.9	Discussion		Editors asked to check if this change is correct
S3-020519	Pseudo-CR to WLAN Interworking draft: Removal of the sentence related to a SIM/USIM software application (Rel-6)	GEMPLUS Card International	7.9	Discussion		Agreed. Editor to update document accordingly
S3-020520	Pseudo-CR to WLAN Interworking draft: Changes to UICC are allowed (Rel-6)	GEMPLUS Card International	7.9	Discussion		Agreed. Section 4.2 requires full review. Editors asked to update document accordingly
S3-020521	Pseudo-CR to WLAN Interworking draft: Editorial changes concerning abbreviations (Rel-6)	GEMPLUS Card International	7.9	Discussion		Agreed. Editors also asked to replace abbreviations with ref to vocabulary document.
S3-020522	Draft TS 33.cde - 0.1.0: Wireless Local Area Network (WLAN) Interworking Security (Release 6)	Ericsson	7.9	Discussion		Noted. Some changes may not be revision marked.
S3-020523	3G-WLAN – Trust Model	Ericsson	7.9	Discussion / Approval		Final para of 2.2 as editors note. Editors asked to insert text into Annex B of Draft TS WLAN.
S3-020524	3G-WLAN - Security Evaluation and Countermeasures Proposal	Ericsson	7.9	Discussion / Approval		Delegates to consider and contribute for next meeting. Noted
S3-020525	IEEE 802.11 and WECA Status Updates	Ericsson	7.9	Information		Noted
S3-020526	Draft TS 33.cde - 0.0.1: Security of Multimedia Broadcast/Multicast Service (Release 6)	Hutchison 3G UK	7.19	Discussion		Noted. Contribution requested in form of Pseudo-CRs
S3-020527	Registration and SA lifetimes	Hutchison 3G UK	7.1	Discussion / Decision		E-mail discussion to provide CR to next meeting (A Escott)
S3-020528	HTTP Security	Nokia	7.17	Discussion / Decision		LS to SA WG2 in S3-020572
S3-020529	WITHDRAWN - Repeat of S3-020513					WITHDRAWN
S3-020530	WITHDRAWN - Repeat of S3-020514					WITHDRAWN
S3-020531	WITHDRAWN - Repeat of S3-020515					WITHDRAWN

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020532	MBMS – Trust and Threats	Ericsson	7.19	Discussion / Decision		Editor to reorganise and add this to draft TR
S3-020533	MBMS – Security layer selection	Ericsson	7.19	Discussion / Decision		Covered by summary in S3-020573
S3-020534	MBMS - key management comparison	Ericsson	7.19	Discussion / Approval		Covered by summary in S3-020573
S3-020535	MBMS - re-keying	Ericsson	7.19	Discussion / Approval		Covered by summary in S3-020573
S3-020536	Security need evaluation of UTRAN and GERAN IP transport interfaces	Nokia	7.2	Discussion / Approval		Gb I/f also high priority. CR contributions requested on High priority I/fs identified
S3-020537	Group release security mechanism	Lucent Technologies	7.4	Discussion / Approval		e-mail discussion over need for protection. Response LS to RAN2 in S3-020565
S3-020538	MBMS Security Architecture Proposal	Nortel Networks	7.19	Discussion		More consideration needed. Progress at next meeting
S3-020539	3G-WLAN – Security Endpoint	Ericsson	7.9	Discussion / Approval		Delegates asked to consider and contribute to e-mail discussion
S3-020540	Reply LS on "Gb evolution"	TSG GERAN	7.5	Information		Noted.
S3-020541	Conclusions on Proof of Possession discussion	E-mail discussion chairman	7.7	Discussion / Decision		Discussed and noted
S3-020542	Trust and PKI email discussion input paper	Nokia	7.7	Discussion / Decision		Noted. Used for discussion of other contributions
S3-020543	Draft report of TSG SA meeting #17 - version 0.0.4	Secretary	5	Information		Noted
S3-020544	On the security of EAP/SIM and EAP/AKA and their use in WLAN-3G-interworking	Siemens	7.9	Discussion		Principles endorsed as a working assumption
S3-020545	A5/3 and GEA3 and their relation with EGPRS	Ericsson	7.5	Discussion		K. Boman to create CR to 55.919 to clarify CS EDGE use of algorithm for next meeting
S3-020546	Proposed CR to 33.108-5.1.0: Essential correction to the LI events generated during RAU, when PDP context is active (Rel-5)	SA WG3-LI Group	4.2	Approval		Noted. E-mail discussion in LI group.
S3-020547	Response LS to CN WG4, SA WG5: adopts the security requirements in chapter 1.8	SA WG3	7.1	Approval	S3-020576	Revised in S3-020576
S3-020548	Proposed CR to 33.203: Re-use and re-transmission of RAND and AUTN (Rel-5)	Ericsson	7.1	Approval	S3-020560	Revised to include mechanism in S-CSCF in specification - S3-020560
S3-020549	WITHDRAWN - Duplicate of TD544	Siemwns	7.9	Discussion		WITHDRAWN - DUPLICATED TD 544
S3-020550	Liaison statement on Interoperability Issues and SIP in IMS	SA WG3		Approval	S3-020578	revised in S3-020578

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020551	LS to CN WG1 on IETF Sec-agree alternative	SA WG3		Approval	S3-020580	revised in S3-020580
S3-020552	Proposed CR to 33.210: Adding requirement to provide mandatory support for 3DES encryption in NDS/IP. Remove AES references and dependencies (Rel-5)	Telenor	7.2	Approval	S3-020562	Revised in S3-020562
S3-020553	Proposed CR to 33.203: Correction of IP address acquisition in P-CSCF	Nokia	7.1	Action		Approved
S3-020554	Proposed CR to 33.203-5.3.0: Sending error response when P-CSCF receives unacceptable proposal (Rel-5)	SA WG3	7.1	Approval		Approved
S3-020555	Proposed CR to 33.203: Indication in the UE that the SA is no longer active in P-CSCF (Rel-5)	SA WG3	7.1	Approval		Approved. LS to CN1 in S3-020556
S3-020556	LS to CN WG1 on CR impacts in S3-020555 (Monika)	SA WG3	7.1	Approval	S3-020579	Revised in S3-020579
S3-020557	On the use of EAP/SIM in 3G-WLAN-interworking	Nokia, Ericsson	7.9	Discussion		Agreed with changes to 7th bullet (see report). Editors asked to update the WLAN draft accordingly
S3-020558	Proposed CR to 33.203: The use of SAs in user authentication failures (Rel-5)	SA WG3	7.1	Approval		Approved. Append to LS in TD556
S3-020559	Proposed CR to 33.203: Clean up one Editor's note in 33.203 (Rel-5)	AT&T Wireless	7.1	Approval		Approved
S3-020560	Proposed CR to 33.203: Re-use and re-transmission of RAND and AUTN (Rel-5)	Ericsson	7.1	Approval	S3-020590	Revised in S3-020590
S3-020561	New requirements about functionality to make subscription to different domains independent or linked based on operator decision	SA WG3	6.1	Approval	S3-020577	revised in S3-020577
S3-020562	Proposed CR to 33.210: Adding requirement to provide mandatory support for 3DES encryption in NDS/IP. Remove AES references and dependencies (Rel-5)	SA WG3	7.2	Approval	S3-020563	Revised in S3-020563
S3-020563	Proposed CR to 33.210: Adding requirement to provide mandatory support for 3DES encryption in NDS/IP. Remove AES references and dependencies (Rel-5)	SA WG3	7.2	Approval		Approved
S3-020564	LS to RAN2: Reuse of COUNT-C Values for Ciphering of RB Using RLC TM During Handover	SA WG3	7.4	Approval	S3-020583	revised in S3-020583
S3-020565	LS to RAN2: Group Release security solution	SA WG3	7.4	Approval	S3-020584	revised in S3-020584
S3-020566	LS to GERAN cc SA WG2: Security enhancements for GERAN	SA WG3	7.5	Approval	S3-020589	revised in S3-020589
S3-020567	WITHDRAWN - Wrong document supplied - correct doc allocated to S3-020591					WITHDRAWN
S3-020568	Proposed CR to 33.200: Removal of Automatic Key Management from Rel-5 (Rel-5)	SA WG3 (Secretary)	7.3	Approval		A Escott to check and update CR at next meeting
S3-020569	LS to SA WG2 on Presence General Requirements (K Boman)	SA WG3	7.17	Approval	S3-020588	revised in S3-020588
S3-020570	Cellular – WLAN Interworking: Activities in ETSI/MMAC and WIG Status	ETSI BRAN Chairman	7.9	Presentation		Presented. Useful background information
S3-020571	Reply LS to SA WG2 on 3GPP System to WLAN Inter working architecture	SA WG3	7.9	Approval	S3-020586	Revised in S3-020586

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020572	Liaison to SA WG2 on HTTP Security investigation within IMS	SA WG3	7.17	Approval	S3-020587	Revised in S3-020587
S3-020573	MBMS Security: A Summary of three contributions SA3-020533, 534 & 535	Ericsson	7.19	Presentation		More consideration needed. Progress at next meeting
S3-020574	Proposed WID: Network Domain Security; Authentication Framework (NDS/AF)	SA WG3	7.20	Approval		
S3-020575	TR 33.810 v1.1.0: NDS/AF Feasibility Study	Nokia, Siemens, SSH, Telenor, T-Mobile	7.20	Approval		Approved. To be sent to SA#18 for approval
S3-020576	Response LS to CN WG4, SA WG5: adopts the security requirements in chapter 1.8	SA WG3	7.1	Approval		Approved
S3-020577	New requirements about functionality to make subscription to different domains independent or linked based on operator decision	SA WG3	6.1	Approval		Approved
S3-020578	Liaison statement on Interoperability Issues and SIP in IMS	SA WG3		Approval		Approved
S3-020579	LS to CN WG1 on CR impacts in S3-020555 (Monika)	SA WG3	7.1	Approval		Approved. TDs 555 and 558 appended
S3-020580	LS to CN WG1 on IETF Sec-agree alternative (K Boman)	SA WG3		Approval		Approved
S3-020581	LS on Lr interface security	SA WG3	7.11	Approval	S3-020582	revised in S3-020582
S3-020582	LS on Lr interface security	SA WG3	7.11	Approval		Approved
S3-020583	LS to RAN2: Reuse of COUNT-C Values for Ciphering of RB Using RLC TM During Handover	SA WG3	7.4	Approval		Approved
S3-020584	LS to RAN2: Group Release security solution	SA WG3	7.4	Approval		Approved
S3-020585	Proposed CR to 33.102 for information: USIM support in GERAN only terminals (Rel-5)	SA WG3	7.4	Information		Noted
S3-020586	Reply LS to SA WG2 on 3GPP System to WLAN Inter working architecture	SA WG3	7.9	Approval		Approved
S3-020587	Liaison to SA WG2 on HTTP Security investigation within IMS	SA WG3	7.17	Approval		Approved
S3-020588	LS to SA WG2 on Presence General Requirements (K Boman)	SA WG3	7.17	Approval		Approved
S3-020589	LS to GERAN cc SA WG2: Security enhancements for GERAN	SA WG3	7.5	Approval		Approved
S3-020590	Proposed CR to 33.203: Re-use and re-transmission of RAND and AUTN (Rel-5)	Ericsson	7.1	Approval		To be discussed over e-mail and updated for next meeting (Postponed)
S3-020591	Proposed CR to 33.102 for information: USIM support in GERAN only terminals (Rel-5)	Siemens	7.1	Approval		To be discussed over e-mail and updated for next meeting (Postponed)

**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	CHRISTOFFE RSSON, Per	Ph1
TS	02.09	4.5.1	Security aspects	CHRISTOFFE RSSON, Per	Ph2
TS	02.09	5.2.1	Security aspects	CHRISTOFFE RSSON, Per	R96
TS	02.09	6.1.1	Security aspects	CHRISTOFFE RSSON, Per	R97
TS	02.09	7.1.1	Security aspects	CHRISTOFFE RSSON, Per	R98
TS	02.09	8.0.1	Security aspects	CHRISTOFFE RSSON, 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	CHRISTOFFE RSSON, Per	R99
TS	21.133	4.1.0	3G security; Security threats and requirements	CHRISTOFFE RSSON, 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	22.022	5.0.0	Personalisation of Mobile Equipment (ME); Mobile functionality specification	NGUYEN NGOC, Sebastien	Rel-5
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	3.1.0	Immediate Service Termination (IST); Stage 2	HOWARD, Peter	R99
TS	23.035	4.1.0	Immediate Service Termination (IST); Stage 2	HOWARD, Peter	Rel-4
TS	23.035	5.1.0	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	5.1.0	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	5.4.0	3G security; Lawful interception architecture and functions	WILHELM, Berthold	Rel-5
TS	33.108	5.1.0	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	33.201	none	Access domain security - TO BE DELETED	POPE, Maurice	Rel-5
TS	33.203	5.3.0	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	KOIJEN, Geir	Rel-5
TR	33.810	1.0.1	3G Security; Network Domain Security / Authentication Framework (NDS/AF); Feasibility Study to support NDS/IP evolution	VIITANEN, Tommi *Added by M Pope	Rel-6
TR	33.900	0.4.1	Guide to 3G security	BROOKSON, Charles	Rel-5
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	33.903	none	Access Security for IP based services - TO BE DELETED	VACANT,	Rel-4
TR	33.903	none	Access Security for IP based services - TO BE DELETED	VACANT,	Rel-5
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
TS	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
TS	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	CHRISTOFFE RSSON, 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	43.020	5.0.0	Security-related network functions	GILBERT, Henri	Rel-5
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

TS	55.216	6.0.0	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	CHRISTOFFE RSSON, Per *Added by M Pope	Rel-6
TS	55.217	6.0.0	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data	CHRISTOFFE RSSON, Per *Added by M Pope	Rel-6
TS	55.218	6.0.0	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	CHRISTOFFE RSSON, Per *Added by M Pope	Rel-6
TR	55.919	6.0.0	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report	CHRISTOFFE RSSON, Per *Added by M Pope	Rel-6

**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
33.107	028	-	Rel-5	Event Time	F	5.4.0	S3-25	S3-020489	agreed
33.108	002		Rel-5	Essential corrections to the Annex C.1 (ULIC)	F	5.1.0	S3-25	S3-020491	agreed
33.108	003		Rel-5	Missing PDP Context Modification event	F	5.1.0	S3-25	S3-020492	agreed
33.108	003		Rel-6	Aggregation of IRI Records	B	5.1.0	S3-25	S3-020493	agreed
33.203	024	-	Rel-5	Correction of IP address acquisition in P-CSCF	F	5.3.0	S3-25	S3-020553	agreed
33.203	025	-	Rel-5	Sending error response when P-CSCF receives unacceptable proposal	F	5.3.0	S3-25	S3-020554	agreed
33.203	026	-	Rel-5	The use of SAs in user authentication failures	F	5.3.0	S3-25	S3-020558	agreed
33.203	027	-	Rel-5	Clean up one Editor's note in 33.203	F	5.3.0	S3-25	S3-020559	agreed
33.210	003	-	Rel-5	Adding requirement to provide mandatory support for 3DES encryption in NDS/IP. Remove AES references and dependencies	F	5.1.0	S3-25	S3-020563	agreed
33.203	028	-	Rel-5	Indication in the UE that the SA is no longer active in P-CSCF	F	5.3.0	S3-25	S3-020555	agreed

**Annex E: List of Liaisons****E.1 Liaisons to the meeting**

<b>TD number</b>	<b>Title</b>	<b>Source TD</b>	<b>Comment/Status</b>
S3-020457	Secure registration of IP addresses	N1-021848	Revised CR from S3-020375 in S3-020553
S3-020458	LS on on Diameter security issues	N4-020994	Response in S3-020547
S3-020459	LS on use of IP as transport for the Inter-GMLC Interface	N4-020999	Noted
S3-020460	IMS authentication vector distribution on the Cx interface	N4-021031	Response to SA WG3 questions. Noted
S3-020461	LS back to SA1 and SA2 on enhanced user privacy and new security requirements for LCS	N5-020564	Noted
S3-020462	LS reply on Packet Switched Streaming (PSS) in Rel-6 Work Programme	S1-021504	Noted
S3-020463	Liaison Statement on subscriber certificates	S1-021685	Response to SA WG3 on Subscriber Certificates. Noted.
S3-020464	LS reply on "Answer to "LS on PSS Release 6 work programme""	S1-021700	Noted
S3-020465	Support of LCS enhanced user privacy in OSA	S1-021717	Noted
S3-020466	Reply LS on Push Security	S1-021734	P Howard to lead e-mail discussion if any issues are identified in the draft TS
S3-020467	New requirements about functionality to make subscription to different domains independent or linked based on operator decision	S1-021831	Attached CR had been rejected in SA#17. Response LS in S3-020561
S3-020468	Response to T3-020406/S1-021427 (Response "Liaison Statement on Access to IMS Services using 3GPP release 99 and release 4 UICCs" (S1-020577))	S1-021835	Noted. Response LS in S3-020561
S3-020469	LS on Speech Enabled Services	S1-021846	TR 22.977 and TS 22.243 should be reviewed and contribution to e-mail group. L Finklestein to create response LS to SA WG1 by 4 November
S3-020470	Draft Working Item Description PSS Rel-6 and LS response to: "Answer to Liaison Statement regarding PSS Release 6 work pro-gramme" (S2-022050/ S4 (02)0375) from SA2, and "LS reply on Packet Switched Streaming (PSS) in Rel-6 Work Programme" (S5-024235/S4(0)0376) from SA5	S4-020484	No comments on WID. Noted
S3-020471	LS on Subscriber Certificates	T3-020628	Response to SA WG3 on Subscriber Certificates. Noted.
S3-020472	LS on User Equipment Management Feasibility Study (TR 32.802)	T3-020666	Noted
S3-020473	LS on Rel-6 WID for User Equipment Management	T3-020667	Noted
S3-020474	Response LS on Security enhancements for GERAN	GP-022819	Reply LS in S3-020566. P Howard to develop WID for next meeting
S3-020475	Liaison on Security and Charging Issues with use of HTTP within IMS	S2-022609	Reply LS in S3-020572
S3-020476	LS on 3GPP System to WLAN Inter working architecture	S2-022611	LS response to SA WG2 in S3-020586
S3-020477	Reply LS on "Gb evolution"	S2-022618	Noted
S3-020478	LS to 3GPP TSG WG CN4, CN, SA3, SA2, and GSMA SerG on the protocol development for the GMLC Lr-interface	S11102059	LS provided in S3-020582
S3-020479	LS response on subscriber certificates	N1-022051	Noted
S3-020480	Liaison statement on Interoperability Issues and SIP in IMS	N1-022160	Response in SP-020550

TD number	Title	Source TD	Comment/Status
S3-020481	LS on Status of protocol work on Ze interface	N4-021259	Noted
S3-020482	LS on re-used of START value for ciphering of RB using RLC TM during SRNS relocation	R2-022684	Agreed change needed in Rel-4. Response LS in S3-020564
S3-020483	LS to SA3 on Group release security solution	R2-022702	Other contributions considered. Need for protection to be discussed over e-mail. Response LS in S3-020565
S3-020485	Response to IETF LS on Interoperability Issues and SIP in IMS	SP-020627	Noted
S3-020497	LS on change to LI email subscription and access controlled SA3-LI document area	S3LI02_155r1	Return to LI to clarify reasons for the closing of FTP site
S3-020540	Reply LS on "Gb evolution"	GP-022821	Noted.

## E.2 Liaisons from the meeting

TD number	Title	Comment/Status	TO	CC
S3-020576	Response LS to CN WG4, SA WG5: adopts the security requirements in chapter 1.8	Approved	SA WG5 CN WG4	
S3-020577	New requirements about functionality to make subscription to different domains independent or linked based on operator decision	Approved	SA WG1 SA WG2 SA WG5	T WG3
S3-020578	Liaison statement on Interoperability Issues and SIP in IMS	Approved	TSG CN TSG SA CN WG1 SA WG1 SA WG2	SA Wg4 SA WG5 CN WG2 CN WG3 CN WG4 CN WG5
S3-020579	LS to CN WG1 on CR impacts in S3-020555 (Monika)	Approved. TDs 555 and 558 appended	CN WG1	
S3-020580	LS to CN WG1 on IETF Sec-agree alternative (K Boman)	Approved. TDs 386 and 516 appended	CN WG1	
S3-020582	LS on Lr interface security	Approved	LiF SIG	SA WG2 CN WG4
S3-020583	LS to RAN2: Reuse of COUNT-C Values for Ciphering of RB Using RLC TM During Handover	Approved	RAN WG2	
S3-020584	LS to RAN2: Group Release security solution	Approved	RAN WG2	
S3-020586	Reply LS to SA WG2 on 3GPP System to WLAN Inter working architecture	Approved	SA WG2	SA WG1
S3-020587	Liaison to SA WG2 on HTTP Security investigation within IMS	Approved. TD 528 appended	SA WG2	SA WG1 SA WG5
S3-020588	LS to SA WG2 on Presence General Requirements (K Boman)	Approved. TDs 507 and 508 appended	SA WG2	SA WG1
S3-020589	LS to GERAN cc SA WG2: Security enhancements for GERAN	Approved	TSG GERAN	SA WG1 SA WG2

**Annex F: Actions from the meeting**

- AP 25/01:** P. Howard to lead an e-mail discussion group to discuss IST issues and report to next SA WG3 meeting.
- AP 25/02:** (B. Wilhelm / C. Brookson) LI group to consider implications of Subscriber Certificate work on LI.
- AP 25/03:** C. Brookson to circulate draft 33.900 to SA WG3 for update and approval at next meeting as a Rel-6 TR.
- AP 25/04:** C. Brookson to ask operators whether there is any support for FIGS in Release 6 and report to SA WG3 meeting #26.
- AP 25/05:** B. Wilhelm to ask the LI group to provide more information on the reasons for the restricted access to the LI FTP area, in order for a better understanding of the issues involved for SA WG3 and TSG SA to be gained in considering the request (re: [TD S3-020497](#) / [S3LI02\\_155r1](#)).
- AP 25/06:** A. Escott to lead e-mail discussion group on registration of SA lifetimes and provide a CR for SA WG3 meeting #26.
- AP 25/07:** B. Owen to lead an e-mail discussion to conclude on the need to secure the Group Release function.
- AP 25/08:** P. Christoffersson (mechanism) and G. Rose (CR to 33.102) to co-ordinate the use of f8 to provide protection for Group Release mechanism, if the SA WG3 e-mail discussion on the need to have protection concludes that protection is desirable.
- AP 25/09:** P. Howard to develop WID for GERAN Security Enhancements (Rel-6).
- AP 25/10:** K. Boman to clarify the use of the term EDGE for CS and PS domains in TR 55.919 (CR to be drafted).
- AP 25/11:** P. Howard to lead e-mail discussion on Push Security issues (TS 22.174) and co-ordinate any comments to SA WG1.

**3GPP TSG SA WG3 (Security) meeting #26**

**19-22 November 2002, Oxford, England**

---

**Source: Secretary SA WG3**

**Title: Draft Report - version 0.0.4**

**Document for: Comment**

**Draft Report**



**An Oxford College**



## Contents

<b>1</b>	<b>Opening of the meeting .....</b>	<b>4</b>
<b>2</b>	<b>Agreement of the agenda and meeting objectives .....</b>	<b>4</b>
2.1	3GPP IPR Declaration .....	4
<b>3</b>	<b>Assignment of input documents.....</b>	<b>4</b>
<b>4</b>	<b>Reports from 3GPP SA3 meetings.....</b>	<b>4</b>
4.1	SA3#25, 8-11 October 2002 .....	4
4.2	SA3 LI #7, 12-14 November 2002 .....	4
<b>6</b>	<b>Reports and liaisons from other groups.....</b>	<b>5</b>
6.1	3GPP working groups.....	5
6.2	IETF co-ordination .....	5
6.3	ETSI SAGE .....	5
6.4	GSMA SG .....	5
6.5	3GPP2 .....	6
6.6	TIA TR-45 .....	6
6.7	Other Groups .....	6
<b>7</b>	<b>Technical issues .....</b>	<b>6</b>
7.1	IP multimedia subsystem (IMS) .....	6
7.2	Network domain security: IP layer (NDS/IP).....	7
7.3	Network domain security: MAP layer (NDS/MAP).....	8
7.4	UTRAN network access security .....	8
7.5	GERAN network access security.....	8
7.6	Immediate service termination (IST).....	9
7.7	Support for subscriber certificates .....	9
7.8	Digital rights management (DRM) .....	10
7.9	WLAN inter-working.....	10
7.10	Visibility and configurability of security .....	11
7.11	Push.....	11
7.12	Priority.....	11
7.13	Location services (LCS).....	11
7.14	User equipment functionality split (UEFS).....	11
7.15	Open service architecture (OSA).....	12
7.16	Generic user profile (GUP) .....	12
7.17	Presence.....	12
7.18	User equipment management (UEM).....	12
7.19	Multimedia Broadcast/Multicast Service (MBMS).....	12
7.20	Network domain security: Authentication framework.....	13
7.21	Fraud information gathering system (FIGS) .....	13
7.22	Guide to 3G security (TR 33.900).....	13

<b>8</b>	<b>Review and update of work programme .....</b>	<b>13</b>
<b>9</b>	<b>Future meeting dates and venues.....</b>	<b>14</b>
<b>10</b>	<b>Any other business .....</b>	<b>14</b>
<b>11</b>	<b>Close.....</b>	<b>14</b>
	<b>Annex A: List of attendees at the SA WG3#26 meeting and Voting List.....</b>	<b>15</b>
<b>A.1</b>	<b>List of attendees.....</b>	<b>15</b>
<b>A.2</b>	<b>SA WG3 Voting list.....</b>	<b>16</b>
	<b>Annex B: List of documents.....</b>	<b>17</b>
	<b>Annex C: Status of specifications under SA WG3 responsibility.....</b>	<b>23</b>
	<b>Annex D: List of CRs to specifications under SA WG3 responsibility agreed at this meeting.....</b>	<b>27</b>
	<b>Annex E: List of Liaisons .....</b>	<b>28</b>
<b>E.1</b>	<b>Liaisons to the meeting .....</b>	<b>28</b>
<b>E.2</b>	<b>Liaisons from the meeting.....</b>	<b>29</b>
	<b>Annex F: Actions from the meeting.....</b>	<b>30</b>

## 1 Opening of the meeting

Prof. M. Walker opened the meeting and welcomed delegates to Oxford on behalf of the hosts the *European Friends of 3GPP*.

## 2 Agreement of the agenda and meeting objectives

[TD S3-020592](#) Draft Agenda for SA WG3 meeting #26. The agenda was reviewed and **approved**.

### 2.1 3GPP IPR Declaration

The Chairman reminded delegates of their formal responsibilities under the 3GPP IPR agreement.

## 3 Assignment of input documents

The available documents were assigned to their respective agenda items.

## 4 Reports from 3GPP SA3 meetings

### 4.1 SA3#25, 8-11 October 2002

[TD S3-020593](#) Draft Report of SA WG3 meeting #25. The draft report was reviewed by the meeting. Some modifications were made on-line. The final version (with the change bars removed) was **approved** as version 1.0.0 which will be placed on the 3GPP SA WG3 FTP server area.

**AP 26/01: Secretary to as European Friends if they can arrange the S3#30 (7-10 October) in Italy.**

Actions from meeting #25:

AP 25/01: Completed. IST input provided to this meeting

AP 25/02: Completed ?

AP 25/03: Draft has been circulated and no comments received.

AP 25/04: Operators were reported to continue the FIGS documents. It was agreed that no changes are made and the Stage1 and Stage2 documents will be reproduced in Rel-6.

AP 25/05: LI group have input a new LS explaining why they request restricted FTP access.

AP 25/06: Completed. CRs to the meeting.

AP 25/07: Discussion complete and summarised in [TD S3-020649](#).

AP 25/08: The CR was produced in [TD S3-020585](#) which will be updated at this meeting.

AP 25/09: Completed in [TD S3-020655](#)

AP 25/10: Clarified in CRs to this meeting.

AP 25/11: The e-mail did not provide any comment, so a review was made of the TS and comments provided.

### 4.2 SA3 LI #7, 12-14 November 2002

The report of the previous meeting was not available at the start of this meeting, but was later provided as a draft in [TD S3-020698](#) which was **noted**.

[TD S3-020615](#) Proposed CR to 33.107: Essential correction to the LI events generated during inter-SGSN RAU, when PDP context is active (Rel-5). This CR was **approved**.

[TD S3-020616](#) Proposed CR to 33.108: Essential correction to the LI events generated during RAU, when PDP context is active (Rel-5). This CR was **approved**.

[TD S3-020617](#) Proposed CR to 33.107: Incorrect implementation of the Serving System reporting (Rel-5). This CR was **approved**.

[TD S3-020618](#) Proposed CR to 33.108: Changes to TS 33.108 for U.S. LI Requirements (Rel-5). There was some objection to the proposals in this CR, as it appeared to make the requirements statements invalid. It

was agreed to update the proposal in [TD S3-020670](#) which was presented again to the meeting and was again updated to turn the procurement text into notes. The LS was re-provided in [TD S3-020699](#) which was **approved**.

[TD S3-020614](#) LS (from SA WG3 LI) on change to LI subscription. It was thought that this would need support at the TSG SA Plenary as it provides a different access method for the LI group documents than is provided for all other 3GPP working documents. It was commented that it is important that 3GPP work is not kept secret in any way to prevent future criticism on some topics. The SA WG3 LI Group Chairman reported that she intended to go to the TSG SA meeting and would be available to support this request and answer any questions raised. The LS was updated to clarify the access criteria as any 3GPP Member in [TD S3-020671](#) which was **approved**.

## 6 Reports and liaisons from other groups

### 6.1 3GPP working groups

[TD S3-020663](#) LS (from SA WG4) on "Work Item Description PSS Rel-6". This was introduced by Ericsson and was provided for information and was **noted**.

[TD S3-020595](#) Reply LS (from SA WG5) on Draft Work Item Description PSS Rel-6. This was dealt with in the reply provided in [TD S3-020663](#) and was therefore **noted**.

### 6.2 IETF co-ordination

[TD S3-020599](#) IETF Status Update. This was introduced by Ericsson and provided the latest status and comments on IETF-dependent documents. The document was reviewed and **noted**.

[TD S3-020630](#) IETF status report: SIP security agreement. This was dealt with under agenda item 7.1 (see below).

### 6.3 ETSI SAGE

P. Christoffersson provided a verbal report on the activities and issues ongoing in ETSI SAGE.

The GSM version of MILENAGE has been delivered as an alternative for operators to the COMP 128 algorithms. The alleged attacks on Rijndael were not considered to pose any immediate threats. However, a replacement block cipher for MILENAGE may be considered to be developed next year, for backup reasons. Some bureaucracy regarding export control has now to be finalized before deliveries can start.

It was clarified that this algorithm was partly sponsored by the GSMA. Ownership and distribution rights will be jointly shared between 3GPP and GSMA.

SAGE has proposed to undertake a GSM plaintext study to get a better background for evaluation of alleged attacks on A5 algorithms. GSMA funding may be sought for external expertise in performing this study.

[TD S3-020675](#) Specification of the MILENAGE-2G Algorithms: an Example Algorithm Set for the GSM Authentication and Key Generation Functions A3 and A8. This TS was **approved** for presentation to TSG SA #18 for Approval. **The name MILENAGE-2G needs to be changed to G-MILENAGE throughout the document and M. Pope agreed to do this before inputting the 3GPP version to TSG SA for approval.**

### 6.4 GSMA SG

[TD S3-020673](#) LS (from GSMA) regarding the introduction of new example authentication algorithm for GSM. It was **agreed** that the name of the algorithm should be GSM-MILENAGE, which could be abbreviated to G-MILENAGE. The LS was then **noted**.

[TD S3-020674](#) LS (from GSMA) on introduction and adoption of A5/3 and GEA3. This was provided for information and was **noted**. **Manufacturers were requested to note the cut-off date for implementation, October 2004**, agreed in SA WG3 and supported by the GSMA.

It was reported that there are still ongoing issues under discussion, e.g. Smart Card Cloning issues, which will be reported to SA WG3 when any conclusions are drawn.

[TD S3-020678](#) Terms of Reference of the OCG ad-hoc group on Security (OCG Security). This was provided for information and was **noted**.

## 6.5 3GPP2

There was nobody available to report on the activities of 3GPP2.

## 6.6 TIA TR-45

There was nobody available to report on the activities of TIA TR-45.

## 6.7 Other Groups

There were no specific contributions under this agenda item.

# 7 Technical issues

## 7.1 IP multimedia subsystem (IMS)

[TD S3-020601](#) (LS from SA WG1) Requirement to allow access to IMS by means of SIM. This was introduced by T-mobile and describes the position of SA WG1 on the issues for access to IMS using SIM. Feedback was requested on the attached CRs. There was some uncertainty over the latest versions of the CRs attached for SA WG3 comment and so this was investigated. It was found that the attached CRs had been updated over e-mail by SA WG1 and these were provided ([TD S3-012298](#) and [TD S1-022300](#)) were provided in [TD S3-020682](#) which was then discussed.

The technical implications of these proposals from SA WG1 were recognised to have a large impact (above Category "F" CRs) which should be taken into account, as it would take some time to include changes in the SA WG3 specifications. (It was also noted that the SA WG1 CRs were marked as Category "F").

[TD S3-020602](#) Security considerations regarding IMS access with SIM authentication. This was presented by T-Mobile and outlines some potential IMS attack scenarios. It concludes that GSM AKA can be mapped onto IMS AKA with minimal changes and proposes that SA WG3 decide on one of the alternatives for *Mapping GSM AKA to Digest-AKA* provided in the contribution and to adapt IMS AKA accordingly.

**General discussion:** The SA WG3 Chairman questioned when the use of the SIM for all forms of 3GPP access was valid - indeed if the SIM can be used for all 3GPP applications (and future applications), then the worth of the more complicated USIM becomes less valuable, as the lower security provisions of the SIM are also accepted. It was also commented that if any problems should come from the allowing of the use of SIM functionality then this may also impact the image of the whole system, including USIM usage. It was stated that the allowing of the use of SIM is an operator decision and therefore the responsibility of allowing this belongs to individual operators, therefore this should be allowed in the standards. There was some discussion on this, but no unanimous decision reached on the security aspects in the meeting.

It was reported that any introduction of a new version of UMTS AKA in the IETF would require an expert review, which would take an unspecified amount of time. It was explained that the changes may be possible without introducing a new version of the RFC, by populating certain parameters in AKA version 1.

A summary of the required changes to implement the proposal was provided in [TD S3-020609](#). The Discussion document was then [noted](#).

[TD S3-020609](#) Proposed CR to 33.203: Allowing IMS access with SIM cards (Rel-5). This was introduced by T-Mobile and provided the required changes to implement the proposals in [TD S3-020602](#). The changes were discussed and modifications proposed. A drafting group was set up to discuss and agree exactly what changes are required. The CR was revised in [TD S3-020684](#) which also included a reply LS to SA WG1. The CR was reviewed, and the text "**implemented as (a) SIM**" was considered incorrect and should be changed to "**implemented with a SIM**". The CR was updated in [TD S3-020703](#) and was [approved](#).

[TD S3-020606](#) Proposed CR to 33.203: Authentication errors cause SA handling in conflict with INVITE (Rel-5). This was presented by Nokia and discussed. There was some concerns that this CR would allow the use of fraudulent session keys which could not then be verified by forcing a re-authentication to detect the presence of a valid USIM in the UE. It was decided that further discussion was needed to ensure that this does not countermand existing security and a group was set up to discuss this and return to the meeting. A CR was provided in [TD S3-020701](#) and a LS to CN WG1 in [TD S3-020702](#) (see below). The related LS attached to [TD S3-020606](#) was reviewed and revised in [TD S3-020704](#) which was [approved](#) ([TD S3-020703](#) was attached).

[TD S3-020626](#) Proposed CR to 33.203: INVITE is refused during re-transmission (Rel-5). This was presented by Nokia and was felt to need some further discussion and clarification on the reason for this change and a group was set up to discuss this and return to the meeting. A CR was provided in [TD S3-020701](#) (see below).

[TD S3-020701](#) Proposed CR to 33.203: Open issues in SA handling (Rel-5). This was presented by Nokia. It was noted that the work in other groups will probably be needed, particularly with respect to 24.228 and 24.229. This CR was **approved** and the SA WG3 Chairman undertook to raise the CR co-ordination issue at TSG SA.

[TD S3-020702](#) Liaison on (IMS) SA handling and the lifetime of old SA pair in Network Initiated Authentication. This LS was **approved** and [TD S3-020701](#) was attached.

[TD S3-020627](#) Proposed CR to 33.203: TCP and UDP share same SA (Rel-5). This was presented by Nokia. It was reported that there were other parts of the specification which also need similar changes and it was decided that the complete specification should be checked and a complete CR provided. This was done and a revised CR proposal provided in [TD S3-020679](#). Editorial changes were considered necessary which was left **for e-mail approval by Friday 29 November 2002**.

[TD S3-020628](#) Re-use and re-transmission of RAND and AUTN. This was introduced by Ericsson and summarised the agreements made by e-mail. This contribution was provided for information and was **noted**. A resulting CR based on these discussions was provided in [TD S3-020629](#).

[TD S3-020629](#) Proposed CR to 33.203: Re-use and re-transmission of RAND and AUTN (Rel-5). This was presented by Ericsson and modified slightly in the Reasons for Change. The updated CR was provided in [TD S3-020680](#) which was **approved**.

[TD S3-020630](#) IETF status report: SIP security agreement. This was presented by Ericsson and asked SA WG3 to agree on:

- *Approve the accompanied CR on updated sec-agree syntax to TS 33.203 conditionally. If the draft passes IETF Last Call, IMS Release 5 shall use this format.*
- *Approve the accompanied CR on HTTP Digest based back-up plan to TS 33.203 conditionally. If the draft does not pass IETF Last Call, IMS Release 5 shall use this format.*

Associated CRs were provided in [TD S3-020631](#) and [TD S3-020632](#) depending on whether HTTP Digest passes the IETF Last Call (see below).

[TD S3-020632](#) Proposed CR to 33.203: Update of SIP Security Agreement Syntax in Appendix H (Rel-5). The principles of this CR were agreed and the CR was updated editorially in [TD S3-020681](#) which was **approved**. With this [TD S3-020631](#) was then obsolete and was **withdrawn**.

[TD S3-020643](#) Proposed CR to 33.203: Registration and SA lifetimes (Rel-5). This was introduced by Hutchison 3G UK and was based upon e-mail discussions and agreements made before the meeting. It was thought that the method for UE setting of maximum SA Lifetime should be clearly specified, to avoid confusion. This was done and the CR updated in [TD S3-020683](#) which was **approved**.

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

[TD S3-020619](#) Security needs: Evaluation of UTRAN IP transport interfaces. This was presented by Ericsson and recommends that SA WG3 undertakes further study of threats and trust models for such interfaces considering not only the risks but also the cost aspects should security on, e.g. lur, lub, lupc, lur-g and lu-BC interfaces, be included in TS 33.210 and that security for those interfaces is introduced at a later stage only if proven necessary. It was noted that SA WG3 had already agreed to make the UTRAN lu interface protection high priority (agreed at meeting #25). **It was agreed that a security analysis identified in this contribution needs to be performed,, and also to include the ongoing requirements work in SA WG1, particularly, analysing the impact of Network Sharing.**

[TD S3-020646](#) Securing UTRAN/GERAN IP Transport interfaces and specifically the lu interface with NDS/IP mechanisms in Rel-6. This was presented by Nokia and proposed to approve a related CR to TS 33.210 ([TD S3-020647](#)) or to inform RAN WG3 that they should make a reference to TS 33.210 in their lu specification. The CR was then considered and this contribution **noted**.

[TD S3-020647](#) Proposed CR to 33.210: Securing UTRAN/GERAN IP Transport interfaces and specifically the lu interface with NDS/IP mechanisms in Rel-6 (Rel-6). After some discussion, it was considered that more study of the requirements was needed and alignment to the IMS interface security Annex was

desirable. A drafting group met to update the CR and this was provided in [TD S3-020685](#) which was **approved**.

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

[TD S3-020645](#) Proposed CR to 33.200: Removal of Automatic Key Management from Release 5 (Rel-5). This CR was **approved**.

### 7.4 UTRAN network access security

[TD S3-020648](#) Introduction of a second UMTS encryption and integrity protection algorithm. This was presented by Vodafone and asks SA WG3 to consider four proposals for the provision of a second encryption and integrity protection algorithm for more rapid deployment in case of and breakage of an algorithm. It was commented that not only the block cipher algorithm KASUMI needs to be investigated, but also whether a change from the structures (e.g. change from f8 and f9 structures) in case of there being a weakness found in the structures. The proposals were **agreed** in principle and a LS to TSG SA (for agreement and forwarding to PCG for funding decisions) and copied to GSMA SG, was provided in [TD S3-020686](#) which was **approved**.

### 7.5 GERAN network access security

[TD S3-020649](#) Group release security mechanism. This was presented by Lucent Technologies and provided the conclusions reached during an e-mail discussion on the threats and need for a Group Release Message security mechanism. SA WG3 were asked to study these results and decide whether a Group Release Message protection mechanism was required. There was much discussion about the effectiveness of protecting the Group release messages when there are other messages which are not protected and the perception that a simple "jamming" attack would be effective and cannot be practically protected against. It was finally agreed that this would not be protected for Rel-5, but a complete study on DoS threats should be carried out by SA WG3 with a view to possible protection mechanisms for Rel-6. With this decision, the proposed CRs in [TD S3-020672](#) and [TD S3-020687](#) were obsolete.

[TD S3-020669](#) LS (from RAN WG2) on outcome of group release discussions in RAN2. This was noted and a response informing RAN WG2 of the decision not to protect the Group Release messages for Rel-5 was provided in [TD S3-020688](#) which was **approved**.

[TD S3-020668](#) LS (from RAN WG2) on Correction to the START formula in 33.102. RAN WG2 requested SA WG3 to consider a draft CR to 33.102 (33.102) in order to align the START formulae in stage 2 and stage 3 (25.331) specifications. The attached CRs were considered and corrected where omissions were discovered. The CRs were accepted in principle pending the check of the affect on test specifications. The updated CRs were provided in [TD S3-020689](#), [TD S3-020690](#) and [TD S3-020691](#) which were **approved**.

[TD S3-020610](#) Proposed CR to 33.102 for information: USIM support in GERAN only terminals (Rel-5). This was presented by Siemens based on agreements reached over e-mail discussions and was **approved**.

[TD S3-020655](#) Proposed WID: GERAN A/Gb mode security enhancements. This was presented by Vodafone. Some modifications to the WID were made and the updated version was provided in [TD S3-020692](#) which was then **approved**. 4 companies indicated support and a request for more suppliers to consider support of this work by contribution was made.

[TD S3-020656](#) Proposed CR to TR 55.919: Algorithms for ECSD and EGPRS (Rel-6). This was presented by Ericsson and was based on a request from SA WG3 to provide such a CR to this meeting. This CR was **approved**.

[TD S3-020657](#) Proposed CR to 55.216: EGPRS algorithm (Rel-6). This CR was **approved**.

[TD S3-020658](#) Proposed CR to 55.217: EGPRS algorithm (Rel-6). This CR was **approved**.

[TD S3-020659](#) Proposed CR to 55.218: EGPRS algorithm (Rel-6). This CR was **approved**.

[TD S3-020665](#) ECSD and Ciphering. This was presented by Nokia and was also submitted to the GERAN meeting ongoing during the same week as this SA WG3 meeting (GP-023213). Nokia proposed specifying the use of A5/3 to derive BLOCK output parameters for both GMSK and 8-PSK modulated channels by generating two 348-bit keys and using 114-bits, discarding the remaining bits. There was some objection to changing the system that is currently working, and only changes needed to deal with the asymmetrical uplink/downlink case should be corrected. **Delegates were asked to discuss this further and bring an acceptable solution to the next SA WG3 meeting.**



[TD S3-020693](#) LS (from TSG GERAN) on ECSD and Ciphering. This was presented by Nokia. TSG GERAN asked SA WG3 to specify the usage of A5/3 according to the suggestions in the liaison (8-PSK modulated channel then use only "EDGE A5/3". This was received at the end of the meeting and was in contradiction to the proposal received from Nokia at this meeting, so it was decided that an e-mail discussion was required after the meeting.

**AP 26/02: V. Niemi to lead an e-mail discussion group on use of A5/3 for GERAN 8-PSK modulated channels (TD S3-020693). Response LS to GERAN to be approved before 10 January 2003.**

## 7.6 Immediate service termination (IST)

[TD S3-020661](#) Extending MAP-based IST capability to PS services. This was presented by Vodafone and reported the results of an e-mail discussion that was started on the applicability of IST to the PS service. No response was received to the e-mail discussion, implying that there was no interest in pursuing the topic.

## 7.7 Support for subscriber certificates

[TD S3-020597](#) LS (from SA WG2) on subscriber certificates. This was presented by Nokia and is a response to [TD S3-020447](#) sent from the last SA WG3 meeting. SA WG2 asked SA WG3 to take their view into account (detailed in attachment to the LS, 3.4 "New Gateway Type Element"). The LS was then **noted**.

[TD S3-020605](#) Comments on S3-020500 "Contribution to discussion on architecture and trust for subscriber certificates". This was presented by Nokia and provided comments on the Siemens contribution to SA WG3 meeting #25 ([TD S3-020500](#) which commented on a Nokia contribution to that meeting). Siemens provided a response to this in [TD S3-020638](#).

[TD S3-020638](#) Issues relating to a PKI for subscriber certificates. This was presented by Siemens and provided a response to Nokia's contribution in [TD S3-020605](#).

After extensive discussion a general agreement was reached: 3 alternatives for revocation of, and lifetime of certificates and whether this needs standardisation at all.

[TD S3-020625](#) Subscriber digital signatures require the use of smart cards. This was presented by Gem Plus and discussed the reasons for the need of Smart-Card security for Subscriber digital signatures and concludes that the tamper-resistant smart card will be the unique component of the UE to deal securely with digital signatures and requested SA WG3 to include this as a requirement for the support of Subscriber Certificate work. After some discussion the principle of the need for a Smart card to secure the signatures was agreed, but further study was needed to ensure that the chosen solution is flexible enough. Other contributions were then considered. (see [TD S3-020634](#), [TD S3-020637](#) and [TD S3-020636](#)). The use of a Smart Card secret mechanism raised the question of whether a bootstrapping mechanism would then be needed. Given the decision to focus on a bootstrapping mechanism, it was not considered necessary to make a decision on this contribution at this time. The document was therefore **noted** at this time and may be submitted again in the future at an appropriate time. **It was agreed that the default working principle for the creation of user based signature would be based upon the use of the UICC, except where exceptions are identified, such as for the bootstrapping method discussed below.**

[TD S3-020634](#) Architecture to support subscriber certificates based on new "gateway" type element. This was presented by Nokia and proposed *to endorse the SA WG2 recommendation about the endpoint of certificate request, i.e. the endpoint is not existing element in PS domain or in IMS; to create new TS for Stage 2 description of subscriber certificates; and to use the architecture and signalling flows presented in this document as basis for creating the new TS*. This was reviewed and used as a basis for discussion of [TD S3-020636](#).

[TD S3-020637](#) Work in OMA and W3C on certificate handling. This was presented by Siemens and summarised the work ongoing in OMA and W3C on certificate handling. This was reviewed and used as a basis for discussion of [TD S3-020636](#).

[TD S3-020636](#) Bootstrapping for subscriber certificates. This was presented by Siemens and discusses the use of the work in the WAPF in the 3GPP context, in particular with respect to providing the "Bootstrapping information" to establish a shared secret. There was some discussion on the proposals in the contribution. It was generally agreed that SA WG3 should work with OMA and help ensure all the necessary elements for the support in 3GPP is adequately covered. The contribution was reviewed and comments made on the mechanisms. It was generally recognised that the work requires further study and Architectural matters were in need of verification and development. **The principles of the contribution were accepted as a basis and**



**further work needs to be done in co-operation with other 3GPP WGs and OMA groups. SA WG3 assumed the role to keep an overview on co-ordinating this work.**

[TD S3-020677](#) Alternative proposals for subscriber certificate supporting architecture. It was noted that SA WG2 decisions made these alternatives obsolete and the contribution was therefore **noted** without a deep technical analysis in the meeting.

## 7.8 Digital rights management (DRM)

There were no specific contributions under this agenda item.

## 7.9 WLAN inter-working

[TD S3-020596](#) LS (from SA WG2) on: "3GPP System – WLAN Interworking". This was introduced by Orange France. The LS provided the Security issues that the SA WG2 WLAN group had identified and asked SA WG3 to provide answers and to continue updating them on progress in the WLAN Security area. A reply LS was provided in [TD S3-020694](#) based on discussions and contributions provided to this meeting

[TD S3-020667](#) EAP Related IETF Documents. This was presented by Gemplus and was a copy of a contribution to the SA WG2 meeting. It proposed to add the EAP-SIM and EAP-AKA IETF documents to the IETF dependencies list. This was **agreed** and it was noted that SA WG2 were sending the relevant information to the IETF dependencies list co-ordinator.

[TD S3-020600](#) 3GPP TS 33.234 V0.2.0: Wireless Local Area Network (WLAN) Interworking Security. This was presented by the editor and outlines the changes made to the draft since version 0.1.0. Comments were made on the Mutual authentication, the meaning of the term "Legacy WLAN terminals" and the availability of the referenced draft WLAN specification. The non-security-related requirements were identified for deletion. The editor undertook to update the document with agreements from discussions on other contributions and provide an updated version of the draft TS in [TD S3-020695](#) which was **noted**.

[TD S3-020608](#) Pseudo CR to requirements for WLAN interworking with 3GPP. This was introduced by Orange France and proposes changes to the draft WLAN TS in order to remove what Orange France considered to be non security-related or vague requirements. After some discussion it was considered that the requirements need to be separated into "loose coupling" (interworking) and "tight coupling" (integration). It was agreed that a replacement Pseudo-CR should be produced to do this and Orange France agreed to do this based on the latest version and e-mail discussion.

**AP 26/03: S. Nguyen Ngoc to lead e-mail discussion on separating security requirements of WLAN interworking Security draft into "loose" and "tight" requirements.**

Contributions on Identity confidentiality protection in [TD S3-020611](#), [TD S3-020676](#), [TD S3-020624](#) and [TD S3-020654](#) were considered together for a general discussion.

[TD S3-020611](#) Enhancing EAP/SIM and EAP/AKA Authentication with PEAP (Sources: Intel, Cisco, AT&T Wireless, Gemplus, Transat). *<PEAP proposal>* This was presented by Intel and proposes the use of PEAP with EAP-SIM and EAP-AKA to provide a long-term solution for enhanced security and user privacy for WLAN Authentication. A companion document was also provided in [TD S3-020676](#) "PEAP PKI Considerations" which was also presented by Intel. It was clarified that the "GSM vulnerability" stated in first paragraph of the introduction was intended to refer to the key length for ciphering and not for authentication.

The benefits were analysed to see what areas they could be useful for:

- EAP/SIM, EAP/AKA over PEAP: Some additional security was identified, but the need for this in particular scenarios needed study.
- PEAP protection for User IDs using encrypted TLS tunnels: This would provide some protection against a false server requesting the User IDs.

[TD S3-020624](#) WLAN Identity Privacy with Cryptographic Temporary Identifiers. *<TID proposal>* This was presented by Nokia and discussed the security implications of SA WG2 architectural choices and proposed a mechanism based on cryptographic Temporary Identifiers.

[TD S3-020654](#) WLAN – Pseudonym Generation for EAP-SIM/AKA. *<Pseudonym proposal>* This was presented by Ericsson and discussed the security implications of SA WG2 architectural choices and proposed a mechanism based on pseudonym generation as a form of encrypted IMSI.

It was concluded that the proposals from *TID* and *Pseudonym* proposals were essentially equivalent in principle, and both contributions identify the need for a recovery mechanism which needs further investigation. It was **agreed** that the *TID* and *Pseudonym* schemes should be taken as a basis for further study with the view to providing a combination of these two proposals for a final solution. Further discussion and contribution based on these schemes was invited.

There was a request to allow the *PEAP* proposal to be agreed as an option for implementation. **It was recognised that PEAP may be required for some other mechanisms, and if it is adopted for use in 3GPP, then the Temporary Identity scheme should be reviewed, considering the PEAP mechanism for use in Identity confidentiality.**

**Intel were asked to elaborate the reported benefits of the PEAP scheme and present them as proposals for requirements (re: TD S3-020611) for contribution to the next meeting.**

**TD S3-020653** Pseudo-CR to 33.234: Pseudonym generation and management in 3G-WLAN. This was presented by Ericsson and introduces changes proposed in **TD S3-020654**. It was agreed to add an editors note informing readers about the possibility of reviewing the Identity confidentiality scheme if PEAP is used in 3GPP security mechanisms.

**TD S3-020695** 3GPP TS 33.234 V0.3.0: Wireless Local Area Network (WLAN) Interworking Security. This was provided for information including updates to the TS agreed at this meeting and was **noted**. Delegates were asked to review this draft and contribute to the next SA WG3 meeting.

**TD S3-020639** WLAN-3G interworking security requirements relating to a functional split on the terminal side. This was presented by Siemens and concludes that the functional split on the terminal side for WLAN-3G interworking may become quite relevant. and requests to include pertinent security requirements in TS 33.234. It was **agreed** that the requirements captured in section 2 of this contribution will be included in TS 33.234.

**TD S3-020650** Need for a WLAN specific UICC application. This was presented by Gemplus and presents some potential threats during (re-)Authentication when CK and IK may be exposed and shows how these threats can be avoided if the keying material derivations are performed in a WLAN specific UICC application in charge of the UMTS AKA authentication and the computation of required specific keys. There was no support for this proposal and therefore it was **not accepted**.

**TD S3-020651** Pseudo-CR to 33.234: Change to the User Equipment definition. **The use of UE was considered in need of change as it was not in line with the definition in 3GPP standards. It was agreed that this should be modified to clarify the meaning in this context.** The principles of the changes were **agreed** and the editor was asked to edit this into the draft TS.

## 7.10 Visibility and configurability of security

There were no specific contributions under this agenda item.

## 7.11 Push

**TD S3-020662** Review of Push stage 1 specification (TS 22.174v1.1.0). This was presented by Vodafone and was a response to a LS from SA WG1 asking for a security review of TS 22.174. The review was done to version 1.1.0, which is identical with respect to the comments made, to the approved version 6.0.0. It proposed for an off-line discussion group to meet and further analyse the comments and TS and provide a LS to SA WG1 for agreement at this meeting. There was no time for an off-line meeting, and a LS reply was provided in **TD S3-020696** which was **approved**.

## 7.12 Priority

There were no specific contributions under this agenda item.

## 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)

There were no specific contributions under this agenda item.

## 7.16 Generic user profile (GUP)

There were no specific contributions under this agenda item.

## 7.17 Presence

[TD S3-020664](#) Response (from SA WG2) to Liaison on HTTP Security investigation within IMS. This was presented by Nokia and reports some review of functionalities and overall architecture aspects of usage of HTTP within IMS. This was provided for information and was reviewed and **noted**.

[TD S3-020603](#) TR 33.cde v0.2.0: Presence Service Security (Release 6). This was presented by the Editor and was reviewed. Comments were made to many sections and the editor undertook to update the draft according to agreements reached.

[TD S3-020623](#) Presence, Instant Messaging and IMS security in Rel-6. This was presented by Ericsson and was provided to initiate discussion on the desired procedure and documentation of Presence. Ericsson proposed two alternatives to solve the problem: Change the scope of TS 33.203 to include other IMS-based services; or to create a new TS for additional IMS-based services. A related CR was attached to the contribution to add IMS-based services to the Scope of TS 33.203 (Release 6). This was discussed and thought that the impacts of this change should be analysed and a decision made at the next meeting.

[TD S3-020622](#) IMS based anonymity in Presence. This was presented by Ericsson and discussed anonymity in Presence. Ericsson proposed including privacy header parameters "none", "id", "critical" and "user" for Presence security. A Pseudo-CR to include the proposals was attached to the contribution. The Lawful Interception group were asked to take the LI parts of this Pseudo-CR into account and they would not be included in the TR. The proposals were **agreed** and the Editor asked to include this in the draft TR.

[TD S3-020621](#) Pseudo CR to 33.cde (Presence Security): Confidentiality protection between UE and P-CSCF in IMS/Presence. This was presented by Ericsson and proposed changes to include confidentiality protection for IMS Presence. There was and it was considered necessary to check this and an editors note about backward compatibility would be included in the draft. It was agreed that an editors note is needed in section 6 that this assumes the use of IPsec, and the suitability of S-MIME is under study. The principles, with comments, were **agreed** for inclusion in the draft.

[TD S3-020598](#) LS (from CN WG1) on verification of the identity of watchers. This was presented by Ericsson and asked for guidance on authentication of non IMS watchers. A review of the LS was performed by Ericsson and a contribution provided in [TD S3-020620](#) which suggested that a response is provided to CN WG1 based on this discussion. Clarifications were made and a response LS to CN WG1 was provided in [TD S3-020697](#) based upon the agreements. It was agreed to approve this by e-mail after the meeting.

**Deadline for comments: 26 November 2002; Approval: 29 November 2002.**

[TD S3-020666](#) TLS versus IPsec for HTTP security. This was presented by Nokia and introduces the advantages when using TLS with HTTP connection. Nokia proposed that SA WG3 consider the advantage of TLS for HTTP security, and adopt it as a working assumption for further development. After much discussion it was felt that this could not be taken as a working assumption until further study has been performed.

**Delegates were asked to study these proposals and discuss over e-mail and contribute to the next meeting so that a decision can be made.**

## 7.18 User equipment management (UEM)

[TD S3-020594](#) LS (from SA WG5-SWGA) on Rel-6 WID for User Equipment Management. This was presented by Vodafone and was provided to SA WG3 for information. The LS was reviewed and **noted**.

[TD S3-020607](#) LS (from T WG3) on User Equipment Management. This was presented by Vodafone and was a response from T WG3 to SA WG5 on the LS in [TD S3-020594](#). The LS was provided to SA WG3 for information and **noted**.

## 7.19 Multimedia Broadcast/Multicast Service (MBMS)

[TD S3-020604](#) TR 33.cde v0.0.2: Security of Multimedia Broadcast/Multicast Service (Release 6). This was presented by the Editor who highlighted the changes since the previously distributed version. The document was briefly reviewed and used as a basis for contributions received (see below).

**TD S3-020613** Pseudo-CR to 33.cde (MBMS Security): MBMS: Reorganisation of Requirement chapters. This was presented by Siemens and proposed some re-arrangement of sections in the draft. These changes were **agreed**.

**TD S3-020635** Integrity protection for MBMS data. This was presented by Siemens and discussed integrity protection for MBMS data requirements. It was agreed that integrity protection should normally be provided for both Broadcast and Multicast data, but the feasibility of Broadcast data protection should be investigated. It was agreed that the Gmb interface shall be integrity protected. It was agreed that integrity protection for data should be optional for use. The principles of the contribution were **agreed**.

**TD S3-020641** Key distribution at Application Layer for MBMS. This was presented by Ericsson and discussed the key handling and the key distribution from the BM-SC to the UE for MBMS services at the Application Layer. Ericsson proposed that SA WG3 should continue the study of the Application Layer Security and make further investigations and contributions to SA WG3 meetings, based on the proposals given in this contribution. Delegates were asked to consider the issues raised in this document and contribute to future meetings.

**TD S3-020642** Proposed message flows for joining a multicast service. This was presented by Hutchison 3G UK and contained some high level flows for the authentication and authorisation of a user joining a multicast service and flows for the network to remove users from a multicast services. Hutchison 3G UK proposed to add the attached pseudo-CR to the MBMS TS. It was thought that the architectural issues for authorisation should be forwarded to SA WG2 for decision. The contribution was then **noted**.

**TD S3-020644** Pseudo-CR to 33.cde (MBMS Security): Clarification of re-keying requirement. This was presented by Hutchison 3G UK. The proposed changes were agreed, although it was noted that the re-keying issue was considered to be an operator decision, and the mechanism should be kept as simple as practical.

**TD S3-020652** MBMS security. This was presented by Nokia and highlighted several issues that have been found during the analysis of the alternatives discussed at SA WG3 meeting #25 and proposed that SA WG3 take the highlighted issues into account when developing the MBMS security solution. It was concluded that SA WG3 cannot progress on many issues until SA WG2 develop and stabilise the MBMS Architecture. It was agreed that an ad-hoc meeting should be set up to discuss any results from SA WG2 architecture work. It was agreed to try to join SA WG2#30 in Milan on 24 February 2003. If this is not possible, then 24 February would be reserved in the SA WG3 meeting #27 and invite experts from SA WG2, third option is to send some SA WG3 delegates to SA WG2#29 in January 2003.

## 7.20 Network domain security: Authentication framework

**TD S3-020640** Updated WID: Network Domain Security; Authentication Framework (NDS/AF). This was presented by Nokia and had been sent for e-mail comment, which were included in this contribution. **It was noted that this was really a new work item based upon the completed Feasibility study Work Item.** The WID was **approved**.

## 7.21 Fraud information gathering system (FIGS)

**TD S3-020660** Renumbering of FIGS specifications. This was presented by Vodafone and proposed the changes needed to make the FIGS specification numbering consistent with their scope. No other specifications were identified as being impacted. This proposal was **agreed** and the SA WG3 Chairman agreed to include this information in his report to TSG SA #18.

**AP 26/04: M Pope to ensure the FIGS specification numbers are modified as proposed in TD S3-020660 if approved at SA#18.**

## 7.22 Guide to 3G security (TR 33.900)

There were no specific contributions under this agenda item.

## 8 Review and update of work programme

It was decided to do this off-line. Time scales for Rel-6 WIs require update. **WI Rapporteurs should provide updates of the current status to M. Pope by Tuesday 26 November 2002.**

## 9 Future meeting dates and venues

An investigation for an ad-hoc meeting with SA WG2 to discuss MBMS issues will be made for 1) 24 February, Sophia Antipolis, 2) 24 February, Milan or 3) January with SA WG2 in San Francisco.

The planned meetings were as follows:

Meeting	Date	Location	Host
S3#27	25 - 28 February 2003	Sophia Antipolis	ETSI
S3#28	06 - 09 May 2003	Berlin	European 'Friends of 3GPP'
S3#29	15-18 July 2003	San Francisco (tbc)	NA 'Friends of 3GPP' (tbc)
S3#30	7-10 October 2003	Italy (tbc) ??	tbd

### LI meetings planned

Meeting	Date	Location	Host
SA3 LI-#7	12 - 14 November 2002	San Diego US	
SA3 LI-#8	19 - 21 February 2003	Paris FR	
SA3 LI-#9	13 - 15 May 2003	Sophia Antipolis FR	
SA3 LI-#10	16 - 18 September 2003	US	

### TSGs RAN/CN/T and SA Plenary meeting schedule

TSG RAN/CN/T #18	3 – 6 December	New Orleans USA	NA 'Friends of 3GPP'
TSG SA #18	9 – 12 December	New Orleans USA	NA 'Friends of 3GPP'
Meeting	2003	Location	Primary Host
TSG RAN/CN/T #19	11-14 March (tba)	UK	European 'Friends of 3GPP'
TSG SA #19	17-20 March	UK	European 'Friends of 3GPP'
TSG RAN/CN/T #20	3-6 June	Hämeenlinna, FIN	Nokia
TSG SA #20	9-12 June	Hämeenlinna, FIN	Nokia
TSG RAN/CN/T #21	16-19 September	Germany	
TSG SA #21	22-25 September	Germany	
TSG RAN/CN/T #22	9-12 December	US	
TSG SA #22	15-18 December	US	
Meeting	2004 DRAFT TBD	Location	Primary Host
TSG#23	March 9-12 & 15-18	China	
TSG#24	June 1-4 & 7-10	Korea	
TSG#25	7-10 & 13-16 September	USA	
TSG#26	7-10 & 13-16 December	TBD	

## 10 Any other business

[TD S3-020700](#) CALL FOR PAPERS - IEE TECHNICAL SEMINAR ON: "SECURE GSM AND BEYOND: END TO END SECURITY FOR MOBILE COMMUNICATIONS". This was provided for information and was noted.

## 11 Close

The Chairman thanked the host, *European Friends of 3GPP*, for the meeting arrangements, and the delegates for their hard work and co-operation during the meeting, and closed the meeting.



## Annex A: List of attendees at the SA WG3#26 meeting and Voting

### List

#### A.1 List of attendees

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP ORG
Mr. Hiroshi Aono	NTT DoCoMo Inc.	<a href="mailto:aono@mml.yrp.nttdocomo.co.jp">aono@mml.yrp.nttdocomo.co.jp</a>		+81 468 40 3509	+81 468 40 3788	JP ARIB
Mr. Marc Blommaert	SIEMENS ATEA NV	<a href="mailto:marc.blommaert@siemens.atea.be">marc.blommaert@siemens.atea.be</a>		+32 14 25 34 11	+32 14 25 33 39	BE ETSI
Mr. Krister Boman	ERICSSON L.M.	<a href="mailto:krister.boman@erv.ericsson.se">krister.boman@erv.ericsson.se</a>		+46 31 344 6055	+46 31 7470 5050	SE ETSI
Ms. Brye Bonner	Motorola Inc.	<a href="mailto:brye.bonner@motorola.com">brye.bonner@motorola.com</a>		+1 847.576.5920	+1.847.538.5564	US T1
Mr. Charles Brookson	DTI	<a href="mailto:cbrookson@iee.org">cbrookson@iee.org</a>	+44 7956 567 102	+44 20 7215 3691	+44 20 7931 7194	GB ETSI
Mr. Holger Butscheidt	BMW	<a href="mailto:Holger.Butscheidt@RegTP.de">Holger.Butscheidt@RegTP.de</a>		+49 6131 18 2224	+49 6131 18 5613	DE ETSI
Mr. Steve Canning	CESG	<a href="mailto:steve.canning@CESG.GSI.GOV.UK">steve.canning@CESG.GSI.GOV.UK</a>		+44 1242 221491 / 4137	+44 1242 251908	GB ETSI
Mr. Mauro Castagno	TELECOM ITALIA S.p.A.	<a href="mailto:mauro.castagno@tilab.com">mauro.castagno@tilab.com</a>		+39 0112285203	+39 0112287056	IT ETSI
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	<a href="mailto:chika@isl.melco.co.jp">chika@isl.melco.co.jp</a>		+81 467 41 2181	+81 467 41 2185	JP ARIB
Mr. Per Christoffersson	TELIA AB	<a href="mailto:per.e.christoffersson@telia.se">per.e.christoffersson@telia.se</a>		+46 705 925100		SE ETSI
Mr. Kevin England	mmO2 plc	<a href="mailto:kevin.england@o2.com">kevin.england@o2.com</a>		+447710016799		GB ETSI
Dr. Adrian Escott	Hutchison 3G UK Limited	<a href="mailto:adrian.escott@three.co.uk">adrian.escott@three.co.uk</a>		+44 7866 600924	+44 1628 766012	GB ETSI
Mr. Jean-Bernard Fischer	OBERTHUR CARD SYSTEMS S.A.	<a href="mailto:jb.fischer@oberthurcs.com">jb.fischer@oberthurcs.com</a>		+33 141 38 18 93	+33 141 38 48 23	FR ETSI
Mr. Ozgur Gurleyen	VODAFONE Group Plc	<a href="mailto:ozgur.gurleyen@vodafone.com">ozgur.gurleyen@vodafone.com</a>		+44 1635 685612		GB ETSI
Ms. Tao Haukka	Nokia Korea	<a href="mailto:tao.haukka@nokia.com">tao.haukka@nokia.com</a>		+358 40 5170079		FI TTA
Mr. Guenther Horn	SIEMENS AG	<a href="mailto:guenther.horn@siemens.com">guenther.horn@siemens.com</a>		+49 8963 641494	+49 8963 648000	DE ETSI
Mr. Peter Howard	VODAFONE Group Plc	<a href="mailto:peter.howard@vodafone.com">peter.howard@vodafone.com</a>	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB ETSI
Mr. Yu Inamura	NTT DoCoMo Inc.	<a href="mailto:jane@mml.yrp.nttdocomo.co.jp">jane@mml.yrp.nttdocomo.co.jp</a>		+81-468-40-3809	+81-468-40-3364	JP ARIB
Mr. Tom Inklebarger	AT&T Corp.	<a href="mailto:tominkle@cox.net">tominkle@cox.net</a>		+1 619 466 1408		US T1
Mr. Rafal Jaczynski	POLKOMTEL S.A.	<a href="mailto:rafal.jaczynski@polkomtel.com.pl">rafal.jaczynski@polkomtel.com.pl</a>	+48 601 135 571	+48 22 607 5571	+48 22 607 5695	PL ETSI
Mr. Alex Leadbeater	BT Group Plc	<a href="mailto:alex.leadbeater@bt.com">alex.leadbeater@bt.com</a>		+441473608440	+44 1473 608649	GB ETSI
Mr. Luis Lopez Soria	Ericsson Inc.	<a href="mailto:luis.lopez-soria@ece.ericsson.se">luis.lopez-soria@ece.ericsson.se</a>		+34 91 339 2656	+34 91 339 2538	ES T1
Mr. Sebastien Nguyen Ngoc	ORANGE FRANCE	<a href="mailto:sebastien.nguyennqc@rd.francetelecom.com">sebastien.nguyennqc@rd.francetelecom.com</a>		+33 1 45 29 47 31	+33 1 45 29 65 19	FR ETSI
Mr. Valteri Niemi	NOKIA Corporation	<a href="mailto:valteri.niemi@nokia.com">valteri.niemi@nokia.com</a>		+358 50 4837 327	+358 9 437 66850	FI ETSI
Mr. Petri Nyberg	SONERA Corporation	<a href="mailto:petri.nyberg@sonera.com">petri.nyberg@sonera.com</a>		+358 204066824	+358 2040 0 3168	FI ETSI
Mr. Bradley Owen	Lucent Technologies N. S. UK	<a href="mailto:bvowen@lucent.com">bvowen@lucent.com</a>		+44 1793 736245	+44 1793 897414	GB ETSI
Mr. Anand Palanigounder	Nortel Networks	<a href="mailto:anand@nortelnetworks.com">anand@nortelnetworks.com</a>		+1 972 684 4772	+1 972 685 3123	GB T1
Miss Mireille PAULIAC	GEMPLUS Card International	<a href="mailto:mireille.pauliac@GEMPLUS.COM">mireille.pauliac@GEMPLUS.COM</a>		+33(0)442365441	+33(0)442365792	FR ETSI
Mr. Maurice Pope	ETSI Secretariat	<a href="mailto:maurice.pope@etsi.fr">maurice.pope@etsi.fr</a>	+33 (0)6 07 59 08 49	+33 4 92 94 42 59	+33 4 92 38 52 59	FR ETSI
Ms. Stéphanie Salgado	SchlumbergerSema	<a href="mailto:salgado@montrouge.sema.slb.com">salgado@montrouge.sema.slb.com</a>		+33 1 46 00 75 11	+33 1 46 00 79 70	FR ETSI
Mr. Ville Salmensuu	SSH Communications Security	<a href="mailto:ville.salmensuu@ssh.com">ville.salmensuu@ssh.com</a>	+358 40 569 1977	+358 20 500 7496		FI ETSI
Mr. Stefan Schroeder	T-MOBILE DEUTSCHLAND	<a href="mailto:STEFAN.SCHROEDER@T-MOBILE.DE">STEFAN.SCHROEDER@T-MOBILE.DE</a>		+49 228 936 3312	+49 228 936 3309	DE ETSI
Mr. Ramachandran Subramanian	QUALCOMM EUROPE S.A.R.L.	<a href="mailto:rsubrama@qualcomm.com">rsubrama@qualcomm.com</a>		+1 858 651 2350	+1 858 651 2880	US ETSI
Mr. Benno Tietz	Vodafone D2 GmbH	<a href="mailto:benno.tietz@vodafone.com">benno.tietz@vodafone.com</a>		+49 211 533 2168	+49 211 533 1649	DE ETSI
Mr. Tommi Viitanen	Nokia Telecommunications Inc.	<a href="mailto:tommi.viitanen@nokia.com">tommi.viitanen@nokia.com</a>		+358405131090	+358718074385	FI T1
Prof. Michael Walker	VODAFONE Group Plc	<a href="mailto:mike.walker@vodafone.com">mike.walker@vodafone.com</a>	+44 77 85 277687	+44 1635 673 886	+44 1634 234939	GB ETSI
Ms. Monica Wifvesson	ERICSSON L.M.	<a href="mailto:monica.wifvesson@emp.ericsson.se">monica.wifvesson@emp.ericsson.se</a>		+46 46 193634	+46 46 231650	SE ETSI
Mr. Berthold Wilhelm	BMW	<a href="mailto:berthold.wilhelm@regtp.de">berthold.wilhelm@regtp.de</a>		+49 681 9330 562	+49 681 9330 725	DE ETSI
Dr. Qing Xuan	VODAFONE Group Plc	<a href="mailto:qing.xuan@vf.vodafone.co.uk">qing.xuan@vf.vodafone.co.uk</a>		+44(0) 1635 674781	+44 1635 523615	GB ETSI
Mr. Yanmin Zhu	Samsung Electronics Co., Ltd	<a href="mailto:zym@samsung.co.kr">zym@samsung.co.kr</a>		+861068427711	+861068481898	KR TTA

40 attendees

3GPP

SA WG3

## A.2 SA WG3 Voting list

Based on the attendees lists for meetings #24, #25 and #26, the following companies are eligible to vote at SA WG3 meeting #27:

Company	Country	Status	Partner Org
ALCATEL S.A.	FR	3GPPMEMBER	ETSI
AT&T Corp.	US	3GPPMEMBER	T1
AT&T Wireless Services, Inc.	US	3GPPMEMBER	T1
BUNDESMINISTERIUM FUR WIRTSCHAFT	DE	3GPPMEMBER	ETSI
BT Group Plc	GB	3GPPMEMBER	ETSI
Communications-Electronics Security Group	GB	3GPPMEMBER	ETSI
Cisco Systems France	FR	3GPPMEMBER	ETSI
DTI - Department of Trade and Industry	GB	3GPPMEMBER	ETSI
Ericsson Incorporated	US	3GPPMEMBER	T1
Telefon AB LM Ericsson	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 Network Systems 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
NOKIA KOREA	KR	3GPPMEMBER	TTA
Nokia Telecommunications Inc.	US	3GPPMEMBER	T1
Nortel Networks (USA)	US	3GPPMEMBER	T1
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
POLKOMTEL S.A.	PL	3GPPMEMBER	ETSI
QUALCOMM EUROPE S.A.R.L.	FR	3GPPMEMBER	ETSI
Research In Motion Limited	CA	3GPPMEMBER	ETSI
SAMSUNG Electronics Research Institute	GB	3GPPMEMBER	ETSI
Samsung Electronics Ind. Co., Ltd.	KR	3GPPMEMBER	TTA
SchlumbergerSema - Schlumberger Systèmes S.A	FR	3GPPMEMBER	ETSI
SIEMENS AG	DE	3GPPMEMBER	ETSI
SIEMENS ATEA NV	BE	3GPPMEMBER	ETSI
SONERA Corporation	FI	3GPPMEMBER	ETSI
SSH Communications Security Corp	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

45 Individual Member Companies

**Annex B: List of documents**

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020592	Draft Agenda for SA WG3 meeting #26	SA WG3 Chairman	2	Approval		Approved
S3-020593	Draft Report of SA WG3 meeting #25	SA WG3 Secretary	4.1	Approval		Small modifications and approved (Approved v1.0.0 will be put on FTP server)
S3-020594	LS (from SA WG5-SWGA) on Rel-6 WID for User Equipment Management	SA WG5-SWGA	7.18	Information		Noted
S3-020595	Reply LS (from SA WG5) on Draft Work Item Description PSS Rel-6	SA WG5	6.1	Information		Noted. Reply dealt with in s3-020664
S3-020596	LS (from SA WG2) on: "3GPP System – WLAN Interworking"	SA WG2	7.9	Action		Response LS in S3-020694
S3-020597	LS (from SA WG2) on subscriber certificates	SA WG2	7.7	Action		Noted
S3-020598	LS (from CN WG1) on verification of the identity of watchers	CN WG1	7.17	Action		Response in S3-020697 based on S3-020620
S3-020599	IETF Status Update	3GPP-IETF Status Coordinator	6.2	Information		Noted
S3-020600	3GPP TS 33.234 V0.2.0: Wireless Local Area Network (WLAN) Interworking Security	Editor	7.9	Discussion	S3-020695	Editor to update with comments. Provided in S3-020695
S3-020601	(LS from SA WG1) Requirement to allow access to IMS by means of SIM	SA WG1	7.1	Action	S3-020682	Later CRs available - document re-issued in S3-020682
S3-020602	Security considerations regarding IMS access with SIM authentication	T-Mobile	7.1	Discussion / Approval		Discussed at length. Noted. Proposal CR provided in S3-020609
S3-020603	TR 33.cde v0.2.0: Presence Service Security (Release 6)	Editor (K Boman)	7.17	Discussion		Editor to update draft according to comments and agreements
S3-020604	TR 33.cde v0.0.2: Security of Multimedia Broadcast/Multicast Service (Release 6)	Editor (A Escott)	7.19	Discussion		Noted. Used for discussion of other contributions
S3-020605	Comments on S3-020500 "Contribution to discussion on architecture and trust for subscriber certificates"	Nokia	7.7	Discussion		Discussed with S3-020638 and agreements reached. Noted
S3-020606	Proposed CR to 33.203: Authentication errors cause SA handling in conflict with INVITE (Rel-5)	Nokia	7.1	Approval		Evening session to discuss. CR in S3-020701
S3-020607	LS (from T WG3) on User Equipment Management	T WG3	7.18	Information		Noted
S3-020608	Pseudo CR to requirements for WLAN interworking with 3GPP	Orange France	7.9	Discussion / Approval		e-mail discussion to separate out loose and tight requirements
S3-020609	Proposed CR to 33.203: Allowing IMS access with SIM cards (Rel-5)	T-Mobile	7.1	Approval	S3-020684	Revised with comments in S3-020684
S3-020610	Proposed CR to 33.102 for information: USIM support in GERAN only terminals (Rel-5)	Siemens	7.5	Approval		Equivalent of S3-020591, discussed over e-mail. Approved



TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020611	Enhancing EAP/SIM and EAP/AKA Authentication with PEAP	Intel, Cisco, AT&T Wireless, Gemplus, Transat	7.9	Discussion / Approval		Temp Identity protection mechanism based on S3-020624 and S3-020654. May be reconsidered if PEAP is adopted for 3GPP use elsewhere. Intel asked to update contribution for next meeting
S3-020612	PEAP PKI Considerations	Intel, Cisco, AT&T Wireless, Gemplus, Transat	7.9	Discussion	S3-020676	Revised in s3-020676
S3-020613	Pseudo-CR to 33.cde (MBMS Security): MBMS: Reorganisation of Requirement chapters	Siemens	7.19	Discussion		Agreed
S3-020614	LS (from SA WG3 LI) on change to LI subscription	SA WG3 LI Group	4.2	Action	S3-020671	Modified in S3-020671
S3-020615	Proposed CR to 33.107: Essential correction to the LI events generated during inter-SGSN RAU, when PDP context is active (Rel-5)	SA WG3 LI Group	4.2	Approval		Approved
S3-020616	Proposed CR to 33.108: Essential correction to the LI events generated during RAU, when PDP context is active (Rel-5)	SA WG3 LI Group	4.2	Approval		Approved
S3-020617	Proposed CR to 33.107: Incorrect implementation of the Serving System reporting (Rel-5)	SA WG3 LI Group	4.2	Approval		Approved
S3-020618	Proposed CR to 33.108: Changes to TS 33.108 for U.S. LI Requirements (Rel-5)	SA WG3 LI Group	4.2	Approval	S3-020670	Some objection to detraction of requirements, Revised in S3-020670
S3-020619	Security needs: Evaluation of UTRAN IP transport interfaces	Ericsson	7.2	Discussion / Decision		Agreed to do security analysis and take account of SA1 work, and NW Sharing impacts
S3-020620	Watcher Authorization in Presence	Ericsson	7.17	Discussion / Decision		Used as basis for LS to CN WG1 in S3-020697
S3-020621	Pseudo CR to 33.cde (Presence Security): Confidentiality protection between UE and P-CSCF in IMS/Presence	Ericsson	7.17	Discussion / Decision		Agreed with addition of comments made and editors notes
S3-020622	IMS based anonymity in Presence	Ericsson	7.17	Discussion / Decision		Agreed. Changes to be added to draft TR
S3-020623	Presence, Instant Messaging and IMS security in Rel-6	Ericsson	7.17	Discussion / Decision		Change of scope to 33.203 to be analysed and decision made at next meeting
S3-020624	WLAN Identity Privacy with Cryptographic Temporary Identifiers	Nokia	7.9	Discussion / Approval		This and S3-020624 taken as basis for combined solution
S3-020625	Subscriber digital signatures require the use of smart cards	GEMPLUS Card International	7.7	Discussion / Approval		UICC based user certificates accepted as working principle, except for identified exceptions

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020626	Proposed CR to 33.203: INVITE is refused during re-transmission (Rel-5)	Nokia	7.1	Approval		Evening session to discuss. CR in S3-020701
S3-020627	Proposed CR to 33.203: TCP and UDP share same SA (Rel-5)	Nokia	7.1	Approval	S3-020679	Check for other parts of specification to update in same way. Revised in S3-020679
S3-020628	Re-use and re-transmission of RAND and AUTN	Ericsson	7.1	Information		Noted. Related CR in S3-020629
S3-020629	Proposed CR to 33.203: Re-use and re-transmission of RAND and AUTN (Rel-5)	Ericsson	7.1	Approval	S3-020680	Modification to Reasons for Change made and provided in S3-020680
S3-020630	IETF status report: SIP security agreement	Ericsson, Nokia	7.1	Discussion / Decision		Discussed - CR in S3-020632 considered, S3-020631 withdrawn
S3-020631	WITHDRAWN - Proposed CR to 33.203: Update of SIP Security Agreement Syntax in Appendix H (Rel-5)	Ericsson, Nokia	7.1	Discussion / Decision		WITHDRAWN - Covered by agreement of S3-020632 / S3-020681
S3-020632	Proposed CR to 33.203: Update of SIP Security Agreement Syntax in Appendix H (Rel-5)	Ericsson, Nokia	7.1	Discussion / Decision	S3-020681	(Only if IETF draft not agreed) - updated in S3-020681
S3-020633	WITHDRAWN - Proposal for Annex H by extending HTTP Digest for SA management	Nokia	7.1	Discussion / Approval		WITHDRAWN
S3-020634	Architecture to support subscriber certificates based on new "gateway" type element	Nokia	7.7	Discussion / Approval		Noted. Used as basis to S3-020636
S3-020635	Integrity protection for MBMS data	Siemens	7.19	Discussion / Decision		Agreed principles
S3-020636	Bootstrapping for subscriber certificates	Siemens	7.7	Discussion / Devision		Agreed in principle. Work needed in coordination of other groups work
S3-020637	Work in OMA and W3C on certificate handling	Siemens	7.7	Discussion		Noted. Used as basis to S3-020636
S3-020638	Issues relating to a PKI for subscriber certificates	Siemens	7.7	Discussion		(Short reply to Nokia's comments on S3-020500). Discussed and agreements reached. Noted
S3-020639	WLAN-3G interworking security requirements relating to a functional split on the terminal side	Siemens	7.9	Discussion		Agreed to include the requirements captured in section 2 in TS 33.234
S3-020640	Updated WID: Network Domain Security; Authentication Framework (NDS/AF)	Nokia	7.20	Approval		Approved (New WID)
S3-020641	Key distribution at Application Layer for MBMS	Ericsson	7.19	Discussion		Delegates asked to consider issues and contribute to future meetings
S3-020642	Proposed message flows for joining a multicast service	Hutchison 3G UK	7.19	Discussion / Decision		SA Wg2 responsibility for authorisation work. Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020643	Proposed CR to 33.203: Registration and SA lifetimes (Rel-5)	Hutchison 3G UK	7.1	Approval	S3-020683	Revised in S3-020683
S3-020644	Pseudo-CR to 33.cde (MBMS Security): Clarification of re-keying requirement	Hutchison 3G UK	7.19	Approval		Agreed. Note the mechanism needs to be kept as simple as practical
S3-020645	Proposed CR to 33.200: Removal of Automatic Key Management from Release 5 (Rel-5)	Hutchison 3G UK	7.3	Approval		Approved
S3-020646	Securing UTRAN/GERAN IP Transport interfaces and specifically the lu interface with NDS/IP mechanisms in Rel6	Nokia	7.2	Discussion / Approval		Noted. Related CR in S3-020647
S3-020647	Proposed CR to 33.210: Securing UTRAN/GERAN IP Transport interfaces and specifically the lu interface with NDS/IP mechanisms in Rel6 (Rel-6)	Nokia	7.2	Approval	S3-020685	Revised in S3-020685
S3-020648	Introduction of a second UMTS encryption and integrity protection algorithm	Vodafone	7.4	Discussion / Decision		Agreed in principle - LS to TSG SA in S3-020686
S3-020649	Group release security mechanism	Lucent technologies	7.4	Discussion / Approval		Decision not to protect GRM for Rel-5. Full DoS Study needed for Rel-6.
S3-020650	Need for a WLAN specific UICC application	GEMPLUS Card International	7.9	Discussion / Approval		
S3-020651	Pseudo-CR to 33.234: Change to the User Equipment definition	GEMPLUS Card International	7.9	Approval		Agreed - terminology of UE needs clarifying in this context
S3-020652	MBMS security	Nokia	7.19	Discussion		Attempt to have joint session with S3/S2 experts during a meeting
S3-020653	Pseudo-CR to 33.234: Pseudonym generation and management in 3G-WLAN	Ericsson	7.9	Approval		Agreed to add this + editors note on potential use of PEAP
S3-020654	WLAN – Pseudonym Generation for EAP-SIM/AKA	Ericsson	7.9	Discussion / Decision		This and S3-020624 taken as basis for combined solution
S3-020655	Proposed WID: GERAN A/Gb mode security enhancements	Vodafone	7.5	Approval	S3-020692	Modified in S3-020692
S3-020656	Proposed CR to TR 55.919: Algorithms for ECSD and EGPRS (Rel-6)	Ericsson, Telia	7.5	Approval		Approved
S3-020657	Proposed CR to 55.216: EGPRS algorithm (Rel-6)	Ericsson, Telia	7.5	Approval		Approved
S3-020658	Proposed CR to 55.217: EGPRS algorithm (Rel-6)	Ericsson, Telia	7.5	Approval		Approved
S3-020659	Proposed CR to 55.218: EGPRS algorithm (Rel-6)	Ericsson, Telia	7.5	Approval		Approved
S3-020660	Renumbering of FIGS specifications	Vodafone	7.21	Discussion / Decision		Agreed. Chairman to report to SA#18
S3-020661	Extending MAP-based IST capability to PS services	Vodafone	7.6	Discussion / Decision		Noted. No further IST work for PS needed at this point.
S3-020662	Review of Push stage 1 specification (TS 22.174v1.1.0)	Vodafone	7.11	Discussion / Decision		LS to SA1 in S3-020696
S3-020663	LS (from SA WG4) on "Work Item Description PSS Rel-6"	SA WG4	6.1	Information		Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020664	Response (from SA WG2) to Liaison on HTTP Security investigation within IMS	SA WG2	7.17	Information		Noted
S3-020665	ECSD and Ciphering	Nokia	7.5	Discussion		Delegates were asked to discuss this further and bring an acceptable solution to the next SA WG3 meeting
S3-020666	TLS versus IPsec for HTTP security	Nokia	7.17	Discussion /Decision		E-mail discussion and decision at next meeting
S3-020667	EAP Related IETF Documents	Nokia, Ericsson, Gemplus, Intel	7.9	Information		Proposal agreed EAP-SIM & EAP-AKA to be added to dependencies list
S3-020668	LS (from RAN WG2) on Correction to the START formula in 33.102	RAN WG2	7.4	Action		Attached CRs updated in S3-020689, S3-020690 and S3-020691
S3-020669	LS (from RAN WG2) on outcome of group release discussions in RAN2	RAN WG2	7.4	Action		Response in S3-020688
S3-020670	Proposed CR to 33.108: Changes to TS 33.108 for U.S. LI Requirements (Rel-5)	SA WG3 LI Group	4.2	Approval	S3-020699	Updated in S3-020699
S3-020671	LS (from SA WG3 LI) on change to LI subscription	SA WG3 LI Group	4.2	Action		Approved
S3-020672	Proposed CR to 33.102: USIM support in GERAN only terminals (Rel-5)	SA WG3	7.4	Approval		Provided for info in meeting#25 (S3-020585). Obsolete by decision not to protect GRM in Rel-5 (see S3-020649)
S3-020673	LS (from GSMA) regarding the introduction of new example authentication algorithm for GSM	GSMA Security Group	6.4	Information		Noted. G-Milenage agreed as abbreviation for algorithm
S3-020674	LS (from GSMA) on introduction and adoption of A5/3 and GEA3	GSMA Security Group	6.4	Information		Noted
S3-020675	Specification of the MILENAGE-2G Algorithms: an Example Algorithm Set for the GSM Authentication and Key Generation Functions A3 and A8	GSMA Security Group	6.4	Information		Approved. Change MILENAGE-2G to 2G-MILENAGE before pres to SA#18 for approval
S3-020676	PEAP PKI Considerations	Intel, Cisco, AT&T Wireless, Gemplus, Transat	7.9	Discussion		Support for S3-020611. Noted
S3-020677	Alternative proposals for subscriber certificate supporting architecture	Alcatel	7.7	Discussion		Noted. Superseded by SA WG2 architecture decisions
S3-020678	Terms of Reference of the OCG ad-hoc group on Security (OCG Security)	C. Brookson	6.4	Information		Noted
S3-020679	Proposed CR to 33.203: TCP and UDP share same SA (Rel-5)	Nokia	7.1	Approval		Editorial changes needed. For e-mail approval by Friday 29 November 2002.
S3-020680	Proposed CR to 33.203: Re-use and re-transmission of RAND and AUTN (Rel-5)	Ericsson	7.1	Approval		Approved
S3-020681	Proposed CR to 33.203: Update of SIP Security Agreement Syntax in Appendix H (Rel-5)	Ericsson, Nokia	7.1	Approval		Approved
S3-020682	(LS from SA WG1) Requirement to allow access to IMS by means of SIM	SA WG1	7.1	Action		Discussed

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020683	Proposed CR to 33.203: Registration and SA lifetimes (Rel-5)	Hutchison 3G UK	7.1	Approval		Approved
S3-020684	Proposed CR to 33.203: Allowing IMS access with SIM cards (Rel-5)	T-Mobile	7.1	Approval	S3-020703 S3-020704	CR Revised in S3-020703. LS revised in S3-020704
S3-020685	Proposed CR to 33.210: Securing UTRAN/GERAN IP Transport interfaces and specifically the Iu interface with NDS/IP mechanisms (Rel-6)	Nokia	7.2	Approval		Approved
S3-020686	LS to TSG SA: Introduction of a second UMTS encryption and integrity protection algorithm (UEA2 and UIA2)	SA WG3	7.4	Approval		Approved
S3-020687	Proposed CR to 33.102: USIM support in GERAN only terminals (Rel-5)	Lucent technologies	7.5	Approval		Obsolete by decision not to protect GRM for Rel-5 (see S3-020649)
S3-020688	Response LS to RAN WG2: Group Release security solution	SA WG3	7.5	Approval		Approved
S3-020689	CR to 33.102: Correction to the START formula (R99)	SA WG3	7.5	Approval		Approved
S3-020690	CR to 33.102: Correction to the START formula (Rel-4)	SA WG3	7.5	Approval		Approved
S3-020691	CR to 33.102: Correction to the START formula (Rel-5)	SA WG3	7.5	Approval		Approved
S3-020692	Proposed WID: GERAN A/Gb mode security enhancements	Vodafone	7.5	Approval		Approved
S3-020693	LS (from TSG GERAN) on ECSD and Ciphering	TSG GERAN	7.5	Action		E-mail discussion and response LS lead by V. Niemi
S3-020694	Reply LS to SA WG2 on: "3GPP System – WLAN Interworking"	SA WG3 (Sebastien)	7.9	Approval		Approved
S3-020695	3GPP TS 33.234 V0.3.0: Wireless Local Area Network (WLAN) Interworking Security	Editor	7.9	Information		Noted
S3-020696	Reply LS to SA WG1 on Push Security	SA WG3 (P Howard)	7.11	Approval		Approved
S3-020697	LS to CN WG1: Presence Security Architecture	SA WG3 (K Boman)	7.17	Approval		For e-mail approval after meeting
S3-020698	Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #4/02 on lawful interception - San Diego 12-14 November 2002	SA WG3 LI Group	4.2	Information		Noted
S3-020699	Proposed CR to 33.108: Changes to TS 33.108 for U.S. LI Requirements (Rel-5)	SA WG3 LI Group	4.2	Approval		Approved
S3-020700	CALL FOR PAPERS - IEE TECHNICAL SEMINAR ON: "SECURE GSM AND BEYOND: END TO END SECURITY FOR MOBILE COMMUNICATIONS"	C. Brookson	10	Information		Noted
S3-020701	Proposed CR to 33.203: Open issues in SA handling (Rel-5)	Nokia	7.1	Approval		Approved
S3-020702	Liaison to CN WG1 on (IMS) SA handling and the lifetime of old SA pair in Network Initiated Authentication	SA WG3	7.1	Approval		Approved. S3-020701 attached
S3-020703	Proposed CR to 33.203: Allowing IMS access with SIM cards (Rel-5)	T-Mobile	7.1	Approval		Approved
S3-020704	LS on Requirement to allow access to IMS by means of SIM	SA WG3	7.1	Approval		Approved. S3-020703 attached

**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	CHRISTOFFE RSSON, Per	Ph1
TS	02.09	4.5.1	Security aspects	CHRISTOFFE RSSON, Per	Ph2
TS	02.09	5.2.1	Security aspects	CHRISTOFFE RSSON, Per	R96
TS	02.09	6.1.1	Security aspects	CHRISTOFFE RSSON, Per	R97
TS	02.09	7.1.1	Security aspects	CHRISTOFFE RSSON, Per	R98
TS	02.09	8.0.1	Security aspects	CHRISTOFFE RSSON, 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	CHRISTOFFE RSSON, Per	R99
TS	21.133	4.1.0	3G security; Security threats and requirements	CHRISTOFFE RSSON, 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	22.022	5.0.0	Personalisation of Mobile Equipment (ME); Mobile functionality specification	NGUYEN NGOC, Sebastien	Rel-5
TS	22.032	3.0.0	Immediate Service Termination (IST); Service description; Stage 1	HOWARD, Peter	R99

Specification			Title	Editor	Rel
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	3.1.0	Immediate Service Termination (IST); Stage 2	HOWARD, Peter	R99
TS	23.035	4.1.0	Immediate Service Termination (IST); Stage 2	HOWARD, Peter	Rel-4
TS	23.035	5.1.0	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	5.1.0	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	5.4.0	3G security; Lawful interception architecture and functions	WILHELM, Berthold	Rel-5
TS	33.108	5.1.0	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	33.201	none	Access domain security - TO BE DELETED	POPE, Maurice	Rel-5
TS	33.203	5.3.0	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	KOIJEN, Geir	Rel-5
TR	33.810	1.0.1	3G Security; Network Domain Security / Authentication Framework (NDS/AF); Feasibility Study to support NDS/IP evolution	VIITANEN, Tommi	Rel-6
TR	33.900	0.4.1	Guide to 3G security	BROOKSON, Charles	Rel-5
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	33.903	none	Access Security for IP based services - TO BE DELETED	VACANT,	Rel-4
TR	33.903	none	Access Security for IP based services - TO BE DELETED	VACANT,	Rel-5
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

Specification			Title	Editor	Rel
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
TS	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
TS	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	CHRISTOFFE RSSON, 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	43.020	5.0.0	Security-related network functions	GILBERT, Henri	Rel-5
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



Specification			Title	Editor	Rel
TS	55.216	6.0.0	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	CHRISTOFFE RSSON, Per	Rel-6
TS	55.217	6.0.0	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 2: Implementors' test data	CHRISTOFFE RSSON, Per	Rel-6
TS	55.218	6.0.0	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	CHRISTOFFE RSSON, Per	Rel-6
TR	55.919	6.0.0	Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report	CHRISTOFFE RSSON, Per	Rel-6

**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
33.102	176		R99	Correction to the START formula	F	3.12.0	S3-26	S3-020689	agreed
33.102	177		Rel-4	Correction to the START formula	A	4.4.0	S3-26	S3-020690	agreed
33.102	178		Rel-5	Correction to the START formula	A	5.1.0	S3-26	S3-020691	agreed
33.107	029		Rel-5	Essential correction to the LI events generated during inter-SGSN RAU, when PDP context is active	F	5.4.0	S3-26	S3-020615	agreed
33.107	030		Rel-5	Incorrect implementation of the Serving System reporting	F	5.4.0	S3-26	S3-020617	agreed
33.108	005		Rel-5	Essential correction to the LI events generated during RAU, when PDP context is active	F	5.1.0	S3-26	S3-020616	agreed
33.108	006		Rel-5	Changes to TS 33.108 for U.S. LI Requirements	F	5.1.0	S3-26	S3-020699	agreed
33.200	022	-	Rel-5	Removal of Automatic Key Management from Release 5	C	5.0.0	S3-26	S3-020645	agreed
33.203	028	-	Rel-5	Re-use and re-transmission of RAND and AUTN	F	5.3.0	S3-26	S3-020680	agreed
33.203	029	-	Rel-5	Update of SIP Security Agreement Syntax in Appendix H	F	5.3.0	S3-26	S3-020681	agreed
33.203	030	-	Rel-5	Registration and SA lifetimes	F	5.3.0	S3-26	S3-020683	agreed
33.203	031	-	Rel-5	Open issues in SA handling	F	5.3.0	S3-26	S3-020701	agreed
33.203	032	-	Rel-5	Allowing IMS access with SIM cards	B	5.3.0	S3-26	S3-020703	agreed
33.210	004	-	Rel-6	Securing UTRAN/GERAN IP Transport interfaces and specifically the lu interface with NDS/IP mechanisms	B	5.1.0	S3-26	S3-020685	agreed
55.216	001		Rel-6	EGPRS algorithm	F	6.0.0	S3-26	S3-020657	agreed
55.217	001		Rel-6	EGPRS algorithm	F	6.0.0	S3-26	S3-020658	agreed
55.218	001		Rel-6	EGPRS algorithm	F	6.0.0	S3-26	S3-020659	agreed
55.919	001		Rel-6	Algorithms for ECSD and EGPRS	F	6.0.0	S3-26	S3-020659	agreed

**Annex E: List of Liaisons****E.1 Liaisons to the meeting**

TD number	Title	Source TD	Comment/Status
S3-020594	LS (from SA WG5-SWGA) on Rel-6 WID for User Equipment Management	S5-022318	Noted
S3-020595	Reply LS (from SA WG5) on Draft Work Item Description PSS Rel-6	S5-024469	Noted. Reply dealt with in s3-020664
S3-020596	LS (from SA WG2) on: "3GPP System – WLAN Interworking"	S2-023122	Response LS in S3-020694
S3-020597	LS (from SA WG2) on subscriber certificates	S2-023130	Noted
S3-020598	LS (from CN WG1) on verification of the identity of watchers	N1-022226	Response in S3-020697 based on S3-020620
S3-020607	LS (from T WG3) on User Equipment Management	T3-020890	Noted
S3-020614	LS (from SA WG3 LI) on change to LI subscription	S3LI02_182	Modified in S3-020671
S3-020663	LS (from SA WG4) on "Work Item Description PSS Rel-6"	S4-020733	Noted
S3-020664	Response (from SA WG2) to Liaison on HTTP Security investigation within IMS	S2-023675	Noted
S3-020668	LS (from RAN WG2) on Correction to the START formula in 33.102	R2-023258	Agreed principle. Attached CRs updated in S3-020689, S3-020690 and S3-020691
S3-020669	LS (from RAN WG2) on outcome of group release discussions in RAN2	R2-023263	Response in S3-020688
S3-020671	LS (from SA WG3 LI) on change to LI subscription	S3-020614	Approved
S3-020673	LS (from GSMA) regarding the introduction of new example authentication algorithm for GSM	GSMA	Noted. G-Milenage agreed as abbreviation for algorithm
S3-020674	LS (from GSMA) on introduction and adoption of A5/3 and GEA3	GSMA	Noted
S3-020682	(LS from SA WG1) Requirement to allow access to IMS by means of SIM	S1-022109 (with updated CR attachments)	Discussed
S3-020693	LS (from TSG GERAN) on ECSD and Ciphering	GP-023402	E-mail discussion and response LS lead by V. Niemi

**E.2 Liaisons from the meeting**

<b>TD number</b>	<b>Title</b>	<b>Comment/Status</b>	<b>TO</b>	<b>CC</b>
S3-020671	LS (from SA WG3 LI) on change to LI subscription	Approved	<b>TSG SA</b>	
S3-020686	LS to TSG SA: Introduction of a second UMTS encryption and integrity protection algorithm (JEA2 and UIA2)	Approved	<b>TSG SA</b>	<b>GSMA-SG, ETSI-SAGE, 3GPP2 SA4, TIA TR45- AHAG</b>
S3-020688	Response LS to RAN WG2:Group Release security solution	Approved	<b>TSG RAN, RAN WG2</b>	
S3-020694	Reply LS to SA WG2 on: "3GPP System – WLAN Interworking"	Approved	<b>SA WG2</b>	
S3-020696	Reply LS to SA WG1 on Push Security	Approved	<b>SA WG1</b>	<b>SA WG2, T WG2</b>
S3-020697	LS to CN WG1: Presence Security Architecture	For e-mail approval after meeting	<b>CN WG1</b>	
S3-020702	Liaison to CN WG1 on (IMS) SA handling and the lifetime of old SA pair in Network Initiated Authentication	Approved. S3-020701 attached	<b>CN WG1</b>	
S3-020704	LS on Requirement to allow access to IMS by means of SIM	Approved. S3-020703 attached	<b>TSG SA, SA WG1, CN WG1, CN WG4, SA WG2, T WG3</b>	

**Annex F: Actions from the meeting**

- AP 26/01:** Secretary to ask European Friends if they can arrange the S3#30 (7-10 October) in Italy.
- AP 26/02:** V. Niemi to lead an e-mail discussion group on use of A5/3 for GERAN 8-PSK modulated channels (TD S3-020693). Response LS to GERAN to be approved before 10 January 2003.
- AP 26/03:** S. Nguyen Ngoc to lead e-mail discussion on separating security requirements of WLAN interworking Security draft into "loose" and "tight" requirements.
- AP 26/04:** M Pope to ensure the FIGS specification numbers are modified as proposed in TD S3-020660 if approved at SA#18.