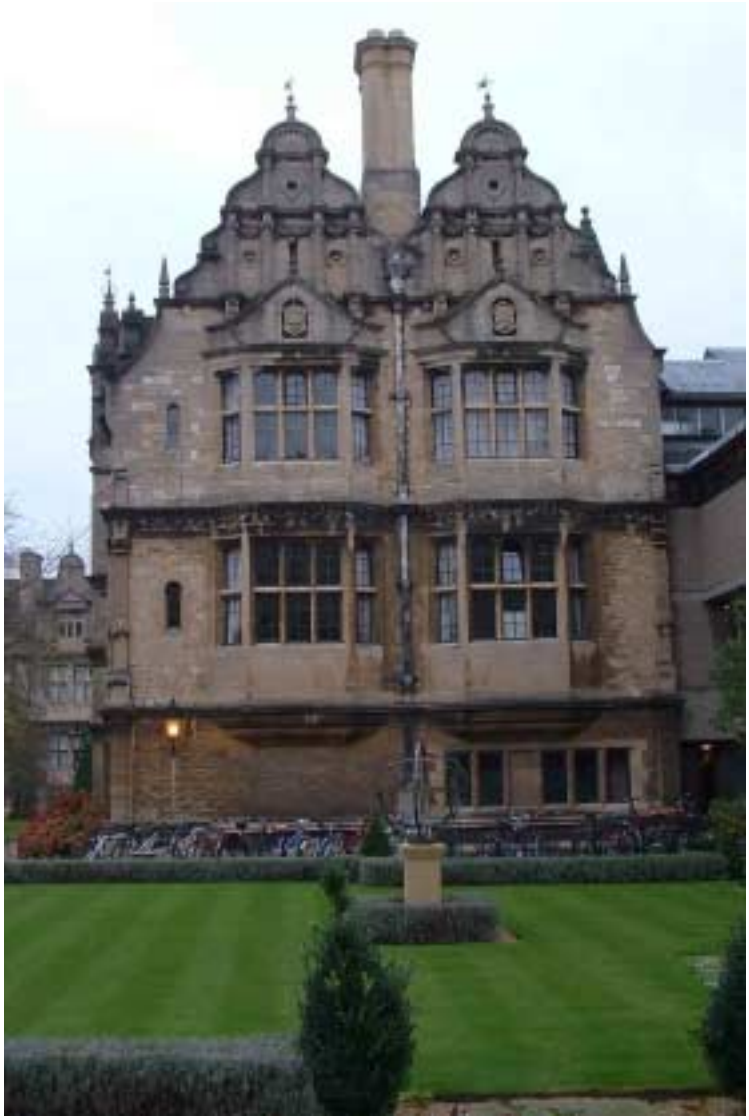
**3GPP TSG SA WG3 (Security) meeting #26**

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

| | |
|---|---|
| **Source:** | **Secretary SA WG3** |
| **Title:** | **Report - version 1.0.0** |
| **Status:** | **Approved** |

**Report**



**An Oxford College**

## Contents

# 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 serer area.

**AP 26/01: Secretary to ask 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.

## 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 S3-020663 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 GSM-MILENAGE (see TD S3-020673 under agenda item 6.4) 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 removed 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. Iur, Iub, Iupc, Iur-g and Iu-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 Iu 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 Iu 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 Iu 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 Iu 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**. Secretarys note: Following an e-mail discussion a CR was created and approved in TD S3-030015 (of SA WG3 meeting #27).

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 their 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 "authentication and key derivation" and "data transfer". 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 "authentication and key derivation" and "data transfer" 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 identifed 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) | 3GPP2 (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. | aono@mml.yrp.nttdocomo.co.jp | | +81 468 40 3509 | +81 468 40 3788 | JP | ARIB |
| Mr. Marc Blommaert | SIEMENS ATEA NV | marc.blommaert@siemens.atea.be | | +32 14 25 34 11 | +32 14 25 33 39 | BE | ETSI |
| Mr. Krister Boman | ERICSSON L.M. | krister.boman@erv.ericsson.se | | +46 31 747 4055 | +46 31 7470 5050 | SE | ETSI |
| Ms. Brye Bonner | Motorola Inc. | brye.bonner@motorola.com | | +1 847.576.5920 | +1.847.538.5564 | US | T1 |
| Mr. Charles Brookson | DTI | cbrookson@iee.org | +44 7956 567 102 | +44 20 7215 3691 | +44 20 7931 7194 | GB | ETSI |
| Mr. Holger Butscheidt | BMWi | Holger.Butscheidt@RegTP.de | | +49 6131 18 2224 | +49 6131 18 5613 | DE | ETSI |
| Mr. Steve Canning | CESG | steve.canning@CESG.GSI.GOV.UK | | +44 1242 221491 / 4137 | +44 1242 251908 | GB | ETSI |
| Mr. Mauro Castagno | TELECOM ITALIA S.p.A. | mauro.castagno@tilab.com | | +39 0112285203 | +39 0112287056 | IT | ETSI |
| Mr. Takeshi Chikazawa | Mitsubishi Electric Co. | chika@isl.melco.co.jp | | +81 467 41 2181 | +81 467 41 2185 | JP | ARIB |
| Mr. Per Christoffersson | TELIA AB | per.e.christoffersson@telia.se | | +46 705 925100 | | SE | ETSI |
| Mr. Kevin England | mmO2 plc | kevin.england@o2.com | | +447710016799 | | GB | ETSI |
| Dr. Adrian Escott | Hutchison 3G UK Limited | adrian.escott@three.co.uk | | +44 7866 600924 | +44 1628 766012 | GB | ETSI |
| Mr. Jean-Bernard Fischer | OBERTHUR CARD SYSTEMS S.A. | jb.fischer@oberthurcs.com | | +33 141 38 18 93 | +33 141 38 48 23 | FR | ETSI |
| Mr. Ozgur Gurleyen | VODAFONE Group Plc | ozgur.gurleyen@vodafone.com | | +44 1635 685612 | | GB | ETSI |
| Ms. Tao Haukka | Nokia Korea | tao.haukka@nokia.com | | +358 40 5170079 | | FI | TTA |
| Mr. Guenther Horn | SIEMENS AG | guenther.horn@siemens.com | | +49 8963 641494 | +49 8963 648000 | DE | ETSI |
| Mr. Peter Howard | VODAFONE Group Plc | peter.howard@vodafone.com | +44 7787 154058 | +44 1635 676206 | +44 1635 231721 | GB | ETSI |
| Mr. Yu Inamura | NTT DoCoMo Inc. | jane@mml.yrp.nttdocomo.co.jp | | +81-468-40-3809 | +81-468-40-3364 | JP | ARIB |
| Mr. Tom Inklebarger | AT&T Corp. | tominkle@cox.net | | +1 619 466 1408 | | US | T1 |
| Mr. Rafal Jaczynski | POLKOMTEL S.A. | rafal.jaczynski@polkomtel.com.pl | +48 601 135 571 | +48 22 607 5571 | +48 22 607 5695 | PL | ETSI |
| Mr. Alex Leadbeater | BT Group Plc | alex.leadbeater@bt.com | | +441473608440 | +44 1473 608649 | GB | ETSI |
| Mr. Luis Lopez Soria | Ericsson Inc. | luis.lopez-soria@ece.ericsson.se | | +34 91 339 2656 | +34 91 339 2538 | ES | T1 |
| Mr. Sebastien Nguyen Ngoc | ORANGE FRANCE | sebastien.nguyenngoc@rd.francetelecom.com | | +33 1 45 29 47 31 | +33 1 45 29 65 19 | FR | ETSI |
| Mr. Valtteri Niemi | NOKIA Corporation | valtteri.niemi@nokia.com | | +358 50 4837 327 | +358 9 437 66850 | FI | ETSI |
| Mr. Petri Nyberg | SONERA Corporation | petri.nyberg@sonera.com | | +358 204066824 | +358 2040 0 3168 | FI | ETSI |
| Mr. Bradley Owen | Lucent Technologies N. S. UK | bvowen@lucent.com | | +44 1793 736245 | +44 1793 897414 | GB | ETSI |
| Mr. Anand Palanigounder | Nortel Networks | anand@nortelnetworks.com | | +1 972 684 4772 | +1 972 685 3123 | GB | T1 |
| Miss Mireille PAULIAC | GEMPLUS Card International | mireille.pauliac@GEMPLUS.COM | | +33(0)442365441 | +33(0)442365792 | FR | ETSI |
| Mr. Maurice Pope | ETSI Secretariat | maurice.pope@etsi.fr | +33 (0)6 07 59 08 49 | +33 4 92 94 42 59 | +33 4 92 38 52 59 | FR | ETSI |
| Mr. Jose Puthenkulam | Intel Corporation SARL | jose.p.puthenkulam@intel.com | | +1 503 264 6121 | +1 503 264 8154 | FR | ETSI |
| Ms. Stéphanie Salgado | SchlumbergerSema | salgado@montrouge.sema.slb.com | | +33 1 46 00 75 11 | +33 1 46 00 79 70 | FR | ETSI |
| Mr. Ville Salmensuu | SSH Communications Security | ville.salmensuu@ssh.com | +358 40 569 1977 | +358 20 500 7496 | | FI | ETSI |
| Mr. Stefan Schroeder | T-MOBILE DEUTSCHLAND | STEFAN.SCHROEDER@T-MOBILE.DE | | +49 228 936 3312 | +49 228 936 3309 | DE | ETSI |
| Mr. Ramachandran Subramanian | QUALCOMM EUROPE S.A.R.L. | rsubrama@qualcomm.com | | +1 858 651 2350 | +1 858 651 2880 | US | ETSI |
| Mr. Benno Tietz | Vodafone D2 GmbH | benno.tietz@vodafone.com | | +49 211 533 2168 | +49 211 533 1649 | DE | ETSI |
| Mr. Tommi Viitanen | Nokia Telecommunications Inc. | tommi.viitanen@nokia.com | | +358405131090 | +358718074385 | FI | T1 |
| Prof. Michael Walker | VODAFONE Group Plc | mike.walker@vodafone.com | +44 77 85 277687 | +44 1635 673 886 | +44 1634 234939 | GB | ETSI |
| Ms. Monica Wifvesson | ERICSSON L.M. | monica.wifvesson@emp.ericsson.se | | +46 46 193634 | +46 46 231650 | SE | ETSI |
| Mr. Berthold Wilhelm | BMWi | berthold.wilhelm@regtp.de | | +49 681 9330 562 | +49 681 9330 725 | DE | ETSI |
| Dr. Qing Xuan | VODAFONE Group Plc | qing.xuan@vf.vodafone.co.uk | | +44(0) 1635 674781 | +44 1635 523615 | GB | ETSI |
| Mr. Yanmin Zhu | Samsung Electronics Co., Ltd | zym@samsung.co.kr | | +861068427711 | +861068481898 | KR | TTA |

41 attendees

## 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 (Now known as "3") | GB | 3GPPMEMBER | ETSI |
| Intel Corporation SARL | FR | 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 |

46 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. Porposal 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: Authenticaton 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 detration 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 co-ordination 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 Iu interface with NDS/IP mechanisms in Rel6 | Nokia | 7.2 | Discussion / Approval | | Noted. Releated CR in S3-020647 |
| S3-020647 | Proposed CR to 33.210: Securing UTRAN/GERAN IP Transport interfaces and specifically the Iu 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 pronciple - 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: Algoritms for ECSD and EGPRS (Rel-6) | Ericsson, Telia | 7.5 | Approval | | Approved |
| S3-020657 | Proposed CR to 55.216: EGPRS algoritm (Rel-6) | Ericsson, Telia | 7.5 | Approval | | Approved |
| S3-020658 | Proposed CR to 55.217: EGPRS algoritm (Rel-6) | Ericsson, Telia | 7.5 | Approval | | Approved |
| S3-020659 | Proposed CR to 55.218: EGPRS algoritm (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 agorithm |
| 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. Superceded 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 | CHRISTOFFERSSON, Per | Ph1 |
| TS | 02.09 | 4.5.1 | Security aspects | CHRISTOFFERSSON, Per | Ph2 |
| TS | 02.09 | 5.2.1 | Security aspects | CHRISTOFFERSSON, Per | R96 |
| TS | 02.09 | 6.1.1 | Security aspects | CHRISTOFFERSSON, Per | R97 |
| TS | 02.09 | 7.1.1 | Security aspects | CHRISTOFFERSSON, Per | R98 |
| TS | 02.09 | 8.0.1 | Security aspects | CHRISTOFFERSSON, Per | R99 |
| TS | 02.31 | 7.1.1 | Fraud Information Gathering System (FIGS); Service description; Stage 1 | WRIGHT, Tim | R98 |
| TS | 02.31 | 8.0.1 | Fraud Information Gathering System (FIGS); Service description; Stage 1 | WRIGHT, Tim | R99 |
| TS | 02.32 | 7.1.1 | Immediate Service Termination (IST); Service description; Stage 1 | WRIGHT, Tim | R98 |
| TS | 02.33 | 7.3.0 | Lawful Interception (LI); Stage 1 | BONNER, Brye | R98 |
| TS | 02.33 | 8.0.1 | Lawful Interception (LI); Stage 1 | BONNER, Brye | R99 |
| TS | 03.20 | 3.3.2 | Security-related Network Functions | NGUYEN NGOC, Sebastien | Ph1 |
| TS | 03.20 | 3.0.0 | Security-related Network Functions | NGUYEN NGOC, Sebastien | Ph1-EXT |
| TS | 03.20 | 4.4.1 | Security-related Network Functions | NGUYEN NGOC, Sebastien | Ph2 |
| TS | 03.20 | 5.2.1 | Security-related Network Functions | NGUYEN NGOC, Sebastien | R96 |
| TS | 03.20 | 6.1.0 | Security-related Network Functions | NGUYEN NGOC, Sebastien | R97 |
| TS | 03.20 | 7.2.0 | Security-related Network Functions | NGUYEN NGOC, Sebastien | R98 |
| TS | 03.20 | 8.1.0 | Security-related Network Functions | NGUYEN NGOC, Sebastien | R99 |
| TS | 03.31 | 7.0.0 | Fraud Information Gathering System (FIGS); Service description; Stage 2 | WRIGHT, Tim | R98 |
| TS | 03.31 | 8.0.0 | Fraud Information Gathering System (FIGS); Service description; Stage 2 | WRIGHT, Tim | R99 |
| TS | 03.33 | 7.2.0 | Lawful Interception; Stage 2 | BONNER, Brye | R98 |
| TS | 03.33 | 8.1.0 | Lawful Interception; Stage 2 | BONNER, Brye | R99 |
| TS | 03.35 | 7.0.1 | Immediate Service Termination (IST); Stage 2 | WRIGHT, Tim | R98 |
| TS | 21.133 | 3.2.0 | 3G security; Security threats and requirements | CHRISTOFFERSSON, Per | R99 |
| TS | 21.133 | 4.1.0 | 3G security; Security threats and requirements | CHRISTOFFERSSON, Per | Rel-4 |
| TS | 22.022 | 3.2.1 | Personalisation of Mobile Equipment (ME); Mobile functionality specification | NGUYEN NGOC, Sebastien | R99 |
| TS | 22.022 | 4.1.0 | Personalisation of Mobile Equipment (ME); Mobile functionality specification | NGUYEN NGOC, Sebastien | Rel-4 |
| TS | 22.022 | 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 | KOIEN, 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 | CHRISTOFFERSSON, Per | Rel-4 |
| TS | 42.031 | 4.0.0 | Fraud Information Gathering System (FIGS); Service description; Stage 1 | WRIGHT, Tim | Rel-4 |
| TS | 42.031 | 5.0.0 | Fraud Information Gathering System (FIGS); Service description; Stage 1 | WRIGHT, Tim | Rel-5 |
| TS | 42.033 | 4.0.0 | Lawful Interception; Stage 1 | BONNER, Brye | Rel-4 |
| TS | 42.033 | 5.0.0 | Lawful Interception; Stage 1 | BONNER, Brye | Rel-5 |
| TS | 43.020 | 4.0.0 | Security-related network functions | GILBERT, Henri | Rel-4 |
| TS | 43.020 | 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 | CHRISTOFFERSSON, 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 | CHRISTOFFERSSON, 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 | CHRISTOFFERSSON, 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 | CHRISTOFFERSSON, 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 Iu 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 agorithm |
| 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

| TD number | Title | Comment/Status | TO | CC |
|---|---|---|---|---|
| S3-020671 | LS (from SA WG3 LI) on change to LI subscription | Approved | **TSG SA** | |
| S3-020686 | LS to TSG SA: Introduction of a second UMTS encryption and integrity protection algorithm (UEA2 and UIA2) | Approved | **TSG SA** | **GSMA-SG, ETSI-SAGE, 3GPP2 SA4, TIA TR45-AHAG** |
| S3-020688 | Response LS to RAN WG2:Group Release security solution | Approved | **TSG RAN, RAN WG2** | |
| S3-020694 | Reply LS to SA WG2 on: "3GPP System – WLAN Interworking" | Approved | **SA WG2** | |
| S3-020696 | Reply LS to SA WG1 on Push Security | Approved | **SA WG1** | **SA WG2, T WG2** |
| S3-020697 | LS to CN WG1: Presence Security Architecture | For e-mail approval after meeting | **CN WG1** | |
| 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 | **CN WG1** | |
| S3-020704 | LS on Requirement to allow access to IMS by means of SIM | Approved. S3-020703 attached | **TSG SA, SA WG1, CN WG1, CN WG4, SA WG2, T WG3** | |

## 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 "authentication and key derivation" and ""data transfer" 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.