3GPP TSG SA WG3 Security — S3#22 **version 0.0.2**

25-28 February 2002

Bristol, UK

Source:	**Secretary 3GPP TSG-SA WG3**
Title:	**Draft Report of SA WG3 meeting #22**
Document for:	**Information**

1 Opening of the meeting

Mr. V. Niemi, SA WG3 Vice Chairman, opened the meeting as the SA WG3 Chairman was not available on the first day.

Mr. S. Ward, Orange PLC, welcomed delegates to Bristol and provided the domestic arrangements for the meeting.

Prof. M. Walker Chaired the meeting from the second day onwards.

2 Meeting objectives and approval of the agenda

TD S3-020001 Draft agenda for meeting #22.

The main objectives were to prepare the documents to next SA Plenary meeting: 33.203, 33.210 (already for info at SA#14) and MAPsec automatic Key management in 33.200.

Also joint sessions with OSA experts and another with CN WG4 experts on MAPsec. A Presentation of the GUP was also scheduled.

Progress on Rel-6 work as time allows.

The agenda was approved without change.

NOTE: Some additional agenda items were identified during the course of the meeting which are reflected in the numbering of this report.

3 Assignment of input documents

The available documents were allocated to agenda items. Three new items were added for documents in other categories: 7.8 on Presence, 7.9 on IST and 7.10 on Configurability of ciphering.

4 Reports from 3GPP SA3 meetings

4.1 SA3#21, 27-30 November 2001, Sophia Antipolis, France

TD S3-020002 Draft Report of SA WG3 meeting #21. The report was considered for final comments and approval. Concerning the request for a replacement for the Chairmanship of the LI Group, B. Wilhelm reported that the LI group had now found a new Chairperson.

The decision on the mandatory merged Zb/Zc interface was reported as erroneous - the implementation of this interface was agreed as optional. The draft report was updated to reflect this change.

The report was then approved with these changes and the approved version 1.0.0 will be placed on the FTP server.

Actions from the meeting:

AP 21/1: *Colin Blanchard to contact the editor of the GUP draft to determine the background and the rationale for the requirements in the security section (section 6).*
Completed (GUP security requirements used standard requirements, SA WG3 should decide whether they are appropriate).

AP 21/2: *Stuart Ward to invite Paul Amery to give SA WG3 a briefing on GUP work.*
Completed (GUP presentation at this meeting)

AP 21/3: *P. Howard to set up an e-mail discussion on this in order to produce a proposal for a CR to 29.198 for CN WG5.*
Superseded by Joint session with CN WG5 at this meeting.

AP 21/4: *Stuart Ward to start off an e-mail discussion on Location Services Privacy and report back to SA WG3 meeting #22.*
The action was reviewed (using S3#21 TD S3-010575). The Chairman suggested that a drafting session should be set up in order to review the draft TSs on Location Services privacy. Stefan agreed to chair a drafting session. More recent versions of the TSs were provided in TD S3-020113 and TD S3-020114. A response LS was provided in TD S3-020142.

AP 21/5: *A. Escott agreed to check the draft TS 22.146 and determine if any input is needed and report back to the next SA WG3 meeting.*
A Escott agreed to provide a more recent draft of TS 22.146 after the meeting for review.

AP 21/6: *G. Rose to evaluate the EAP/SIM authentication technique to determine it's validity for increased authentication strength.*
No security problems have been found, but some comments will be provided by G. Rose to the group for discussion.

AP 22/1: Greg Rose to provide the comments to SA WG3. This was completed during the meeting (see TD S3-020125).

AP 21/7: *D. Castellanos to set up an e-mail discussion on Presence service, with support from Nokia, Telenor and Vodafone.*
This was completed with contribution TD S3-020096.

TD S3-020142 Reply LS on "Enhanced user privacy for location services". This was introduced by T-Mobil, TD S3-020113 and TD S3-020114 were used as a basis for this LS. The LS was modified and provided in TD S3-020145 which was approved.

4.2 SA3#21bis, 31 January – 1 February 2001, Antwerp. Belgium

TD S3-020003 Draft Report of MAPSEC and NDS/IP ad-hoc (Rel-5) January 2002 - v0.0.1rm. The report from the MAPsec ad-hoc meeting was reviewed. The report was approved and updated to v1.0.0 on the ftp server. Document S3z020038 was re-provided in TD S3-020115 and reviewed. SA WG3 confirmed this reply LS to CN WG4.

On item 5.4 (Rel-5 MAPsec changes) a CR a cover sheet had been prepared by A. Escott in order to explain why a single CR was used for the Rel-5 update for clarification at the TSG SA Plenary.

On item 5.5 (MAPsec DoI) Ericsson had provided a contribution on this (TD S3-020098). For other technical issues, Nokia had provided a contribution for the joint session with CN WG4 (TD S3-020081).

A modification was made to the text of 6.2 to clarify that the work needed was out of the scope of the specification.

On 6.4 (Zb/Zc merging) contribution had been requested at this meeting, but no contributions were available. It was agreed that this issue should be included in the agenda under 7.4 and S3z020025 was copied to this meeting as TD S3-020116.

Geir Koien reported that a reference needed updating and he would do this off-line.

The report was then approved and the updated version 1.0.0 placed on the FTP server after the meeting.

TD S3-020004 . Draft Report of aSIP ad-hoc (Rel-5) January 2002 - v.0.0.1. It was noticed that S3z020026 had been mis-reported in the title of the contribution, and this was corrected to S3-020026. it was reported that S3z020014 had been handled via e-mail after the meeting.

K. Boman agreed to provide an updated version of S3z020032 in TD S3-020117.

Unprotected re-registration e-mail discussion had not occurred, however there were input contributions to the meeting in TD S3-020091 and TD S3-020106.

The decision on moving the SIP security into the main body of 33.203 was deferred to this SA WG3 meeting.

S3z020017 had been updated by Ericsson and contributed to this meeting in TD S3-020092, which also covered the updated requirements of the authors of S3z020029.

The conclusion from the ad-hoc (see S3z020019) that SIP signalling between UE and P-CSCF is not needed for Rel-5 would need confirmation at this SA WG3 meeting.

ISIM: TD S3-020042 was to be considered by SA WG3 at this meeting.

S3z020004: There were no contributions on this but it was requested that some decision be made at this meeting.

S3z020006 - Postponed to this meeting: This had been superseded by TD S3-020109 and TD S3-020110.

S3z020027 - Postponed to this meeting: Re-provided in TD S3-020118.

TD S3-020005 Extract of Draft SA WG3 part of Report for TSG SA meeting #14 - version 0.0.4.

The Configurability and visibility CR in SP-010760 (Ciphering) had been sent back to SA WG3 for further discussion. This was provided in TD S3-020119 for discussion under new Agenda Item 7.10.

Support for subscriber certificates: SA WG1 were asked to provide information to SA WG3 - this was provided in TD S3-020120 for discussion under new Agenda Item 7.4.

It was noted that the request from the SA Plenary for provision of separate independent CRs for Rel-5 MAPsec would not be done by SA WG3 as the complete set of changes were dependent upon each other and all changes would be required in order to provide the complete automatic Key Management system.

The updated report was approved and will be put on the FTP server as version 1.0.0.

4.3 3GPP SA3 Lawful interception sub-group

TD S3-020068 Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #1/02 on lawful interception. The report was introduced by B Wilhelm. The election of Brye Bonner as Chairperson was approved by SA WG3.

TD S3-020048 LS from LI group: VASP MMS Connectivity. This was a SA WG3 LS to the LI group (TD S3-010571). This LS was noted and the LI group were asked to send such LSs directly to the affected groups, if SA WG3 advice is not needed on the issues.

TD S3-020049 Proposed LS to SA WG1/SA WG2: Reply to LS on “Privacy Override Indicator”. This was updated to include the contact person and provided in TD S3-020128 which was agreed for transmission.

TD S3-020050 Proposed LS to ETSI TC SEC on WI IP Interception. This was agreed for transmission

TD S3-020051 Proposed LS to ETSI TC SEC WG LI on a new ASN.1 branch for 3GPP. This was agreed for transmission.

TD S3-020052 Proposed LS to ETSI TC SEC WG LI on the handling of ASN.1 parameters for LI. This was provided to SA WG3 for information and was noted.

TD S3-020053 Proposed [DRAFT] Response to email “NP-010710: AMR-WB TSs from SA4”. This was updated to remove "[DRAFT]" and provided in TD S3-020129 which was approved.

TD S3-020054 LS from LI group: MM7 working assumptions. This reported that the LS forwarded by SA WG3 on this had not yet been dealt with in the SA WG3-LI group. The LS was then noted.

TD S3-020069 Proposed CR to 33.107: PDP context Deactivation cause (Rel-5). This CR was approved.

TD S3-020070, TD S3-020071. These two CRs were merged into a single CR in TD S3-020130 which was approved.

TD S3-020072 Proposed CR to 33.107: The use of H.248 in setting up a bearer intercept point at the MGW (Rel-5). This CR was approved.

TD S3-020073 Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-99). The suitability of this change for Rel-99 was considered. There was no objection to this and the CR was approved.

TD S3-020074 Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-4). This CR was approved.

TD S3-020075 Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-5). This CR was approved.

TD S3-020076 Revised Work Item Description (revision of SP-000309): Rel-5 LI HO interface. The work "Pack" was updated to "Packet" and the WID provided in TD S3-020131 which was approved.

TD S3-020100 3GPP TS 33.108: Handover Interface for Lawful Intercept (Release 5) - Version 0.7.3. This was provided for approval. It was noted that sections 5 (CS) and 7 (IMS) were still for further study. It was considered that this would be unlikely to be completed for June 2002 and a covering note should be added to explain that this includes PS domain requirements, but not CS or IMS domains (although the CS requirements were expected to be fairly strait-forward to include by June 2002). The inclusion of Annex G was questioned, and it was considered that TSG SA should be consulted on the inclusion of US-specific information in the 3GPP version of the TS. The draft was therefore approved for presentation to TSG SA#15 for information **with indications about the missing functionality and Regional Annex G, asking TSG SA for advice on how to deal with these issue.**

5 Reports and liaisons from other groups

5.1 3GPP SA plenary

There were no contributions under this agenda item.

5.2 3GPP working groups

IMS security:

TD S3-020007 Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem. This was provided for information and had been noted at the ad-hoc meeting. The LS was then noted.

TD S3-020018 LS on IMS identifiers and ISIM and USIM. The proposal for a workshop had been rejected at SA#14. The LS was therefore noted.

TD S3-020038 IMS Security requirements. This was introduced by Nortel Networks and reports that SA WG1 sees no issues with having the CS and PS domain call control and MM procedures residing in the MT, and therefore all associated security procedures can terminate at the MT. For IMS, SA WG1 sees the need for the user to have integrated TE and MT, based on open OS, where malicious software could be loaded which impacts the operation of the IMS procedures. SA WG1 would like procedures in place for Release 5 timeframe for backwards compatibility when such terminals are standardised for Release 6. The Liaison also answers questions posed by SA WG3 regarding IMS and provided plans for SA WG3 work on UE functional split - seeing no need to modify security procedures in 33.102 for CS and PS domains; to ensure that the network is secure against attacks from software IMS clients; to add a section "security for the local interface between TE and MT in UE functional Split scenarios; Other work for UE Functional Split is considered unfeasible for Rel-5.

SA WG1 asked SA WG3 to address the security concerns arising from potentially malicious software IMS clients independently of whether the client exists in the TE or MT, or an integrated UE. SA WG3 were asked to provide requirements to SA WG2 and CN WG1 on these matters.

It was noted that the May meeting of SA WG1 was co-located with SA WG3 in Victoria, Canada and a joint session could be sought.

It was agreed to respond to SA WG1 outlining the problems with the approach, the problems with producing adequate mechanisms for Rel-5 but that the issues will be studied in order to see what can be achieved for Rel-5 and Rel-6 time frames. Siemens provided this LS in TD S3-020133 which was reviewed and updated in TD S3-020166 which was approved.

It was also suggested that the Security for the TE - MT interface should be included in 33.102, in a general way, independent of IMS. It was considered that this should be considered for review during the joint session with SA WG1.

TD S3-020041 Liaison Statement on UE functionality split. This was copied to SA WG3 for information and was noted. SA WG3 recognise that this confirms the view of SA WG3 that the situation is volatile at the moment.

TD S3-020042 Liaison Statement on ISIM for support of IMS. This was considered at the ad-hoc meeting and a reply provided in TD S3-020033 which was dealt with under agenda item 7.3.

TD S3-020059 Liaison Statement on Access to IMS Services using 3GPP Release 1999 and Rel-4 UICCs. SA WG1 asked SA WG3 to confirm that the access independent requirement (e.g. non-IMS-aware UICCs can gain access to IMS services) can be fulfilled without degrading the security of the 3GPP system. Vodafone had provided a contribution (TD S3-020109) on backward compatibility issues which could fulfil the requirements, if agreed in SA WG3. A response from SA WG2 was also provided in TD S3-020127 which was also considered. The information was utilised in the update of TS 33.200.

TD S3-020127 LS from SA WG2: LS on Stage 2 for use of USIMs and ISIMs for IMS. A CR was attached which proposed that Rel-5 IMS-aware UICCs should have an ISIM application. SA WG3 were asked to advise other WGs if they see any security problems with this approach. It was decided to consider this after dealing with TD S3-020109. The information was utilised in the update of TS 33.200.

TD S3-020060 Liaison Statement on ISIM for support of IMS. There was no action provided to SA WG3 and the LS was noted.

S3-020026 LS S5-020003 (S1-011241) Packet Switched Streaming Service. This was a reply from SA WG5 to SA WG1 laision contained in TD S3-020015 and was noted.

OSA:

TD S3-020014 Liaison Statement on Confirmation of OSA Support for VASP MMS Connectivity. This was copied to SA WG3 for information and was noted.

TD S3-020043 LS reply to: " Liaison Statement on Confirmation of OSA Support for VASP MMS Connectivity." This was copied to SA WG3 for information and was noted.

Generic User Profile:

MAPsec:

TD S3-020008 DRAFT LS on MAPsec error handling (response to S3z010121). This was dealt with and responded to in the ad-hoc meeting and so was noted.

TD S3-020016 Liaison statement on Protocol Specification of the Ze-interface. This LS suggested, and was covered by the joint session held at this meeting and was therefore noted.

User Equipment Management:

TD S3-020039 Liaison Statement on User Equipment Management Feasibility Study (SA5's TR 32.802). (Update of TD S3-020025 / TD S3-020032 with a later version of the attached TR). SA WG5 requested confirmation of the user management security of the TR 32.802 (section 8) and the overall security-related aspects of the TR. Section 6.3.4 appeared to be outside of standardisation scope, and was a manufacturers issue. Some concerns were raised which were collected together in a LS provided in TD S3-020136 which was approved.

Streaming:

TD S3-020015 Liaison Statement on Draft stage 1 TS for Packet Switched Streaming Service. This LS had been replied to by SA WG5 in TD S3-020026 and was noted.

TD S3-02026 LS S5-020003 (S1-011241) Packet Switched Streaming Service. This was provided for information and was noted.

TD S3-020061 Liaison Statement on Packet switched streaming service stage 1 TS for release 5. The attached TS was missing, and therefore no comments could be made. The LS was noted.

TD S3-020019 Reply to "Liaison Statement on Extended Streaming Service". This was provided for information and was noted.

Push:

TD S3-020027 LS reply on: “Draft Push Service Stage 1”. SA WG3 noted that the charging work had started. The LS was noted.

TD S3-020057 LS reply on ” Response to: Liaison Statement on Revised Push Service Stage 1”. The attachment was actually provided in TD S3-020058. This was introduced by Vodafone and asked WGs to review their draft TS 22.174 and provide comments. Peter Howard agreed to review this and collect comments from others and provide them to the next meeting.

TD S3-020087 LS reply on: “Draft Push Service Stage 1”. This was provided by SA WG2 for information and was noted.

RAN:

TD S3-020009 LS on Removal of Tr mode DCCH. This was introduced by Nokia and reports that RAN have removed the "TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)" has been removed from Release 1999 (but not Rel-4). SA WG3 were asked to remove this from the protection list. They also ask SA WG3 if the list could be moved from 33.102, replacing it with a reference to 25.331. This request was not considered the best way forward as SA WG3 are responsible for maintaining the list of Protected messages. Nokia agreed to respond to the LS in TD S3-020154 which was approved. A corresponding CR was provided in TD S3-020155 which was approved. Note: ME and RAN are affected and should be crossed for the presentation to TSG SA.

TD S3-020017 LS on HFN initialisation at CN domain switch for SRBs. This had already been dealt with in RAN WG2 and was therefore noted.

GERAN:

TD S3-020028 Liaison Statement on Count Input to Ciphering Algorithm. This was introduced by Nokia and suggests using a combination of the HFN and TDMA FN for the 28-bit Count Input, and some rules for the working of this scheme. SA WG3 did not see a problem identified in the contribution with sending a repeated message in a different cipher stream, as it is the opposite that would be a problem. Nokia agreed to provide a reply LS confirming the use of HFN and TDMA FN in the way suggested in TD S3-020156 which was approved.

Others:

TD S3-020139 Response to LS (S3z020043) on START value calculation and Additional principles adopted by TSG-RAN WG2. This was presented by Nokia. RAN WG2 reported that the HFN part of the Count-C may be unavoidably re-used on Inter-RAT handover (Item 6). This was considered as a necessary and of low consequence, for Release 1999. A response LS to RAN WG2 was provided in TD S3-020149 which was approved.

TD S3-020011 LS from SA WG5 to T2 (S5-010703_T2-010903) on VASP MMS connectivity. This LS was provided for information and was noted.

TD S3-020012 Liaison Statement from SA WG5: “Reply to LS on Presence Service”. This LS was provided for information and was noted.

TD S3-020013 Liaison Statement from T WG2: Reply to SyncML with Follow-Up Questions. This LS was provided for information and was noted. Delegates were encouraged to review the work and provide any concerns to the next meeting.

TD S3-020022 Liaison Statement from SA WG2 on " IP version interworking on the transport plane". This was introduced by Ericsson and asked SA WG3 to review the implications on LI specifications. The LI group were asked to take this document into their next meeting.

TD S3-020023 Liaison Statement from SA WG5 on Impacts of Subscriber and Equipment Trace. Document TD S3-020056 on the same subject was considered to determine if there was any impact

from this LS. The reply LS to TD S3-020056 provided in TD S3-020157 was copied to SA WG5 for information.

TD S3-020056 Response Liaison Statement from CN WG4 on Trace and Availability of IMSI and IMEI. CN WG4 asked SA WG3 if there were any security implications on spreading IMSI/IMEI information over signalling interfaces for tracing functionality. SA WG3 considered that the channels that the IMSI/IMEI would be transmitted over are protected and therefore cause no security concerns. A response LS was provided in TD S3-020157 which was approved.

TD S3-020031 Liaison Statement from SA WG2 on "Prefix allocation for IPv6 stateless address autoconfiguration". This was introduced by Ericsson. The LI group was asked to consider this LS at their next meeting. SA WG3 members were asked to review this and provide comments on issues to C. Brookson, who agreed to collect comments together for the next meeting.

TD S3-020036 Liaison Statement from CN WG4 on Lawful Interception For OoBTC. This was introduced by Ericsson. The LI group was asked to consider this LS at their next meeting. The LS was then noted.

TD S3-020037 Liaison Statement on AMR-WB and Lawful Interception. TSG CN and CN WG4 were added as CC: to TD S3-020129.

TD S3-020047 Liaison Statement on Lawful Intercept related information in CN WG5 specifications. The LI group was asked to consider this LS at their next meeting. The LS was then noted.

TD S3-020083 Liaison Statement from SA WG1 on Digital Rights Management (DRM). This was introduced by Nokia and asks SA WG3 to review the attached DRM draft. The ownership of the stage 2 of this WI was discussed and the Chairman undertook to raise this at the TSG SA Plenary. Nokia agreed to take inputs from delegates and provide a WID for the next meeting.

AP 22/2: Chairman to raise ownership of DRM Stage 2 at TSG SA #15.

TD S3-020084 LS from SA WG1on Priority Service Feasibility Study TR - draft. The security implications of this service needed study. Delegates were asked to review and send comments on security requirements to L. Valerius, who agreed to collect them together for the next SA WG3 meeting.

TD S3-020085 LS on 3GPP System – WLAN interworking. This LS was provided for information and was noted. SA WG3 delegates were asked to review the security implications in the attached TS and send comments to S. Schroeder, who agreed to collect them together for the next meeting. G. Koien agreed to contact the contact point and invite him to the Helsinki meeting to present the draft to SA WG3.

TD S3-020086 Liaison Statement from T WG2 on MM7 Security Mechanisms for Release 5. SA WG3 were asked to review the draft authentication draft for VASP. A quick review revealed the use of the basic authentication scheme, which is a cleartext password system. SA WG3 delegates were asked to review the attached TS and send comments to G. Rose, who agreed to collect them together for the next meeting. The Chairman undertook to report the security analysis being carried out by SA WG3 to the TSG SA meeting.

AP 22/3: Chairman to report the ongoing Security Analysis on MM7 Rel-5 to TSG SA #15.

TD S3-020140 3GPP requirements draft. This was provided by Ericsson for information and was noted.

5.3 IETF co-ordination

TD S3-020045 Correspondence from S Hayes (TSG CN Chairman): Results from recent IETF coordination meeting. This was provided for information and reported the overall progress in IETF for meeting 3GPP delivery dates, mechanisms for providing 3GPP-specific headers and concerns regarding interoperability. Bundles 1 and 2 of RFCs are defined for IETF delivery, but the contents of a third bundle, for June 2002, this will probably include security IETF dependent deliverables, but the content is still under discussion. The need to implement SIP over TLS - item (i) - caused some concern for interoperability and it was decided to respond to the TSG CN Chairman, questioning the need for this and requesting the mandating of TLS to be removed from the specification, as it is very unlikely to be implemented, for commercial reasons. **The SA WG3 Chairman agreed to put the feelings of the group to the TSG CN Chairman (3GPP representative to the IETF group) and report the conversation back to SA WG3.**

AP 22/4: The SA WG3 Chairman agreed to put the feelings of the group concerning mandated support of TLS to the TSG CN Chairman (3GPP representative to the IETF group) and report the conversation back to SA WG3.

It was reported that CN WG1 had rejected item (a) - loose routing - for security reasons and the possibility that the mobile could bypass the network.

5.4 Others (e.g. ETSI SAGE, ETSI MSG, GSMA, TIA TR-45)

GSMA:

TD S3-020088 JOINT NEWS RELEASE: ETSI and ECBS co-operate in the Development of Standards for the Security of Telecommunications and M-Commerce. This was provided by the SA WG3 Secretary for information and was noted.

Charles Brookson provided a verbal report of the developments within the GSMA Security Group. IMEI Security was a big issue due to the rising rate of stolen handsets and the GSMA had found that their requirements for inability to change the IMEI (since July 2001) were not fully conformant from a number of manufacturers. Operators have signed a letter to Manufacturers from the GSMA on this matter.

ETSI SAGE:

Per Christofferssen provided a verbal report of the developments within SAGE. SAGE started work early February on A5/3. The design authority is ETSI MCC. The requirements specification had been updated and completed. The basis will be KASUMI and it has been decided to base the work on f8 (in 4 different modes), which should ease implementations in handsets for both 2G and 3G. No external evaluation has been considered necessary as KASUMI has already been scrutinised. Expected delivery is May - June 2002.

TIA TR-45:

Greg Rose provided a verbal report on the AHAG developments. Much work is being moved to 3GPP2 S-WG4 (Security Group). Regarding the Joint Control document, it was decided not to change this and therefore the Joint Control agreement does not need to be revised. AHAG and S-WG4 will communicate between them and AHAG will act as a channel back to TIA. Liaison between 3GPP2 S-WG4 and 3GPP SA WG3 is being discussed and a suitable liaison person will be chosen.

6 Maintenance of Rel-4 specifications and earlier

6.1 TS 33.200, MAP security

This was dealt with under agenda item 7.5.

7 Technical issues

7.1 Generic user profile (Monday afternoon at 13:00)

TD S3-020121 Presentation: The 3GPP Generic User Profile (GUP). This was presented by Paul Amery (Orange) and provided an overview of the GUP proposals and advantages of providing GUP. The security aspects, particularly the trust model, would need some analysis in SA WG3. Mr Amery was thanked for his presentation. TD S3-020122, TD S3-020123 and TD S3-020124 were provided for further information and delegates were asked to consider these outside the meeting. These documents were then noted.

TD S3-020020 Status of the Generic User Profile Work. This was provided by the 3GPP Joint ad-hoc on Generic User Profile (GUP) and was introduced by Motorola. It was noted that the stage 2 and stage 3 documents attached to the LS had been updated since the LS was produced. **The latest versions should be reviewed by SA WG3 delegates and any comments should be sent to SA WG1, SA WG2, T WG2 and/or the GUP Joint ad-hoc group, as appropriate**.

TD S3-020021 Release of In-Process Stage 1 Specification to SA1 for Review and Continuing Development. This was provided by the 3GPP Joint ad-hoc on Generic User Profile (GUP) for information and was noted.

TD S3-020024 Comments on UP-010141 and relationship of GUP to Subscription Management. This was provided by SA WG5 for information. Delegates were encouraged to keep these SA WG5 comments into account for 33.140. The document was then noted.

TD S3-020040 Comments on UP-010141 and relationship of GUP to Subscription Management. This was provided by SA WG5 for information. Delegates were encouraged to keep these SA WG5 comments into account for 33.140. The document was then noted.

TD S3-020055 Liaison Statement on coordination of data definitions, identified in GUP development. This was provided by T WG2 and asked TSG SA to endorse the proposal for a single group to be responsible for coordination of Data Descriptions. It was noted that the April meeting of T WG2 was now a T WG2/GUP meeting. No particular security problems were identified with the request to keep all the Data Definition work in a single place, as SA WG3 would only be interested in the actual mechanism and content of messages, particularly those containing security-related parameters.

A review session was set up to provide initial comments on the Stage 1 GUP, and S. Ward agreed to organise an e-mail discussion on this and provide comments to the next meeting.

7.2 OSA including joint session with CN5 experts

TD S3-020126 Parlay/OSA: an open API for service development. This was presented by C. Abarca on behalf of the Joint API Group (made up from ETSI, 3GPP and Parlay). Load control mechanisms were questioned, in particular for SIP. It was responded that the API may be modified to take SIP needs into account, but that there would not be a SIP-specific API created by the group.

TD S3-020102 Encryption of challenge in CHAP-based OSA authentication. This was introduced by Alcatel and discussed a specific functionality in 29.198-3 v4.2.0, which makes the challenge used for CHAP-based authentication to be encrypted when passed from the verifier to the claimant. There was some discussion on the need for encryption, and it was generally considered unnecessary for this. Delegates were asked to check this against a threat analysis and report any foreseen problems. The contribution was then noted.

TD S3-020104 Use of one-way hash function for CHAP in OSA. This was introduced by Alcatel and identified an issue in TS 29.198-3 v4.2.0 with regards to the one-way hash function (MD5) to be used to realize CHAP-based authentication. It was reported that the use of RFC 1994 would need to be specified, as it only specifies a packet-based system, which will need further clarification on the content of the packets for 3GPP. Alcatel's proposed solution for Issue #2 was provided in TD S3-020101.

TD S3-020101 Authentication Scheme Negotiation in OSA. This was introduced by Alcatel and discussed the mechanism defined in TS 29.198-3 v4.2.0 to negotiate the authentication scheme used between the client application and the framework/services. It was pointed out that the original "proscribe" mechanism was consciously designed to allow the framework to dictate the security level applied, and no negotiation was needed. CN WG5 would be reluctant to remove mechanisms from the list, but could accept that mechanisms which are already included are left in for backwards

compatibility (of the compiled coding and libraries), even if they are not used. No preference for either of the two solutions was made from the security point of view (except that a solution was strongly requested) and CN WG5 would be asked to consider the issue and choose a solution.

TD S3-020103 Security of terminateAccess() function in OSA. This was introduced by Alcatel and identified various issues in TS 29.198-3 v4.2.0 with regards to the security mechanism used to protect the terminateAccess() function.

It was generally recognised that these issues were real security issues and that the proposed solutions were sensible. Alcatel agreed to produce some CRs to cover the issues and send them to the SA WG3 e-mail list for further comments.

AP 22/5: O Paradaens to create CRs for OSA security issues and distribute to SA WG3 e-mail list for comment.

TD S3-020044 Liaison Statement on Support of security algorithms in OSA framework (response to S3-010696). This proposed a joint session, which was included in this meeting. The LS was therefore noted.

The joint session was then closed and the Chairman thanked the CN WG5 experts for coming to the meeting.

7.3 IP multimedia subsystem security

TD S3-020117 aSIP-Access Security for IP-Based Services. This was presented by K. Boman (Ericsson) and described the work that was needed at this meeting to achieve completion of 33.203 in order to present it for approval at SA#15. It proposed an evening drafting group during this meeting and a timescale for finalisation over e-mail for final version available 7 March 2002 (i.e before start of SA#15).

TD S3-020089 HTTP AKA Internet Draft. This was introduced by Nokia and presented that latest submitted version of the HTTP AKA Internet Draft. This showed that it is very straight-forward to use HTTP Digest for AKA. It was clarified that the draft will be presented to the next IETF meeting 17-22 **March** 2002, fast approval was expected as this is an update to an existing IETF mechanism. The handling of integrity protection of critical messages in headers was questioned. It was explained that this was a solution for running AKA in SIP, and addition of integrity protection would need to be added to this for 3GPP use. **It was agreed that this would need to be verified for adequate security and delegates were asked to consider this and make contribution to a technical discussion.**

TD S3-020095 New and updated SIP drafts. This was provided for information and introduced by Ericsson. It was noted that the attachments were erroneous, so the document was resubmitted with the correct attachments in TD S3-020134 which was noted.

TD S3-020067 SIP Message Integrity Protection Work in the IETF. This was introduced by Nortel Networks and provided a general introduction to the proposed mechanisms for SIP message integrity protection. There was some clarification requested over the use of AKA as an algorithm for auth-algorithms (section 6.1) whereas it is a procedure. Nortel Networks was asked to try to clarify this to the SA WG3 delegates. The contribution was then noted.

TD S3-020093 A security framework for IMS utilising HTTP Digest. This was introduced by Ericsson and proposed a framework based on HTTP Digest for Authentication of IMS subscriber, Bidding Down protection and SIP signalling protection between UE and P-CSCF. The contribution concludes with a proposal that SA WG3 adopt the framework as a working assumption. It also asks SA WG3 to consider whether the choosing of the algorithm (from a list provided by the P-CSCF) by the UE is acceptable. Under the assumption that the HTTP Digest is the way forward as a security framework for IMS (this is still to be discussed, due to potential issues on HTTP Digest for AKA) then the principles of the contribution were accepted, pending further investigation and discussion.

TD S3-020094 On integrity protecting SIP-signalling in IMS. This had been contributed to the ad-hoc meeting, but was postponed to this meeting. Ericsson introduced the document which reports that the IETF are fulfilling milestones to provide SIP signalling with integrity protection in a time frame fitting in with Rel-5 and that SIP level protection is more optimal solution than the proposed IPSec solution. It proposed that SIP solution be taken as a working assumption in SA WG3 and it is moved from Annex C into the main body of 33.203.

Siemens commented that there was still an equal case for IPSec as the solution and may also be available in time for Rel-5 (assuming June 2002) and this provided also confidentiality, not yet done in

SIP. Ericsson reported that solutions are being drafted currently in the IETF, and that there would also be issues in negotiating port numbers for IPSec with the IETF.

TD S3-020108 Uniqueness of IP address/port number checking in the P-CSCF. This was introduced by Nokia and discusses the need for uniqueness of IP Addresses and ports for an IPsec solution. It was clarified that this analysis contribution did not impact the selection between SIP level and IPsec solutions. It was clarified that the solution would require an extra database in the P-CSCF. The proposals in this contribution were taken into account in the editing session.

The SA WG3 Chairman suggested the following: There are two potential solutions:

A = IPsec solution

B = HTTP Digest solution

Option 1: Choose between A) and B).

Option 2: Promote either A) or B) to a Working Assumption and retain other in the Annex until outstanding issues are clearer.

Both solutions require more work, and both rely upon the IETF. A show of hands showed a strong majority in favour of Option 2. It was also agreed that the choice between A) and B) was not a security issue as such as both can meet the security requirements. (Architectural considerations may show a difference in constraint). Other considerations were then explored, and general perceptions in the meeting, as presented in the table below:

	IPsec Solution	**HTTP Digest solution**
Covers Security requirements	Yes	Yes
Architectural Constraint	Higher Constraining	Lower Constraining
Complexity for Confidentiality	Less Complex	More Complex
IETF involvement	Equal dependency	Equal dependency
Maturity of solution	Equal maturity	Equal maturity
S3 Resources to develop back-up (Annex) solution if X chosen	High resource to develop HTTP Digest	Lower resource to develop IPsec Solution (in IETF)
S3 Resources to develop solution	Lower resource to develop IPsec Solution (in IETF)	High resource to develop HTTP Digest
Overall Favour/company as X chosen, other in Annex	8	7

There were 12 abstentions - informal show of hands voting - 1 vote / Company.

Due to the closeness of the indications received, it was decided to leave both solutions in Annex C until more stability of a solution can be determined. The SA WG3 Chairman undertook to present this situation to TSG SA#15.

AP 22/6: SA WG3 Chairman to present reasons for keeping both SIP level and HTTP Digest solutions in Annex C of 33.203 until the IETF work is more stable and a clear choice can be made.

TD S3-020091 Unprotected REGISTER messages. This was introduced by Ericsson and extends the discussion held in the ad-hoc meeting on unprotected re-registration for when the UE is moving out of and back into radio coverage (or power-off, power-on of the UE). It proposed some text for update of TS 33.203 to cover their solution. The indication of non-integrity protected register message sent to the S-CSCF was questioned. It was explained that CN WG1 had requested this possibility as a home network option and the associated IE was already to be included in CN WG1 specifications. A further proposal was provided by Nokia in TD S3-020106, the relevant part of which was then considered:

TD S3-020106 Unprotected registrations during SA lifetime. This was introduced by Nokia and discussed whether the network should accept the unprotected re-registration messages sent from a registered UE. It was proposed to combine the relevant parts of these changes with those of the Ericsson proposal in TD S3-020091 and the updated text was provided in TD S3-020137 which was agreed in the drafting group to be included in TS 33.203.

For section 2.2.2: This describes a potential attack for DoS from a malicious sending of bad RES to the P-CSCF. It was commented that an integrity failed response would be rejected and not sent to the

S-CSCF. It was concluded that this did not constitute a security problem to which a solution was offered.

For section 2.2.3: This discussed network-initiated re-authentication. This suggests investigation of the setting of the user to un-registered in the case that the user fails to be authenticated. It was commented that this should be already covered in Rel-5. A further contribution on this was provided by Siemens in TD S3-020132.

TD S3-020107 SA handling and use. This was introduced by Hutchison 3G and proposed revised text to 33.203 for the handling of SAs and some new text on the use of SAs. The attached CR proposal was withdrawn for further consideration and TD S3-020132 was considered which had been written taking this contribution into account. This would be used in the evening editing session.

TD S3-020132 Security association management in the UE and the P-CSCF. This was written taking into consideration TD S3-020092, TD S3-020107and TD S3-020106. *(Note that the reference to TD S3-020091 should have read TD S3-020106 in this contribution)*. The principles of this contribution were accepted and the detailed text considered in the evening editing session.

TD S3-020092 Requirements and a proposed solution for SA_ID. This was introduced by Ericsson and included for detailed discussion in the evening editing session.

TD S3-020090 On P-CSCF behaviour at Integrity check failures. This was introduced by Ericsson and aimed to clarify the behaviour of the P-SCSF when the integrity check fails in SM7 during the registration/authentication procedure. Ericsson asked SA WG3 to evaluate the impacts of the working assumption made at the ad-hoc meeting and to ensure that this is the desire behaviour. SA WG3 preferred to leave the working assumption in order that any problems with it could be determined during elaboration of the work based upon it. The text of this contribution was included in the evening editing session.

TD S3-020082 Updates to SIP-Level Solution for IMS Integrity Protection. This was introduced by Nortel Networks and proposed changes to Annex C, section C.2 of 33.203 in order to reflect recent IETF work on HTTP Digest. This was included for detailed discussion in the evening editing session.

TD S3-020109, TD S3-020110 and TD S3-020147 were contributed directly to the evening editing session.

Report of drafting meeting:

K. Boman reported that the meeting considered TDs S3-020078, 82, 92, 107, S3-020110, and 132. There was not time to consider the changes proposed in TD 108.

The Editor agreed to produce a new version incorporating agreements during this meeting.

TD S3-020109 Proposed changes to 33.203 v1.1.0 regarding ISIM. This was introduced by Vodafone and proposed ISIM-related changes to 33.203. The use of "the UICC" should be changed to "a UICC". Other editorial changes were suggested. It was agreed that the descriptive parts (parts of section 8) would be moved to an informative Annex. After some discussion, P. Howard agreed to update the proposal with comments and it was agreed to include this in section 8 and an informative annex of 33.203.

TD S3-020125 Comments on draft EAP/SIM. This was introduced by Qualcomm and provides a report of an analysis of "draft-haverinen-pppext-eap-sim-02.txt". In summary, The mechanism as proposed appears adequately secure for the purposes described, none of the comments below are expected to be a problem in practice. V. Niemi thanked Qualcomm for this analysis and undertook to inform the editing group for the draft. The document was noted.

TD S3-020135 Problem with use of RES in Digest-AKA. This was introduced by Qualcomm. It suggested that the use of RES, with its reduced entropy, as the “password” for HTTP-Digest introduces a “choke point” in the computation of the various digests. The contribution described an attack based on this, and proposed a modification to "draft-niemi-sipping-digest-aka-00.txt" which should address the problem, using IK for the function. There was some discussion on this, Siemens commented that they would prefer that a new mechanism was provided, rather than re-using keys intended for other uses. Qualcomm was asked to take this again and provide proposed updates to the RFC drafts, for consideration in SA WG3.

TD S3-020138 Reply Liaison from CN WG1 Statement on Registrations without user authentication and Identity Spoofing. A. Escott agreed to provide a response to this LS when TS 33.200 is approved to attach to it, which was allocated TD S3-020160, which was approved in principle, to be circulated by e-mail.

TD S3-020158 33.203 version 1.2.0. This was provided by the editor and is **to be reviewed by correspondence for comments by 6 March 2002. Approved version for TSG SA presentation on 7 March 2002**.

TD S3-020161 LS to CN WG1 on SA handling. This will be drafted by A Escott for e-mail approval.

TD S3-020099 Security Mechanism Agreement for SIP Connections. This was provided by Ericsson for information and was noted.

TD S3-020033 LS response to SA WG2: The use of USIMs and ISIMs for IMS. This was introduced by Vodafone and had been developed after discussion at the ad-hoc meeting of a number of LSs from various WGs. It was suggested that this LS should not be approved until 33.203 is approved and can be attached to the LS. Some discussion on the derivation of IMPU from the IMSI took place, and it was decided to continue the debate via e-mail. P. Howard agreed to organise an e-mail correspondence on this. The final document for the resulting LS was allocated as TD S3-020167.

7.4 Network domain security: IP network layer (NDS/IP)

TD S3-020006 Draft 33.210 version 0.8.0 (provided to email list for comment 05/12/2002). This was a previous version of the document and was noted.

TD S3-020034 Update information –TS 33.210 (and 33.210 v110). This was the updated version following the Antwerp ad-hoc meeting and was noted.

TD S3-020080 Proposed Changes to 33.210 about the ISAKMP SA. This was introduced by Nokia and proposed changes to 33.210 to clarify the Security Associations, defining bi-directional SAs. The motivation for defining bi-directional SAs was questioned. It was clarified that the proposal did not change anything, but only clarifies the current situation. It was suggested that in this case there should be two separate definitions. The editor undertook to include a modified version of this in 33.210 (which was provided in TD S3-020144, see below).

TD S3-020112 A proposal for evolution of Network Domain Security for Release 6 – Introduction of an authentication framework. This was introduced by Telenor and suggested the creation of a new WID and TS for Rel-6 Network Domain Security. It was suggested that the work should begin with a feasibility study. This was agreed and Telenor agreed to provide a WID proposal for the next SA WG3 meeting.

TD S3-020116 SA mode in Zb interface. This was introduced by Alcatel and had been postponed from the ad-hoc meeting. It was agreed that tunnel-mode needs to be mandated when passing through a SEG. Agreed changes to sections: 5.1, 5.5, 5.3.2 remove complete last paragraph, 5.6.1, 5.6.2 (also make change for Za text).
Not accepted changes to sections: 5.2

With the changes agreed from these contributions, the editor agreed to update the document and the Chairman asked if there were any more issues which would prevent approval of the updated document. There were no problems indicated so simple approval was expected.

TD S3-020144 Updated version of 33.210. This was provided by the editor for approval and was approved.

7.5 MAP security including joint session with CN4 experts (Wednesday afternoon)

Ian Park attended for the joint session with CN WG4 experts and explained that the hope was to identify where existing CN WG4 work could satisfy the

TD S3-020064 Proposed CR to 33.200: NIST Special Publication 800-38A updates on MEA-1 (Rel-4). This was introduced by Nokia and updates the references to the published NIST-800 and adds FIPS-197 reference and associated textual update to reflect the availability of the documents. Editorial changes from TD S3-020066 were moved into this CR and updated in TD S3-020147 (see below).

TD S3-020147 Proposed CR to 33.200: NIST Special Publication 800-38A updates on MEA-1 (Rel-4). This CR was approved.

TD S3-020065 Proposed Text for Cover Sheet for MAPsec Release 5 CR. This was introduced by the Rapporteur of 33.200 (A. Escott) to explain to TSG SA the reasons for a single CR to update 33.200 to Rel-5. The proposed text was agreed for the cover sheet for the presentation of the CR to 33.200 to TSG SA. and was modified in line with changes to the CR and included in TD S3-020146.

TD S3-020062 Clarification of MAP security text. The proposal was updated on line and the agreements included in the updated CR in TD S3-020146.

TD S3-020066 Proposed CR to 33.200: Automatic Key Management (Rel-5). This was introduced by A. Escott. The CR was reviewed carefully and some modifications made for clarification. The CR was updated in TD S3-020146 which was approved.

TD S3-020079 Use of COPS protocol in Ze interface. This was introduced by Nokia and discussed COPS usage in Ze interface for local Security Association and Policy distribution. After some discussion, SA WG3 concluded that they did not wish to endorse the proposal to specify the use of COPS, as it was not a matter for SA WG3. SA WG3 prefer an IP-based protocol which should include confidentiality and integrity. A LS to CN WG4 was provided in TD S3-020148 which was approved.

TD S3-020081 The MAP Dialogue PDU requirements for MAP Security. This was introduced by Nokia and was provided for information. The document was noted and Nokia were requested to input the contribution to CN WG4.

TD S3-020098 MAPsec DoI update. This was presented by Ericsson and SA WG3 were asked to review the updated MAP Security Domain of Interpretation" draft which will be resubmitted at the end of the week, comments were requested off-line. The document was then noted and delegates were asked to review the changes in the document overnight and provide any comments to the meeting. The updated version was provided in TD S3-020150.

TD S3-020150 MAPsec DoI Comparison document (v5 to v4). This was provided to show the changes of the MAP-DoI draft. No comments were received at the meeting and the document was noted.

7.6 Support for subscriber certificates

TD S3-020077 Usage scenarios for subscriber certificates. This was introduced by Nokia and provided scenarios for certificate use mechanisms. The document was noted.

TD S3-020120 Liaison statement on support for subscriber certificates. SA WG1 asked SA WG3 to identify where the requirements for support of subscriber certificates are defined and consider an efficient method for co-ordinating the necessary work. Nokia undertook to provide an update to the WID, identifying the scenarios and including TD S3-020077 as an example. This was provided in TD S3-020153 which was revised to remove Qualcomm from the list and add Motorola, and revised in TD S3-020162 which was approved.

TD S3-020159 Reply LS to SA WG1 on support for subscriber certificates. This was introduced by Nokia. It was agreed to copy this to other affected WGs and provided in TD S3-020163 which was approved.

TD S3-020105 Public key certificates for cellular subscribers. This was provided by Nokia for information and noted. Comments should be provided to V. Niemi directly.

7.7 New A3/A8 based on MILENAGE

TD S3-020063 A3/A8 based on MILENAGE. This was provided by Siemens ATea and proposed that SA WG3 adopt the proposal contained within it and inform the GSMA and 3GPP about the optimal way of defining a A3 / A8 version, based on MILENAGE and conversion functions c2 / c3. The use of RES was also suggested as an alternative to this proposal. This was considered as a subject for the experts in ETSI SAGE to provide advice upon. It was agreed to forward this to ETSI SAGE with the alternative idea of using SRES included for evaluation and advice. A LS containing this was provided in TD S3-020151 and was modified slightly, and copied also to ETSI MCC (for potential funding issues) and the updated version provided in TD S3-020164 which was approved.

7.8 Presence

TD S3-020096 On Service Requirements of Presence Service. This was introduced by Ericsson and discussed the current security and privacy requirements on the presence service (TS 22.141). It was suggested that this should be sent to SA WG1 attached to a LS containing the conclusions of the analysis. This was provided in TD S3-020152 and updated in TD S3-020165 to include CC to CN WG1 which was approved.

7.9 IST

TD S3-020097 Proposed CR to 43.035: IST implementation for non-CAMEL subscribers (Rel-4). It was explained that this change had been accepted late after approval in SMG10/SA WG3 and the Rel-4 version had been created to the non-updated Release 1999 version of the specification. The CR was therefore Category "A". This CR was approved.

TD S3-020111 IST specification numbering. This was presented by Vodafone. Extract:

> *"Immediate Service Termination (IST) was originally designed as a GSM core network feature and involved creating two new stage 1 and stage 2 specifications under SMG10 control, GSM 02.32 and 03.35, respectively. When the 3G Release 99 specifications were created these GSM specifications should have been transposed to 22.032 and 23.035 respectively, as the feature is independent of the type of radio access. Unfortunately, it appears that the specifications were transposed to 42.032 and 43.035 instead when the GERAN Release 4 specifications were created implying that the feature is applicable to GERAN radio access but not UTRAN radio access. Vodafone consider this to have been an oversight rather than something that was done deliberately by SA3/SMG10.*
>
> *It is proposed that SA3 resolve this situation by making it clear that the IST feature is applicable to all 3GPP core networks regardless of the type of radio access. One solution would be to create 22.032 and 23.035 and delete 42.032 and 43.035, but this could be problematic. An LS to SA and GERAN may be required to help resolve this situation."*

It was agreed by SA WG3 that IST was independent of the Bearer and therefore should be in the 2x.03x specification set. The SA WG3 Secretary agreed to take this to the MCC Specifications Manager and provide advice.

> **AP 22/7: M Pope to take TD S3-020111 to MCC specifications manager for a way forward in including IST in UTRAN Rel-4.**

7.10 Configurability of ciphering

TD S3-020005 was checked for the report on the Configurability of Ciphering CR which had been sent back to SA WG3 by TSG SA.

TD S3-020035 Reply to Liaison Statement on Configuration of ciphering. This was introduced by Sunil Chotai and asked SA WG3 to consider the issues raised, the revised requirements and timescale feasibility. The LS was noted.

TD S3-020119 CR to 33.102: Configurability of cipher use - returned from TSG SA. This was provided for review of the revised proposal at SA#14, which had also been rejected. No further input had been received for this topic, and the document was noted. The Configurability of ciphering issue should be considered by delegates and an e-mail dialog will be run by Peter Howard in order to assess interest and provide a complete CR proposal to the next meeting.

> **AP 22/8: Peter Howard to run e-mail dialog on Configurability of ciphering.**

8 Review and update of work programme

The work programme for SA WG3 was reviewed and updated by the group and M. Pope undertook to update the main Project Plan at MCC with the new information.

9 Future meeting dates and venues

9.1 Proposed meeting with CN WGs, Fort Lauderdale, USA, 8-12 April 2002

TD S3-020141 e-mail from TSG CN Chairman: Joint meeting with CN WGs in April 2002. The TSG CN Chairman reported some confusion within CN WGs on 33.203 and requested experts from SA WG3 to present the content of 33.203 and clarify things. 6 - 10 delegates indicated they could go to the CN WG meetings for 2 days 8-9 April 2002, SA WG3 specific ad-hoc on IMS on 8 April, Joint meeting with CN WGs on 9 April 2002.

The planned meetings were then as follows:

Meeting	Date	Location	Host
IMS ad-hoc	8 April 2002	Fort Lauderdale, FL, USA	North American Friends
Joint meetings CN WGs	9 April 2002	Fort Lauderdale, FL, USA	North American Friends
S3#23 + AHAG	14 - 17 May 2002	Victoria, Canada	AT&T Wireless
S3#24	9 - 12 July 2002	Helsinki, Finland (TBC)	Nokia
S3#25	8 - 11 October 2002	Munich, Germany (TBC)	Siemens (TBC)

10 Any other business

There was no other business.

11 Close of meeting

The Chairman thanked delegates for their hard work and co-operation in this critical meeting for completion of TSs for the TSG SA plenary, thanked the hosts for the arrangements and closed the meeting.

Annex A: List of attendees at the SA WG3#20 meeting and Voting List

A.1 List of attendees

Name	Company	e-mail	3GPP ORG	
TO BE COMPLETED				

A.2 SA WG3 Voting list

Based on the attendees lists for meetings #20, #21 and #22, the following companies are eligible to vote at SA WG3 meeting #23:

Company	Country	Status	Partner Org
TO BE COMPLETED			

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020001	Draft agenda for meeting #22	SA WG3 Chairman	2	Approval		Approved (addition of 7.8 and 7.9)
S3-020002	Draft Report of SA WG3 meeting #21	SA WG3 Secretary	4.1	Approval		Approved with change on Z interface decision. Updated v1.0.0 on FTP server
S3-020003	Draft Report of MAPSEC and NDS/IP ad-hoc (Rel-5) January 2002 - v0.0.1rm	SA WG3 Secretary	4.2	Information		Early draft. Approved vsn 1.0.0
S3-020004	Draft Report of aSIP ad-hoc (Rel-5) January 2002 - v.0.0.1	SA WG3 Secretary	4.2	Information		Early draft. Approved vsn 1.0.0
S3-020005	Extract of Draft SA WG3 part of Report for TSG SA meeting #14 - version 0.0.4	TSG SA / SA WG3 Secretary	4.2	Information		From Draft SA report. Noted.
S3-020006	Draft 33.210 version 0.8.0 (provided to email list for comment 05/12/2002)	Rapporteur	7.4	Information		Old version - Noted
S3-020007	Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem	CN WG1	5.2	Information		Presented to IMS ad-hoc - Nothing to do there - Noted.
S3-020008	DRAFT LS on MAPsec error handling (response to S3z010121)	CN WG4	5.2	Action		Considered in MAPsec ad-hoc, AI 5.1. Response in S3z020028.
S3-020009	LS on Removal of Tr mode DCCH	RAN WG2	5.2	Action		Response LS in S3-020154 and LS in S2-020155
S3-020010	LS on START value calculation	RAN WG2	5.2	Action		Dealt with at ad-hoc meeting & e-mail
S3-020011	LS to T2 (S5-010703_T2-010903) on VASP MMS connectivity	SA WG5	5.2	Information		Noted
S3-020012	Liaison Statement: “Reply to LS on Presence Service”	SA WG5	5.2	Information		Noted
S3-020013	Liaison Statement Reply to SyncML with Follow-Up Questions	T WG2	5.2	Information		Noted. Delegates to review and comment to next meeting
S3-020014	Liaison Statement on Confirmation of OSA Support for VASP MMS Connectivity	SA WG2	5.2	Information		Noted.
S3-020015	Liaison Statement on Draft stage 1 TS for Packet Switched Streaming Service	SA WG1	5.2	Action		Reply from SA WG5 in s3-020026. Noted
S3-020016	Liaison statement on Protocol Specification of the Ze-interface	TSG CN	5.2	Action		Considered in MAPsec ad-hoc, AI 5.1. Response in S3z020028. Noted
S3-020017	LS on HFN initialisation at CN domain switch for SRBs	RAN WG2	5.2	Action		Noted
S3-020018	LS on IMS identifiers and ISIM and USIM	SA WG2	5.2	Action		SA#14 Plenary rejected Workshop proposal. Noted.
S3-020019	Reply to "Liaison Statement on Extended Streaming Service"	SA WG4	5.2	Information		Noted
S3-020020	Status of the Generic User Profile Work	3GPP Joint ad-hoc on Generic User Profile (GUP)	7.1	Action		Attachment UP-010129 provided in S3-020021
S3-020021	Release of In-Process Stage 1 Specification to SA1 for Review and Continuing Development	3GPP Joint ad-hoc on Generic User Profile (GUP)	7.1	Information		Noted.
S3-020022	Liaison Statement on " IP version interworking on the transport plane"	SA WG2	5.2	Action		Forwarded to LI group
S3-020023	Liaison Statement on Impacts of Subscriber and Equipment Trace	SA WG5	5.2	Action		TD S3-020157 copied to SA WG5 for information
S3-020024	Comments on UP-010141 and relationship of GUP to Subscription Management	SA WG5	5.2	Information		Noted.

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020025	Liaison Statement on User Equipment Management Feasibility Study (SA5's TR 32.802)	SA WG5		Action	S3-020032	Updated attachment in S3-020032
S3-020026	LS S5-020003 (S1-011241) Packet Switched Streaming Service	SA WG5	5.2	Information		Reply from SA WG5 in S3-020015. Noted
S3-020027	LS reply on: "Draft Push Service Stage 1"	SA WG5	5.2	Information		Noted
S3-020028	Liaison Statement on Count Input to Ciphering Algorithm	GERAN WG2	5.2	Action		Response in S3-020156
S3-020029	Reply Liaison Statement on Prevention of Identity Spoofing in IMS	CN WG1	5.2	Action		
S3-020030	Liaison Statement on transportation of SIP session keys from S-CSCF to P-CSCF	CN WG1	5.2	Action		
S3-020031	Liaison Statement on "Prefix allocation for IPv6 stateless address autoconfiguration"	SA WG2	5.2	Action		Forwarded to LI Group. C Brookson to collect comments for next meeting
S3-020032	Liaison Statement on User Equipment Management Feasibility Study (SA5's TR 32.802)	SA WG5	5.2	Action	S3-020039	Updated attachment (32.802-101) -> S3-020039
S3-020033	LS response to SA WG2: The use of USIMs and ISIMs for IMS	IMS ad-hoc	7.3	Approval	S3-010167	e-mail debate
S3-020034	Update information –TS 33.210 (and 33.210 v110)	Rapporteur	7.4	Information		Old version - Noted
S3-020035	Reply to Liaison Statement on Configuration of ciphering	CN WG1	5.2	Action		Noted
S3-020036	Liaison Statement on Lawful Interception For OoBTC	CN WG4	5.2	Information		Forwarded to LI group
S3-020037	Liaison Statement on AMR-WB and Lawful Interception	CN WG4	5.2	Information		Forwarded to LI group. LS in S3-020129 covers the response
S3-020038	IMS Security requirements	SA WG1	5.2	Action		To review for Joint session with SA WG1
S3-020039	Liaison Statement on User Equipment Management Feasibility Study (SA5's TR 32.802)	SA WG5	5.2	Action		Response LS in S2-020136
S3-020040	Comments on UP-010141 and relationship of GUP to Subscription Management	SA WG5	5.2	Information		Noted
S3-020041	Liaison Statement on UE functionality split	T WG3	5.2	Information		Noted
S3-020042	Liaison Statement on ISIM for support of IMS	T WG3	5.2	Action		Considered in ad-hoc - reply in S3-020033
S3-020043	LS reply to: " Liaison Statement on Confirmation of OSA Support for VASP MMS Connectivity."	SA WG1	5.2	Information		Noted.
S3-020044	Liaison Statement on Support of security algorithms in OSA framework (response to S3-010696)	CN WG5	5.2	Information		Joint session held in S3#22. Noted.
S3-020045	Correspondence from S Hayes (TSG CN Chairman): Results from recent IETF coordination meeting	SA WG3 Secretary	5.3	Information		Received over e-mail. S3 Chairman to report feelings of S3 to CN Chairman
S3-020046	Proposed CR to 33.200: NIST Special Publication 800-38A updates on MEA-1 (Rel-4)	Nokia	6.1	Approval	S3-020064	WITHDRAWN (updated in S3-020064)
S3-020047	Liaison Statement on Lawful Intercept related information in CN5 specifications	CN WG5	5.2	Information		Forwarded to LI group
S3-020048	LS from LI group: VASP MMS Connectivity	SA WG3-LI	4.3	Action		Noted.
S3-020049	Proposed LS to SA WG1/SA WG2: Reply to LS on "Privacy Override Indicator"	SA WG3-LI	4.3	Approval	S3-020128	Contact added in S3-020128.
S3-020050	Proposed LS to ETSI TC SEC on WI IP Interception	SA WG3-LI	4.3	Approval		Agreed for transmission

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020051	Proposed LS to ETSI TC SEC WG LI on a new ASN.1 branch for 3GPP	SA WG3-LI	4.3	Approval		Agreed for transmission
S3-020052	Proposed LS to ETSI TC SEC WG LI on the handling of ASN.1 parameters for LI	SA WG3-LI	4.3	Approval		Noted
S3-020053	Proposed [DRAFT] Response to email "NP-010710: AMR-WB TSs from SA4"	SA WG3-LI	4.3	Approval	S3-020129	DRAFT removed in S3-020129
S3-020054	LS from LI group: MM7 working assumptions	SA WG3-LI	4.3	Action		Noted
S3-020055	Liaison Statement on coordination of data definitions, identified in GUP development	T WG2	5.2	Action		S. Ward to organise an e-mail discussion on this and provide comments to the next meeting
S3-020056	Response Liaison Statement on Trace and Availability of IMSI and IMEI	CN WG4	5.2	Action		Response in S3-020157
S3-020057	LS reply on " Response to: Liaison Statement on Revised Push Service Stage 1"	SA WG1	5.2	Action		No attachment - See S3-020058.
S3-020058	Liaison Statement on revised "Draft Push Service Stage 1"	SA WG1	5.2	Action		Draft Spec attached. P. Howard to review and collect comments
S3-020059	Liaison Statement on Access to IMS Services using 3GPP release 99 and release 4 UICCs	SA WG1	5.2	Action		Response in S3-020127
S3-020060	Liaison Statement on ISIM for support of IMS	SA WG1	5.2	Information		Noted
S3-020061	Liaison Statement on Packet switched streaming service stage 1 TS for release 5	SA WG1	5.2	Information		No attachment. Noted
S3-020062	Clarification of MAP security text	Rapportuer (A. Escott)	7.5	Discussion		Agreements in S3-020146
S3-020063	A3/A8 based on MILENAGE	Siemens Atea	7.7	Discussion		LS to SAGE in S3-020151
S3-020064	Proposed CR to 33.200: NIST Special Publication 800-38A updates on MEA-1 (Rel-4)	Nokia, Siemens	6.1	Approval	S3-020147	Editorials from S3-020066 added and updated in S3-020147
S3-020065	Proposed Text for Cover Sheet for MAPsec Release 5 CR	MAP Rapportuer	7.5	Discussion / Decision		Agreed cover sheet text
S3-020066	Proposed CR to 33.200: Automatic Key Management (Rel-5)	MAP Rapportuer	7.5	Approval	S3-020146	Updated in S2-020146
S3-020067	SIP Message Integrity Protection Work in the IETF	Nortel Networks	7.3	Discussion		Noted
S3-020068	Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #1/02 on lawful interception	SA WG3 LI group	4.3	Information		Noted. New Chair of SA WG3-LI group approved.
S3-020069	Proposed CR to 33.107: PDP context Deactivation cause (Rel-5)	SA WG3 LI group	4.3	Approval		Approved
S3-020070	Proposed CR to 33.107: Addition of PDP context modification Event (Rel-5)	SA WG3 LI group	4.3	Approval	S3-020130	Merged with S3-020071
S3-020071	Proposed CR to 33.107: Transferring the QoS information element across the X2 interface (Rel-5)	SA WG3 LI group	4.3	Approval	S3-020130	Merged with S3-020070
S3-020072	Proposed CR to 33.107: The use of H.248 in setting up a bearer intercept point at the MGW (Rel-5)	SA WG3 LI group	4.3	Approval		Approved
S3-020073	Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-99)	SA WG3 LI group	4.3	Approval		Approved
S3-020074	Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-4)	SA WG3 LI group	4.3	Approval		Approved
S3-020075	Proposed CR to 33.107: Inter-SGSN RA update with active PDP context (Rel-5)	SA WG3 LI group	4.3	Approval		Approved
S3-020076	Revised Work Item Description (revision of SP-000309): Rel-5 LI HO interface	SA WG3 LI group	4.3	Approval	S3-020131	Editorial modified in S3-020131
S3-020077	Usage scenarios for subscriber certificates	Nokia	7.6	Discussion		Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020078	Draft TS 33.203 v 1.1.0: Access security for IP-based services (Rel-5)	Rapporteur (K. Boman)	7.3			Used in evening editing session
S3-020079	Use of COPS protocol in Ze interface	Nokia	7.5	Discussion		LS to CN WG4 in S3-020148
S3-020080	Proposed Changes to 33.210 about the ISAKMP SA	Nokia	7.4	Discussion / Decision		Agreed changes included by editor
S3-020081	The MAP Dialogue PDU requirements for MAP Security	Nokia	7.5	Discussion		Noted. Nokia to input to CN WG4
S3-020082	Updates to SIP-Level Solution for IMS Integrity Protection	Nortel Networks	7.3	Discussion / Decision		Used in evening editing session
S3-020083	Liaison Statement on Digital Rights Management (DRM)	SA WG1	5.2	Information / Discussion		Chairman to raise ownership of Stage 2 DRM at SA#15
S3-020084	LS on Priority Service Feasibility Study TR - draft	SA WG1	5.2	Action		L Valerius to collect comments on security requirements for next meeting
S3-020085	LS on 3GPP System – WLAN interworking	SA WG1	5.2	Information		Noted. S. Schroeder to collect comments for next meeting
S3-020086	Liaison Statement on MM7 Security Mechanisms for Release 5	T WG2	5.2	Note and Comment on draft		G Rose to collect comments for next meeting. Chairman to report ongoing Security Analysis to SA#15
S3-020087	LS reply on: “Draft Push Service Stage 1”	SA WG2	5.2	Information		Noted
S3-020088	JOINT NEWS RELEASE: ETSI and ECBS co-operate in the Development of Standards for the Security of Telecommunications and M-Commerce	SA WG3 Secretary	5.4	Information		Noted
S3-020089	HTTP AKA Internet Draft	Nokia	7.3	Discussion / Decision		Delegates to consider if adequate security
S3-020090	On P-CSCF behaviour at Integrity check failures	Ericsson	7.3	Discussion / Decision		Used in evening editing session
S3-020091	Unprotected REGISTER messages	Ericsson	7.3	Discussion / Decision	S3-020137	Changes included in S3-020137
S3-020092	Requirements and a proposed solution for SA_ID	Ericsson, Nortel Networks, Nokia	7.3	Discussion / Decision		Used in evening editing session
S3-020093	A security framework for IMS utilising HTTP Digest	Ericsson	7.3	Discussion / Decision		Principles accepted. For further discussion
S3-020094	On integrity protecting SIP-signalling in IMS	Ericsson	7.3	Discussion / Decision		No decision made on choice between SIP/Digest
S3-020095	New and updated SIP drafts	Ericsson	7.3	Information	S3-020134	Noted. Correct attachments in S3-020134
S3-020096	On Service Requirements of Presence Service	Ericsson	7.8	Information		LS to SA WG1 in S3-020152
S3-020097	Proposed CR to 43.035: IST implementation for non-CAMEL subscribers (Rel-4)	Ericsson	7.9	Approval		Approved
S3-020098	MAPSec DoI update	Ericsson	7.5			Reviewed. Updated version in S3-020150
S3-020099	Security Mechanism Agreement for SIP Connections	Ericsson	7.3	Information		Noted
S3-020100	3GPP TS 33.108: Handover Interface for Lawful Intercept (Release 5) - Version 0.7.3	SA WG3 LI group	4.3	Approval		Approved - For info SA#15: S3 Chair to inform TSG SA of lack of CS and IMS LI requirements

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020101	Authentication Scheme Negotiation in OSA	Alcatel	7.2	Adoption		Discussed and noted. No preference for solutions
S3-020102	Encryption of challenge in CHAP-based OSA authentication	Alcatel	7.2	Adoption		Discussed and noted
S3-020103	Security of terminateAccess() function in OSA	Alcatel	7.2	Adoption		Discussed and noted. O Paradaens to create CR for OSA sec for SA WG3 comment
S3-020104	Use of one-way hash function for CHAP in OSA	Alcatel	7.2	Adoption		Discussed and noted. Solution proposal to issue#1 in S3-020101
S3-020105	Public key certificates for cellular subscribers	Nokia	7.6	Discussion		Noted
S3-020106	Unprotected registrations during SA lifetime	Nokia	7.3	Discussion / Approval	S3-020137	Relevant changes included in S3-020137
S3-020107	SA handling and use	Hutchison 3G UK	7.3	Discussion / Decision		Used in evening editing session
S3-020108	Uniqueness of IP address/port number checking in the P-CSCF	Nokia	7.3	Discussion / Decision		Decision on Pseudo-CR?
S3-020109	Proposed changes to 33.203 v1.1.0 regarding ISIM	Vodafone	7.3	Approval		Used in evening editing session
S3-020110	Proposed editorial clarifications to 33.203 v1.1.0	Vodafone	7.3	Approval		Used in evening editing session
S3-020111	IST specification numbering	Vodafone	7.9	Decision		M Pope to check with MCC specs manager
S3-020112	A proposal for evolution of Network Domain Security for Release 6 – Introduction of an authentication framework	Telenor	7.4	Discussion / Agreement		Agreed - Telenor to provide WID next meeting
S3-020113	Version 1.1.0 of TR 23.871 Enhanced user privacy in location services	Secretary SA WG3	4.1	Information		For use in ad-hoc drafting group on LCS privacy
S3-020114	Draft CR to 22.071: for introduction of a Codeword setting	Secretary SA WG4	4.1	Information		For use in ad-hoc drafting group on LCS privacy
S3-020115	LS to CN WG4 on joint session on Ze interface	SA WG3 MAP ad-hoc	4.2	Approval		Sent from ad-hoc, with footnote that SA WG3 to approve it. Confirmed by SA WG3
S3-020116	SA mode in Zb interface	Alcatel	7.4	Approval		From ad-hoc meeting. Agreed changes included by editor
S3-020117	Update of S3z020032 : aSIP-Access Security for IP-Based Services	K Boman	7.3			Drafting session set up
S3-020118	Need for section 7.3.3	Hutchison 3G UK	8	Discussion / Decision		
S3-020119	CR to 33.102: Configurability of cipher use - returned from TSG SA	Vodafone / TSG SA	7.10	Discussion		Presented to TSG SA for Configurability CR and returned to SA WG3 for further elaboration. P Howard to run e-mail dialog on Conf. Ciphering
S3-020120	Liaison statement on support for subscriber certificates	SA WG1	7.4	Action		Latest vsn to review and send comments to S1, S2, T2, GUP-joint group
S3-020121	Presentation: The 3GPP Generic User Profile (GUP)		7.1	Presentation		Presented. Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020122	Work Item Description: The 3GPP Generic User Profile (updated)		7.1	Information		Noted.
S3-020123	LS to TSG SA: Generic User Profile (GUP) time scales	SA WG1	7.1	Information		Noted.
S3-020124	Stage 1 Service Requirement for the 3GPP Generic User Profile (GUP)		7.1	Information		Noted.
S3-020125	Comments on draft EAP/SIM	Qualcomm	7.3	Discussion		Noted.
S3-020126	Parlay/OSA: an open API for service development	Chelo Abarca, Andy Bennett, Ard-Jan Moerdijk, Musa Unmehopa	7.2	Presentation		Presented
S3-020127	LS from SA WG2: LS on Stage 2 for use of USIMs and ISIMs for IMS	SA WG2	5.2	Action		Utilised in update of 33.200
S3-020128	Proposed LS to SA WG1/SA WG2: Reply to LS on “Privacy Override Indicator”	SA WG3-LI	4.3	Approval		Approved
S3-020129	Proposed [DRAFT] Response to email “NP-010710: AMR-WB TSs from SA4”	SA WG3-LI	4.3	Approval		Approved
S3-020130	Proposed CR to 33.107: Addition of PDP context modification Event and Transferring the QoS information element across the X2 interface (Rel-5)	SA WG3	4.3	Approval		Approved
S3-020131	Revised Work Item Description (revision of SP-000309): Rel-5 LI HO interface	SA WG3 LI group	4.3	Approval		Approved
S3-020132	Security association management in the UE and the P-CSCF	Siemens	7.3	Discussion / Approval		Used in evening editing session
S3-020133	Draft response to S3-020038: Security for UE functional split, reply to S1-020300	SA WG3	5.2	Approval	S3-020166	Updated in S3-020166
S3-020134	New and updated SIP drafts (resubmitted with correct attachments)	Ericsson	7.3	Information		Noted
S3-020135	Problem with use of RES in Digest-AKA	Qualcomm	7.3	Discussion		Qualcomm to update with changes to IETF drafts
S3-020136	Reply Liaison Statement on the User Equipment Management Feasibility Study (SA5's TR 32.802)	SA WG3	5.2	Approval		Approved
S3-020137	Pseudo-CR to 33.203: Unprotected registrations during SA lifetime	Nokia, Ericsson	7.3	Approval		Agreed in drafting group to be included in TS 33.203
S3-020138	Reply Liaison Statement on Registrations without user authentication and Identity Spoofing	CN WG1	7.3	Action		Response in S3-020160
S3-020139	Response to LS (S3z020043) on START value calculation and Additional principles adopted by TSG-RAN WG2	RAN WG2	5.2	Discussion		Response in S3-020149
S3-020140	3GPP requirements draft	Vesa Torvinen (E-mail received 26/02/2002)	5.2	Information		Noted
S3-020141	e-mail from TSG CN Chairman: Joint meeting with CN WGs in April 2002	SA WG3 Secretary	9.1	Decision		6-10 experts to meet for 2 days - 1 day IMS, 1 day Joint CN WGs
S3-020142	Reply LS on “Enhanced user privacy for location services”	SA WG3	4.1	Approval	S3-020145	Updated in S3-020145
S3-020143	On NW initiated re-authentications	Ericsson	7.3	Discussion / Decision		Utilised in editorial session
S3-020144	Updated version of 33.210	Editor (G. Koein)	7.4	Approval		Approved
S3-020145	Reply LS on “Enhanced user privacy for location services”	SA WG3	4.1	Approval		Approved
S3-020146	Updated CR to 33.200 (Rel-5)	A Escott	7.5	Approval		Approved
S3-020147	Proposed CR to 33.200: NIST Special Publication 800-38A updates on MEA-1 (Rel-4)	SA WG3	7.5	Approval		Approved
S3-020148	LS to CN WG4: Ze interface security	SA WG3	7.5	Approval		Approved

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3-020149	Response to S3-020139	SA WG3	5.2	Approval		Approved
S3-020150	MAPsec DoI Comparison document (v5 to v4)	Siemens	7.5	Information		Noted
S3-020151	LS to ETSI SAGE: Use of MILENAGE as the basis for a new GSM A3/A8 algorithm	SA WG3	7.7	Approval	S3-020164	Updated in S3-020164
S3-020152	LS to SA WG1, SA WG2: "Requirements on Presence Service"	SA WG3	7.8	Approval	S3-020165	Updated in S3-020165
S3-020153	Updated WID : Support for Subscriber Certificates	SA WG3	7.6	Approval	S3-020162	Revised in S3-020162
S3-020154	Reply LS to S3-020009 (V Niemi)	SA WG3	5.2	Approval		Approved
S3-020155	CR to 33.102: Removal of Tr mode DCCH (Rel-99)	SA WG3	5.2	Approval		Approved
S3-020156	Reply to GERAN WG2 LS (S3-020028) - V Niemi	SA WG3	5.2	Approval		Approved
S3-020157	LS to CN WG4 on spreading IMSI/IMEI over signalling interfaces (reply to S3-020056)	SA WG3	5.2	Approval		**M Pope to write LS.** Channels are protected so no security concerns Approved
S3-020158	33.203 version 1.2.0	Editor (K. Boman)	7.3	Review/Approval		To be reviewed by correspondence for comments by 6 March 2002
S3-020159	Reply LS to SA WG1 on support for subscriber certificates	SA WG3		Approval	S3-020163	Revised in S3-020163
S3-020160	Response to S3-020138 on Registrations without user authentication and Identity Spoofing	SA WG3		Approval		Approved in principle. A Escott to create and circulate by e-mail when TS 33.200 is approved.
S3-020161	LS to CN WG1 on SA handling (A Escott)	SA WG3	7.3	Approval		For e-mail approval
S3-020162	Updated WID : Support for Subscriber Certificates	SA WG3	7.6	Approval		Approved
S3-020163	Reply LS to SA WG1 on support for subscriber certificates	SA WG3	7.6	Approval		Approved
S3-020164	LS to ETSI SAGE: Use of MILENAGE as the basis for a new GSM A3/A8 algorithm	SA WG3	7.8	Approval		Approved
S3-020165	LS to SA WG1, SA WG2: "Requirements on Presence Service"	SA WG3	7.8	Approval		Approved
S3-020166	Draft response to S3-020038: Security for UE functional split, reply to S1-020300	SA WG3	5.2	Approval		Approved
S3-020167	LS response to SA WG2: The use of USIMs and ISIMs for IMS	SA WG3	5.2			P Howard organising e-mail debate for update

Annex C: Status of specifications under SA WG3 responsibility

NOTE: If the Editors are still not accurate - please provide the secretary with an update in order to update the main specifications database.

Specification			Title	Editor	Rel
			TO BE COMPLETED		

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	163		R99	Removal of Tr mode DCCH	F	3.10.0	S3-22	S3-020155	Agreed (R99 only as already done for Rel-4)
33.107	017		Rel-5	PDP context Deactivation cause	B	5.1.0	S3-22	S3-020069	Agreed
33.107	018		Rel-5	The use of H.248 in setting up a bearer intercept point at the MGW	B	5.1.0	S3-22	S3-020072	Agreed
33.107	019		R99	Inter-SGSN RA update with active PDP context	F	3.4.0	S3-22	S3-020073	Agreed
33.107	020		Rel-4	Inter-SGSN RA update with active PDP context	A	3.4.0	S3-22	S3-020074	Agreed
33.107	021		Rel-5	Inter-SGSN RA update with active PDP context	A	5.2.0	S3-22	S3-020075	Agreed
33.107	022		Rel-5	Addition of PDP context modification Event and Transferring the QoS information element across the X2 interface	B	5.2.0	S3-22	S3-020130	Agreed
33.200	020		Rel-4	NIST Special Publication 800-38A updates on MEA-1	F	4.2.0	S3-22	S3-020147	Agreed
43.035	001		Rel-4	IST implementation for non-CAMEL subscribers	A	4.0.0	S3-22	S3-020097	Agreed
33.200	021		Rel-5	Automatic Key Management	B	4.3.0	S3-22	S3-020146	Agreed

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD number	Title	Source TD	Comment/Status
S3-020007	Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem	N1-012041	Presented to IMS ad-hoc - Nothing to do there - Noted.
S3-020008	DRAFT LS on MAPsec error handling (response to S3z010121)	N4-011449	Considered in MAPsec ad-hoc, AI 5.1. Response in S3z020028.
S3-020009	LS on Removal of Tr mode DCCH	R2-012774	Response LS in S3-020154 and LS in S2-020155
S3-020010	LS on START value calculation	R2-012775	Dealt with at ad-hoc meeting & e-mail
S3-020011	LS to T2 (S5-010703_T2-010903) on VASP MMS connectivity	S5-010750	Noted
S3-020012	Liaison Statement: “Reply to LS on Presence Service”	S5-010755	Noted
S3-020013	Liaison Statement Reply to SyncML with Follow-Up Questions	T2-011184	Noted. Delegates to review and comment to next meeting
S3-020014	Liaison Statement on Confirmation of OSA Support for VASP MMS Connectivity	S2-013589	Noted.
S3-020015	Liaison Statement on Draft stage 1 TS for Packet Switched Streaming Service	S1-011241	Noted
S3-020016	Liaison statement on Protocol Specification of the Ze-interface	NP-010685	Considered in MAPsec ad-hoc, AI 5.1. Response in S3z020028. Noted
S3-020017	LS on HFN initialisation at CN domain switch for SRBs	R2-012776	Noted
S3-020018	LS on IMS identifiers and ISIM and USIM	S2-013599	SA#14 Plenary rejected Workshop proposal. Noted.
S3-020019	Reply to "Liaison Statement on Extended Streaming Service"	S4-010660	Noted
S3-020020	Status of the Generic User Profile Work	UP-010128	Attachment UP-010129 provided in S3-020021
S3-020021	Release of In-Process Stage 1 Specification to SA1 for Review and Continuing Development	UP-010129	Noted.
S3-020022	Liaison Statement on " IP version interworking on the transport plane"	S2-020291	Forwarded to LI group
S3-020023	Liaison Statement on Impacts of Subscriber and Equipment Trace	S5-020013	TD S3-020157 copied to SA WG5 for information
S3-020024	Comments on UP-010141 and relationship of GUP to Subscription Management	S5-020016	Noted.
S3-020026	LS S5-020003 (S1-011241) Packet Switched Streaming Service	S5-020044	Noted
S3-020027	LS reply on: “Draft Push Service Stage 1”	S5-020045	Noted
S3-020028	Liaison Statement on Count Input to Ciphering Algorithm	G2-020145	Response in S3-020156
S3-020029	Reply Liaison Statement on Prevention of Identity Spoofing in IMS	N1-020155	
S3-020030	Liaison Statement on transportation of SIP session keys from S-CSCF to P-CSCF	N1-020154	
S3-020031	Liaison Statement on "Prefix allocation for IPv6 stateless address autoconfiguration"	S2-020326	Forwarded to LI Group. C Brookson to collect comments for next meeting
S3-020035	Reply to Liaison Statement on Configuration of ciphering	N1-020035	Noted
S3-020036	Liaison Statement on Lawful Interception For OoBTC	N4-020186	Forwarded to LI group
S3-020037	Liaison Statement on AMR-WB and Lawful Interception	N4-020268	Forwarded to LI group. LS in S3-020129 covers the response
S3-020038	IMS Security requirements	S1-020300	To review for Joint session with SA WG1
S3-020039	Liaison Statement on User Equipment Management Feasibility Study (SA5's TR 32.802)	S5-020027	Response LS in S2-020136
S3-020040	Comments on UP-010141 and relationship of GUP to Subscription Management	S5-020028	Noted
S3-020041	Liaison Statement on UE functionality split	T3-020079	Noted
S3-020042	Liaison Statement on ISIM for support of IMS	T3-020139	Considered in ad-hoc - reply in S3-020033
S3-020043	LS reply to: “ Liaison Statement on Confirmation of OSA Support for VASP MMS Connectivity.”	S1-020470	Noted.
S3-020044	Liaison Statement on Support of security algorithms in OSA framework (response to S3-010696)	N5-020113	Joint session held in S3#22. Noted.
S3-020045	Correspondence from S Hayes (TSG CN Chairman): Results from recent IETF coordination meeting		Received over e-mail. S3 Chairman to report feelings of S3 to CN Chairman

TD number	Title	Source TD	Comment/Status
S3-020047	Liaison Statement on Lawful Intercept related information in CN5 specifications	N5-020162	Forwarded to LI group
S3-020048	LS from LI group: VASP MMS Connectivity	N5-020162	Noted.
S3-020050	Proposed LS to ETSI TC SEC on WI IP Interception	S3LI02_047r1	Noted.
S3-020054	LS from LI group: MM7 working assumptions	S3LI02_058r1	Noted
S3-020055	Liaison Statement on coordination of data definitions, identified in GUP development	T2-020254	S. Ward to organise an e-mail discussion on this and provide comments to the next meeting
S3-020056	Response Liaison Statement on Trace and Availability of IMSI and IMEI	N4-020302	Response in S3-020157
S3-020057	LS reply on " Response to: Liaison Statement on Revised Push Service Stage 1"	S1-020541	No attachment - See S3-020058.
S3-020058	Liaison Statement on revised "Draft Push Service Stage 1"	S1-020543	Draft Spec attached. P. Howard to review and collect comments
S3-020059	Liaison Statement on Access to IMS Services using 3GPP release 99 and release 4 UICCs	S1-020577	Response in S3-020127
S3-020060	Liaison Statement on ISIM for support of IMS	S1-020579	Noted
S3-020061	Liaison Statement on Packet switched streaming service stage 1 TS for release 5	S1-020605	No attachment. Noted
S3-020083	Liaison Statement on Digital Rights Management (DRM)	S1-020493	Chairman to raise ownership of Stage 2 DRM at SA#15
S3-020084	LS on Priority Service Feasibility Study TR - draft	S1-020642	L Valerius to collect comments on security requirements for next meeting
S3-020085	LS on 3GPP System – WLAN interworking	S1-020636	Noted. S. Schroeder to collect comments for next meeting
S3-020086	Liaison Statement on MM7 Security Mechanisms for Release 5	T2-020298	G Rose to collect comments for next meeting. Chairman to report ongoing Security Analysis to SA#15
S3-020087	LS reply on: "Draft Push Service Stage 1"	S2-020868	Noted
S3-020120	Liaison statement on support for subscriber certificates	S1-020645	Latest vsn to review and send comments to S1, S2, T2, GUP-joint group
S3-020127	LS from SA WG2: LS on Stage 2 for use of USIMs and ISIMs for IMS	S2-020912	Utilised in update of 33.200
S3-020138	Reply Liaison Statement on Registrations without user authentication and Identity Spoofing		Response in S3-020160
S3-020139	Response to LS (S3z020043) on START value calculation and Additional principles adopted by TSG-RAN WG2		Response in S3-020149
S3-020140	3GPP requirements draft		Noted
S3-020141	e-mail from TSG CN Chairman: Joint meeting with CN WGs in April 2002		6-10 experts to meet for 2 days - 1 day IMS, 1 day Joint CN WGs

E.2 Liaisons from the meeting

TD number	Title	Comment/Status	TO	CC
TD S3-020129	Proposed [DRAFT] Response to email "NP-010710: AMR-WB TSs from SA4"	Approved	SA WG4	TSG CN CN WG4
TD S3-020136	Reply Liaison Statement on the User Equipment Management Feasibility Study (SA5's TR 32.802)	Approved	SA WG5 SWG-A	T WG2 T WG3
TD S3-020145	Reply LS on "Enhanced user privacy for location services"	Approved	SA WG1 SA WG2	
TD S3-020148	LS to CN WG4: Ze interface security	Approved	CN WG4	
TD S3-020149	Response to S3-020139	Approved	RAN WG2	
TD S3-020154	Reply LS to S3-020009	Approved	RAN WG2	
TD S3-020156	Reply to GERAN WG2 LS (S3-020028)	Approved	TSG GERAN	
TD S3-020157	TO BE PROVIDED - M POPE LS to CN WG4 on spreading IMSI/IMEI over signalling interfaces (reply to S3-020056)	Approved	CN WG4	
TD S3-020160	TO BE PROVIDED - A ESCOTT Response to S3-020138 on Registrations without user authentication and Identity Spoofing	Approved (e-mail distribution for confirmation)	CN WG1	
TD S3-020161	TO BE PROVIDED - A ESCOTT LS to CN WG1 on SA handling	For e-mail approval	CN WG1	
TD S3-020163	Reply LS to SA WG1 on support for subscriber certificates	Approved	SA WG1	CN WG1, CN WG4, SA WG5, T WG2, T WG3
TD S3-020164	LS to ETSI SAGE: Use of MILENAGE as the basis for a new GSM A3/A8 algorithm	Approved	ETSI SAGE	GSMA-SG, MCC
TD S3-020165	LS to SA WG1, SA WG2: "Requirements on Presence Service"	Approved	SA WG1, SA WG2	CN WG1
TD S3-020166	Draft response to S3-020038: Security for UE functional split, reply to S1-020300	Approved	SA WG1	SA WG2, T WG2, CN WG1, TSG GERAN
TD S3-020167	TO BE PROVIDED - P HOWARD LS response to SA WG2: The use of USIMs and ISIMs for IMS	For e-mail discussion / approval	SA WG2	

LI Group LSs for other groups:

TD number	Title	Comment/Status	TO	CC
TD S3-020051	Proposed LS to ETSI TC SEC WG LI on a new ASN.1 branch for 3GPP	Agreed for transmission	ETSI TC SEC-LI	
TD S3-020128	Proposed LS to SA WG1/SA WG2: Reply to LS on "Privacy Override Indicator" Additional reply to S1-011286	Approved	SA WG1, SA WG2	
TD S3-020129	Proposed [DRAFT] Response to email "NP-010710: AMR-WB TSs from SA4"	Approved	SA WG4	

Annex F: List of Actions from the meeting

AP 22/1: **Greg Rose to provide the comments to SA WG3.**

AP 22/2: **Chairman to raise ownership of DRM Stage 2 at TSG SA #15.**

AP 22/3: **Chairman to report the ongoing Security Analysis on MM7 Rel-5 to TSG SA #15.**

AP 22/4: **The SA WG3 Chairman agreed to put the feelings of the group concerning mandated support of TLS to the TSG CN Chairman (3GPP representative to the IETF group) and report the conversation back to SA WG3.**

AP 22/5: **O Paradaens to create CRs for OSA security issues and distribute to SA WG3 e-mail list for comment.**

AP 22/6: **SA WG3 Chairman to present reasons for keeping both SIP level and HTTP Digest solutions in Annex C of 33.203 until the IETF work is more stable and a clear choice can be made.**

WID updates

S3-020131	Revised Work Item Description (revision of SP-000309): Rel-5 LI HO interface	SA WG3 LI group	4.3	Approval		Approved
S3-020162	Updated WID : Support for Subscriber Certificates	SA WG3	7.6	Approval		Approved

TSs approved for SA presentation:

TD S3-020100 TS 33.108 for information

33.203: E-mail approval of update to TD S3-020158

TD S3-020144 TS 33.210 for approval

3GPP TSG SA WG3 #21bis aSIP ad hoc **version 1.0.0**
Antwerp, Belgium
31st January – 1st February 2002

Source: **SA WG3 Secretary**

Title: **Report of the aSIP ad hoc meeting, (S3 21b)**

Status: **Approved**

---

1 Opening of the meeting

The meeting was opened by V. Niemi, SA WG3 Vice Chairman, and outlined the schedule for the ad-hoc meeting.

Olivier Paridaens welcomed delegates to Antwerp, Belgium, on behalf of Alcatel, and provided domestic arrangements for the ad-hoc meeting.

2 Approval of the agenda and objectives of the meeting

TD S3z020001 Proposed agenda and objectives for aSIP ad-hoc meeting. This was presented by the Chairman. A new Agenda Item 4b: "Incoming LSs" was added and with this, the agenda was then approved.

Meeting objectives:

- The primary objective was to make progress on TS33.203v100 and prepare the specification for approval at SA#15.
- The secondary objective was to make progress on SIP signalling protection and discuss the two different options currently kept in the Annex of TS33.203v100.
- The third objective was to progress the discussion on ISIM taking into account the output from SA#14.

The objectives were agreed.

3 Allocation of documents to agenda items

Documents were allocated to their respective agenda items.

TD S3-020006, TD S3-020007, TD S3-020029, TD S3-020030 and TD S3-020031 for the SA WG3 meeting #22 (Bristol) were allocated in addition to those specifically provided to this meeting.

4 SA#14 report and status report of TS33.203v100

The parts of the draft report of SA#14 were considered for ISIM and IETF dependency issues.

TD S3z020032 aSIP-Access Security for IP-Based Services. This was presented by K. Boman, and provided the aims and expectations from the ad-hoc meeting, and the open issues remaining in TS 33.203.

The open issues still left at the end of the ad-hoc meeting would need to be seriously considered and contributed to for the SA WG3 meeting #22 (Bristol) in order to stabilise the document for approval at SA#15.

K. Boman was thanked for the presentation of his views on the way forward.

4b Incoming LSs

TD S3-020007 Liaison Statement on privacy of IPv6 addresses allocated to terminals using the IM CN subsystem. This was introduced by Lucent. There was nothing that could be done by the ad-hoc meeting, and so the LS was noted and would be further considered at the SA WG3 meeting.

TD S3-020029 Reply Liaison Statement on Prevention of Identity Spoofing in IMS. This was introduced by Hutchinson 3G UK. The solution 1 was not considered a good solution to the group, and after some discussion on the way forward, it was agreed to consider the Ericsson contribution in TD S3z020014 which provided a potential procedure:

TD S3z020014 On the use of KSI-IMS. this was introduced by Ericsson and proposed that the P-CSCF allocates and stores a new identifier each time the S-CSCF triggers an IMS-AKA procedure during the registration procedure. For clarification of the procedures, the draft of 33.203, provided in TD S3z020018 was used (in particular, section 7.3.1.1). It was suggested that the Public Identity may be needed so that the P-CSCF knows the destination SA. There was some discussion on the Mobile Terminated case, and further investigation on the impact of the availability of the Public Address/IMPU. The KSI-IMS solution described here could not be agreed upon at the ad-hoc meeting, and it was agreed that further investigation on protection against such attacks needs to be done. It was recognised that whether to send back the KSI or the IMPU was still an open issue.

TD S3z020026 LS S5-020003 (S1-011241) Packet Switched Streaming Service. This was introduced by Hutchinson 3G UK, and provided a scenario where the SA keys can outlive their intended lifetime, providing an opportunity for key compromise.

It was agreed that a LS would be created for CN WG1 informing them that solution 2 was more acceptable to SA WG3 ad-hoc than solution 1. A. Escott agreed to produce this LS for e-mail approval on the SA WG3 list. (TD S3z020041). Schedule: Distribution to e-mail list for comment Monday 4 February. Comments following Monday 11 February - Revised version available Tuesday 12 February, for final e-mail approval Friday 15 February.

TD S3-020030 Liaison Statement (from CN WG1) on transportation of SIP session keys from S-CSCF to P-CSCF. This was presented by Vodafone. For the second point, it was agreed that a maximum of 3 re-authentication attempts was acceptable. For the final point, Ericsson contribution section 4 of TD S3z020009 was introduced:

> TD S3z020009 Results of a conference call with IETF ADs and SIP WG chairs regarding IMS security. Section 4: Key Transport. This was introduced by Ericsson and discussed. It recommended that an application layer mechanism be used to protect key transport (e.g. S/MIME or XML Digital Signatures). It was generally accepted that the IETF had rejected the use of EAP for AKA, which implies that SA WG3 need to find another mechanism if the IETF protocols are to be used. Hop-by-hop protection was still considered the method used in SA WG3.

It was agreed that a LS to CN WG1 was needed to confirm the maximum of 3 re-authentication attempts, corresponding to the action in their LS, which P. Howard agreed to draft this, for SA WG3 e-mail approval (TD S3z020039). Schedule: Distribution to e-mail list for comment Monday 4 February. Comments following Monday 11 February - Revised version available Tuesday 12 February, for final e-mail approval Friday 15 February.

TD S3-020031 Liaison Statement on "Prefix allocation for IPv6 stateless address auto-configuration". This was introduced by the Chairman, and delegates were asked to read this through to analyse potential impacts on security with an aim to closing the open issue on privacy at the SA WG3 meeting #22 (Bristol). The LS was then noted.

TD S3z020033 Liaison Statement on ISIM for support of IMS. This was introduced by Vodafone, along with the attached presentation slides. SA WG3 were asked to confirm the requirement of up to 4 simultaneously active applications. It was considered that the security implications may come about if an application is temporarily closed in order to activate a parallel IMS subscription application, which is considered equivalent as removal of the (U)SIM. It was agreed that for multiple subscriptions, each would need independent data and applications. It was agreed to list the security issues identified in a response LS to T WG3 including pointing out that no compelling security reason implies the ruling out of Case 1a. **C. Blanchard agreed to create a draft LS for consideration at the SA WG3 meeting #22 (Bristol) in TD S3-020033.**

TD S3-020010 LS (from RAN WG2) on START value calculation. Ericsson had provided a draft response to this in TD S3z020035.

TD S3z020035 [draft] Response to the LS from RAN2 on START value calculation (response to S3-020010). It was agreed that this response would be discussed and approved over e-mail on the SA WG3 list, led by D. Castellanos. Schedule: Distribution to e-mail list for comment Monday 4 February. Comments following Monday 11 February - Revised version available Tuesday 12 February, for final e-mail approval Friday 15 February.

5 IETF

5.1 Report from the IETF meeting in December (Salt Lake City)

TD S3z020021 IETF #52 status report. This was introduced by Ericsson. The IETF has proposed that 3GPP define a new body to transport 3GPP-specific information which would bring greater independence from the IETF work. This would result in a larger SIP messages. The Bis version of RFC SIP is being produced and a serious look at the security parts in Bis is being taken in order to ensure that the IESG passes the standard. The report was then noted.

5.2 3GPP related IETF drafts

TD S3z020034 Correspondence from CN Chairman. This is the report of the IETF#52 meeting from the TSG CN Chairman and was introduced by Ericsson. An RFC number is expected to be allocated on 7 March for SIP Bis, which will allow TSG CN to add the references into their specifications at the Plenary for Rel-5 specification finalisation. EAP for AKA was not considered by the IETF as stable enough and other, simpler mechanisms (e.g. HTTP Digest) could be used. This letter was then noted.

TD S3z020009 Results of a conference call with IETF ADs and SIP WG chairs regarding IMS security. This was presented by Ericsson. SA WG3 were asked to consider the information provided and to make decisions regarding progressing 33.203, in particular to decide if the suggested protocols satisfy the security requirements and any issues this raises, in order to provide early guidance to CN WG1 and CN WG4. Ericsson proposed the use of HTTP Digest for AKA, as recommended by the IETF. Also, the proposal from the IETF meeting #52, that 3GPP define a new body was recommended as a good way forward by Ericsson, which could solve the Key transport issue. It was reported that CN WG1 are currently working on the development of a new body, and this should be available for June 2002. The development of this new body, for transport, was considered a CN WG1 issue.

It was concluded that the removal of EAP from the requirements in 33.203 would remove the implication for development of Stage 3 EAP work. It was agreed to recommend this course of action to SA WG3 meeting #22 (Bristol) and also to recommend to CN WG1 to follow the IETF recommendations for AKA transport using HTTP Digest. It was decided to draft an LS to CN WG1 and CN WG4 informing them of the changes agreed in the ad-hoc for approval by e-mail on the SA WG3 list. D. Castellanos (Ericsson) agreed to draft this LS (TD S3z020040). Schedule: Distribution to e-mail list for comment Monday 4 February. Comments following Monday 11 February - Revised version available Tuesday 12 February, for final e-mail approval Friday 15 February.

End to end security between S-CSCF and P-CSCF: It was considered that this is not required, as the security will be provided by NDS/IP in the 3GPP context.

6 SIP signalling protection

6.1 Integrity

TD S3z020008 Reflection attacks in IMS. This was introduced by Vodafone and proposed to add a direction bit to the integrity check to provide robust and future-proof protection against reflection attacks.

TD S3z020030 Anti-Replay Protection for the SIP-level Security Solution. This was introduced by Nortel Networks and proposed adjustments to the behaviour of the IMS UE and P-CSCF to accomplish anti-replay protection at the SIP-level. (Comments from Siemens to this contribution were provided in TD S3z020037 and proposed enhancement, taking later agreements in the IETF meeting into account, was included TD S3z020042).

TD S3z020042 Updates from IETF to SIP-Level Solution for IMS Integrity. This was introduced by Nortel Networks and updates the information given in TD S3z020030 to "*reflect the agreements reached since IETF#52 among those parties that seek to enhance HTTP Digest such that it is a viable solution mechanism for SIP message integrity in the IMS*".

It was commented that replay protection mechanism which does not introduce extra messages / round trips in the call set-up would be desirable, and such a mechanism should be investigated.

TD S3z020037 Comments and questions on the revised anti-replay protection scheme for the SIP level integrity solution in TD S3z020030. This was introduced by Siemens and outlined the required clarifications and open issues, and questioning some of the points in TD S3z020030.

Nortel Networks agreed that some of the issues raised had not been considered by the IETF editing group, and undertook to take the comments into account and try to bring a finalised version to the SA WG3 meeting #22 (Bristol). It was hoped that the draft RFC would be publicly available by then (i.e. it is expected to be submitted to IETF in advance of their next meeting) and that some form of Profiling could be done for 3GPP requirements. All delegates were asked to make an effort to ensure early availability of the RFC.

TD S3z020011 Unprotected re-registration during SA lifetime. This was introduced by Nokia and discussed whether or not unprotected re-registration should be permitted. Vodafone had provided a contribution which conflicted with this proposal in section 7 of TD S3z020006 which was considered.

> TD S3z020006, section 7: This was introduced by Vodafone and suggests that the network should clear the registration if the integrity check repeatedly fails at the P-CSCF (in the case of a lost SM8). Recovery can be achieved only by treating the registration as a new registration and performing authentication.

It was generally concluded that there may be a need to allow unprotected re-registrations, but that protection against associated attacks requires further examination. Suitable policies for handling re-registration requests from both P-CSCF and UE needs to be put in place.

Delegates were asked to continue this discussion over e-mail in order to come to a generally acceptable solution for the SA WG3 meeting #22 (Bristol). **A. Escott was asked to lead this discussion based upon the contributions in this ad-hoc on the subject**.

TD S3z020016 On integrity protecting SIP-signalling in IMS: See discussion below.

TD S3z020010 Primary choice between IPsec and SIPsec: See discussion below.

TD S3z020036 Integrity protection for SIP messages in the IMS at network or application layer? See discussion below.

> Discussions on moving SIP security into the main body of 33.203 and leaving the IPSec solution in the Annex for a fall-back solution took place. The progress of the SIP security draft was questioned, as there did not seem to be any visible progress (indeed it had been withdrawn into a editing group in the IETF with a reported target for completion of the draft SIP Bis in February 2002, in order to meet the submission deadline for the IETF. As there were differences of opinion on this from different companies, **it was decided to leave this decision until the SA WG3 meeting #22 (Bristol) in order to base the decision on the SA WG3 "preferred solution" upon progress on the two drafts made by that time.**

TD S3z020017 Requirements on SA_ID. This was postponed to the SA WG3 meeting #22 (Bristol). Delegates were asked to consider this in the meantime and comment on e-mail if necessary.

TD S3z020029 Set-up Procedures for the SIP-level Security Solution. This was postponed to the SA WG3 meeting #22 (Bristol). Delegates were asked to consider this in the meantime and comment on e-mail if necessary, in particular on the proposed use of elements for the SA.

6.2 Confidentiality

TD S3z020018 Editorial changes to TS33.203v100.

TD S3z020019 The need for confidentiality protection for the first/last hop. This was introduced by Ericsson and discusses the provision of confidentiality for the first and last hop for the Rel-5 timeframe. It proposes a working assumption that SIP signalling is only integrity protected for Rel-5 and provided a roadmap for SA WG3 to follow. It also proposed that the Security Mode set-up procedure should still take encryption into account, utilising NULL encryption for Rel-5. The assumption for the use of S/MIME in Rel-6 was questioned. It was decided that such discussions need to take place at a later date and any assumptions made by SA WG3 at this time would not include the use of a S/MIME solution. It was concluded that confidentiality is not needed for SIP signalling between the UE and P-CSCF for Rel-5, since the USer Plane is not confidentiality protected. This will be sought for future Releases.

TD S3z020020 SIP layer confidentiality between UA and P-CSCF. This was covered by discussions on TD S3z020019 and was noted.

7 ISIM

A Liaison Statement from T WG3 was provided in TD S3z020033 which was dealt with under agenda item 4.

8 Further contributions to TS33.203v100

TD S3z020004 Pseudo-CR to 33.203 v1.0.0: Incorporation of Integration Guidelines for R5 into TS33.203. This was postponed to the SA WG3 meeting #22 (Bristol). Delegates were asked to consider the usefulness of the inclusion of integration guidelines material in 33.203, for Rel-5.

TD S3z020006 Proposed changes to 33.203. (Section 7 of this contribution was considered under agenda item 6.1 with TD S3z020011). This was postponed to the SA WG3 meeting #22 (Bristol). Delegates were asked to consider this in the meantime and comment on e-mail if necessary.

TD S3z020007 Maximum number of requested authentication vectors. This was introduced by Vodafone and discusses the maximum number of Authentication Vectors that can be requested and stored. It discussed the issue and suggested some preliminary maximum values. The meeting did not feel that this required specification, but if CN WG4 requested this for any technical reason then this would be considered and decided upon in SA WG3 and then communicated to CN WG4.

TD S3z020027 Need for section 7.3.3. This was postponed to the SA WG3 meeting #22 (Bristol) due to lack of time.

TD S3z020031 Network Handling of Untrusted IMS Clients. This was briefly introduced by Nortel Networks and recommends SA WG3 to consider the threats posed by untrusted IMS clients and discuss the mitigation solutions to standardise. Delegates were asked to consider these issues and what, if anything, can be done for Rel-5 in the time frame.

9 AOB

There were no contributions under this agenda item.

10 Closing of the meeting (February 1st at 16:00)

Documents not dealt with at the meeting, due to lack of time. Postponed to Bristol meeting:

TD S3z020006 Proposed changes to 33.203. (Section 7 of this contribution was considered under agenda item 6.1 with TD S3z020011).

TD S3z020017 Requirements on SA_ID.

TD S3z020029 Set-up Procedures for the SIP-level Security Solution.

TD S3z020004 Pseudo-CR to 33.203 v1.0.0: Incorporation of Integration Guidelines for R5 into TS33.203.

TD S3z020006 Proposed changes to 33.203.

TD S3z020027 Need for section 7.3.3 (in 33.203).

The Chairman thanked Alcatel for providing the arrangements for the ad-hoc meetings, thanked delegates for their co-operation and work during the meetings and closed the meeting.

3GPP TSG SA WG3 Security #21bis — MAPSEC/NDS ad-hocs **version 1.0.0**

31 January, 2002

Antwerp, Belgium

Source: **SA WG3 Secretary**

Title: **Report of MAPSEC and NDS/IP ad-hoc**

Status: **Approved at SA WG3 meeting #22**

1 Opening of the meeting (9:00)

The meeting was opened by V. Niemi, SA WG3 Vice Chairman, and outlined the schedule for the ad-hoc meetings.

Olivier Paridaens welcomed delegates to Antwerp, Belgium, on behalf of Alcatel, and provided domestic arrangements for the ad-hoc meetings.

2 Approval of the agenda

TD S3z020002 Draft agenda for MAPSEC and NDS/IP ad-hoc meetings. The agenda was reviewed, agenda item 6.7 "Release 6 issues" and was then approved.

3 Allocation of the input documents

TD S3-020008 and TD S3-020016 for the SA WG3 meeting #22 (Bristol), were allocated to MAP/NDS agenda item 5.1.

4 Report from SA#14

The relevant part of the report from SA #14 (section 7.3.3) was reviewed, where separate CRs for the Release 5 version of MAP Security was requested. Also it was noted that TSG CN had reported that the Ze interface specification work in CN would not be complete by March 2002.

5 MAPSEC issues (handled until no later than 13:00)

5.1 Relevant LSs

TD S3-020008 LS on MAPsec error handling (response to S3z010121). This was presented by Siemens. It was noted that CN believe the messages protected are consistent with flows given in 33.200CR007. The problem reported on DoS attack scenarios had already been identified and considered by SA WG3, and protection against this had been considered too expensive for the gain achieved (similar attacks will still exist if this is protected against). The stable draft of TS 33.200 was available after the SA#14 meeting (noted as version 1.0.0).

TD S3-020016 Liaison statement on Protocol Specification of the Ze interface. This was presented by Vodafone and requested time during the SA WG3#22 meeting (Bristol) for discussion with CN WG4 experts on the Ze interface. It was, unfortunately, too late for the proposal for SA WG3 experts to attend the CN WG4 meeting, but it was agreed that this would be useful and some time during the meeting should be allocated (host needed contacting to determine the best slot for this). A response LS to CN WG4, responding to the LS in TD S3-020008 and TD S3-020016 was provided in TD S3z020028. This was modified slightly and re-provided in TD S3z020038 which was approved. **(Note that this carries a footnote explaining the status of the LS, which needs final approval on the SA WG3 e-mail list)**.

5.2 Status of 33.200 Rel. 5

TD S3z020023 Latest version TS 33.200 Rel-5. The MAP Rapporteur provided this for information and shows the proposed Release 5 version of MAP Security with change bars from the Release 4 version. The current version was noted. See the discussion on structuring the CR(s) under agenda item 5.3.

5.3 How to structure CRs proposed to SA#15

TD S3z020023 Latest version TS 33.200 Rel-5. The MAP Rapporteur provided this for information and shows the proposed Release 5 version of MAP Security with change bars from the Release 4 version. This was the proposal for a single CR to TSG SA for approval and production of Release 5. It was argued that if several separate CRs were produced, then there was a need for all CRs to be approved, as they were mainly relying on each other. As TSG SA had requested a set of functionally separate CRs to produce Release 5, this possibility was investigated. It was concluded that the changes could be split into around 7-8 parts, but that they would not be really separate, and the process was rather artificial. e.g. KAC affects Ze and Zd interfaces, and these changes would all need to be approved or rejected together. After some discussion it was agreed that a single CR was the only practical way forward, as if any parts were not approved, then none of the changes should be included as the document would then be incomplete. **A cover document will be created by the MAP Security Rapporteur, explaining the reason for a single CR and the dependencies of the changes, for inclusion with the CR to TSG SA Plenary**.

5.4 Ze interface

TD S3z020013 Proposed additions to 33.200 about COPS usage in Ze interface for Local Security Association and Policy Distribution. This was introduced by Nokia and proposed an additional section 8.2 concerning Local Security Association and Policy Distribution in the Ze interface, using the COPS protocol. The exact COPS message content would need to be developed by CN WG4. The detail of the proposal was presented by Nokia and some issues were discussed:

Dependencies upon IETF work. It was suggested that COPS extension may be required to be done in the IETF. It was suggested that 3GPP could produce the COPS specification for MAP security and input it to the IETF for information.

It was agreed that this contribution should be re-submitted to the joint session with CN WG4 experts at the SA WG3#22 meeting (Bristol).

TD S3z020024 Secure connection between KAC and NE. This was introduced by Alcatel and discussed the need for a mandatory protected connection between the KAC and NEs. The proposed changes were approved and the MAPsec Rapporteur was asked to include it in the Rel-5 changes CR. Some text was recognised as needed for clause 8, in order to mandate the protection of trigger messages. It was also suggested that "protection in this context did not imply encryption, in the case of physical proximity protection of the elements, however, the Introduction to the Specification states that the techniques .are based upon cryptographic techniques, so both these sections were also in need of modification to clarify the situation in line with the changes to section 8. It was generally agreed that the protection of the internal interface is optional, and each operator may decide how to protect his own internal network. It was finally agreed that the issue needed more consideration and discussion than was available at the ad-hoc, and an e-mail discussion, based on a proposed text from the Rapporteur would take place the following week in order to finalise the text for the SA WG3 meeting #22 (Bristol).

NOTE: Changes are considered appropriate for Rel-5 only, not reflected back into Rel-4.

5.5 MAPSEC DoI

D. Castellanos (Ericsson) provided a verbal progress report on progress. There is to be a submission after a presentation in December - work ongoing after this meeting and an updated version is likely to be submitted to the IETF for comments, and then it will be provided to the SA WG3 meeting #22 (Bristol).

5.6 Other technical issues

The Chairman raised the issue of the "dialog portion", as there are some MAPsec items which do not contain this dialog portion. Protection of the dialog portion would lead to two security headers in the MAP message. Also, adding such messages for protection will require an analysis of the method of protection for them. This could give problems for CN WG4 for inclusion in the protected messages list.

These issues were recognised as being post Rel-5 issues. It was concluded that these issues could be discussed with CN WG4 in the joint session in Bristol. Nokia were asked to provide a contribution discussing these issues to the Bristol meeting, after discussion with CN WG4 experts.

6 NDS/IP issues (handled until no later than 15:30)

6.1 Relevant LSs

There were no contributions under this agenda item.

6.2 Status of 33.210

TD S3z020005 Draft TS 33.210 v 1.0.1. This was briefly introduced by the Rapporteur, he reported that IPsec input was still outstanding. The IP version for the SEG-SEG interface may need specification in order to avoid interoperability problems. It was agreed to remove the editors note, acknowledging that this is an issue which is out of the Scope of this specification.
Annex C: The SCTP protocol may be used as an alternative to TCP, but protection of this presents additional challenges. The IETF is aware of this and a draft RFC is available which proposes a solution to this problem. It was suggested that this could be included as information in the text (as it is unlikely that full material will be available for the Bristol meeting) as notes on the transfer of DIAMETER using SCTP. A proposal was provided in TD S3z020015.

TD S3z020015 On Use of IPSec for SCTP. This was introduced by Ericsson, and suggested some text to cover SCTP to transfer DIAMETER messages over the Cx interface, referring to the draft RFC. This proposal was agreed and the Rapporteur was asked to add the agreements reached at this ad-hoc for the SA WG3 meeting #22 (Bristol).

TD S3z020012 Comments to 33.210 v1.0.0: IP network layer security. This was introduced by Siemens and each proposed changed was considered. the comments and agreed modifications to the proposals were noted by the Rapporteur, who agreed to update the draft 33.210 to include this information and distribute it for the SA WG3 meeting #22 (Bristol).

NOTE to Rapporteur: (Geir): The final change to Annex C was discussed. The proposed changed were not agreed and the text re-instated as before. It was, however, agreed to delete the words: "such as Mm, Mk, Mg and Sr" .

6.3 AES issues

There were no contributions under this agenda item.

6.4 Zb/Zc merging

TD S3z020025 SA mode in Zb interface. This was introduced by Alcatel and pointed out some contradictions in the document in specifying the use of tunnel mode towards a SEG, whereas the possibility to use transport mode is also allowed in some situations (between NEs in the operators own network). The contradiction pointed out in the contribution was recognised by the group, however, no agreement on whether to mandate tunnel mode only instead of generalising with the use of the SA terminology, as proposed in the contribution, could be reached in the limited time available. **It was therefore agreed that this should be the subject of contribution to the SA WG3 meeting #22 (Bristol) for a decision and resolution of the contradiction**.

6.5 Relation to 33.203

There were no contributions under this agenda item.

6.6 Other technical issues

There were no contributions under this agenda item.

6.7 Release 6 issues

TD S3z020022 A proposal for evolution of Network Domain Security for Release 6 – Introduction of an authentication framework. This was provided for information and proposes an enhancement to a WI. The document was noted and delegates asked to review this for contribution to the SA WG3 meeting #22 (Bristol).

7 Review of output documents

Output Liaison: S3z020038: LS to CN WG4 on joint session on Ze interface. To: CN WG4.

8 AOB

There were no contributions under this agenda item.

9 Closing of the meeting

The Chairman thanked the hosts for the meeting arrangements, and the delegates for their hard work and co-operation during the meeting and closed the meeting.