3GPP TSG SA WG3 Security — S3#13 **S3-000311**

23-26 May, 2000

Yokohama, Japan

3GPP TSG SA WG3 Security — S3#12 **Draft Report**

11-14 April, 2000, Stockholm, Sweden

Source: **Secretary**

Title: **Draft Report Version 0.0.2**

Document for: **Comment**

Stockholm waterfront

Contents

1 Opening of the meeting

The SA WG3 Vice Chairman, Mr. S. Pütz, Chaired the meeting in the absence of the SA WG3 Chairman, Mr. M. Walker. Mr. Pütz opened the meeting and Mr. R. Blom, Ericsson, welcomed delegates to Stockholm and explained the domestic arrangements. A Social Dinner had been planned for the Evening of the Tuesday (19.00 start).

2 Objectives of meeting

The Chairman outlined the meeting objectives and schedule, provided in TD S3-000266.

- Content and schedule for Release 2000 Security work.
- 3GPP/3GPP2 Security Harmonisation discussions to come to common agreement for the meeting with TIA TR-45 (AHAG) on 12 April 2000.
- 2G Security issues - GPRS encryption and A5/2 algorithm.
- Finalisation of remaining Release 1999 security issues
- Start work on Release 2000 security issues.

3 Approval of the agenda

The Draft Agenda, given in TD S3-000215 was considered and the scheduling discussed. It was then approved without change.

4 Registration and assignment of input documents

The documents available at the start of the meeting were allocated to their appropriate agenda items.

5 Approval of meeting report from S3#11

The report from SA WG3#11 version 0.3.0, provided in TD S3-000216 had been distributed by e-mail for comment. It was further commented upon in the meeting and some minor changes made. The updated report, version 1.0.0 was then approved (available on the 3GPP FTP server, SA WG3 area).

The List of actions from the previous meeting were checked, Action 11/5 was outstanding, 11/10 was partially completed (comments to Mr. G. Køien). All other actions had been completed.

6 Reports / Liaisons from other 3GPP and SMG groups

6.1 3GPP and SMG plenary

TD S3-000229 Draft Report of TSG SA Meeting #7 - version 0.0.1. The Chairman highlighted the items from the Plenary of concern to SA WG3 using TD S3-000230 "Notes on S3 presentation at SA#7" and TD S3-000234 (presentation slides).

- Liaison with N1 is needed on the value of integrity checking for Emergency Calls.
- SA WG3 was asked to clarify the terminology of R98- and R99+ used in their specifications.
- TSG SA formally approved the 3GPP cipher and integrity protection algorithm.
- The need to have a standardized UMTS authentication algorithm was approved. To be developed by ETSI SAGE, subject to funding confirmation.
- Authentication failure notification: MS behaviour on authentication failure is still open. Authentication failure notification was allowed for late inclusion in Release 1999 if completed by CN#8/SA#8.
- MAP Security and EUIC were agreed to be moved to Release 2000, so SA WG3 need to remove these features from the Release 1999 Specifications with CRs and to re-insert them into the new Release 2000 specifications with more CRs. A proposed procedure was to create the Release 1999 version (3.5.0) with the agreed Release 1999 features and then to create an equivalent Release 2000 specification (version 4.0.0). This will then be updated via CRs to include the full agreed Release 2000 features. (i.e. in this way V3.5.0 = V4.0.0). Some discussion over the formalities of updating the specification with CRs at the same SA Plenary as the Release 2000 version 4.0.0 is approved took place.

At the end it was proposed to request TSG SA for a two step approval procedure: First to present CRs related to Release 1999 to remove MAP Security and EUIC at TSG SA#8. This will result in TS 33.102 version 3.5.0. After plenary approval of these CRs S3 will present in a second step also at SA#8 a set of other CRs related to R00. Approval of this set of CRs would produce TS 33.102 version 4.0.0. After TSG SA#8, both versions will be produced by MCC. If SA WG3 can explain the benefit of this procedure to TSG SA, it should not become a problem to get it approved (full visibility is given).

SA WG3 therefore need to create CRs to produce the Release 2000 version at the same time as the CRs to remove MAP Security and EUIC from the current Release 1999 version (version 3.4.0). These CRs should then be further discussed by SA WG3 and enhanced to include any additional security required for Release 2000. It should be noted that TSG CN need the Security requirements very soon, in order to avoid the non-inclusion in Release 2000 due to lack of time. Therefore, SA WG3 could assume that the CRs to Release 1999, removing MAP Security and EUIC will be approved at TSG SA#8 and produce CRs to an expected version 3.5.0 for approval at TSG SA#8.

6.2 3GPP WGs and SMG STCs

TD S3-000225: Reply to Location of conversion functions c2 and c3. This was provided for information and noted.

TD S3-000235: Liaison Statement to TSGs on Enhanced User Identity Confidentiality. This LS was noted.

TD S3-000239: Draft Meeting Report of CN WG2 (SA WG3 experts invited). This was provided for information and noted.

TD S3-000223: LS on Open Service Architecture - Security. Delegates were asked to check if they have any problems with the document.

ACTION #12/1: All to check the OSA Security document TD S3-000223 and contribute any security problems or issues to the May 2000 meeting of SA WG3.

TD S3-000218: USIM triggered authentication and key setting during PS connections. CN WG1 do not feel they can complete the work on this for Release 1999 but will consider it for Release 2000. This was noted and the topic was included in the Release 2000 work plan considerations.

TD S3-000217: Liaison response to S3's LS (S3-000190) on Functions of Key Distribution and Key Administration for MAP security. This was provided for information and noted.

TD S3-000224: Answer to LS on Functions of Key Distribution and Key Administration for MAP security. SA WG2 state that there is no impact on Release 1999 work if key update frequency is in the order of weeks or months. Some discussion took place on the validity of the frequency of key updates assumed by SA WG2, and also whether this referred to single network Key updates or complete updates of all roaming partners keys. This was postponed to the MAP Security ad-hoc meeting at SA WG3 #13 (see also the discussion under MAP Security, below).

TD S3-000226: Liaison statement to TSG-S WG3 on GTP Signalling Security. CN WG2 asked SA WG3 to answer the following questions by their meeting 22-26 May 2000:

- Is IPSec the **only** protection mechanism to be used for GTP signalling?
- Is protection required for both GTP User plane and GTP Control plane signalling?

More detail on the CRs to 29.060 mentioned in the liaison were needed in order to understand the meaning of the liaison. As SA WG3 have not yet defined the GTP Security requirements it was argued that CN WG2 should not be defining protocols for this at this time. This was postponed to the MAP Security ad-hoc meeting at SA WG3 #13 (see also the discussion under MAP Security, below).

TD S3-000164: LS from SMG9 to SA WG3 (and SA WG1) on New SIM toolkit feature: "Auto-answer & Mute-ringing". This was presented to the meeting. A response to this LS from SA WG1 was provided in TD S3-000264. This implies some disadvantages regarding privacy with this feature, and will be reviewed by SA WG1, but is not seen as a requirement at present. SA WG1 requested contributions on this in order to decide if it should be included in a Release. SA WG3 were asked for their opinion. It was discussed and concluded that this would allow eavesdropping on users, but activating the mobile without the users knowledge and is against the principles of security.

TD S3-000265: Around Auto-answer. This discusses the Auto-answer proposal, which asks for the feature to be included in SIM Toolkit, and states that this is already a feature of TDMA and mobile "headsets" (hands-free adapters) which allow auto-answer of incoming calls. It argues that the eavesdropping threat is not real, as the incoming call identity (CLI) is used for screening the callers which are auto-answered. The security level of the CLI was questioned, as visited networks can modify the CLI before forwarding to the MS.

It was concluded that the potential security problems and threats override the advantage of such a feature. If such a feature is requested, then it should be included in SA WG3 as a new security concept for study. A response Liaison statement from SA WG3 to SMG9 was prepared and presented in TD S3-000270 which outlines the security problems with use of CLI for authentication and that SA WG3 will consider the security requirements of this feature if it is a requirement of SA WG1.

6.3 3GPP partners

No input.

6.4 Others (GSMA, GSM2000, T1P1, SAGE, TIA, TR-45)

TD S3-000237: DRAFT LS to GSM-A on Authentication Algorithm. It was reported that there had been no early discussion and agreement on funding and progress had been delayed. The GSM Association Security Group and SA WG3 were asked to co-ordinate their work in future to prevent such problems. It was clarified that the GSM Association have regular liaison with GSM 2000. As there had not been a GSM Association SG meeting, this liaison had not yet been responded to by the GSM Association SG.

TD S3-000236: Work plan for the design of the 3GPP Authentication Algorithm (MCC Task Force). The minutes of the GSM 2000 meeting, where the A5/3 algorithm production was discussed are provided in TD S3-000271. A preference for basing the new A5/3 algorithm on Kasumi was expressed. These documents were noted.

7 Work item management: New work item structure as defined by SA

Mr. M. Pope, MCC, presented TD S3-000278, TD S3-000279 and TD S3-000280. The Features, Building Blocks and Work tasks were discussed and it was agreed that the Work Plan in TD S3-000281 could be used as a starting point for feedback to SA WG2 on 17 April. There was a problem with reviewing the document and cross-mapping it into the proposals from SA WG2 IGC proposals in time. It was agreed that the updated Work Plan (TD S3-000305) should be used by the Security IGC for inclusion in the overview document.

8 Content and schedule of R00 security work

TD S3-000247, TD S3-000248, TD S3-000249.

Unfortunately, nobody was available from SA WG2 to give a presentation of the current thinking on Release 2000 Network Architecture, however, Mr. P. Howard provided a short summary of the available documents.

TD S3-000248: Release 2000 QoS Key Issues. This document provided for consideration with TD S3-000247 and was noted.

TD S3-000247: Key issues for Release 2000. This document provided the Key Issues list from SA WG2 ad-hoc group and was noted. It should be considered by SA WG3 delegates.

TD S3-000249: Draft TR 23.821 v0.2.0 “Architecture Principles for Release 2000”. This document was provided for information for consideration with TD S3-000246 and was noted.

TD S3-000246: TR 23.821 V0.12.0: Architecture Principles for Release 2000. This provides a general Network architecture and should be considered by SA WG3 delegates. The document was noted.

TD S3-000244: Draft R2000 Project Plan for Security v0.0.2. SA WG2 have started producing draft project plans for Release 2000, and this document provides the Security Project Plan. It includes the Features, Building Blocks and Work Tasks, which were later introduced under Agenda Item 7. It was suggested that SA WG3 concentrate on the Work Tasks and assign Rapporteurs and consider setting up of small Working Parties, if necessary, for some of the larger work tasks.

After some discussion it was agreed that Mr. P. Howard would update the document for further discussion later in the meeting. This was done and document TD S3-000281 was presented along with an update on rejection of unencrypted calls, provided in TD S3-000301 which was agreed to be included. Some modifications were made to the document and the new version provided in TD S3-000305. It was proposed that this document is attached to the LS to SA WG2 in TD S3-000300 (see below).

ACTION #12/2: C. Brookson to contact SMG10 WPD Chairman to ask him to produce a WI description sheet for Lawful Interception for Release 2000.

TD S3-000300: Proposed LS on R00 working methods. This Liaison was approved and TD S3-000305 will be attached and sent to SA WG2.

ACTION #12/3: Secretary: TD S3-000300 (with TD S3-000305 attached) to be sent to SA WG2.

The use of TD S3-000305 for updating the SA IGC table on Security WIs was proposed. It was decided that the Security IGC would be asked to use this document as a basis for filling in the table.

A list of open issues from TSG SA#7 was provided in TD S3-000238, which was noted.

MAP Security:

The timing of the MAP Security for Release 2000 was discussed. TSG SA had asked SA WG3 to produce the CRs (at least for Layer III) for approval in June 2000 so that other groups can complete their work in good time. It was proposed to set up an ad-hoc group on Core Network Signalling Security, and was further suggested that such an ad-hoc should meet at the time of SA WG3 Plenary (e.g. by reducing plenary by one day and holding the ad-hoc the day before). Another suggestion to add one day to the SA WG3 Plenary and reserve a day for ad-hoc meetings. This suggestion was taken and it was arranged after the meeting to hold a 1-day MAP Security ad-hoc meeting after SA WG3 #13, in Japan and also after SA WG3 #14 in Norway.

9 Review 3G security project plan

This was dealt with under agenda item 8, above.

10 Joint session with TIA TR-45 AHAG on 3GPP/3GPP2 harmonisation

TD S3-000232: Draft agenda for joint session with TIA TR-45 AHAG on 3GPP/3GPP2 security harmonisation. The agenda was considered before the joint meeting to determine what preparation SA WG3 needed to do before the meeting. Under the agenda item 6.1: "Joint control of 3GPP AKA specifications" for this meeting, the SA WG3 requirements were discussed. One solution would be to extract the AKA parts of the specification for joint maintenance by the two groups. Another would be to identify the sections which are under joint responsibility and ensure that both groups are aware of proposed change requests. This could be done via liaison rather than formal procedures. It was requested that corrections should not be delayed by unnecessary bureaucracy and should proceed quickly, and that only proposals for functional changes to AKA should be fully approved by both Projects.

TD S3-000309 Liaison statement on HE initiated cancellation of AV in SN: Liaison to AHAG to clarify the revocation of vectors mechanism. The liaison was approved.

ACTION #12/4: Chairman: TD S3-000309 to be sent to TR-45 AHAG.

11 2G security issues

The report on the GSM discussions are included in the report provided in the SMG10 area of the ETSI SMG FTP server. http://docbox.etsi.org/tech-org/smg/Document/smg10/plenary/SMG10-reports/2000.

Action Points #12/5 to #12/12 are allocated under this agenda item.

12 3G security issues

12.1 Algorithms

The need for a test algorithm for 3GPP authentication was discussed. TS 34.108 requires updating for 3GPP as it is currently based upon GSM algorithm. Ericsson have proposed a test algorithm clause for this, which will be presented to T WG1 for approval at their meeting the following week. SA WG3 were asked if they would like to have input on this. SA WG3 did not need to see this proposal, but should review the test specifications in general to ensure that the security functions are covered by them. SA WG3 would like to review the test algorithm at the May 2000 meeting.

ACTION #12/5: TS 34.108 to be forwarded to M. Pope for distribution to the SA WG3 list to review and comment to the next SA WG3 meeting.

TD S3-000282: Final document on the Evaluation of the 3GPP Confidentiality and Integrity algorithms. An error in Figure 6 was noted and the report will be updated for consideration for publication at the next SA WG3 meeting.

SA WG3 were asked by AHAG at the joint meeting to inform ETSI SAGE that TR-45 have decided to use SHA-1 for the default local authentication algorithm in 3GPP2 and ask them to also consider this as a candidate for 3GPP.

12.2 Review of other specifications

TD S3-000251: Review of TS 24.008. A list of inconsistencies had been identified and detailed in this document. Two proposed CRs to 24.008 were provided in this contribution to correct the problems found.

ACTION #12/6: B. Vinck to forward the proposed changes to CN WG1 colleagues for discussion and action in CN WG1.

Two open issues were identified (VLR and SGSN behaviour on MS reject of authentication token and MS indication of synchronisation failure to the network). These issues need specification in 33.102 before they can be included in 24.008. This should be done via e-mail discussion.

ACTION #12/7: P. Howard to set up e-mail discussion on open issues. All: to consider the open issues and make proposals to SA WG3 in time to provide proposals to CN WG1 on 24.008 (deadline for all changes to 24.008 and 33.102, Release 1999 specifications is June 2000).

<<Ger to draft text for inclusion in LS on impact of Positive acknowledgement of authentication success ?? >> Complete this!!

12.3 Open R99 security issues

The review of other groups' specifications is ongoing. B. Vinck agreed to continue his review to ensure security requirements are included.

TD S3-000242: Identifying specifications that implement “Secure UMTS-GSM Interoperation”. This contribution, from Ericsson, was noted. Ericsson offered to proceed with the work of reviewing the affected specifications.

12.4 R00 security issues

CN WG4 and SA WG5 have requested that SA WG3 finalise the security requirements for Release 2000 as soon as possible in order for them to complete their work in time for the Release 2000 deadline. The MAP Security work should be reviewed by SA WG3 delegates after this meeting and contributions made on Layer 1 and Layer 2 Security for Release 2000 at the May 2000 meeting.

13 Review of (draft) S3 specifications

13.1 TS 21.133 Threats and requirements

There were no contributions for this TS.

13.2 TS 22.022 Personalisation of ME

There were no contributions for this TS.

13.3 TS 33.102 Security architecture

TD S3-000268: CR 092: "Removal of enhanced user identity confidentiality". This CR was approved.

TD S3-000269: CR093: "Removal of network domain security". This CR was approved.

TD S3-000263: CR 091: "Inclusion of the radio bearer identity to the integrity mechanism". This CR was approved and it was agreed to forward it to RAN WG2.

TD S3-000262: CR 090: "Clarification of BEARER and DIRECTION parameters". This CR was approved and a corresponding CR to 33.105 will be produced by Nokia.

TD S3-000295: CR 088: "Initialisation of synchronisation for ciphering and integrity protection". This CR was approved and it was agreed to forward it to T WG3 and RAN WG2.

TD S3-000261: CR089: "Addition of another variant of sequence number generation". This CR was approved.

TD S3-000291: This CR was postponed to Meeting #13. Delegates are asked to consider this proposal before the meeting in terms of it's acceptability and whether the solution will pass export controls.

TD S3-000293: CR 083: "Authentication and key agreement (minimal)" This CR was approved.

TD S3-000257 and TD S3-000256 were withdrawn. Work is ongoing in 25.331 and consistency of the work should be verified before presenting these CRs.

TD S3-000294: CR084: "Conversion functions for GSM-UMTS interoperation". This CR was approved.

TD S3-000253: CR on "Authentication and key agreement (editorial)" concerning Better presentation of the mechanism for authentication and key agreement, was presented for information. Delegates were asked to check the need for the restucturing proposed in the CR for Release 1999 and/or Release 2000.

ACTION #12/8: Delegates to check the need for restucturing proposed in the CR in TD S3-000253 for Release 1999 and/or Release 2000.

TD S3-000292: CR094: "Cipher and integrity key update once every 24 hours". This CR was approved.

TD S3-000289: CR096 " Clarification on the HFN handling". The order of preference was proposed for removal from this CR. This was done and the CR was approved.

TD S3-000290: CR 081: "Clarification on the UIA and UEA selection". This CR was postponed and delegates were asked to investigate the impact of the proposals and contribute to the next meeting. An e-mail discussion will be set up for this item.

TD S3-000288: CR 080: "Clarification on ciphering and integrity protection at intersystem handover". This CR was approved.

TD S3-000302: CR 095: "Handling of emergency call": This CR was approved.

13.4 TS 33.103 Integration guidelines

There were no contributions for this TS.

13.5 TS 33.105 Algorithm requirements

There were no contributions for this TS.

13.6 TS 33.106 LI requirements

There were no contributions for this TS.

13.7 TS 33.107 LI architecture

There were no contributions for this TS.

13.8 TR 33.120 Security principles and objectives

There were no contributions for this TR.

13.9 TR 33.900 Guide to 3G security

TD S3-000181: TR 33.900 V1.3.0. This was presented by C Brookson and noted. SA WG3 are asked to input any comments to Mr. C Brookson. This document is expected to be approved for presentation to TSG SA as version 2.0.0 in the May 2000 meeting of SA WG3.

13.10 TR 33.901 Criteria for algorithm design process

There were no contributions for this TR.

13.11 TR 33.902 Formal analysis

There were no contributions for this TR.

14 Approval of output documents

TD S3-000299. This liaison was discussed and details contained in TD S3-000304 were incorporated and the updated document provided in TD S3-000307.

TD S3-000283 This Liaison was discussed and it was felt that more investigation into what AHAG want from SA WG3 is required before submitting the liaison. It was agreed to send a liaison to AHAG to clarify this and TD S3-000283 was withdrawn.

TD S3-000287. Withdrawn as a result of TD S3-000283 decision.

TD S3-000297. Proposal on authentication vector generation algorithm for conformance testing. This was dealt with under agenda item 12.1, above.

TD S3-000306: Liaison statement to SMG and CN WG1/SMG3 on GPRS ciphering. This liaison was approved.

TD S3-000308: Liaison statement to CN WG4: Evaluation of the impact on positive authentication reporting on network performance. This liaison was approved.

15 Future meeting dates and venues

TD S3-000298 provides a liaison from CN Chairman asking for a joint meeting between CN WGs and SA WG3 before the next TSG Plenaries (i.e. for May or early June 2000). It was agreed to propose 14-15 June 2000 (Host to be confirmed). This was later revised for 13-14 June 2000 hosted by ETSI in Sophia Antipolis.

ACTION #12/9: Chairman to send the proposed dates for a joint meeting to relevant people.

Meeting	Date	Location	Host
S3 CN Sig. Sec ad-hoc			
S3#13	23 - 26 May 2000	Tokyo	DoCoMo
S3 / CN WGs Joint ad-hoc on Requirements Impacts	13-14 June 2000 (note)	Sophia Antipolis	ETSI
S3#14	1-4 August 2000	Oslo	TeleNor
S3#15 Probably joint with AHAG	Early September 2000	To be confirmed	Host required
S3#16	27-30 November 2000	Israel (TBC)	Motorola (TBC)

NOTE: After the meeting it was decided to hold a joint CN/S3 meeting on 13-14 June 2000, hosted by ETSI in Sophia Antipolis.

TD S3-000284 contained the invitation to the next meeting, in Yokohama, Japan. This was noted.

16 Any other business

There were no additional topics raised.

17 Close of meeting

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

Annex A: List of documents at the meeting

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000215	Draft Agenda for Meeting #12	Chairman	2	Approval		Approved without change
S3-000216	Draft Report of Meeting #11, version 0.3.0	Secretary	5	Approval		Approved with changes (new version 1.0.0)
S3-000217	Liaison response to S3's LS (S3-000190) on Functions of Key Distribution and Key Administration for MAP security	SA WG5	6.2	Information		Noted
S3-000218	USIM triggered authentication and key setting during PS connections	CN WG1	6.2	Discussion		Considers feature as suitable only for R2000. Noted and considered in R2000 discussions
S3-000219	Reply to LS on "Introduction of rejection of non ciphered calls for GPRS"	CN WG1/SMG3	11.1	Discussion		Rejects CR to 04.08 in S3-000058 B. Vinck to draft an LS to CN WG1 and SMG on SMG10 GPRS ciphering agreements, based upon TDs 201 and 205
S3-000220	CR to 33.102: Ciphering (revised TD 128)	Siemens Atea	x	Approval		CR066r1 Approved by e-mail before the meeting for SA#7
S3-000221	CR to 33.102: Data integrity (revised TD 129)	Siemens Atea	x	Approval		CR067r1 Approved by e-mail before the meeting for SA#7
S3-000222	Initiation of COUNT-I and COUNT-C	Siemens Atea	13.3	Decision		Postponed to Meeting#13
S3-000223	LS on OPEN SERVICE ARCHITECTURE - SECURITY	SA WG2	6.2	Discussion		All to check OSA Security and revisit at SA3#13
S3-000224	Answer to LS on Functions of Key Distribution and Key Administration for MAP security	SA WG2	6.2	Discussion		Postponed to SA3#13 MAP security ad-hoc
S3-000225	Reply to Location of conversion functions c2 and c3	T WG3	6.2	Discussion		Noted
S3-000226	Liaison statement to TSG-S WG3 on GTP Signalling Security	CN WG2	6.2	Discussion		Postponed to SA3#13 MAP security ad-hoc
S3-000227	Requirements Specification for the GSM A5/3 Encryption Algorithm version 0.2	ETSI SAGE	11.2	Information	S3-000285	Revised V0.3 in TD 285
S3-000228	CR to 33.900: O&M Access Control and IP network Security	Orange UK	13.9	Approval		Not a CR as not under Change Control (v1.2.0)
S3-000229	Draft Report of TSG SA Meeting #7 - version 0.0.1	Secretary	6.1	Information		Noted
S3-000230	Notes on S3 presentation at SA#7	Chairman	6.1	Information		Noted
S3-000231	SA WG3 "to-do list" for meeting #12	Chairman	8, 12	Discussion / Action		Noted
S3-000232	Draft agenda for joint session with TIA TR-45 AHAG on 3GPP/3GPP2 security harmonisation	Vice-Chairman 3GPP TSG-SA WG3 and Chairman TIA TR-45 AHAG	10	Approval		Approved
S3-000233	TR-45 AHAG AKA Issues	TR45.2 / TR 45 AHAG	10	Discussion		Discussed in joint AHAG meeting

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000234	SA WG3 report to TSG SA#7 (presentation)	Chairman	6.1	Information		Noted
S3-000235	Liaison Statement to TSGs on Enhanced User Identity Confidentiality	TSG SA WG2	6.2	Discussion		Noted
S3-000236	Work plan for the design of the 3GPP Authentication Algorithm (MCC Task Force)	ETSI SAGE	6.4	Discussion		Noted
S3-000237	DRAFT LS to GSM-A on Authentication Algorithm	3GPP TSG SA (drafting person)	6.4	Information		Noted
S3-000238	Open Issues for Release 99 List (from TSG SA Plenary)	TSG SA	8, 12.3	Discussion		Noted
S3-000239	Draft Meeting Report of CN WG2 (SA WG3 experts invited)	MCC CN WG2 Secretary	6,2	Information		Noted
S3-000240	CR to 33.102: Clarification on ciphering and integrity protection at intersystem handover	Ericsson	13.3	Approval	S3-000288	Revised in TD 288
S3-000241	CR to 33.102: Clarification on the UIA and UEA selection	Ericsson	13.3	Approval	S3-000289 S3-000290	Replaced by TDs 289, 290
S3-000242	Identifying specifications that implement “Secure UMTS-GSM Interoperation”.	Ericsson	12.2	Discussion		Noted. Ericsson to review affected specifications
S3-000243	Cipher and Integrity key update	Ericsson	10, 13.3	Discussion	S3-000292	Revised in TD292
S3-000244	DRAFT R2000 Project Plan for Security v0.0.2	P Howard	9	Discussion	S3-000281	Presented and noted.
S3-000245	Project Plan for Security v1.2.1	P Howard	9	Discussion		
S3-000246	23.821 V0.12.0: Architecture Principles for Release 2000	P Howard	8	Discussion		Noted
S3-000247	Key issues for Release 2000	SA WG2 drafting group (P Howard)	8	Discussion		Noted with TD 248
S3-000248	Release 2000 QoS Key Issues	SA WG2 QoS drafting group (P Howard)	8	Discussion		Noted
S3-000249	draft TR 23.821 v0.2.0 “Architecture Principles for Release 2000”	SA WG2 editor (Telia)	8	Information		Noted with TD 246
S3-000250	Support for multiple GEA in TS 24.008	Siemens Atea	11.1	Discussion		Includes CR
S3-000251	Review of TS 24.008	Siemens Atea	12.2	Discussion		Includes 2 proposed CRs to 24.008
S3-000252	CR to 03.20: GPRS Ciphering algorithm negotiation	Siemens Atea	11.1	Approval	S3-000286	Updated in TD 286
S3-000253	CR to 33.102: Authentication and key agreement (editorial)	Siemens Atea	13.3	Information		CR082. Delegates to check the need for restucturing proposed in the CR. R99 and/or R00 ? Postponed to SA3#13
S3-000254	CR to 33.102: Authentication and key agreement (minimal)	Siemens Atea	13.3	Approval	S3-000293	Revised in TD 293
S3-000255	CR to 33.102: Conversion functions for GSM-UMTS interoperation	Siemens Atea	13.3	Approval	S3-000294	Revised in TD294
S3-000256	CR to 33.102: 3G-3G Handover	Siemens Atea	13.3	Approval		CR085
S3-000257	CR to 33.102: 3G-2G and 2G-3G Handover for CS services	Siemens Atea	13.3	Approval		CR086 Postponed to SA3#13
S3-000258	CR to 33.102: Limitation and reduction of the effective cipher key length by the serving network	Siemens Atea	13.3	Approval	S3-000291	Revised in TD 291
S3-000259	CR to 33.102: Initialisation of synchronisation for ciphering and integrity protection	Siemens Atea	13.3	Approval	S3-000295	Revised in TD 295
S3-000260	LS from SMG2 to SMG10 on “double ciphering” in GSM/GPRS Dual Transfer Mode	SMG2	11.1	Discussion		P. Hpward to draft response for agreement after the meeting
S3-000261	CR to 33.102: Addition of another variant of sequence number generation	Nokia	13.3	Approval		CR089. Approved

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000262	CR to 33.102: Clarification of BEARER and DIRECTION parameters	Nokia	13.3	Approval		CR090 Approved. Corresponding CR to 33.105 to be provided (Nokia)
S3-000263	CR to 33.102: Inclusion of the radio bearer identity to the integrity mechanism	Nokia	13.3	Approval		CR091 Approved
S3-000264	LS from SA WG1 : Answer to LS New SIM toolkit feature: "Auto-answer & Mute-ringing	SA WG1	6.2	Discussion		Not accepted, response in TD270
S3-000265	Around Auto-answer	GemPlus	6.2	Discussion		Not accepted, response in TD270
S3-000266	Objectives and meeting schedule for Meeting#12	Chairman	2	Information		Noted
S3-000164	LS from SMG9 to SA WG3 (and SA WG1) on New SIM toolkit feature: "Auto-answer & Mute-ringing"	SMG9	6.2	Discussion		Not accepted, response in TD270
S3-000267	CN WG2 TD N2B000428 CR to 29.060	CN WG2	6.1	Information		To be considered for decision at meeting#13
S3-000268	CR to 33.102: Removal of enhanced user identity confidentiality	Siemens Atea	13.3	Approval		CR092. Approved
S3-000269	CR to 33.102: Removal of network domain security	Siemens Atea	13.3	Approval		CR093 Approved
S3-000270	Response Liaison to SMG9 on "Auto-Answer and Mute ringing"	SA WG3	6.2	Approval		Not presented. To be cobsidered at meeting#13
S3-000271	Minutes of GSM 2000 meeting.	C Brookson	6.4	Information		Noted
S3-000272	Global Challenge for Initial Registration	TIA TR-45.2 Security Focus Group Chair	10	Discussion		Noted. AHAG to forward further results of studies to SA WG3
S3-000273	Overview of 3GPP (Presentation Slides)	SA WG3 Vice Chair (S Puetz)	10	Presentation		Noted
S3-000274	TIA TR-45 and 3GPP2 Security (Presentation Slides)	Chair, TR-45 Adhoc Authentication Group	10	Presentation		Noted
S3-000275	3GPP Security/AKA - Requirements and development (Presentation Slides)	Siemens Atea	10	Presentation		Noted
S3-000276	The ESA Process (Presentation Slides)	Qualcomm Inc.	10	Presentation		Noted
S3-000277	CR095 to 29.060: GTP Security	Nortel		Information		To be considered for meeting#13
S3-000278	Proposal for the Release 2000 Features, Building Blocks and Work Tasks v.0.9	TSG SA WG2 IGC meeting	7	Information		Noted. Security Work Plan to be used as a basis for updating the tables.
S3-000279	Examples of Features, Building Blocks and Work Tasks	MCC	7	Presentation		Presented.
S3-000280	Practical aspects of the handling of 3GPP Work Program	MCC	7	Information		Noted.
S3-000281	DRAFT R2000 Project Plan for Security v0.0.2 (revised TD 244)	P Howard	9	Discussion	S3-000305	Discussed and revised in TD 305
S3-000282	Final document on the Evaluation of the 3GPP Confidentiality and Integrity algorithms	ETSI SAGE		Discussion		To be updated and considered for approval at next meeting
S3-000283	LS to CN WG4 on TR-45 Recommendations	SA WG3 (G Koien)		Approval		Withdrawn, Liaison with AHAG needed on their requirements
S3-000284	Invitation to SA WG3 Meeting #13 (Japan)	Chairman		Information		Noted

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000285	Requirements Specification for the GSM A5/3 Encryption Algorithm version 0.3 (rev of TD 227)	C Brookson	11.2	Information	S3-000303	Noted. P. Howard to produce a cover note to the A5/3 requirements specification
S3-000286	CR to 03.20: GPRS Ciphering algorithm negotiation (revised TD 252)	Siemens Atea	11.1	Approval		CR A022 Postponed to SA3#13
S3-000287	Proposed CR to 33.102 (REL 2000): Selective deletion of Authentication Vectors from the profile of a roaming subscriber	Siemens Atea	13.3	Discussion		33.102 v4.0.0 not yet created.
S3-000288	CR to 33.102: Clarification on ciphering and integrity protection at intersystem handover	Ericsson	13.3	Approval		CR080 Approved
S3-000289	CR to 33.102: Clarification on the HFN handling	Ericsson	13.3	Approval		CR096 Approved with changes
S3-000290	CR to 33.102: Clarification on the UIA and UEA selection	Ericsson	13.3	Approval		CR081 Postponed to SA3#13
S3-000291	CR to 33.102: Limitation and reduction of the effective cipher key length by the serving network	Siemens Atea	13.3	Approval		CR087 Postponed to SA3#13
S3-000292	CR to 33.102: Cipher and integrity key update once every 24 hours	Ericsson	10, 13.3	Discussion		CR094. Approved
S3-000293	CR to 33.102: Authentication and key agreement (minimal)	Siemens Atea	13.3	Approval		CR083 Approved
S3-000294	CR to 33.102: Conversion functions for GSM-UMTS interoperation	Siemens Atea	13.3	Approval		CR084 Approved
S3-000295	CR to 33.102: Initialisation of synchronisation for ciphering and integrity protection	Siemens Atea	13.3	Approval		CR088 Approved
S3-000296	LS to CN WG4: Evaluation of the impact on positive authentication reporting on network performance	SA WG3			S3-000308	Replaced by TD 308
S3-000297	Proposal on authentication vector generation algorithm for conformance testing	Ericsson				Disussed under 12.1
S3-000298	LS preseting an Invitation to S3 on joint meeting CN / S3 on security requirements for R'00	Chairman		Information		Joint meeting arranged 13-14 June, ETSI.
S3-000299	Proposed LS on A5/3	Vodafone Airtouch			S3-000307	Replaced by TD 307
S3-000300	Proposed LS on R00 working methods	Vodafone Airtouch				To send to SA WG2 with TD305 attached.
S3-000301	Update to S3-000281 on rejection of unencrypted calls	Vodafone Airtouch				Included with TD 301
S3-000302	CR to 33.102: Handling of emergency call	Ericsson		Approval		CR095 Approved
S3-000303	Requirements Specification for the GSM A5/3 Encryption Algorithm version 0.3 (rev of TD 227)	C Brookson	11.2	Information		Noted. To forward to SMG#31bis
S3-000304	Report to SMG Plenary for A5/3 algorithm	SA WG3			S3-000307	Included with TD 299 in TD307
S3-000305	DRAFT R2000 Project Plan for Security v0.0.3 (revised TD 281)	P Howard	9	Discussion		To be attached to TD 300 and sent to SA WG2
S3-000306	LS to SMG and CN WG1/SMG3 on GPRS ciphering	SA WG3		Approval		Approved. To be sent to SMG and CN WG1/SMG3
S3-000307	Liaison Statement on A5/3	SMG10		Approval		Approved Forwarded to SMG#31bis
S3-000308	LS to CN WG4: Evaluation of the impact on positive authentication reporting on network performance	SA WG3		Approval		Approved. To be forwarded to CN WG4

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000181	TR 33.900 V1.3.0					Noted. Comments to C Brookson
S3-000309	Liaison statement on HE initiated cancellation of AV in SN	SA WG3		Approval		Approved. To be sent to TR-45 AHAG

Annex B: List of attendees

Taken from secretary's memory and Hosted Event list: PLEASE UPDATE !!!

Name			Company	e-mail	3GPP Member	
Mr.	Andersson	Stefan	ERICSSON L.M.	stefan.x.andersson@ecs.ericsson.se	ETSI	SE
Mr.	Blom	Rolf	ERICSSON L.M.	rolf.blom@era.ericsson.se	ETSI	SE
Mr.	Brookson	Charles	DTI	cbrookson@iee.org	ETSI	GB
Mr.	Castellanos	David	ERICSSON L.M.	davis.castellunos-damca@ece.ericsson.se	ETSI	SE
Mr.	Chikazawa	Takeshi	Mitsubishi Electric Co.	chika@isl.melco.co.jp	ARIB	JP
Mr.	Christoffersson	Per	TELIA AB	per.e.christoffersson@telia.se	ETSI	SE
Mr.	Finkelstein	Louis	Motorola Inc.	louisf@ccrl.mot.com	T1	US
Ms.	Horak	Monika	GIESECKE & DEVRIENT GmbH		ETSI	DE
Mr.	Horn	Guenther	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI	DE
Mr.	Howard	Peter	VODAFONE AirTouch Plc	peter.howard@vf.vodafone.co.uk	ETSI	GB
Mr.	Brown	Daniel	Motorola Inc.		T1	US
Mrs.	Koskinen	Tiina	NOKIA Corporation	tiina.s.koskinen@nokia.com	ETSI	FI
Mr.	Køien	Geir	TELENOR AS	geir-myrdahl.koien@telenor.com	ETSI	NO
Mr.	Marcovici	Michael	Lucent Technologies	marcovici@lucent.com	ETSI	DE
Mr.	Nguyen Ngoc	Sebastien	France Telecom	sebastien.nguyenngoc@cnet.francetelecom.fr	ETSI	FR
Dr.	Niemi	Valtteri	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI	FI
Mr.	Nyberg	Petri	SONERA Corporation	petri.nyberg@sonera.fi	ETSI	FI
Mr.	Pope	Maurice	ETSI	maurice.pope@etsi.fr	ETSI	FR
Dr.	Pütz	Stefan	Deutsche Telekom MobilNet	stefan.puetz@t-mobil.de	ETSI	DE
Mr.	Rousseau	Ludovic	GEMPLUS Card International	ludovic.rousseau@gemplus.com	ETSI	FR
Mr.	Tietz	Benno	MANNESMANN Mobilfunk GmbH	benno.tietz@d2mannesmann.de	ETSI	DE
Mr.	Trautmann	Peter	BMWi	peter.trautmann@regtp.de	ETSI	DE
Mr.	Vinck	Bart	SIEMENS ATEA NV	bart.vinck@vnet.atea.be	ETSI	BE
Mr.	Bob	Lubarsky	T-Mobil		ETSI	DE
Mr.	Reginald	Lee	One-2-one	reginald.lee@one2one.co.uk	ETSI	GB
Mr.	Hiroshi	Aono	NTT DoCoMo	aono@mml.yrp.nttdocomo.co.jp	ARIB	JP
Mr.	Krister	Boman	ERICSSON L.M.		ETSI	SE
Mr.	Stuart	Ward	ORANGE PCS LTD	stuart.ward@orange.co.uk	ETSI	GB
Mr.	Kook-Helli	Lee	Samsung Electronics Co., Ltd		TTA	KR
Mr.	Jae Yoel	Kim	Samsung Electronics Co., Ltd	kimjy@telecom.samsung.co.kr	TTA	KR

Annex C: Status of specifications under SA WG3 and SMG 10 responsibility

C.1 SA WG3 specifications

Specification			Title		Editor**	Rel	Comment
TS	21.133	3.1.0	Security Threats and Requirements	April 99	Per Christoffersson	R99	
TS	22.022	3.0.1	Personalisation of GSM ME Mobile functionality specification - Stage 1	Oct 99		R99	Transfer>TSG#4, CR at TSG#5
TS	33.102	3.4.0	Security Architecture	Mar 00	Bart Vinck	R99	
TS	33.103	3.2.0	Security Integration Guidelines	Oct 99	Bart Vinck	R99	TSG#7: 3.2.0
TS	33.105	3.3.0	Cryptographic Algorithm requirements	June 99	Bart Vinck	R99	CR at TSG#5 TSG#7: 3.3.0
TS	33.106	3.1.0	Lawful interception requirements	Jun 00	Bart Vinck	R99	
TS	33.107	3.0.0	Lawful interception architecture and functions	Dec 99		R99	New at TSG#6 approved
TS	33.120	3.0.0	Security Objectives and Principles	April 99	Tim Wright	R99	
TR	33.900	1.2.0	Guide to 3G security	Mar 00		R99	New at TSG#6
TR	33.901	3.0.0	Criteria for cryptographic Algorithm design process	June 99	Vinck Bart	R99	3.1.0 ex SAGE
TR	33.908	3.0.0	Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	Mar 00	M. Walker	R99	CR at TSG#4,CR at TSG#5 TSG#7: 3.4.0
TR	33.909	3.0.0	ETSI SAGE 3GPP Standards Algorithms Task Force: Report on the evaluation of 3GPP standard confidentiality and integrity algorithms	Jun 00	M. Walker	R99	TSG#7 SP-000039 : S3-000105=NP-000049
TS	35.203	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data		M. Walker	R99	TSG#7: refered to in 33.908: Is a reference in 33.908

** Editors need update.

C.2 SMG10 Specifications

Specification latest version		Title	Release	ETSI Number		ETSI WI ref
01.31	7.0.1	Fraud Information Gathering System (FIGS); Service requirements - Stage 0	Release 1998			RTR/SMG-100131Q7
01.31	8.0.0	Fraud Information Gathering System (FIGS); Service requirements - Stage 0	Release 1999			RTR/SMG-100131Q8
01.33	7.0.0	Lawful Interception requirements for GSM	Release 1998			
01.33	8.0.0	Lawful Interception requirements for GSM	Release 1999			
01.61	8.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	Release 1997	TS	101 106	DTS/SMG-100161Q6
02.09	3.1.0	Security Aspects	Phase 1	GTS	02.09	DGTS/SMG-010209
02.09	4.5.0	Security Aspects	Phase 2	ETS	300 506	RE/SMG-010209PR2
02.09	5.2.0	Security Aspects	Phase 2+	ETS	300 920	RE/SMG-010209QR2
02.09	6.1.0	Security Aspects	Release 1997	EN	300 920	DEN/SMG-010209Q6R1
02.09	7.1.0	Security Aspects	Release 1998	EN	300 920	DEN/SMG-010209Q7R1
02.09	8.0.0	Security Aspects	Release 1999			DEN/SMG-010209Q8
02.31	7.1.1	Fraud Information Gathering System (FIGS) Service description - Stage 1	Release 1998	TS	101 107	RTS/SMG-100231Q7
02.31	8.0.0	Fraud Information Gathering System (FIGS) Service description - Stage 1	Release 1999			RTS/SMG-100231Q8
02.32	7.1.1	Immediate Service Termination (IST); Service description - Stage 1	Release 1998	TS	101 749	DTS/SMG-100232Q7
02.32	8.0.0	Immediate Service Termination (IST); Service description - Stage 1	Release 1999			DTS/SMG-100232Q8
02.33	7.3.0	Lawful Interception - Stage 1	Release 1998	TS	101 507	DTS/SMG-100233Q7
02.33	8.0.0	Lawful Interception - Stage 1	Release 1999			DTS/SMG-100233Q8
03.20	3.0.0	Security-related Network Functions	Phase 1 extension	GTS	03.20-EXT	RGTS/SMG-030320B
03.20	3.3.2	Security-related Network Functions	Phase 1	GTS	03.20	DGTS/SMG-030320
03.20	4.4.1	Security-related Network Functions	Phase 2	ETS	300 534	RE/SMG-030320PR
03.20	5.2.0	Security-related Network Functions	Release 1996			
03.20	6.1.0	Security-related Network Functions	Release 1997	TS	100 929	RTS/SMG-030320Q6R1
03.20	7.2.0	Security-related Network Functions	Release 1998	TS	100 929	RTS/SMG-030320Q7
03.20	8.0.0	Security-related Network Functions	Release 1999			RTS/SMG-030320Q8
03.31	7.0.0	Fraud Information Gathering System (FIGS); Service description - Stage 2	Release 1998			
03.31	8.0.0	Fraud Information Gathering System (FIGS); Service description - Stage 2	Release 1999			
03.33	7.1.0	Lawful Interception - stage 2	Release 1998	TS	101 509	DTS/SMG-100333Q7
03.33	8.0.0	Lawful Interception - stage 2	Release 1999			DTS/SMG-100333Q8
03.35	7.0.0	Immediate Service Termination (IST); Stage 2	Release 1998			DTS/SMG-100335Q7
03.35	8.0.0	Immediate Service Termination (IST); Stage 2	Release 1999			DTS/SMG-100335Q8
10.20	-	Lawful Interception requirements for GSM	Release 1999			DTS/SMG-101020Q8

Annex D: List of CRs to specifications under SA WG3 and SMG 10 responsibility

D.1 SA WG3 CRs at the Meeting (and by e-mail after meeting#11)

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	New Vers	Date	Source	WG	WG meeting	WG TD	WG status	Remarks
33.102	047	2	R99	Interoperation and intersystem handover/change between UTRAN and GSM BSS	C	3.3.1	3.4.0	21/02/2000	S3	S3	S3-11	S3-000208	agreed	Agreed by e-mail after meeting 10/03/00
33.102	050		R99	Refinement of Cipher key and integrity key lifetime	F	3.3.1	3.4.0	18/02/2000	S3	S3	S3-11	S3-000101	agreed	agreed by e-mail 09/03/00
33.102	064	2	R99	Distribution and Use of Authentication Data between VLRs/SGSNs	F	3.3.1	3.4.0	21/02/2000	S3	S3	S3-11	S3-000212	agreed	Agreed by e-mail after meeting 10/03/00
33.102	066	1	R99	Ciphering	C	3.3.1	3.4.0	21/02/2000	S3	S3	S3-11	S3-000220	agreed	Agreed by e-mail 10/03/00
33.102	067	1	R99	Data integrity	C	3.3.1	3.4.0	21/02/2000	S3	S3	S3-11	S3-000221	agreed	Agreed by e-mail 10/03/00
33.102	071	1	R99	Use of default IK at emergency call with no (U)SIM or when authentication has failed	F	3.3.1	3.4.0	22/02/2000	S3	S3	S3-11	S3-000178	agreed	Agreed by e-mail after meeting 09/03/00
33.102	074		R99	Clarification about CK and IK which are transmitted in clear over the Iu-interface	B	3.3.1	3.4.0	28/02/2000	S3	S3	S3-11	S3-000108	agreed	Agreed by e-mail after meeting 09/03/00
33.102	076		R99	Cipher key and integrity key lifetime	F	3.3.1	3.4.0	28/02/2000	S3	S3	S3-11	S3-000193	agreed	Agreed by e-mail after meeting 09/03/00
33.102	077		R99	Cipher key and integrity key setting	F	3.3.1	3.4.0	28/02/2000	S3	S3	S3-11	S3-000194	agreed	Agreed by e-mail after meeting 09/03/00
33.102	079	1	R99	Local Authenication and connection establishment	C	3.3.1	3.4.0	09/03/2000	S3	S3	S3-11	S3-000149	agreed	Agreed by e-mail after meeting 09/03/00
33.102	080		R99	Clarification on ciphering and integrity protection at intersystem handover	F	3.4.0	3.5.0	11/04/2000	S3	S3	S3-12	S3-000288	agreed	
33.102	081		R99	Clarification on the UIA and UEA selection	F	3.4.0		11/04/2000	S3	S3	S3-12	S3-000290	Postponed	Postponed to S3-13
33.102	082		R99	Authentication and key agreement (editorial)	D	3.4.0		11/04/2000	S3	S3	S3-12	S3-000253	Postponed	Postponed to S3-13
33.102	083		R99	Authentication and key agreement (minimal)	F	3.4.0	3.5.0	11/04/2000	S3	S3	S3-12	S3-000293	agreed	
33.102	084		R99	Conversion functions for GSM-UMTS interoperation	C	3.4.0	3.5.0	11/04/2000	S3	S3	S3-12	S3-000294	agreed	
33.102	085		R99	3G-3G Handover	C	3.4.0		11/04/2000	S3	S3	S3-12	S3-000256	Postponed	Postponed to S3-13
33.102	086		R99	3G-2G and 2G-3G Handover for CS services	F	3.4.0		11/04/2000	S3	S3	S3-12	S3-000257	Postponed	Postponed to S3-13

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	New Vers	Date	Source	WG	WG meeting	WG TD	WG status	Remarks
33.102	087		R99	Limitation and reduction of the effective cipher key length by the serving network	F	3.4.0		11/04/2000	S3	S3	S3-12	S3-000291	Postponed	Postponed to S3-13
33.102	088		R99	Initialisation of synchronisation for ciphering and integrity protection	C	3.4.0	3.5.0	11/04/2000	S3	S3	S3-12	S3-000295	agreed	
33.102	089		R99	Addition of another variant of sequence number generation	C	3.4.0	3.5.0	11/04/2000	S3	S3	S3-12	S3-000261	agreed	
33.102	090		R99	Clarification of BEARER and DIRECTION parameters	F	3.4.0	3.5.0	11/04/2000	S3	S3	S3-12	S3-000262	agreed	
33.102	091		R99	Inclusion of the radio bearer identity to the integrity mechanism	C	3.4.0	3.5.0	11/04/2000	S3	S3	S3-12	S3-000263	agreed	
33.102	092		R99	Removal of enhanced user identity confidentiality	F	3.4.0	3.5.0	11/04/2000	S3	S3	S3-12	S3-000268	agreed	
33.102	093		R99	Removal of network domain security	F	3.4.0	3.5.0	11/04/2000	S3	S3	S3-12	S3-000269	agreed	
33.102	094		R99	Cipher and integrity key update once every 24 hours	F	3.4.0	3.5.0	14/04/2000	S3	S3	S3-12	S3-000292	agreed	
33.102	095		R99	Handling of emergency call	F	3.4.0	3.5.0	14/04/2000	S3	S3	S3-12	S3-000302	agreed	
33.102	096		R99	Clarification on the HFN handling	F	3.4.0	3.5.0	14/04/2000	S3	S3	S3-12	S3-000289	agreed	

D.2 SMG10 CRs at the Meeting

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	New Vers	Date	Source	WG	WG meeting	WG TD	WG status	Remarks
03.20	A022		R99	GPRS Ciphering algorithm negotiation	C	8.0.0		11/04/2000	SMG10	10	S3-12	S3-000286	Postponed	Postponed to SA3_13

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD Number	Title	Source	Comment
S3-000164	LS from SMG9 to SA WG3 (and SA WG1) on New SIM toolkit feature: "Auto-answer & Mute-ringing"	SMG9	Not accepted, response in TD270. (See also TD 264)
S3-000217	Liaison response to S3's LS (S3-000190) on Functions of Key Distribution and Key Administration for MAP security	SA WG5	Noted
S3-000219	Reply to LS on "Introduction of rejection of non ciphered calls for GPRS"	CN WG1/SMG 3	Rejects CR to 04.08 in S3-000058. B. Vinck to draft an LS to CN WG1 and SMG on SMG10 GPRS ciphering agreements, based upon TD S3-000201 and TD S3-000205
S3-000223	LS on OPEN SERVICE ARCHITECTURE - SECURITY	SA WG2	All to check OSA Security and revisit at SA3#13
S3-000224	Answer to LS on Functions of Key Distribution and Key Administration for MAP security	SA WG2	Postponed to SA3#13 MAP security ad-hoc
S3-000226	Liaison statement to TSG-S WG3 on GTP Signalling Security	CN WG2	Postponed to SA3#13 MAP security ad-hoc
S3-000235	Liaison Statement to TSGs on Enhanced User Identity Confidentiality	TSG SA WG2	Noted.
S3-000237	DRAFT LS to GSM-A on Authentication Algorithm	3GPP TSG SA (drafting person)	Noted
S3-000260	LS from SMG2 to SMG10 on "double ciphering" in GSM/GPRS Dual Transfer Mode	SMG2	P. Hpward to draft response for agreement after the meeting
S3-000264	LS from SA WG1 : Answer to LS New SIM toolkit feature: "Auto-answer & Mute-ringing	SA WG1	Not accepted, response in TD270
S3-000298	LS preseting an Invitation to S3 on joint meeting CN / S3 on security requirements for R'00	Chairman	Joint meeting arranged 13-14 June, ETSI.

E.2 Liaisons from the meeting

TD Number	Title	Status	Comment
S3-000283	LS to CN WG4 on TR-45 Recommendations	Withdrawn	Liaison with AHAG needed on their requirements
S3-000300	Proposed LS on R00 working methods	Approved	To send to SA WG2 with TD305 attached.
S3-000306	LS to SMG and CN WG1/SMG3 on GPRS ciphering	Approved	To be sent to SMG and CN WG1/SMG3
S3-000307	Liaison Statement on A5/3	Approved	To be forwarded to SMG#31bis
S3-000308	LS to CN WG4: Evaluation of the impact on positive authentication reporting on network performance	Approved	To be forwarded to CN WG4
S3-000309	Liaison statement on HE initiated cancellation of AV in SN	Approved	To be sent to TR-45 AHAG

Annex F: List of Actions from the meeting

ACTION #12/1: All to check the OSA Security document TD S3-000223 and contribute any security problems or issues to the May 2000 meeting of SA WG3.

ACTION #12/2: C. Brookson to contact SMG10 WPD Chairman to ask him to produce a WI description sheet for Lawful Interception for Release 2000.

ACTION #12/3: Secretary: TD S3-000300 (with TD S3-000305 attached) to be sent to SA WG2.

ACTION #12/4: Chairman: TD S3-000309 to be sent to TR-45 AHAG.

ACTION #12/5: B. Vinck to draft the LS to CN WG1 and SMG on SMG10 GPRS ciphering agreements, based upon TD S3-000201 and TD S3-000205. (CC: T WG2)

ACTION #12/6: P. Howard to update the SMG10 work plan for GPRS encryption.

ACTION #12/7: S. Nguyen to produce a draft Stage 2 description document for rejection of unciphered GPRS calls for the May 2000 meeting.

ACTION #12/8: B. Vinck to draft a liaison to CN WG1 and SMG on changes to TS 24.008 needed for GEA/2 algorithm indication bits.

ACTION #12/9: P. Howard to draft a response to SMG2 that SMG10 do not foresee any problems with double ciphering of LLC data.

ACTION #12/10: P. Howard to produce a cover note to the A5/3 requirements specification explaining the specific requirements that are proposed in the document. This to be forwarded to SMG, SMG2, CN WG1, CN WG2 and SMG9.

ACTION #12/11: Lision to GSM Association and SMG to be created about support for increased key length work Item for R00.

ACTION #12/12: Chairman to check the urgency of the security work on GTP with CN WG2.

ACTION #12/13: TS 34.108 to be forwarded to M. Pope for distribution to the SA WG3 list to review and comment to the next SA WG3 meeting.

ACTION #12/14: B. Vinck to forward the proposed changes to CN WG1 collegues for discussion and action in CN WG1.

ACTION #12/15: P. Howard to set up e-mail discussion on open issues. All: to consider the open issues and make proposals to SA WG3 in time to provide proposals to CN WG1 on 24.008 (deadline for all changes to 24.008 and 33.102, Release 1999 specifications is June 2000).

ACTION #12/16: Delegates to check the need for restucturing proposed in the CR in TD S3-000253 for Release 1999 and/or Release 2000.

ACTION #12/17: Chairman to send the proposed dates for a joint meeting to relevant people.