3GPP TSG SA WG 3 (Security) meeting #11
Mainz, 22-24 January, 2000

Source: Secretary, M Pope, MCC

Title: Draft Report of meeting #11 version 0.0.3

Document for: Approval

Mainz Cathedral

1 Opening of the meeting

Mr. Wolfgang Heidrich welcomed delegates to Mainz and the RegTP premises. Mr. Peter Troutmann then provided domestic arrangements for the meeting. The Chairman, Dr. Stefan Pütz, then welcomed delegates and opened the meeting.

2 Approval of the agenda

TD S3-000095: The draft agenda was approved. A presentation from the USECA project was added for the afternoon of the second day of the meeting and a new item 6.3 was included to review 02.09.

3 Registration and assignment of input documents

The received documents were allocated to their agenda items and new documents registered.

4 Approval of meeting reports

4.1 TSG-SA3 Meeting no. 9

TD S3-000067: This report was not approved at the previous meeting, due to lack of time for consideration by delegates. It had subsequently been reviewed after meeting#10 and no comments had been received. The report was therefore approved.

4.2 TSG-SA3 Meeting no. 10

TD S3-00096: The report of the previous meeting had been sent out to the mailing list for comments by e-mail and version 1.0.0 had been produced, containing changes related to the comments received. The report was discussed and modifications made to sections 8 and 13.

5 Reports / Liaisons from other 3GPP and SMG groups

5.1 3GPP and SMG plenary

The Secretary reported the presentation given to SMG#31 and the results of the presentation.

5.2 3GPP WGs and SMG STCs

TD S3-000102: This liaison from RAN WG2 asks for comment upon the cipher key renewal procedure and proposes that in case of a cipher key checking failure, then the old cipher key is used to prevent loss of the UE. After some discussion on this liaison, it was clarified that there is no SA WG3 requirement for a checking procedure on the establishment of cipher keys. The checking procedure is not considered necessary by SA WG3, because computational errors cannot be accounted for in the system, and transmission errors are unlikely to occur only in the cipher key and means there are probably transmission problems with the connection.

A response to RAN WG2 was created in TD S3-000157 which outlines the potential risks if, for example, a false BS can prevent the renewal of the cipher key. This document was discussed and revised in TD S3-000158 which was approved.

TD S3-000103: LS on RANAP Signalling procedures in case of Unsuccessful Integrity check. A reply was proposed in TD S3-000169, which was revised in TD S3-000202 and approved.

TD S3-000107: Reply LS from SA WG1 on additional Terminal Baseline Implementation Capabilities for secure interoperation with GSM. This was noted for information.

TD S3-000124: USIM triggered authentication and key setting during PS connections. This Liaison required updating and transmitting to CN WG1 after the meeting. It was updated during the meeting and provided in TD S3-000153.

5.3 3GPP partners

No input.

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

TD S3-000104: Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms. The document provides the public report from SAGE for comments. It was reported that the PCG will discuss the publication of the algorithms in their meeting in May 2000. It was decided to wait until the PCG have made decisions and the algorithm is published before considering publication of this report as a 3GPP TR.

A response to ETSI SAGE was drafted in TD S3-000154, revised in TD S3-000171 and agreed. The document was updated as an output of SA WG3 in TD S3-000200 which was approved. The reception of this report and the completion by SAGE of their tasks will be reported to TSG SA plenary, as provided in the response liaison to SAGE, copied to SA in TD S3-000200.

ACTION #11/1: TD S3-000200 to be sent to SAGE and TSG SA. (M Pope)

TD S3-000105: General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms. This report was noted.

TD S3-000146: LS from SPAN6 to SMG10 (and TC Security) on Lawful Interception (LI) in the IN environment. This was noted and should be forwarded to SMG10 WPD for information.

ACTION #11/2: TD S3-000146 to be forwarded to SMG10 WPD Chairman. (M. Pope)

TD S3-000180: This liaison was introduced by Vodafone-Airtouch. This had been presented to meeting#10 and due to lack of time, discussed via e-mail and re-presented to the meeting with revisions. After some discussion, it was decided that the document should be updated to clarify SA WG3 agreed position on the approval of changes to the document between 3GPP and TR45. The revised document was presented in TD S3-000199 and revised in TD S3-000204. It was decided that further discussion was required and it was decided to approve the liaison by e-mail.

ACTION #11/3: M Pope to send TD S3-000204 to group for e-mail discussion.

6 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

7 3G security issues

7.1 Open R99 security issues (MAP security, EUIC, n/w encryption, auth. failure indicator)

MAP security: It was proposed to send a liaison statement to SA WG5 to integrate MAP security mechanisms into 33.105, using O&M mechanisms for key changes, and to verify if 33.102 requires update and any other work that needs to be done. A proposed liaison to SA WG5 on Functions of Key Distribution and Key Administration for MAP security is given in TD S3-000152. This proposes that SA WG5 look after layer 2 (standardisation of the interfaces between the KAC and network) and the layer 1 (transport mechanisms for key exchange) should not be standardised, but subject to a Recommendation from the GSM Association and agreed as part of roaming agreements. The requirements that could be achieved for Release 99 and Release 00 requirements were discussed. The liaison was revised after the drafting group met (see below) in TD S3-000190 which was approved.

ACTION #11/4: LS in TD S3-000190 to be transmitted to SA WG5. (M Pope)

It was then agreed to set up a drafting group to provide a report on MAP Security status to be used for presentation to the next TSG SA Plenary, in order to make the status of the work for Release 1999 clear, and the progress and improvements expected for Release 2000. The output of this drafting group is given in TD S3-000173. It was then discussed and updated in TD S3-000187 which was approved.

A liaison to CN WG2 was proposed in TD S3-000174, which was discussed and updated in TD S3-000188 which was approved.

ACTION #11/5: LS in TD S3-000188 to be transmitted to CN WG2. (M Pope)

TD S3-000152: After the drafting group met, the liaison was updated in TD S3-000190 was approved.

ACTION #11/6: LS in TD S3-000190 to be transmitted to SA WG5 and SA WG2. (M Pope)

7.2 Confidentiality/integrity algorithm

See the report of agenda item 5.4.

7.3 Authentication algorithm

Algorithm work: SA WG3 intends to task ETSI SAGE to do the work for the authentication algorithm, subject to the approval of funding.

ACTION #11/7: Chairman to report this to TSG SA Plenary.

7.4 Review of other specifications (Authentication & Key Agreement, Confidentiality and Integrity Protection, Secure 2G-3G Interworking etc.)

TD S3-000097: Identifying specification which implements 3GPP AKA. This contribution was introduced by Telenor. The verification of the implementation of changes for authentication in the specifications needs to be done. These should be reviewed and any issues dealt with at the CN WG2B / SA WG3 joint session next week.

24.008 will be reviewed by Bart Vinck
31.xxx will be reviewed by Stefan Pütz

ACTION #3/8: All to review the identified specifications and feedback results to G. Køien for the joint CN WG2B / SA WG3 meeting (ALL)

TD S3-000150: Initial status report of specifications which implement ciphering and integrity protection. This contribution was introduced by Nokia. A liaison to RAN WG2 was required on security issues which appear to be missing from some of their RRC specifications. Conformance testing specifications do not cover security fully, but are not yet mature, SA WG3 should ensure that security is fully covered in these specifications.

A Liaison to RAN WG2 concerning the integrity protection mechanism (TD S3-000203) was also agreed as reported under agenda item 8.3.

TD S3-000175: 3G Capabilities and Security Review Framework (Draft). There was nobody available to present this report at the meeting, so the contribution was noted and delegates asked to consider it for discussion at SA WG3 meeting#12.

ACTION #11/9: All: Review the draft document which will be discussed at the next meeting of SA WG3.

7.5 R00 security issues

This was not discussed, due to lack of time at the meeting.

8 Review CRs to S3 specifications

8.1 TS 21.133 Threats and requirements

No input.

8.2 TS 22.022 Personalisation of ME

No input. A Rapporteur is still required for this document.

8.3 TS 33.102 Security architecture

TD S3-000111: CR051 to 33.102: Conversion function c3 at USIM. This CR was modified slightly and reproduced as CR051r1 in TD S3-000159 which was agreed.

TD S3-000112: CR052 to 33.102: Trigger points of AFR during AKA. The failure report to the HLR was agreed to be mandatory, so the CR was modified in this way. The deletion of the explanation of the f1* text should be verified to ensure that this is included elsewhere before deleting it and the deletion was removed

from this CR for inclusion in a new CR if required. The final chage requires clarification to make it clear that it is the CK, IK pair which are compared and not CK against IK. The CR was reproduced as CR052r1 in TD S3-000160 which was agreed.

TD S3-000113: CR053 to 33.102: Removal of EUIC from 'Authentication Data Request' procedure. An updated CR053r1 was produced in TD S3-000163 and was agreed.

TD S3-000098: CR045r1 to 33.102: Refinement of EUIC (revision of S3-000081). The liaison from CN WG2 in TD S3-000145 was also considered during the discussions. The CR was discussed in depth to check whether the concerns raised in the liaison were covered and whether the proposed solution to User identity confidentiality (and location) fully covered the potential threats. It was proposed that this feature be moved to Release 2000 unless a full threat analysis is provided with the corresponding protection offered by the proposed solution can be completed in time for Release 1999 (March 2000). It was argued that full protection of all threats would probably not be achievable even for Release 2000 and the proposal offered increased protection over that available in current specifications which fulfils the intention of the Enhanced User Identity confidentiality feature. An objection from France Télécom to the approval of the CR at this time was recorded. It was decided that a status report to TSG SA on this topic would be prepared, including the set of related CRs and the concerns expressed in the meeting, for a decision on the inclusion of this feature in Release 1999 or moving it to Release 2000. The draft proposed status report in TD S3-000186 was presented. Some changes and additions were made and it was agreed that an updated report would be created incorporating the comments for liaison to the SA#7 meeting and copied to CN WG2 for their consideration of the open issue on handling of lost TEMSI in the VLR. This agreed report was provided in TD S3-000196.

The CR045 was updated as CR045r2 in TD S3-000182 and further updated as CR045r3 in TD S3-000197 and agreed for presentation to TSG SA for consideration with the EUIC report (liaison) in TD S3-000196.

TD S3-000145: This was discussed in an ad-hoc meeting, and is indirectly answered in TD S3-000196.

TD S3-000114: CR054 to 33.102: Clarification of the scope. The reference to GSM 03.20 for security items not covered by 33.102 was debated. It was decided to delete this sentence from the CR. Some minor modifications were made to the remaining changes and the CR was reproduced as CR054r1 in TD S3-000161 which was agreed.

TD S3-000115: CR055 to 33.102: SQN Generation Requirements. This CR was agreed.

TD S3-000116: CR056 to 33.102: Identification of temporary identities. The reference to 23.060 was added to the references list and the revised CR was reproduced as CR056r1 in TD S3-000162 which was agreed.

TD S3-000117: CR057 to 33.102: Cipher key and integrity key selection. This CR was agreed.

TD S3-000118: CR058 to 33.102: Clarification on ciphering and integrity mode setting. Some revisions to the CR were agreed and the updated CR058r1 was produced in TD S3-000167 and agreed.

TD S3-000119: CR059 to 33.102: Clarification on when integrity protection is started. This CR was agreed.

TD S3-000195: CR on 33.102: HE control over accepting non-ciphered connections. (see TD S3-000120 below).

TD S3-000120: CR060 to 33.102: Clarification on the security mode set-up message sequence flow. This CR required alignment with the proposals presented in TD S3-000195 and it was agreed to do this after the meeting by e-mail. After e-mail discussion, no common solution was agreed in time for the TSG SA Plenary and the CR was postponed.

TD S3-000121: CR061 to 33.102: Unsuccessful integrity check. TD S3-000103 was considered during the discussions and a reply liaison was drafted in TD S3-000169, which was revised in TD S3-000202 and approved, including the resulting updatedCR061r1 in TD S3-000168 which was agreed.

TD S3-000122: CR062 to 33.102: Clarification on signalling messages to be integrity protected. A correction to the reference to 6.5.4 to 6.4.5 was made and the updated CR062r1 in TD S3-000176 was agreed.

TD S3-000123: CR063 to 33.102: Clarification of the HFN handling. The category was corrected to "F" and the change to the figure withdrawn. The updated CR063r1 provided in TD S3-000177 was agreed.

TD S3-000139: Distribution and Use of Current Security Context Data. This contribution presents 6 roaming scenarios between UTRAN R99 and GSM R98 and R99 and discusses the changes of security context involved in such roaming. The conclusions reached in this contribution are subject of the CR to 33.102 given in TD S3-000125.

The support of USIM in R98 GSM terminals was clarified, and there was no service requirement for support of USIM in R98 GSM terminals. This is contrary to the concepts that SA WG3 have been working to, where the support of USIM in R98 GSM terminals has been expected. See TS 22.100 and TS 22.101.

TD S3-000125: CR064 to 33.102: Distribution and Use of Authentication Data between VLRs/SGSNs. A sentence referring to the content of 6.3.4 was added and the revised CR064r1 produced in TD S3-000179. The CR was then agreed to be approved by e-mail after the meeting. The updated CR064r2, provided in TD S3-000212 was approved by e-mail.

TD S3-000126: CR047r1 to 33.102: Interoperation and intersystem handover/change between UTRAN and GSM BSS. This CR was revised as CR047r1 in TD S3-000185. The CR was then agreed to be approved by e-mail after the meeting. The updated CR047r2, provided in TD S3-000208 was approved by e-mail.

TD S3-000127: CR065 to 33.102: Authentication and key agreement.

TD S3-000128: CR066 to 33.102: Ciphering.

TD S3-000129: CR067 to 33.102: Data integrity.

TD S3-000130: CR068 to 33.102: Interoperation and intersystem handover/change between UTRAN and GSM BSS.

TD S3-000131: CR069 to 33.102: Local authentication and connection establishment.

TD S3-000132: CR070 to 33.102: User identity confidentiality.

TD S3-000147: CR071 to 33.102: Use of default IK at emergency call with no (U)SIM or when authentication has failed. The CR was discussed and enhancements made. A revised version was produced in TD S3-000178. This CR needs to be sent to CN WG1 for information and corresponding changes for the CN. It was decided that this needs further discussion and would be sent for approval by e-mail after the meeting.

ACTION #11/10: M Pope to send CR071r1 to CN WG1 when agreed by e-mail.

TD S3-000148: CR072 to 33.102: Clarification on ciphering and integrity protection at intersystem handover. This CR was agreed.

TD S3-000149: CR on 33.102 about local authentication. This will be approved via e-mail deadline: 1st March 2000. If approved, then RAN WG3 will be informed of the function.

ACTION #11/11: All to review and approve the CR in TD S3-000149 by 1 March 2000.

TD S3-000151: CR073 to 33.102: MAP Security. This CR was updated to class F and modified slightly. The revised CR073r1 in TD S3-000189 was agreed.

TD S3-000097: Identifying specification which implements 3GPP AKA. This contribution was introduced by Telenor. The verification of the implementation of changes for authentication in the specifications needs to be done. These should be reviewed and any issues dealt with at the CN WG2B / SA WG3 joint session next week.

TD S3-000203: Liaison statement to R2 concerning the integrity protection mechanism. This liaison was approved and TD S3-000150 and TD S3-000168 attached.

ACTION #11/12: Send TD S3-000203 to RAN WG2 (M Pope).

8.4 TS 33.103 Integration guidelines

TD S3-000099: This CR was also updated as CR005r2 in TD S3-000198 and agreed for presentation to TSG SA for consideration with the EUIC report (liaison) in TD S3-000196.

8.5 TS 33.105 Algorithm requirements

TD S3-000100: This CR was also agreed for presentation to TSG SA for consideration with the EUIC report (liaison) in TD S3-000196.

8.6 TS 33.106 LI requirements

Not dealt with due to lack of time.

8.7 TS 33.107 LI architecture

Not dealt with due to lack of time.

8.8 TR 33.120 Security principles and objectives

Not dealt with due to lack of time.

8.9 TR 33.901 Criteria for algorithm design process

Not dealt with due to lack of time.

8.10 TR 33.902 Formal analysis

Not dealt with due to lack of time.

9 Review of draft 3G specifications

9.1 TR 33.900 Guide to 3G security

Not dealt with due to lack of time.

10 3G security project plan

Not dealt with due to lack of time.

11 Approval of liaison statements, CRs and draft specifications

Due to lack of time and workload, not all issues were addressed at the meeting. It was decided to do e-mail approval on CRs which are required before the next TSG SA Plenary.

ACTION #11/13: M Pope to organise e-mail approval of outstanding CRs.
S. Pütz to present a list of TDs allowed for email approval.

12 Future meetings dates and venues

Meeting	Date	Location	Host
S3#12	11-14 April 2000 (including joint meeting with AHAG)	Stockholm	Ericsson
S3#13	23 - 25 May 2000	Tokyo	DoCoMo
S3#14	1-3 August 2000	Oslo	TeleNor
S3#15	19-21 September 2000	To be confirmed	Host required
S3#16	27-30 November 2000	To be confirmed	Host required

13 Any other business

TD S3-000172: USECA: Dr. Monika Horak (Giesecke & Devrient, R&D-Cards) gave an intersting presentation of the UMTS Security Architecture (USECA) project and showed a USECA demonstrator, which simulated the authentication protocol over several scenarios, including an authentication interception threat. More information and details of the simulator can be obtained by sending a request to Dr. Horak at monika.horak@gdm.de. Suggestions to further enhance the simulators capabilities and scenarios should be

addressed to Dr. Horak and will be considered for incorporation if there is time for the next version of the software (expected completion August 2000). The USECA URL is: http://www.useca.freeserve.co.uk.

14 Close of meeting

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

It was noted that many important documents had not been dealt with in time, and that more work would be needed via e-mail after the meeting in order to prepare submissions to the TSG SA Plenary in March.

Annex A: List of documents at the meeting

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comment
S3-000095	Draft agenda for meeting #11	Chairman	2	Approval		Approved with changes
S3-000096	Draft report of meeting #10	Secretary	4.2	Approval		
S3-000097	Identifying specification which implements 3GPP AKA.	Telenor R&D Agder	7.4	Discussion		
S3-000098	CR 045r1 to 33.102: Refinement of EUIC (revision no. 1 of S3-000081)	T-Mobil	7.1	Approval	S3-000182	
S3-000099	CR to 33.103: Refinement of EUIC according to 33.102	T-Mobil	7.1	Approval	S3-000183	CR005 revised in TD 183
S3-000100	Refinement of EUIC for consistency with 33.102	T-Mobil	7.1	Approval		CR008. Approved
S3-000101	CR to 33.102: Refinement of Cipher and Integrity Key Lifetime	T-Mobil	8.3	Approval		CR050 Approved by e-mail after meeting 09/03/00
S3-000102	LS on an L2&3 based procedure to check whether the UE uses the correct new cipher key during the cipher key change procedure	RAN WG2	5.2	Discussion		Reply in TD 158
S3-000103	LS on RANAP Signalling procedures in case of Unsuccessful Integrity check	RAN WG3	5.2	Discussion		Reviewed after S3-000121. Reply in TD 202
S3-000104	Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms	ETSI SAGE	5.4	Review and comment		Reply in TD 200
S3-000105	General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms	ETSI SAGE	5.4	Review and comment		Reply in TD 171
S3-000106	GPRS encryption	Telia	6.1	Discussion		
S3-000107	Reply LS on additional Terminal Baseline Implementation Capabilities for secure interoperation with GSM	SA WG1	5.2	Discussion		Noted.
S3-000108	CR to 33.102: Clarification about CK and IK which are transmitted in clear over the Iu-interface	Telenor	8.3	Approval		CR074 - Approved by e-mail after meeting 09/03/00
S3-000109	System behaviour on receipt of an invalid Message Authentication Code (MAC)	CN WG1	8.3	Discussion / Decision		Not dealt with
S3-000110	Related CRs and documents on EUIC from other groups	T-Mobil	7.1	Information	S3-000155	Input by Secretary, updated and replaced by TD155
S3-000111	CR to 33.102: Conversion function c3 at USIM	Ericsson	8.3	Approval	S3-000160	CR051 revised in TD 159
S3-000112	CR to 33.102: Trigger points of AFR during AKA	Ericsson	8.3	Approval		CR052 revised in TD 160
S3-000113	CR to 33.102: Removal of EUIC from 'Authentication Data Request' procedure	Ericsson	8.3	Approval	S3-000163	CR053 revised in TD 163
S3-000114	CR to 33.102: Clarification of the scope	Ericsson	8.3	Approval	S3-000161	CR054 revised in TD 161
S3-000115	CR to 33.102: SQN Generation Requirements	Ericsson	8.3	Approval		CR055 Approved
S3-000116	CR to 33.102: Identification of temporary identities	Ericsson	8.3	Approval	S3-000162	CR056 revised in TD 162
S3-000117	CR to 33.102: Cipher key and integrity key selection	Ericsson	8.3	Approval		CR057 Approved
S3-000118	CR to 33.102: Clarification on ciphering and integrity mode setting	Ericsson	8.3	Approval	S3-000167	CR058 revised in TD 137
S3-000119	CR to 33.102: Clarification on when integrity protection is started	Ericsson	8.3	Approval		CR059 Approved
S3-000120	CR to 33.102: Clarification on the security mode set-up message sequence flow	Ericsson	8.3	Approval		CR060 to be approved by e-mail. Common proposal needed with TD 195 (Siemens)

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comment
S3-000121	CR to 33.102: Unsuccessful integrity check	Ericsson	8.3	Approval	S3-000168	CR061 revised in TD 168
S3-000122	CR to 33.102: Clarification on signalling messages to be integrity protected	Ericsson	8.3	Approval	S3-000176	CR062 revised in TD 176
S3-000123	CR to 33.102: Clarification of the HFN handling	Ericsson	8.3	Approval	S3-000177	CR063 revised in TD 177
S3-000124	LS to CN WG1, RAN WG2 and T WG3 on USIM triggered authentication and key setting during PS connections	SA WG3	5.2	Update and Approval	S3-000153	Revised for transmission in TD153
S3-000125	CR to 33.102: Distribution and Use of Authentication Data between VLRs/SGSNs	Ericsson	8.3	Approval	S3-000179	CR064 revised in TD 179 Alternative approach provided in TD 209->212
S3-000126	CR to 33.102: Interoperation and intersystem handover/change between UTRAN and GSM BSS	Ericsson	8.3	Approval	S3-000185	CR047r1 revised in TD 185
S3-000127	CR to 33.102: Authentication and key agreement	Siemens Atea	8.3	Approval		CR065 (Not handled at meeting)
S3-000128	CR to 33.102: Ciphering	Siemens Atea	8.3	Approval	S3-000220	CR066 - for e-mail approval after the meeting. Revised in TD 220
S3-000129	CR to 33.102: Data integrity	Siemens Atea	8.3	Approval		CR067 - for e-mail approval after the meeting
S3-000130	CR to 33.102: Interoperation and intersystem handover/change between UTRAN and GSM BSS	Siemens Atea	8.3	Approval		CR068 (does not fulfil SA WG1 requirements)
S3-000131	CR to 33.102: Local authentication and connection establishment	Siemens Atea	8.3	Approval		CR069 (Does not take revised CRs into account)
S3-000132	CR to 33.102: User identity confidentiality	Siemens Atea	8.3	Approval		CR070 (does not take into account CR065 and TD S3-000197)
S3-000133	CR to 25.301: Ciphering and Integrity	Siemens Atea	8.3	Agreement		RAN WG2 document
S3-000134	CR to 33.105: Ciphering	Siemens Atea	8.5	Approval		CR009 - Approved by e-mail after the meeting 09/03/00
S3-000135	CR to 33.105: Data integrity	Siemens Atea	8.5	Approval		CR010 - Approved by e-mail after the meeting 09/03/00
S3-000136	Discussion on CRs on ciphering	Siemens Atea	8.3	Approval		
S3-000137	GPRS encryption	Siemens Atea	6.1	Approval		
S3-000138	CR to 33.103: Alignment of integration Guidelines with Security Architecture at S3#10	BT	8.4	Approval		CR006 - Approved by e-mail after the meeting 09/03/00
S3-000139	Distribution and Use of Current Security Context Data	Ericsson	8.3	Approval		incl CRs 33.102 CR034, CR046
S3-000140	02.09-450	MCC	6.3	Information		Noted
S3-000141	0209-520	MCC	6.3	Information		Noted
S3-000142	0209-610	MCC	6.3	Information		Noted
S3-000143	0209-710	MCC	6.3	Information		Noted
S3-000144	CR to 29.060: Distribution of security data	Ericsson	8.3	Information		CN document
S3-000145	LS from CN WG2 on comments to Enhanced User Identity Confidentiality	CN WG2	7.1	Discussion		Indirectly answered in TD 196

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comment
S3-000146	LS from SPAN6 to SMG10 on Lawful Interception (LI) in the IN environment	SPAN 6	5.4	Information		Noted. To be forwarded to SMG10 WPD Chairman
S3-000147	CR to 33.102: Use of default IK at emergency call with no (U)SIM or when authentication has failed	Ericsson	8.3	Approval	S3-000178	CR071 revised in TD 178
S3-000148	CR to 33.102: Clarification on ciphering and integrity protection at intersystem handover	Ericsson	8.3	Approval		CR072 Approved
S3-000149	Draft CR on 33.102 about local authentication	Nokia	8.3	Decision		Approved by e-mail after the meeting 09/03/00
S3-000150	Initial status report of specifications which implement ciphering and integrity protection	Nokia	7.4	Discussion		
S3-000151	CR to 33.102: MAP Security	SA WG3	8.3	Approval	S3-000189	CR073 revised and approved in TD 189
S3-000152	Proposed LS to SA WG5 on Functions of Key Distribution and Key Administration for MAP security	T-Mobil / T-Nova	5.2	Discussion / Approval	S3-000190	revised in TD 190
S3-000153	LS to CN WG1, RAN WG2 and T WG3 on USIM triggered authentication and key setting during PS connections (revised TD 124)	SA WG3	5.2	Approval	S3-000213	Approved by e-mail after the meeting 09/03/00 Output LS in TD 213
S3-000154	Response LS to SAGE on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms	SA WG3	5.4	Approval	S3-000171	revised proposal in TD 171
S3-000155	Related CRs and documents on EUIC from other groups (revised TD 110)	T-Mobil	7.1	Information		
S3-000156	CRs from S1 on GPRS encryption	Vodafone-Airtouch				To be updated by P Howard
S3-000157	Draft Reply to the LS R2-000282	SA WG3	5.2	Approval	S3-000158	Revised and approved in TD158
S3-000158	Reply to the LS R2-000282	SA WG3	5.2			Approved
S3-000159	CR051r1 to 33.102 (revised TD 111)	Ericsson	8.3	Approval		CR051r1Approved
S3-000160	CR052r1 to 33.102: Conversion function c3 at USIM (revised TD 112)	Ericsson	8.3	Approval		CR052r1 Approved
S3-000161	CR054r1 to 33.102: Clarification of the scope (revised TD114)	Ericsson	8.3	Approval		CR054r1 Approved
S3-000162	CR056r1 to 33.102: Identification of temporary identities (revised TD116)	Ericsson	8.3	Approval		CR056r1Approved
S3-000163	CR053r1 to 33.102: Removal of EUIC from 'Authentication Data Request' procedure (revised TD 113)	Ericsson	8.3	Approval		CR053r1 Approved
S3-000164	LS from SMG9 to SA WG3 (and SA WG1) on New SIM toolkit feature: "Auto-answer & Mute-ringing"	SMG9	5.2	Discussion		Not dealt with
S3-000165	Response to T3-99-432, "LS on 'Clarification of the information storage in USIM"	SA WG2	5.2	Information		Not dealt with
S3-000166	Draft Reply to Liaison on TIPHON Quality of Service	SA WG2 / SMG12	5.2	Information		Not dealt with
S3-000167	CR to 33.102: Clarification on ciphering and integrity mode setting (revised TD 118)	Ericsson	8.3	Approval		CR058r1 approved
S3-000168	CR061r1 to 33.102: Unsuccessful integrity check (revised TD 121)	Ericsson	8.3	Approval		CR061r1 approved
S3-000169	Liaison to RAN WG2 (response to TD 103)	SA WG3	5.2	Approval	S3-000202	Revised and approved in TD 202
S3-000170	3G Security Guide					
S3-000171	Reply liaison to ETSI SAGE on Delivery of algorithm specifications (revision of TD 154)	SA WG3	5.4	Approval	S3-000200	Agreed document in TD 200
S3-000172	Presentation of the USECA project	USECA Project	13	Information		Noted
S3-000173	Proposed MAP Security status report	Drafting group		Approval	S3-000187	revised in TD 187
S3-000174	Proposed LS to CN WG2 concerning the status of MAP Security	Drafting group		Approval	S3-000188	Revised in TD 188

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comment
S3-000175	3G Capabilities and Security Review Framework (Draft)	BT	7.4	Discussion		Not presented. Document noted and input to meeting#12
S3-000176	CR to 33.102: Clarification on signalling messages to be integrity protected (revision of TS 122)	Ericsson	8.3	Approval		CR062r1 approved
S3-000177	CR to 33.102: Clarification of the HFN handling (revisen of TD 123)	Ericsson	8.3	Approval		CR063r1 Approved
S3-000178	CR to 33.102: Use of default IK at emergency call with no (U)SIM or when authentication has failed (revised TD 147)	Ericsson	8.3	Approval		CR071r1 Approved by e-mail after the meeting 09/03/00
S3-000179	CR to 33.102: Distribution and Use of Authentication Data between VLRs/SGSNs (revised TD 125)	Ericsson	8.3	Approval	S3-000212	CR064r1 Approved, Later unapproved after e-mail discussion? Revised in TD 212
S3-000180	Proposed LS from S3 on TR45 acceptance of 3GPP for ESA (revision of S3-000085)	SA WG3		Approval	S3-000199	Revised in TD 199
S3-000181	TR 33.900 V1.3.0					
S3-000182	CR 045r2 to 33.102: Refinement of EUIC (revision no. 1 of S3-000098)	T-Mobil	7.1	Approval	S3-000197	CR045r2 revised in TD 197
S3-000183	CR to 33.103: Refinement of EUIC according to 33.102 (revision of TD 099)	T-Mobil	7.1	Approval	S3-000198	CR005r1 revised in TD 198
S3-000184	CR to 03.20 on clarification of GPRS encryption	Vodafone-Airtouch		Approval		CR A023 Approved, CRs A022 and A024 created for R97 and R99 (Approved)
S3-000185	CR to 33.102: Interoperation and intersystem handover/change between UTRAN and GSM BSS (revision of TD 126)	Ericsson	8.3	Approval		CR047r2 - for e-mail approval after the meeting. Alternative approach provided in TD 208
S3-000186	EUIC report	Drafting group			S3-000196	revised in TD 196
S3-000187	MAP Security status report	Drafting group		Approval		Approved
S3-000188	LS to CN WG2 concerning the status of MAP Security	Drafting group		Approval		Approved
S3-000189	CR073r1 to 33.102: MAP Security	SA WG3	8.3	Approval		CR073r1 approved
S3-000190	LS to SA WG5 on Functions of Key Distribution and Key Administration for MAP security	SA WG3	5.2	Approval		Approved
S3-000191	Input paper for discussion of GPRS encryption	Vodafone-Airtouch / France Telecom			S3-000201	revised in TD 201
S3-000192	Draft LS to CN WG1 on rejection of non-ciphered connections in GPRS				S3-000206	Updated as LS in TD 206 to send with TD205 attached
S3-000193	CR to 33.102 on Cipher key and integrity key lifetime	Vodafone-Airtouch		Approval		CR076 Approved by e-mail after the meeting 09/03/00
S3-000194	CR to 33.102 on Cipher key and integrity key setting	Vodafone-Airtouch		Approval		CR077 Approved by e-mail after the meeting 09/03/00

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comment
S3-000195	CR to 33.102 Cipher mode negotiation	Siemens Atea	7.1	Approval		To be approved by e-mail. Common proposal needed with TD 120 (Ericsson)
S3-000196	LS to TSG SA and CN WG2 : EUIC status	SA WG3		Approval		Approved
S3-000197	CR 045r3 to 33.102: Refinement of EUIC (revision of S3-000182)	T-Mobil	7.1	Approval		CR045r3 Agreed for presentation to SA
S3-000198	CR005r2 to 33.103: Refinement of EUIC according to 33.102 (revision of TD 183)	T-Mobil	7.1	Approval		CR005r2 Agreed for presentation to SA
S3-000199	Proposed LS from S3 on TR45 acceptance of 3GPP for ESA (revision of S3-000180)	SA WG3		Approval	S3-000204	revised in TD 204
S3-000200	Reply liaison to ETSI SAGE on Delivery of algorithm specifications (revision of TD 171)	SA WG3	5.4	Approval		Approved
S3-000201	Input paper for discussion of GPRS encryption	Vodafone-Airtouch / France Telecom			S3-000205	revised in TD 205
S3-000202	Response LS to RAN WG3 on RANAP Signalling procedures in case of Unsuccessful Integrity Check (revision of TD 169)	SA WG3		Approval		Approved
S3-000203	LS to RAN WG2 concerning the integrity protection mechanism	SA WG3		Approval		Approved
S3-000204	Proposed LS from S3 on TR45 acceptance of 3GPP for ESA (revision of S3-000180)	SA WG3		Approval	S3-000214	e-mail approval. Revision marks removed in TD 210 for transmission to TR-45
S3-000205	Discussion paper for GPRS encryption (revision of TD 201)	SMG10 / SA WG3		Approval		Approved and attached to TD 206
S3-000206	LS to SMG3/CN WG1: Introduction of rejection of non ciphered calls for GPRS	SMG10 / SA WG3		Approval		Approved and TD 205 attached
S3-000207	CR078 to 33.102: Conversion functions	Siemens Atea		Approval		e-mail approval
S3-000208	CR to 33.102: Interoperation and intersystem handover/change between UTRAN and GSM BSS (revision of TD 126)	Ericsson		Approval		CR047r2. Rev2 of TD 126. Approved by e-mail after the meeting
S3-000209	CR to 33.102: Distribution and Use of Authentication Data between VLRs/SGSNs (revision(2) of TD 125)	SA WG3		Approval	S3-000212	CR064rX - revision(2) of TD 125
S3-000210	LS to TR-45: Proposed Procedures for joint control of 3GPP AKA specifications (revised TD 204)	SA WG3		Approval		Approved by e-mail
S3-000211	TR-45 Committee Correspondence: re: Principles for Global Authentication,	TR-45		Discussion		Response in TD 210
S3-000212	CR to 33.102: Distribution and Use of Authentication Data between VLRs/SGSNs (revision of TD 209)	SA WG3		Approval		CR064r2 - revision of TD 209 aligned with other CRs. Approved by e-mail after the meeting
S3-000213	LS to CN WG1, RAN WG2 and T WG3 on USIM triggered authentication and key setting during PS connections (Output of approved draft in TD153)	SA WG3	5.2	Approval		Approved

Annex B: List of attendees

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.	Brown	Daniel	Motorola Inc.		T1	US
Mr.	Castagno	Mauro	OMNITEL	mauro.castagno@omnitel.it	ETSI	IT
Dr.	Chen	Lily	Motorola Inc.	lchen1@email.mot.com	T1	US
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
Mr.	Herrmann	Christoph	PHILIPS GmbH	herrmann@pfa.research.philips.com	ETSI	DE
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.	Ishii	Kazuhiko	NTT DoCoMo	ishii@mml.yrp.nttdocomo.co.jp	ARIB	JP
Mr.	Jaczynski	Rafal	POLKOMTEL S.A.	rafal.jaczynski@polkomtel.com.pl	ETSI	PL
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
Dr.	Schmitz	Roland	Deutsche Telekom AG	schmitz@tzd.telekom.de	ETSI	DE
Mr.	Tellanos	David	ERICSSON L.M.	davis.castellunos-damca@ece.ericsson.se	ETSI	SE
Mr.	Tietz	Benno	MANNESMANN Mobilfunk GmbH	benno.tietz@d2mannesmann.de	ETSI	DE
Mr.	Toye	Peter	ALCATEL BELL	peter.toye@alcatel.be	ETSI	BE
Mr.	Trautmann	Peter	BMWi	peter.trautmann@regtp.de	ETSI	DE
Mr.	Vinck	Bart	SIEMENS ATEA NV	bart.vinck@vnet.atea.be	ETSI	BE
Dr.	Wasel	Josef	PHILIPS GmbH	josef.wasel@philips.com	ETSI	DE
Mr.	Wilhelm	Berthold	BMWi	berthold.wilhelm@regtp.de	ETSI	DE

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

C.1 SA WG3 specifications

Specification			Title		Editor**	Comment
TS	21.133	3.1.0	Security Threats and Requirements	April 99	Per Christoffersson	CR@TSG#6
TS	22.022	3.0.1	Personalisation of GSM ME Mobile functionality specification - Stage 1	Oct 99		
TS	33.102	3.3.1	Security Architecture	Mar 00	Bart Vinck	CR@TSG#6
TS	33.103	3.1.0	Security Integration Guidelines	Oct 99	Bart Vinck	CR@TSG#6
TS	33.105	3.2.0	Cryptographic Algorithm requirements	June 99	Bart Vinck	CR@TSG#6
TS	33.106	3.1.0	Lawful interception requirements	Jun 99	Bart Vinck	CR@TSG#6
TS	33.107	3.0.0	Lawful interception architecture and functions	Dec 99		New at TSG#6
TS	33.120	3.0.0	Security Objectives and Principles	April 99	Tim Wright	
TR	33.900	1.0.0	Guide to 3G security	Dec 99		New at TSG#6
TR	33.901	3.0.0	Criteria for cryptographic Algorithm design process	June 99	Vinck Bart	

** 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
01.33	7.0.0	Lawful Interception requirements for GSM	Release 1998			
01.61	6.0.1	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
02.31	7.1.1	Fraud Information Gathering System (FIGS) Service description - Stage 1	Release 1998	TS	101 107	RTS/SMG-100231Q7
02.32	7.1.1	Immediate Service Termination (IST); Service description - Stage 1	Release 1998	TS	101 749	DTS/SMG-100232Q7
02.33	7.3.0	Lawful Interception - Stage 1	Release 1998	TS	101 507	DTS/SMG-100233Q7
02.48	6.0.0	Security mechanisms for the SIM Application Toolkit; Stage 1	Release 1997	TS	101 180	DTS/SMG-090248Q6
02.48	7.0.0	Security mechanisms for the SIM Application Toolkit; Stage 1	Release 1998	TS	101 180	RTS/SMG-090248Q7
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	5.3.0	Security-related Network Functions	Phase 2+			
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
03.31	7.0.1	Fraud Information Gathering System (FIGS); Service description - Stage 2	Release 1998			
03.33	7.1.0	Lawful Interception - stage 2	Release 1998	TS	101 509	DTS/SMG-100333Q7
03.35	7.0.0	Immediate Service Termination (IST); Stage 2	Release 1998			

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

D.1 SA WG3 CRs at the Meeting

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	New Vers	Date	Source	WG	WG meeting	WG TD	WG status	Work item
33.102	045	1	R99	Refinement EUIC	F	3.3.0		18/02/2000	T-Mobil	S3	S3-11	S3-000098	revised	Security
33.102	045	2	R99	Refinement EUIC	F	3.3.0		18/02/2000	T-Mobil	S3	S3-11	S3-000182	revised	Security
33.102	045	3	R99	Refinement EUIC	F	3.3.0		18/02/2000	T-Mobil	S3	S3-11	S3-000197		Security
33.102	047	1	R99	Interoperation and intersystem handover/change between UTRAN and GSM BSS	C	3.3.1		21/02/2000	Ericsson	S3	S3-11	S3-000126	revised	Security
33.102	047	2	R99	Interoperation and intersystem handover/change between UTRAN and GSM BSS	C	3.3.1		21/02/2000	Ericsson	S3	S3-11	S3-000126		Security
33.102	050		R99	Refinement of Cipher key and integrity key lifetime	F	3.3.1		18/02/2000	T-Mobil	S3	S3-11	S3-000101		Security
33.102	051		R99	Conversion function c3 at USIM	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000111	revised	Security
33.102	051	1	R99	Conversion function c3 at USIM	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000159	agreed	Security
33.102	052		R99	Trigger points of AFR during AKA	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000112	revised	Security
33.102	052	1	R99	Trigger points of AFR during AKA	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000160	agreed	Security
33.102	053		R99	Removal of EUIC from 'Authentication Data Request' procedure	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000113	revised	Security
33.102	053	1	R99	Removal of EUIC from 'Authentication Data Request' procedure	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000163	agreed	Security
33.102	054		R99	Clarification of the scope	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000114	revised	Security
33.102	054	1	R99	Clarification of the scope	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000161	agreed	Security
33.102	055		R99	SQN Generation Requirements	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000115	agreed	Security
33.102	056		R99	Identification of temporary identities	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000116	revised	Security
33.102	056	1	R99	Identification of temporary identities	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000162	agreed	Security
33.102	057		R99	Cipher key and integrity key selection	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000117	agreed	Security
33.102	058		R99	Clarification on ciphering and integrity mode setting	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000118	revised	Security
33.102	058	1	R99	Clarification on ciphering and integrity mode setting	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000167	agreed	Security
33.102	059		R99	Clarification on when integrity protection is started	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000119	agreed	Security
33.102	060		R99	Clarification on the security mode set-up message sequence flow	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000120		Security
33.102	061		R99	Unsuccessful integrity check	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000121		Security
33.102	062		R99	Clarification on signalling messages to be integrity protected	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000122	revised	Security
33.102	062	1	R99	Clarification on signalling messages to be integrity protected	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000176	agreed	Security
33.102	063		R99	Clarification of the HFN handling	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000123	revised	Security
33.102	063	1	R99	Clarification of the HFN handling	F	3.3.1		18/02/2000	Ericsson	S3	S3-11	S3-000177	agreed	Security
33.102	064		R99	Distribution and Use of Authentication Data between VLRs/SGSNs	F	3.3.1		21/02/2000	Ericsson	S3	S3-11	S3-000125	revised	Security

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	New Vers	Date	Source	WG	WG meeting	WG TD	WG status	Work item
33.102	064	1	R99	Distribution and Use of Authentication Data between VLRs/SGSNs	F	3.3.1		21/02/2000	Ericsson	S3	S3-11	S3-000179	agreed	Security
33.102	065		R99	Authentication and key agreement	D	3.3.1		21/02/2000	Siemens Atea	S3	S3-11	S3-000127	postponed	Security
33.102	066		R99	Ciphering	C	3.3.1		21/02/2000	Siemens Atea	S3	S3-11	S3-000128		Security
33.102	067		R99	Data integrity	C	3.3.1		21/02/2000	Siemens Atea	S3	S3-11	S3-000129		Security
33.102	068		R99	Interoperation and intersystem handover/change between UTRAN and GSM BSS	C	3.3.1		21/02/2000	Siemens Atea	S3	S3-11	S3-000130		Security
33.102	069		R99	Local authentication and connection establishment	C	3.3.1		21/02/2000	Siemens Atea	S3	S3-11	S3-000131		Security
33.102	070		R99	User identity confidentiality	C	3.3.1		21/02/2000	Siemens Atea	S3	S3-11	S3-000132		Security
33.102	071		R99	Use of default IK at emergency call with no (U)SIM or when authentication has failed	F	3.3.1		22/02/2000	Ericsson	S3	S3-11	S3-000147	revised	Security
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		22/02/2000	Ericsson	S3	S3-11	S3-000178		Security
33.102	072		R99	Clarification on ciphering and integrity protection at intersystem handover	F	3.3.1		22/02/2000	Ericsson	S3	S3-11	S3-000148	agreed	Security
33.102	073		R99	MAP Security	D	3.3.1		22/02/2000	S3	S3	S3-11	S3-000151	revised	Security
33.102	073	1	R99	MAP Security	D	3.3.1		22/02/2000	S3	S3	S3-11	S3-000189	agreed	Security
33.102	074		R99	Clarification about CK and IK which are transmitted in clear over the Iu-interface	B	3.3.1		28/02/2000	Telenor	S3	S3-11	S3-000108		Security
33.102	075		R99	Local Authenication and connection establishment	F	3.3.1		28/02/2000	Nokia	S3	S3-11	S3-000149		Security
33.102	076		R99	Cipher key and integrity key lifetime	F	3.3.1		28/02/2000	Vodafone-Airtouch	S3	S3-11	S3-000193		Security
33.102	077		R99	Cipher key and integrity key setting	F	3.3.1		28/02/2000	Vodafone-Airtouch	S3	S3-11	S3-000194		Security
33.103	005		R99	Refinement EUIC (according to TS 33.102)	F	3.1.0		18/02/2000	T-Mobil	S3	S3-11	S3-000099	revised	Security
33.103	005	1	R99	Refinement EUIC (according to TS 33.102)	F	3.1.0		18/02/2000	T-Mobil	S3	S3-11	S3-000183	revised	Security
33.103	005	2	R99	Refinement EUIC (according to TS 33.102)	F	3.1.0		18/02/2000	T-Mobil	S3	S3-11	S3-000198		Security
33.103	006		R99	Alignment of integration Guidelines with Security Architecture at S3#10	F	3.1.0		21/02/2000	BT	S3	S3-11	S3-000138		Security
33.105	008		R99	Refinement of EUIC (according to 33.102)	F	3.2.0		18/02/2000	T-Mobil	S3	S3-11	S3-000100		Security
33.105	009		R99	Ciphering	C	3.2.0		21/02/2000	Siemens Atea	S3	S3-11	S3-000134		Security
33.105	010		R99	Data integrity	D	3.2.0		21/02/2000	Siemens Atea	S3	S3-11	S3-000135		Security

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	Work item
03.20	A022		R97	GPRS encryption	F	6.1.0		28/02/2000	SMG10	10	S3-11		agreed	GPRS
03.20	A023		R98	GPRS encryption	A	7.2.0		28/02/2000	SMG10	10	S3-11	S3-000184	agreed	GPRS
03.20	A024		R99	GPRS encryption	A	8.0.0		28/02/2000	SMG10	10	S3-11		agreed	GPRS

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD Number	Title	Source	Comment
S3-000102	LS on an L2&3 based procedure to check whether the UE uses the correct new cipher key during the cipher key change procedure	RAN WG2	Response in TD S3-000158
S3-000103	LS on RANAP Signalling procedures in case of Unsuccessful Integrity check	RAN WG3	Response in TD S3-000202
S3-000104	Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms	ETSI SAGE	Response in TD S3-000200
S3-000105	General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms	ETSI SAGE	Report noted: (Response included in TD S3-000200)
S3-000107	Reply LS on additional Terminal Baseline Implementation Capabilities for secure interoperation with GSM	SA WG1	Noted
S3-000109	System behaviour on receipt of an invalid Message Authentication Code (MAC)	CN WG1	Not dealt with
S3-000145	LS from CN WG2 on comments to Enhanced User Identity Confidentiality	CN WG2	Indirectly answered in TD S3-000196
S3-000146	LS from SPAN6 to SMG10 on Lawful Interception (LI) in the IN environment	SPAN 6	Noted. To be forwarded to SMG10 WPD Chairman
S3-000164	LS from SMG9 to SA WG3 (and SA WG1) on New SIM toolkit feature: "Auto-answer & Mute-ringing"	SMG9	Not dealt with
S3-000165	Response to T3-99-432, “LS on 'Clarification of the information storage in USIM”	SA WG2	Not dealt with (for information)
S3-000166	Draft Reply to Liaison on TIPHON Quality of Service	SA WG2 / SMG12	Not dealt with (for information)

E.2 Liaisons from the meeting

TD Number	Title	Status	Comment
S3-000153	LS to CN WG1, RAN WG2 and T WG3 on USIM triggered authentication and key setting during PS connections (revised TD 124)	Not dealt with	e-mail approval after meeting Approved in TD 213.
S3-000158	Reply to the LS R2-000282	Approved	Sent.
S3-000188	LS to CN WG2 concerning the status of MAP Security	Approved	Sent.
S3-000190	LS to SA WG5 on Functions of Key Distribution and Key Administration for MAP security	Approved	Sent.
S3-000196	LS to TSG SA and CN WG2 : EUIC status	Approved	Sent.
S3-000200	Reply liaison to ETSI SAGE on Delivery of algorithm specifications (revision of TD 171)	Approved	Sent.
S3-000202	Response LS to RAN WG3 on RANAP Signalling procedures in case of Unsuccessful Integrity Check	Approved	Sent.
S3-000203	LS to RAN WG2 concerning the integrity protection mechanism	Approved	TD S3-000150 and TD S3-000168 attached. Sent.
S3-000204	Proposed LS from S3 on TR45 acceptance of 3GPP for ESA (revision of S3-000180)	Not dealt with	e-mail approval after meeting. Approved in TD 210.
S3-000206	LS to SMG3/CN WG1: Introduction of rejection of non ciphered calls for GPRS	Approved	TD S3-000205 attached. Sent.
S3-000210	LS to TR-45: Proposed Procedures for joint control of 3GPP AKA specifications (revised TD 204)	Approved	Sent.
S3-000213	LS to CN WG1, RAN WG2 and T WG3 on USIM triggered authentication and key setting during PS connections (Output of approved draft in TD153)	Approved	Sent.

Annex F: List of Actions from the meeting

ACTION #11/1:	**TD S3-000200 to be sent to SAGE and TSG SA. (M Pope)**
ACTION #11/2:	**TD S3-000146 to be forwarded to SMG10 WPD Chairman. (M. Pope)**
ACTION #11/3:	**M Pope to send TD S3-000204 to group for e-mail discussion.**
ACTION #11/4:	**Liaison in TD S3-000206 to be forwarded to CN WG1. (M. Pope)**
ACTION #11/5:	**TD S3-000156 to be be updated with results of discussions. (P. Howard)**
ACTION #11/6:	**LS in TD S3-000190 to be transmitted to SA WG5. (M Pope)**
ACTION #11/7:	**LS in TD S3-000188 to be transmitted to CN WG2. (M Pope)**
ACTION #11/8:	**LS in TD S3-000190 to be transmitted to SA WG5 and SA WG2. (M Pope)**
ACTION #11/9:	**Chairman to report this to TSG SA Plenary.**
ACTION #3/10:	**All to review the identified specifications and feedback results to G. Køien for the joint CN WG2B / SA WG3 meeting (ALL)**
ACTION #11/11:	**All: Review the draft document which will be discussed at the next meeting of SA WG3.**
ACTION #11/12:	**M Pope to send CR071r1 to CN WG1 when agreed by e-mail.**
ACTION #11/13:	**All to review and approve the CR in TD S3-000149 by 1 March 2000.**
ACTION #11/14:	**Send TD S3-000203 to RAN WG2 (M Pope).**
ACTION #11/15:	**M Pope to organise e-mail approval of outstanding CRs. S. Pütz to present a list of TDs allowed for email approval.**