3GPP TSG SA WG3 Security — S3#10 **S3-000096**

19-21 January, 2000

Antwerp, Belgium

Source: **Secretary, Maurice Pope, MCC**

Title: **Draft Report of SA WG3 Meeting #10, Draft version 1.0.0**

Document for: **Approval**

The 'Osterrieth' house on the Meir, Antwerp

Contents

1 Opening of the meeting

The Chairman of SA WG3, Prof. M Walker explained that he is unable to chair the meetings until after March 2000 due to Governmental instructions to remain independent with regards to auction work in Vodafone Airtouch. The Vice Chairman, Dr. S. Pütz agreed to chair the meetings while this situation continued.

2 Approval of the agenda

TD S3-000021: A minor re-scheduling to allow Prof. Walker to be available for agenda items 8.2 and 8.3 was agreed. A new item 8.4 "Terminal Security" and item 7.2 "A5/1" were added to the agenda. With these changes, the agenda was approved.

3 Registration and assignment of input documents

The available documents were allocated to agenda items as appropriate.

4 Approval of meeting reports

4.1 TSG-SA3 Meeting no. 9

TD S3-000022: A new version of the report is given in TD S3-000067. To allow all delegates a review of this report in detail, 28th January 2000 was agreed as deadline for any comments and objections.

A rapporteur for 22.022 is needed. It was suggested that the same company as before in SA WG1 nominates a Rapporteur. Peter Howard will take over in the interim.

4.2 TSG-SA3 Ad Hoc Meeting with Experts from N1 and N2

TD S3-000016: Draft Report of 3GPP joint meeting of experts on open R99 security issues - draft 04. The draft report was presented by Peter Howard. Decisions and Actions are given at the end of the report. The report was undergoing e-mail approval until 20 January 2000. The report was noted by SA WG3.

5 Reports / Liaisons from other 3GPP and SMG groups

5.1 3GPP and SMG plenary

TD S3-000029: This extract of the TSG SA#6 meeting report was checked and some comments given. These comments will be taken into account in the next version of the TSG SA#6 report.

TD S3-000030: Notes on the SA WG3 presentation to TSG SA#6. This document was noted for information.

TD S3-000045: Invitation to the IP Workshop. This was noted for information.

TD S3-000054: Presentation given to the SA#6 meeting. This was noted for information. Slide 30 bullet 2 was clarified to mean that Mobile IP Security will not affect the 3G Security.

5.2 3GPP WGs and SMG STCs

TD S3-000023: Liaison statement to SA WG3 on USIM-Terminal Link. It was agreed that 22.022 is a part of Release 1999. The multiple GID-value issue was considered to be a matter for SA WG1. A response liaison statement to T WG3, copied to SA WG1 was prepared and is contained in TD S3-000061.

TD S3-000024: Response to the liaison statement (from SA WG2) on 'Clarification of the information storage in USIM'. This liaison statement was noted for information. A response from SA WG2 is awaited on this. It was agreed that some information may be available from the SA WG2 meeting report and this would be checked and the issue re-visited later in the meeting. The report was not available during the meeting and the issue was postponed.

TD S3-000028: Statement on security issues in VHE/OSA. This states that the encrypted IMSI is not needed for VHE. This appeared to be a mis-understanding and it was agreed to produce a response on this part of the liaison statement. This is contained in TD S3-000062.

TD S3-000056: Liaison statement on Enhanced User Identity Confidentiality – open questions. The main confidentiality problem is related to the sending of the IMSI in clear (especially during paging). Some problems have been identified and are recognised by SA WG3, but there is some time to tackle them for Release 1999. It was decided to prepare a liaison statement in response to this document, which is contained in TD S3-000063. This was discussed and comments made. An updated version is contained in TD S3-000069. This was again updated and the final version is given in TD S3-000087.

5.3 3GPP partners

No documents.

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

TD S3-000025: Finalisation of the f8 and f9 algorithm design work. Report from SAGE stating that the reports have been delivered. This was reported under agenda Item 8.2 and was noted.

TD S3-000026: Results of independent evaluation of 3GPP f8 and f9 algorithms. This reports the results of the evaluation and was noted.

TD S3-000027: Extension of shortened keys to full-length keys. This suggests replacing the practice of '0' padding short keys to make a longer key, to repeat the sequence of the shorter key. This requires a CR to 33.102 to include this functionality. See also the action under item 9.5.

TD S3-000053: TR45 Comittee Correspondence in response to Liaison from SA WG3. This was noted for information.

6 Amalgamation of S3 and SMG10

After consideration on this by the Members of the Security group, it was agreed that the two groups should meet together, but the 3GPP specific and GSM Specific work should be tackled separately on the agenda. The report of the SMG10 part of the meetings should be produced separately and stored only on the SMG10 area of the ETSI Server (i.e. it shall not be stored on the 3GPP SA WG3 server).

%Move into SMG10 Report%

7 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.

8 3G security issues

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

TD S3-000015: This Liaison was discussed, modified slightly and a contact person added. The resulting liaison statement, given in TD S3-000060 was approved.

TD S3-000011: Presentation slides on MAP Security, and TD S3-000012: List of issues related to MAP Security. The objectives for protection of a minimum set of messages in the MAP for Release 1999 was presented. The protection of 4 application contexts, authentication messages between VLR and HLR and subscriber registration data are proposed for Release 1999. Further messages should be protected for Release 2000.

The feasibility of completion of this for Release 1999 was questioned. The changes will take quite a lot of work in CN to update the MAP messages specifications. The presented set of messages is considered a compromise between full security and what is achievable in Release 1999.

CN will be asked to include these changes for Release 1999 in priority as follows:

1 infoRetrievalContext
1 interVlrInfoRetrievalContext
2 networkFunctionalSsContext

2 anyTimeInfoHandlingContext

It was agreed to send a liaison statement to CN WG2 outlining the requirements and priorities, as what SA WG3 see as achievable for Release 1999. This Liaison is given in TD S3-000070. A prioritised list for other messages for Release 2000 will be produced at a future meeting.

The Key Management was discussed. The transport of secured keys over MAP could be specified in time for Release 1999, but this may produce a poor system which may need changing again. It was also questioned whether the transport needs to be standardised. It was emphasised that if the feature is to be included in Release 1999, then large resources are needed to produce the necessary CRs.

TD S3-000048: Enhancements on the extended Proposal for Securing MAP Based Transmission of Sensitive Data between Network Elements (Ericsson proposal). The proposed solution could not be implemented in time for Release 1999 MAP Security. It was not considered possible to modify the Release 1999 limited protection proposal in order to be compatible with this proposal in the remaining time-frame. The proposal will be used for further consideration as a solution for Release 2000 MAP Security. Companies interested in MAP Security were asked to consider this proposal and make comments at the next meeting.

TD S3-000059: Proposed liaison statement to CN , CN WG2 and TSG SA on MAP security. It was decided to convene a small group of interested people to re-draft the Liaison based upon the discussions at the meeting on MAP Security. The updated liaison is given in TD S3-000077.

Network-wide encryption: It was reported that the progress on inserting the hooks into the Release 1999 Core Network in preparation for Release 2000 Network-wide encryption was unclear. This would need to be re-evaluated at the next meeting of SA WG3 (meeting #11).

Authentication failure reporting: It was reported that CN WG2 has started to draft the necessary CRs. A concern in CN WG2 was raised regarding the need of an acknowledgement of authentication failure reporting. After a short discussion in SA WG3, the issue was seen as a mis-understanding between the groups. A CR was approved in TD S3-000076) removing the acknowledge part of the *Authentication Failure Report* mechanism.

8.2 Confidentiality/integrity algorithm

The algorithms had been finalised by ETSI SAGE and evaluations carried out, and proposed changes resolved.

ETSI have been told not to publish this by the French authorities, due to their claim that publishing the standards would constitute a violation of Wasenaar agreements, and claims from some Manufacturers that publication may make export difficult.

Meetings have been ongoing, but the results were not currently known.

A statement to allow the algorithm only to be used for 3GPP may be added to resolve the claimed problems.

US have published on the NIST web site many algorithms of equivalent strength to the 3GPP algorithms and the French authorities have been asked to reconsider.

SA WG3 are not in agreement with these claims and a letter concerning this has been sent to the ETSI Director-General asking for resolution and release of the algorithm.

It was reported that a development has occurred and the publication of the algorithm is not opposed by the French Authorities, but they wanted more details on the use and distribution of the algorithm.

8.3 Authentication algorithm

A letter was sent by the SA WG3 Chairman to the SAGE Chairman after the 8th SA WG3 meeting. A new liaison statement to SAGE was expected to be produced at the last SA WG3 meeting (Meeting #9), and SAGE have waited for this before responding to the first liaison. This liaison statement was not created due to timing of the SAGE meeting, as it was considered better to discuss the content of the liaison again in SA WG3.

A standard authentication algorithm is preferred, in order to provide a minimum level of security for all 3GPP networks, to remove the risk of some operators choosing a weak algorithm. The requirements for variety in the algorithm also needs to be considered when asking SAGE to do the work as this will affect their work. The inclusion

of variety reduces the risks if the algorithm is compromised, as not all operators will be affected by this. It also allows operators to have their own secret algorithm, providing a stronger defence against attacks.

After some discussion on the requirements to be forwarded to SAGE it was concluded that SAGE would be asked to design an algorithm with an operator-specific part as a preference, leaving the specific design parameters to SAGE, and with a timescale which will allow the algorithms to be available in time for early Release 1999 equipment production (publication by end of September 2000). SAGE will also be asked to produce a framework of the algorithm.

The liaison statement should also be copied to T WG3 where the 3GPP expertise lies for USIM (Cards). The liaison statement is contained in TD S3-00057. A revised version was agreed in TD S3-00089.

8.4 Terminal Security

TD S3-000052: 3GPP terminal identity security: levels, requirements and mechanisms. This was presented by Bosch using OHP slides in TD S3-000071. After some questions for clarification, the proposal was discussed in length, any many differing views were expressed. It was concluded that this cannot be included in Release 1999, but should be considered further for inclusion in Release 2000, when the possible impacts of changes to standards on other groups can be ascertained. It was generally agreed that a provable identity is desirable for 3GPP. Contributions on this are expected and e-mail discussions should be held by interested parties.

Non-ciphered mode in 3GPP: A cipher indicator had been agreed as a requirement for 3GPP which should be implemented on all terminals. This decision needs to be publicised more broadly to the other 3GPP groups. The relevant specifications will be reviewed to ensure that the other groups (e.g. T WG2) have taken this into account.

IP encryption: It was suggested that encryption for messages over an IP network should be mandated to prevent security problems, such as "channel hijack". This should be considered by members and it will be discussed at the next meeting (SA WG3 Meeting#11).

9 Review CRs to S3 specifications

9.1 TS 21.133 Threats and requirements

The action from SA WG3 meeting #9 on reviewing the specification was postponed to SA WG3 meeting #11. Input is required.

9.2 TS 22.022 Personalisation of ME

No input. (See agenda Item 4.1).

9.3 TS 33.102 Security architecture

TD S3-000041: Draft CR to TS 33.102 V 3.3.0 on Visibility and configurability. This CR was postponed to the next meeting, as the proposing company could not be present during discussions at this meeting. Either an updated version or the same document will be considered.

TD S3-000043: Draft CR to 33.102 v 3.3.1 on Clarification on cipher key and integrity key lifetime. This CR was agreed.

TD S3-000044: Draft CR to 33.102 v3.3.1 on local authentication and connection establishment. This CR was agreed.

TD S3-000046: CR to 33.102 v3.3.1: refinement of EUIC after S3/N2 meeting. Editorial modifications were made to the CR and it was agreed as TD S3-000081.

TD S3-000049: CR to 33.102 v3.3.1: Clarification on enhanced distribution of authentication data within one serving network domain. It was decided that a clarification is needed and the CR was postponed. A new version of the CR is expected for the next meeting.

TD S3-000050: CR to 33.102 v3.3.1: Interoperation and intersystem handover/change between UTRAN and GSM BSS. This was updated and resubmitted as TD S3-000079. This CR was discussed and some suggestions for modification made, it was decided to postpone this to the next meeting in order for an updated CR to be presented

including the agreements and clarifications made. The placing of conversion functions (e.g. in the USIM) was discussed. A liaison statement to T WG2 and T WG3 will be produced S. Nguyen Ngoc and is contained in TD S3-000083 A revised version, given in TD S3-000090 was agreed. E-mail discussions should be used before the next presentation of this CR. Items for discussion: Conversion of quintuplets to triplets in R99+, <please add items>.

TD S3-000051: CR to 33.102 v3.3.1: Clarification on the reuse of Avs. This CR was agreed.

TD S3-000076: 33.102 v 3.3.1, CR 049 on Authentication failure reporting. This CR was agreed with minor changes agreed at meeting #9.

TD S3-000047: Problems caused by 2G-3G interoperation. This document was presented by T-Mobil. It outlines the potential security problems with 2G-3G interoperation. This topic had been discussed at the SA WG3 meeting #5 (see TD S3-99217) and it was decided that there could be an impact on the 3G timescales if improvements are required for this in Release 1999. It should be investigated for inclusion in Release 2000. This should be re-visited at the next meeting, based upon further contribution.

TD S3-000074: Proposed CR to 33.102 section 6.4.3 on USIM triggered authentication and key setting during PS connections (TD S3-99549 from meeting#9). This was taken along with TD S3-000075: LS to CN WG1, RAN WG2 and T WG3 on USIM triggered authentication and key setting during PS connections (TD S3-99550 from meeting#9). It needs to be clarified whether this has been transmitted. More work on this is needed. This depends upon the trust in the serving network when authenticating packet-switched calls. Coordination with CN WG1 and T WG2 and T WG3 is needed to ensure that anything can be implemented.

It was decided to draft a liaison statement to T WG3, T WG2 and CN WG1. This will be agreed by e-mail after the meeting and transmitted.

Action: M. Pope to check whether the Liaison in TD S3-99550 has been sent and report to the group.

Action: P. Howard to draft a liaison statement and send it to the group for e-mail approval.

9.4 TS 33.103 Integration guidelines

TD S3-000034: The possible inconsistency in the use of UEA/UIA or of f8/f9 needs to be resolved. UEA/UIA indicate the group of algorithms, whereas f8 and f9 are the individual alogorithms. It was that the integration guidelines should use f8/f9 and equate them to the UEA/UIA, which describe the fields. It was proposed that this is clarified in the document. This will be done by a note in the document. A CR will be produced to include these changes.

9.5 TS 33.105 Algorithm requirements

TD S3-000078: CR006 to 33.105 v 3.2.0. Authentication and key agreement. It was agreed that this needs to be reviewed and a liaison to SAGE is needed about the use of f5 as optional (5.1.6.7). The updated CR is given in TD S3-000084

Action: V. Niemi and R. Blom to prepare a CR to include the SAGE recommendation to repeat keys instead of zero-padding for shorter key lengths.

TD S3-000082: CR007 to 33.105 v3.2.0 on Enhanced user confidentiality. This provides terminology changes to the document. (EMUI - EMSI and IMUI - IMSI). This CR was agreed, but the CR needs to be updated because some terminology changes remain (see TD S3-000082, A5). The subject should be "Editorial changes to Terminology".

9.6 TS 33.106 LI requirements

Some editorial errors have been found in the graphics. This will be updated with a CR at the next meeting.

9.7 TS 33.107 LI architecture

Some editorial errors have been found in the graphics. This will be updated with a CR at the next meeting.

9.8 TR 33.120 Security principles and objectives

No input.

9.9 TR 33.901 Criteria for algorithm design process

No input.

9.10 TR 33.902 Formal analysis

No input.

10 Review of draft 3G specifications

The following SA WG3 documents were provided for information and were noted. They are the latest versions after inclusion of relevant CRs after TSG SA Meeting #6.

TD S3-000031: 21.133 v 3.1.0: Security Threats and Requirements

TD S3-000032: 22.022 V 3.0.1: Personalisation of GSM ME Mobile functionality specification - Stage 1

TD S3-000033: 33.102 v 3.3.1: Security Architecture

TD S3-000034: 33.103 v 3.1.0: Security Integration Guidelines

TD S3-000035: 33.105 V 3.2.0: Cryptographic Algorithm requirements

TD S3-000036: 33.106 V 3.1.0: Lawful interception requirements

TD S3-000037: 33.107 V 3.0.0: Lawful interception architecture and functions

TD S3-000038: 33.120 V 3.0.0: Security Objectives and Principles

TD S3-000039: 33.901 V 3.0.0: Criteria for cryptographic Algorithm design process

TD S3-000040: 33.902 V 3.1.0: Formal Analysis of the 3G Authentication Protocol with Modified Sequence number Management

10.1 TR 33.900 Guide to 3G security

TD S3-000064: Presented for information. Comments are welcome. MAP Security was reported as missing and text will be drafted for the next meeting. This document is to be presented for approval at SA#7. **Mr. C. Brookson proposed an all-day editorial meeting to discuss the above document at the Department of Trade & Industry on the 16th February in London. Start at 0900, finish about 1600. Please email to cbrookson@iee.org if interested, to check meeting arrangements.**

Action: Delegates are asked to check the document 33.900 and make comments to the editor in good time before the next meeting.

11 3G security project plan – review of other specifications

The project plan is being submitted to SA WG2 with no changes since the last SA WG3 meeting. This will be reviewed at the next meeting.

TD S3-000072 provides a list of 3GPP specifications and their titles for information.

A review of the 3GPP specifications from other groups was thought desirable, to ensure that the correct interpretation of the security requirements has been made. It was suggested that features would be investigated by people, instead of looking at individual specifications. Responsibilities were assigned to identify documents and their features, and features and related documents. Brief status reports on each of the features should be provided to the group. The most important features will be provided to the group by e-mail by C. Blanchard.

Action: ***C Blanchard to send a matrix of features and importance to the group by e-mail.***

As a starting point, the following features will be checked:

- Authentication & Key Agreement;
  - K Geir agreed to take responsibility for the coordination of this work.
- Confidentiality and Integrity Protection;
  V. Niemi agreed to take responsibility for the coordination of this work.
- Secure 2G-3G Interworking.
  R Blom agreed to take responsibility for the coordination of this work.

Action: ***All: The protection of Security Parameters on the Iu interface needs to be considered for discussion at the next meeting.***

12 Any other business

no input.

13 Approval of liaison statements, CRs and draft specifications

TD S3-000062: Response to the Statement on security issues in VHE/OSA (TD S3-000028). The liaison statement was approved for transmission to SA WG1 and SA WG2.

TD S3-000069: Response to liaison statement on Enhanced User Identity Confidentiality – open questions. The liaison was modified slightly in TD S3-000087 and approved for transmission to CN WG1.

TD S3-000070: LS to CN WG2 on Protection of MAP Messages for Release 1999. The LS was approved for transmission to CN WG2.

TD S3-000061: Liaison statement to T3 and SA WG1 on ME personalisation (Response to LS in TD S3-000023). The liaison statement was modified for clarification in TD S3-000088 and approved for transmission to T WG3 and SA WG1.

NOTE: Document S3-000088 is not available. Please send it to me.

TD S3-000057: Liaison statement to SAGE and T WG3 on 3G Authentication Algorithm Requirements. The liaison statement was modified for clarification in TD S3-000089 and approved for transmission to SAGE and T WG3.

NOTE: 33.105 CR006 allocated for the attached CR.

TD S3-000077: LS to SA, CN and CN WG2 on MAP security. The LS was approved for transmission to CN WG2.

Action: ***M. Pope to accept changes and transmit the LS in S3-000077.***

TD S3-000083: LS to T WG2 and T WG3 on placing of the conversion functions. The liaison statement was modified to clarify the conversion functions inclusion (c4, c5) and a response deadline added, in TD S3-000090 and approved for transmission to SAGE and T WG3.

Action: ***M. Pope to send the liaison to the Leaders List.***

TD S3-000085: Proposed LS from S3 on TR45 acceptance of 3GPP for ESA. This needed consideration on the implications of TR45 approval of CRs to 33.102 in the future. This will be discussed and clarified via e-mail.

TD S3-000073: Report on TR45.2, 10-14 January, 2000, Panama City, Florida. This was presented for information and noted.

TD S3-000076: 33.102 v 3.3.1, CR 049 on Authentication failure reporting. Agreed.

TD S3-000084: CR006 to 33.105 v 3.2.0 on Authentication and key agreement. Agreed.

TD S3-000082: CR007 to 33.105 v3.2.0 on Enhanced user confidentiality. This was agreed, but CR needs to be updated because some terminology changes remain (see TD S3-000082 A5). The subject should be "Editorial changes to Terminology".

Action: M Pope to replace "IMUI" and "EMUI" with "IMSI" and "EMSI" respectively and equivalent changes to Annex C before submitting the CR to TSG SA#7.

TD S3-000080: Revised Draft CR to 03.20 V 7.2.0 on GSM Encryption. There was an objection to the approval of this CR from Siemens. The CR was modified editorially and provided in TD S3-000086 and agreed.

14 Future meetings dates and venues

A request to move the May 2000 meeting was made by the new support person (David Williams). It was discussed and found not to be possible as all has already been fixed with the Hosts.

Meeting	Date	Location	Host
S3#11	22-24 February 2000	Mainz	RegTP
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	Week of 11th or 18th September 2000	To be confirmed	Host required
S3#16	November 2000	To be confirmed	Host required

15 Close of meeting

The Chairman thanked the host for arranging the meeting and thanked delegates and Secretary for their hard work during the meeting.

Annex A: List of documents at the meeting

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comment
S3-000021	Draft Agenda for Meeting #10	Chairman	1	Approval		Approved with changes
S3-000022	Report of TSG SA WG3 Meeting #9 - draft	Secretary	4.1	Approval	S3-000067	Replaced by later draft
S3-000023	LS to S3 on USIM-Terminal Link	T WG3	5.2	Discussion/ Response		Response in TD S3-000061
S3-000024	Response to the LS (from SA WG2) on 'Clarification of the information storage in USIM'	T WG3	5.2	Information		Clarification from the WG2 Report sought.
S3-000025	Finalisation of the f8 and f9 algorithm design work	ETSI SAGE 3GPP Task Force	5.4	Discussion		Noted
S3-000026	Results of independent evaluation of 3GPP f8 and f9 algorithms	ETSI SAGE 3GPP Task Force	5.4	Discussion		Noted
S3-000027	Extension of shortened keys to full-length keys	ETSI SAGE 3GPP Task Force	5.4	Discussion		CR to 33.102 needed
S3-000028	Statement on security issues in VHE/OSA	CN OSA ad-hoc	5.2	Discussion		Response in TD S3-000062
S3-000029	SA WG3 extract of TSG SA #5 Draft Meeting Report	MCC	5.1	Information		Noted. Some minor modifications requested.
S3-000030	Notes on S3 presentation at SA#6	Vice Chairman	5.1	Information		Noted.
S3-000031	21.133 v 3.1.0: Security Threats and Requirements	Secretary	9	Information		Noted.
S3-000032	22.022 V 3.0.1: Personalisation of GSM ME Mobile functionality specification - Stage 1	Secretary	9	Information		Noted.
S3-000033	33.102 v 3.3.1: Security Architecture	Secretary	9	Information		Noted.
S3-000034	33.103 v 3.1.0: Security Integration Guidelines	Secretary	9	Information		Noted.
S3-000035	33.105 V 3.2.0: Cryptographic Algorithm requirements	Secretary	9	Information		Noted.
S3-000036	33.106 V 3.1.0: Lawful interception requirements	Secretary	9	Information		Noted.
S3-000037	33.107 V 3.0.0: Lawful interception architecture and functions	Secretary	9	Information		Noted.
S3-000038	33.120 V 3.0.0: Security Objectives and Principles	Secretary	9	Information		Noted.
S3-000039	33.901 V 3.0.0: Criteria for cryptographic Algorithm design process	Secretary	9	Information		Noted.
S3-000040	33.902 V 3.1.0: Formal Analysis of the 3G Authentication Protocol with Modified Sequence number Management	Secretary	9	Information		Noted.
S3-000041	Draft CR to TS 33.102 V 3.3.0 on Visibility and configurability	Telia	9.3	Approval		CR042 Postponed to next meeting
S3-000042	Draft CR to 03.20 V 7.1.0 on GSM Encryption	SMG10	7.1	Approval	S3-000080	A019 - Revised and agreed in S3-000065
S3-000043	Draft CR to 33.102 v 3.3.1 on Clarification on cipher key and integrity key lifetime	Ericsson	9.3	Approval		CR043. Agreed
S3-000044	Draft CR to 33.102 v3.3.1 on local Authenication and connection establishment	Ericsson	9.3	Approval		CR044 Agreed
S3-000045	Invitation to the 3GPP IP WORKSHOP 7-9 February 2000	MCC	5.1	Information		Noted
S3-000046	CR to 33.102 v3.3.1: refinement of EUIC after S3/N2 meeting	T-Mobil	9.3	Approval	S3-000081	CR045 - Modified and agreed (S3-000081)
S3-000047	Problems caused by 2G-3G interoperation	T-Mobil	9.3	Discussion		Contributions expected at meeting#11
S3-000048	Enhancements on the extended Proposal for Securing MAP Based Transmission of Sensitive Data between Network Elements	Ericsson	8.1	Discussion		Re-presented S3-000010 from Ad-hoc meeting
S3-000049	CR to 33.102 v3.3.1: Clarification on enhanced Distribution of authentication data within one serving network domain	Ericsson	9.3	Approval		CR046 Postponed

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comment
S3-000050	CR to 33.102 v3.3.1: Interoperation and intersystem handover/change between UTRAN and GSM BSS	Ericsson	9.3	Approval	S3-000079	Withdrawn - replaced
S3-000051	CR to 33.102 v3.3.1: Clarification on the reuse of Avs	Ericsson	9.3	Approval		CR048
S3-000052	3GPP terminal identity security: levels, requirements and mechanisms	Bosch	8.4	Discussion /decision		Further contribution and e-mail discussions expected on the ideas presented here
S3-000053	TR45 Comittee Correspondence in response to Liaison from SA WG3 (S3-99460)	TIA - Engineering Committee TR45	5.4	Discussion		SA #6 document SP-99513.
S3-000054	S3 status report to TSG SA #6.	Chairman	5.1	Information		Noted
S3-000055	Way forward for open R'99 security issues	Adhoc group on open R'99 security issues	8.1	Discussion		SA #6 document SP-99622
S3-000056	LS on Enhanced User Identity Confidentiality – open questions	CN WG1	5.2	Action		Final response in S3-000087
S3-000057	LS to SAGE and T WG3 on 3G Authentication Algorithm Requirements	SA WG3	13			Modified and agreed (S3-000089)
S3-000058	CR to 04.08 v7.2.0 on GPRS encryption	SMG10	7.1			Agreed
S3-000059	Proposed LS to CN , CN WG2 and TSG SA on on MAP security	Vodafone-Airtouch	8.1		S3-000077	Revised in S3-000077
S3-000060	Proposed LS to SA WG2 on Functions of Key Distribution and Key Administration for MAP security	SA WG3	8.1			Approved
S3-000061	LS to T3 and SA WG1 - Draft LS to T3 on ME personalisation (Response to LS in TD S3-000023)	SA WG3	5.2		S3-000088	Revised in S3-000088
S3-000062	Response to the Statement on security issues in VHE/OSA (TD S3-000028)	SA WG3	5.2			Approved.
S3-000063	Response to LS on Enhanced User Identity Confidentiality – open questions	SA WG3	5.2		S3-000069	Discussed and updated.
S3-000064	33.900 v 1.2.0	Editor	9	Information		Noted. Changes to editor before next meeting.
S3-000065	Revised Draft CR to 03.20 V 7.2.0 on GSM Encryption	SMG10	7.1		Withdrawn (Duplication)	Withdrawn
S3-000066	LS to CN WG2 on Protection of MAP Messages for Release 1999	SA WG3	8.1	Approval	Withdrawn (Duplication)	Withdrawn
S3-000067	Report of TSG SA WG3 Meeting #9 - draft (18/01/2000)	Secretary	4.1	Approval		Approved
S3-000068	Proposed LS to CN , CN WG2 and TSG SA on on MAP security	Vodafone-Airtouch	8.1		Withdrawn (Duplication)	Withdrawn - S3-000077
S3-000069	Response to LS on Enhanced User Identity Confidentiality – open questions	SA WG3	5.2	Approval	S3-000087	Modified and agreed (S3-000087)
S3-000070	LS to CN WG2 on Protection of MAP Messages for Release 1999	SA WG3	8.1	Approval		Approved
S3-000071	Presentation slides to S3-000052	Bosch	8.3	Information		Noted
S3-000072	List of 3GPP Specifications and Titles	MCC		Information		Noted
S3-000073	Report on TR45.2, 10-14 January, 2000, Panama City, Florida	Vodafone-Airtouch		Information		Noted
S3-000074	Proposed CR to 33.102 section 6.4.3 on USIM triggered authentication and key setting during PS connections			Approval		549 from meeting#9
S3-000075	LS on USIM triggered authentication and key setting during PS connections			Approval		550 from meeting#9
S3-000076	33.102 v 3.3.1, CR 049 on Authentication failure reporting	SA WG3	9	Approval		CR049 - Agreed
S3-000077	LS to SA, CN and CN WG2 on MAP security	SA WG3		Approval		Approved
S3-000078	CR006 to 33.105 v 3.2.0 on Authentication and key agreement			Approval	S3-000084	Revised in S3-000084
S3-000079	CR to 33.102 v3.3.1: Interoperation and intersystem handover/change between UTRAN and GSM BSS	Ericsson	9.3	Approval		CR047

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comment
S3-000080	Revised Draft CR to 03.20 V 7.2.0 on GSM Encryption	SMG10	7.1	Approval	S3-000086	CR A019 - Agreed with editorial change to forward to SMG for approval (S3-000086). A cover sheet on GPRS encryption export restriction problems
S3-000081	CR to 33.102 v3.3.1: refinement of EUIC after S3/N2 meeting	T-Mobil	9.3	Approval		CR-050 - Agreed
S3-000082	CR007 to 33.105 v3.2.0 on Enhanced user confidentiality	SA WG3		Approval		Agreed
S3-000083	LS to T WG2 and T WG3 on placing of the conversion functions	SA WG3		Approval	S3-000090	Modified and approved as S3-000090
S3-000084	CR006 to 33.105 v 3.2.0 on Authentication and key agreement			Approval		Agreed
S3-000085	Proposed LS from S3 on TR45 acceptance of 3GPP for ESA	SA WG3		Approval		To be discussed and clarified via e-mail.
S3-000086	Revised Draft CR to 03.20 V 7.2.0 on GSM Encryption	SMG10	7.1	Approval		Objection from Siemens, Agreed.
S3-000087	Response to LS on Enhanced User Identity Confidentiality – open questions	SMG10		Approval		Approved
S3-000088	LS to T3 and S1 on ME personalisation (Response to LS in TD S3-000023)	SA WG3	5.2	Approval		Approved
S3-000089	LS to SAGE and T WG3 on 3G Authentication Algorithm Requirements	SA WG3	13	Approval		Approved
S3-000090	LS to T WG2 and T WG3 on placing of the conversion functions	SA WG3		Approval		Approved
S3-000091	LS to CN WG2 on Authentication Failure Report	SA WG3				Sent after meeting. Content agreed at meeting#10
S3-000092	LS to SA WG2 (CC CN WG2) on EUIC	SA WG3				Sent after meeting.

Annex B: List of attendees

Name			Company	e-mail	3GPP Member	
Mr.	Aamodt	Tom Erling	TELENOR AS	tom-erling.aamodt@telenor.com	ETSI	NO
Mr.	Hiroshi	Aono	NTT DoCoMo	aono@mml.yrp.nttdocomo.co.jp	ARIB	JP
Mr.	Colin	Blanchard	BT	colin.blanchard@bt.com	ETSI	GB
Mr.	Rolf	Blom	ERICSSON L.M.	rolf.blom@era.ericsson.se	ETSI	SE
Mr.	Charles	Brookson	DTI	cbrookson@iee.org	ETSI	GB
Mr.	Takeshi	Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp	ARIB	JP
Mr.	Øyvind	Eilertsen	TELENOR AS	oyvind.eilertsen@telenor.com	ETSI	NO
Mr.	Louis	Finkelstein	Motorola Inc.	louisf@ccrl.mot.com	T1	US
Mr.	Guenther	Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI	DE
Mr.	Peter	Howard	VODAFONE AirTouch Plc	peter.howard@vf.vodafone.co.uk	ETSI	GB
Mr.	Geir	Køien	TELENOR AS	geir-myrdahl.koien@telenor.com	ETSI	NO
Mr.	Michael	Marcovici	Lucent Technologies	marcovici@lucent.com	ETSI	DE
Mr.	Mitsuru	Matsui	Mitsubishi Electric Co.	matsui@iss.isl.melco.co.jp	ARIB	JP
Mr.	David F.	Miles	BT Cellnet	dmiles@cellnet.co.uk	ETSI	GB
Mr.	Petri	Nyberg	Sonera	petri.nyberg@sonera.com	ETSI	FI
Mr.	Sebastien	Nguyen Ngoc	France Telecom	sebastien.nguyenngoc@cnet.francetelecom.fr	ETSI	FR
Mr.	Maurice	Pope	ETSI	maurice.pope@etsi.fr	ETSI	FR
Dr.	Stefan	Pütz	Deutsche Telekom MobilNet	stefan.puetz@t-mobil.de	ETSI	DE
Mr.	Jim	Reeds	AT&T Labs	reeds@research.att.com	T1	US
Mr.	Ludovic	Rousseau	GEMPLUS Card International	ludovic.rousseau@gemplus.com	ETSI	FR
Mr.	Benno	Tietz	MANNESMANN Mobilfunk GmbH	benno.tietz@d2mannesmann.de	ETSI	DE
Mr.	Peter	Toya	Alcatel Bell	peter.toya@alcatel.be	ETSI	BE
Mr.	Valtteri	Niemi	Nokia	valtteri.niemi@nokia.com	ETSI	FI
Mr.	Bart	Vinck	SIEMENS ATEA NV	bart.vinck@vnet.atea.be	ETSI	BE
Mr.	Berthold	Wilhelm	BMWi	berthold.wilhelm@regtp.de	ETSI	DE
Mr.	Wael	Adi	BOSCH TELECOM DANMARK A/S	wadi@tu-bs.de	ETSI	DK
Prof.	Michael	Walker	VODAFONE AirTouch Plc	mike.walker@vf.vodafone.co.uk	ETSI	GB

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

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 00	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	

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			
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	4.4.1	Security Aspects	Phase 2	ETS	300 506	RE/SMG-010209PR1
02.09	5.1.1	Security Aspects	Phase 2+	ETS	300 920	RE/SMG-010209QR1
02.09	6.0.1	Security Aspects	Release 1997	EN	300 920	DEN/SMG-010209Q6
02.09	7.0.0	Security Aspects	Release 1998			
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	3.0.1	Security-related Network Functions	Phase 1			
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	EN	300 929	DEN/SMG-030320QUIC
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	042		R99	Visibility and configurability	C	3.3.0		04/02/2000	Telia	S3	S3-10	S3-000041	postponed	Security
33.102	043		R99	Clarification on cipher key and integrity key lifetime lifetime	C	3.3.0		04/02/2000	Ericsson	S3	S3-10	S3-000043	agreed	Security
33.102	044		R99	local Authenication and connection establishment	D	3.3.0		04/02/2000	Ericsson	S3	S3-10	S3-000044	agreed	Security
33.102	045		R99	Refinement EUIC	F	3.3.0		04/02/2000	T-Mobil	S3	S3-10	S3-000081	agreed	Security
33.102	046		R99	Clarification on enhanced Distribution of authentication data within one serving network domain	F	3.3.0		04/02/2000	Ericsson	S3	S3-10	S3-000049	postponed	Security
33.102	047		R99	Interoperation and intersystem handover/change between UTRAN and GSM BSS	C	3.3.0		04/02/2000	Ericsson	S3	S3-10	S3-000079	postponed	Security
33.102	048		R99	Clarification on the reuse of Avs	C	3.3.0		04/02/2000	Ericsson	S3	S3-10	S3-000051	agreed	Security
33.102	049		R99	Authentication failure reporting	F	3.3.0		04/02/2000	S3	S3	S3-10	S3-000076	agreed	Security
33.102	050		R99	Refinement EUIC	F	3.3.0		04/02/2000	T-Mobil	S3	S3-10	S3-000081	agreed	Security
33.105	006		R99	Authentication and key agreement	F	3.1.0		09/02/2000	S3	S3	S3-10	S3-000084	agreed	Security
33.105	007		R99	Enhanced user confidentiality	F	3.1.0		09/02/2000	S3	S3	S3-10	S3-000082	agreed	Security

D.2 Full list of SA WG3 CRs after the meeting

TSG Status	Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	New Vers	Date	Source	WG	WG meeting	WG TD	WG status	Work item
approved	21.133	001		R99	Data integrity of user traffic	C	3.0.0	3.1.0	16/12/1999	S3	S3	S3-08	S3-99450	agreed	
approved	33.102	001		R99	Mechanism for data integrity of signalling messages	C	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	002		R99	Description of layer on which ciphering takes place	C	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	003		R99	Conditions on use of authentication information	C	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	004		R99	Modified re-synchronisation procedure for AKA protocol	C	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	005		R99	Sequence number management scheme protecting against USIM lockout	C	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	006		R99	Criteria for Replacing the Authentication “Working Assumption”	C	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	007		R99	Functional modification of Network domain security mechanisms	C	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	008		R99	Cipher key lifetime	C	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	009		R99	Mechanism for user domain security	C	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	010		R99	Replacement of incorrect diagrams	F	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	011		R99	Precision of the status of annex B	C	3.0.0	3.1.0	24/06/1999	S3	S3	S3_04	S3-99203	agreed	
approved	33.102	012		R99	Re-organisation of clause 6	D	3.1.0	3.2.0	10/10/1999	S3	S3	S3#6	S3-99338	agreed	
approved	33.102	013		R99	Integrity protection procedures	C	3.1.0	3.2.0	10/10/1999	S3	S3	S3#6	S3-99333	agreed	
approved	33.102	014		R99	Security of MAP-Based Transmissions	C	3.1.0	3.2.0	10/10/1999	S3	S3	S3#6	S3-99334	agreed	
approved	33.102	015		R99	Secure UMTS-GSM Interoperation	C	3.1.0	3.2.0	10/10/1999	S3	S3	S3#6	S3-99332	agreed	
approved	33.102	016		R99	Network-wide confidentiality	C	3.1.0	3.2.0	10/10/1999	S3	S3		S3-99344	agreed	
approved	33.102	017		R99	Authentication Management Field (AMF)	C	3.1.0	3.2.0	10/10/1999	S3	S3		S3-99348	agreed	
approved	33.102	018		R99	Support for window and list mechanisms for sequence number management in authentication scheme	C	3.1.0	3.2.0	10/10/1999	S3	S3		S3-99349	agreed	
approved	33.102	019		R99	Modification of text for window and list mechanisms	D	3.1.0	3.2.0	10/10/1999	S3	S3		S3-99350	agreed	
approved	33.102	020		R99	Cipher/integrity key setting	C	3.1.0	3.2.0	22/10/1999	S3	S3		S3-99351	agreed	
approved	33.102	021		R99	A generalised scheme for sequence number management	C	3.1.0	3.2.0	22/10/1999	S3	S3		S3-99352	agreed	
approved	33.102	022	1	R99	Refinement of Enhanced User Identity Confidentiality	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-08	S3-99459	agreed	
approved	33.102	025		R99	Length of KSI	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-07	S3-99389	agreed	
approved	33.102	026	1	R99	Mobile IP security	B	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99541	agreed	
approved	33.102	027	1	R99	Clarification of re-authentication during PS connections	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99552	agreed	

TSG Status	Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	New Vers	Date	Source	WG	WG meeting	WG TD	WG status	Work item
approved	33.102	030		R99	Handling of the MS UEA and UIA capability information	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-08	S3-99409	agreed	
approved	33.102	031		R99	Removal of alternative authentication mechanism described in annex D	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99542	agreed	
approved	33.102	032		R99	Removal of network-wide encryption mechanism form application security section	F	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99543	agreed	
approved	33.102	033		R99	Interoperation and intersystem handover/change between UTRAN and GSM BSS	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99545	agreed	
approved	33.102	034		R99	Distribution of authentication data within one serving network domain	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99544	agreed	
approved	33.102	035		R99	Authentication and key agreement	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99538	agreed	
approved	33.102	036		R99	Sequence number management	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99539	agreed	
approved	33.102	037	1	R99	Authentication and key agreement	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99548	agreed	
approved	33.102	038		R99	Clarification on system architecture	C	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99528	agreed	
approved	33.102	039		R99	Updated definitions and abbrviations	D	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99529	agreed	
approved	33.102	040		R99	An authentication failure report mechanism from SN to HE	B	3.2.0	3.3.0	16/12/1999	S3	S3	S3-09	S3-99536	agreed	
withdrawn	33.102	041		R99	UIA and UEA identifications	B	3.2.0		16/12/1999	S3	S3	S3-09	S3-99520	agreed	
	33.102	042		R99	Visibility and configurability	C	3.3.0		04/02/2000	Telia	S3	S3-10	S3-000041	postponed	Security
	33.102	043		R99	Clarification on cipher key and integrity key lifetime lifetime	C	3.3.0		04/02/2000	Ericsson	S3	S3-10	S3-000043	agreed	Security
	33.102	044		R99	local Authenication and connection establishment	D	3.3.0		04/02/2000	Ericsson	S3	S3-10	S3-000044	agreed	Security
	33.102	045		R99	Refinement EUIC	F	3.3.0		04/02/2000	T-Mobil	S3	S3-10	S3-000081	agreed	Security
	33.102	046		R99	Clarification on enhanced Distribution of authentication data within one serving network domain	F	3.3.0		04/02/2000	Ericsson	S3	S3-10	S3-000049	postponed	Security
	33.102	047		R99	Interoperation and intersystem handover/change between UTRAN and GSM BSS	C	3.3.0		04/02/2000	Ericsson	S3	S3-10	S3-000079	postponed	Security
	33.102	048		R99	Clarification on the reuse of Avs	C	3.3.0		04/02/2000	Ericsson	S3	S3-10	S3-000051	agreed	Security
	33.102	049		R99	Authentication failure reporting	F	3.3.0		04/02/2000	S3	S3	S3-10	S3-000076	agreed	Security
	33.102	050		R99	Refinement EUIC	F	3.3.0		04/02/2000	T-Mobil	S3	S3-10	S3-000081	agreed	Security
approved	33.103	001	1	R99	Refinement of Enhanced User Identity Confidentiality	C	3.0.0	3.1.0	16/12/1999	S3	S3	S3-08	S3-99456	agreed	
approved	33.103	002	1	R99	Corrections to figure 1	D	3.0.0	3.1.0	16/12/1999	S3	S3	S3-07	S3-99390	agreed	
approved	33.103	004		R99	Change length of KSI (and other miscellaneous corrections)	C	3.0.0	3.1.0	16/12/1999	S3	S3	S3-08	S3-99415	agreed	
approved	33.105	001		R99	Resources for cryptographic algorithms in the USIM	C	3.0.0	3.1.0	10/10/1999	S3	S3	S3#6	S3-99335	agreed	

TSG Status	Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	New Vers	Date	Source	WG	WG meeting	WG TD	WG status	Work item
approved	33.105	002		R99	MAC used for data integrity of signalling messages	C	3.0.0	3.1.0	10/10/1999	S3	S3	S3#6	S3-99337	agreed	
approved	33.105	003		R99	Cipher keystream block length	C	3.0.0	3.1.0	10/10/1999	S3	S3		S3-99301	agreed	
approved	33.105	004		R99	Time variant parameter for synchronisation of ciphering	D	3.1.0	3.2.0	16/12/1999	S3	S3	S3-07	S3-99384	agreed	
approved	33.105	005		R99	Direction bit in f9	D	3.1.0	3.2.0	16/12/1999	S3	S3	S3-08	S3-99455	agreed	
	33.105	006		R99	Authentication and key agreement	F	3.1.0		09/02/2000	S3	S3	S3-10	S3-000084	agreed	Security
	33.105	007		R99	Enhanced user confidentiality	F	3.1.0		09/02/2000	S3	S3	S3-10	S3-000082	agreed	Security
approved	33.106	001		R99	Lawful Interception Requirements	C	3.0.0	3.1.0	16/12/1999	S3	S3	S3-09	S3-99522	agreed	
approved	33.902	001		R99	Formal analysis of the 3G authentication protocol	B	3.0.0	3.1.0	16/12/1999	S3	S3	S3-09	S3-99505	agreed	

D.3 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
02.09	A005	1	2	Modification of section 3.5.3 to enhance IMEI security	F	4.4.1		09/02/2000	SMG10	10		e-mail	agreed	
02.09	A006	1	96	Modification of section 3.5.3 to enhance IMEI security	A	5.1.0		09/02/2000	SMG10	10		e-mail	agreed	
02.09	A007	1	97	Modification of section 3.5.3 to enhance IMEI security	A	6.0.0		09/02/2000	SMG10	10		e-mail	agreed	
02.09	A008	1	98	Modification of section 3.5.3 to enhance IMEI security	A	7.0.0		09/02/2000	SMG10	10		e-mail	agreed	
03.20	A019		R97	GPRS Encryption	F	6.1.0		11/02/2000	SMG10		S3-10	e-mail	agreed	Security
03.20	A019		R98	GPRS Encryption	A	7.2.0		11/02/2000	SMG10		S3-10	e-mail	agreed	Security
03.20	A019		R99	GPRS Encryption	A	8.0.0		11/02/2000	SMG10		S3-10	e-mail	agreed	Security

D.4 Full list of SMG10 CRs after the meeting

SMG Status	Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	New Vers	Date	Source	WG	WG meeting	WG TD	WG status	Work item
approved	01.31	A001		R98	Removal of references to the J, K and Y-interfaces and some cleaning up	D	7.0.0	7.0.1	01/05/1998	SMG10	10			agreed	
approved	01.33	A001	1	R98	Lawful interception and GPRS	B	5.0.0	7.0.0	05/02/1998	SMG10	10		98D005	agreed	GPRS + LI
approved	02.09	A003	4	2	Correction of User data confidentiality feature	C	4.3.0	4.4.0	09/06/1997	SMG10	10			agreed	
approved	02.09	A004	4	R96	Correction of User data confidentiality feature	C	5.0.1	5.1.0	09/06/1997	SMG10	10			agreed	
rejected	02.09	A005		2	Modification of section 3.5.3 to enhance IMEI security	F	4.4.0		06/08/1999	SMG10	10			agreed	
	02.09	A005	1	2	Modification of section 3.5.3 to enhance IMEI security	F	4.4.1		09/02/2000	SMG10	10			agreed	
rejected	02.09	A006		96	Modification of section 3.5.3 to enhance IMEI security	A	5.0.1		06/08/1999	SMG10	10			agreed	
	02.09	A006	1	96	Modification of section 3.5.3 to enhance IMEI security	A	5.1.0		09/02/2000	SMG10	10			agreed	
rejected	02.09	A007		97	Modification of section 3.5.3 to enhance IMEI security	A	6.0.0		06/08/1999	SMG10	10			agreed	
	02.09	A007	1	97	Modification of section 3.5.3 to enhance IMEI security	A	6.0.0		09/02/2000	SMG10	10			agreed	
rejected	02.09	A008		98	Modification of section 3.5.3 to enhance IMEI security	A	7.0.0		06/08/1999	SMG10	10			agreed	
	02.09	A008	1	98	Modification of section 3.5.3 to enhance IMEI security	A	7.0.0		09/02/2000	SMG10	10			agreed	
approved	02.31	A001	1	R98	Removal of references to the J, K and Y-interfaces and some cleaning up	F	7.0.0	7.1.0	01/05/1998	SMG10	10			agreed	
approved	02.32	A001		R98	Applicability of IST and IST indicator	C	7.0.0	7.1.0	01/05/1998	SMG10	10			agreed	
approved	02.33	A001	2	R98	Lawful Interception and GPRS	B	5.0.0	7.0.0	03/03/1998	SMG10	10		98D005	agreed	GPRS + LI
approved	02.33	A002	2	R98	Location Dependent Interception	C	7.0.0	7.1.0	09/10/1998	SMG10	10			agreed	LI
approved	02.33	A003	2	R98	Lawful Interception security	C	7.0.0	7.1.0	09/10/1998	SMG10	10			agreed	LI
approved	02.33	A004		R98	Inclusion of the Warrent Reference Number	F	7.1.0	7.2.0	08/02/1999	SMG10	10				
approved	02.33	A005		R98	Addition of intercept events for lawful interception for GPRS. Correction to target identities and intercept related data are also included	B	7.2.0	7.3.0	28/04/1999	SMG10-C	10	email	AP99-070	email agreed	GPRS, Lawful Interception
approved	03.20	A001		2	Length of ciphering key Kc for signalling and testing purposes	D		4.3.2		SG chairman/PT12					

SMG Status	Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	New Vers	Date	Source	WG	WG meeting	WG TD	WG status	Work item
approved	03.20	A002	4	R96	CR 03.20-A002r4 on Definition of ciphering for HSCSD	B	4.3.2	5.1.0	05/02/1997	SMG3 WPA	3	Sept 96	97P043	agreed	HSCSD
approved	03.20	A003	3	2	Ciphering Algorithm(s) support (phase 2)	F	4.3.2	4.4.0	06/02/1997	SMG3 SA	3	9701p	97P131	agreed	
approved	03.20	A004	1	R96	Ciphering Algorithm(s) support (phase 2+)	A	5.0.0	5.1.0	06/02/1997	SMG3 SA	3	9701p	97P131	agreed	
approved	03.20	A006	1	R97	GPRS interaction with existing security mechanisms	B	5.1.1	5.2.0	13/10/1997	SMG10	10	97-3	182/97	agreed	GPRS
approved	03.20	A007	1	R97	GPRS security	B	5.1.1	5.2.0	13/10/1997	SMG10	10	97-3	183/97	agreed	GPRS
approved	03.20	A010		R98	Proposed annex E on CTS security	B	6.0.1	7.0.0	08/02/1999	SMG10	10				CTS
approved	03.20	A011	4	R97	Correction of the handling of the Ciphering Key Sequence Number (CKSN)	F	6.0.1	6.1.0	24/06/1999	SMG3	3		N1-99354		GPRS
postponed	03.20	A012		R97	Clarification on security triplet re-use conditions	A	6.0.1		29/06/1999	SMG10	10		AP99-051	agreed	TEI
approved	03.20	A013		R98	Introduction of CTS-FP authentication and signature generation by CTS-SN.	B	7.0.0	7.1.0	29/06/1999	SMG10	10		AP99-055	agreed	CTS
approved	03.20	A014		R98	CTS Security functions in case of license exempt frequencies	F	7.0.0	7.1.0	29/06/1999	SMG10	10		AP99-030	agreed	CTS
postponed	03.20	A015		R96	Clarification on security triplet re-use conditions	F	5.2.1		29/06/1999	SMG10	10		AP99-050	agreed	TEI
approved	03.20	A016	4	R98	Correction of the handling of the Ciphering Key Sequence Number (CKSN)	F	7.0.0	7.1.0	19/08/1999	SMG3	3		N1-99354		GPRS
approved	03.20	A017		R99	Introduction of EDGE variant of A5 algorithm	B	7.1.0	7.2.0	05/08/1999	SMG10	10	99-2	AP99-100		EDGE
approved	03.20	A018		R98	Clarification on security triplet re-use conditions	F	7.1.0	7.2.0	05/08/1999	SMG10	10	99-2	AP99-112		
	03.20	A019		R98	GPRS Encryption	F	7.1.0		04/02/2000	SMG10		S3-10	S3-000086	agreed	Security
approved	03.33	A001	1	R98	Addition of lawful interception for GPRS	B	7.0.0	7.1.0	22/06/1999	SMG10-C	10	email	AP99-075	email agreed	GPRS, Lawful Interception

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD Number	Title	Source	Comment
S3-000053	TR45 Comittee Correspondence in response to Liaison from SA WG3 (S3-99460)	TIA - Engineering Committee TR45	SA #6 document SP-99513.
S3-000056	LS on Enhanced User Identity Confidentiality – open questions	CN WG1	Final response in S3-000087

E.2 Liaisons from the meeting

TD Number	Title	Status	Comment
S3-000060	Proposed LS to SA WG2 on Functions of Key Distribution and Key Administration for MAP security	Approved	sent 10/02/2000
S3-000062	Response to the Statement on security issues in VHE/OSA (TD S3-000028)	Approved.	sent 10/02/2000
S3-000070	LS to CN WG2 on Protection of MAP Messages for Release 1999	Approved	sent 10/02/2000
S3-000075	USIM triggered authentication and key setting during PS connections	Approved	550 from meeting#9 Sent 10/02/2000
S3-000077	LS to SA, CN and CN WG2 on MAP security	Approved	Sent 03/02/2000
S3-000085	Proposed LS from S3 on TR45 acceptance of 3GPP for ESA	Ongoing	To be discussed and clarified via e-mail.
S3-000087	Response to LS on Enhanced User Identity Confidentiality – open questions	Approved	sent 10/02/2000
S3-000088	LS to T3 and S1 on ME personalisation (Response to LS in TD S3-000023)	Approved	Sent 09/02/2000
S3-000089	LS to SAGE and T WG3 on 3G Authentication Algorithm Requirements	Approved	Sent 09/02/2000
S3-000090	LS to T WG2 and T WG3 on placing of the conversion functions	Approved	Sent 09/02/2000
S3-000091	LS to CN WG2 on Authentication Failure Report	Approved	Sent 27/01/2000. Content agreed at meeting#10
S3-000092	LS to SA WG2 (CC CN WG2) on EUIC	Approved	Sent 27/01/2000