3GPP TSG SA WG3 Security — S3#14 **S3-000401**

2-4 August, 2000

Oslo, Norway

3GPP TSG SA WG3 Security — S3#13 Draft report version 0.0.3

May 24 – May 26, 2000, Yokohama, Japan

Source: **Vice-Chairman 3GPP TSG-SA WG3**

Title: **Draft report of meeting #13**

Document for: **Approval**

Motomachi (a popular shopping street) Yokohoma City, Japan

1 Opening of the meeting

The meeting was chaired by Mr. M. Marcovici, who opened the meeting and welcomed delegates. He thanked the hosts, NTT DoCoMo, for the arrangements.

2 Message from the S3 Chairman, Professor Michael Walker

TD S3-000325: Message from the Chairman. The SA WG3 chairman apologised for being unavailable for this meeting, and reported his intention to resume Chairmanship of SA WG3/SMG10 from the next meeting.

3 Objectives of meeting

The Chairman detailed the objectives for the meeting, as follows:

- To finalise documents for Release 1999 with the CRs input.
- To update the SA WG3 schedule for Release 2000.
- To finalise positions and create input documents for the joint meeting with CN WGs.

4 Approval of the agenda

The agenda, provided in TD S3-000310 was approved.

5 Registration and assignment of input documents

The available documents were allocated to appropriate agenda items.

6 Approval of meeting report from S3#12

The report was considered and some editorial corrections made.

The status of the actions from the meeting were checked:

12/1: No feedback had been received.
12/2: Open. Clarification of the role of SMG10 WPD is needed with respect to 3GPP work.
12/3: The LS was sent.
12/4: The liaison was not received by AHAG. This should be sent after this meeting.

ACTION #13/1: Chairman: To send the liaison in TD S3-000309 to AHAG.

12/5: Drafted and sent to SMG#31bis and other parties.
12/6: Completed.
12/7: Input doc to SA WG3 meeting #13: TD S3-000332.
12/8: Completed (part of AP 12/5).
12/9: Completed. Comments received and a new version was produced, which was approved by e-mail, 19 May 2000. This is available for information in TD S3-000348.
12/10: Completed.

12/11: Completed.
12/12: Completed. Joint meeting with CN 13-14 June 2000 arranged where this can be discussed.
12/13: Completed.
12/14: Completed.
12/15: Ongoing. Need to evaluate CN WG1 specifications before necessary changes can be made to the security architecture. To be revisited under agenda item 10.3.
12/16: No comments were received. The Action was closed.
12/17: Completed. Joint meeting with CN WGs 13-14 June 2000, Sophia Antipolis.

With the changes, the reort was approved. The approved version is version 1.0.0, available on the FTP server.

7 Reports / Liaisons from other 3GPP and SMG groups

7.1 Eurocrypt - 3GPP presentation (S3 Chair)

TD S3-000326: This presentation was noted.

7.2 3GPP and SMG plenary

TD S3-000316: SMG10 status report to SMG# 31bis. The report to SMG#31bis was presented by Mr. P. Howard, for information to SMG10. The report was discussed and noted.

TD S3-000354: Report on SMG 31bis. Mr. P. Howard introduced the report from Stefan Pütz on SMG#31bis SMG10 issues. For rejection of unciphered GPRS calls for R00 onwards, there were discussions about the need for standardisation of this feature, and SMG asked SMG10 to produce a WI description for SMG#32, in co-operation with SMG1, SMG2, SMG3 and SMG9 (and 3GPP equivalents).

For GEA 2, SMG resolved a date for introduction of the algorithm, a resolution of SMG on this is provided in TD S3-000317 (see agenda item 9). SMG also asked SMG10 to set up a workshop, but this did not seem possible before SMG#32 in June. It was proposed that the Work Item description should be produced in time for the joint meeting with CN WGs, and then could be raised here to ensure visibility to the experts available there before SMG#32. The "GEA support" negotiation mechanism (mandatory for R99 MEs type approved after December 2002) requires some study, as it either has to be backward compatible, or including a mechanism in earlier versions should be studied.

7.3 3GPP WGs and SMG STCs

TD S3-000320: Answer to LS on Functions of Key Distribution and Key Administration for MAP security (postponed TD 224). As the subject of the original liaison from SA WG3 has been moved to Release 2000, the response was no longer required and the document was noted.

TD S3-000341: Liaison Statement from SMG2 to SMG10/SA WG3 on Security functions in GERAN Release 2000. SMG2 request advice from SA WG3 on the ciphering algorithms for GERAN and the placing of the ciphering functions. Also the parameters required for ciphering and integrity checking requirements and parameters. These questions were discussed under agenda item 10.4.

TD S3-000365: Liaison statement from CN WG4 to SA WG3 on GTP signalling security. This liaison asks SA WG3 whether IPSec is **the** protection mechanism to be used, or **one** mechanism to be used for GTP signalling. A response was requested for the current CN WG4 meeting, which closes on 26 May. SA WG3 were not in a position to provide the information requested, as this was a subject for discussion at the joint meeting with CN WGs in June. P. Howard accepted to produce a reply liaison, which is provided in TD S3-000370 which was discussed and approved under agenda item 12.

TD S3-000366: LS from CN WG4 on Key Exchange and Key Distribution. A draft liaison had been prepared in TD S3-000344 which was also considered. This liaison was updated in TD S3-000381 and approved (see agenda item 12) which should to be copied to CN WG4 along with a further liaison to CN WG4 informing them that SA WG3 have a preference for the Layer 1, but need to further consider the Layer 2 issues, and that this will not be finalised until after TSG CN#8 Plenary in June 2000. The Layer 3, however, should be stabilised by June 2000. After much discussion on the pros and cons of using the existing MAP security solution and evaluating IKE for key management, it was decided that a position paper asking for time to evaluate the best way forward would be produced for the joint meeting with CN WGs.

ACTION #13/2: P. Howard and R. Lubarsky: To create a liaison statement to CN4 on SA WG3 position on Key management solutions. To be approved by e-mail in time for the Joint SA WG3/CN WGs meeting.

7.4 3GPP partners

TD S3-000345: New format IMEI. This proposal was based on a request from ARIB to increase the address space for IMEI, as the expectations for same-model terminals for 3GPP manufacturers is above the limit under the current scheme. The proposal provides a larger address space and asks SA WG3 to verify any security problems. The default IMEI fallback suggestion caused some concern, as the IMEI would become anonymous, which could impact the Lawful Interception requirements. It was agreed that Nokia would draft a liaison to CN WG1 and CN WG4 expressing that the use of a default IMEI is not allowed, but that a cut-off date (deadline) should be set for all equipment to accept the new IMEI format (e.g. a technical advice note from the GSM Association). The Liaison to be copied to T WG3. This liaison was provided in TD S3-000352 which was modified slightly, in TD S3-000358 and approved.

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

TD S3-000315: Use of SHA-1 for AKA f0-f5. This was introduced by the Chairman on behalf of TR-45 AHAG, and provides a report on SHA-1 evaluation for AKA functions f0 to f5. This is the algorithm being selected by TR-45 as a hash function in AKA, and selection by 3GPP would be useful for harmonisation between 3GPP and 3GPP2 systems. It was agreed that a liaison should be created, with this document and forwarded to SAGE and the GSM Association Security Group for their comments on SHA-1. The liaison was produced in TD S3-000384 which was discussed and approved under agenda item 12.

TD S3-000360: Draft report of the joint session with TIA TR-45 AHAG on 3GPP/3GPP2 security harmonisation version 0.0.2. Actions from the meting:

Action 1: Not done. B. Vinck will do immediately.

Action 2: Not done. B. Vinck will do immediately.

Action 3: The Chairman reported that AHAG had proposed the dates of September 13 or 14 2000 for the joint meeting, in Washington D.C.

Action 4: Ongoing. P. Howard will contact T. Wright to ascertain progress on the investigation for NNI issues.

Action 5: It was decided that Recommendation 2 would not be addressed at present, Recommendations 1 is complete but no official answer had been received from AHAG, and Recommendation 3 still needs a liaison to be produced but is awaiting a response from CN WG4.

ACTION #13/3: G. Køien: Liaison on Recommendation 1 to be forwarded to AHAGand Liaison on Recommendation 3 to be completed.

ACTION #13/4: Chairman: To produce a liaison to AHAG that Recommendation 2 is still under discussion (depends if there is a timer in the VLR or not) and ask their opinion.

Action 6: (AHAG Action point).

The report was slightly modified (IS-41 changed to ANSI-41) and re-produced as version 0.0.3, to be transmitted to AHAG. This report to be submitted for approval at the next Joint SA WG3 / AHAG meeting.

ACTION #13/5: M. Pope: To transmit the updated report version 0.0.3 to AHAG contact.

The planning for the joint meeting with AHAG was discussed. AHAG had offered September 13 or 14 for the meeting in Washington D.C. (Dollas Airport area). It was decided that the date for the SA3#15 meeting would be 12-15 September, and the Chairman would ask whether this could be hosted in Washington D.C. in order to be able to meet jointly with AHAG.

8 Content and schedule of R00 security work

TD S3-000313 and TD S3-000314: Draft Release 2000 Project Plan, version 0.0.4 (with and without revision marks). Mr. P. Howard presented the changes to the document since the last meeting.

The presentation by SA WG2 of well-defined and understandable system architecture concepts and principles, which was due for this meeting had not been fulfilled. SA WG3 therefore need to continue to develop the requirements capture and provide the assumptions that have been made on the system architecture.

ACTION #13/6: M Pope: Check if any documentation from SA WG2 on system architecture is available, if so, then send it to the SA WG3 mailing list.

Each of the work items were allocated to delegates who were tasked to draft Work Item description sheets for SA3#13 meeting, for approval and forwarding to TSG SA#8.

Work Item:	Priority	Allocated to:
Architectural deliverables		
Access security for IP-based services	Required R00	R Blom/ V Niemi
Network-based end-to-end security	Desired R00	P Howard
User plane protection in access network	Required R00	S Ward
Core network security: minimal solution	Required R00	R Lubarsky
Core network security: full solution	Desired R00	R Lubarsky
GERAN access security/termination of packet domain encryption in GSM BSC	Required R00	B Vinck
Enhanced User Identity Confidentiality	Under evaluation	S Ward
Other security deliverables		
FIGS	Under evaluation	P Howard
Secure mobile platform for applications	Required R00	C Blanchard
OSA/VHE security	Required R00	C Blanchard
Visibility and configurability including Ability of terminal/USIM to reject unencrypted connections	Required R00	S Nguyen Ngoc
Study on the evolution of GSM CS algorithms	Required R00	C Brookson
Study on the evolution of GSM PS algorithms and the introduction of GEA2	Required R00	C Brookson
Lawful Interception in the R’2000 architecture	Required R00	C Brookson

NOTE: It was understood that the people who volunteered to create the work item description drafts do not necessarily agree that their organisations endorse the Work Items.

These Work Item descriptions should be produced and sent for approval by e-mail, deadline for drafts: 5 June 2000. After distribution of the drafts, comments should be made before 9 June 2000, when the drafts will be updated and presented to the Joint meeting with CN WGs (by P. Howard). The output of the joint meeting discussions will be sent again to the e-mail list (by 16 June 2000) for approval by 21 June 2000. Approved Work Item descriptions will then be forwarded to TSG SA#8 for approval (26-28 June 2000).

ACTION #13/7: All: Draft Work Item descriptions to be produced by 5 June 2000. 2nd draft after SA WG3 comments 9 June 2000 for input to joint meeting. Joint meeting comments included by 16 June 2000 and sent to e-mail list. For e-mail approval by 21 June 2000.

TD S3-000318: Proposal for the Release 2000 Features, Building Blocks and Work Tasks Version 1.0. This had been briefly reviewed in the MAP Security ad-hoc meeting. The implications of the merging of items and deletion of an item needs to be reflected in this document. P. Howard undertook to do this and feed it back to SA WG2.

ACTION #13/8: P. Howard: Update the Release 2000 Features, Building Blocks and Work Tasks document in TD S3-000318 in line with changes to the work programme made at SA3#13 and forward to SA WG2.

9 2G security issues

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

Action Point #13/9 is allocated under this agenda item.

10 3G security issues

10.1 Algorithms

These are dealt with under agenda items 10.3 and 10.4.

10.2 Review of other specifications

There was no contribution under this agenda item.

10.3 Open R99 security issues

TD S3-000327: Clarification on UMTS AKA for GSM R'99 mobiles. This contribution was presented by GemPlus, and asks for clarification from SA WG3, SMG9 and T WG3 for the required support of UMTS AKA for GSM R99 MEs. After some discussion, it was realised that SA WG1 need to be consulted on the requirements for GSM R99 terminals support of USIM, before SA WG3 can respond.

It was agreed to formulate a liaison statement to SA WG1 about this. This was provided in TD S3-000375 and discussed under agenda item 12 (later revised in TD S3-000385).

10.4 R00 security issues

The questions asked by SMG2 in TD S3-000341 about the ciphering and integrity checking requirements for GERAN were discussed. A draft reply liaison was produced in TD S3-000376 (see agenda item 12).

TD S3-000332: Proposal for rejection of unciphered calls. This contribution is the result of an action on France telecom to provide a proposal after SA3#12. The proposal was intended for both GPRS and 3GPP systems. 2 options are provided: Accept all non-ciphered connections without informing the user, the user approves acceptance of non-ciphered connections, reject non-ciphered connections and inform the user and reject non-ciphered connections without informing the user. A new signalling message may be required to prevent repeated attempts to establish non-ciphered connections when the terminal rejects one. T WG3/SMG9, T WG2, RAN WG2 (to be checked) and CN WG1 (to be checked) were identified as being impacted by this procedure.

There was some concern expressed about the rejection of calls without informing the user, as the user would not know why no more calls were being received. Also, to accept calls without informing the user can lead to the user not knowing that calls are non-ciphered. The option (2) to manually prompt the user for acceptance could have large impact on protocols, interrupting call establishment in order to prompt the user.

After some discussion over the implications and likely user requirements it was decided that options (1) and (3) were the only necessary options. The "user" should not be involved in the call set-up procedure, i.e. option (2). Some more discussion over re-setting the default values when changing networks or when the user changes his options in roaming environments. This was further discussed among interested parties. <Return> .<See also TD373>

TD S3-000343: Draft report of MAP ad-hoc group meeting V0.0.1. The action points were checked for relevance to the SA WG3 meeting. Some minor modifications were made and version 0.0.2 produced (on the ftp server) for approval at the next meeting. Delegates are asked to send any comments on the report to the Secretary before the next SA WG3 meeting.

TD S3-000355: Independence of confidentiality and integrity in MAP Layer III and other layer III issues (amendment of TD S3-000312 which was discussed in the MAP Security ad-hoc meeting).

11 Review of (draft) S3 specifications

11.1 TS 21.133 Threats and requirements

There was no contribution on this document.

11.2 TS 22.022 Personalisation of ME

TD S3-000324: CR to 22.022: Update of the specification of ME personalisation to make it applicable for 3GPP. This CR was revised in TD S3-000383 which was approved.

11.3 TS 33.102 Security architecture

TD S3-000357: This issue was the subject of some CRs in TD S3-000323 CR101: After some discussion on the confusion in the text of 33.102, a drafting group was set up to look into and clarify the text related to the SIM/USIM/Release issues. The results of this were provided in TD S3-000378

TD S3-000378: CR103 to 33.102: Clarification on terminology in user domain. Some changes to the CR were proposed by the author, who will re-issue the document to the e-mail list for approval. The proposals will also be sent to T WG3.

ACTION #13/10: B. Vinck: To update TD S3-000378 and send to SA WG3 list for e-mail approval and to T WG3 for review.

TD S3-000323: CRs to 33.102.

CR097: This CR was modified to "see note above" and approved as CR097R1.

CR098: This CR was approved.

CR099: Objection to the UE being relied upon to reject IK (e.g. in case of rogue UEs). The USIM currently does the comparisons and has the necessary data. The CR was then withdrawn by T-Mobil for further consideration.

CR100: This CR was postponed to e-mail approval after the meeting.

CR101: It was felt that delegates should consult with T WG3 colleagues to ensure common understanding, and this CR was postponed to e-mail approval after the meeting.

TD S3-000330: CR088R1. CR088 had been approved at meeting#12. This proposes changes to the original CR changes. B. Vinck undertook to check the changes made.

ACTION #13/11: B. Vinck: To check the changes to the original CR088 and comment on the proposals in TD S3-000330.

TD S3-000334: CR was approved.

ACTION #13/12: C. Blanchard: To verify that network-wide encryption has been completely removed from 33.103, Release 1999.

TD S3-000338: GSM AKA and conversion function c3 (Ericsson). There was an objection to this proposal from T-Mobil. Ericsson requested a decision from SA WG3 on the principles of GSM AKA and c3. SA WG3 would like to keep the options open for operators to choose for their own networks.

TD S3-000322: Improved conversion functions for GSM-UMTS interoperation. The proposal is to add the IMSI to the Kc to increase the complexity of brute force attacks. There were questions about the secrecy of the IMSI and it's availability everywhere that it is needed for key transformations. It was decided that more investigation is needed on the availability of IMSI everywhere that it is needed and on the advantages of making such a change for Release 1999. It was decided to discuss the subject by e-mail after the meeting.

ACTION #13/13: All: To discuss conversion functions for GSM-UMTS interoperation.
M. Marcovici: To send a revised CR to 33.102 for approval by e-mail.

11.4 TS 33.103 Integration guidelines

TD S3-000335: CR to 33.103: Removal of EUIC from 33.103. This CR was approved.

TD S3-000336: CR to 33.103: Removal of MAP Security from 33.103. This CR was approved.

TD S3-000337: CR to 33.103: SQN length. This CR was approved.

11.5 TS 33.105 Algorithm requirements

TD S3-000342: CR to 33.105: Clarification of BEARER and DIRECTION parameters, corresponding to CR090 to CR to 33.102 (TD 262). This CR was approved.

11.6 TS 33.106 LI requirements

There was no contribution on this document.

11.7 TS 33.107 LI architecture

There was no contribution on this document.

11.8 TR 33.120 Security principles and objectives

There was no contribution on this document.

11.9 TR 33.900 Guide to 3G security

There was no contribution on this document.

11.10 TR 33.901 Criteria for algorithm design process

There was no contribution on this document.

11.11 TR 33.902 Formal analysis

There was no contribution on this document.

12 Approval of output documents

TD S3-000350: Liaison Statement to SA WG2, SA WG5 and CN WG4 on Protocol Choice for Layer I of MAP Security. This proposed liaison was discussed and a request for additional information to the addressed groups was made, to ensure that it is clear that the current protocol (IO/IEC) given in 33.102 may be changed, if IKE is found fully suitable. The updated liaison was presented in TD S3-000356 , which was revised in TD S3-000359 and approved.

TD S3-000351: LS to CN4 on MAP over IP. Some discussion over the text occurred and it was decided to revise the liaison which was presented in TD S3-000364 which was approved.

TD S3-000357: Draft LS Clarification on UMTS AKA for SIM. This liaison was discussed and revised in TD S3-000375 which, after further refinement was revised in TD S3-000385 which was approved.

TD S3-000347: Replaced by TD S3-000353: The liaison on Protection Mode security issues was discussed, modified slightly in TD S3-000363 which was approved.

TD S3-000361: Draft LS to SMG10 WPD on Clarification on new working conditions and reporting. This suggests that SMG10 WPD become a sub WG of SA WG3. and report their progress to SA WG3. SMG10 WPD are asked for their response to the proposal. This liaison was modified slightly, as provided in TD S3-000371 which was approved.

TD S3-000376: Draft Reply to an SMG2 LS about Security functions in GERAN (TD S3-000341). This was modified and updated in TD S3-000379 which was approved.

TD S3-000270: (Contained in TD S3-000319) Liaison was discussed modified slightly and provided again in TD S3-000380, which was approved.

TD S3-000344: Draft LS to SA2 on use of IP for security key distribution. Liaison was discussed modified slightly, and provided again in TD S3-000381, which was approved and copied to CN WG4 and SA WG5.

TD S3-000377: Proposed LS to N4 on MAP security Layer III. This liaison was modified slightly and provided in TD S3-000382 which was approved with attached documents S3-000312, S3-000355 and S3-000368.

TD S3-000364: LS to CN4 on Security for MAP over IP. This liaison was approved.

TD S3-000369: Draft LS to SAGE on consideration of SHA-1 for 3GGP(1) Authentication by ETSI SAGE. The liaison was modified to add references to literature and provided in TD S3-000384 which was approved.

TD S3-000374: Proposed LS to CN WG4 on replay protection. This document was superseded by other discussions and was withdrawn.

TD S3-000370: Reply liaison statement to CN WG4 on GTP signalling security (TD S3-000321). This was updated in TD S3-000386 and approved.

TD S3-000387: Liaison Statement on AHAG recommendation on Home Control ability to control the duration of the Security Association. This Liaison was approved.

13 Future meeting dates and venues

The invitation to the joint meeting with CN WGs was provided in TD S3-000372 for information and was noted.

Meeting	Date	Location	Host
S3 / CN WGs Joint ad-hoc on Requirements Impacts	13-14 June 2000	Sophia Antipolis	ETSI
S3#14	1-4 August 2000	Oslo	TeleNor
S3#15 Probably joint with AHAG	12-15 September 2000	Washington USA (to be confirmed)	Host required
S3#16	27-30 November 2000	Israel (TBC)	Motorola (TBC)

14 Any other business

Deadlines for e-mail approvals: 9 June for items needed for the SA WG3/CN WGs joint meeting, 16 June for other items.

15 Close of meeting

The Chairman thanked the hosts for the facilities provided and the smooth running of the meeting, the delegates for their hard work and co-operation and closed the meeting.

Annex A: List of documents at the meeting

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000310	Draft Agenda for Meeting #13	Chairman (M. Marcovici)	2	Approval		Approved
S3-000311	Draft Report of Meeting #12, version 0.0.2	Secretary	6	Approval		Approved with editorial changes (V1.0.0)
S3-000312	Independence of confidentiality and integrity in MAP Layer III and other layer III issues	Siemens AG	ad-Hoc MAP Sec 5.2	Discussion / Decision	S3-000355	B Lubarsky to act as editor for MAP Security working document, for production as CR(s) when finalised. Attached to TD382
S3-000313	Draft R00 Project Plan version 0.0.4 (with Revision marks)	Vodafone Airtouch	8, ad-Hoc MAP Sec 5.1	Discussion		3.1.1.4 updated to remove IPSec for minimal solution
S3-000314	Draft R00 Project Plan version 0.0.4 (without Revision marks)	Vodafone Airtouch	8, ad-Hoc MAP Sec 5.1	Discussion		See TD 313
S3-000315	LS from AHAG: Use of SHA-1 for AKA f0-f5	AHAG (F Quick)	7.5	Discussion		Response LS in TD384
S3-000316	SMG10 status report to SMG# 31bis	Chairman (M. Marcovici)	9.1	Information		Noted
S3-000317	SMG Resolution on GEA2 algorithm implementation SMG#31bis TD P-00-237	Chairman (M. Marcovici)	7.2	Information		Noted
S3-000318	Proposal for the Release 2000 Features, Building Blocks and Work Tasks Version 1.0	Vodafone Airtouch	8, ad-Hoc MAP Sec 5.1	Discussion		Noted. To be considered by SA WG3 for realistic timescales
S3-000319	Documents Postponed from Meeting #12 to Meeting#13	Secretary	Various	Discussion		
S3-000320	Answer to LS on Functions of Key Distribution and Key Administration for MAP security (postponed TD 224)	SA WG2	7.3	Discussion		Noted. (no response required)
S3-000321	Liaison statement to TSG-S WG3 on GTP Signalling Security (postponed TD 226)	CN WG2	7.3	Discussion		Response in TD386
S3-000322	Improved conversion functions for GSM-UMTS interoperation	Motorola, Lucent	11.3			E-mail discussion after the meeting.
S3-000323	5 CRs to 33.102	T-Mobil	11.3	Approval		CRs 097 & 098 approved. 099 was withdrawn, CRs 100, 101 were postponed
S3-000324	CR to 22.022: Update of the specification of ME personalisation to make it applicable for 3GPP	SA WG3	11.2	Approval	S3-000383	revised in TD383
S3-000325	Message from the Chairman	M. Walker	2	Information		Noted.
S3-000326	On the Security of 3GPP Networks (Presentation slides)	M. Walker	7.1	Presentation		Noted.
S3-000327	Clarification on UMTS AKA for GSM R'99 mobiles	GemPlus	10.3	Discussion		LS to SA1 in TD385
S3-000328	Use of IPSec IKE for layer 2 key distribution	Motorola	MAP AH 5.3	Discussion		V. Niemi to write LS to SA2 on Nes being IP-aware

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000329	Use IPSec to secure GTP messages	Motorola	MAP AH 5.2	Discussion		Discussed. More investigation needed on IPSec use and details. P.Howard to produce a draft position document for the Joint meeting with CN.
S3-000330	Initialisation of synchronisation for ciphering and integrity protection (Proposed 33.102:CR088R1)	T-Mobil	11.3			B. Vinck to check differences to approved 33.102 CR088
S3-000331	Using IKE for Layer I of MAP Security	T-Mobil	MAP AH 5.3			Drafting group to discuss and contribute to SA3.
S3-000332	Proposal for rejection of unciphered calls	France Telecom	10.4			To be taken into account when dafting response to TD373 (S. Nguyen Ngoc)
S3-000333	On the need for designing a new standard A5 algorithm for GSM	France Telecom	9.2			Discussed. A5/3 Req spec to be approved at SA3#14 and forwarded to SMG#32 for approval.
S3-000334	CR to 33.102: Removal of NW Wide Encryption	Ericsson	11.3	Approval		CR102. Approved
S3-000335	CR to 33.103: Removal of EUIC from 33.103	Ericsson	11.4	Approval		CR007 Approved
S3-000336	CR to 33.103: Removal of MAP Security from 33.103	Ericsson	11.4	Approval		CR008 Approved
S3-000337	CR to 33.103: SQN length	Ericsson	11.4	Approval		CR009 Approved
S3-000338	GSM AKA and conversion function c3	Ericsson	11.3	Discussion /Approval		Includes CR to 33.102. SA3/SMG10 would like operator choice for AKA
S3-000339	MAP Security Layer III open items	Ericsson	MAP AH 5.2			Note to be forwarded to CN WG4 on the Protection Modes and structure of TVP (32 bits suggested)
S3-000340	Agenda for MAP ad-hoc meeting	Chairman (M. Marcovici)	MAP AH Sec, 3	Approval		Approved
S3-000341	LS from SMG2 to SMG10/SA WG3 on Security functions in GERAN R00	SMG2	7.3	Discusion		Discussed under 10.4. Reply in TD379
S3-000342	CR to 33.105: Clarification of BEARER and DIRECTION parameters, corresponding to CR090 to CR to 33.102 (TD 262)	Nokia	11.5	Approval		CR011 Approved
S3-000343	Draft report of MAP ad-hoc group meeting V0.0.1	Secretary	10.4			Discussed and updated as V0.0.2 for comments to Secretary.
S3-000344	Draft LS to SA2 on use of IP for security key distribution	MAP AH Meeting	12	Approval	S3-000381	Revised in TD381

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000345	IMEI coding change	Nokia	7.4	Discussion		Some concerns on default IMEI use (problem for LI) LS to CN1, CN4, T3 provided in TD358
S3-000346	Withdrawn (allocated in error)	MAP AH Meeting	12	Approval		Withdrawn
S3-000347	Liaison statement to CN4 on Protection Mode 0 for MAP Security	SA WG3	12	Approval	S3-000353	revised in TD353
S3-000348	Reply LS to SMG2 on double encryption	SMG10		Information		Approved by e-mail 19/05/2000
S3-000349	Report of GSM 2000 Security Meeting No. 7	C Brookson	7.5	Information		Noted
S3-000350	Liaison Statement to SA WG2, SA WG5 and CN WG4 on Protocol Choice for Layer I of MAP Security	SA WG3	12	Approval	S3-000356	Replaced by TD 356
S3-000351	LS to CN4 on MAP over IP	SA WG3	12		S3-000364	Revised in TD364
S3-000352	Draft LS to CN, CN1, CN4, T3 and GSM SG about hexadecimal coding of IMEI	SA WG3	12	Approval	S3-000358	Modified in TD 358 and Approved. To be sent to CN, CN1, CN4, T3 and GSM SG
S3-000353	Liaison statement to CN4 on Protection Mode 0 for MAP Security	SA WG3	12	Approval	S3-000363	Updated in TD 363
S3-000354	Report on SMG 31bis	SA WG3 vice Chairman	7.2	Information		Discussed & noted
S3-000355	Independence of confidentiality and integrity in MAP Layer III and other layer III issues (amendment of TD 312)	Siemens AG	10.4	Discussion / Decision		Agreed and Attached to TD382
S3-000356	Liaison Statement to SA WG2, SA WG5 and CN WG4 on Protocol Choice for Layer I of MAP Security	SA WG3	12	Approval	S3-000359	Updated in TD359
S3-000357	Draft LS Clarification on UMTS AKA for SIM	SA WG3	12	Approval	S3-000375	revised in TD375
S3-000358	Draft LS to CN, CN1, CN4, T3 and GSM SG about hexadecimal coding of IMEI	SA WG3	12	Approval		Approved
S3-000359	Liaison Statement to SA WG2, SA WG5 and CN WG4 on Protocol Choice for Layer I of MAP Security (revision of TD 356)	SA WG3	12	Approval		Approved
S3-000360	Draft report of the joint session with TIA TR-45 AHAG on 3GPP/3GPP2 security harmonisation version 0.0.2	Secretary	7.5			Noted. To be submitted for approval at the next joint meeting.
S3-000361	Draft LS to SMG10 WPD on Clarification on new working conditions and reporting	SMG10	12	Approval	S3-000371	Updated in TD 371
S3-000362	Requirements Specification for the GSM A5/3 Encryption Algorithm V0.5	GSM Association	9.2		S3-000367	Updated in TD 367
S3-000363	Liaison statement to TSG-N WG4 on Security Policy for MAP Security (revision of TD 359)	SA WG3	12	Approval		Approved. To be forwarded to CN4
S3-000364	LS to CN4 on Security for MAP over IP	SA WG3	12	Approval		Approved. To be forwarded to CN4
S3-000365	Liaison statement from CN WG4 to SA3 on GTP signalling security	CN WG4	7.3			Response LS to CN4 in TD 370
S3-000366	LS from CN WG4 on Key Exchange and Key Distribution	CN WG4	7.3			LS to be produced for further discussion
S3-000367	Requirements Specification for the GSM A5/3 Encryption Algorithm V0.6	GSM Association	9.2			Noted (new version not received, but changes agreed during meeting)

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000368	Replay protection for core network signalling messages	Siemens AG / Vodafone Airtouch	10.4	Decision		Agreed and Attached to TD382
S3-000369	Draft LS to SAGE on consideration of SHA-1 for 3GGP(1) Authentication by ETSI SAGE	SA WG3	12	Approval	S3-000384	revised in TD 384
S3-000370	Reply laision statement to CN WG4 on GTP signalling security	SA WG3	12	Approval	S3-000386	Replaced by TD386
S3-000371	LS to SMG10 WPD on Clarification on new working conditions and reporting	SMG10/SA WG3	12	Approval		Approved
S3-000372	Invitation to joint SA3/CN WG meeting	Secretary	13	Information		Noted
S3-000373	Response to LS on non ciphered calls for GPRS	New SMG9	12	Approval		S. Nguyen Ngoc to provide a response taking TD332 into account for e-mail approval.
S3-000374	Proposed LS to CN WG4 on replay protectection	Vodafone Airtouch				Withdrawn
S3-000375	Draft LS Clarification on UMTS AKA for SIM (revision of TD357)	SA WG3	12	Approval	S3-000385	Revised in TD385
S3-000376	Draft Reply to an SMG2 LS about Security functions in GERAN	SA WG3	12	Approval	S3-000379	updated in TD 379
S3-000377	Proposed LS to N4 on MAP security Layer III	Vodafone Airtouch/ Motorola/ Siemens	12	Approval	S3-000382	revised in TD382
S3-000378	CR to 33.102: Clarification on terminology in user domain	Siemens Atea	11.3	Approval		To be updated and approved by e-mail (CC T3 for info)
S3-000379	Draft Reply to an SMG2 LS about Security functions in GERAN	SA WG3	12	Approval		Approved
S3-000380	Answer to LS New SIM toolkit feature: "Auto-answer & Mute-ringing"	SA WG3	12	Approval		Approved
S3-000381	LS to SA2 on use of IP for security key distribution	SA WG3	12	Approval		Approved
S3-000382	LS to CN4 on MAP security Layer III	SA WG3	12	Approval		Approved
S3-000383	CR to 22.022: Update of the specification of ME personalisation to make it applicable for 3GPP	SA WG3	11.2	Approval		CR002 Approved
S3-000384	LS to SAGE on consideration of SHA-1 for 3GGP(1) Authentication by ETSI SAGE	SA WG3	12	Approval		Approved
S3-000385	LS Clarification on UMTS AKA for SIM (revision of TD375)	SA WG3	12	Approval		Approved
S3-000386	Reply laision statement to CN WG4 on GTP signalling security	SA WG3	12	Approval		Approved
S3-000387	Liaison Statement on AHAG recommendation on Home Control ability to control the duration of the Security Association	SA WG3	12	Approval		Approved
S3-000388	liaison statement to AHAG that Recommendation 2 is still under discussion (depends if there is a timer in the VLR or not) and ask their opinion	Chairman (M. Marcovici)	e-mail	Approval		For e-mail approval after meeting #13
S3-000389	liaison statement to CN4 on SA WG3 position on Key management solutions	P Howard & R. Lubarsky	e-mail	Approval		For e-mail approval after meeting #13

Annex B: List of attendees

Name			Company	e-mail	3GPP Member	
Mr	Seppo	Alanara	Nokia	seppo.alanara@nokia.com	ETSI	FI
Mr.	Hiroshi	Aono	NTT DoCoMo, Inc	aono@mml.yrp.nttdocomo.co.jp	ARIB	JP
Mr.	Stephen	Billington	Motorola	Stephen.billington@motorola.com	Other	GB
Mr.	Colin	Blanchard	BT	colin.blanchard@bt.com	ETSI	GB
Mr.	Rolf	Blom	Ericsson	rolf.blom@era.ericsson.se	ETSI	SE
Mr.	Krister	Boman	Ericsson	Krister.Boman@emw.ericsson.se	ETSI	SE
Mr.	Charles Brice	Brookson	Dept Trade & Industry	cbrookson@iee.org	ETSI	GB
Mr.	David	Castellanos	Ericsson	David.castellanos-zamora@ece.ericsson.se	ETSI	SE
Mrs.	Lily	Chen	Motorola	lchen1@email.mot.com	Other	US
Mr.	Takeshi	Chikazawa	Mitsubishi Electric Co	chika@isl.melco.co.jp	ARIB	JP
Mr.	Hokyu	Choi	Samsung Electronics	choihk@telecom.samsung.co.kr	TTA	KR
Mr.	Per	Christoffersson	Telia Promotor	Per.E.Christoffersson@telia.se	ETSI	SE
Mr.	Louis	Finkelstein	Motorola	louisf@labs.mot.com	T1	US
Mr.	Guenther	Horn	Siemens AG	Guenther.horn@mchp.siemens.de	ETSI	DE
Mr.	Peter	Howard	Vodafone	peter.howard@vodafone.co.uk	ETSI	GB
Mr.	Kazuhiko	Ishii	NTT DoCoMo, Inc	ishii@mml.yrp.nttdocomo.co.jp	ARIB	JP
Mr.	Rafal	Jaczynski	Polkomtel SA	Rafal.jaczynski@polkomtel.com.pl	ETSI	PL
Mr.	Patrick	Johnson	Nortel Networks	pjohnson@nortelnetworks.com	T1	US
Mr.	Kenichiro	Kamachi	NEC Co.	k-kamachi@cj.jp.nec.com	ARIB	JP
Mr.	Geir	Koien	Telenor	Geir-myrdahl.koien@telenor.com	ETSI	NO
Mr.	Hyeonwoo	Lee	Samsung Electronics	woojaa@samsung.co.kr	TTA	KR
Mr.	Kook-Heui	Lee	Samsung Electronics	Kookheui@telecom.samsung.co.kr	TTA	KR
Mr.	Reginald	Lee	One2One	Reginald.Lee@one2one.co.uk	ETSI	GB
Mr.	Robert	Lubarsky	T-Mobil	Robert.Lubarsky@T-Mobil.de	ETSI	DE
Mr.	Michael	Marcovici	Lucent Technologies	marcovici@lucent.com	T1	US
Mrs.	Shiho	Moriai	NTT	shiho@isl.ntt.co.jp	ARIB	JP
Mr.	Hirotaka	Nakno	NTT DoCoMo, Inc	nakano@mml.yrp.nttdocomo.co.jp	ARIB	JP
Mr.	Sebastien	Nguyen Ngoc	France Telecom	Sebastien.nguyenngoc@francetelecom.fr	ETSI	FR
Mr.	Valtteri	Niemi	Nokia	valtteri.niemi@nokia.com	ETSI	FI
Mr.	Seong	Park	Samsung Electronics	sipark@telecom.samsung.co.kr	TTA	KR
Mr.	Maurice	Pope	ETSI	maurice.pope@etsi.fr	ETSI	FR
Mr.	Ludovic	Rousseau	Gemplus	Ludovic.Rousseau@gemplus.com	ETSI	FR
Mr.	Kazuyuki	Sato	NTT DoCoMo, Inc	kz@mml.yrp.nttdocomo.co.jp	ARIB	JP
Mr.	Benno	Tietz	Mannesmann Mobilfunk	benno.tietz@d2mammesmann.de	ETSI	DE
Mr.	Bart	Vinck	Siemens ATEA	bart.vinck@vnet.atea.be	ETSI	BE
Mr.	Stuart	Ward	Orange	stuart.ward@orange.co.uk	ETSI	GB
Mr.	Berthold	Wilhelm	Reg TP	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	Rel	Comment
TS	21.133	3.1.0	Security Threats and Requirements	April 99	Per Christoffersson	R99	
TS	22.022	3.0.1	Personalisation of GSM ME Mobile functionality specification - Stage 1	Oct 99		R99	Transfer>TSG#4, CR at TSG#5
TS	33.102	3.4.0	Security Architecture	Mar 00	Bart Vinck	R99	TSG#7: 3.4.0
TS	33.103	3.2.0	Security Integration Guidelines	Oct 99	Bart Vinck	R99	TSG#7: 3.2.0
TS	33.105	3.3.0	Cryptographic Algorithm requirements	June 99	Bart Vinck	R99	TSG#7: 3.3.0
TS	33.106	3.1.0	Lawful interception requirements	Jun 00	Bart Vinck	R99	
TS	33.107	3.0.0	Lawful interception architecture and functions	Dec 99		R99	New at TSG#6 approved
TS	33.120	3.0.0	Security Objectives and Principles	April 99	Tim Wright	R99	
TR	33.900	1.2.0	Guide to 3G security	Mar 00		R99	New at TSG#6
TR	33.901	3.0.0	Criteria for cryptographic Algorithm design process	June 99	Vinck Bart	R99	
TR	33.902	3.1.0	Formal Analysis of the 3G Authentication Protocol	Oct 99		R99	
TR	33.908	3.0.0	Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	Mar 00	M. Walker	R99	TSG#7: S3-000105=NP-000049
TR	33.909	3.0.0	ETSI SAGE 3GPP Standards Algorithms Task Force: Report on the evaluation of 3GPP standard confidentiality and integrity algorithms	Jun 00	M. Walker	R99	TSG#7: Is a reference in 33.908
TS	35.201	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications		M. Walker	R99	ex SAGE - not publicly available; supplied by ETSI under licencE
TS	35.202	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification		M. Walker	R99	ex SAGE - not publicly available; supplied by ETSI under licence
TS	35.203	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data		M. Walker	R99	ex SAGE - not publicly available; supplied by ETSI under licence
TS	35.204	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data		M. Walker	R99	ex SAGE - not publicly available; supplied by ETSI under licence

C.2 SMG10 Specifications

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

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

D.1 SA WG3 CRs at the Meeting (and by e-mail after meeting#12)

To be completed after e-mail approvals

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	Next Vers	Date	Source	WG	WG meeting	WG TD	WG status	Remarks
22.022	002		R99	Update of the specification of ME personalisation to make it applicable for 3GPP	F	3.0.1	3.1.0	29/05/2000	S3	S3	S3-13	S3-000383	agreed	Security
33.102	097	1	R99	Align of note and star in figure 18	D	3.4.0	3.5.0	18/05/2000	S3	S3	S3-13	S3-000323	agreed	Security
33.102	098		R99	Security mode set-up procedure	F	3.4.0	3.5.0	18/05/2000	S3	S3	S3-13	S3-000323	agreed	Security
33.102	099		R99	Clarification on condition on rejecting keys CR and IK	F	3.4.0		18/05/2000	S3	S3	S3-13	S3-000323	withdrawn	Security
33.102	100		R99	Replace COUNT by STARTCS and STARTPS	F	3.4.0		18/05/2000	S3	S3	S3-13	S3-000323	postponed	Security
33.102	101		R99	Clarification on the interworking procedure when a UICC has to support GSM and UMTS AKA	F	3.4.0		18/05/2000	S3	S3	S3-13	S3-000323	postponed	Security
33.102	102		R99	Removal of NW Wide Encryption	F	3.4.0	3.5.0	29/05/2000	S3	S3	S3-13	S3-000334	agreed	Security
33.103	007		R99	Removal of EUIC from 33.103	F	3.2.0	3.3.0	29/05/2000	S3	S3	S3-13	S3-000335	agreed	Security
33.103	008		R99	Removal of MAP Security from 33.103	F	3.2.0	3.3.0	29/05/2000	S3	S3	S3-13	S3-000336	agreed	Security
33.103	009		R99	SQN length	F	3.2.0	3.3.0	29/05/2000	S3	S3	S3-13	S3-000337	agreed	Security
33.105	011		R99	Clarification of BEARER and DIRECTION parameters	F	3.3.0	3.4.0	29/05/2000	S3	S3	S3-13	S3-000342	agreed	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	Remarks
None														

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD Number	Title	Source	Comment
S3-000315	LS from AHAG: Use of SHA-1 for AKA f0-f5	AHAG (F Quick)	Response LS in TD384
S3-000320	Answer to LS on Functions of Key Distribution and Key Administration for MAP security (postponed TD 224)	SA WG2	Noted. (no response required)
S3-000321	Liaison statement to TSG-S WG3 on GTP Signalling Security (postponed TD 226)	CN WG2	Response in TD386
S3-000341	LS from SMG2 to SMG10/SA WG3 on Security functions in GERAN R00	SMG2	Response in TD379
S3-000365	Liaison statement from CN WG4 to SA3 on GTP signalling security	CN WG4	Response in TD370
S3-000366	LS from CN WG4 on Key Exchange and Key Distribution	CN WG4	LS to be produced for further discussion
S3-000373	Response to LS on non ciphered calls for GPRS	New SMG9	S. Nguyen Ngoc to provide a response taking TD332 into account for e-mail approval.

E.2 Liaisons from the meeting

TD Number	Title	Status	Comment
S3-000348	Reply LS to SMG2 on double encryption	Approved	Approved by e-mail 19/05/2000
S3-000358	Draft LS to CN, CN1, CN4, T3 and GSM SG about hexadecimal coding of IMEI	Approved	To be forwarded to CN, CN1, CN4, T3 and GSM SG
S3-000359	Liaison Statement to SA WG2, SA WG5 and CN WG4 on Protocol Choice for Layer I of MAP Security (revision of TD 356)	Approved	To be forwarded to SA2, SA5 and CN4
S3-000363	Liaison statement to TSG-N WG4 on Security Policy for MAP Security (revision of TD 359)	Approved	To be forwarded to CN4
S3-000364	LS to CN4 on Security for MAP over IP	Approved	To be forwarded to CN4
S3-000371	LS to SMG10 WPD on Clarification on new working conditions and reporting	Approved	To be forwarded to SMG10 WPD Chairman
S3-000379	Draft Reply to an SMG2 LS about Security functions in GERAN	Approved	To be forwarded to SMG2
S3-000381	LS to SA2 on use of IP for security key distribution	Approved	To be forwarded to SA2
S3-000382	LS to CN4 on MAP security Layer III	Approved	To be forwarded to CN4. TD312, 355 & 368 attached
S3-000384	LS to SAGE on consideration of SHA-1 for 3GGP(1) Authentication by ETSI SAGE	Approved	To be forwarded to ETSI SAGE
S3-000385	LS to SMG9 /T3 on clarification on UMTS AKA for SIM	Approved	To be forwarded toSMG9/T3
S3-000386	Reply laision statement to CN WG4 on GTP signalling security	Approved	To be forwarded to CN4
S3-000388	liaison statement to AHAG that Recommendation 2 is still under discussion (depends if there is a timer in the VLR or not) and ask their opinion	(e-mail approval)	Chairman to produce
S3-000389	liaison statement to CN4 on SA WG3 position on Key management solutions	(e-mail approval)	P. Howard and R. Lubarsky to produce for e-mail approval

Annex F: List of Actions from the meeting

ACTION #13/1: **Chairman: To send the liaison in TD S3-000309 to AHAG.**

ACTION #13/2: **P. Howard and R. Lubarsky: To create a liaison statement to CN4 on SA WG3 position on Key management solutions. To be approved by e-mail in time for the Joint SA WG3/CN WGs meeting.**

ACTION #13/3: **G. Køien: Liaison on Recommendation 1 to be forwarded to AHAGand Liaison on Recommendation 3 to be completed.**

ACTION #13/4: **Chairman: To produce a liaison to AHAG that Recommendation 2 is still under discussion (depends if there is a timer in the VLR or not) and ask their opinion.**

ACTION #13/5: **M. Pope: To transmit the updated report version 0.0.3 to AHAG contact.**

ACTION #13/6: **M Pope: Check if any documentation from SA WG2 on system architecture is available, if so, then send it to the SA WG3 mailing list.**

ACTION #13/7: **All: Draft Work Item descriptions to be produced by 5 June 2000. 2nd draft after SA WG3 comments 9 June 2000 for input to joint meeting. Joint meeting comments included by 16 June 2000 and sent to e-mail list. For e-mail approval by 21 June 2000.**

ACTION #13/8: **P. Howard: Update the Release 2000 Features, Building Blocks and Work Tasks document in TD S3-000318 in line with changes to the work programme made at SA3#13 and forward to SA WG2.**

ACTION #13/9: **S. Nguyen Ngoc: To provide a response to TD S3-000373 (New SMG9)for approval by e-mail.**

ACTION #13/10: **B. Vinck: To update TD S3-000378 and send to SA WG3 list for e-mail approval and to T WG3 for review.**

ACTION #13/11: **B. Vinck: To check the changes to the original CR088 and comment on the proposals in TD S3-000330.**

ACTION #13/12: **C. Blanchard: To verify that network-wide encryption has been completely removed from 33.103, Release 1999.**

ACTION #13/13: **All: To discuss conversion functions for GSM-UMTS interoperation.**
M. Marcovici: To send a revised CR to 33.102 for approval by e-mail.

Annex G: Subjects for e-mail approval after the meeting

1 P. Howard and R. Lubarsky: To create a liaison statement to CN4 on SA WG3 position on Key management solutions. To be approved by e-mail in time for the Joint SA WG3/CN WGs meeting

2 Draft Work Item descriptions to be produced by 5 June 2000. 2nd draft after SA WG3 comments 9 June 2000 for input to joint meeting. Joint meeting comments included by 16 June 2000 and sent to e-mail list. For e-mail approval by 21 June 2000.

3 S. Nguyen Ngoc: To provide a response to TD S3-000373 (New SMG9)for approval by e-mail.

4 B. Vinck: To update TD S3-000378 and send to SA WG3 list for e-mail approval and to T WG3 for review.

5 33.102 CR100: This CR was postponed to e-mail approval after the meeting.

6 33.102 CR101: This CR was postponed to e-mail approval after the meeting.

7 TD S3-000322: M. Marcovici to send a revised CR to 33.102 for approval by e-mail.

Deadlines for e-mail approvals: 9 June for items needed for the SA WG3/CN WGs joint meeting, 16 June for other items.