3GPP TSG SA WG3 Security — S3#18 **S3-010141**

21 - 24 May, 2001

Phoenix, USA

3GPP TSG SA WG3 Security — S3#17

27 February - 02 March, 2001

Göteburg, Sweden

Source: **Secretary**

Title: **Draft report version 0.0.4**

Document for: **Comment**

---

1 Opening of the meeting 3
1.1 Joint SA WG2/SA WG3 meeting preparation session 3
1.2 SA WG3 main meeting session 4

2 Meeting objectives 4

3 Approval of the agenda 5

4 Registration and assignment of input documents 5

5 Approval of report from S3#16 5

6 Reports / Liaisons 6
6.1 3GPP plenary 6
6.2 3GPP WGs 6
6.3 Lawful interception sub-group 8
6.4 SAGE 8
6.5 Others (ETSI MSG, GSMA, GSM2000, T1P1, TIA, TR-45, AHAG) 8

7 Joint meeting with S2 9

8 Work programme 9
8.1 Review security work programme 9
8.2 Status of security work items 9
8.3 New security work items 9

9 Security issues 9
9.1 GERAN 9
9.2 Location services 9
9.3 MExE security 10
9.4 Report on the Design and Evaluation of The MILENAGE Algorithm Set 10

10 S3 specifications/reports 10
10.1 3G TS 33.102 Security architecture (2G/3G interoperation etc.) 10
10.2 3G TS 33.103 Integration guidelines 12
10.3 3G TS 33.105 Algorithm requirements 12
10.4 Draft TR and TS on network domain security 12

10.5 Draft TR and TS on IM subsystem security 13
10.6 Draft 3G TR 33.900 Guide to 3G security 13
10.7 GSM TS 03.35 IST 13
10.8 3G TS 33.106 / 3G TS 33.107 LI 13

11 Future meeting dates and venues 14

12 Any other business 14

13 Close of meeting 14

Annex A: List of attendees at the SA WG3#16 meeting 15

Annex B: List of documents 17

B.1 Documents at SA WG3 meeting #17 17

B.2 Documents forwarded to NDS ad-hoc meeting 27

B.3 Documents forwarded to IMS ad-hoc meeting 28

B.4 Documents Postponed to meeting #18 29

Annex C: Status of specifications under SA WG3 responsibility 30

Annex D: List of CRs to specifications under SA WG3 responsibility 32

Annex E: List of Liaisons 33

E.1 Liaisons to the meeting 33

E.2 Liaisons from the meeting 35

Annex F: List of actions from the meeting 36

Annex G: SA WG3 Work Plan 37

---

1 Opening of the meeting

Mr. Krister Boman welcomed delegates to Goteberg, Sweden, on behalf of Ericsson and provided the domestic arrangements for the meeting.

1.1 Joint SA WG2/SA WG3 meeting preparation session

M. Marcovici Chaired and opened the preparation meeting and outlined the objectives, which were to review the input documents from SA WG3 to the joint meeting and to provide an updated agenda for the meeting.

The draft agenda was considered in TD S3-010054. It was agreed that discussions should be based on contributions to the meeting, and the list of issues were identified and the agenda updated to include these.

Mr. K Boman presented the "aSIP Access Security for IP-based services" presentation to SA WG3, and this was updated taking into account comments made and provided in TD S3-010082 which was forwarded to the joint meeting for presentation and discussion.

TD S3-010028 Trust Models for IM Domain Security. This was introduced by Motorola, who intended to present this to the joint meeting with SA WG2 for discussion. It was questioned whether the material was appropriate for the joint meeting, but Motorola stated that it contained architectural issues and that their comments would be useful. The document was noted and Motorola presented it to the joint meeting.

It was decided to consider the Liaisons from SA WG2 before the meeting:

TD S3-010018 LS on Replacement of 23.121 for R4 onwards. This asks all WGs to check and update their specifications for Rel4 onwards to replace references to 23.121 with the new 23.221 as this has been created for Rel4 onwards by SA WG2. It was noted that this document is not yet under change control, and no action should be taken until it is approved by TSG SA. The SA WG3 Secretary Clarified with the SA WG2 Secretary that this was valid for Release 4 onwards.

AP ~~16~~17/01: All SA WG3 Rapporteurs to check references to 23.121 for Rel4 onwards documents and modify to 23.221 via CRs. - To be done only if 23.121 is approved at the SA#11 meeting.

TD S3-010022 Proposed Reply LS on “Proposal not to use the IMSI as the identity of an IM subscriber". It was recognised that the Caller ID issues need to be investigated and that 23.228 contained some text, but that the information flows needed some correction. It was decided to ask SA WG2 to look at this. It was also agreed to raise the issue of Private User Identifications containing the IMSI. It was questioned also whether the NAI confidentiality needs protecting. SA WG2 views would be collected on this if time allowed. This was not dealt with in the joint session, and further discussion ensued in the SA WG3 meeting. It was decided that a response liaison would be created pointing out the potential issues to SA WG2, which was provided in TD S3-010115 which was approved.

TD S3-010036 LS on "IM User Identities". It was noted that SA WG2 were preparing a response on this issue. **<RETURN?>**

TD S3-010041 Removal of Visited Control S-CSCF option from the Rel 5 architecture. SA WG2 informed groups of the removal of the Visited Control Option in the S-CSCF. This was a fundamental change and will require further review in SA WG3. **Delegates should review this for contribution to SA WG3 meeting #18**.

TD S3-010017 Response to LS on some issues related to optimised IP speech support in GERAN. This raised the question whether IPsec and header removal/compression are mutually exclusive. This was further dealt with at the joint session and in SA WG3 (see below).

TD S3-010034 LS on Security implications of supporting "hiding". It was decided that this needed discussion in the SA WG3 plenary meeting, and that a new agenda item may be needed for the topic. The LS was further considered later in the meeting and it was agreed that the issue would be postponed to the next meeting (or next joint meeting with SA WG2), as there was no time to deal with it at the joint sessions.

TD S3-010021 Proposed Reply LS on the Work Item “Cx Interface specification”. This LS had been copied to SA WG3 for information, and was noted.

Second joint session preparation:

Documents for the morning joint session with SA WG2 were considered as follows:

SA WG2 TD S2-010618 from the joint session was considered, but the annex was not included. It was agreed to come back to this in the morning joint session with SA WG2.

TD S3-010016 Response to LS (T2-000793) on discussion document on UE functionality split over physical devices. It was agreed to come back to this in the morning joint session SA WG2.

SA WG2 TD S2-010511 from the joint session was introduced briefly by AT&T.

SA WG2 TD S2-010718 Network hiding mechanisms for TS XX.YYY (from the joint session) was considered, it was asked whether the security mechanisms should be included in SA WG2 specifications.

TD S3-010083 Providing the S-CSCF name to the P-CSCF. Ericsson briefly introduced this contribution. Ericsson concluded that it is a bad idea to send data, that is supposed to be hidden, to the entity it should be hidden from, and proposed not to introduce any additional mechanism (other means to achieve the result was provided in a contribution to SA WG2). It was suggested that this was a standardisation issue in order to achieve vendor-independence. It was agreed to come back to this in the morning joint session SA WG2.

Report of the joint sessions:

The report of the joint session was provided by SA WG2 Secretary and provided to SA WG3 in TD S3-010105. This was provided for information at the meeting and was noted. Delegates were asked to check the report and make comments to the SA WG2 Secretary.

1.2 SA WG3 main meeting session

S. Puetz Chaired and opened the meeting in the absence of Michael Walker, who was not able to attend the meeting. He welcomed delegates to the meeting and outlined the schedule.

IPR Declaration: The Chairman reminded delegates of the 3GPP IPR policy and their obligation to declare essential IPRs to their respective Partner Organisations (SDOs), as provided in TD S3-010092.

2 Meeting objectives

The objectives of the meeting were to complete as much as possible the work to be submitted to SA#11 Plenary in March 2001 for approval/information.

3 Approval of the agenda

The agenda, provided in TD S3-010001 was updated to add new items, where contributions had been provided and re-produced in TD S3-010096 which was approved.

4 Registration and assignment of input documents

The available documents were allocated to their respective agenda items.

5 Approval of report from S3#16

The report of the previous meeting, provided in TD S3-010002 including comments received over e-mail was checked. The list of attendees needed completion, which was done and with these changes, the report was approved as version 1.0.0.

The list of actions was considered:

AP 16/01: Completed - It was reported that The GSM Association and ETSI are still negotiating the MoU for A5/3. When agreed, the other 3GPP Partner SDOs will be asked to agree the deployment of A5/3. This needs to be completed before ETSI SAGE can start work, which is expected to be completed within 3 months of the start of their work.

AP 16/02: Completed.

AP 16/03: Ongoing ?

AP 16/04: The links to the SA WG3 WI sheets on the ftp server had not been included in the report. The Secretary, Mr. M. Pope agreed to add these links as a new annex in the final version (1.0.0) of the report.

AP 16/05: Completed / continuing action (interested companies to contribute to ITU-T)

AP 16/06: Not completed. C Brrokson to continue e-mail discussion.

AP 16/07: Completed.

AP 16/08: Completed, but the report has not yet been published by the SDOs. M Pope undertook to check if the TR had been published, and to provide the status of Partner agreements to SA WG3.

AP 17/01: M Pope to check if the KASUMI Evaluation report has been published as a TR, and to report the status of the SDO agreements to the SA WG3 e-mail list.

AP 16/09: Completed, M Pope undertook to provide the status of Partner agreements to SA WG3.

AP 16/10: Completed.

The postponed TD S3-000691 was reported as being withdrawn by Vodafone and was not presented to this meeting.

TDs S3-000723 and S3-000734 had been postponed from meeting #16 and needed to be returned to at this meeting. These were provided in TD S3-010097 and TD S3-010098.

6 Reports / Liaisons

6.1 3GPP plenary

There was no report on SA WG3 issues from the TSG SA#10 Plenary.

6.2 3GPP WGs

TD S3-010004 LS from T WG2: Bluetooth as USAT local link mechanism. This LS was copied to SA WG3 for information and noted.

TD S3-010005 LS from T WG2: IM Subsystem Address Storage on USIM. This LS was a reply to SA WG2 and was noted.

TD S3-010007 LS from T WG3: Minimum clock frequency indication. T WG3 informed SA WG3 of their change to the minimum clock frequency to 3 MHz (from 3.25 MHz). It was noted that 33.105 would need modification to reflect this. Nokia agreed to prepare a CR for this, which was provided in TD S3-010111 (see agenda item 10.3). The LS was noted.

TD S3-010009 LS from CN WG1: UE Triggered Authentication and Key Agreement During Connections. This was introduced by Vodafone and related document TD S3-010053 " UE-triggered re-authentication during connections", from Vodafone, was dealt with at the same time. The mechanism for forcing re-authentication was questioned in the Vodafone contribution, and it was suggested not to include the mechanism in Rel-4, and to consider whether it should be included in Rel-5 specifications. It was noted that the WI " UE triggered authentication during connections" (ID SEC1-UETADC) has no supporting companies, **SA WG3 agreed to delete this work item from the work plan**.

TD S3-010010 Reply LS to SA WG2 for "IM Subsystem Address Storage on USIM". This LS was copied to SA WG3 for information and noted.

TD S3-010011 Response LS from CN WG4 on SA WG3 agreements on MAPSec. It was agreed to handle this at the NDS ad-hoc meeting. TD S3-010011 was therefore noted.

TD S3-010106 provided the liaison to CN WG4 on the postponing of Map Security (NDS) to Release 5, which was approved.

TD S3-010013 LS from T WG3: Introduction of Operator PLMN Name List for 3G Rel-4. TD T3-010098 provides the CR to allow Network modification of the UE displayed PLMN Name. The security risk of unauthorised modification of the display name was thought to be of no impact over the current situation. The LS was therefore noted.

TD S3-010016 Response to LS (T2-000793) on discussion document on UE functionality split over physical devices. This suggests that SA WG2 should study the architectural impact of UE functionality split, and SA WG3 should study the security impacts. TD S3-010031 contained a response to the LS from SA WG1, which suggested that SA WG3 should determine which scenarios can be provided from a security viewpoint. SA WG2, however, thought that a wider scope should be defined by SA WG1 before SA WG3 consider restricting scenarios on security grounds. A short consideration of the scenarios in the T WG2 document revealed large potential security issues, so it was agreed that a liaison statement should be produced asking SA WG1 to define the requirements before a full analysis of the security implications could be evaluated. AT&T Wireless agreed to produce this LS, which was provided in TD S3-010112 which was presented to the meeting, updated editorially in TD S3-010133 and approved.

TD S3-010019 LS on authentication test algorithm to be implemented in test USIM. Siemens reported that there were some concerns over the implementation of the procedures. In particular, the use of f1 and f1* caould cause a lack of testing for f1 implementations. Siemens agreed to produce a LS, which was provided in TD S3-010113 which was updated in TD S3-010137 to correct the document header and was approved.

TD S3-010020 Elaboration of KEY IDENTIFICATION EVENT (T WG3 Chairman). This contribution was briefly explained by P. Howard. The proposed feature introduces a new "event" that indicates that a key on the MMI has been pressed and includes the key identification, in accordance with the “Get Inkey” command. This puts the responsibility of detecting a key being pressed on the UE, whilst "freeing up" the USAT to perform other activities. T WG3 asked SA WG1 to indicate if the feature was considered useful, and SA WG3 to investigate potential security threats. SA WG1 replied to this LS in TD S3-010032 and agreed that the functionality could be useful for Multimedia applications, which attached a Release 5 CR to 22.038. It was decided that a LS to T WG3 and SA WG1 should be created informing them that SA WG3 would perform a security analysis of the feature (for Release 5). This was provided in TD S3-010114 which was modified in TD S3-010128 and approved.

TD S3-010023 Response on LS regarding security aspects of UE conformance testing. This was sent for information and noted.

TD S3-010030 LS from SA WG1: Convergence of QoS approaches in 3GPP and TIPHON. This was intended for TSG SA and was noted.

TD S3-010034 LS on Security implications of supporting "hiding". Due to lack of time, this was postponed to the SA WG3 meeting #18.

TD S3-010035 LS on integrity protection for GERAN. This was introduced by Nokia, and outlines that integrity protection for GERAN is being designed to be equivalent as for UTRAN, with some exceptions, mainly due to the design of GERAN and the overhead that can be tolerated. GERAN proposed a kjoint meeting with SA WG3 either seperate from, or in conjunction with one of their ad-hoc meetings. It was agreed that Mr. Niemi would contact the GERAN ad-hoc Chairman to try to find a suitable date for the meeting, and create a LS to this effect. This was provided in TD S3-010116 which was modified slightly in TD S3-010129 and approved. (This was again modified to remove "Draft" from the cover sheet in TD S3-010135).

TD S3-010036 LS on "IM User Identities". SA WG2 had formulated a response to this LS and discussed it in the joint session (S2-010757). M. Marcovici agreed to check this response and provided the document to the meeting. It was agreed to forward this to the ad-hoc meeting on IMS (26 April 2001).

TD S3-010037 LS reply to SA WG3 on request for information to complete security work items. CN WG4 asked SA WG3 to describe any specific areas of concern they have with respect to TrFO if any have been raised by their group. This LS was noted.

TD S3-010039 LS from RAN WG2 on Checking the integrity of UE security capabilities. This was introduced by Nokia in conjeunction with TD S3-010070 "GSM ciphering capability protection in UTRAN" (Nokia), which discusses responses to the questions asked by RAN WG2 and a CR in TD S3-010109. The technical solution presented in TD S3-010109 was approved and a liaison statement to RAN WG2 was created in TD S3-010118, which was modified slightly in TD S3-010130 (This was again modified to remove "Draft" from the cover sheet in TD S3-010136), and a companion CR in TD S3-010117. The LS and CR were then approved.

TD S3-010041 LS from SA WG2 on Removal of Visited Control S-CSCF option from the Rel 5 architecture. This was provided for information and noted.

TD S3-010043 LS on MExE and Security Collaboration. The T WG2 MExE group had started a Security Analysis Activity and attached the Work Item Description for this activity. T WG2 MExE would also like to hear SA WG3 views on participation, and possible joint meetings, regarding this activity. It was agreed that the supporting companies in the WI sheet would support the security aspects in SA WG3.

TD S3-010017 Response to LS on some issues related to optimised IP speech support in GERAN. This issue was discussed briefly at the joint session and the LS was later presented to SA WG3. After some discussion, it was agreed that a response would be sent to SA WG2 and GERAN asking for further clarification **<RETURN?>**

TD S3-010125 LS from CN WG1: Re-transmission of authentication requests. The referenced attached CR to this LS was not included (*this was made available after the meeting in TD S3-010134 for information*). P. Howard had drafted a corresponding CR to 33.102, in TD S3-010124 (see agenda item 10.1).

6.3 Lawful interception sub-group

No report was provided by the LI subgroup, but their input documents were dealt with under agenda item 10.8.

6.4 SAGE

It was reported that the MILENAGE work is complete and the work on A5/3 will commence when formal SDO agreements are finalised.

6.5 Others (ETSI MSG, GSMA, GSM2000, T1P1, TIA, TR-45, AHAG)

TD S3-010058 The Wireless Communication Transfer Protocol (WCTP). It was agreed that this contribution should be considered with TD S3-010003 (see below).

TD S3-010003 Using Kasumi in WAP specification. This asks SA WG3 to take the steps necessary to allow the KASUMI algorithm in the WAP Forum as an additional algorithm in their TLS cipher suite, for both air-link level and data communication level ciphering. It was clarified that the owner of KASUMI is Mitsubishi, rather than 3GPP or ETSI as implied in this contribution. It was reported that the WAP Forum were looking into the use of AES rather than KASUMI at present. This was considered an IPR issue, and M. Pope agreed to take this request back to ETSI MCC for processing.

AP 17/02: M Pope to take the request from the WAP Forum for use of KASUMI (TD S3-010003) to the ETSI Lawyer for processing as appropriate.

TD S3-010025 LIASON TO ETSI, FOR FORWARDING TO 3GPP, AND COMMUNICATIONS TO TIA TR-45.7, FOR FORWARDING TO 3GPP2, ON IMT2000 MANAGEMENT. It was decided to postpone this liaison to the next meeting. Delegates were asked to contact their SA WG5 colleagues to see if they have dealt with the document.

TD S3-010095 Request to investigate an extension of the A5 cipher key length. The GSMA SG expressed a concern among GSM operators that the upcoming A5/3 must be able to exploit the same full key size of 128 bit as the 3G cipher algorithm allows, whereas GSM infrastructure currently only allows 64 bits. GSMA SG asked SA WG3 to study the possibility of allowing both key lengths in GSM, and to provide their views to GSMA SG. There was some discussion on the creation of another security architecture for GSM. The current specification of A5/3 is planned for 64 bit keys, following the GSM architecture. It was generally felt that A5/3 should not be introduced and then improved a year later, due to equipment investments. Charles Brookson agreed to create a WI for agreement as the next SA WG3 meeting, to study this issue and to provide the analysis and proposals to SA WG3. In

the meantime, no steps should be taken to fix the key length for A5/3. Delegates were invited to make contribution on this issue to the next SA WG3 meeting.

7 Joint meeting with S2

TD S3-010084 contained the agenda for the joint meeting. The draft report of the joint sessions were provided by the SA WG2 Secretary in TD S3-010105 and was noted. Delegates were asked to comment directly to the SA WG2 Secretary (alain.sultan@etsi.fr).

8 Work programme

8.1 Review security work programme

The Security WI project plan was updated after the meeting by the SA WG3 Secretary, showing changes resulting from this meeting to the version available after TSG SA meeting #10. This is provided in Annex G of this report.

8.2 Status of security work items

TD S3-010093 End-to-End Encryption of Wireless VoIP (E^3 VoIP). Lucent presented the slides which discussed the advantages and issues of End to End encryption. The presentation was discussed and noted.

8.3 New security work items

TD S3-010090 Work Item Description for Network based end-to-end security. The proposed WI was introduced by BT, after questions for clarification on the scope of the WI, the WI was updated to include these clarifications and provided in TD S3-010123 which was approved.

TD S3-010089 Re-Introduction of Network Wide End to End Encryption. The re-introduction of this text (which had been removed from Release 1999) into Release 5 at this stage was not thought appropriate as the work is still ongoing. It was agreed that the complete set of changes should be elaborated and a single CR created to insert this. The CR was therefore not accepted.

TD S3-010033 Requirement for End-to-End Encryption of IP Multimedia Subsystem Controlled Voice over IP Calls. P. Howard agreed to develop a response LS to SA WG1 informing them that SA WG3 have agreed a WI on Network based end-to-end security, for Release 5. This to be agreed by e-mail after the meeting.

9 Security issues

9.1 GERAN

The GERAN related contributions were dealt with under other agenda items.

9.2 Location services

Nokia provided a presentation on Location Services as an overview for SA WG3, before discussing the input documents on the current problems with ciphering in GERAN. The presentation was noted.

TD S3-010069 Status in ciphering communication between MS and SMLC in GPRS. This proposes two possible ways to solve the ciphering problem. This was discussed and noted.

TD S3-010008 LS from TSG GERAN: updated information on ciphering of RRLP messages between SMLC and MS in GPRS. This LS proposes two ways of solving the LCS ciphering issue, but discards one due to efficiency reasons. TSG GERAN asked SA WG3 ciphering experts to consider the proposal to employ an instance of the LLC layer in the SMLC and to provide opinions on which ciphering key should be used to cipher messages. This was discussed and noted.

TD S3-010088 LCS for GPRS and the BSS+ Solution. This proposed LS was presented by Ericsson for information and advice. This was discussed and noted.

There was a general discussion on these issues and it was agreed that a response LS should be sent to GERAN. A drafting group was tasked to produce a response to be approved by e-mail after the meeting.

AP 17/03: V. Niemi to convene a group to produce a LS to GERAN on the GERAN LCS ciphering issue, to be approved by e-mail.

9.3 MExE security

The MExE issues were dealt with under other agenda items.

9.4 Report on the Design and Evaluation of The MILENAGE Algorithm Set

TD S3-010014 Analysis of Milenage. This was introduced by Qualcomm International. It was reported that there was no concerns discovered with the algorithm, but an (avoidable) potential weakness had been noted. It was explained that the statement in the report: "It is the authors' opinion that the algorithm set does not satisfy the design criteria" was an **error**, based on a mis-reading of the ETSI SAGE design criteria. The document was revised by Qualcomm International, removing the misleading statement and provided in TD S3-010108 The author apologised for this statement appearing in the evaluation report. It was agreed that the report (TD S3-010108) will be sent to ETSI SAGE for information.

The meeting thanked Qualcomm International for having performed this valuable work.

TD S3-010015 Milenage evaluation report version 1.0. This was introduced by Per Christoffersson, and is the 5th document in the MILENAGE series. SA WG3 were asked to approve the document for forwarding to SA#11 for approval as a TR. The report was approved. It was ***stressed*** that rapid publication of this report by the SDOs would help prevent external evaluations being made which may lead to rumours and/or false claims being made on it's integrity.

10 S3 specifications/reports

10.1 3G TS 33.102 Security architecture (2G/3G interoperation etc.)

TD S3-010042: Draft LS to T WG3: TR 31.900 - SIM/USIM Internal and External Interworking Aspects. This LS was produced as a response to the T WG3 LS (TD S3-010012 - TD T3-010109) and was presented by Siemens Atea. There was some discussion on the topics raised. There was good support for not allowing Scenario F because of the reduced security when connecting through all 3G NEs except for the HLR/AuC. Scenario E should not be allowed as it violates the security requirements, and there should be no USIM-subscription allowed in a 2G HLR network. Scenarios D and E were seen as theoretical implementations only, and unlikely to be used in practice, and a note to this effect was included in the LS. The 2G/3G terminology was discussed, and it was concluded that more study on this is needed and a note would be added to the response liaison stating the concerns over the proposed definition. The LS was updated to Exclude Scenario F and include the note and reviewed, the final version, provided in TD S3-010099 was approved and transmitted immediately to T WG3. A response was received in TD S3-010122 which was presented by the Chairman. T WG3

requested more information on why their assumption that there will be 3G USIMs provided by 2G Network providers and they wished to keep scenario F as a valid scenario. It was recognised that a response to this was needed, but due to lack of time, it was agreed that a reply LS would be prepared after the meeting for e-mail approval. **V Niemi agreed to lead this drafting group**.

Siemens requested a decision from SA WG3 on the location of the Confidentiality and Integrity Protection functions for IMS following the joint session with SA WG2. They suggested that the confidentiality function should be in the P-CFCS and the Integrity function could, as a compromise for agreement within SA WG3, be located in the Home Network (e.g. S-CFCS or HSS). Ericsson requested that such a decision should not be taken before analysis of the scenario, and that this should be a working assumption. The urgency for decision on this matter was also voiced and it was suggested that a working assumption would not really be adequate and a decision needs to be made in a short time-frame. Ericsson agreed that a decision on the location of the security functions should be made at this meeting, but that some time would be needed to investigate the proposed solution.

Ericsson suggested that a meeting between this meeting and the May 2001 meeting should be held to stabilise the specifications.

The presentation file (COMPROMISE PROPOSAL.ppt) included in TD S3-010094 was provided by Siemens as a compromise solution, with accompanying CR. This presentation slide was ~~was~~ modified slightly and provided in TD S3-010100 which was approved.

TD S3-010097 Comments from K Holley on S3-000700 (re-presented S3-000723). This was provided for information and was noted.

TD S3-010052 CR to 33.102: Add requesting node type and identity to authentication data request. It was pointed out that the change was to an informative annex (sequence numbering key management scheme). Vodafone replied that the scheme had become a de-facto method for implementation, although operators could choose to use another scheme. The reason for non-acceptance was also commented upon, as it gave the impression that non-implementation of this scheme would lead to insecure and/or inefficient key management. It was agreed that the consequences for super-charged networks could not be determined at present, and that the consequences if not approved should be modified accordingly. Vodafone agreed to update the CR and re-present it to SA WG3. The CR was updated to remove the identity of the requesting node in TD S3-010103 which was approved. It was agreed to send this CR to CN WG4 to inform them of the change. **This CR shall be sent to TR-45 for information.**

TD S3-010056 CR to 33.102: Additional Parameters in Authentication Failure Report (REL-4). This was presented by Ericsson, the attachment to the document provided background for discussion leading to the proposed CR. It was clarified that the *System Capability* parameter is in the 3GPP2 system, but not in the 3GPP system at present. It was suggested that this parameter be removed from the CR. The CR was updated in TD S3-010104 which was approved. **This CR shall be sent to TR-45 for information.** A stage 3 CR was also required, and Ericsson undertook to ensure this was done in CN WG4, which was provided in TD S3-010110 which was approved.

TD S3-010068 Authentication Positive Notification Procedure. This was introduced by Lucent. Vodafone reported that they had done some work on the Stage 3 in CN WG4 and had the following assumptions for implementation possibilities:

1 PAR sent for all Authentications of all users in a H-PLMN
2 PAR sent for all Authentications for Specified users
3 PAR applied for specified AVs (implies some form of AV tagging is needed).

The requirements were not fixed, and no CR had been presented for this, and it was recognised that this could not be completed in time for Rel-4. **It was agreed to ask TSG SA to move this to Rel-5,**

and a liaison statement was produced to TR-45 and CN WG4 informing them of this in TD S3-010120: "Clarification on positive authentication report". It was requested that this change should be planned as "Post-Rel-5", and that TR-45 and CN WG4 should be told this. This was agreed and the LS updated in TD S3-010131 which was approved. **It was agreed to ask TSG SA to move this to Post-Rel-5.**

TD S3-010121 LS to TR45 AHAG: Define responsibility and procedure. This was presented by Lucent and outlines a procedure to inform SA WG3 and AHAG of LSs and CRs affecting documents under joint control. This was modified editorially and provided in TD S3-010132 which was approved.

TD S3-010006 CR to 33.102: RES has to be a multiple of 8 bits (R99). This CR was approved. **This CR shall be sent to TR-45 for information.**

TD S3-010094 CR to 33.102: Timing of security mode procedure. This CR was approved.

TD S3-010064 CR to 33.102: Add bit ordering convention (R99). This CR was approved. **This CR shall be sent to TR-45 for information.**

TD S3-010085 CR to 33.102 v 3.7.0: Optional Support for USIM-ME interface for GSM-Only ME (replaces TD S3-010047) (R99). This was related to TD S3-010044 (Problem with no USIM-ME interface in GSM only ME). This document had been agreed in SA WG3 meeting #16.

This was further updated in TD S3-010119, which was presented by Siemens Atea and reviewed. Some minor changes were made and the CR finalised in TD S3-010126 which was approved.

TD S3-010046 CR to 33.102 v 3.7.0: Definition corrections (R99). The CR was reviewed and updated in TD S3-010127 which was approved. It was noted by the Secretary after the meeting that the Category was incorrect, and the CR was then revised to show Category "F" in TD S3-010138 (approved).

TD S3-010124 CR to 33.102: Correction to the handling of re-transmitted authentication request messages on the ME (R99). This CR was approved. **This CR shall be sent to TR-45 for information.**

10.2 3G TS 33.103 Integration guidelines

TD S3-010065 CR to 33.103: Add bit ordering convention (R99). This CR was approved.

10.3 3G TS 33.105 Algorithm requirements

TD S3-010111 CR to 33.105: Change of minimum clock frequency. This CR was produced in response to TD S3-010007 and was approved.

TD S3-010048 CR to 33.105: RES has to be a multiple of 8 bits (R99). This CR was approved. **This CR shall be sent to TR-45 for information.**

TD S3-010066 CR to 33.105: Add bit ordering convention (R99). This CR was approved.

10.4 Draft TR and TS on network domain security

TS 33.200: The Rapporteur for NDS, Geir M. Køien, reported progress since the last meeting and the results were provided in TD S3-010055. Geir Køien was thanked for the good job he had done in producing this specification. The outstanding issues were listsed in an attachment to TD S3-010055. He asked whether the material should be presented to TSG SA for information as Rel-4, or as both Rel-4 and Rel-5, or to move it to Rel-5. He also requested that inputs to this document should be

---

presented in the form of CRs (i.e. with change bars) in order that changes are clear to everybody and not open to interpretation after the meeting.

The TS was reviewed on-line. There was still many parts which are written in TR-style (i.e. general advice rather than requirements). It was recognised that some information was still missing, and how this could be completed in time for Rel-4 was questioned, given the short time-scale.

The way to provide some material from the document, and contributions at the meeting was considered in time for Rel-4 (2 weeks timescale before SA Plenary). Realistically, it was considered only possible to provide this for Rel-5.

It was agreed to ask TSG SA to move MAP Security to Rel-5. An ad-hoc meeting was arranged to concentrate on the elaboration of this document (see agenda item 11). A Liaison Statement to CN WG4 was produced to inform them of this decision, provided in TD S3-010106 which was approved

The Rapporteur asked for contributions to be produced in the format of Change Requests to aid implementation and understanding of the proposed modifications.

10.5 Draft TR and TS on IM subsystem security

An ad-hoc meeting was arranged to concentrate on the elaboration of this document (see agenda item 11).

10.6 Draft 3G TR 33.900 Guide to 3G security

There were no contributions on this document.

10.7 GSM TS 03.35 IST

TD S3-010049 CR to 03.35: IST implementation for non-CAMEL subscribers (R99). This had been approved at SA WG3, but had not been presented to SA Plenary, and Ericsson asked for endorsement in order to ensure it is sent to TSG SA#11. The CR was approved.

10.8 3G TS 33.106 / 3G TS 33.107 LI

~~TD S3-010066 CR to 33.106: Add bit ordering convention (R99). This CR was approved.~~

TD S3-010059 CR to 33.106: Release 5 updates. This CR was modified slightly (removing Release 2000 from the definition of 3GMS) and provided in TD S3-010107 which was approved. ***The LI group were asked to consider modifying "3GMS" to "3GPP MS" in the document.***

TD S3-010060 CR to 33.106: Update of TS 33.106 for Release 4. This CR was approved.

TD S3-010062 CR to 33.107: Correction of Location information parameters in interception event records (R99). This CR was approved.

TD S3-010061 CR to 33.107: Update of TS 33.107 for Release 4. This was presented for comments from SA WG3. The LI group would like comments for their meeting next week and will update accordingly before sending them to SA WG3 for e-mail approval, if there are no substantial comments from SA WG3. (**Comments to B McKibben and/or editor**). The document was therefore noted.

TD S3-010063 CR to 33.107: Update of TS 33.107 for Release 5. This was presented for comments from SA WG3. The LI group would like comments for their meeting next week and will update accordingly before sending them to SA WG3 for e-mail approval, if there are no substantial comments from SA WG3. (**Comments to B McKibben and/or editor**). The document was therefore noted.

3GPP TSG SA WG3 Security — S3#17 14 **Draft report version 0.0.4**

TD S3-010038 LS Response Lawful Intercept support on the Mc interface. This was introduced by Ericsson. CN WG4 asked SA WG3 to confirm their working assumption and to arrange a join meeting to resolve the issue if necessary. It was agreed that the LS should be forwarded to the LI group for consideration.

AP 17/04: M Pope to forward the LS in TD S3-010038 to the LI Group for action. The LI group to responsd to CN WG4 and to inform SA Plenary as appropriate.

11 Future meeting dates and venues

An ad-hoc meeting to focus on Network Domain Security drafting covering the outstanding issues was arranged. The output to be a mutually agreed version of the NDS specification for approval at the SA WG3 meeting, with the aim to submit to TSG SA for information in June 2001.

An ad-hoc meeting to focus on Access Security drafting covering the outstanding issues was arranged.

The meetings were decided for 24-25 April for Network Domain Security and 26 April for Access Security in Madrid, hosted by Ericsson (hosting to be confirmed).

A list of documents forwarded from this meeting to the ad-hoc meetings is provided in Annex X.

Meeting	Date	Location	Host
GERAN ad-hoc joint meeting	10-11 April 2001	Helsinki, Finland	Nokia
NDS ad-hoc meeting	24-25 April 2001	Madrid, Spain	Ericsson
IMS ad-hoc meeting	26 April 2001	Madrid, Spain	Ericsson
S3#18	21 or 22 – 24 May 2001	Phoenix, Arizona (TBC)	Motorola (TBC)
S3#19	3 or 4 - 6 July 2001	London (TBC)	Vodafone (TBC)
S3#20	15 or 16 – 18 October 2001	~~Sidney~~Sydney, Australia (TBC)	Qualcomm Int. (TBC)
S3#21	TBD	TBD	TBD

12 Any other business

Elections for the Chairman and two Vice Chairmen candidatures were announced to be held at the next SA WG3 meeting (May 2001). Delegates were asked to forward any candidatures to MCC in good time before the meeting.

Output documents

The list of approved CRs to be forwarded to TSG SA is provided in Annex D.

The list of approved output LSs is provided in Annex E, section E.2.

The list of documents forwarded to the ad-hoc meetings and postponed to the next meeting is provided in Annex B, sections B.2, B.3 and B.4.

13 Close of meeting

The Chairman thanked the Hosts for the excellent facilities provided for the meeting, and the delegates for their hard work and co-operation and closed the meeting.

Annex A: List of attendees at the SA WG3#~~16~~ 17 meeting

~~**TO BE CORRECTED: THE UPDATED ATTENDEES LIST WAS MISSING AT END OF MEETING !**~~

Name	Company	e-mail	3GPP ORG	
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp	ARIB	JP
Mr. Kazuhiko Ishii	NTT DoCoMo Inc.	ishii@mml.yrp.nttdocomo.co.jp	ARIB	JP
Mrs. Teruharu Serada	NEC Corporation	serada@aj.jp.nec.com	ARIB	JP
Mr. Stefan Andersson	ERICSSON L.M.	stefan.x.andersson@ecs.ericsson.se	ETSI	SE
Mr. Jari Arkko	ERICSSON L.M.	jarkko@piuha.net	ETSI	SE
Mr. Marc Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	ETSI	BE
Ing. Krister Boman	ERICSSON L.M.	krister.boman@emwericsson.se	ETSI	SE
Mr. Charles Brookson	DTI	cbrookson@iee.org	ETSI	GB
Miss Tao Bu	NOKIA Corporation	tao.bu@nokia.com	ETSI	FI
Mr. Denis CARABIN	GEMPLUS Card International	denis.carabin@gemplus.com	ETSI	FR
Mr. David Castellanos	ERICSSON L.M.	david.castellanos@ece.ericsson.se	ETSI	ES
Mr. Xiaobao Chen	Lucent Technologies N. S. UK	xchenl@lucent.com	ETSI	GB
Mr. Per Christoffersson	TELIA AB	per.e.christoffersson@telia.se	ETSI	SE
Mr. Laurent COUREAU	France Telecom	laurent.coureau@francetelecom.com	ETSI	FR
Mr. Guenther Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI	DE
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vf.vodafone.co.uk	ETSI	GB
Mrs. Tiina Koskinen	NOKIA Corporation	tiina.s.koskinen@nokia.com	ETSI	FI
Mr. Carlos Lazaro	TELEFONICA de España S.A.	lazaro_c@tsm.es	ETSI	ES
Mr. Alexander Leadbeater	BT	alex.leadbeater@bt.com	ETSI	GB
Mr. Anders Liljekvist	ERICSSON L.M.	anders.liljekvist@era.ericsson.se	ETSI	SE
Mr. Petri Nyberg	SONERA Corporation	petri.nyberg@sonera.com	ETSI	FI
Mr. Vasilis Polychronidis	Openwave Systems (N.I.) Ltd	vasilis.polychronidis@openwave.com	ETSI	US
Dr. Stefan Pütz	Deutsche Telekom MobilNet	stefan.puetz@t-mobil.de	ETSI	DE
Mr. Bill Robinson	MOTOROLA Ltd	bill.robinson@motorola.com	ETSI	GB
Mr. Greg Rose	QUALCOMM EUROPE S.A.R.L.	ggr@qualcomm.com	ETSI	US
Ms. Stéphanie Salgado	SCHLUMBERGER	salgado@montrouge.tt.slb.com	ETSI	FR
Mr. Lee Valerius	NORTEL NETWORKS (EUROPE)	YES - NO	ETSI	US
Mr. Stuart Ward	ORANGE PCS LTD	stuart.ward@orange.co.uk	ETSI	GB
Mr. Ernest Woodward	Intel Sweden AB	ernest.e.woodward@intel.com	ETSI	US
Mr. George Babut	Rogers Wireless Inc.	gbabut@rci.rogers.com	T1	CA
Ms. Lilly Chen	Motorola Inc.	lchen1@email.mot.com	T1	US
Mr. Janos Csirik	AT&T Corp.	janos@research.att.com	T1	US
Mr. John Ioannidis	AT&T Wireless Services, Inc.	ji@research.att.com	T1	US
Mr. Michael Marcovici	Lucent Technologies	marcovici@lucent.com	T1	US
Mr. Dewayne Sennett	AT&T Wireless Services, Inc.	dewayne.sennett@attws.com	T1	US
Mr. Hugh Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	T1	US
Mr. Daisuke Igarashi	NTT DoCoMo Inc.	igarashi@nw.yrp.nttdocomo.co.jp	TTC	JP
Mr. Johnson Oyama	Nippon Ericsson K.K.	johnson.oyama@nrj.ericsson.se	TTC	JP

Mr. Maurice Pope	Mobile Competence Center	maurice.pope@etsi.fr	ETSI	FR
Mr. Daniel Brown	T1 Standards Committee	adb002@email.mot.com	T1	US
Mr. Tom Inklebarger	AT&T Wireless Services, Inc	tominkle@home.com	T1	US
Pekka Hiitola	Nokia	pekka.hiitola@nokia.com	ETSI	FI
Peter Windirsch	Deutsche Telekom	Peter.Windirsch@t-systems.de	ETSI	DE
Sebastien Nguyen Ngoc	France Telecom	sebastien.nguyenngoc@francetelecom.com	ETSI	FR
Marc Bojarzin	Materna	marc.bojarzin@materna.de	ETSI	DE
Mrs. Geneviève Mange	ALCATEL S.A.	G.Mange@alcatel.de	ETSI	DE
Mr. Louis Finkelstein	Motorola	louisf@labs.mot.com	T1	US

Annex B: List of documents

B.1 Documents at SA WG3 meeting #17

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010001	Draft Agenda for SA WG3 meeting #17	Chairman	3	Approval	S3-010096	updated and revised in TD96
S3-010002	Draft report of meeting #16 (v0.0.5 with revision marks)	Secretary	5	Approval		Modified and approved
S3-010003	Using Kasumi in WAP specification	WAP Security Group	6.5	Discussion		M Pope to contact ETSI Lawyers on use of KASUMI in WAP Forum
S3-010004	Bluetooth as USAT local link mechanism	T WG2	6.2	Information		Noted
S3-010005	LS from T WG2: IM Subsystem Address Storage on USIM	T WG2	6.2	Information		Noted
S3-010006	CR to 33.102: RES has to be a multiple of 8 bits (R99)	Siemens Atea	10.1	Approval		Approved.To be sent to TR-45.
S3-010007	LS from T WG3: Minimum clock frequency indication	T WG3	6.2	Action		Noted. Nokia prepared CR in TD111
S3-010008	LS from TSG GERAN: UPDATED INFORMATION ON CIPHERING OF RRLP MESSAGES BETWEEN SMLC AND MS IN GPRS	TSG GERAN	6.2	Action		Discussed and Noted
S3-010009	LS from CN WG1: UE Triggered Authentication and Key Agreement During Connections	CN WG1	6.2	Action		Dealt with TD53, - WI to be deleted
S3-010010	Reply LS to SA WG2 for "IM Subsystem Address Storage on USIM"	CN WG1	6.2	Information		Noted
S3-010011	Response LS from CN WG4 on SA3 agreements on MAPSec	CN WG4	6.2	Action		To be dealt with at NDS ad-hoc
S3-010012	LS from T WG3: TR 31.900 - SIM/USIM Internal and External Interworking Aspects	T WG3	6.2	Action		Response in TD99
S3-010013	LS from T WG3: Introduction of Operator PLMN Name List for 3G Rel-4	T WG3	6.2	Action		Noted

3GPP TSG SA WG3 Security — S3#17 **18** **Draft report version 0.0.4**

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010014	Analysis of Milenage	Qualcomm	9.4	Discussion	S3-010108	Error in statement corrected in TD 108
S3-010015	Milenage evaluation report version 1.0	ETSI SAGE	9.4	Approval		Approved. Rapid publication by SDOs desirable
S3-010016	Response to LS (T2-000793) on discussion document on UE functionality split over physical devices	SA WG2	6.2	Discussion		Response in TD133
S3-010017	Response to: LS on some issues related to optimised IP speech support in GERAN	SA WG2	6.2	Discussion		Response LS to be created ?
S3-010018	LS on Replacement of 23.121 for R4 onwards	Lucent (TSG-SA WG2)	6.2	Discussion		Check if Rel4 or Rel5. Noted. Editors to check references to 23.121 in their specs.
S3-010019	LS on authentication test algorithm to be implemented in test USIM	T WG1	6.2	Information		Reply LS in TD137
S3-010020	Elaboration of KEY IDENTIFICATION EVENT	T WG3 Chairman	6.2	Discussion		SA WG1 response in TD32. SA WG3 response in TD128
S3-010021	Proposed Reply LS on the Work Item “Cx Interface specification”	SA WG2	6.2	Information		Noted
S3-010022	Proposed Reply LS on “Proposal not to use the IMSI as the identity of an IM subscriber	SA WG2	6.2	Discussion		Response LS in TD115
S3-010023	Response on LS regarding security aspects of UE conformance testing	T WG1	6.2	Discussion		Noted
S3-010024	Mobile Execution Environment (Presentation)	Motorola	9.3	Information		POSTPONED TO NEXT MEETING
S3-010025	LIASON TO ETSI, FOR FORWARDING TO 3GPP, AND COMMUNICATIONS TO TIA TR-45.7, FOR FORWARDING TO 3GPP2, ON IMT2000 MANAGEMENT	ITU-T Q16/4 SG4	6.5	Information		POSTPONED TO NEXT MEETING (check SA WG5 response)

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010026	3GPP TS 33.200 V0.3.1	Motorola	10.4	Discussion	S3-010067	Combined with TD29
S3-010027	MAP DOI Status	Ericsson	10.4	Discussion and decision		Companion to TD102. To be handled in NDS ad-hoc
S3-010028	Trust Models for IM Domain Security	Motorola	10.5	Discussion and decision		Noted. Presented to Joint session
S3-010029	NDS architecture for IP-Based protocols	Motorola	10.4	Discussion and decision	S3-010067	Combined with TD26
S3-010030	LS from SA WG1: Convergence of QoS approaches in 3GPP and TIPHON	SA WG1	6.2	Discussion		Intended for TSG SA - Noted.
S3-010031	LS from SA WG1: UE functionality split	SA WG1	6.2	Discussion		Response in TD133
S3-010032	Response to LS (T3-010xxx) from T3 chairman on the Elaboration of KEY IDENTIFICATION EVENT	SA WG1	6.2	Discussion		Noted. SA WG3 response in TD128
S3-010033	Requirement for End-to-End Encryption of IP Multimedia Subsystem Controlled Voice over IP Calls	SA WG1	8.2+E76	Discussion		P Howard to develop response and approve by e-mail
S3-010034	LS on Security implications of supporting "hiding"	TSG-CN1/SA2 SIP ad hoc	6.2	Discussion		POSTPONED to next meeting (or joint SA WG2 meeting)
S3-010035	LS on integrity protection for GERAN	TSG GERAN ad hoc #4	6.2	Discussion		Agreed for transmission by GERAN Chairman. Response in TD129
S3-010036	LS on "IM User Identities"	TSG-CN1-TSG-SA2 SIP AD-Hoc	6.2	Discussion		(SA WG2 response in S2-010757). To be handled in IMS ad-hoc
S3-010037	LS reply to SA3 on request for information to complete security work items	CN WG4	6.2	Discussion		Noted
S3-010038	LS Response Lawful Intercept support on the Mc interface	CN WG4	6.2	Discussion		M Pope to forward to LI group

3GPP TSG SA WG3 Security — S3#17 **20** **Draft report version 0.0.4**

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010039	LS on Checking the integrity of UE security capabilities	RAN WG2	6.2	Discussion		Response CR & LS in TD117, TD118 (see also TD70)
S3-010040	Support of certificates in 3GPP security architecture	Nokia	10.1	Discussion		rev of S3-000709
S3-010041	Removal of Visited Control S-CSCF option from the Rel 5 architecture	SA WG2	6.2	Discussion		Noted
S3-010042	Draft LS to T3: TR 31.900 - SIM/USIM Internal and External Interworking Aspects	SA WG3 (Siemens Atea)	10.1	Approval	S3-010099	Updated in TD99
S3-010043	LS on MExE and Security Collaboration	T WG2	6.2	Discussion		WI supporting companies to support the security aspects
S3-010044	Problem with no USIM-ME interface in GSM-only ME	Siemens Atea	10.1	Discussion and decision		~~POSTPONED TO NEXT MEETING~~Dealt with at S3#16 - background to TD126)
S3-010045	Terminology in TS 33.102/TR 31.900	Siemens Atea	10.1	Discussion and decision		POSTPONED TO NEXT MEETING
S3-010046	CR to 33.102 v 3.7.0: Definition corrections (R99)	Siemens Atea	10.1	Approval	S3-010127	Updated in TD127
S3-010047	CR to 33.102 v 3.7.0: Optional Support for USIM-ME interface for GSM-Only ME (R99)	Siemens Atea	10.1	Approval	S3-010085	Updated in TD085
S3-010048	CR to 33.105: RES has to be a multiple of 8 bits (R99)	Siemens Atea	10.3	Approval		Approved To be sent to TR-45
S3-010049	CR to 03.35: IST implementation for non-CAMEL subscribers (R99)	Ericsson L.M.	10.7	Approval		Approved
S3-010050	MAP-SA Negotiation and Distribution Procedures	Ericsson L.M.	10.4	Discussion and decision		To be handled in NDS ad-hoc
S3-010051	CR to 33.200: Cleanup of MAPsec structure of protected operations (REL-4)	Ericsson	10.4	Approval		To be handled in NDS ad-hoc

3GPP TSG SA WG3 Security — S3#17 **21** **Draft report version 0.0.4**

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010052	CR to 33.102: Add requesting node type and identity to authentication data request (REL-4)	Vodafone	10.1	Approval	S3-010103	Revised in TD103
S3-010053	UE-triggered re-authentication during connections	Vodafone	8.2	Decision		WI deleted
S3-010054	Agenda for Joint Meeting – 3GPP SA WG2/3GPP SA WG3	Joint meeting Chairman	7	Approval	S3-010084	Approved at JM
S3-010055	Update information on TS33200 (v031 to v032)	Telenor	10.4			Noted
S3-010056	CR to 33.102: Additional Parameters in Authentication Failure Report (REL-4)	Ericsson	10.1	Approval	S3-010104	Revised in TD104
S3-010057	Protection Profiles for MAP Security	Ericsson	10.4	Discussion and Decision		To be handled in NDS ad-hoc
S3-010058	The Wireless Communication Transfer Protocol (WCTP)	T WG2	6.2	Discussion		Considered with TD003
S3-010059	CR to 33.106: Release 5 updates	SA WG3-LI	10.8	Approval	S3-010107	Revised in TD107
S3-010060	CR to 33.106: Update of TS 33.106 for release 4	SA WG3-LI	10.8	Approval		Approved
S3-010061	CR to 33.107: Update of TS 33.107 for Release 4	SA WG3-LI	10.8	Comment		Noted. Comments requested
S3-010062	CR to 33.107: Correction of Location information parameters in interception event records (R99)	SA WG3-LI	10.8	Approval		Approved
S3-010063	CR to 33.107: Update of TS 33.107 for Release 5	SA WG3-LI	10.8	Comment		Noted. Comments requested
S3-010064	CR to 33.102: Add bit ordering convention (R99)	Vodafone	10.1	Approval		Approved To be sent to TR-45
S3-010065	CR to 33.103: Add bit ordering convention (R99)	Vodafone	10.2	Approval		Approved
S3-010066	CR to 33.106: Add bit ordering convention (R99)	Vodafone	10.3	Approval		Approved
S3-010067	NDS architecture for IP-Based protocols (replaces TDs 26 & 29)	Motorola	10.4	Discussion and decision		To be handled in NDS ad-hoc
S3-010068	Authentication Positive Notification Procedure	Lucent	10.1	Discussion and decision		Move to Post-Rel-5
S3-010069	STATUS IN CIPHERING COMMUNICATION BETWEEN MS AND SMLC IN GPRS	Nokia	9.2	Decision		(postponed from S3#16) Noted

3GPP TSG SA WG3 Security — S3#17 **22** **Draft report version 0.0.4**

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010070	GSM ciphering capability protection in UTRAN	Nokia	6.2/10.1	Discussion		Response CR & LS in TD117, TD118. (see also TD39)
S3-010071	An analysis of 3G TS 23.228 v170 “IP Multimedia (IM) Subsystem - Stage 2” from a security point of view.	Siemens AG		Discussion and Decision		To be handled in IMS ad-hoc
S3-010072	Considerations on trust and risk	Siemens AG		Discussion and Decision		Presented at joint meeting in support of TD 77
S3-010073	Summary of arguments and proposal for a decision on location of security functions	Siemens AG		Discussion and Decision		Presented at joint meeting in support of TD 78
S3-010074	Open issues in IM domain security beyond location of security functions	Siemens AG		Discussion and Decision		To be handled in IMS ad-hoc
S3-010075	Mandate 3DES for use of ESP with GTP-C	Siemens AG		Discussion and Decision		To be handled in NDS ad-hoc
S3-010076	An analysis of 3G TS 23.228 v170 “IP Multimedia Subsystem - Stage 2” from a security point of view	Siemens AG	JM	Presentation		Presented & discussed in joint session
S3-010077	Considerations on trust and risk	Siemens AG	JM	Presentation		Presented & discussed in joint session
S3-010078	Summary of arguments	Siemens AG	JM	Presentation		Presented & discussed in joint session
S3-010079	Open issues beyond location of security functions	Siemens AG	JM	Presentation		Presented & discussed in joint session
S3-010080	Overview of alternative information flows for IMS authentication and key agreement	Siemens AG	JM	Presentation		Presented & discussed in joint session
S3-010081	Authentication and protection mechanisms for IM CN SS	Ericsson, Nokia, Lucent and Orange				To be handled in IMS ad-hoc
S3-010082	aSIP - Access Security for IP-based services	Ericsson (Rapporteur)	JM			Presented & discussed in joint session

3GPP TSG SA WG3 Security — S3#17 **23** **Draft report version 0.0.4**

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010083	Providing the S-CSCF name to the P-CSCF	Ericsson	JM			Presented & discussed in joint session
S3-010084	Draft agenda for the joint SA WG2/SA WG3 meeting	SA WG3	JM	Approval		Approved at JM
S3-010085	CR to 33.102 v 3.7.0: Optional Support for USIM-ME interface for GSM-Only ME (replaces TD47) (R99)	Siemens Atea	10.1	Approval	S3-010119	Updated in TD119
S3-010086	Protection Profiles for MAP Security	Siemens	10.4			To be handled in NDS ad-hoc
S3-010087	CR to 33.200: MAP Protection Profiles (REL-4)	Siemens	10.4	Approval		To be handled in NDS ad-hoc
S3-010088	LCS for GPRS and the BSS+ Solution	Ericsson	9.2	Information and Advice		Noted
S3-010089	Re- Introduction of Network Wide End to End Encryption	BT	8.2	Discussion and decision		Rejected. Complete e-e system to be developed and a single CR created to introduce it in R5
S3-010090	Work Item Description for Network based end-to end-security	BT	8.2	Discussion & Action	S3-010123	revised in TD123
S3-010091	IPsec and IKE profile for network domain security	Ericsson	10.4	Discussion and decision		Companion to TD101. To be handled in NDS ad-hoc
S3-010092	IPR statement	MCC	1	Information		Noted
S3-010093	End-to-End Encryption of Wireless VoIP (E3 VoIP)	Lucent	8.2	Discussion and decision		Presented & discussed
S3-010094	Proposal for compromise on IM domain security and CR to 33.102: Timing of security mode procedure	Siemens	10.1	Decision and Approval	S3-010100 (not CR)	Compromise updated in TD100. CR approved
S3-010095	LS from GSMA SG: Request to investigate an extension of the A5 cipher key length	GSMA SG	6.5	Discussion		Delegates to contribute to next meeting
S3-010096	Revised agenda for meeting #17	Chairman	2	Approval		Approved

3GPP TSG SA WG3 Security — S3#17 **24** **Draft report version 0.0.4**

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010097	Comments from K Holley on S3-000700 (re-presented S3-000723)	BT	10.8	Information		Postponed from S3#16. Noted.
S3-010098	Response to LS on "Clarification of UMTS-AKA for GSM R'99 Mobiles" & support of UMTS AKA for GSM only R4 MEs	SA WG1	6.2	Discussion		POSTPONED TO NEXT MEETING
S3-010099	LS to T3: TR 31.900 - SIM/USIM Internal and External Interworking Aspects (update of TD42)	SA WG3 (Siemens Atea)	10.1	Approval		Approved
S3-010100	Proposal for compromise on IM domain security	Siemens	10.1	Approval		Approved
S3-010101	IPsec, IKE, MAPSEC DOI Profiles for the 3GPP	Ericsson		Presentation		Companion to TD91. To be handled in NDS ad-hoc
S3-010102	MAP DOI: Modifications and Status	Ericsson		Presentation		Companion to TD27. To be handled in NDS ad-hoc
S3-010103	CR to 33.102: Add requesting node type and identity to authentication data request (REL-4) (rev of TD52)	Vodafone	10.1	Approval		Approved To be sent to TR-45
S3-010104	CR to 33.102: Additional Parameters in Authentication Failure Report (REL-4) (rev of TD56)	Ericsson	10.1	Approval		Approved To be sent to TR-45
S3-010105	Minutes of the S2/S3 joint meeting - draft 0.1	SA WG2 Secretary	JM	Information		Noted. Comments to SA WG2 Secretary
S3-010106	LS to CN WG4 on Move of TS 33.200 - Network Domain Security from Rel-4 to Rel-5	SA WG3		Approval		Approved
S3-010107	CR to 33.106: Release 5 updates	SA WG3-LI	10.8	Approval		Approved
S3-010108	Analysis of Milenage	Qualcomm	9.4	Information		Noted. Send to ETSI SAGE for information
S3-010109	CR to 33.102: GSM ciphering capability Handling in Security Mode set up procedure (R99)	Nokia		Approval	S3-010117	Updated in TD117
S3-010110	LS to CN4 on Additional Parameters in AFR procedure	Ericsson		Approval		Approved
S3-010111	CR to 33.105: Change of minimum clock frequency	Nokia		Approval		Approved

3GPP TSG SA WG3 Security — S3#17 **25** **Draft report version 0.0.4**

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010112	LS to SA WG1 on UE functionality split over physical devices	AT&T Wireless		Approval	S3-010133	Updated in TD133
S3-010113	LS to T WG1 on testing UE procedures	Siemens		Approval		Approved (updated in TD137 with correct header)
S3-010114	Response to LS (S1-010200) to T3 and S1 on the Elaboration of KEY IDENTIFICATION EVENT			Approval	S3-010128	Updated in TD128
S3-010115	Response LS (to TD22) on multiple user identities			Approval		Approved
S3-010116	(Draft) Reply to LS on integrity protection for GERAN	Nokia		Approval	S3-010129	Updated in TD129
S3-010117	CR to 33.102: GSM ciphering capability Handling in Security Mode set up procedure (R99) (rev of TD109)	Nokia		Approval		Approved
S3-010118	(Draft) LS to TSG RAN on UE ciphering capabilities	Nokia		Approval	S3-010130	Updated in TD130
S3-010119	CR to 33.102 v 3.7.0: Optional Support for USIM-ME interface for GSM-Only ME (replaces TD85) (R99)	Siemens Atea, Ericsson	10.1	Approval	S3-010126	Updated in TD126
S3-010120	LS to TR-45: Clarification on positive authentication report	SA WG3			S3-010131	Updated in TD131
S3-010121	LS to TR45 AHAG: Define responsibility and procedure	SA WG3		Discussion and decision	S3-010132	Updated in TD132
S3-010122	TR 31.900 - SIM/USIM Internal and External Interworking Aspects	T WG3	10.1	Discussion		Response to TD99. V. Niemi to draft response LS for e-mail approval
S3-010123	Work Item Description for Network based end-to-end security (rev of TD90)	BT	8.2	Discussion & Action		Approved
S3-010124	CR to 33.102: Correction to the handling of re-transmitted authentication request messages on the ME (R99)	Vodafone	10.1	Approval		Approved To be sent to TR-45
S3-010125	LS from CN WG1: Re-transmission of authentication requests	CN WG1	6.2	Discussion and decision		Attachment CR missing (provided after meeting in TD134). Response in TD124

3GPP TSG SA WG3 Security — S3#17 **26** **Draft report version 0.0.4**

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010126	CR to 33.102 v 3.7.0: Optional Support for USIM-ME interface for GSM-Only ME (replaces TD85) (R99)	Siemens Atea, Ericsson	10.1	Approval		See also TD44. Approved
S3-010127	CR to 33.102: Definition corrections (R99) (rev of TD46)	Siemens Atea	10.1	Approval		Approved. (Corrected by Secretary to Cat F and in TD138)
S3-010128	Response to LS (S1-010200) to T3 and S1 on the Elaboration of KEY IDENTIFICATION EVENT	SA WG3		Approval		Approved
S3-010129	(Draft) Reply to LS on integrity protection for GERAN (Response to TD22)	SA WG3		Approval	S3-010135	Approved (updated to remove "draft" in TD135
S3-010130	(Draft) LS to TSG RAN on UE ciphering capabilities	Nokia		Approval	S3-010136	Approved (updated to remove "draft" in TD136
S3-010131	LS to TR-45: Clarification on positive authentication report	SA WG3		Approval		Approved
S3-010132	LS to TR45 AHAG: Define responsibility and procedure	SA WG3		Discussion and decision		Approved
S3-010133	LS to SA WG1 on UE functionality split over physical devices	AT&T Wireless		Approval		Approved
S3-010134	Attachment to TD 125: CR to 24.008 Re-transmission of authentication requests	CN WG1	6.2	Information		Provided after meeting for information
S3-010135	Reply to LS on integrity protection for GERAN (Response to TD22)	SA WG3		Approval		Approved
S3-010136	LS to TSG RAN on UE ciphering capabilities	SA WG3		Approval		Approved
S3-010137	LS to T WG1 on testing UE procedures	SA WG3		Approval		Approved
S3-010138	CR142r1 to 33.102: Definition corrections (R99) (rev of TD127 with correct Category F)	SA WG3	10.1	Approval		Approved

B.2 Documents forwarded to NDS ad-hoc meeting

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010011	Response LS from CN WG4 on SA3 agreements on MAPSec	CN WG4	6.2	Action		To be dealt with at NDS ad-hoc
S3-010027	MAP DOI Status	Ericsson	10.4	Discussion and decision		Companion to TD102. To be handled in NDS ad-hoc
S3-010050	MAP-SA Negotiation and Distribution Procedures	Ericsson L.M.	10.4	Discussion and decision		To be handled in NDS ad-hoc
S3-010051	CR to 33.200: Cleanup of MAPsec structure of protected operations (REL-4)	Ericsson	10.4	Approval		To be handled in NDS ad-hoc
S3-010057	Protection Profiles for MAP Security	Ericsson	10.4	Discussion and Decision		To be handled in NDS ad-hoc
S3-010067	NDS architecture for IP-Based protocols (replaces TDs 26 & 29)	Motorola	10.4	Discussion and decision		To be handled in NDS ad-hoc
S3-010075	Mandate 3DES for use of ESP with GTP-C	Siemens AG		Discussion and Decision		To be handled in NDS ad-hoc

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010086	Protection Profiles for MAP Security	Siemens	10.4			To be handled in NDS ad-hoc
S3-010087	CR to 33.200: MAP Protection Profiles (REL-4)	Siemens	10.4	Approval		To be handled in NDS ad-hoc
S3-010091	IPsec and IKE profile for network domain security	Ericsson	10.4	Discussion and decision		Companion to TD101. To be handled in NDS ad-hoc
S3-010101	IPsec, IKE, MAPSEC DOI Profiles for the 3GPP	Ericsson		Presentation		Companion to TD91. To be handled in NDS ad-hoc
S3-010102	MAP DOI: Modifications and Status	Ericsson		Presentation		Companion to TD27. To be handled in NDS ad-hoc

B.3 Documents forwarded to IMS ad-hoc meeting

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010036	LS on "IM User Identities"	TSG-CN1-TSG-SA2 SIP AD-Hoc	6.2	Discussion		(SA WG2 response in S2-010757). To be handled in IMS ad-hoc
S3-010071	An analysis of 3G TS 23.228 v170 “IP Multimedia (IM) Subsystem - Stage 2” from a security point of view.	Siemens AG		Discussion and Decision		To be handled in IMS ad-hoc
S3-010074	Open issues in IM domain security beyond location of security functions	Siemens AG		Discussion and Decision		To be handled in IMS ad-hoc
S3-010081	Authentication and protection mechanisms for IM CN SS	Ericsson, Nokia, Lucent and Orange				To be handled in IMS ad-hoc

B.4 Documents Postponed to meeting #18

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010025	LIASON TO ETSI, FOR FORWARDING TO 3GPP, AND COMMUNICATIONS TO TIA TR-45.7, FOR FORWARDING TO 3GPP2, ON IMT2000 MANAGEMENT	ITU-T Q16/4 SG4	6.5	Information		POSTPONED TO NEXT MEETING (check SA WG5 response)
S3-010034	LS on Security implications of supporting "hiding"	TSG-CN1/SA2 SIP ad hoc	6.2	Discussion		POSTPONED to next meeting (or joint SA WG2 meeting)
S3-010044	Problem with no USIM-ME interface in GSM-only ME	Siemens Atea	10.1	Discussion and decision		POSTPONED TO NEXT MEETING
S3-010045	Terminology in TS 33.102/TR 31.900	Siemens Atea	10.1	Discussion and decision		POSTPONED TO NEXT MEETING
S3-010098	Response to LS on “Clarification of UMTS-AKA for GSM R’99 Mobiles” & support of UMTS AKA for GSM only R4 MEs	SA WG1	6.2	Discussion		POSTPONED TO NEXT MEETING

3GPP TSG SA WG3 Security — S3#17 **30** **Draft report version 0.0.4**

Annex C: Status of specifications under SA WG3 responsibility

Specification			Title	Editor	Rel	Comment
TS	01.31	7.0.1	Fraud Information Gathering System (FIGS); Service requirements - Stage 0	WRIGHT, Tim	R1998	#23: 5.0.0 #25: 7.0.0 (5.x.y withdrawn) #26: 7.0.1
TS	01.31	8.0.0	Fraud Information Gathering System (FIGS); Service requirements - Stage 0	WRIGHT, Tim	R1999	
TS	01.33	7.0.0	Lawful Interception requirements for GSM	MILES, David F.	R1998	#25: 7.0.0 (renumbered from 10.20)
TS	01.33	8.0.0	Lawful Interception requirements for GSM	MILES, David F.	R1999	
TS	01.61	8.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	VANNESTE, Geneviève	R1999	
TS	02.09	3.1.0	Security Aspects	GILBERT, Henri	Ph1	#6b: 3.1.0
TS	02.09	4.5.0	Security Aspects	GILBERT, Henri	Ph2	#7: 4.2.1 #12: 4.3.0 #22: 4.4.0 edito:4.4.1 #31:4.5.0
TS	02.09	5.2.0	Security Aspects	GILBERT, Henri	R1996	#20: 5.0.0 #22: 5.1.0 edito 5.1.1 #31:5.2.0
TS	02.09	6.1.0	Security Aspects	GILBERT, Henri	R1997	#27: 6.0.0 edito:6.0.1 #31:6.1.0
TS	02.09	7.1.0	Security Aspects	GILBERT, Henri	R1998	#29: 7.0.0 #31:7.1.0
TS	02.09	8.0.0	Security Aspects	GILBERT, Henri	R1999	
TS	02.31	7.1.1	Fraud Information Gathering System (FIGS) Service description - Stage 1	WRIGHT, Tim	R1998	#23: 5.0.0 #25: 7.0.0 #26: 7.1.0 (5.0.0 withdrawn)
TS	02.31	8.0.0	Fraud Information Gathering System (FIGS) Service description - Stage 1	WRIGHT, Tim	R1999	
TS	02.32	7.1.1	Immediate Service Termination (IST); Service description - Stage 1	WRIGHT, Tim	R1998	#25: 7.0.0 #26: 7.1.0
TS	02.32	8.0.0	Immediate Service Termination (IST); Service description - Stage 1	WRIGHT, Tim	R1999	
TS	02.33	7.3.0	Lawful Interception - Stage 1	MCKIBBEN, Bernie	R1998	#20: 5.0.0 #25: 7.0.0 (5.0.0 withdrawn) #27: 7.1.0 #28: 7.2.0 #29: 7.3.0
TS	02.33	8.0.0	Lawful Interception - Stage 1	MCKIBBEN, Bernie	R1999	
TS	03.20	3.0.0	Security-related Network Functions	GILBERT, Henri	Ph1-EXT	#7: 3.0.0
TS	03.20	3.3.2	Security-related Network Functions	GILBERT, Henri	Ph1	
TS	03.20	4.4.1	Security-related Network Functions	GILBERT, Henri	Ph2	#7: 4.2.1 #10: 4.3.0 #17: .3.2 #21: 4.4.0
TS	03.20	5.2.1	Security-related Network Functions	GILBERT, Henri	R1996	#20: 5.0.0 #21: 5.1.0 #23: 5.2.0 SMG#29: CRs but postponed, then forgotten!
TS	03.20	6.1.0	Security-related Network Functions	GILBERT, Henri	R1997	#25: 6.0.0 SMG#29: 6.1.0 #32:6.2.0
TS	03.20	7.3.0	Security-related Network Functions	GILBERT, Henri	R1998	#28: 7.0.0 SMG#29: 7.1.0 #30: 7.2.0 #32:7.3.0
TS	03.20	8.1.0	Security-related Network Functions	GILBERT, Henri	R1999	#32:8.1.0
TS	03.31	7.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 2	WRIGHT, Tim	R1998	#26: 7.0.0
TS	03.31	8.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 2	WRIGHT, Tim	R1999	
TS	03.33	7.1.0	Lawful Interception - stage 2	MILES, David F.	R1998	#27: for info #28: 7.0.0 #29: 7.1.0
TS	03.33	8.0.0	Lawful Interception - stage 2	MILES, David F.	R1999	
TS	03.35	7.0.0	Immediate Service Termination (IST); Stage 2	WRIGHT, Tim	R1998	#27: 7.0.0
TS	03.35	8.0.0	Immediate Service Termination (IST); Stage 2	WRIGHT, Tim	R1999	
TS	10.20	0.0.0	Lawful Interception requirements for GSM	MCKIBBEN, Bernie	R1999	
TS	21.133	3.1.0	Security Threats and Requirements	CHRISTOFFERSSON, Per	R1999	
TS	22.022	3.2.0	Personalisation of GSM ME Mobile functionality specification - Stage 1	NGUYEN NGOC, Sebastien	R1999	Transfer>TSG#4,CR at TSG#5

TS	33.102	3.6.0	Security Architecture	~~VINCK, Bart~~Blommaert, Marc	R1999	TSG#7: 3.4.0 TSG#8:3.5.0 TSG#9:3.6.0
TS	33.103	3.4.0	Security Integration Guidelines	BLANCHARD, Colin	R1999	TSG#7: 3.2.0 TSG#8:3.3.0 TSG#9:3.4.0
TS	33.105	3.5.0	Cryptographic Algorithm requirements	CHIKAZAWA, Takeshi	R1999	TSG#7: 3.3.0 TSG#8:3.4.0 TSG#9:3.5.0
TS	33.106	3.1.0	Lawful interception requirements	WILHELM, Berthold	R1999	.
TS	33.107	3.0.0	Lawful interception architecture and functions	WILHELM, Berthold	R1999	New at TSG#6 approved
TS	33.120	3.0.0	Security Objectives and Principles	WRIGHT, Tim	R1999	.
TR	33.900	1.2.0	Guide to 3G security	BROOKSON, Charles	R1999	New at TSG#6
TR	33.901	3.0.0	Criteria for cryptographic Algorithm design process	BLOM, Rolf	R1999	.
TR	33.902	3.1.0	Formal Analysis of the 3G Authentication Protocol	HORN, Guenther	R1999	
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	WALKER, Michael	R1999	TSG#7: S3-000105=NP-000049 TSG#7 SP-000039
TR	33.909	3.0.0	ETSI SAGE 3GPP Standards Algorithms Task Force: Report on the evaluation of 3GPP standard confidentiality and integrity algorithms	WALKER, Michael	R1999	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	WALKER, Michael	R1999	ex SAGE - not publicly available; supplied by ETSI under licence TSG#7: 3.1.0 ex SAGE 3.1.0
TS	35.202	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	WALKER, Michael	R1999	ex SAGE - not publicly available; supplied by ETSI under licence TSG#7: 3.1.0 ex SAGE 3.1.0
TS	35.203	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	WALKER, Michael	R1999	ex SAGE - not publicly available; supplied by ETSI under licence TSG#7: 3.1.0 ex SAGE 3.1.0
TS	35.204	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	WALKER, Michael	R1999	ex SAGE - not publicly available; supplied by ETSI under licence TSG#7: 3.1.0 ex SAGE 3.1.0
TS	41.031	0.0.0	Fraud Information Gathering System (FIGS); Service requirements - Stage 0	WRIGHT, Tim	Rel-4	
TS	41.033	0.0.0	Lawful Interception requirements for GSM	MILES, David F.	Rel-4	
TS	41.061	0.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	..,	Rel-4	
TS	42.009	0.0.0	Security Aspects	GILBERT, Henri	Rel-4	
TS	42.031	0.0.0	Fraud Information Gathering System (FIGS) Service description - Stage 1	WRIGHT, Tim	Rel-4	
TS	42.032	0.0.0	Immediate Service Termination (IST); Service description - Stage 1	WRIGHT, Tim	Rel-4	
TS	42.033	0.0.0	Lawful Interception - Stage 1	MILES, David F.	Rel-4	
TS	43.020	0.0.0	Security-related Network Functions	GILBERT, Henri	Rel-4	#32:8.1.0
TS	43.031	0.0.0	Fraud Information Gathering System (FIGS); Service description; Stage 2	WRIGHT, Tim	Rel-4	
TS	43.033	0.0.0	Lawful Interception - stage 2	MILES, David F.	Rel-4	
TS	43.035	0.0.0	Immediate Service Termination (IST); Stage 2	WRIGHT, Tim	Rel-4	
TS	50.020	0.0.0	Lawful Interception requirements for GSM	..,	Rel-4	

3GPP TSG SA WG3 Security — S3#17 **32** **Draft report version 0.0.4**

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

Note: SA WG3 agreed CRs to be presented to TSG SA#11 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WG status	Acronym	Remarks
03.35	001		R99	IST implementation for non-CAMEL subscribers	F	8.0.0	S3-17	S3-010049	agreed	IST	Late approval (CN#5 approved corresponding CRs in CN)
33.102	135		R99	RES has to be a multiple of 8 bits	F	3.7.0	S3-17	S3-010006	agreed	Security	To be sent to TR-45.
33.102	136		R99	Add bit ordering convention	F	3.7.0	S3-17	S3-010064	agreed	Security	To be sent to TR-45.
33.102	137		R99	Timing of security mode procedure	F	3.7.0	S3-17	S3-010094	agreed	Security	S3 TD has incorrect CR number - corrected for SA submission
33.102	138		Rel-4	Add requesting node type to authentication data request	C	3.7.0	S3-17	S3-010103	agreed	SEC1	To be sent to TR-45.
33.102	139		Rel-4	Additional Parameters in Authentication Failure Report	C	3.7.0	S3-17	S3-010104	agreed	SEC1-FIGS	To be sent to TR-45.
33.102	140		R99	Correction to the handling of re-transmitted authentication request messages on the ME	F	3.7.0	S3-17	S3-010124	agreed	Security	To be sent to TR-45.
33.102	141		R99	Optional Support for USIM-ME interface for GSM-Only ME	F	3.7.0	S3-17	S3-010126	agreed	Security	
33.102	142	1	R99	Definition corrections	F	3.7.0	S3-17	S3-010138	agreed	Security	
33.102	143		R99	GSM ciphering capability Handling in Security Mode set up procedure	F	3.7.0	S3-17	S3-010117	agreed	Security	
33.103	013		R99	Add bit ordering convention	F	3.4.0	S3-17	S3-010065	agreed	Security	
33.105	016		R99	Add bit ordering convention	F	3.6.0	S3-17	S3-010066	agreed	Security	
33.105	017		R99	RES has to be a multiple of 8 bits	F	3.6.0	S3-17	S3-010048	agreed	Security	To be sent to TR-45.
33.105	018		R99	Minimum clock frequency updated	F	3.6.0	S3-17	S3-010111	agreed	Security	Alignment with T WG3 request
33.106	002		Rel-4	Update of TS 33.106 for release 4	B	3.1.0	S3-17	S3-010060	agreed	CSSPLIT	
33.106	003		Rel-5	Release 5 updates	B	3.1.0	S3-17	S3-010107	agreed	CSSPLIT	
33.107	002		R99	Correction of Location information parameters in interception event records	F	3.1.0	S3-17	S3-010062	agreed	Security	

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD Number	Title	Source	Comment
S3-010005	LS from T WG2: IM Subsystem Address Storage on USIM	T WG2	Noted
S3-010007	LS from T WG3: Minimum clock frequency indication	T WG3	Noted. Nokia prepared CR in TD111
S3-010008	LS from TSG GERAN: UPDATED INFORMATION ON CIPHERING OF RRLP MESSAGES BETWEEN SMLC AND MS IN GPRS	TSG GERAN	Discussed and Noted
S3-010009	LS from CN WG1: UE Triggered Authentication and Key Agreement During Connections	CN WG1	Dealt with TD53, - WI to be deleted
S3-010010	Reply LS to SA WG2 for "IM Subsystem Address Storage on USIM"	CN WG1	Noted
S3-010011	Response LS from CN WG4 on SA3 agreements on MAPSec	CN WG4	To be dealt with at NDS ad-hoc
S3-010012	LS from T WG3: TR 31.900 - SIM/USIM Internal and External Interworking Aspects	T WG3	Response in TD99
S3-010013	LS from T WG3: Introduction of Operator PLMN Name List for 3G Rel-4	T WG3	Noted
S3-010016	Response to LS (T2-000793) on discussion document on UE functionality split over physical devices	SA WG2	Response in TD133
S3-010017	Response to: LS on some issues related to optimised IP speech support in GERAN	SA WG2	Response LS to be created ?
S3-010018	LS on Replacement of 23.121 for R4 onwards	Lucent (TSG-SA WG2)	Check if Rel4 or Rel5. Noted. Editors to check references to 23.121 in their specs.
S3-010019	LS on authentication test algorithm to be implemented in test USIM	T WG1	Reply LS in TD137
S3-010020	Elaboration of KEY IDENTIFICATION EVENT	T WG3 Chairman	SA WG1 response in TD32. SA WG3 response in TD128
S3-010021	Proposed Reply LS on the Work Item “Cx Interface specification”	SA WG2	Noted
S3-010022	Proposed Reply LS on “Proposal not to use the IMSI as the identity of an IM subscriber	SA WG2	Response LS in TD115
S3-010023	Response on LS regarding security aspects of UE conformance testing	T WG1	Noted
S3-010025	LIASON TO ETSI, FOR FORWARDING TO 3GPP, AND COMMUNICATIONS TO TIA TR-45.7, FOR FORWARDING TO 3GPP2, ON IMT2000 MANAGEMENT	ITU-T Q16/4 SG4	POSTPONED TO NEXT MEETING (check SA WG5 response)
S3-010030	LS from SA WG1: Convergence of QoS approaches in 3GPP and TIPHON	SA WG1	Intended for TSG SA - Noted.
S3-010031	LS from SA WG1: UE functionality split	SA WG1	Response in TD133
S3-010032	Response to LS (T3-010xxx) from T3 chairman on the Elaboration of KEY IDENTIFICATION EVENT	SA WG1	Noted. SA WG3 response in TD128
S3-010033	Requirement for End-to-End Encryption of IP Multimedia Subsystem Controlled Voice over IP Calls	SA WG1	P Howard to develop response and approve by e-mail
S3-010034	LS on Security implications of supporting "hiding"	TSG-CN1/SA2 SIP ad hoc	POSTPONED to next meeting (or joint SA WG2 meeting)
S3-010035	LS on integrity protection for GERAN	TSG GERAN ad hoc #4	Agreed for transmission by GERAN Chairman. Response in TD129

3GPP TSG SA WG3 Security — S3#17 **34** **Draft report version 0.0.4**

TD Number	Title	Source	Comment
S3-010036	LS on "IM User Identities"	TSG-CN1-TSG-SA2 SIP AD-Hoc	(SA WG2 response in S2-010757). To be handled in IMS ad-hoc
S3-010037	LS reply to SA3 on request for information to complete security work items	CN WG4	Noted
S3-010038	LS Response Lawful Intercept support on the Mc interface	CN WG4	M Pope to forward to LI group
S3-010039	LS on Checking the integrity of UE security capabilities	RAN WG2	Response CR & LS in TD117, TD118 (see also TD70)
S3-010041	Removal of Visited Control S-CSCF option from the Rel 5 architecture	SA WG2	Noted
S3-010043	LS on MExE and Security Collaboration	T WG2	WI supporting companies to support the security aspects
S3-010098	Response to LS on “Clarification of UMTS-AKA for GSM R’99 Mobiles” & support of UMTS AKA for GSM only R4 MEs	SA WG1	POSTPONED TO NEXT MEETING
S3-010122	TR 31.900 - SIM/USIM Internal and External Interworking Aspects	T WG3	Response to TD99. V. Niemi to draft response LS for e-mail approval
S3-010125	LS from CN WG1: Re-transmission of authentication requests	CN WG1	Attachment CR missing (provided after meeting in TD134). Response in TD124

E.2 Liaisons from the meeting

TD Number	Title	Status	To CC
S3-010099	LS to T3: TR 31.900 - SIM/USIM Internal and External Interworking Aspects (update of TD42)	Approved	**T3, N1, T2** S1
S3-010106	LS to CN WG4 on Move of TS 33.200 - Network Domain Security from Rel-4 to Rel-5	Approved	**N4**
S3-010110	LS to CN4 on Additional Parameters in AFR procedure	Approved	**N4**
S3-010137	LS to T WG1 on testing UE procedures	Approved	**T1** T3
S3-010115	Response LS (to TD22) on multiple user identities	Approved	**S2**
S3-010128	Response to LS (S1-010200) to T3 and S1 on the Elaboration of KEY IDENTIFICATION EVENT	Approved	**S1, T3**
S3-010131	LS to TR-45: Clarification on positive authentication report	Approved	**TR-45 AHAG** TR45.2, N4
S3-010132	LS to TR45 AHAG: Define responsibility and procedure	Approved	**TR-45 AHAG**
S3-010133	LS to SA WG1 on UE functionality split over physical devices	Approved	**T2, S1, S2** SA, T, T3, N1
S3-010135	Reply to LS on integrity protection for GERAN (Response to TD22)	Approved	**GERAN ad-hoc** GERAN
S3-010136	LS to TSG RAN on UE ciphering capabilities	Approved	**RAN** RAN2, SA

Annex F: List of actions from the meeting

AP 17/01: **M Pope to check if the KASUMI Evaluation report has been published as a TR, and to report the status of the SDO agreements to the SA WG3 e-mail list.**

AP 17/02: **M Pope to take the request from the WAP Forum for use of KASUMI (TD S3-010003) to the ETSI Lawyer for processing as appropriate.**

AP 17/03: **V. Niemi to convene a group to produce a LS to GERAN on the GERAN LCS ciphering issue, to be approved by e-mail.**

AP 17/04: **M Pope to forward the LS in TD S3-010038 to the LI Group for action. The LI group to responsd to CN WG4 and to inform SA Plenary as appropriate.**

3GPP TSG SA WG3 Security — S3#17 **37** **Draft report version 0.0.4**

Annex G: SA WG3 Work Plan

Revision marks are used to show the changes agreed at this meeting.

WI ID	WG	Rel	Split	WI Name	Acronym	Appr Level	Start	End	% comp	WG Appd	TSG Appd	WI Description	Notes	Rapporteur	Action S3 (S3#1
1273	SA1	Rel5	No	**Provisioning of IP-based multimedia services**	IMS	TSG	Mon 21/02/00	Thu 16/05/02	11%	Yes	Yes	SP-000216	S1 WI proposed S1-000290...	Mark Cataldo, Motorola	
1298	SA3		No	**Access Security for IP-~~multimedia~~ based services**	IMS-ASEC	TSG	Mon 04/09/00	Fri 22/06/01	0%	Yes	Yes	SP-000420	"end March 2001 from tdoc AHR00-0031. 14/09/00: End date modified to 29 June 2001 (was 03/01). TR created 08/00; TR approval 12/00; TS draft 03/01 (distribution to other groups); TS approval 06/01"	Krister Boman, Ericsson	
1299	SA3		No	**Lawful interception**	IMS-LI	TSG	Mon 04/09/00	Thu 29/03/01	10%	No	Yes	SP-000309	end March 2001 from tdoc AHR00-0031	Berthold Wilhelm, Reg TP	
1322	SA2	Rel4	No	**Enable bearer independent CS architecture**	CSSPLIT	TSG	Mon 03/01/00	Fri 15/03/02	42%	Yes	Yes	SP-000288		Alexander Milinski, Siemens	
1331	SA3		No	**Lawful interception**	CSSPLIT		Mon 21/08/00	Fri 23/03/01	0%	No	No		Requirements capture: S3#14 (Aug 00), Feature specification: S3#15 (Sep 00), Definition of architecture		

3GPP TSG SA WG3 Security — S3#17 **38** **Draft report version 0.0.4**

WI ID	WG	Rel	Split	WI Name	Acronym	Appr Level	Start	End	% comp	WG Appd	TSG Appd	WI Description	Notes	Rapporteur	Action S3 (S3#1
1637	SA1	NA	Yes	**OSA enhancements**	OSA1	WG	Mon 03/01/00	Fri 10/08/01	20%	No	No	SP-000216		Jörg Swetina, SIEMENS AG	
1419	SA3	Rel5	No	**OSA security (!)**	OSA1-SEC	TSG	Mon 03/01/00	Fri 10/08/01	0%	Yes	Yes	SP-000302	Christophe to contact BT and Ericsonn in S3 and S1	Colin Blanchard, BT	Revise be re reflect timesc
1421	SA3		No	Stage 3	OSA1-SEC		Mon 23/10/00	Fri 10/08/01	0%	No	No		Presentation to S3 of trust and security management framework service capability feature: S3#14, Aug, Presentation to S3 of threats and countermeasure analysis: S3#15, Sep , Decision if implementation is to be standardised and how much re-use can be made S3#17: No progress in S3 – seems to be behind schedule.		
1423	SA3		No	(possibly) changes required from supporting platforms, e.g. gsmSCF, HLR	OSA1-SEC		Mon 11/09/00	Thu 14/12/00	0%	No	No				
1445	T2	NA	Yes	**MExE enhancements**	MEXE1	TSG	Mon 03/01/00	Fri 15/12/00	53%	Yes	Yes	TP-000117			

WI ID	WG	Rel	Split	WI Name	Acronym	Appr Level	Start	End	% comp	WG Appd	TSG Appd	WI Description	Notes	Rapporteur	Action S3 (S3#1
1447	SA3	Rel4	No	**MExE Security**	MEXE1-SEC	TSG	Tue 22/02/00	Fri 15/12/00	63%	Yes	Yes		Presentation to S3 of R00 MExE: S3#14, Aug, Email discussion on threats and countermeasures, Aug, Threats and countermeasures analysis: MExE Aug, Presentation to S3 of threats and countermeasures analysis: S3#15, Sept, Feature specification: S3#16,	Colin Blanchard, BT	End da be al MExE analysi 010296
2045	SA3		No	Stage 3	MEXE1-SEC		Mon 17/07/00	Fri 15/12/00	0%	No	No				
1541	CN4	Rel4	No	**Transcoder-Free Operation**	TrFO		Mon 03/01/00	Fri 30/03/01	78%	No	No		Lead given to CN4 from CN...		
112	CN4		No	**OoBTC solution**	TRFO-OOBTC	WG	Mon 03/01/00	Fri 30/03/01	89%	Yes	No	N4-000531		Tosshiyuki Tamura, NEC	
1617	SA3		No	Prevention of user fraud	TRFO-OOBTC		Mon 21/08/00	Fri 30/03/01	100%	No	No		S3 awaiting liaison on any security issues from N4. N4 replied to S3#17 that they had not identified any issues. WI considered to be complete.		
1536	SA2	NA	Yes	**Location Services enhancements**	LCS1	TSG	Mon 03/04/00	Fri 29/11/02	16%	No	No	SP-000292		Jan Kall, Nokia	

3GPP TSG SA WG3 Security — S3#17 **40** **Draft report version 0.0.4**

WI ID	WG	Rel	Split	WI Name	Acronym	Appr Level	Start	End	% comp	WG Appd	TSG Appd	WI Description	Notes	Rapporteur	Action S3 (S3#1
521	SA3		No	**New security aspects of LCS (not identified)**	LCS1-SEC		Fri 14/04/00	Fri 28/12/01	~~0~~15%	No	No	SP-000421	"to be more detailed: evaluate possible impact of new LCS features on security, Evaluate privacy options in call related LCS for specific Client, separate for MT and MO LR; 14/09/00: End date 28/12/01 WI may need to be split to improve on this date."	Valtteri Niemi, Nokia	
1542	SA2	Rel4	No	**Ensure reliable QoS for PS domain (Master)**	QoSPS		Mon 03/01/00	Thu 21/06/01	21%	No	No		as a result propose QoS negotiation and reservation mechanisms to be used in UMTS		
1624	SA3		No	**Security aspects**			Fri 02/06/00	Fri 29/12/00	0%	No	No		14/09/00: End date modified to end December 00. S3 awaiting liaison on any security issues from S2 Still awaiting input at S3#17, Feb 01		
1800	T3	NA	Yes	**(U)SIM toolkit enhancements**	USAT1		Mon 05/06/00	Fri 28/09/01	28%	No	No	not needed			
2100	SA3		No	**USIM Toolkit security**	USAT1-API-MULTOS	TSG	Wed 18/10/00	Fri 30/03/01	0%	No	Yes	SP-000421	Approved at TSG SA #09	Peter Howard, Vodafone	

WI ID	WG	Rel	Split	WI Name	Acronym	Appr Level	Start	End	% comp	WG Appd	TSG Appd	WI Description	Notes	Rapporteur	Action S3 (S3#1
1571	SA3	NA	No	**Security enhancements**	SEC1	TSG	Mon 03/01/00	Fri 28/09/01	24%	No	Yes	SP-000421	Added BB UE authentication and rapporteur added	Peter Howard, Vodafone	
~~2099~~	~~SA3~~	~~Rel4~~	~~No~~	~~**UE triggered authentication during connections**~~	~~SEC1-UETADC~~	~~TSG~~	~~Tue 14/03/00~~	~~Tue 14/03/00~~	~~0%~~	~~Yes~~	~~Yes~~	~~SP-000421~~	~~Approved TSG SA #09~~DELETED S3#17 (no supporting companies)	~~Peter Howard, Vodafone~~	
1587	SA3	Rel4	No	**Evolution of GSM CS algorithms (e.g. A5/3 development and deployment)**	SEC1-CSALGO1	TSG	Mon 03/01/00	Mon 15/01/01	34%	Yes	Yes	SP-000306	Reqts capture: S3#14, Aug, Security feature specification: S3#16, Nov, Feasibility study, Jan 01, CRs on def of sec archi, May 01, Integration of sec archi, Feb 01, Complete CRs with S3 review, Apr 01, CRs to be approved at TSG, May 01 S3#17: No supporting companies or rapporteur.	?	Need n reflect S3#17. include and CS
1588	SA3	Rel4	No	**Evolution of GSM PS algorithms (e.g. GEA 2 deployment)**	SEC1-PSALGO1	TSG	Tue 22/02/00	Fri 22/12/00	73%	Yes	Yes	SP-000307	Complete TSG#09 (09/2000) No supporting companies or rapporteur.	?	Need n reflect S3#17. include and CS

3GPP TSG SA WG3 Security — S3#17 **42** **Draft report version 0.0.4**

WI ID	WG	Rel	Split	WI Name	Acronym	Appr Level	Start	End	% comp	WG Appd	TSG Appd	WI Description	Notes	Rapporteur	Action S3 (S3#1
1589	SA3		No	Main aspects	SEC1-PSALGO1		Tue 22/02/00	Fri 24/11/00	28%	No	No		Final decision on whether GEAx support is optional also for R97: CN#8, Jun , CRs on definition of security architecture, Jun, Integration of security architecture, Aug, Complete CRs, Sep, CRs approved at TSG level, Sep. Complete TSG#09 (09/2000)		Propos is dele done a
1572	SA3	Rel5	Yes	**Protection for user plane data**	SEC1-PUPD	TSG	Mon 14/02/00	Fri 22/06/01	0%	Yes	Yes	SP-000298		Stuart Ward, Orange	Is any to hap within timefra
1573	SA3		No	Integrity protection in access network	SEC1-PUPD		Mon 14/02/00	Fri 22/06/01	0%	No	No		Requirements capture: S3#14, Aug, Security feature specification: S3#15, Sep , Feasibility study, Jan 01, Definition of security architecture, CRs approved at TSG level, Mar 01, Integration of security architecture , Concept presented to CN, RAN, T, GERAN		

WI ID	WG	Rel	Split	WI Name	Acronym	Appr Level	Start	End	% comp	WG Appd	TSG Appd	WI Description	Notes	Rapporteur	Action S3 (S3#1
1575	SA3		No	Network based end-to-end security	SEC1-PUPDNBE2E		Mon 14/02/00 Fri 02/03/01	Fri 22/06/01 Fri 28/12/01	0%	NoYes	No	S3-010123	Req capture, S3#14 Aug, Sec feature specification, S3#16, Nov, Feasibility study, S3, Jan 01, Def of sec archi, CRs approved at TSG, Mar 01, Integration of security architecture , Apr 01, CRs, Oct 01, CRs approved at TSG, Dec 01 S3#17: Replace with new WID in S3-010123. To be approved at SA#11. S3#17, Feb, Approval of WI; S3#19, May, Feasibility study and definition of security architecture; Dec, specifications approved at TSG level.	Peter Howard, Vodafone	
1576	SA3		Yes	**Network domain security**	SEC1-NDS	TSG	Mon 21/02/00	Fri 28/09/01	29%	Yes	Yes	SP-000420	"GTP security due R4 (12/00); rest R5 (06/01)" S3#17: All due in Rel-5	Geir M. Køien, Telenor	WID to and timesc added.
1577	SA3	Rel5	No	Control plane protection in core network (e.g., GTP, CAP, MAP/IP, provided by IPsec)	SEC1-NDS		Mon 21/02/00	Thu 21/06/01	35%	No	No				

WI ID	WG	Rel	Split	WI Name	Acronym	Appr Level	Start	End	% comp	WG Appd	TSG Appd	WI Description	Notes	Rapporteur	Action S3 (S3#1
1578	SA3		No	Main aspects	SEC1-NDS		Fri 12/05/00	Thu 21/06/01	0%	No	No		Specif of protocol stacks for CN interfaces, Aug, Req capture, S3#14, Aug , Def of GTP sig security archi, CRs, S3#15 Sep , Security feature specification, S3#15, Sep , Def of sec archi, Mar 01, Integration of sec archi Feb 01, CRs approved at TSG Jun 01		
1580	SA3	Rel5	No	User plane protection in core network (e.g., provided by IPsec)	SEC1-NDS		Mon 21/02/00	Thu 21/06/01	35%	No	No		S3#17: Not started.		
1581	SA3		No	Main aspects	SEC1-NDS		Mon 21/02/00	Thu 21/06/01	7%	No	No				
2098	SA3		No	Study of network-based denial of service	SEC1-NDS	TSG	Thu 14/09/00	Fri 28/09/01	0%	No	Yes	SP-000421	Approved TSG SA#09	~~Peter Howard, Vodafone~~Rong Shi and Dan Brown, Motorola	
1583	SA3	~~Rel4~~ Rel5	No	**MAP application layer security**	SEC1-MAPAL	TSG	Tue 22/02/00	~~Fri 24/11/00~~ Fri 21/09/01	65%	Yes	Yes				WID to and timesc added.

WI ID	WG	Rel	Split	WI Name	Acronym	Appr Level	Start	End	% comp	WG Appd	TSG Appd	WI Description	Notes	Rapporteur	Action S3 (S3#1
1584	SA3		No	Main aspects	SEC1-MAPAL	WG	Tue 22/02/00	~~Fri 24/11/00~~ Fri 21/09/01	0%	Yes	No		Integration of security architecture ,Jun, CRs approved at TSG level, Jun , Definition of security architecture, CRs approved at TSG level Sep		
1586	SA3		No	**Key management for core network security**	SEC1-KMCN	TSG	Mon 03/01/00	Fri 22/06/01	0%	Yes	Yes	SP-000301	Work on MAP based key management, Jun , Decision to specify or not MAP based solution: S3#14, Aug , Decide on dates for an IP/IKE based solution: S3#14, Aug, CRs on MAP based solution (if OK), Jun 01	Peter Howard, Vodafone	WID to and timesc added.
1594	SA3	~~Rel4~~ Rel5	No	**Visibility and Configurability of security**	SEC1-VCS	TSG	Mon 03/01/00	Tue 05/12/00	0%	Yes	Yes	SP-000305	Requirements capture, Aug , Definition of security architecture, CRs approved at TSG level, Dec S3#17: Behind schedule. Action at S3#18. Release to be determined	Sébastien Nguyen Ngoc, France Telecom	WID to and timesc added remove
1595	SA3	Rel5	No	**FIGS**	SEC1-FIGS		Mon 03/01/00	Fri 22/06/01	0%	No	No		14/9/00: work behind schedule - WID modification agreed at SA#10	SP-000628	

3GPP TSG SA WG3 Security — S3#17 **46** **Draft report version 0.0.4**

WI ID	WG	Rel	Split	WI Name	Acronym	Appr Level	Start	End	% comp	WG Appd	TSG Appd	WI Description	Notes	Rapporteur	Action S3 (S3#1
~~1612~~	~~SA3~~	~~?~~	~~No~~	~~**General security issues**~~		~~TSG~~	~~Mon 03/01/00~~	~~Fri 30/03/01~~	~~0%~~	~~Yes~~	~~Yes~~	~~SP-000310~~	~~to be deleted since it should be replaced by new work items at SA#9 (home control and MS triggered authentication)~~	~~Peter Howard, Vodafone~~	
2026	SA3	~~?~~ Rel-6	No	**Enhanced HE control of security (including positive authentication reporting)**			Mon 03/01/00	~~Wed 03/01/01~~ Fri 14/06/02	0%	No	No	SP-000421	Added by P-000575 without any dates. 18/10/00: Change of WI title, added hyperlink rapporteur new end date 03/01 New end date and correct Release to be decided at S3#18	Peter Howard, Vodafone	WID to and timesc added.
2027	SA3		No	Stage 2			Wed 03/01/01	~~Wed 03/01/01~~ Fri 14/06/02	0%	No	No		New end date and correct Release to be decided at S3#18		WID to and timesc added.