Technical Specification Group Services and System Aspects
Meeting #10, Bangkok, Thailand, 11-14 December 2000

TSGS#10(00)0621

Source:	**SA WG3 Secretary**
Title:	**Reports of SA WG3 meetings held since SA#09**
Document for:	**Information**
Agenda Item:	**7.3.1**

Attached are the SA WG3 meeting reports for the **ad-hoc** meeting (called #15bis) and SA WG3 Plenary meeting #16, held since SA#09.

3GPP TSG SA WG3 Security — S3#15bis ad-hoc

Ad-Hoc meeting 08-09 November, 2000

Munich, Germany

Source: **Secretary 3GPP TSG-SA WG3**

Title: **Report version 1.0.0**

Status: **Approved**

Contents

1 Opening of the meeting

The Chairman, Michael Michovici, welcomed delegates to the SA WG3 ad hoc meeting, in Munich, Germany, hosted by Siemens. Mr. G. Horn (Siemens) welcomed delegates to Munich and provided the domestic arrangements for the meeting.

2 Meeting objectives

The Chairman outlined the objectives, which were to discuss IM Subsystem Security, network domain security and some critical Release 2000 items (limited in time to 1 hour), including GPRS work.

3 Approval of the agenda

The draft agenda, provided in TD S3z000003 was approved without changes.

4 Registration and assignment of input documents

The available documents were allocated to their respective agenda items.

4.1 General Discussion (Limited to 1 hr Wednesday)

TD S3z000011: Draft LS on Integrity Protection in GERAN. This LS from GERAN on options for integrity protection of signalling messages was presented by P. Howard, and the proposed response in TD S3z000024 was considered.

TD S3z000024: Proposed Reply LS on GERAN integrity protection. This proposed reponse to GERAN recommended that the reduction of MAC length to <32 bits was not in line with the recommendations from ETSI SAGE, and that 32 bits was considered the minimum protection needed. It also did not recommend the ability to switch on and off the protection due to the potential delay to the GERAN work in developing a secure mechanism to do this. Thirdly, it stated that the protection in GERAN should be at least equivalent to that in UTRAN and therefore the MAC protection was required. The proposal was modified slightly and agreed in TD S3z000032.

TD S3z000012: Integrity-protection for GERAN-signalling. This proposal for the protection of GERAN messages using a MAC which could be varied in length depending upon the space left in the message for the MAC bits was considered. It was commented and generally agreed that reduction in security requirements should only be made on explicit request for technical reasons, and not proposed by SA WG3, and that GERAN should be asked to identify exactly which messages would need a reduced MAC length for reasons of efficiency, so that SA WG3 could consider mechanisms. This information was included in the LS to GERAN in TD S3z000032.

TD S3z000030: Proposed Reply LS to "Protection of GTP Messages using IPSec". This liaison was considered along with TD S3z000004: LS from CN WG4 on Protection of GTP Messages using IPSec, and was discussed and agreed (with minor modifications) in TD S3z000033. (TD S3z000004 was noted).

TD S3z0000026: Liaison Statementfrom GERAN regarding ciphering of RRLP messages between the SMLC and MS in GPRS. This LS on LCS was not discussed in the meeting, but was forwarded to the SA WG3 meeting #16 for consideration.

4.2 IM subsystem security

TD S3z000028 and TD S3z000029. These contributions contained TS 23.228 version 1.0.0, with and without revision marks, and were provided for information for the discussions below and were noted. It was also noted that version 1.2.0 now exists.

TD S3z000010: Authentication and protection mechanisms for IM CN SS. This was presented by Ericsson, followed by the presentation of TD S3z000022: IMS authentication and integrity/confidentiality protection, by Siemens, using the slides provided in TD S3z000035. The Ericsson contribution proposed a method of providing Integrity and Confidentiality mechanisms in different Network Elements. The Siemens presentation suggested some disadvantages of this method and proposed a method where the mechanisms are co-located in a single NE, avoiding the disadvantages of the Ericsson proposal.

A discussion of both contributions followed and the different approaches were identified as being due to different interpretations of SA WG2 TS 23.228 definition of the proxy CSCF funtionality. It was agreed that a liaison to SA WG2 was needed on this for clarification and further discussion in SA WG3. The Ericsson contribution also pointed out the need for liaison to SA WG2 on the use of IMSI for user identity. It was agreed that this should be done for approval at SA WG3 meeting #16.

ACTION AH01: Ericsson to draft an LS to SA WG2 on clarification of the proxy CSCF function and to consider the need for a LS on the use of IMSI for user identity, for discussion and approval at SA WG3 meeting #16.

The need to specify the requirements for “Trust“ for the visited network, etc. was also identified, before any of the detail of the mechanisms could be discussed. AT&T Wireless agreed to send relevant draft RFCs on Trust Management to SA WG3 for information, and to contribute these to the SA WG3 meeting #16, along with a short presentation on Trust Management (15 minutes).

ACTION AH02: AT&T Wireless to provide RFCs on Trust Mamagement to SA WG3 and provide a short presentation at SA WG3 meeting #16.

TD S3z000027: S-CSCF issues and security in IM CN SS. This contribution suggested that SA WG3 should urgently look at the SA WG2 security architecture work, which has developed with little involvement of SA WG3. It was agreed that SA WG3 delegates should analyse the architecture work and provide contribution to SA WG3 meeting #16 in order to provide an agreed position to SA WG2 on any identified problems.

TD S3z000037: Some notes on 3GPP TSG CN1 SIP #1 meeting. This contribution requested that SA WG3 views are provided to CN WG1 and SA WG2 on many issues identified at the meeting. It was agreed that these issues should be the subject to contribution to SA WG3 meeting #16. The following general principles were agreed, for contributions:

- Minimise the trust needed between 2 parties.
- Minimise the number of entities which have trust
- Scalability of trust
- Trust models in the new architecture
- Degrees of trust
- Whether the home network can devolve trust
- Regulate “transitivity“ of trust
- Formulate trust in terms of risk assessment
- Performance issues
- Lawful Interception issues
- Access independence issues
- “Fate sharing“ – each entity has most to lose by exposing its’ own secret information.

ACTION AH03: C Brookson to e-mail a list of trust issues for discussion before SA WG3 meeting #16.

TD S3z000008. TR 33.8xx v0.2.0: Principles of Access security for IP-based services. This was provided by Telenor for information and was noted. This draft TR will be updated by the editor taking into account the results of discussions at this meeting.

TD S3z000009. TS 33.xxx v0.1.0: Access security for IP-based services. This was a skeleton (ToC) awaiting inclusion of some agreed material from TR 33.8xx (TD S3z000008). It was provided for information and noted.

TD S3z000023. Comments on 3G TR 33.8xx and 3G TR 33.800. These comments were discussed and the editor agreed to include comments in the drafts. It was noted that these documents are Release 5, but early completion is desirable in order to allow the stage 3 to be developed in good time.

4.3 Network Domain Security

TD S3z000007: TR 33.800 v0.2.4: Principles for Network Domain Security. This TR was provided for information. And noted. It will be updated by the Rapporteur (Mr. G. Koien) with the agreed contributions from this meeting and presented to SA WG3 #16 (see below).

TD S3z000013. General Structure of Secure MAP Operations. This contribution was introduced by Ericsson and discussed. It was questioned whether the Protection Mode 0 is still relevant, when it provides no security enhancement, and the newly proposed Security Protection Profiles (PPs) – see TD S3z000014. Some concerns were expressed over the order of the messages to be protected by the MAC functions. It was agreed that these concerns should be further investigated and a cross check with TS 29.002 should be performed, and contributions made to SA WG3 meeting #16. CN WG4 also needed to be asked about the policy on message protection in the Core Network and the value of the implementation of Protection Mode 0, with respect to signalling load.

Ericsson agreed to draft a liaison statement to CN WG4 for discussion and approval by the SA WG3 meeting #16.

TD S3z000014: Protection Profiles for MAP Security. This contribution proposed the introduction of a set of Protection Profiles, and provided some example profiles showing which mesages to be protected under different PPs. The examples were based upon the MAP messages to be protected as identified by SA WG3 previously. It was considered that further analysis of the message protection requirements was needed. Comments to this contribution were also provided in TD S3z000031.

TD S3z000031: Comment to S3z000014. This included an embedded document showing proposed revisions to TD S3z000014 and suggests that “Fallback“ should be against the Protection Profile, and not the Security Association. It was also considered that negotiation mechanism would need to be defined to deal with changing PPs until an acceptable PP is agreed, which could endanger the timescales for Rel4 MAP Security.

TD S3z000015: Structure of Security Header. Some discussion over the inclusion of the original Component Identifier occurred, as this could be more properly included in the SPI, as it is not a Security item. It was agreed that this should be questioned on a contribution basis to SA WG3 and CN WG4.

TD S3z000016: Refinement of MAP Security Association. This contribution was introduced and discussed. It was commented that the definition of the SA lifetime should be made more precise, and described as an expiry time rather than a duration. It was also commented that the MAP Protection Profiles would be agreed in general between Operators, rather than sent as SA parameters. It was finally agreed to include this in the TR, and contributions were invited for the SA WG3 meeting #16.

TD S3z000017. Replay Protection for MAP Security. It was suggested that slowly-changing IVs could be a security weakness. This was discussed, and it was requested that a paper with supporting information on this suggestion should be contributed to the next SA WG3 meeting #16 for consideration.

TD S3z000018: MAP Security Domain of Interpretation for ISAKMP. This IETF draft RFC was provided for information. Delegates were asked to consider the document and provide detailed comments to the IETF. The document was then noted.

TD S3z000021: SA negotiation protocol for the ZA interface. This contribution was introduced using presentation slides, provided in TD S3z000034. It detailed suggested problems with the use of IKE for SA negotiation using KACs. After some discussion and explanation, it was considered that this requires serious consideration, and urgent contributions should be made to SA WG3 meeting #16 to come to a decision on the use of IKE for this.

TD S3z000019: Introduction of MAP security. This contribution requested the mandatory support of MAP Security after a cut-off date to be specified. This would cause much debate for operators and manufacturers to comply with the cut-off date and after discussion it was agreed that Operators and Manufacturers should be consulted. Mr. C. Brookson undertook to contribute this to the GSMA to get their reaction and to look for a suitable cut-off date which can be complied with.

ACTION AH01: C. Brookson to take the question of a cut-off date for Mandatory Support of MAP Security to the GSM Association at their next meeting and report back to SA WG3.

TD S3z000020: Modification of MAP security header. This contribution outlined the request from CN WG4 for clarification from SA WG3 on the definition of the MAP Security header. Ericsson agreed to

produce a proposed liaison statement to CN WG4 for consideration at SA WG3 meeting #16. (Other items were later included in this draft LS).

ACTION AH02: Ericsson to produce a draft LS to CN WG4 for consideration at SA WG3 meeting #16. LS to include MAP Security Header information (S3z000020),

TD S3z000007: TR 33.800 v0.2.4: Principles for Network Domain Security. The open issues detailed in this TR were introduced by the Editor, as background for discussion of TDs S3z000023, S3z000002 and S3z000025.

In addition, it was noted that Lawful Interception part had no material. It was requested that the SA WG3 LI group consider appropriate input under this item. Mr. B. Wilhelm agreed to ask SA WG3 LI group for this at their next meeting.

ACTION AH03: B. Wilhelm to ask SA WG3 LI group for input to TR 33.800 on relevant LI issues at their November 2000 meeting.

It was also noted that the Definitions, abbreviations should be contributed to the 3GPP Vocabulary document (TR 21.905). It was agreed to replace the content of Clause 4 with references to the relevant information, instead of duplicating the text in the TR. It was further noted that the Ga interface (charging information) had not been standardised so that the feasibility of protecting this interface in a standardised way would need to be investigated. Contribution on this was required if any progress is to be made.

The Iu/Iur interfaces were also in need of contribution for final decision on the inclusion of security work on these interfaces at the SA WG3 meeting #16.

Delegates were asked to consider all the open issues provided in the TR and to make comments to SA WG3 meeting #16 in order to finalise the document for provision to SA meeting #10 in December 2000 for information.

TD S3z000023: Comments on 3G TR 33.8xx and 3G TR 33.800. This provided comments to TR 33.800 (TD S3z000007). The main concern was the inclusion of much of the material in the TR into the companion TS. The Editor undertook to try to make a identify and mark within the TR, what is expected to be included in the TS.

The editor, Mr. G. Koien agreed to update the TR with all comments received at this meeting and distribute as soon as possible for consideration at SA WG3 meeting #16.

Mr. Koien also indicated that he would be preparing a contribution to SA WG3 meeting #16 suggesting that tunnel-mode was used everywhere to simplify the security. Delegates were asked to consider the pros and cons of the suggestion for contribution to SA WG3 meeting #16.

TD S3z000002: Network Domain Security: 3G TS 33.1de V0.0.1. No contribution had been received for this document and input was requested. The editor, G. Koien agreed to include the parts of TR 33.800 that he considered relevant for this TS for distribution and input to SA WG3 meeting #16 in order to stabilise it for presentation at SA meeting #10 for information. Contribution on this was therefore urgently requested for the SA WG3 meeting #16.

TD S3z000025: Security Services using Public Key Cryptography. This contribution was introduced by Motorola and argued that symmetric key schemes were adequate for the one to many environment, but that the many-to-many environment envisaged for IP-based networks required an asymmetric key system. It suggested that a WI be defined in SA WG3 to include this for Rel4, or to include it within a suitable existing Rel4 WI for MM Access. Mr. Brookson reported that PKI had been evaluated for GSM, but rejected on the grounds of signalling load and smart-card capacity limitations, when using PKI in the wireless environment. These constraints would need re-evaluation for 3GPP systems. It was also stated that the use of PKI in the wireless environment had already been discussed and rejected by SA WG3, following the joint CN/SA WG3 meeting.

It was also questioned whether MultiMedia security was to be covered in the wireless environment, and this would need further discussion in SA WG3 meeting #16. Contributions on this subject were invited.

TD S3z000005: Inter-PLMN Backbone Guidelines. This contribution was provided for information, and noted.

5 IM subsystem security (Rapporteur Krister Boman)

This was dealt with under agenda item 4.1.

6 Network Domain Security (Rapporteur Geir Koien)

This was dealt with under agenda item 4.3.

7 Any other business

There was no contribution under this agenda item. It was noted that Emergency Call issues would need to be handled at SA WG3 meeting #16 and contributions were requested in advance in order to progress towards a solution.

8 Close of meeting

The Chairman thanked the hosts for providing the facilities, and the delegates for their hard work and closed the meeting.

Annex A:
List of documents and their status at the meeting:

NUMBER	TITLE	SOURCE	AGENDA ITEM	Document For	REPLACED BY
S3z000001	Principles of Newtork Domain Security: TR	Telenor	4.3		S3z000007
S3z000002	Network Domain Security: 3G TS 33.1de V0.0.1	Telenor	4.3		
S3z000003	Draft agenda for the ad-hoc meeting	Chairman	2		
S3z000004	LS on Protection of GTP Messages using IPSec	CN WG4	4.1		
S3z000005	Inter-PLMN Backbone Guidelines	Telenor (original: GSMA)	4.3	Information	
S3z000006	Proposed Reply LS to CN WG4: "Protection of GTP Messages using IPSec"	Telenor	4.1	Discussion	S3z000030
S3z000007	TR 33.800 v0.2.4: Principles for Network Domain Security	Rapporteur (Telenor)	4.3	Information	
S3z000008	TR 33.8xx v0.2.0: (Principles of) Access security for IP-based services	Rapporteur (Telenor)	4.2	Information	
S3z000009	TS 33.xxx v0.1.0: Access security for IP-based services	Rapporteur (Telenor)	4.2	Information	
S3z000010	Authentication and protection mechanisms for IM CN SS	Ericsson	4.2	Discussion / Decision	
S3z000011	Draft LS on Integrity Protection in GERAN	TSG GERAN	4.1	Discussion	
S3z000012	Integrity-protection for GERAN-signalling	Siemens	4.1	Discussion	
S3z000013	General Structure of Secure MAP Operations	Ericsson	4.3		
S3z000014	Protection Profiles for MAP Security	Ericsson	4.3		
S3z000015	Structure of Security Header	Ericsson	4.3		
S3z000016	Refinement of MAP Security Association	Ericsson	4.3		
S3z000017	Replay Protection for MAP Security	Ericsson	4.3		
S3z000018	MAP Security Domain of Interpretation for ISAKMP	Ericsson	4.3		
S3z000019	Introduction of MAP security	Siemens	4.3	Discussion/ Decision	
S3z000020	Modification of MAP security header	Siemens	4.3		
S3z000021	SA negotiation protocol for the ZA interface	Siemens	4.3		
S3z000022	IMS authentication and integrity/confidentiality protection	Siemens	4.2		
S3z000023	Comments on 3G TR 33.8xx and 3G TR 33.800	Siemens	4.3		
S3z000024	Proposed Reply LS on GERAN integrity protection	S3_15bis_Adhoc	4.1	Approval	
S3z000025	Security Services using Public Key Cryptography	Motorola	4.3	Discussion	
S3z000026	Liaison Statement to SA WG3 regarding ciphering of RRLP messages between the SMLC and MS in GPRS	TSG GERAN	4.1	Discussion	
S3z000027	S-CSCF issues and security in IM CN SS	BT	4.2	Discussion	
S3z000028	3G TS 23.228 V1.0.0 (with revision marks)	BT	4.2	Information	
S3z000029	3G TS 23.228 V1.0.0 (revision marks accepted)	BT	4.2	Information	
S3z000030	Proposed Reply LS to "Protection of GTP Messages using IPSec"	Telenor/Motorola	4.1	Discussion	
S3z000031	Comment to S3z000014	Siemens	4.3		
S3z000032	Reply LS on GERAN integrity protection		4.1		
S3z000033	Reply LS to "Protection of GTP Messages using IPSec"		4.1		
S3z000034	SA negotiation protocol for the ZA interface (presentation slides)	Siemens	4.3		
S3z000035	IMS authentication and integrity/confidentiality protection (Presentation slides)	Siemens	4.2	Information	

NUMBER	TITLE	SOURCE	AGENDA ITEM	Document For	REPLACED BY
S3z000036	SOME NOTES ON 3GPP TSG CN1 SIP #1 MEETING 17TH – 19TH OCTOBER 2000, SOPHIA ANTIPOLIS, FRANCE	BT	4.2	Information	S3z000037
S3z000037	SOME NOTES ON 3GPP TSG CN1 SIP #1 MEETING 17TH – 19TH OCTOBER 2000, SOPHIA ANTIPOLIS, FRANCE	BT	4.2	Information	

Annex B:
List of Participants

Name	Firma
Günther Horn	Siemens AG
Dirk Kröselberg	Siemens AG
Klaus Müller	Siemens AG
Marc Blommaert	Siemens ATEA
Michael Marcovici	Lucent
Uri Blumenthal	Lucent
Maurice Pope	ETSI
Takeshi Chikazawa	Mitsubishi
Peter Howard	Vodafone
Sebastien Nguyen Ngoc	France Telecom
Geir M. Køien	Telenor R&D
Per Christoffersson	Telia
Dan Brown	Motorola
Lily Chen	Motorola
Stephen Billington	Motorola
Krister Boman	Ericsson
Anders Liljekvist	Ericsson
David Castellano	Ericsson
Valtteri Niemi	Nokia
Berthold Wilhelm	RegTP
Charles Brookson	Department of Trade and Industry, U.K.
Roland Schmitz	T-Nova
Peter Windirsch	T-Nova
Patrick Johnson	Nortel Networks
J. Ioannidis	AT&T Wireless
Benno Tietz	d2mannesmann
Colin Blanchard	BT

3GPP TSG SA WG3 Security — S3#16

28-30 November, Sophia Antipolis, France

Source: **Secretary 3GPP TSG-SA WG3**

Title: **Draft report version 0.0.3**

Document for: **Comment**

Contents

1 Opening of the meeting

The Chairman, Prof. Michael Walker, welcomed delegates to the 16th SA WG3 meeting, in Sophia Antipolis, France, hosted by ETSI.

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 S3-000733.

2 Meeting objectives

The Chairman outlined the objectives, the primary being to progress and prepare the NW Dom Sec and IM Subsystem work. CRs for SA#10 needed to be prepared. SIM-Terminal interface issues also need to be discussed.

The SA WG3 LI group would give a report under 6.3 at 11.30 Tuesday and 11.30 Thursday.

3 Approval of the agenda

The draft agenda, provided in TD S3-000640 was updated with the following changes, and provided in TD S3-000716 which was approved:

Add Agenda Items 9.4 DoS and 9.5 Emergency Calls, 9.6 User Equipment Conformance.

4 Registration and assignment of input documents

The available documents were allocated to their respective agenda items.

5 Approval of reports from S3#15 and S3#15bis

TD S3-000641: The report was reviewed and the actions considered:

AP 15/1:	C. Brookson to ask the GSMA whether they would contribute their document on RAND generation to SA WG3. It was decided not to contribute the document as it was part of the AuC generation process (GSMA document) Action Closed.
AP 15/2:	M Pope to attach updated project plan to the meeting report. Action Completed.
AP 15/3:	M Marcovici to send this to AHAG for information. Sent out, Action taken by AHAG to be confirmed. Action Closed.
AP 15/4:	M. Pope to obtain a number for the TS “Network Domain Security” (Release 2000) and a number for the 33.8xx-series TR “Principles for Network Domain Security”. Completed. TS 33.200, TR 33.800
AP 15/5:	G Koien to use the content of TD S3-000504 and TD S3-000556 for the TR “Principles for Network Domain Security”. Completed.
AP 15/6:	M. Pope to obtain a number for the TS “Access Security for IP based services (R4/R5)” and for the TR "Principles for Access Security for IP based services (R4/R5)". To be checked

The report was then approved without change.

TD S3-000697: Report of ad-hoc meeting, Munich. The report was introduced by Mr. M. Marcovici, who had chaired the meeting, and the report was endorsed.

6 Reports / Liaisons

6.1 3GPP plenary

TD S3-000677 Report to SA3 from SA #9. This was presented by the Chairman and noted.

6.2 3GPP WGs

TD S3-000646 LS from CN WG4 on positive authentication reporting. CN WG4 acknowledges that this could be implemented in their specifications, but will not do so unless there is a service requirement for roaming/interworking between 3GPP and 3GPP2 systems. It was reported that AHAG were to discuss this LS in their December 2000 meeting. The *usefulness* of this LS was noted by SA WG3. It was also noted that positive authentication reporting was still a requirement from SA WG3 and a reply LS to CN WG4 was created to inform them of this and provided in TD S3-000740. It was also reported that a WI exists in the project plan covering this “Enhanced Home Control of Security“ (ID=2026).

TD S3-000647 LS from CN (cc: CN WG4) on Positive Authentication Reporting. It was noted that a response already proposed in TD S3-000605 and also that a WI already existed for this. P. Howard agreed to create a reply LS to clarify this to TSG CN (cc: CN WG4) which was provided in TD S3-000740.

TD S3-000648 LS from RAN WG2 on Security issues. This was an old liaison and had already been dealt with in SA WG3 (Bart Vinck had clarified the issue with RAN WG2) and so was noted.

TD S3-000649 Reply LS from SA WG2 (to SA WG1) on Support of VHE User Profiles. This LS was for information and was noted.

TD S3-000657 LS from CN WG4 on Clarifications to the Security Mode usage, and error cases. This LS was for information and was noted.

TD S3-000658 LS from CN WG4 on Security for MAP over IP. CN WG4 reported that they will study addressing mechanisms and report their findings back to SA WG3. This LS was then noted.

TD S3-000662 LS from SA WG2 on "IM Subsystem Address Storage on USIM". It was noted that the location of the subscriber ID and Home Domain Name on the USIM for stand-alone SIP client connected to an ME was for further study within SA WG3. A response that it is likely to be required to be stored in the USIM was drafted by Siemens and provided in TD S3-000758.

6.3 Lawful interception sub-group

Mr. B. McKibben, the SA WG3 LI Group Chairman, provided a verbal report of progress in the LI group. No meetings had been held since the Washington meeting, but a meeting was being held in parallel with the present SA WG3 meeting. Initial draft of 33.107 (Rel5 LI) was expected to be available by the end of the meeting. January would be available for comment in order to finalise in March 2001. Finalise 33.106 for SA WG3 review and comment also this week. Comments upon the architecture (33.102) document would be provided if considered necessary. Mr. McKibben was thanked for his report.

Later in the meeting, the LI group Chairman returned to provide a report of progress in the parallel LI meeting and to present CRs for approval.

TD S3-000750 Release 4 draft of TS 33.106. The LI group Chairman reported that this Lawful Interception document was expected to be completed for submission to SA WG3 for approval at SA WG3#17 and presented the document briefly. The document was noted.

TD S3-000747 CR to 03.33: Addition of parameters to the X3-Interface. This CR was modified to correct the cover sheet in TD S3-000762 and was agreed.

TD S3-000748 CR to 33.107: Addition of parameters to the X3-Interface. This CR was modified to correct the cover sheet in TD S3-000763 and was agreed.

TD S3-000749 CR to 03.33: Deletion of mono-mode and addition of optimal routing. This CR was modified to correct the cover sheet and split into 2 CRs for R98 and R99 in TD S3-000764 and TD S3-000765 Which were agreed.

TD S3-000751 LS from LI group to SA WG3: Comments on TR 33.800. The LI group had reviewed the document and reported that they had no input to make. The LS was noted.

TD S3-000752 Proposed LS from LI / SA WG3 to CN WG4: Lawful Intercept support on the Mc interface. This LS asks for the support of interception requirements in MGW. The LS was modified to add the contact details and provided in TD S3-000766 and approved.

6.4 SAGE

TD S3-000644 LS on Increasing maximum number of bits to be enciphered with f8. This stated that the increase in the number of bits to be encrypted with f8 did not produce any problems and informed SA WG3 that no change to the f8 specification or to the test data would be made. The LS was noted.

TD S3-000730 SAGE deliverables 1, 2, 3, 4. The SAGE evaluation deliverables were presented by P. Christoffersson for information and were noted. A further document (the evaluation report) was expected to be completed in February 2001. SA WG3 were asked to recommend the quick publication of these reports. SA WG3 agreed to ask TSG SA to approve them for publication on the 3GPP web site, and to ask the PCG to endorse them for open publication on the Organisational Partners (SDOs) web sites.

AP 16/09: Chairman to recommend to SA#10 to approve the SAGE deliverables (1, 2, 3 and 4) for publication on the 3GPP server and to ask PCG to endorse them for publication by the Partner SDOs.

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

TD S3-000643 Application on external devices (GSM Certification Forum). This contribution was provided for information and was noted.

TDS3-000711 Rogue-Shell threat analysis and the attached Lucent's optional solution was presented by Michael Marcovici, Lucent Technologies for information. This is a Lucent contribution, which had been presented at TR-45 AHAG and TR-45.2 meetings. Lucent's proposed Rogue-Shell solution for ANSI-41 networks had been adopted in principle by TR-45.2 (it was noted that this is not an AHAG authored or officially endorsed contribution). The implementation details had been delegated to the appropriate air interfaces subcommittees and to TR-45.2 subcommittee (at their discretion, they may choose to implement as-is, change the proposed architecture, or not to implement any of the proposed enhancements). It was also expected that the "Rogue-Shell" threat and solutions will be further addressed at future TR-45 AHAG meetings. The contribution was noted.

Note: SA WG3 should wait for a formal LS from TR-45 AHAG, addressing the above issues, before considering if any further action or evaluation is warranted.

It was reported that TR-45.3 had recommended that a liaison officer from AHAG to SA WG3 should be appointed, and TR-45 will be asked to approve this at their next meeting.

Charles Brookson, the Chairman of the joint working party between the GSMA and SA3, reported the progress on the new A5/3 algorithm for GSM. It is also likely that the algorithm can be used for EDGE and as GEA3 for GPRS. A specification has been written, and development time is about 4 to 6 months at an estimated cost of 100K ECU.

The GSMA and ETSI were agreeing the basis of the distribution of the new algorithm, it was intended that it should be owned and distributed in the in the same way as the existing algorithm for 3G, Kasumi:

i) The GSMA has already indicated a willingness to fund the development cost of the new algorithm;

ii) The Algorithm, being a 3GPP specification, would be jointly owned by the 3GPP Partners, but the GSMA should be granted custodianship as already practised for the existing A5 algorithm;

iii) The Partners should be urged to seek the necessary authorisation for the open publication of the new Algorithm, and was also the case for the GEA algorithms.

A5/3 will be developed by SAGE, and based on Kasumi. There are significant advantages in using Kasumi, as the development time and costs were much less than a new algorithm, and multimode GSM/3G mobiles could use the same algorithm. It could also be used when and if the key length for A5 is extended from 64 to 128 bits offering better security for customers.

It was agreed that SA should be informed on the above in the SA3 Chairman's report.

AP 16/01: Chairman to report the development of A5/3 progress to SA Plenary and ask for agreement of the 3GPP Partners.

7 Joint meeting with T3

TD S3-000721 Agenda for joint meeting with T3. The draft agenda for the joint session was approved.

7.1 Review of purpose of meeting

The purpose of the meeting was to discuss the retransmission of authentication request, and Interworking between USIM and ME concerns raised by T WG3.

7.2 Introductions

Each delegate introduced themselves for the benefit of all present.

7.3 Assignment of documents

Documents were assigned to the different parts of the joint session agenda.

7.4 Retransmission of authentication request

TD S3-000655 LS from T WG3: Re-transmission of authentication request using the same quintet.

T WG3 requested a change to the placing of the authentication termination on update of START, moving the mechanism from the SIM/USIM to the ME. It was stated that the mechanism was placed in the SIM/USIM in order to keep security functionality together, and for simplicity of the architecture model, but that there was no security reason for it not being placed in the ME. The need for the retransmission of authentication request itself was identified as necessary, particularly in the GSM environment and GPRS. For the 3GPP system, it would be needed when a packet-mode GSM subscriber roams into the 3GPP network. An indicator to distinguish between Packet mode and Circuit mode would need to be provided to the USIM if it were implemented there. It was agreed to move the mechanism to the ME and a CR would be needed for this. The CR would be based upon that in TD S3-000713 (see below) and a drafting group was asked to develop this in an evening session, this was provided in TD S3-000725.

The following issues were raised and discussed, considering the agreement to move the mechanism into the ME:

a) Storing RES may not be necessary, as it can be (re-)calculated by the USIM when needed.

   This would not be necessary for the USIM placing of the mechanism, but was needed for the ME placing.

b) Do IK and CK need to be returned as well as RES?

   Yes.

c) In the case that GSM access service is supported by the USIM what should be done with the cipher key Kc?

   This is not relevant due to moving the mechanism to the ME.

d) Can deletion of parameters on power down of the USIM and termination of the USIM session only be considered?

   This requires clarification when the mechanism is moved into the ME. SA WG3 would need to study this issue.

e) Clarification on the generation of START values was requested, due to some perceived ambiguity in TS 33.102, sections 6.4.8 and 6.4.5.

   The editor, Mr. Marc Blommaert was asked to check this and generate a CR to correct it if necessary.

f) Should both associated (RAND, AUTN) pairs for both PS and CS domains be stored?

This would need study in SA WG3 after moving the mechanism to the ME.

g) Clarification on why exactly the requirement that the stored values have to be deleted immediately upon update of the associated START parameter is necessary was requested.

This is not relevant due to moving the mechanism to the ME.

The Editor of TS 33.102 (Mr. Marc Blommaert) was asked to check all the points raised.

AP 16/02: Editor of 33.102 (M Blommaert) to check the points raised in TD S3-000655 when reviewing the document and take necessary actions.

It was decided that a response liaison should be produced to T WG3 and CN WG1, copy SA WG1 and T WG2, which was produced in TD S3-000741.

TD S3-000713 Proposed CR to 33.102: Re-transmission of authentication request using the same quintet. This CR was accepted in principle. The editor of 33.102 (Marc Blommaert) was asked to form a group to double-check the proposal, and the need for storing both AUTN and RAND should be reviewed by this group. (Planned 17.00 Tuesday).

TD S3-000712 Discussion paper to "Re-transmission of authentication request using the same quintet" (S3-000578). This was covered by the discussion of TD S3-000713 and was noted.

7.5 Interworking between USIM and ME

TD S3-000661 3G TR ab.cde: SIM/USIM Internal and External Interworking Aspects. SA WG3 delegates were asked to review this draft TR and to examine the alignment of it with TS 33.102. Marc Blommaert was asked to check whether the text of section 6.8 of TS 33.102 could be replaced by parts of this TR, for review at the next SA WG3 meeting. The report was noted.

AP 16/03: M Blommaert to review section 6.8 of 33.102 to see if text can be replaced by reference to the SIM/USIM Internal and External Interworking aspects draft TR (T WG3) for report to SA WG3#17 meeting.

TD S3-000682 Problem with no USIM-ME interface in GSM-only ME. This contribution suggested that the GSM level security was maintained in the 3GPP environment when roaming, as an introduction to the proposed CR in TD S3-000680 (below).

TD S3-000680 Proposed CR to 33.102: Optional support for USIM-ME interface for GSM-only R99 ME. This proposed CR provided many changes and it was decided that serious checking was needed outside of the main meeting to ensure that it covers all requirements and does not introduce further problems. The possibility of allowing a 32-bit RES response to be accepted by a 3GPP network needed to be checked and the proposed CR updated as appropriate. (See discussion under agenda item 10.1)

TD S3-000681 Rejection of non ciphered connections. France Telecom presented a mechanism to have a 4-valued parameter, controlled by the SIM/USIM to control the rejection of non-ciphered calls in the CS domain. ***(The importance of inclusion of this in the PS domain was also questioned and this should be considered by SA WG3 delegates)***.

Value 0: The Terminal rejects all non-ciphered calls and informs the user. (default state which can move to Value 1 temporarily by the user).

Value 1: The Terminal accepts all non-ciphered calls and informs the user (temporary state which resets to Value 0 on return to Ciphering-enabled network).

Value 2: Set in SIM: Terminal rejects all non ciphered calls (permanent state).

Value 3: Set in SIM: Terminal accepts all non ciphered calls (permanent state).

It was noted that Value 0 would reject a call, notify the user in order that the setting can be set to Value 1 if required and it may be that the user is not attending to the indications and would not receive any unciphered calls. The setting of Value 2 was considered a potential problem, as a user roaming into a non-ciphered network would have all calls rejected. It was clarified that the use of this by operators was expected to be only for very specific circumstances (e.g. a closed domain).

After some discussion of the mechanism, it was agreed in principle as a working hypothesis for SA WG3, and the need for liaison with other groups would be necessary in order to gauge the impact on those groups' work. It was thought that the ciphering indicator should also be integrated into the mechanism in order to

give early warning of the state of ciphering in the network. It was also thought that a “health warning“ should be provided about the limited expected use of Value 2.

France telecom agreed to produce a CR to 33.102 to include this proposal as a Release 4 mechanism, which would be liased to T WG3, CN WG1, T WG2 and SA WG1.

It was clarified that the mechanism would not be applicable to Emergency Calls (all Emergency Calls would be accepted).

7.6 Conclusions

The moving of the positive authentication reporting into the ME was agreed. A response LS was to be created answering the questions from T WG3 (and other affected groups) in the light of this agreement and corresponding CRs would be produced.

8 Work programme

8.1 Review security work programme

TD S3-000696 Security workplan status report. The issues on the Project Plan were presented by P. Howard. Inputs were awaited from SA WG2 on QoS Parameters and from CN WG4 on TrFO which meant that the SA WG3 work had not progressed. P. Howard agreed to produce a liaison statement to these groups on this, which was provided in TD S3-000742. The Project Plan needed to be checked and updated at this meeting. The WI Rapporteurs, P. Howard and M. Pope agreed to meet outside the meeting to progress this for presentation to the meeting. This was done and the resulting updated SA WG3 Project plan appended as an annex to this report.

M. Pope was also asked to add references to the WI description sheets (on the FTP server) as an annex to meeting reports from now on. This was agreed.

AP 16/04: M Pope to add references to the SA WG3 WI sheets (on the FTP server) to the meeting report.

8.2 Status of security work items

TD S3-000694 Extension of FIGS to the packet switched domain. This was presented by P. Howard. It was noted that FIGs was not an approved WI in 3GPP at present, due to the lack of supporting companies when presented for approval. The contribution clarifies the use of FIGs in the CS domain, and it’s applicability and the issues raised for it’s use in the PS domain (GPRS and UTRAN). The use of CAMEL Phase 4 would need to be decided quickly, and would require liaison to CN WG2. The use of TAP would need liaison to TADIG and the use of IST (Instant Service Termination) in the PS domain would need further study and work. It was commented that the Ga interface would also require study. After the presentation, further supporting companies were received, which was supported by Vodafone, BT, Orange and the DTI, Ericsson agreed to check whether they could also be added to the list. The original proposed WI sheet from SA#08, SP-000304, would be updated with the supporting companies and additional justification from the contribution for agreement by SA WG3, this was provided by P. Howard in TD S3-000745 which was approved.

TD S3-000642 Liaison to ETSI for forwarding to 3GPP TSG-SA3 - Response to "Use of the Fraud Information Gathering System". This contribution provided a draft of ITU Recommendation M.3210.1, and requested input from SA WG3 on the GPRS, IP domain issues and Handling of data service related information. It was decided that this should be discussed by the companies supporting the FIGs WI outside of the main meeting.

AP 16/05: Companies supporting FIGs should discuss the issues in ITU-T Rec. M.3210.1 for GPRS and IP domain, for input to ITU-T.

8.3 New security work items

There were no contributions under this agenda item.

9 Security issues

9.1 GERAN

TD S3-000651 Draft LS on Integrity Protection in GERAN. This LS had been dealt with at the ad-hoc meeting (#15bis) and a response had been transmitted to GERAN (TD S3-000714). The LS from GERAN was then noted.

TD S3-000714 Reply LS on GERAN integrity protection (S3z000032). This was transmitted from the ad-hoc meeting (#15bis) and was presented to SA WG3 for formal approval. The LS was approved.

TD S3-000708 GERAN integrity protection. This contribution proposed to ask GERAN to detail the critical messages which need to avoid segmentation in order to allow maximum number of security bits to be included in messages without disrupting performance. It was agreed to ask GERAN for this information.

TD S3-000645 Liaison Statement to SA WG3 regarding ciphering of RRLP messages between the SMLC and MS in GPRS. This LS was introduced by Nokia. It was agreed that a response LS would be drafted informing GERAN that SA WG3 need to consider this further and will respond after SA WG3 meeting #17.

9.2 Location services

There were no contributions under this agenda item.

9.3 MExE security

TD S3-000693 MExE security issues. This LS was presented by Vodafone. It suggested that SA WG3 advise T WG2-MexE on the security requirements for APIs in trusted and untrusted domains. A liaison about this contribution had been received from the T WG2-MexE group in TD S3-000704 which was considered.

TD S3-000704 LS from T WG2/MExE: MExE group comments to "MExE security issues" Vodafone document. This contribution was sent to pre-empt the discussion of the Vodafone contribution in TD S3-000693 and provided details on the working and understanding of the T WG2-MExE group. It reported a mismatch in the assumptions that had been made by Vodafone with the assumptions of T WG2-MExE.

It was decided that SA WG3 will review the MExE security issues when the security model is verified. P. Howard agreed to draft a liaison replying to T WG2-MExE and inviting them to a SA WG3 meeting.

9.4 Denial of Service

TD S3-000678 Internet-based DoS attacks on UMTS network. It was decided to take the discussion of this off-line, and C Brookson agreed to lead an e-mail discussion group on this. Comments should be included in the Security Guidelines document (TR 33.900).

AP 16/06: C. Brookson to initiate an e-mail discussion on Internet-based DoS attacks and include agreements in TR 33.900.

9.5 Emergency Calls

There were no contributions under this agenda item.

9.6 User Equipment Conformance

TD S3-000695 Security aspects of UE conformance. This contribution identified some Conformance Testing Security requirements which had not been included in the T WG1 documents. It suggested a LS is drafted to T WG1 highlighting the deficiencies in their conformance specifications. It was agreed that this should be done, except for the security indicators, which needed further work, and P. Howard agreed to draft this LS.

10 S3 specifications/reports

10.1 3G TS 33.102 Security architecture

TD S3-000664 Proposed CR to 33.102: Correction for integrity protection when using GSM SIM cards in UMTS ME. This CR proposed to add a parameter to the ME to allow SIM cards to offer integrity protection when inserted in a 3G Terminal on a UMTS network. Some concerns were expressed on the need for this, as operators could provide their subscribers with USIMs in order to allow this. Potential security threats were also considered, as an attacker may be able to change the START value in the ME. It was generally agreed that something needs to be done by SA WG3 in order to meet the requirement of using a SIM in a UMTS ME on a UMTS network, but the proposal as it stood was rejected.

TD S3-000665 Proposed CR to 33.102: Clarification of terms R99+ and R98-. The Chairman suggested that SA WG3 terminology should be corrected in a single CR as a group, and these changes should be re-submitted as part of such a CR. This CR was therefore rejected at this time.

TD S3-000666 Proposed CR to 33.102: Corrections on ciphering and integrity protection. This CR was agreed.

TD S3-000669 Proposed CR to 33.102: Corrections to Counter Check procedure. This was updated with minor editorial changes and provided in TD S3-000726, which was agreed.

TD S3-000671 Proposed CR to 33.102: Intersystem handover for CS Services – from GSM BSS to UTRAN. This CR was considered, and it was decided to provide some time for review of any potential threats that the CR may introduce. This was done, and no threats were identified, and the CR was then modified slightly, and provided in TD S3-000727, which was agreed.

TD S3-000675 CR to 33.102: Additional parameters in AFR (Rel4). It was identified that a CR to 29.002 would also be needed if this CR was accepted and alignment with the FIGs specifications should also be done, particularly with respect to FIGs over CAMEL. An analysis of any additional parameters and requirements should be made at the ad-hoc meeting on FIGS. However, there was no time to hold this ad-hoc meeting during the week, so the CR was postponed until discussions could take place.

TD S3-000680 Proposed CR to 33.102: Optional support for USIM-ME interface for GSM-only R99 ME. The changing from variable-length RES to fixed 32-bit RES had been discussed at an ad-hoc. Delegates were asked to consider this. The CR was not approved at this time.

TD S3-000690 Proposed CR to 33.102: START value handling for MS with a GSM SIM inserted. This CR was modified and provided in TD S3-000739, which was agreed.

TD S3-000692 Changes to authentication data request message to enhance index value allocation in the AuC. This was introduced by Vodafone, and proposed creating a LS to CN WG4 requesting the addition of values to the MAP Authentication Data Request message for Release 4: *Requesting Node Type* (CS, PS) and *Requesting Node Identity*, in TS 29.002. It also proposed that a Release 4 CR is created to 33.102 to include this. There was some reluctance to accept this at this time, and **delegates were asked to consider it for contribution at SA WG3#17 meeting.**

TD S3-000707 Subject: Correction on use of GSM MS classmark in UMTS. This CR was revised and provided in TD S3-000729, which was agreed.

TD S3-000725 Proposed CR to 33.102: Re-transmission of authentication request using the same quintet (rev of S3-000713). This CR was agreed.

TD S3-000726 Proposed CR to 33.102: Corrections to Counter Check procedure (rev S3-000669). This CR was agreed.

TD S3-000727 Proposed CR to 33.102: Intersystem handover for CS Services – from GSM BSS to UTRAN (rev S3-000671). The concerns on this CR were withdrawn and the CR was agreed.

TD S3-000676 Proposed CR to GSM 03.35: IST implementation for non-CAMEL subscribers. This Cr reflected the already approved CRs to CN specifications and it was considered that more time was needed to check the consistency and correctness of the changes. **It was decided to send this for e-mail approval by 8 December 2000.**

TD S3-000724 Draft liaison statement to CN4 regarding Positive Authentication Reporting. This LS was approved.

TD S3-000732 Reply LS to S3-000662: LS for "IM Subsystem Address Storage on USIM". This was revised in TD S3-000758 and approved.

TD S3-000757 LS for "Security risks in introduction phase of MAP security". This LS was approved.

TD S3-000746 Draft LS to GERAN about ciphering of RRLP messages between SMLC and MS in GPRS. This LS was approved.

TD S3-000736 Proposal not to use the IMSI as the identity of an IM subscriber. This LS was modified and provided in TD S3-000759 which was approved.

TD S3-000737 Proposed LS to CN4 on SA3 agreements on MAPSec. This LS was modified and provided in TD S3-000760 which was approved.

TD S3-000745 Update to FIGS/IST work item description. This revised WI description was approved.

TD S3-000740 LS to CN, cc: CN4 on Positive authentication reporting. This LS was approved.

TD S3-000741 LS to CN1, cc: T2/T3: Authentication request retransmission. This was modified to correct spelling and provided in TD S3-000761 which was approved.

TD S3-000742 LS to SA2, cc: CN4: Request for information to complete security work items. This LS was approved.

TD S3-000738 Standardisation of security parameter bit ordering in USIM and AuC. This suggests an e-mail discussion of the issue, which was agreed.

AP 16/07: P. Howard to lead an e-mail discussion on Standardisation of security parameter bit ordering in USIM and AuC (TD S3-000738 as a basis).

10.2 3G TS 33.103 Integration guidelines

There were no contributions under this agenda item.

10.3 3G TS 33.105 Algorithm requirements

TD S3-000667 Proposed CR to 33.105: Layer 2 related corrections. This CR reflected the response from ETSI SAGE that they had verified that increasing the number of bits to cipher using f8 had no security impact, and also included a clarification on plaintext blocks. The CR was agreed.

10.4 3G TR 33.908 General report on confidentiality / integrity algorithm design and evaluation

TD S3-000659 TR 33.908 v 3.0.0 This was provided for information to show the current version of SAGE Report version 1.0, which described the evaluation that would be done. The report was noted.

Mr. Pope explained that the SAGE Report version 1.0 had been approved at SA#07 and SAGE had subsequently used the same report for the evaluation results, updating to version 1.1 and 2.0 for the final results report. It was decided that in order to preserve the original information, that a new report would be produced in 3GPP, containing the evaluation results of SAGE Report version 2.0, which was provided in TD S3-000660.

10.5 3G TR 33.909 Evaluation of confidentiality / integrity algorithm

TD S3-000660 33.909 v0.0.1: Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms. This was provided by Mr. Pope for approval and was the SAGE evaluation report version 2.0, put into 3GPP TR format. The TR was approved by SA WG3 **to be forwarded to TSG SA#10 for approval** in order that 3GPP may publish it. It was noted that publications by the 3GPP Partners Organisational Bodies (SDOs) would require the endorsement of the PCG. The Chairman undertook to ask TSG SA to forward this to the PCG with the recommendation that it is approved for publication by the Partner SDOs.

AP 16/08: Chairman to ask TSG SA#10 to forward the TR 33.909 to PCG (if approved by TSG SA) for approval for publication by the Partner SDOs.

10.6 Draft 3G TR 33.900 Guide to 3G security

There were no contributions under this agenda item. However, the editor was asked to update the document with input received at this meeting (see agenda item 9.4).

10.7 Draft TR and TS on network domain security

TD S3-000650 Update information TR 33.800 v024 -> v035. The changes since version 0.2.4 were presented by the editor (Mr. G Koien). SA WG3 were asked whether it was thought stable enough to present the TR to SA#10 for information with a view of TSG SA approval at SA#11. The document was reviewed, and section 5.5.4, concerning firewalls was thought to be inappropriate for the document, and it was agreed to move the information, along with figure 1 to the Security Guidelines document (Editor: C Brookson), and to mark the section as outside of the scope of this TR. Section 6.0, which gave initial ideas for the document will be removed before presentation to TSG SA., sections 6.1.x will be marked “for further study“. The inclusion of the SA lifetime had been agreed in the Munich ad-hoc meeting (#15bis), to be an absolute time indicator. The Editor included a proposal on how to code this, but pointed out that this diverges from the method used in RFC-2407 (DoI). SA WG3 accepted the use of absolute time. Delegates were asked to review the document, and in particular, to consider the text in section 9 and make contributions.

IPSec/key management was accepted as a working assumption for Network Domain Security, and the contents of TD S3-000670 (see discussion of TD S3-000670, second part, below) would need to be incorporated into TR 33.800 and TS 33.200. It was recognised that the updates to TR 33.800 and TS 33.200) on Network Domain Security were not feasible in time for presentation to the TSG SA#10 meeting, so the editor, Mr. G. Koien, was asked to write a letter to the Chairman, explaining why the presentation to SA Plenary of the TR and TS is late. The TR and TS will then be sent to the SA WG3 mailing list for approval in January 2001, and the Chairman would ask TSG SA to receive the agreed TR and TS, by e-mail, for information at the end of January in order that it may be presented for approval at the TSG SA#11 meeting in March 2001.

TD S3-000663 Simplifying assumption for the use of IPsec in UMTS. This contribution proposed to discourage or disallow the use of:

- IP Payload compression;
- The use of Transport mode (tunnelling should be used);
- The use of AH (ESP should be used); and
- The use of nested tunnels (chained ESP tunnel mode should be used).

It was generally agreed that these items should be disallowed for interoperability reasons, except for the use of nested tunnels, which needed more study.

TD S3-000687 Restricting the IPsec usage. This contribution discourages the use of ESP without authentication, and the use of ESP-DES, in favour of the ESP-3DES transform, or another, better crypto transform (e.g. AES). The principle of the contribution was agreed by SA WG3 and the document noted.

TD S3-000668 (Ericsson), TD S3-000670 (Telenor) and TD S3-000686 (Siemens) were presented and then discussed.

TD S3-000668 IKE negotiation of SAs over the Za interface.

TD S3-000670 UMTS Key Management *(first part, on Key management, discussed here)*.

TD S3-000686 SA negotiation protocol for the ZA interface.

After some discussion on the proposed solutions, there was general agreement that a simple solution should be aimed for, and there was some sympathy for the solution outlined in TD S3-000670. This was accepted as basis for the key management architecture by SA WG3, and delegates were asked to study the scalability issues of the proposal. The scenario provided in TD S3-000686 (multiple tunnels) was not required as a working assumption by SA WG3. Delegates were asked to check for any problems and to inform the group in good time before the SA WG3#17 meeting.

TD S3-000672 Proposed LS to CN4 on SA3 agreements on MAPSec. This proposed LS informed CN WG4 of the progress achieved in SA WG3. It was decided to update this LS with the further progress achieved at this meeting and re-submit it for approval. This was done and provided in TD S3-000735.

TD S3-000673 Protection Profiles for MAP Security. This contribution provided some alternatives for the specification of the internal structure of Protection Profiles for MAP Security, taking into account the proposals received at the ah-hoc meeting (#15bis). The evaluation was used to stimulate discussion in SA WG3 on the choice of Protection Profiles and the results of the discussion would need to be liased to CN WG4, as it will impact their work. After some discussion, the proposal of this contribution was accepted by SA WG3 as a working assumption and a LS to CN WG4 was produced to inform them of this recommended solution, in order that they can check the efficiency impacts of the mechanisms. Ericsson agreed to produce this LS, which was provided in TD S3-000735.

TD S3-000674 Algorithm Selection for MAP Security. This contribution recommended the use of AES Rijndael as the mandatory encryption algorithm, and Twofish and Blowfish as optional algorithms. It also recommended the use of SHA-1 as the mandatory MAC algorithm and MD5 as an optional one. There was some reservation over the use of Blowfish expressed, due to the high overheads it involves. It was proposed that only 1 algorithm should be mandated for each function, without optional algorithms, in order to reduce complexity. It was agreed that AES-Rijndael will be mandated for the Encryption algorithm. It was suggested that Rijndael (in MAC mode) should also be used for the MAC algorithm. This was endorsed by SA WG3. Therefore, AES will be used for both Encryption and MAC and SA WG3 need to define the meaning of AES in MAC mode. This agreement was included in the LS to CN WG4 (TD S3-000735).

TD S3-000766 Presentation on Key Management in IETF. This was presented by AT&T. there was some discussion and questions, and the presentation was noted.

TD S3-000683 IETF draft: A Roadmap for IPsec Policy Management, TD S3-000684 IETF draft: IPSP Requirements and TD S3-000685 IETF draft: IPsec Policy Architecture were all provided as supporting information for TD S3-000766 These documents were noted.

TD S3-000688 Introduction of MAP security. This was an update to a contribution provided to the ad-hoc meeting (#15bis) (S3z000019), modifying the conclusion on how to handle cut-off dates for the introduction of MAP security with Profile Mode 1 for all UMTS PLMNs (and possibly for GSM PLMNs). The proposal was agreed and it was noted that a LS to the TSG SA Plenary and another to the GSMA Security Group (containing more detailed information) would be needed. A draft LS was provided in TD S3-000757, but it was decided that this should not be done until the Stage 2 of MAP Security work is stable, so that a cut-off date can be decided upon with full knowledge of the implications of the MAP Security enhancements to operators.

TD S3-000670 UMTS Key Management (*second part, on MAP Security, discussed here*). This proposal was introduced by Telenor, and suggested that:

Revert to a model where MAP is used for its own key management

Use IKE between KACs

Use http both for distribution between KACs and between KACs and NEs, using TTL/SSL for transport security. TD S3-000703 “Using HTTP to distribute MAPsec SAs“ was then introduced as a possible realisation of the proposed method.

The use of http was not supported by SA WG3. The working assumption was to use IKE between KACs and to define a mechanism for distribution between KACs and NEs, The use of IPSec was agreed as a working hypothesis for this. It was noted that the issue of key fetching would need to be revisited.

TD S3-000715 Reply LS to CN WG4 on "Protection of GTP Messages using IPSec" (S3z000033). This was agreed at the ad-hoc meeting (#15bis) and was presented to SA WG3 for formal approval. The LS was approved.

10.8 Draft TR and TS on IM subsystem security

TD S3-000679 Options for Access Security for IM Domain. This was presented by Motorola and outlines the problems with the traditional trust model when applied to the Multimedia environment, where there are mixed end-user types. It provided 3 strategies and proposed that SA WG3 study strategy #2. It was agreed that this should be studied further in SA WG3.

TD S3-000689 (Siemens), TD S3-000699 (Ericsson) and TD S3-000710 (Nokia) were presented and a discussion followed.

TD S3-000689 IMS authentication and integrity/confidentiality protection. This was presented using the slides provided in TD S3-000753 and points out the pros and cons of the Siemens and Ericsson proposals.

TD S3-000699 Authentication and protection mechanisms for IM CN SS. This was an updated proposal from the one presented and discussed at the ad-hoc meeting (#15bis) and re-uses the current architecture.

TD S3-000710 IMS authentication in both visited and home networks. This proposal suggested a compromise solution between the Siemens and Ericsson models.

It was agreed that the architecture should be discussed before full agreement upon the pros and cons of each model could be finalised and agreed upon. Due to lack of time, it was agreed that the discussion on the integrity protection termination should be **postponed** to the next meeting (SA WG3#17).

Control of authentication (checking of RES): There was little support for the Nokia compromise, although it was recognised that the intended flexibility was useful and a compromise, taking the best features of both the Siemens and Ericsson proposals, should be sought. It was highlighted that the HS relationship may not be the same as it is between the Home and Visited PLMN in the IMSS environment (i.e. based on agreements and therefore with a known trust model).

The Chairman stated that some operators may consider that a visited UMTS network could falsely report ongoing calls to the Home UMTS network and the Home network may still want the option to control authentication even when agreements exist with the visited network.

Therefore a combination of the Siemens and Ericsson proposals to allow the Home Network to delegate the authentication to the visited network, depending on the trust relationship which exists between them, was suggested. It was thought that this could be accomplished by modifying the Siemens proposal to include authentication parameters back to the HSS (i.e. f(RES), where f is some function), to allow the home control of authentication. It was agreed that an e-mail discussion should be initiated on this and a new proposal brought to the SA WG3 meeting #17.

AP 16/10: K. Bowman to initiate an e-mail discussion on IMS authentication and provide a mutually agreeable proposal to SA WG3 meeting #17.

Location of Confidentiality and Integrity Functions: It was suggested that the architecture defined by SA WG2 should be clarified from the security viewpoint. It was decided that a joint meeting with SA WG2 should be set up, and this may be done by **co-locating the next meetings of SA WG2 and SA WG3**, which are scheduled for the same week.

TD S3-000702 Draft LS to SA WG2: Clarification on the role of the P-CSCF. This LS was modified in TD S3-000755 and approved. TD S3-000756 will be attached.

TD S3-000705 Authentication framework and algorithm boundary conditions. This document was presented for information and was noted.

TD S3-000706 Extensions to TD36 for 3GPP security. This document was presented for information and was noted.

TD S3-000709 Support of certificates in 3GPP security architecture. This document was postponed to SA WG3 meeting #17. Delegates were asked to consider the proposals before the next meeting.

11 Future meeting dates and venues

A calendar of planned 3GPP meetings was provided in TD S3-000698 for information.

Meeting	Date	Location	Host
S3#17	27 February - 1 March 2001	Sophia Antipolis, France	ETSI Secretariat
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	Madrid (TBC)	Ericsson (TBC)

12 Any other business

The following documents were not discussed at the meeting due to lack of time:

TD number	Title	Source	Agenda	Document for
S3-000691	Emergency call handling	Vodafone	9.5	Discussion
S3-000700	3G TR 33.8xx V0.3.0	Ericsson	10.8	Information
S3-000701	3G TS 33.2xx V0.1.1	Ericsson	10.8	Information
S3-000723	Comments from K Holley on S3-000700	BT	10.8	Information
S3-000734	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
S3-000735	Proposed LS to CN4 on SA3 agreements on MAPSec (rev S3-000672)	Ericsson	10.7	Approval
S3-000743	LS to T1, cc: CN1/RAN2: Security aspects of UE conformance testing	Vodafone	9.6	Approval
S3-000744	LS to T2-MExE: MExE security issues	Vodafone	9.3	Approval

13 Close of meeting

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

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

TO BE COMPLETED

Name			Company	e-mail	3GPP Member	

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-000640	Draft agenda for SA WG3 meeting #16	Chairman	2	Approval	S3-000716	Revised in TD716
S3-000641	Draft report of SA WG3 meeting #15 version 0.0.6	Secretary	5	Approval		PDF Workplan attached. Approved
S3-000642	Liason to ETSI for forwarding to 3GPP TSG-SA3	Q24/4 Rapporteur group	8.3	Discussion		To be discussed by the companies supporting the FIGs WI
S3-000643	Application on external devices	GSM Certification Forum and EICTA CCIG	6.5	Information		Noted
S3-000644	LS on Increasing maximum number of bits to be enciphered with f8	ETSI SAGE 3GPP Task Force	6.4	Information		Noted
S3-000645	Liaison Statement to SA WG3 regarding ciphering of RRLP messages between the SMLC and MS in GPRS	TSG GERAN	9.2	Discussion		Needs further consideration in SA WG3. Response LS to be drafted.
S3-000646	LS on positive authentication reporting	CN WG4	6.2	Discussion		Noted. (PAR is a SA WG3 requirement)
S3-000647	LS on Positive Authentication Reporting	CN WG4	6.2	Discussion		Response in TD740
S3-000648	LS on Security issues	RAN WG2	6.2	Discussion		Noted (old LS, subject already dealt with).
S3-000649	Reply LS (to SA WG1) on Support of VHE User Profiles	SA WG2	6.2	Information		Noted.
S3-000650	Update information TR 33.800 v024 -> v035	Rapporteur (Telenor)	10.7	Discussion		Discussed & Noted
S3-000651	Draft LS on Integrity Protection in GERAN	TSG GERAN ad-hoc#2	9.1	Information		Noted. A response from ad-hoc in TD714
S3-000652	Withdrawn	MCC / ETSI SAGE		Approval		WITHDRAWN
S3-000653	Withdrawn	MCC / ETSI SAGE		Approval		WITHDRAWN

S3-000654	Withdrawn	MCC / ETSI SAGE		Information		WITHDRAWN
S3-000655	LS from T WG3: Re-transmission of authentication request using the same quintet	T WG3	7	Discussion		Mech. To be moved to ME. Response in TD725. Joint session with some T WG3 delegates requested
S3-000656	Withdrawn	MCC / ETSI SAGE		Approval		WITHDRAWN
S3-000657	LS on Clarifications to the Security Mode usage, and error cases	CN WG4	6.2	Information		CC to SA WG3. Noted
S3-000658	LS on Security for MAP over IP	CN WG4	6.2	Discussion		Noted
S3-000659	33.908 v 3.0.0:	MCC	10.4	Information		SAGE Report v1.0. Provided for information. Noted
S3-000660	33.909 v0.0.1: Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms	MCC/ETSI SAGE	10.4	Approval		SAGE Report v2.0. Approved.
S3-000661	3G TR ab.cde: SIM/USIM Internal and External Interworking Aspects	T WG3	7	Information		Supports S3-000655. Noted.
S3-000662	LS for "IM Subsystem Address Storage on USIM"	SA WG2	6.2	Discussion		Further study needed. Info response in TD758
S3-000663	Simplifying assumption for the use of IPsec in UMTS	Telenor	10.7	Discussion / Decision		Items should be disallowed for interoperability reasons, except for the use of nested tunnels, which needed more study
S3-000664	Proposed CR to 33.102: Correction for integrity protection when using GSM SIM cards in UMTS ME	Nokia	10.1	Approval		Rejected. Noted that something needs to be done

S3-000665	Proposed CR to 33.102: Clarification of terms R99+ and R98-	Nokia	10.1	Approval		Rejected. All such corrections to be submitted in a single CR
S3-000666	Proposed CR to 33.102: Corrections on ciphering and integrity protection	Nokia	10.1	Approval		Approved
S3-000667	Proposed CR to 33.105: Layer 2 related corrections	Nokia	10.3	Approval		Approved
S3-000668	IKE negotiation of SAs over the Za interface	Ericsson	10.7	Discussion		Delegates were asked to check for any problems and to inform next meeting
S3-000669	Proposed CR to 33.102: Corrections to Counter Check procedure	Nokia	10.1	Approval	S3-000726	revised in TD 726
S3-000670	UMTS Key Management	Telenor	10.7	Discussion / Decision		Delegates were asked to check for any problems and to inform next meeting
S3-000671	Proposed CR to 33.102: Intersystem handover for CS Services – from GSM BSS to UTRAN	Ericsson	10.1	Discussion		revised in TD727
S3-000672	Proposed LS to CN4 on SA3 agreements on MAPSec	Ericsson	10.7	Approval	S3-000735	revised in TD735
S3-000673	Protection Profiles for MAP Security	Ericsson	10.7	Discussion		LS in TD735
S3-000674	Algorithm Selection for MAP Security	Ericsson	10.7	Discussion		AES-Rijndael will be mandated for the Encryption algorithm. Rijndael (in MAC mode) should be used for the MAC algorithm
S3-000675	CR to 33.102: Additional parameters in AFR (Rel4)	Ericsson	10.1	Approval		Postponed for discussion
S3-000676	Proposed CR to GSM 03.35: IST implementation for non-CAMEL subscribers	Ericsson	12	Discussion		For e-mail approval by 8 December 2000
S3-000677	Report to SA3 from SA #9	Chairman	6.1	Information		Noted

S3-000678	Internet-based DoS attacks on UMTS network	Motorola	9.4	Discussion		Offline comments to list
S3-000679	Options for Access Security for IM Domain	Motorola	10.8	Discussion		To be studied further in SA WG3
S3-000680	Proposed CR to 33.102: Optional support for USIM-ME interface for GSM-only R99 ME	Siemens Atea	7, 10.1	Approval		not approved at this time
S3-000681	Rejection of non ciphered connections	France Telecom, Telia	10.1	Discussion / Approval		Mechanism agreed in principle as a working hypothesis
S3-000682	Problem with no USIM-ME interface in GSM-only ME	Siemens	7, 10.1	Discussion / Decision		Intro to TD680. Noted
S3-000683	IETF draft: A Roadmap for IPsec Policy Management	IETF	10.7	Information		Noted
S3-000684	IETF draft: IPSP Requirements	IETF	10.7	Information		Noted
S3-000685	IETF draft: IPsec Policy Architecture	IETF	10.7	Information		Noted
S3-000686	SA negotiation protocol for the ZA interface	Siemens	10.7	Discussion / Decision		Delegates were asked to check for any problems and to inform next meeting
S3-000687	Restricting the IPsec usage	Siemens	10.7	Discussion / Decision		Noted
S3-000688	Introduction of MAP security	Siemens	10.7	Discussion / Decision		Agreed. Reply LS to be drafted after study of cut-off date.
S3-000689	IMS authentication and integrity/confidentiality protection	Siemens	10.8	Discussion / Decision		Presented & discussed with TD699 and TD710.
S3-000690	Proposed CR to 33.102: START value handling for MS with a GSM SIM inserted	Vodafone	10.1	Approval	S3-000739	Revised in TD 739
S3-000691	Emergency call handling	Vodafone	9.5	Discussion		Postponed to next meeting

S3-000692	Changes to authentication data request message to enhance index value allocation in the AuC	Vodafone	10.1	Discussion		delegates to consider and contribute to next meeting
S3-000693	MExE security issues	Vodafone	9.3	Decision		TD704 refers
S3-000694	Extension of FIGS to the packet switched domain	Vodafone	8.3	Decision		Updated WI in TD745
S3-000695	Security aspects of UE conformance	Vodafone	9.6	Decision		Postponed to next meeting
S3-000696	Security workplan status report	Vodafone	8.1	Information		LS in TD742
S3-000697	Draft report of ad-hoc meeting 15bis version 0.0.3	Secretary	5	Approval		Endorsed
S3-000698	Calendar of 3GPP meetings	Secretary	11	Information		Noted
S3-000699	Authentication and protection mechanisms for IM CN SS	Ericsson	10.8	Discussion / Decision		Presented & discussed with TD689 and TD710.
S3-000700	3G TR 33.8xx V0.3.0	Ericsson	10.8	Information		Not dealt with (noted)
S3-000701	3G TS 33.2xx V0.1.1	Ericsson	10.8	Information		Not dealt with (noted)
S3-000702	Draft LS to SA WG2: Clarification on the role of the P-CSCF	Ericsson	10.8	Approval	S3-000755	revised in TD755
S3-000703	Using HTTP to distribute MAPsec SAs	Telenor	10.7	Discussion / Decision		use IKE between KACs working assumption. Need a mechanism for distribution between KACs and NEs, IPSec a working hypothesis for this. Key fetching to be revisited

S3-000704	LS from T WG2/MExE: MExE group comments to "MExE security issues" Vodafone document	T WG2/MExE	9.3	Discussion		MexE Security to be reviewed by SA WG3 and T WG2-MexE representatives to be invited to SA WG3 meeting (LS to be drafted)
S3-000705	Authentication framework and algorithm boundary conditions	ETSI EP TIPHON	10.8	Discussion		Noted
S3-000706	Extensions to TD36 for 3GPP security	ETSI EP TIPHON	10.8	Discussion		Noted
S3-000707	Subject: Correction on use of GSM MS classmark in UMTS	Nokia	10.1	Approval	S3-000729	revised in TD729
S3-000708	GERAN integrity protection	Nokia	9.1			GERAN to be asked for info.
S3-000709	Support of certificates in 3GPP security architecture	Nokia	10.8			Postponed
S3-000710	IMS authentication in both visited and home networks	Nokia	10.8			Presented & discussed with TD689 and TD699.
S3-000711	ROGUES MS-SHELL THREAT ANALYSIS (ANSI-41)	Lucent	6.5	Discussion		Noted
S3-000712	Discussion paper to “Re-transmission of authentication request using the same quintet”(S3-000578)	NTT DoCoMo, Gemplus	7	Discussion		Covered by TD713 discussion (noted)
S3-000713	Proposed CR to 33.102: Re-transmission of authentication request using the same quintet	NTT DoCoMo, Gemplus	7	Approval	S3-000725	Updated in S3-000725
S3-000714	Reply LS on GERAN integrity protection (S3z000032)	SAWG3 ad-hoc 15bis	9.1			Transmitted from ad-hoc (Noted)
S3-000715	Reply LS to CN WG4 on "Protection of GTP Messages using IPSec" (S3z000033)	SAWG3 ad-hoc 15bis	10.7			Approved
S3-000716	Revised Agenda for the meeting (rev of S3-000640)	Chairman	2	Approval		Approved
S3-000717	Withdrawn (replaced by single doc S3-000730)	SAGE	6.4			WITHDRAWN
S3-000718	Withdrawn (replaced by single doc S3-000730)	SAGE	6.5			WITHDRAWN
S3-000719	Withdrawn (replaced by single doc S3-000730)	SAGE	6.6			WITHDRAWN
S3-000720	Withdrawn (replaced by single doc S3-000730)	SAGE	6.7			WITHDRAWN

S3-000721	Agenda for joint session with T WG3	Chairman	7	Approval		Approved
S3-000722	TS 33.200	Editor		Approval		WITHDRAWN
S3-000723	Comments from K Holley on S3-000700	BT	10.8	Information		Not dealt with
S3-000724	Draft liaison statement to CN4 regarding Positive Authentication Reporting	Qualcomm		Approval		Approved
S3-000725	Proposed CR to 33.102: Re-transmission of authentication request using the same quintet (rev of S3-000713)	Drafting group	7	Approval		Approved
S3-000726	Proposed CR to 33.102: Corrections to Counter Check procedure (rev S3-000669)	Nokia	10.1	Approval		Approved
S3-000727	Proposed CR to 33.102: Intersystem handover for CS Services – from GSM BSS to UTRAN (rev S3-000671)	Ericsson	10.1	Discussion		Approved
S3-000728	Document re-allocated in error				S3-000739	WITHDRAWN
S3-000729	Subject: Correction on use of GSM MS classmark in UMTS (rev S3-000707)	Nokia	10.1	Approval		Approved
S3-000730	SAGE deliverables 1, 2, 3, 4	ETSI SAGE	6.4	Information		Replaces TDs 717-720. Noted. Chairman to recommend to SA#10 to approve for publication on the 3GPP server and to ask PCG to endorse them for publication by the Partner SDOs
S3-000731	Encryption Algorithms for MAP Security	Mitsubishi Electric, NTT DoCoMo	10.7	Discussion / Decision		WITHDRAWN
S3-000732	Reply LS to S3-000662: LS for "IM Subsystem Address Storage on USIM"	SA WG3		Approval	S3-000758	Revised in TD758
S3-000733	IPR statement	MCC	-	Information		Presented by Chairman
S3-000734	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

S3-000735	Proposed LS to CN4 on SA3 agreements on MAPSec (rev S3-000672)	Ericsson	10.7	Approval		Postponed
S3-000736	Proposal not to use the IMSI as the identity of an IM subscriber	Ericsson		Approval	S3-000759	Revised in TD759
S3-000737	Proposed LS to CN4 on SA3 agreements on MAPSec	Ericsson			S3-000760	Revised in TD760
S3-000738	Standardisation of security parameter bit ordering in USIM and AuC	Vodafone	12	Discussion		E-mail discussion after the meeting.
S3-000739	Proposed CR to 33.102: START value handling for MS with a GSM SIM inserted	Vodafone	10.1	Approval		Approved
S3-000740	LS to CN, cc: CN4 on Positive authentication reporting	Vodafone	6.2	Approval		Approved
S3-000741	LS to CN1, cc: T2/T3: Authentication request retransmission	Vodafone	10.1	Approval	S3-000761	Revised in TD761
S3-000742	LS to SA2, cc: CN4: Request for information to complete security work items	Vodafone	8.1	Approval		Approved
S3-000743	LS to T1, cc: CN1/RAN2: Security aspects of UE conformance testing	Vodafone	9.6	Approval		Postponed
S3-000744	LS to T2-MExE: MExE security issues	Vodafone	9.3	Approval		Postponed
S3-000745	Update to FIGS/IST work item description	Vodafone	8.3	Approval		Approved
S3-000746	Draft LS to GERAN about ciphering of RRLP messages between SMLC and MS in GPRS	Nokia/SA WG3		Approval		Approved
S3-000747	CR to 03.33: Addition of parameters to the X3-Interface	SA3-LI Group	6.3	Approval	S3-000762	Revised in TD762
S3-000748	CR to 33.107: Addition of parameters to the X3-Interface	SA3-LI Group	6.3	Approval	S3-000763	Revised in TD763
S3-000749	CR to 03.33: Deletion of mono-mode and addition of optimal routing	SA3-LI Group	6.3	Approval	S3-000764 S3-000765	Revised in TD764 and TD765 (one CR per Release)
S3-000750	Release 4 draft of TS 33.106	SA3-LI Group	6.3	Information		Noted
S3-000751	LS from LI group to SA WG3: Comments on TR 33.800	SA3-LI Group	6.3	Information		Noted
S3-000752	Proposed LS from LI / SA WG3 to CN WG4: Lawful Intercept support on the Mc interface	SA3-LI Group	6.3	Approval	S3-000766	revised in TD766
S3-000753	Presentation: Evaluation of IMS security architectures	Siemens		Discussion		Presented

S3-000754	draft-blom-rtp-encrypt-00 paper	Ericsson		Information		Supports S3-000699. Not provided at the meeting.
S3-000755	LS to SA WG2: Clarification on the role of the P-CSCF (rev of 702)	Ericsson	10.8	Approval		Approved. TD756 to be attached
S3-000756	S3z-000047 revised for attachment to S3-000755	SA WG3	10.8	Information		Attached to TD 755
S3-000757	LS for "Security risks in introduction phase of MAP security"	Siemens				Approved
S3-000758	Reply LS to S3-000662: LS for "IM Subsystem Address Storage on USIM "	SA WG3		Approval		Approved
S3-000759	Proposal not to use the IMSI as the identity of an IM subscriber	Ericsson		Approval		Approved
S3-000760	LS to CN4 on SA3 agreements on MAPSec (rev 737)	Ericsson		Approval		Approved
S3-000761	LS to CN1, cc: T2/T3: Authentication request retransmission	Vodafone	10.1	Approval		Approved
S3-000762	CR to 03.33: (R98) Addition of parameters to the X3-Interface	SA3-LI Group	6.3	Approval		Approved
S3-000763	CR to 33.107: Addition of parameters to the X3-Interface	SA3-LI Group	6.3	Approval		Approved
S3-000764	CR to 03.33 R98: Deletion of mono-mode and addition of optimal routing	SA3-LI Group	6.3	Approval		Approved
S3-000765	CR to 03.33 R99: Deletion of mono-mode and addition of optimal routing	SA3-LI Group	6.3	Approval		Approved
S3-000766	Presentation on Key Management in IETF	AT&T	10.7	Information		Presented and noted.
S3-000767	CR to 03.33 (R99): Addition of parameters to the X3-Interface	SA3-LI Group	6.3	Approval		Approved

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	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	

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

Note: Includes SA WG3 agreed CRs to be presented to TSG SA#10 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WG status	Remarks
03.33	002		R98	Addition of parameters to the X3-Interface	C	7.1.0	S3-16	S3-000762	agreed	Cat C but already covered by agreed LI requirements
03.33	003		R99	Addition of parameters to the X3-Interface	C	8.0.0	S3-16	S3-000767	agreed	Cat C but already covered by agreed LI requirements
03.33	004		R98	Deletion of mono-mode and addition of optimal routeing	F	7.1.0	S3-16	S3-000764	agreed	
03.33	005		R99	Deletion of mono-mode and addition of optimal routeing	A	8.0.0	S3-16	S3-000764	agreed	
33.102	129		R99	Corrections on ciphering and integrity protection	F	3.6.0	S3-16	S3-000666	agreed	
33.102	130		R99	Re-transmission of authentication request using the same quintet	F	3.6.0	S3-16	S3-000725	agreed	
33.102	131		R99	Corrections to Counter Check procedure	F	3.6.0	S3-16	S3-000726	agreed	
33.102	132		R99	Intersystem handover for CS Services – from GSM BSS to UTRAN	F	3.6.0	S3-16	S3-000727	agreed	
33.102	133		R99	Correction on use of GSM MS classmark in UMTS	F	3.6.0	S3-16	S3-000729	agreed	
33.102	134		R99	START value handling for MS with a GSM SIM inserted	F	3.6.0	S3-16	S3-000739	agreed	
33.105	015		R99	Layer 2 related corrections	F	3.5.0	S3-16	S3-000667	agreed	
33.107	001		R99	Addition of parameters to the X3-Interface	F	3.0.0	S3-16	S3-000763	agreed	

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD Number	Title	Source	Comment
S3-000642	Liaison to ETSI for forwarding to 3GPP TSG-SA3	Q24/4 Rapporteur group	To be discussed by the companies supporting the FIGs WI
S3-000644	LS on Increasing maximum number of bits to be enciphered with f8	ETSI SAGE 3GPP Task Force	Noted.
S3-000645	Liaison Statement to SA WG3 regarding ciphering of RRLP messages between the SMLC and MS in GPRS	TSG GERAN	Needs further consideration in SA WG3. Response LS to be drafted.
S3-000646	LS on positive authentication reporting	CN WG4	Noted. (PAR is a SA WG3 requirement)
S3-000647	LS on Positive Authentication Reporting	CN WG4	Response in TD740
S3-000648	LS on Security issues	RAN WG2	Noted (old LS, subject already dealt with).
S3-000649	Reply LS (to SA WG1) on Support of VHE User Profiles	SA WG2	Noted.
S3-000651	Draft LS on Integrity Protection in GERAN	TSG GERAN ad-hoc#2	Noted. A response from ad-hoc in TD714
S3-000655	LS from T WG3: Re-transmission of authentication request using the same quintet	T WG3	Mech. To be moved to ME. Response in TD725 Joint session with some T WG3 delegates requested
S3-000657	LS on Clarifications to the Security Mode usage, and error cases	CN WG4	Noted.
S3-000658	LS on Security for MAP over IP	CN WG4	Noted.
S3-000662	LS for "IM Subsystem Address Storage on USIM"	SA WG2	Further study needed. Info response in TD758
S3-000704	LS from T WG2/MExE: MExE group comments to "MExE security issues" Vodafone document	T WG2/MExE	MexE Security to be reviewed by SA WG3 and T WG2-MexE representatives to be invited to SA WG3 meeting (LS to be drafted)
S3-000705	Authentication framework and algorithm boundary conditions	ETSI EP TIPHON	Noted.
S3-000706	Extensions to TD36 for 3GPP security	ETSI EP TIPHON	Noted.
S3-000751	LS from LI group to SA WG3: Comments on TR 33.800	SA3-LI Group	Noted.

E.2 Liaisons from the meeting

TD Number	Title	Status	Comment
S3-000714	Reply LS on GERAN integrity protection (S3z000032)	Noted	Transmitted from ad-hoc
S3-000715	Reply LS to CN WG4 on "Protection of GTP Messages using IPSec" (S3z000033)	Approved	
S3-000724	Draft liaison statement to CN4 regarding Positive Authentication Reporting	Approved	

TD Number	Title	Status	Comment
S3-000740	LS to CN, cc: CN4 on Positive authentication reporting	Approved	
S3-000742	LS to SA2, cc: CN4: Request for information to complete security work items	Approved	
S3-000746	Draft LS to GERAN about ciphering of RRLP messages between SMLC and MS in GPRS	Approved	
S3-000755	LS to SA WG2: Clarification on the role of the P-CSCF (rev of 702)	Approved	TD756 to be attached
S3-000757	LS for "Security risks in introduction phase of MAP security"	Approved	
S3-000758	Reply LS to S3-000662: LS for "IM Subsystem Address Storage on USIM "	Approved	
S3-000759	Proposal not to use the IMSI as the identity of an IM subscriber	Approved	
S3-000760	LS to CN4 on SA3 agreements on MAPSec (rev 737)	Approved	
S3-000761	LS to CN1, cc: T2/T3: Authentication request retransmission	Approved	

Annex F: List of actions from the meeting

AP 16/01: **Chairman to report the development of A5/3 progress to SA Plenary and ask for agreement of the 3GPP Partners.**

AP 16/02: **Editor of 33.102 (M Blommaert) to check the points raised in TD S3-000655 when reviewing the document and take necessary actions.**

AP 16/03: **M Blommaert to review section 6.8 of 33.102 to see if text can be replaced by reference to the SIM/USIM Internal and External Interworking aspects draft TR (T WG3) for report to SA WG3#17 meeting.**

AP 16/04: **M Pope to add references to the SA WG3 WI sheets (on the FTP server) to the meeting report.**

AP 16/05: **Companies supporting FIGs should discuss the issues in ITU-T Rec. M.3210.1 for GPRS and IP domain, for input to ITU-T.**

AP 16/06: **C. Brookson to initiate an e-mail discussion on Internet-based DoS attacks and include agreements in TR 33.900.**

AP 16/07: **P. Howard to lead an e-mail discussion on Standardisation of security parameter bit ordering in USIM and AuC (TD S3-000738 as a basis).**

AP 16/08: **Chairman to ask TSG SA#10 to forward the TR 33.909 to PCG (if approved by TSG SA) for approval for publication by the Partner SDOs.**

AP 16/09: **Chairman to recommend to SA#10 to approve the SAGE deliverables (1, 2, 3 and 4) for publication on the 3GPP server and to ask PCG to endorse them for publication by the Partner SDOs.**

AP 16/10: **K. Bowman to initiate an e-mail discussion on IMS authentication and provide a mutually agreeable proposal to SA WG3 meeting #17.**