3GPP TSG SA WG3 (Security)   3GPP S3-99xxx
Stockholm, 23-26 March, 1999

Draft version 0.0.3
Draft Report of the 3GPP Security Meeting #2,
23-26 March 1999, Stockholm

The historic Vasa Museum, Stockholm

1   Welcome and introduction

Mr. Per Christoffersson welcomed delegates to Telia in Haninge, Stockholm and explained the domestic arrangements. A visit to the historic Vasa Museum had been arranged for an evenings entertainment.

The Convenor was Prof. M Walker, and the Secretary for this meeting was Mr. M. Pope.

2   Objectives of meeting

The Convenor, Prof. M. Walker, outlined the objectives of the meeting which are to have some output documents for the next 3GPP TSG meeting, to review the work programme and progress the work on items.

The schedule for the meeting was outlined as follows:

DAY	am/pm	SMG10	3GPP SA3
Tues 25/3	am	Opening Plenary	n/a
	pm	Working Parties	14.00 Start Plenary
		16.45 Plenary	(close 16.45)
Wed 26/3	am	09.00 LCS Presentation + Plenary	09.00 Editing Sessions
	pm	11.00 MExE Joint session	11.00 WPC/3GPP
		14.00 MExE WP Joint session	14.00 Threats and requirements
Thu 27/3	am	09.00 WPB /3GPP SS7 Mtg	09.00 WPB /3GPP SS7 Mtg
		11.00 WPs	11.00 Editing Session
	pm	Closing Plenary	16.00 Plenary
Fri 28/3	am	n/a	Plenary Close 12.30

3   Approval of agenda

The agenda, given in document **[TD S3-99038]** was presented and endorsed with some additions, as given in document **[TD S3-99071]**.

4   Assignment and registration of input documents

The document list was considered and items allocated to agenda items as appropriate. Although **[TD S3-99041]** was not available, most delegates were familiar with it. It was decided that this SMG10 document would be a useful input (for information) and that an equivalent document for SA3 would be created based upon this input. Strategic Decisions will be added to the agenda of future meetings.

> AP1/2:   Chairman to add Strategic Decisions to the agenda of future meetings.

5   Review relevant previous meetings and reports

5.1   S3 plenary, 2-4 February, London

Document **[S3-99043]** was considered. With a correction of an error to the Architecture schedule (1st release end March, rather than Complete end March):

Architecture	23/02/99	Bart Vinck	30	1st list of scope and contents by 12/2/99.	To be combined with Security Architecture as the first chapter.
	Stockholm	& Stefan Pütz		1st draft by end of February.	Adding SIM secure messaging, and that all the security features form the architecture, with examples.
				~~Complete 1st release end March 1999~~	
					Scope agreed as 023.

The list of action points from the previous meeting was reviewed:

> AP 1/1:   No response yet received from Mr. T. Metzger, a colleague of his from RegTP was expected to arrive later in the meeting.
>
> AP 2/1:   It had been clarified at the TSG meeting that no GSM documents are to be replaced, but equivalent documents may exist for UMTS, based upon SMG (GSM) documents. SMG are responsible for the maintenance of their documents, which needs to be done via the CR mechanism.
>
> AP 3/1:   The document reference is incorrect (should be **[S3-99015]**), but the action had been completed. The Liaison statement is contained in document **[S3-99040]** for information.
>
> AP 4/1:   Completed (timetable for deliverable deadlines noted by editors).
>
> AP 5/1:   Complete. Presentation slides were input to TSG meeting #2.

Liaison statements:

LS 1:   This liaison was produced and sent.

5.2   S3 architecture ad hoc, 23 February, Stockholm

Document **[S3-99052]** contains the report of the ad-hoc meeting and was presented to the meeting. The user identity confidentiality section (5.1) asks about mandatory/optional features. It was recommended that the features are specified by the group and mandatory/optional discussions should be done at a later stage, in order to not lose time with continually changing mandatory/optional discussions at an early stage. Entity authentication (section 5.5) should be considered by delegates for discussion in the Thursday Plenary session, document **[S3-99063]** is an input on this subject. SS7 Security issues (section 5.6) will be raised in the joint meeting on SS7 on Thursday morning.

6   Reports/liaisons from other WG's, TSG's (including TSG plenary, 1-5 March, Fort Lauderdale

Document **[S3-99039]** was approved at TSG SA meeting#2. Mr. Pope was asked to process the document to produce a well formatted deliverable for 3GPP.

> AP2/2:   Mr. Pope to process Document [S3-99039] and produce a 3GPP formatted deliverable.

The Convenor presented the report of the TSG SA Meeting #2 given in document **[S3-99060]**, which he had sent to members of SA3 during the meeting.

Documents **[S3-99044], [S3-99045], [S3-99046] and [S3-99047]** were input for information and were noted by the meeting (reports of TSG Meetings #2).

There was some concern over the liaison between SMG1 and SA WG1 on the use of SIM and USIM. The convenor will obtain the relevant document and SMG1 will be asked to produced a revised statement to clarify the real requirements to SA WG1.

> AP3/2:   Chairman to ask SMG1 Chairman to produce a revised statement of requirements from SMG1.

The Architecture group was asked to tackle the high priority work on Radio Access Security work, as TSG RAN are working at a very fast pace.

Document **[S3-99057]** was summarised. A "no-service" mobile (which only registers with the network, but has no service) is the basis of a generic mobile equipment. Other groups would then define services which can be added in a modular way. The architecture WP was asked to consider this.

Document **[S3-99058]** is an expansion on the 2-stage process as described in Document **[S3-99057]**. The document was noted.

The suitability of the A5 algorithm for the wideband air interface was discussed, and it was generally thought inadequate for this application.

> AP4/2:   Chairman to write to TSG T pointing out that A5 is not suitable for the wideband air interface.

Document **[S3-99059]** - meeting report on Terminal capabilities ad-hoc. This document was noted.

Document **[S3-99068]** - Liaison statement from TSG T WG3 on USIM integrity check. This was noted by the meeting and the architecture group was asked to consider the document.

7   Reports/liaisons from non-3GPP organisations

Documents **[S3-99055] [S3-99056]** and **[S3-99070]** (SS7 related inputs) were noted and were dealt with in the joint SS7 meeting.

8   Review status of deliverables

Documents **[S3-99048]** - Security threats and requirements, V0.0.1. This is for production of a first draft for release at the end of March 1999 as version 2.0.0. Per Christoffersson introduced the document highlighting the changes made (mainly small changes to threat analysis). The document keeps the spirit of UMTS 33.21. Delegates were asked to carefully read this document and a thorough review will be made on Wednesday afternoon for final editing.

Document **[S3-99051]** - Security architecture, V0.1.2. This is for production of a first draft for release at the end of March 1999 as version 2.0.0. The document was introduced by the editor, Stefan Puetz. The annexes are not yet completed (requirements analysis and TETRA authentication mechanism). It was proposed to review the sections which are almost complete and add the text to the sections which are incomplete (5.1 and 5.3) during the editing sessions. Section 7 was expected as an output of the joint SS7 meeting. Active involvement by delegates at the drafting sessions was requested in order to fulfil the timescale. Approval is expected to be by correspondence after the meeting. Document **[S3-99063]** contains input to sections 6.3 and 6.4.

A First draft (ToC and Scope) of the Integration requirements document was expected at end of this meeting (not for release at this meeting).

Document **[S3-99049]** - Cryptographic algorithm requirements. A first draft (Toc & Scope) was expected at end of this meeting (no release). Mr. Chikazawa introduced the document which is intended for ETSI SAGE to use to choose the appropriate cryptographic algorithm. The document is based on ETSI Algorithm requirements specifications, except for section 6. Section 6.1 was passed to the Architecture group for review. Comments should be passed to Mr. Chikazawa in written form for update of the document, for final collation at SMG10 plenary later in the week.

Document **[S3-99050]** - Lawful Interception requirements document. A first draft (Toc & Scope) was expected at end of this meeting (no release). The draft required an editing session to add input to the document. The Handover Interface specifications for each Partner region need to be identified and included in order to allow a more global specification.

Architecture & Functions document - There was nothing to do at this meeting.

Guide to 3G Security Features document - A first draft (ToC & Scope) was expected at end of this meeting (no release).

9   Election of Chair and two Vice-Chairs

At the start of the meeting there was one Candidate for Chairman of TC Security (Prof. M. Walker) **[S3-99053]** and one for Vice-Chairman (Dr. S. Peutz) **[S3-99042]**.

The Convenor asked if there were any other candidates for Chairman. None were signalled and **Prof. Michael Walker was elected as Chairman of TSG SA WG3 by acclamation.**

The Convenor asked if there were any other candidates for Vive Chairman. None were signalled and **Dr. Stefan Peutz was then elected as a Vice Chairman of TSG SA WG3 by acclamation.**

Consideration from other regional representatives was requested for the second post of Vice-Chairman. **Mr. Adam Berenzweig presented his candidature [S3-99086] and was elected as Vice Chairman by acclamation.**

10   Enhanced identity confidentiality

Document **[S3-99067]** was introduced. This topic had been discussed in an ad-hoc group and it was proposed to include 2 annexes in the Security Architecture document, one with the IMSI encrypted using a symmetrical encryption algorithm (preferred option), and one where the IMSI is sent in clear.

It was decided that this approach covers the requirements, and that Lawful Interception requirements should be kept in mind. Regulators were asked to ensure that these requirements are interpreted for the 3GPP documents to ensure that it is included in the documents at an early stage of their development.

10.1   End-to-end encryption

Document **[S3-99054]** was introduced. This gives some thoughts on the end-to-end encryption requirements and describes a scheme for key management and ciphering, assuming transcoder-free operation and no tromboning for UMTS calls. It had been checked that the system would not fall under export control restrictions. After some discussion to clarify the proposals, it was decided to take this as a basis for a feature to be included in the Security Architecture document for UMTS, restricted to same network calls. The system has been designed to fulfil the Lawful Interception requirements and contains the same interface as used for GSM. Work on the feature will be contribution-driven and Vodafone undertook to make contributions. Some support was offered (Telia) to try to enhance this feature to cover roaming and inter-networks cases (if resources can be found).

Nokia were concerned that the short timescales to complete this work may have impact on the completion of the other features and wished some prioritisation of the work.

The term "end-to-end" encryption was not considered correct for this service as described, and another name should be considered to better define the system.

It was decided to send a liaison statement to TSG SA, copied to SA WG1 (Services) informing them of the security features in the Architecture document (**[S3-99087]**).

> AP5/2:   Chairman to produce a liaison statement to TSG SA, copied to SA WG1 informing them of the Security Features.

10.2   Lawful Interception

Document **[S3-99050]** contains the LI document. There was not time to edit the document at the editing sessions and the editor undertook to update the document and circulate it by the end of March 1999. Comments and enhancements should be sent by e-mail for inclusion in the document. The document was considered during the plenary session and some comments taken. Mr. Brookson will endeavour to find the relevant LEA requirements documents for other Partner Organisations (Clause 5). The document should also be updated to include packet-oriented data, etc. as it is currently mainly circuit-switched orientated.

Specification work for Lawful Interception will be done in joint sessions with SMG10 WPD. A liaison will be sent to SMG10 WPD requesting this (**[SP-99090]**).

> AP6/2:   Chairman to include the request for joint SMG10 WPD meeting on LI into the report to SMG#29..

> AP7/2:   All editors to ensure that documents for submission to TSG SA are sent to Mr. Pope in good time for formatting into the required 3GPP presentation and allocation to the TSG meeting as Temporary Documents.

11   Methods for algorithm design

Document **[S3-99065]** requests ciphering algorithms to be produced in time for the launch deadline for 3G service in Japan, proposing that the GPRS GEA algorithm is standardised first. A question about the expected channel characteristics was asked, but this has not yet been evaluated. Without a requirement specification, it was thought difficult to choose a specific algorithm until the requirements are known. The document was noted by the meeting.

Document **[S3-99075]** contains the draft cryptographic algorithm specification. A presentation **[S3-99088]** was given by Mr. R. Blom (Ericsson), which gives a summary of the document.

Some discussion over the choice of Open verses Secret or Dedicated algorithms took place. It was thought that a dedicated algorithm, which receives a closed evaluation (possibly) followed by an open evaluation and the drafting of the specification.

The following will be proposed to TSG SA:

SA WG3 need to create the requirements specification, which will be passed to an algorithm design group (e.g. ETSI SAGE) for design, or selection of an algorithm, followed by a commissioned, closed evaluation of the algorithm and finally production of the 3GPP specification. Public evaluation will be decided upon later, and will run in parallel with the implementation phase, due to the timescale requirements. (It is recognised that an open evaluation will leave any algorithm open for continuous criticism, which will need to be managed).

12   Sub-groups to proceed work on deliverables

12.1   Threats and requirements

Mr. Christoffersson presented the report of the editing session, which took document **[S3-99048]** as an input. The updated document is available in **[S3-99089]**.

Document **[S3-99079]** was presented by Motorola, for discussion of the use of the GSM SIM in a UMTS Terminal. Some discussion over the use of a GSM SIM to access the UMTS Network occurred. It was

clarified that the GSM SIM will only gain access to GSM service level, and that the protection of the UMTS Network needs to be studied.

The document was agreed as a statement of the SMG10 understanding of the service requirements. It was agreed to liaise this to SMG#29, SMG1, TSG SA, TSG SA WG1 (attaching the liaison to SMG10 which was attached to Tdoc SMG10 AP99-XXX). The liaison was allocated to document **[SP-99080]**.

12.2   Architecture

Following the drafting sessions, a proposed LS to RAN WG2 was presented. The Liaison outlines the working assumptions of SA WG3 and requests a joint meeting with RAN WG2 to work on ciphering mechanism design. The liaison was updated and approved as **[S3-99081]** and will be sent to TSG RAN WG2.

Other issues discussed was Key lifetime, but no resolution was obtained and further discussion is needed.

User Authentication mechanisms: a stable specification for 3G security architecture was targeted as an output of this meeting. There are two proposals which are causing delays. Some concerns over the robustness of the preferred mechanism was expressed, and a fall-back mechanism was requested, as well as more time to investigate the mechanism. Further discussion at the SMG10 Plenary was requested.

Discussion in Plenary came to the conclusion that the working hypothesis will be to choose the preferred mechanism (Signed Challenge), and keep the other mechanism as a back-up in case of problems with the mechanism, which will be added as an Annex to the document. Both mechanisms will need continued evaluation. The mechanism will be reviewed at the next meeting.

More active participation was requested from the members of the group in order to progress the work in the very short timescales.

12.3   Other sub-groups, as considered necessary

No other sub-groups met at this meeting.

13   Review work of sub-groups and outputs of meeting

The sub-group and editing session reports are given in documents **[S3-99089]** and **[S3-99085]**.

Liaison statements:

Input liaison statements:

Doc. Ref.	Title	Received from	Status: Response / Dates	Comment
S3-99015	Variable length of USIM parameters	T WG3	Response S3-99040	Meeting SA3_01
S3-99057	TSG T review of Terminal Capabilities	TSG T	Noted	Meeting SA3_02
S3-99068	Response from USIM group on Integrity Check (T3-99088)	T WG3	Noted	Meeting SA3_02
S3-99069	The variation of authentication parameter length	CN WG2		Meeting SA3_02
S3-99076	Radio Interface ciphering	RAN WG2		Meeting SA3_02
S3-99077	Timetable for decision on ciphering	RAN WG2		Meeting SA3_02
S3-99078	Ciphering and ARQ dependencies in UTRAN	RAN WG3		Meeting SA3_02
S3-99083	Integrity check by the USIM (reply to S3-99040)	TSG T WG3		Meeting SA3_02
S3-99092	Security Requirements for UMTS Release 99	TSG SA WG1	Received 31 March 1999	For e-mail approval

Output liaison statements:

Doc. Ref.	Liaison Statement Number	Title	Sent to:	Status: Sent / Dates
S3-99040	LS-001	integrity on the USIM	TSG T WG3	Sent 11 March 1999
S3-99080	LS-002	GSM/USIM Interworking	SMG, SMG1, TSG SA and TSG SA WG1	Sent 31 March 1999
S3-99081	LS-003	Security functionality in the RAN	TSG RAN WG2	Sent 31 March 1999
S3-99087	LS-004	Security Features in the Architecture document	TSG-SA	
S3-99090	LS-005	Joint meetings for LI work	SMG10 WPD	

14   AoB

Work programme: Mr. Brookson will update the work programme in line with the progress made so far and will send to Mr. Pope for updating of the 3GPP Work Plan.

> AP8/2:   Mr. Brookson to send an updated work programme to Mr. Pope for updating of the 3GPP Work Plan.

15   Next meeting

The planning for the next meeting needs to e changed due to the TSG SA meeting schedule. The following dates were agreed:

SA3#03   11 - 12 May in Bonn, Germany (Changed from 27-28 April due to TSG SA#3 meeting).

SA3#04   17 - 18 June in UK

SA3#05   3 - 6 August - venue to be decided. (co-located with SMG10)

SA3#06   26 - 27 October in The Hague, Netherlands

SA3#07   16 - 19 November - venue to be decided (co-located with SMG10)

SA3#08   7 - 8 December in Helsinki or Lapland, Finland

16   Close of meeting

The Chairman thanked the hosts for their excellent facilities and the delegates for their committed and constructive work during the meeting, and closed the meeting.

ACTION POINT LIST - Meeting # 2.

AP1/2:   Chairman to add Strategic Decisions to the agenda of future meetings.

AP2/2:   Mr. Pope to process Document [S3-99039] and produce a 3GPP formatted deliverable.

AP3/2:   Chairman to ask SMG1 Chairman to produce a revised statement of requirements from SMG1.

AP4/2:   Chairman to write to TSG T pointing out that A5 is not suitable for the wideband air interface.

AP5/2:   Chairman to produce a liaison statement to TSG SA, copied to SA WG1 informing them of the Security Features.

AP6/2:   Chairman to include the request for joint SMG10 WPD meeting on LI into the report to SMG#29.

AP7/2:   All editors to ensure that documents for submission to TSG SA are sent to Mr. Pope in good time for formatting into the required 3GPP presentation and allocation to the TSG meeting as Temporary Documents.

AP8/2:   Mr. Brookson to send an updated work programme to Mr. Pope for updating of the 3GPP Work Plan.

Technical Specification Group Services and System Aspects **TSGS#3(99)117**
Meeting #3, Yokohama, Japan, 26-28 April 1999
Annex A: List of participants

attendee list   3GPP SA WG3 (Security) Meeting #2

		Person's name:		email	Organisation name, status, partner and Role				
1	Mr.	Wael	Adi	wadi@tu-bs.de	BOSCH TELECOM DANMARK A/S	3GPPMEMBER	ETSI	DK	
2	Mr.	Nigel	Barnes	tuk1107@email.mot.com	MOTOROLA Ltd	3GPPMEMBER	ETSI	GB	
3	Mr.	Adam	Berenzweig	madadam@lucent.com	Lucent Technologies	3GPPMEMBER	T1	US	
4	Mr.	Colin	Blanchard	colin.blanchard@bt.com	BT	3GPPMEMBER	ETSI	GB	
5	Mr.	Rolf	Blom	rolf.blom@era.ericsson.se	ERICSSON L.M.	3GPPMEMBER	ETSI	SE	
6	Mr.	Charles	Brookson	cbrookson@iee.org	DTI	3GPPMEMBER	ETSI	GB	
7	Mr.	Takeshi	Chikazawa	chika@isl.melco.co.jp	Mitsubishi Electric Co.	3GPPMEMBER	ARIB	JP	
8	Mr.	Per	Christoffersson	per.e.christoffersson@telia.se	TELIA AB	3GPPMEMBER	ETSI	SE	
9	Mr.	Stefano	Faccin	stefano.faccin@research.nokia.com	Nokia Telecommunications Inc.	3GPPMEMBER	T1	US	
10	Mr.	Reiner	Gusenburger	reiner.gusenburger@regtp.de	BMWi	3GPPMEMBER	ETSI	DE	
11	Mr.	Guenther	Horn	guenther.horn@mchp.ciemens.de	SIEMENS AG	3GPPMEMBER	ETSI	DE	
12	Mr.	Peter	Howard	peter.howard@vf.vodafone.co.uk	VODAFONE Group Plc	3GPPMEMBER	ETSI	GB	
13	Mr.	Hans	Lindgren	hans.lindgren@era.ericsson.se	ERICSSON L.M.	3GPPMEMBER	ETSI	SE	
14	Mr.	Bernie	Mckibben	p17982@email.mot.com	MOTOROLA GmbH	3GPPMEMBER	ETSI	DE	
15	Mr.	Sebastien	Nguyen Ngoc	sebastien.nguyenngoc@cnet.francetelecom.fr	France Telecom	3GPPMEMBER	ETSI	FR	
16	Mr.	Christos	Nicolacacos	christos.nicolacacos@panasonic-pmdc.co.uk	PANASONIC MOBILE COMMUNICATION	3GPPMEMBER	ETSI	GB	
17	Mr.	Maurice	Pope	maurice.pope@etsi.fr	ETSI	3GPPORG_REP	ETSI	FR	Secretary
18	Dr.	Stefan	Pütz	stefan.puetz@t-mobil.de	Deutsche Telekom MobilNet	3GPPMEMBER	ETSI	DE	
19	Mr.	Roberto	Quattrini	roquattrini@tim.it	TELECOM ITALIA S.p.A.	3GPPMEMBER	ETSI	IT	
20	Mr.	Harri	Rasilainen	harri.rasilainen@etsi.fr	TELECOM. ADMIN. CENTRE	3GPPMEMBER	ETSI	FI	
21	Mr.	Gert	Roelofsen	g.roelofsen@research.kpn.com	KPN	3GPPMEMBER	ETSI	NL	
22	Mr.	Vesa	Tervo	vesa.tervo@nmp.nokia.com	NOKIA Mobile Phones Ltd	3GPPMEMBER	ETSI	GB	
23	Mr.	Benno	Tietz	benno.tietz@d2privat.de	MANNESMANN Mobilfunk GmbH	3GPPMEMBER	ETSI	DE	
24	Mr.	Marco	Tosalli	marco.tosalli@cselt.it	TELECOM ITALIA S.p.A.	3GPPMEMBER	ETSI	IT	
25	Mr.	Peter	Trautmann	peter.trautmann@regtp.de	BMWi	3GPPMEMBER	ETSI	DE	
26	Mr.	Bart	Vinck	bart.vinck@vnet.atea.be	SIEMENS ATEA NV	3GPPMEMBER	ETSI	BE	
27	Prof.	Michael	Walker	mike.walker@vf.vodafone.co.uk	VODAFONE Group Plc	3GPPMEMBER	ETSI	GB	Chairman
28	Mr.	Timothy	Wright	timothy.wright@vf.vodafone.co.uk	VODAFONE Group Plc	3GPPMEMBER	ETSI	GB	

Annex B: List of Documents

Number	Title	Source	Agenda item	Replaced by Tdoc
S3-99038	Agenda for 3GPP Security, 23-26 March, 1999, Stockholm	M Walker - Convenor	3	S3-99071
S3-99039	Security Principles and Objectives as approved at Fort Lauderdale	Secretary	8	
S3-99040	LS to T3 on integrity on the USIM	T Wright, Vodafone	for info	
S3-99041	Strategic decisions document	T Wright, Vodafone		
S3-99042	Candidature for Vice Chairman SA WG3 (Dr. Stefan Pütz)	DeTeMobil	9	
S3-99043	Report of TSG SA WG3 meeting #1 (2-4 Feb 99, London, UK)	Secretary	5.1	
S3-99044	Draft Report TSG-SA Meeting #2, 2-4th March 1999, V 0.0.5	SA Secretary	6	
S3-99045	Report of TSG-CN Meeting #2, 2-4th March 1999	CN Secretary	6	
S3-99046	Draft Report from TSG-T Meeting #2, 2-4th March 1999	T Secretary	6	
S3-99047	Draft report of 2nd TSG RAN Meeting #2, 2-4th March 1999	RAN Secretary	6	
S3-99048	3G Security: Security Threats and Requirements Version 0.0.1	P Christoffersson	8, 12.1	
S3-99049	3G Security: Cryptographic Algorithm Requirements (Ver 0.0.1)	Takeshi Chikazawa	8	
S3-99050	Lawful Interception requirements	Editor	8	
S3-99051	3G security architecture	Stefan Puetz	8, 12.2	
S3-99052	Report Ad-hoc meeting on "3G Security: Security Architecture" specification	Siemens Atea	5.2	
S3-99053	Candidature for Chairman SA WG3 (Pr. Michael Walker)	Vodafone	9	
S3-99054	Some initial thoughts on end-to-end encryption	Vodafone	10.1	
S3-99055	Minutes of SS7 Security Group Meeting Chippenham Wilts	SMG10 WPB	7	
S3-99056	SS7 NETWORK SECURITY THREAT ANALYSIS	SMG10 WPB	7	
S3-99057	3GPP TSG-T is reviewing Terminal Capabilities	3GPP TSG-T Vice-Chairman	6	
S3-99058	Draft Proposed WI for Terminal capabilities	3GPP TSG-T	6	
S3-99059	Meeting Report from the ad hoc meeting on terminal capabilities	3GPP TSG-T	6	
S3-99060	Notes from 3GPP TSG Meeting Fort Lauderdale, 2-4 March 1999	Convenor	6	
S3-99061	Ciphering Models	Ericsson	12.2	
S3-99062	Radio Interface ciphering	Nokia	12.2	
S3-99063	3G security architecture (Sections 6.3 - 6.4)	T-Mobil	8, 12.2	
S3-99064	Work Item Status List for TSG SA WG3 (Security)	3GPP Support group	8	
S3-99065	Deadline time for specification of the first 3G ciphering algorithm	Nokia	11	
S3-99066	Position of integrity protection mechanism	Nokia	12.2	
S3-99067	Enhanced user identity confidentiality	Ericsson	10	
S3-99068	Response from USIM group on Integrity Check (T3-99088)	T WG3	6	
S3-99069	The variation of authentication parameter length	CN WG2	12.2	
S3-99070	A proposal for SS7 based Transmission of Sensitive data between Network Elements	T-Mobil	7	
S3-99071	Agenda for 3GPP Security, 23-26 March, 1999, Stockholm (revised at meeting)	M Walker - Convenor	3	
S3-99072	Agenda for the editing sessions on the 3G security architecture	Rapporteurs	12.2	
S3-99073	Draft section on user domain security	Siemens Atea	12.2	
S3-99074	Extracts from UMTS 23.20 V1.5.0		12.2	
S3-99075	3G Security Cryptographic algorithm specification V1.0.0	Gert Roelofsen	12.2	
S3-99076	Radio Interface ciphering	RAN WG2	12.2	
S3-99077	Timetable for decision on ciphering	RAN WG2	12.2	
S3-99078	Ciphering and ARQ dependencies in UTRAN	RAN WG3	12.2	
S3-99079	Discussion document on GSM/UMTS "Interworking" with regard to SIM and USIM	Motorola	12.1	
S3-99080	Liaison statement to SMG, SMG1, TSG SA and TSG SA WG1 on GSM/USIM Interworking	SA WG3	12.1	
S3-99081	LS to RAN WG2 on Security functionality in the RAN	SA WG3	12.2	
S3-99082	Mobile Equipment Identity (Terminal Identity Module)	Bosche Telecom		
S3-99083	LS to TSG-SA3 on integrity check by the USIM (reply to S3-99040)	TSG T WG3		
S3-99084	3G Security cryptographic algorithm requirements version 0.0.2	Mitsubishi Electric		
S3-99085	Report of editing sessions			
S3-99086	Candidature for Vice Chairman SA WG3 (Mr. Adam Berenzweig)	Lucent Technologies	9	
S3-99087	LS to TSG-SA on Security Features in the Architecture document	SA WG3 Chairman	10.1	
S3-99088	Presentation on draft cryptographic algorithm document	R. Blom, Ericsson	11	
S3-99089	3G Security: Security Threats and Requirements - revision to Version 0.0.1	Per Christoffersson	12.1	
S3-99090	Liaison statement to SMG10 WPD concerning joint meetings for LI work	SA WG3	10.2	
S3-99091	Liaison statement from SA WG1 on Security Requirements for UMTS Release 99	SA WG1	e-mail	S3-99092
S3-99092	Liaison statement from SA WG1 on Security Requirements for UMTS Release 99	SA WG1	e-mail	