

Meeting #9, Helsinki, 7-9 December, 1999

Source: Secretary TSG SA WG3 (Ansgar Bergmann)**Title: Report of TSG SA WG3 Meeting #9 - draft 04****Table of contents**

1	Opening of the meeting; general	3
3	Registration of input documents and assignment of input documents to agenda items	3
4	Approval of meeting reports; action points from earlier meetings	3
5	Reports / Liaisons from other 3GPP and SMG groups.....	4
5.1	TSG-SA plenary and WGs	4
5.2	TSG-CN, TSG-RAN, TSG-T and WGs	4
5.3	SMG plenary	4
5.4	SMG STCs.....	4
5.5	3GPP partners and their bodies	4
5.6	Others (GSMA, GSM2000, T1P1, SAGE, TIA TR-45, etc.).....	4
6	2G security issues	5
6.1	GPRS	5
7	Review of 3G security project plan	5
8	3G security issues	5
8.1	Confidentiality/integrity algorithm.....	5
8.2	Authentication algorithm.....	5
8.3	Terminal security	5
8.4	GLR security review.....	5
8.5	Presentation from S2 on mobile IP	5
9	Review of CRs to TS 3G 33.102	5
10	Review of CRs to TS 3G 33.103	8
11	Review of CRs to other 3G specifications.....	8
11.1	TS 3G 33.106.....	8

11.2	TS 3G 21.133.....	8
11.3	CRs to TR 3G 33.902	8
11.4	TS 3G 33.105.....	8
11.5	TR 3G 33.120	8
11.6	TR 3G 33.901	8
11.7	TS 3G 22.022.....	9
12	Review of draft 3G specifications	9
12.1	TS 3G 33.107.....	9
12.2	TR 3G 33.900	9
12.3	TS 3G 33.048.....	9
13	Update 3G security project plan	9
14	Any other business	9
15	Approval of liaison statements, CRs and draft specifications	9
16	Future meetings dates and venues	10
17	Close of meeting.....	11

1 Opening of the meeting; general

The meeting was chaired by S3 Vice Chairman Michael Markovici who thanked Nokia for hosting the group.

2 Approval of the Agenda

The agenda in S3-99500 was approved:

- 1 Opening of the meeting**
- 2 Approval of the agenda**
- 3 Registration and assignment of input documents**
- 4 Approval of meeting reports**
 - 4.1 TSG-SA3 Meeting no. 8 (joint with SMG10)
- 5 Reports / Liaisons from other 3GPP and SMG groups**
 - 5.1 TSG-SA plenary
 - 5.2 TSG-CN, TSG-RAN, TSG-T and WGs
 - 5.3 SMG plenary
 - 5.4 SMG STCs
 - 5.5 3GPP partners and their bodies
 - 5.6 Others (GSMA, GSM2000, T1P1, SAGE, TIA TR-45, etc.)
- 6 2G security issues**
 - 6.1 GPRS
- 7 Review 3G security project plan**
- 8 3G security issues**
 - 8.1 Confidentiality/integrity algorithm
 - 8.2 Authentication algorithm
 - 8.3 Terminal security
 - 8.4 GLR security
 - 8.5 Presentation from TSG-S2 on mobile IP
- 9 Review of CRs to 3G TS 33.102, Security architecture**
- 10 Review of CRs to 3G TS 33.103, Integration guidelines**
- 11 Review of CRs to other 3G specifications**
 - 11.1 TS 33.106, Lawful interception requirements
 - 11.2 TS 21.133, Security threats and requirements
 - 11.3 TR 33.902, Formal analysis of security mechanisms
 - 11.4 TS 33.105, Cryptographic algorithm requirements
 - 11.5 TS 33.120, Security principles and objectives
 - 11.6 TR 33.901, Criteria for cryptographic algorithm design process
- 12 Review of draft 3G specifications**
 - 12.1 TS 33.107, Lawful interception architecture
 - 12.2 TR 33.900, Guide to 3G security
 - 12.3 TS 33.048, Security mechanisms for the USIM application toolkit
- 13 Update 3G security project plan**
- 14 Any other business**
- 15 Approval of liaison statements, CRs and draft specifications**
- 16 Future meetings dates and venues**
- 17 Close of meeting**

3 Registration of input documents and assignment of input documents to agenda items

See Annex A.

4 Approval of meeting reports; action points from earlier meetings

[The S3#8 meeting report in S3-99499 was approved by S3#9.](#)

The action points from earlier meetings were closed except:

- ✍ **Charles Brookson to draft some text for a press release, making a wider public aware of the 3GPP security specifications: This should be done after SA#6.**
- ✍ **CR to 03.20, LS to GSMA on usage of A5/1 for CTS.**
- ✍ **Further work identified: To elaborate 33.102 annex A.**
- ✍ **GSM 03.48 has to be transformed into a 3GPP specification.**
- ✍ **It was agreed**
 - **to review the main specifications in S3#10;**
 - **to ask S2 to identify the other relevant specifications, so that they can be studied;**
 - **S3 will then try to identify missing aspects in spring 2000.**
 - **Mike Walker will contact the S2 chairman and the co-ordination group.**
 - **A corresponding new section 3.4 will be added to 3G PD 30.810, Project plan for security.**

5 Reports / Liaisons from other 3GPP and SMG groups

5.1 TSG-SA plenary and WGs

S2-99E05 = R2-99g79: This LS on RAN2 LS on Emergency calls using IMEI as UE Identifier had been considered by S2 as being relevant to S1 and S3 rather than S2 and had been forwarded by S2 to S1 and S3 as S2-99E05.

[S3-99554, LS to SA, SA2, CN and CN OSA ad-hoc on Statement on security issues in VHE/OSA \(answer to S2-99E05 = R2-99g79\), was approved.](#)

5.2 TSG-CN, TSG-RAN, TSG-T and WGs

✍ **T2-991036, a LS from T2 to SMG10, S3, cc: SMG9, on Possible security issues with handsets supporting a user input storage mechanism, was postponed to S3#10.**

T2-991082, a LS from T2 to S3, S1, cc. T3, on *Reply to LS on additional Terminal Baseline Implementation Capabilities*, was noted by S3#9.

✍ **S3-99526 (= T3-99413), a LS from T3 on USIM-Terminal link, was postponed to S3#10.**

5.3 SMG plenary

SMG#30bis did not deal with S3 or SMG10 related issues.

5.4 SMG STCs

No input had been received.

5.5 3GPP partners and their bodies

No input had been received.

5.6 Others (GSMA, GSM2000, T1P1, SAGE, TIA TR-45, etc.)

GSMA, GSM2000: Neither GSMA nor GSM2000 had had a meeting between S3#8 and S3#9.

T1P1: No information had been received from T1P1.

SAGE: No information had been received from SAGE. A LS to SAGE

TR-54: Bart Vinck reported on TR-54 activities. See LS in S3-99527.

[An answer to S3-99527 in S3-99551 was approved.](#)

 **To draft a LS to SAGE as Tdoc S3-99556 (rev. of S3-99523).**

6 2G security issues

6.1 GPRS

Mike Walker has sent a letter to ETSI DG explaining that manufacturers had difficulties to get GEA2. Lucent reported at S3#9 that they still have not yet received the algorithm.

 **S3-99546 and S3-99547, CRs on applicability of ciphering for GPRS, both source: SMG10 WPA Chairman, were postponed to S3#10.**

7 Review of 3G security project plan

See section 13.

8 3G security issues

8.1 Confidentiality/integrity algorithm

No input received.

8.2 Authentication algorithm

S3-99509 presents the cipher algorithm Shazam, which has been approved by TIA TR-45.AHAG. This document was presented to S3 for information and consideration as a potential 3GPP and/or GPRS Block Cipher algorithm.

The document was noted.

S3-99523, source Vodafone, discusses authentication algorithm requirements. Preference is given to ask SAGE to specify a single algorithm with exchangeable building blocks rather than to ask SAGE to work out a framework and building blocks.

8.3 Terminal security

 **S3-99510, 3GPP terminal identity security: levels, requirements and mechanisms, source: Bosch, was postponed to S3#10.**

 **Drafting of the updated CRs on terminal security (due for SMG#31) was postponed to S3#10.**

8.4 GLR security review

No input had been received.

8.5 Presentation from S2 on mobile IP

The presentation in S3-99495 was given by Anders Hansmats. 3G 23.923 V1.2.0 was available as S3-99494.

9 Review of CRs to TS 3G 33.102

S3-99512: this CR on SQN_{LO} raises the problem that a Location update request message only has 2 unused octets left and that application of normal encoding rules would require a TLV coding (consuming 2 octets for coding purposes without leaving a value part). It proposes to remove the support for window

and list mechanisms from TS 33.102. The CR was considered superseded by the agreed CRs on the issue, see below.

S3-99501, CR to section 6.3 on Authentication and key agreement, source: Siemens, S3-99503, CR to annex F on Authentication and key agreement, and S3-99504, S3-99513, CR on Sequence Counter (SEQ) Management, source: Ericsson, S3-99516, CR on Handling of AVs in VLR at Location Update:

S3-99504 gives a justification to the CRs on sequence numbering in S3-99501 and S3-99503.

S3-99516 and S3-99501: S3-99516 requests deletion of old AVs when a user leaves and then re-enters a VLR/SGSN. S3-99501 just requests that any AV is only used once. Both proponents agree that a VLR/SGSN doesn't have to delete unused AVs after a location cancellation, but may keep them for some time, provided that there are mechanisms to guarantee that AVs are not too old. If these mechanisms are home environment specific, there is a risk of unnecessary conflict situations in the roaming case. It was concluded that the change of section 6.3.3 (last two paragraphs on top of 6.3.3.1) is preferable to the change in S3-99516; that however S3-99516 also corrects occurrences of "VLR" to become "VLR/SGSN". See also S3-99496, References to Packet Switched Core Network Nodes, source: Ericsson, on the terminology issue.

S3-99513 and S3-99501: There was a debate on the requirements to be raised and how high the degree of specification should be. It was agreed that it should be avoided that the serving network often tries to use AVs which are considered out of range by HE and USIM. On the other hand, it was agreed that to specify a certain generation method does not help to fulfil that requirement. What would be necessary would be a way for the SN to judge whether AVs are probably out of range.

S3-99516 was withdrawn. S3-99532, revising S3-99501 and S3-99513, was further revised in S3-99540 and S3-99548. S3-99548, CR 33.102-037r1, includes requirements on sequence number handling, removes description of any particular method of sequence number handling, improves efficiency of the re-synchronisation procedure, and corrects the notation.

S3-99548 was agreed.

S3-99538, rev. of S3-99503: This CR 33.102-036 impacting Annex F, Example uses of AMF, was approved.

Concerning sequence numbering, also S3-99535 was discussed.

S3-99539, CR 33.102-036 on Sequence number management: This CR, revising S3-99531, S3-99511 and S3-99502, rewriting annex C of 33.102, was approved.

S3-99462, *Preliminary analysis on how to implement an authentication failure report mechanism*, source: Telenor, was presented by Geir Kjøien. This document proposes to introduce an authentication failure report from VLR to HLR and from SGSN to HLR in R99. The proposed mechanism uses a new MAP operation MAP_AUTHENTICATION_FAILURE_REPORT on the Gr and D-interface.

Clarifications at S3#9:

- Peter Howard reported that, as the last N2 of 1999 has already been held, a decision to include this feature, and also MAP security, in R99 would have to be taken by CN next week.
- It was reported that a similar feature is contained in 3GPP2.

The document raises some points for decision.

Agreement in S3#9:

- Concerning the first point raised for decision, whether the feature should become a R99 feature, it was agreed that a LS and a CR should be written under the working assumption that the feature becomes a R99 feature.

- Concerning the second point raised for decision, whether to specify a minimum or a further going solution, it was clarified that a decision is not necessary, as the feature would allow implementation of further reactions of SN and HN.

- Concerning the third point raised for decision, whether the feature should be mandatory in a new MAP version, still networks would be able not to apply it.


- Concerning the fourth point raised for decision, whether it is appropriate to implement the feature for GSM/GPRS specifications pre-dating UMTS, it was concluded to be unacceptable to add the feature to R98 or earlier releases.

S3-99536, CR 33.102-040 on An authentication failure report mechanism from SN to HE, was agreed.

S3-99517: This CR to 33.102 proposes to correct figure 14. It was recognised that a correction is needed; however, it should identify the parameters sent to the UMTS RAN / GSM BSS and the parameters sent to the mobile station MM sub-layer.

CR 33.102-041 in s3-99520 on UIA and UEA identifications: Comments at S3#9:

- There should be means to negotiate "no encryption" between network and mobile.
- For certain MM and CM messages, integrity protection might not be applicable (emergency calls). For this, a communication between CN and RAN is necessary, as the RAN doesn't read MM and CM messages. This would probably be possible by the network not setting integrity protection or by using a specific "null" key for the whole connection.
- There was a discussion whether ciphering should be mandatory if a USIM is provided; the dangers of non-ciphered packet sessions is even higher than for circuit oriented connections.
- It was questioned whether 33.102 should specify 4 bit identifiers for integrity and encryption algorithms at all. It was questioned whether 33.102 should specify 4 bit identifiers for integrity and encryption algorithms at all.

 **Contributions on security handling of USIM-less emergency calls. Contributions on the question in which cases ciphering should be mandatory.**

Still, the CR in s3-99520 was accepted, however further contributions on the matter are possible.

S3-99541, revising S3-99421, CR 33.102-026r1 on Mobile IP security, was agreed.

S3-99542, CR 33.102-031 on Removal of alternative authentication mechanism described in annex D: This CR was agreed with the exception of Lucent.

Lucent gave the following statement:

begin quotation

Lucent objects to the removal, at this time, of the 3G TS 33.102 Annex D "A mechanism for authentication based on a temporary key (based on TETRA)". The reason that this authentication method has been originally approved by SA WG3 as an alternate method is listed in Annex D section 3 (D.3) : "...Serious operational difficulties are discovered with the SQN protocol. Those are problems implementing the protocol that may be discovered during early development or testing. ...".

Although the SQN is expected to be an effective authentication architecture for the 3GPP systems, it is our position that it is prudent to maintain this option in Annex D, until the effectiveness of the SQN architecture can be proven via field testing. It should be noted that maintaining this optional TETRA based authentication method in the document does not effect in any way the implementation of the primary AKA architecture based on SQN.

end quotation.

S3-99409, CR 33.102-030, Handling of the MS UEA and UIA capability information, was approved.

S3-99549, CR to 33.102 on re-authentication (rev. of S3-99492), and S3-99550, LS to N1, R2, T3 on USIM triggered authentication and key setting during PS connections (rev. of S3-99493): The LS in S3-99550 was agreed, the CR in S3-99549 is postponed to S3#10.

 **S3-99549, CR to 33.102 on re-authentication is postponed to S3#10.**

[S3-99529, CR 33.102-39 on Updated definitions and abbreviations, revising S3-99497, was agreed.](#)

As a consequence, as expressed in S3-99498, the terms TMSI and P-TMSI should be used in the S3 specifications.

[S3-99528, CR 33.102-038, introducing the UMTS system architecture with respect to the PS and CS domains in section 4 to clarify the access security, was agreed.](#)

[S3-99543, CR 33.102-032, on Removal of network-wide encryption mechanism form application security section, was agreed.](#)

[S3-99544, CR 33.102-033, on Distribution of authentication data within one serving network domain, was agreed.](#)

[S3-99545, CR 33.102-034, on Interoperation and intersystem handover/change between UTRAN and GSM BSS, was agreed.](#)

[S3-99552, CR 33.102-027r1, on clarification of re-authentication during PS connections \(rev. of S3-99416\), was agreed.](#)

10 Review of CRs to TS 3G 33.103

[Changes corresponding to the agreed CRs on 33.102 will be necessary, and should be prepared for SA#7.](#)

11 Review of CRs to other 3G specifications

11.1 TS 3G 33.106

[CR 33.106-001 in S3-99522, revising S3-99507, was approved.](#)

11.2 TS 3G 21.133

It was commented that this specification contains references to other no more existing specifications. It seems that the initial sections could be deleted, as they only collect material from other specifications.

 **To review 21.133.**

11.3 CRs to TR 3G 33.902

[S3-99505: This CR to 33.902 was approved.](#)

11.4 TS 3G 33.105

 **S3-99524, a CR to 33.105, was postponed to S3#10.**

11.5 TR 3G 33.120

No input had been received. The document is stable.

11.6 TR 3G 33.901

No input had been received. The document is stable.

11.7 TS 3G 22.022

 Specification TS 3G 22.022 had recently been transferred to S3. A rapporteur is missing.

12 Review of draft 3G specifications

12.1 TS 3G 33.107

33.107 was presented as S3-99508, and, with some minor re-formatting, as S3-99530. It was noted that a CR does not apply before a specification is approved; also that these versions should in fact be version 0.1.0 and 0.1.1 (when a specification is agreed to be presented to TSG for information, version 1.0.0 is produced by the support team carrying out the necessary clean ups).

[33.107 in S3-99508 / S3-99530 was approved to be presented to SA for approval as version 1.0.0.](#)

12.2 TR 3G 33.900

S3-99525, TR 3G 33.900 was noted. (the version number should be 0.1.0).

12.3 TS 3G 33.048

No input had been received.

13 Update 3G security project plan

Postponed.

14 Any other business

S3-99518, a note from Polkomtel SA on merging S3 and SMG10: This note expresses that Polkomtel in principle supports the idea of amalgamation of S3 and SMG10, but raises the two following issues:

- 1 Some GSM security related documents might need a restricted distribution
- 2 To inform the meeting whether particular 2G issues are to be discussed.

It was agreed at S3#9 to separate Tdocs and e-mails when requested, but to use 3GPP as default. It was further agreed that if possible, an indication should be given whether GSM issues are expected to be on the agenda. As already expressed in S3-99518, it is difficult to determine the agenda before the Chairman has got an idea which input documents are to come. Therefore, the delegates should at least send a list of their planned contributions (if not the complete documents) to S3/SMG10 timely before the meeting, so that the agenda can be prepared.

15 Approval of liaison statements, CRs and draft specifications

Liaison statements agreed at S3#9:

Tdoc 3GPP	Status	Title
S3-99		
463	approved, sent	Corrected LS to: TIA TR-45.AHAG cc: TIA TR-45, TR-45.2, TR-45.3, TR-45.5 Principles concerning the development of a common authentication mechanism to support global roaming (correcting S3-99460)
537	approved, sent	LS to TSG-CN, CN-2, cc: SA, on A mechanism for reporting authentication failures from VLR/SGSN to HLR
551	approved, sent	LS to TIA TR-45 Plenary, cc: TIA TR-45.2, TIA TR-45 AHAG, 3GPP TSG SA, on 3GPP AKA proposal as presented in TIA TR-45.2./99.11.08.09
553	approved, sent	LS to TSG-SA and TSG-CN on MAP security (rev. of 514 and 519)
554	approved, sent	LS to SA, SA2, CN and CN OSA ad-hoc: Statement on security issues in VHE/OSA (answer to

		S2-99E05)
555	approved, sent	LS to N1 on enhanced User Identity Confidentiality (rev. of 515)
556	to be written by PH	LS to SAGE (rev. of 523)

CRs and new specifications agreed by S3 between SA#5 and SA#6:

TSG_M	SPEC	CR	REV	CAT	SUBJECT	WG_DO	TSG_D	3G_PHA	WG_STA
S3#8	33.10	022	1	C	Refinement of Enhanced User Identity	S3-	SP-	99	agreed
S3#7	33.10	025		C	Length of KSI	S3-	SP-	99	agreed
S3#9	33.10	026	1	B	Mobile IP security	S3-	SP-	99	agreed
S3#9	33.10	027	1	C	Clarification of re-authentication during PS	S3-	SP-	99	agreed
S3#8	33.10	030		C	Handling of the MS UEA and UIA capability	S3-	SP-	99	agreed
S3#9	33.10	032		F	Removal of network-wide encryption mechanism	S3-	SP-	99	agreed
S3#9	33.10	033		C	Interoperation and intersystem handover/change	S3-	SP-	99	agreed
S3#9	33.10	034		C	Distribution of authentication data within one	S3-	SP-	99	agreed
S3#9	33.10	035		C	Authentication and key agreement	S3-	SP-	99	agreed
S3#9	33.10	036		C	Sequence number management	S3-	SP-	99	agreed
S3#9	33.10	037	1	C	Authentication and key agreement	S3-	SP-	99	agreed**
S3#9	33.10	038		C	Clarification on system architecture	S3-	SP-	99	agreed
S3#9	33.10	039		D	Updated definitions and abbreviations	S3-	SP-	99	agreed
S3#9	33.10	040		B	An authentication failure report mechanism from	S3-	SP-	99	agreed
S3#9	33.10	041		B	UIA and UEA identifications	S3-	SP-	99	agreed
S3#9	33.10	031		C	Removal of alternative authentication mechanism	S3-	SP-	99	agreed*
S3#8	33.10	001	1	C	Refinement of Enhanced User Identity	S3-	SP-	99	agreed
S3#7	33.10	002	1	D	Corrections to figure 1	S3-	SP-	99	agreed
S3#8	33.10	004		C	Change length of KSI (and other miscellaneous	S3-	SP-	99	agreed
S3#7	33.10	004		D	Time variant parameter for synchronisation of	S3-	SP-	99	agreed
S3#8	33.10	005		D	Direction bit in f9	S3-	SP-	99	agreed
S3#9	33.10	001		C	Lawful Interception Requirements	S3-	SP-	99	agreed
S3#9	33.90	001		B	Formal analysis of the 3G authentication protocol	S3-	SP-	99	agreed
S3#8	21.13	001		C	Data integrity of user traffic	S3-	SP-	99	agreed
S3#9	33.10	NEW			3G Security; Lawful Interception Architecture	S3-	SP-	99	agreed

*: Lucent objected in S3#9

** : value 50 shall be used pending further study

16 Future meetings dates and venues

Meeting	Date	Location	Host
S3#10	19-21 January 2000	Brussels	Siemens
S3#11	22-24 February 2000	Mainz	RegTP
S3#12	11-14 April 2000 (including joint meeting with AHAG)	Stockholm	Ericsson
S3#13	23 - 25 May	Tokyo	DoCoMo

17 Close of meeting

The meeting was closed.

TSG SA WG 3 #9 document list

Tdoc 3GPP S3-99	AI	other ref	av	Status	Source	Title	Type/CR	Rev	Rel.	Effectuated spec	WI / Topic
T2-991082	5.2		y	noted		LS to S3, S1, cc. T3 on Reply to LS on additional Terminal Baseline Implementation Capabilities	LSin				
T2-991036	5.2		y	postponed to S3#10		LS to SMG10, S3, cc: SMG9 on Possible security issues with handsets supporting a user input storage mechanism	LSin				
R2-99g79		S2-99E05	y	see S2-99E05							
S2-99E05	5.1	R2-99g79	y	answer in 554			LSin				
421	9		y	rev. in 541 agreed		CR to 33.102 on Mobile IP					
462	9		y	consequential CR and LS in 536 and 537	Telenor	Preliminary analysis on how to implement an authentication failure report mechanism	Disc/dec				
463	5.6		y	approved	SMG10/ S3	Corrected LS to: TIA TR-45.AHAG cc:	LSout				

						TIA TR-45, TR-45.2, TR- 45.3, TR-45.5 Principles concerning the development of a common authentication mechanism to support global roaming (correcting S3- 99460)					
492	9		y	rev. in 549	[Peter Howard]	CR to 33.102 on re- authentication					
493	9		y	rev. in 550	[Peter Howard]	LS on re- authentication					
494	8.5		y	noted		23.923 V1.2.0					
495	8.5		y	noted	S2 (Anders Hansmats)	Presentation on Mobile IP					
496	9		y	CR to be generated	Ericsson	References to Packet Switched Core Network Nodes					
497	9		y	revised in 529	Ericsson	draft CR to 33.102 on Updated definitions and abbreviations	CR				
498	9		y	CR to be generated	Ericsson	refer to TMSI / P-TMSI instead of Update IMUI and TMUI					
499	4.1		y	approved		report S3#8					
500	2		y	approved		Agenda S3#9					

501	9		y	rev. in 532	Siemens	CR to TS 33.102 section 6.3 on Authentication and key agreement					
502	9		y	rev. in 531	Siemens	CR to Annex C of TS 33.102 ("K")					
503	9		y	superseded	Siemens	CR to Annex F of TS 33.102					
504	9		y	discussed	Siemens	justification of the proposed changes to section 6.3 and Annex F ("j")					
505	11.3		y	approved	Siemens	Formal analysis of the 3G authentication protocol	CR 33.902-001				
506			-	-		[deleted]					
507	11.3		y	CR to be generated	RegTP	33.106					
508	12.1		y	approved	RegTP	33.107	spec				
509	8.2		y	noted	Lucent	Shazam algorithm					
510	8.3		y	postponed	Bosch	3GPP terminal identity security: levels, requirements and mechanisms					
511	9		n	superseded	Siemens	revised CR to annex C (rev. of 502)					
512	9		y	superseded	Ericsson	CR on SQNLO in GSM					

513	9		y	rev. in 532	Ericsson	SEQ management (PA2)					
514	15		y	revised by 553	T-Mobil	Draft answer to LS from N2 on MAP sec					
515	15		y	rev in 555	T-Mobil	draft LS to N1 on enhanced User Identity Confidentiality					
516	9		y	withdrawn	S3	Handling of AVs					
517	9		y	superseded	T-Mobil	Corrections in fig 14					
518	14		y	It was agreed: to send out intended docs timely before the meeting, so that the agenda can be prepared timely before the meeting; to separate Tdocs and e-mails when requested, but to use 3GPP as default; it can not be guaranteed when GSM is treated during a meeting because there are actions to be done during	Polkomtel SA	Note on merging S3 and SMG10					

				a meeting, documents may arrive late etc.							
519	15	Q	y	rev. in 553	Vodafone	Draft LS to SA and CN on MAP security					
520	9	R	y	agreed	S3	UIA and UEA identifications	CR 33.102-041		99	33.102	Security
521	15	N1-99E71	y	answer written	CN1	LS to S3 on UMTS security issues	LSin				
522	11.1		y	approved	S3	Lawful Interception Requirements (rev. of 507)	CR33.106-001		99	33.106	Security
523	11.4		y	rev in 556	Vodafone	proposed CR to 33.105					
524	11.4		y	postponed to S3#10	S3	CR to 33.105					
525	12.2		y	noted	rapporteur	33.900	spec				
526	5.2	T3-99413	y	postponed to S3#10		LS from T3 on USIM- Terminal Link	LSin				
527			y	done		LS from TR-45	LSin				
528	9		y	agreed	S3	Clarification on system architecture	CR 33.102-038		99	33.102	Security
529	9		y	agreed	S3	Updated definitions and abbreviations	CR 33.102-039	rev. of 497	99	33.102	Security
530	12.1		y	agreed	RegTP/DDI	re-formatting of 33.107					
531	9		y	rev. in 539	Siemens	CR to Annex C of TS 33.102 (rev. of 502)					
532	9		y	rev. in 540 and 548	Siemens	merger of 501 and 513					

533			-	not assigned						
534			-	not assigned						
535	9		y	discussed	Siemens	SQN options				
536	9		y	agreed	S3	An authentication failure report mechanism from SN to HE	CR 33.102-040	99	33.102	Security
537	9		y	approved		LS to TSG-CN, CN-2, cc: SA, on A mechanism for reporting authentication failures from VLR/SGSN to HLR	LSout			
538	9		y	agreed	S3	Authentication and key agreement (rev. of 503)	CR 33.102-035	99	33.102	Security
539	9		y	agreed	S3	Sequence number management (rev. of 502 and 531)	CR 33.102-036	99	33.102	Security
540				revised in 548	S3	Authentication and key agreement (rev. of 501 and 532)	CR 33.102-037	99	33.102	Security
541	9		y	agreed	S3	Mobile IP security (rev. of 421)	CR 33.102-026r1	99	33.102	Security
542	9		y	agreed*	S3	Removal of alternative authentication mechanism	CR 33.102-031	99	33.102	Security

						described in annex D					
543	9		y	agreed	S3	Removal of network-wide encryption mechanism from application security section	CR 33.102-032		99	33.102	Security
544	9		y	agreed	S3	Distribution of authentication data within one serving network domain	CR 33.102-033		99	33.102	Security
545	9		y	agreed	S3	Interoperation and intersystem handover/change between UTRAN and GSM BSS	CR 33.102-034		99	33.102	Security
546			y	postponed to S3#10	SMG10 WPA Chairman	CR on applicability of ciphering for GPRS	CR				
547			y	postponed to S3#10	SMG10 WPA Chairman	CR on applicability of ciphering for GPRS	CR				
548	9		y	agreed**	S3	Authentication and key agreement (rev. of 540)	CR 33.102-037r1		99	33.102	Security
549			y	postponed to S3#10		CR to 33.102 on re-authentication (rev. of 492)					

550			y	approved		LS to N1, R2, T3 on USIM triggered authentication and key setting during PS connections (rev. of 493)					
551			y	approved		LS to TIA TR-45 Plenary, cc: TIA TR-45.2, TIA TR-45 AHAG, 3GPP TSG SA, on 3GPP AKA proposal as presented in TIA TR-45.2./99.11.08.09	LSout				
552	9		y	agreed	S3	clarification of re-authentication during PS connections (rev. of 416)	CR 33.102-027r1		99	33.102	Security
553			y	approved		LS to CN, SA on MAP security etc.	LSout				
554			y	approved		LS to SA, SA2, CN and CN OSA ad-hoc: Statement on security issues in VHE/OSA (answer to S2-99E05_	LSout				

555			y	approved		LS to N1 on enhanced User Identity Confidentiality	LSout				
556			n	to be written by PH		LS to SAGE (rev. of 523)	LSout				

*: Lucent objected in S3#9

** : value 50 shall be used pending further study

Action points from earlier meetings:

- ✎ Charles Brookson to draft some text for a press release, making a wider public aware of the 3GPP security specifications: This should be done after SA#6.
- ✎ CR to 03.20, LS to GSMA on usage of A5/1 for CTS.
- ✎ Further work identified: To elaborate 33.102 annex A.
- ✎ GSM 03.48 has to be transformed into a 3GPP specification.
- ✎ It was agreed
 - to review the main specifications in S3#10;
 - to ask S2 to identify the other relevant specifications, so that they can be studied;
 - S3 will then try to identify missing aspects in spring 2000.
 - Mike Walker will contact the S2 chairman and the co-ordination group.
 - A corresponding new section 3.4 will be added to 3G PD 30.810, Project plan for security.

New action points:

- ✎ T2-991036, a LS from T2 to SMG10, S3, cc: SMG9, on *Possible security issues with handsets supporting a user input storage mechanism*, was postponed to S3#10.
- ✎ S3-99526 (= T3-99413), a LS from T3 on USIM-Terminal link, was postponed to S3#10.
- ✎ To draft a LS to SAGE as Tdoc S3-99556 (rev. of S3-99523).
- ✎ S3-99546 and S3-99547, CRs on applicability of ciphering for GPRS, both source: SMG10 WPA Chairman, were postponed to S3#10.
- ✎ S3-99510, 3GPP terminal identity security: levels, requirements and mechanisms, source: Bosch, was postponed to S3#10.
- ✎ Drafting of the updated CRs on terminal security (due for SMG#31) was postponed to S3#10.
- ✎ Contributions on security handling of USIM-less emergency calls. Contributions on the question in which cases ciphering should be mandatory.
- ✎ S3-99549, CR to 33.102 on re-authentication is postponed to S3#10.
- ✎ To review 21.133.
- ✎ S3-99524, a CR to 33.105, was postponed to S3#10.
- ✎ Specification TS 3G 22.022 had recently been transferred to S3. A rapporteur is missing.