SP-010129

3GPP TSG-SA WG3 (Security)

Status Report to SA#11

19-22 March 2001

Palm Springs, USA

Michael Walker

Chairman 3GPP TSG-SA WG3

Content of Presentation

- Report from TSG-SA WG3 and review of progress (AI 7.3.1)
- Questions for advice from TSG-SA WG3 (AI 7.3.2)
  - nothing to raise
- Approval of contributions from TSG-SA WG3 (AI 7.3.3)

Report and Review of Progress in SA3 (AI 7.3.1)

- Contents for agenda item 7.3.1
  - General overview of progress
  - Cryptographic algorithm development
  - Specifications and reports
  - Work programme
  - Outlook for future meetings
  - Meetings scheduled after SA#11

General Overview of Progress

- SP-010143, Draft report of SA WG3 meeting #17, Gothenburg, 27 February - 2 March 2001 - ***for information***
- Focus has been on completing R99, progressing network domain security for Rel-4/Rel-5, progressing IM subsystem security for Rel-5 and addressing feedback from other groups
- SA WG3 has also reviewed the work programme and has produced a one new work item description

Milenage evaluation: 3G Authentication Algorithms

- SA#11 are asked to approve the the SAGE authentication algorithm evaluation report (SP-010144) and forward it to PCG for official publication by the Partner SDOs
  - Note that the report is already in the public domain – SA WG3 server
- It is stressed that rapid official publication of the evaluation report would help prevent external evaluations being made which may lead to misleading claims about the algorithm
- ***The approval of the report will be handled under agenda item 7.3.3***

Network Domain Security

- Although there has been progress on the specification of MAP security and the specification is reasonably stable, it has not been possible to present TS 33.200 to SA#11 approval as originally planned
- It is requested that the MAP security specifications in TS 33.200 are presented for information in May by e-mail and for approval at the June plenary for inclusion in Rel-4
- Note that CN WG4 have already included provisions for MAP security in their Rel-4 specifications
- An additional SA WG3 ad hoc meeting has been scheduled in April to progress network domain security

IP Multimedia Subsystem Security

- S3#17 agreed a proposal on the location of security functions in the Rel-5 IMS architecture
  - integrity in P-CSCF, authentication in S-CSCF
- Because of the delay in agreeing the location of security functions, it has not been possible to agree a TS to be presented to SA#11 for information as originally planned
- An additional ad hoc meeting has been scheduled in April to progress the IMS security architecture

Specifications and Reports

- CRs are tabled on the following specifications
  - 03.35, Immediate service termination
  - 33.102, Security architecture
  - 33.103, Integration guidelines
  - 33.105, Cryptographic algorithms
  - 33.106, Lawful interception requirements
  - 33.107, Lawful interception architecture

- ***The approval of the CRs will be handled under agenda item 7.3.3***

Work Programme

- One new work item has been agreed by SA WG3
  - SP-010153, New WI: End-to-end security work item description (for approval under AI 7.3.3)

Outlook for Future Meetings

- With the stability of R99, SA WG3 will now continue with the work for Rel-4 and Rel-5
- Main work items
  - Network domain security - MAP security
  - Network domain security - IP security
  - IM subsystem security
- Other work items
  - GERAN security

Meetings Scheduled after SA#11

- SA WG3 NDS ad hoc, 24 - 25 April 2001, Madrid, Spain
- SA WG3 IMS ad hoc, 26 April 2001, Madrid, Spain
- S3#18, 21 or 22 - 24 May 2001, Phoenix, USA (location TBC)
- S3#19, 3 or 4 - 6 July 2001, London, UK (location TBC)
- S3#20, 15 or 16 - 18 October 2001, Sydney, Australia (location TBC)
- Joint meeting with GERAN (date and location TBA)

Approval of Contributions from S3 (AI 7.3.3)

- Contents for agenda item 7.3.3
  - CRs to SA WG3 specifications
  - New SA WG3 report
  - New work item description

CRs on IST

- SP-010130, 1 corrective CR to 03.35: IST implementation for non-CAMEL subscribers
  - CR 001: This CR was reviewed by CN WG2 in July 1999. The rest of the package was approved by TSG CN, but this CR was not previously sent to SA WG3 for approval

CRs on Security Architecture

- SP-010131, 7 corrective CRs to 33.102 (R99)
  - CR 135: Correction that RES shall be a multiple of 8 bits (to reach alignment with stage 3 specifications)
  - CR 136: Clarification on bit ordering to remove ambiguity
  - CR 137: Clarification of time limit for RNC to change keys
  - CR 140: Correction to the handling of re-transmitted authentication request messages on the ME (to reach alignment with stage 3 specification)
  - …(continued)

CRs on Security Architecture

- SP-010131, 7 corrective CRs to 33.102 (R99)
  - …(continued)
  - CR 141: Clarification that it is optional for a GSM-only ME to support the USIM interface (to reach alignment with T3 TR on interworking)
  - CR 142R1: Correction of existing definitions. Addition of new definitions on R98- and R99+ at the request of SA#9
  - CR 143: Correction of a mechanism for protecting a UE's GSM ciphering capability

CRs on Security Architecture

- SP-010132, 2 functional modification CRs to 33.102 (Rel-4)
  - CR 138: Addition of requesting node type to authentication data request
  - CR 139: Addition of parameters to authentication failure report which may be used as secondary fraud indicators

CRs on Integration Guidelines

- SP-010133, 1 corrective CR to 33.103 (R99)
  - CR 013: Clarification on bit ordering to remove ambiguity

CRs on Algorithm Requirements

- SP-010134, 3 corrective CRs to 33.105 (R99)
  - CR 016, Clarification on bit ordering to remove ambiguity
  - CR 017, Correction that RES shall be a multiple of 8 bits (to reach alignment with stage 3 specifications)
  - CR 018, Correction to minimum USIM clock frequency based on advice from T WG3

CRs on Lawful Interception

- SP-010135, 1 category B CR to 33.106 (Rel-4)
  - CR 002: Update for Rel-4
- SP-010136, 1 category B CR to 33.106 (Rel-5)
  - CR003: Update for Rel-5
- SP-010137, 1 corrective CR to 33.107 (R99)
  - CR002: Correction of location information parameters in interception event records
- SP-010146, CR to 33.107 (Rel-4)
  - CR 003: addition of PS for Rel-4

New SA3 Report

- SP-010144, 33.xxx v1.0.0: Report on the evaluation of the 3GPP authentication algorithms (S3-010015)
  - As discussed under agenda item 7.3.1

New Work Item Description

- SP-010153, New WI: End-to-end security work item description (S3-010123)

Technical Specification Group Services and System Aspects Meeting #11, Palm Springs, U.S.A., 19-22 March 2001

TSGS#11(01)0129

Source: **Chairman, Secretary S3**

Title: **Status Report of SA_WG3 (Security)**

Document for: **Information and Decision**

Agenda Item: **7.3**

TSG SA3 STATUS REPORT

1 General Overview of Progress

The SA WG3 meeting #17 was held in Gothenburg, Sweden from the 27 February – 2 March 2001. Dr Stefan Pütz (T-Mobil) chaired the meeting and the secretary was Mr Maurice Pope from the MCC. Two joint sessions with SA WG2 were held during the meeting. The host was Ericsson.

The group has been focussing on completing Release 99, progressing network domain security for R4/R5, progressing IM subsystem security for R5 and addressing feedback from other working groups. SA WG3 has also reviewed the work programme and has produced one new work item description. The draft report of the meeting is provided in SP-010143.

Doc-1st-Level	Doc-2nd-Level	Document title	Comment
SP-010143		Draft report of SA WG3 meeting #17	For information to SA#11

2 Summary of Inputs to SA

The list of documents submitted is attached in Annex 1. The details are summarised in this section.

2.1 Network domain security

The MAP security specifications in TS 33.200 were scheduled to be presented for information at SA#10 and for approval at SA#11. At S3#16 a simplified architecture for securing native IP-based protocols using IPsec was adopted. Although the specifications for MAP security are reasonably stable it was not possible to create a new version of TS 33.200 for approval by SA WG3 and submission to SA#10.

A new draft of 33.200 was planned to be distributed to the SA mailing list for information in the New Year. It was then planned to present TS 33.200 to SA#11 for approval.

However, at S3#17 it was not possible to approve a stable version of TS 33.200. An additional ad-hoc meeting has been scheduled in April to progress the network domain security architecture. It is now planned to send the specification to the SA mailing list for information in May 2001, and to present it to SA#12 for approval in June 2001.

Doc-1st-Level	Doc-2nd-Level	Document title	Comment
SP-010xxx			

2.2 IM subsystem security

Competing proposals have been considered in SA WG3. An email discussion took place with the aim of agreeing a proposal for S3#17. It was not possible to agree a proposal before S3#17, but during the meeting a proposal on the location of security functions was agreed (integrity and confidentiality functions provided in the P-CSCF and the authentication performed in the home network, S-CSCF).

The TS was scheduled to be presented to SA#11 for information and can then be used by other groups as a basis for their specifications. The TS is then scheduled to be presented to SA#12 for approval.

Because of the delay in agreeing the location of security functions, it has not been possible to agree a TS to be presented to SA#11 for information. However, an additional ad-hoc meeting has been scheduled in April to progress the development of the IMS security architecture.

2.3 Specifications/Reports

The following report is submitted to this meeting.

- Authentication Algorithm Specifications

The evaluation results are now presented to SA#11 for approval. SA#10 are asked to forward TR 33.909 to PCG for approval for publication by the Partner SDOs. It is stressed that rapid publication of the evaluation report by the SDOs would help prevent external evaluations being made which may lead to misleading claims about the algorithm.

Doc-1st-Level	Doc-2nd-Level	Document title	Comment
SP-010144	S3-010015	SAGE authentication algorithm evaluation report	For approval by SA#11 and forwarding to PCF for approval for publication by the partner SDOs.

2.4 Change Requests

SA WG3 has generated a number of change requests that reflect a series of clarifications and corrections, especially to ensure a coherent Release 99. Two CRs have been produced to add new functionality to the REL-4 security architecture. Several CRs on lawful interception have also been prepared.

2.4.1 Immediate Service Termination, Stage 2 (03.35)

The following CR was agreed at SA WG3 meeting #17 and is presented to TSG SA #11 for approval.

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
SP-010130	03.35	001		R99	IST implementation for non-CAMEL subscribers	F	8.0.0	S3	S3-17	S3-010049

2.4.2 3G Security Architecture (33.102)

The following CRs were agreed at SA WG3 meeting #17 and are presented to TSG SA #11 for approval.

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc

SP-010131	33.102	135		R99	RES has to be a multiple of 8 bits	F	3.7.0	S3	S3-17	S3-010006
SP-010131	33.102	136		R99	Add bit ordering convention	F	3.7.0	S3	S3-17	S3-010064
SP-010131	33.102	137		R99	Timing of security mode procedure	F	3.7.0	S3	S3-17	S3-010094
SP-010131	33.102	140		R99	Correction to the handling of re-transmitted authentication request messages on the ME	F	3.7.0	S3	S3-17	S3-010124
SP-010131	33.102	141		R99	Optional Support for USIM-ME interface for GSM-Only ME	F	3.7.0	S3	S3-17	S3-010126
SP-010131	33.102	142	1	R99	Definition corrections	F	3.7.0	S3	S3-17	S3-010138
SP-010131	33.102	143		R99	GSM ciphering capability Handling in Security Mode set up procedure	F	3.7.0	S3	S3-17	S3-010117
SP-010132	33.102	138		Rel-4	Add requesting node type to authentication data request	C	3.7.0	S3	S3-17	S3-010103
SP-010132	33.102	139		Rel-4	Additional Parameters in Authentication Failure Report	C	3.7.0	S3	S3-17	S3-010104

2.4.3 3G Integration Guidelines (33.103)

The following CRs were agreed at SA WG3 meeting #17 and are presented to TSG SA #11 for approval.

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
SP-010133	33.103	013		R99	Add bit ordering convention	F	3.4.0	S3	S3-17	S3-010065

2.4.4 3G Algorithm Requirements (33.105)

The following CRs were agreed at SA WG3 meeting #17 and are presented to TSG SA #11 for approval.

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
SP-010134	33.105	016		R99	Add bit ordering convention	F	3.6.0	S3	S3-17	S3-010066
SP-010134	33.105	017		R99	RES has to be a multiple of 8 bits	F	3.6.0	S3	S3-17	S3-010048
SP-010134	33.105	018		R99	Minimum clock frequency updated	F	3.6.0	S3	S3-17	S3-010111

2.4.5 3G Lawful Interception Requirements (33.106)

The following CRs were agreed at SA WG3 meeting #17 and are presented to TSG SA #11 for approval.

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc

SP-010135	33.106	002		Rel-4	Update of TS 33.106 for release 4	B	3.1.0	S3	S3-17	S3-010060
SP-010136	33.106	003		Rel-5	Release 5 updates	B	3.1.0	S3	S3-17	S3-010107

2.4.6 3G Lawful Interception Architecture (33.107)

The following CRs were agreed at SA WG3 meeting #17 and are presented to TSG SA #11 for approval.

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
SP-010137	33.107	002		R99	Correction of Location information parameters in interception event records	F	3.1.0	S3	S3-17	S3-010062
SP-010146	33.107	003		REL-4	Update of TS 33.107 for Release 4 - Inclusion of PS LI requirements	B	3.1.0	S3	S3-17 (e-mail appl)	S3LI01_050

2.5 Work programme

A structured programme of security work items is being regularly reviewed and maintained by SA WG3.

One new WID is presented to SA#11 for approval. Further information on the security work programme is available in the latest version of the project plan (and the security IGC report to SA#11 from SA WG2).

2.5.1 New Work Items

The following new Work Item has been agreed by SA WG3 to be presented to SA#11 for approval.

Doc-1st-Level	Doc-2nd-Level	Work item title	Rapporteur
SP-010153	S3-010123rev	End-to-end security	Colin Blanchard, BT

3 Outlook for Future Meetings

With the stability of the work for Release 99, SA WG3 will now continue with the work for REL-4 and REL-5.

4 Planned Meetings of SA3

Title	Date	Location
NDS ad hoc meeting	24 – 25 April 2001	Madrid, Spain
IMS ad hoc meeting	26 April 2001	Madrid, Spain
S3#18	21 or 22 - 24 May 2001	Arizona, USA (location TBC)
S3#19	3 or 4 – 6 July 2001	London, UK (location TBC)
S3#20	15 or 16 – 18 October 2001	Sydney, Australia (location TBC)
S3#21	TBD	TBD

A joint meeting with the GERAN ad-hoc group is planned, pending confirmation of dates and venue from GERAN.

Annex 1 Documents Provided to SA#11

Tdoc	Title	Agenda
SP-010129	Status Report from SA WG3 to SA#11	7.3.1
SP-010130	1 Corrective CR to 03.35 version 8.0.0	7.3.3
SP-010131	7 Corrective CRs to 33.102 version 3.7.0	7.3.3
SP-010132	2 Category C, Rel-4 CRs to 33.102 version 3.7.0	7.3.3
SP-010133	1 Corrective CR to 33.103 version 3.4.0	7.3.3
SP-010134	3 Corrective CRs to 33.105 version 3.6.0	7.3.3
SP-010135	1 Category C, Rel-4 CR to 33.106 version 3.1.0	7.3.3
SP-010136	1 Category C, Rel-5 CR to 33.106 version 3.1.0	7.3.3
SP-010137	1 Corrective CR to 33.107 version 3.1.0	7.3.3
SP-010143	Draft report of SA WG3 meeting #17	7.3.1
SP-010144	Authentication algorithm evaluation report v1.0	7.3.3
SP-010145	Work Item Description: End-to-end security	7.3.3
SP-010146	CR on 33.107: Update of TS 33.107 for Release 4 - Inclusion of PS LI requirements	7.3.3

Annex 2 CRs Provided to SA#11

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
SP-010130	03.35	001		R99	IST implementation for non-CAMEL subscribers	F	8.0.0	S3	S3-17	S3-010049
SP-010131	33.102	135		R99	RES has to be a multiple of 8 bits	F	3.7.0	S3	S3-17	S3-010006
SP-010131	33.102	136		R99	Add bit ordering convention	F	3.7.0	S3	S3-17	S3-010064
SP-010131	33.102	137		R99	Timing of security mode procedure	F	3.7.0	S3	S3-17	S3-010094
SP-010131	33.102	140		R99	Correction to the handling of re-transmitted authentication request messages on the ME	F	3.7.0	S3	S3-17	S3-010124
SP-010131	33.102	141		R99	Optional Support for USIM-ME interface for GSM-Only ME	F	3.7.0	S3	S3-17	S3-010126
SP-010131	33.102	142	1	R99	Definition corrections	F	3.7.0	S3	S3-17	S3-010138
SP-010131	33.102	143		R99	GSM ciphering capability Handling in Security Mode set up procedure	F	3.7.0	S3	S3-17	S3-010117
SP-010132	33.102	138		Rel-4	Add requesting node type to authentication data request	C	3.7.0	S3	S3-17	S3-010103
SP-010132	33.102	139		Rel-4	Additional Parameters in Authentication Failure Report	C	3.7.0	S3	S3-17	S3-010104
SP-010133	33.103	013		R99	Add bit ordering convention	F	3.4.0	S3	S3-17	S3-010065
SP-010134	33.105	016		R99	Add bit ordering convention	F	3.6.0	S3	S3-17	S3-010066
SP-010134	33.105	017		R99	RES has to be a multiple of 8 bits	F	3.6.0	S3	S3-17	S3-010048
SP-010134	33.105	018		R99	Minimum clock frequency updated	F	3.6.0	S3	S3-17	S3-010111
SP-010135	33.106	002		Rel-4	Update of TS 33.106 for release 4	B	3.1.0	S3	S3-17	S3-010060
SP-010136	33.106	003		Rel-5	Release 5 updates	B	3.1.0	S3	S3-17	S3-010107
SP-010137	33.107	002		R99	Correction of Location information parameters in interception event records	F	3.1.0	S3	S3-17	S3-010062
SP-010146	33.107	003		Rel-4	Update to Rel-4	B	3.1.0	S3	S3-17	S3LI01_050