SP-000620

3GPP TSG-SA WG3 (Security)

Status Report to SA#10

11-14 December, 2000

Bangkok, Thailand, USA

Michael Walker

Chairman 3GPP TSG-SA WG3

Content of Presentation

- Report and review of progress in SA WG3 (AI 7.3.1)
- Questions for advice from SA WG3 (AI 7.3.2)
- Approval of contributions from 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
  - Confidentiality/integrity algorithms
  - Authentication algorithm
  - Specifications and reports
  - Work programme
  - Outlook for future meetings
  - Meetings scheduled after SA#10

General Overview of Progress

- SP-000621, Report of SA WG3 ad hoc meeting and draft report of meeting #16 ***- for information***
  - Report of SA WG3 ad hoc meeting, 8-9 November 2000, Munich, Germany
  - Draft report of SA WG3 meeting #16, 28-30 November 2000, Sophia Antipolis, France
- Focus has been on completing R99, progressing network domain security for R4/R5, progressing IM subsystem security for R5 and addressing feedback from other groups
- SA3 has also reviewed the work programme and has produced a one revised work item description

Publication of KASUMI: Confidentiality & Integrity Algorithms

- SA#7 approved report on the work performed by SAGE task force
  - Published as 3G TR 33.908
- And approved algorithms for distribution to 3GPP partners
  - Publication of algorithm specifications and report on evaluation results was delayed for procedural reasons
- Algorithm specification published on ETSI web site on 4 September 2000 (3G TS 35.20x series)
  - http://www.etsi.org/dvbandca/
- SP-000629, 33.909 v1.0.0: Report on the evaluation of the 3GPP confidentiality and integrity algorithms ***- for approval***

Authentication Algorithm

- SA#7 approved the development of standard authentication algorithm and SAGE work plan tabled at SA#7
  - Funding approved by 3GPP in June 2000
  - SAGE work now complete on schedule
- SP-000630, SAGE authentication algorithm deliverables - ***for approval***

Network Domain Security

- SP-000631, Information on WI “Network domain security” - ***for information***
  - 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 reasonable stable it was not possible to create a new version of TS 33.200 for approval by S3 and submission to SA
  - A new draft of 33.200 will be distributed to the SA mailing list for information in the New Year
  - If acceptable to SA, it is still planned to present TS 33.200 to SA#11 for approval

IP Multimedia Subsystem Security

- Competing proposals have been considered in SA3
- Email discussion to agree proposal for S3#17
- TS scheduled to be presented to SA#11 for information
  - other groups can start to use TS as basis for their specifications
- TS scheduled to be presented to SA#12 for approval

Specifications and Reports

- SP-000623, CRs 002 and 003 to 03.33: Addition of parameters to the X3-Interface
- SP-000624, CRs 004 and 005 to 03.33: Deletion of mono-mode and addition of optimal routing
- SP-000625, CR 001 to 33.107: Addition of parameters to the X3-Interface

Specifications and Reports

- SP-000626, 6 CRs to 33.102 (R99)
- SP-000627, CR 015 to 33.105: Layer 2 related corrections (R99)

Work Programme

- Structured programme of security work items is being reviewed and maintained
  - 15 WIDs approved at SA#8
  - 2 revised WIDs approved at SA#9
  - 6 new WIDs approved at SA#9
  - SP-000629, Revised WI: FIGS/IST work item description ***- for approval***
  - See also latest project plan and security IGC report from S2

Outlook for Future Meetings

- With the stability of R99, SA3 will now continue with the work for R4 and R5.
- Main work items for R4
  - Network domain security - MAP security
  - GERAN security
- Main work items for R5
  - Network domain security
  - IM subsystem security

Meetings Scheduled after SA#10

- S3#17, 27 February - 1 March 2001, Sophia Antipolis, France
- 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, Madrid, Spain (location TBC)

Questions for Advice from S3 (AI 7.3.2)

- Security risks in introduction phase of MAP security

Security Risks in Introduction Phase of MAP security

- SP-000622, LS from SA3: Security risks in introduction phase of MAP security
  - Introduction of MAP security by a limited number of operators would give only limited protection even to those operators who choose to implement MAP security in their networks
  - S3 suggest to set a cut-off date for the introduction of MAP security
  - S3 feel that GSM association are the appropriate body to set such a cut-off date
  - SA are requested to send a corresponding LS to the GSM association

Approval of Contributions from S3 (AI 7.3.3)

- Contents for agenda item 7.3.3
  - CRs to SA3 specifications
  - New SA3 specifications and reports
  - Revised work item descriptions
  - Status report of SA WG3 to SA#10

CRs on Lawful Interception

- SP-000623, CRs 002 and 003 to 03.33: Addition of parameters to the X3-Interface (S3-000762)
  - Note that CR003 to R99 is classified as Cat ‘C’ but corresponds to LI requirements already agreed for R99
- SP-000624, CRs 004 and 005 to 03.33: Deletion of mono-mode and addition of optimal routing (S3-000764)
- SP-000625, CR 001 to 33.107: Addition of parameters to the X3-Interface (S3-000763)

CRs on Security Architecture

- SP-000626, 6 CRs to 33.102
  - CR 129 Corrections on ciphering and integrity protection (S3-000666)
  - CR 130 Re-transmission of authentication request using the same quintet (S3-000725)
  - CR 131 Corrections to Counter Check procedure (S3-000726)
  - CR 132 Intersystem handover for CS Services – from GSM BSS to UTRAN (S3-000727)
  - CR 133 Correction on use of GSM MS classmark in UMTS (S3-000729)
  - CR 134 START value handling for MS with a GSM SIM inserted (S3-000739)
- SP-000627, CR 015 to 33.105: Layer 2 related corrections (S3-000667)

New SA3 Reports and Specifications

- SP-000629, 33.909 v1.0.0: Report on the evaluation of the 3GPP confidentiality and integrity algorithms (S3-000660)
  - SA#10 are asked to forward TR 33.909 to PCG for approval for publication by the Partner SDOs
- SP-000630, SAGE authentication algorithm deliverables (S3-000730)
  - SA#10 are asked to forward authentication algorithm deliverables to PCG for approval for publication by the Partner SDOs

Revised Work Item Description

- SP-000629, Revised WI: FIGS/IST work item description (S3-000745)

Status Report of SA3 to SA#10

- SP-000620, Status report of SA WG3 to SA#10

Technical Specification Group Services and System Aspects **TSGS#10(00)0620**

Meeting #10, Bangkok, Thailand, 11-14 December 2000

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

A TSG-SA WG3 ad hoc meeting was held in Munich, Germany from the 8-9 November 2000. Michael Marcovici (Lucent) chaired the meeting. The secretary was Mr Maurice Pope from the MCC. The host was Siemens.

The TSG-SA WG3 meeting #16 was held in Sophia Antipolis, France from the 28-30 November 2000. Professor Michael Walker (Vodafone) chaired the meeting and the secretary was Mr Maurice Pope from the MCC. A joint meeting with T3 was held on the first day. The host was ETSI.

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. SA3 has also reviewed the work programme and has produced one revised work item description.

Doc-1st-Level	Doc-2nd-Level	Document title	Comment
SP-000621		Report of SA WG3 ad hoc meeting and draft report of meeting #16	For information to SA#10

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 S3 and submission to SA#10. A new draft of 33.200 will be distributed to the SA mailing list for information in the New Year. If acceptable to SA, it is still planned to present TS 33.200 to SA#11 for approval.

Doc-1st-Level	Doc-2nd-Level	Document title	Comment
SP-000631		Information of WI “Network domain security”	For information to SA#10

2.2 IM subsystem security

Competing proposals have been considered in SA3. An email discussion will take place to agree a proposal for S3#17. The TS is 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.

2.3 Specifications/Reports

The following specifications and reports are submitted to this meeting.

2.3.1 Evaluation of Confidentiality/integrity Algorithms

SA#7 approved a report on the work performed by the SAGE task force to design

and specify the 3G confidentiality and integrity algorithms (3G TS 35.20x series). This report was published as 3G TR 33.908. SA#7 also approved the algorithms for distribution to 3GPP partners. However, publication of the algorithm specifications and the report on the evaluation results was delayed for procedural reasons.

On 4 September 2000 the algorithm specification were published on the ETSI web site at the following location:

http://www.etsi.org/dvbandca/

The evaluation results are now presented to SA#10 for approval in 3G TR 33.909 v1.0.0. SA#10 are asked to forward TR 33.909 to PCG for approval for publication by the Partner SDOs.

Doc-1st-Level	Doc-2nd-Level	Document title	Comment
SP-000629	S3-000660	TR 33.909 v1.0.0, Report on the evaluation of the 3GPP confidentiality and integrity algorithms	For approval by SA#10 and forwarding to PCF for approval for publication by the partner SDOs.

2.3.2 Authentication Algorithm Specifications

SA#7 approved the development of a standard authentication algorithm and the corresponding SAGE work plan. 3GPP approved the funding for this work in June 2000. The SAGE work is now complete on schedule. The SAGE authentication algorithm deliverables are presented to SA#10 for approval. SA#10 are asked to forward the SAGE authentication algorithm deliverables to PCG for approval for publication by the Partner SDOs.

Doc-1st-Level	Doc-2nd-Level	Document title	Comment
SP-000630	S3-000730	SAGE authentication algorithm deliverables	For approval by SA#10 and forwarding to PCF for approval for publication by the partner SDOs.

2.4 Change Requests

SA3 has generated a number of change requests that reflect a series of clarifications and corrections, especially to ensure a coherent Release 99. Several CRs on lawful interception have also been prepared.

2.4.1 GSM LI architecture (03.33)

The following CRs were agreed at SA WG3 meeting #16 and are presented to TSG SA #10 for approval.

Note that CR 003 to R99 (version 8.0.0) is classified as category “C” but corresponds to Lawful Interception requirements already agreed for R99.

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
SP-000623	03.33	002		R98	Addition of parameters to the X3-Interface	C	7.1.0	S3	S3-16	S3-000762

SP-000623	03.33	003		R99	Addition of parameters to the X3-Interface	C	8.0.0	S3	S3-16	S3-000762
SP-000624	03.33	004		R98	Deletion of mono-mode and addition of optimal routeing	F	7.1.0	S3	S3-16	S3-000764
SP-000624	03.33	005		R99	Deletion of mono-mode and addition of optimal routeing	A	8.0.0	S3	S3-16	S3-000764

2.4.2 3G LI architecture (33.107)

The following CR was agreed at SA WG3 meeting #16 and is presented to TSG SA #10 for approval.

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
SP-000625	33.107	001		R99	Addition of parameters to the X3-Interface	F	3.0.0	S3	S3-16	S3-000763

2.4.3 Security architecture (33.102)

The following CRs were agreed at SA WG3 meeting #16 and are presented to TSG SA #10 for approval.

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
SP-000626	33.102	129		R99	Corrections on ciphering and integrity protection	F	3.6.0	S3	S3-16	S3-000666
SP-000626	33.102	130		R99	Re-transmission of authentication request using the same quintet	F	3.6.0	S3	S3-16	S3-000725
SP-000626	33.102	131		R99	Corrections to Counter Check procedure	F	3.6.0	S3	S3-16	S3-000726
SP-000626	33.102	132		R99	Intersystem handover for CS Services – from GSM BSS to UTRAN	F	3.6.0	S3	S3-16	S3-000727
SP-000626	33.102	133		R99	Correction on use of GSM MS classmark in UMTS	F	3.6.0	S3	S3-16	S3-000729
SP-000626	33.102	134		R99	START value handling for MS with a GSM SIM inserted	F	3.6.0	S3	S3-16	S3-000739

2.4.4 Algorithm requirements (33.105)

The following CR was agreed at SA WG3 meeting #16 and is presented to TSG SA #10 for approval.

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
SP-000627	33.105	015		R99	Layer 2 related corrections	F	3.5.0	S3	S3-16	S3-000667

2.5 Work programme

A structured programme of security work items is being regularly reviewed and maintained by SA3 and the MCC representative.

Fifteen Work Item Descriptions (WID) were approved at SA#8. Two revised WIDs and six new WIDs were approved at SA#9. One revised WID is presented to SA#10 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#10 from SA WG2.

2.5.1 Revised Work Items

The following revised Work Item has been agreed by SA3 to be presented to SA#10 for approval.

Doc-1st-Level	Doc-2nd-Level	Work item title	Rapporteur
SP-000629		FIGS/IST work item description	Peter Howard

3 Outlook for Future Meetings

With the stability of the work for Release 99, SA3 will now continue with the work for R4 and R5. The main work items for R4 are network domain security and GERAN security, while the main work items for R5 are network domain security and IM subsystem security.

4 Planned Meetings of SA3

Title	Date	Location
S3#17	27 February - 1 March 2001	Sophia Antipolis, France
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	Madrid, Spain (location TBC)

Annex 1 Documents Provided to SA#9

Tdoc	Title	Agenda
SP-000620	Status Report to TSG SA#10	7.3.1
SP-000621	Report of SA WG3 ad-hoc meeting and draft report of meeting #16	7.3.1
SP-000622	LS from SA WG3: Security risks in introduction phase of MAP security	7.3.2
SP-000623	CRs 002 and 003 to 03.33: Addition of parameters to the X3-Interface	7.3.3
SP-000624	CRs 004 and 005 to 03.33: Deletion of mono-mode and addition of optimal routeing	7.3.3
SP-000625	CR001 to 33.107: Addition of parameters to the X3-Interface	7.3.3
SP-000626	CRs to 33.102	7.3.3
SP-000627	CR015 to 33.105: Layer 2 related corrections	7.3.3
SP-000628	Revised WI: FIGS/IST work item description	7.3.3
SP-000629	33.909 v1.0.0: Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms	7.3.3
SP-000630	SAGE deliverables 1, 2, 3 & 4	7.3.3
SP-000631	Information on WI “Network Domain Security”	7.3.1

Annex 2 CRs Provided to SA#9

SA doc	Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
SP-000623	03.33	002		R98	Addition of parameters to the X3-Interface	C	7.1.0	S3	S3-16	S3-000762
SP-000623	03.33	003		R99	Addition of parameters to the X3-Interface	C	8.0.0	S3	S3-16	S3-000762
SP-000624	03.33	004		R98	Deletion of mono-mode and addition of optimal routeing	F	7.1.0	S3	S3-16	S3-000764
SP-000624	03.33	005		R99	Deletion of mono-mode and addition of optimal routeing	A	8.0.0	S3	S3-16	S3-000764
SP-000625	33.107	001		R99	Addition of parameters to the X3-Interface	F	3.0.0	S3	S3-16	S3-000763
SP-000626	33.102	129		R99	Corrections on ciphering and integrity protection	F	3.6.0	S3	S3-16	S3-000666
SP-000626	33.102	130		R99	Re-transmission of authentication request using the same quintet	F	3.6.0	S3	S3-16	S3-000725
SP-000626	33.102	131		R99	Corrections to Counter Check procedure	F	3.6.0	S3	S3-16	S3-000726
SP-000626	33.102	132		R99	Intersystem handover for CS Services – from GSM BSS to UTRAN	F	3.6.0	S3	S3-16	S3-000727
SP-000626	33.102	133		R99	Correction on use of GSM MS classmark in UMTS	F	3.6.0	S3	S3-16	S3-000729
SP-000626	33.102	134		R99	START value handling for MS with a GSM SIM inserted	F	3.6.0	S3	S3-16	S3-000739
SP-000627	33.105	015		R99	Layer 2 related corrections	F	3.5.0	S3	S3-16	S3-000667

Annex 3 Specifications and Reports under SA3 Responsibility

Annex 3.1 SA WG3 Specifications and Reports

Specification			Title	Planned / achieved	Editor	Rel
TS	21.133	3.1.0	Security Threats and Requirements	April 99	Per Christoffersson	R99
TS	22.022	3.2.0	Personalisation of GSM ME Mobile functionality specification - Stage 1	Oct 99	Sebastien Nguyen Ngoc	R99
TS	33.102	3.6.0	Security Architecture	Mar 00	Bart Vinck	R99
TS	33.103	3.4.0	Security Integration Guidelines	Oct 99	Colin Blanchard	R99
TS	33.105	3.5.0	Cryptographic Algorithm requirements	Jun 99	Takeshi Chikazawa	R99
TS	33.106	3.1.0	Lawful interception requirements	Jun 00	Berthold Wilhelm	R99
TS	33.107	3.0.0	Lawful interception architecture and functions	Dec 99	Berthold Wilhelm	R99
TS	33.120	3.0.0	Security Objectives and Principles	April 99	Timothy Wright	R99
TR	33.900	1.2.0	Guide to 3G security	Mar 00	Charles Brookson	R99
TR	33.901	3.0.0	Criteria for cryptographic Algorithm design process	Jun 99	Rolf Blom	R99
TR	33.902	3.1.0	Formal Analysis of the 3G Authentication Protocol	Oct 99	Günther Horn	R99
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	Mar 00	Michael Walker	R99
TR	33.909	1.0.0	ETSI SAGE 3GPP Standards Algorithms Task Force: Report on the evaluation of 3GPP standard confidentiality and integrity algorithms	Dec 00	Michael Walker	R99
TS	35.201	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	Mar 00	Michael Walker	R99
TS	35.202	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	Mar 00	Michael Walker	R99
TS	35.203	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data	Mar 00	Michael Walker	R99
TS	35.204	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	Mar 00	Michael Walker	R99

Annex 3.2 SMG10 Specifications and Reports

Specification			Title	Editor	Rel
	01.31	7.0.1	Fraud Information Gathering System (FIGS); Service requirements - Stage 0	Timothy Wright	R98
	01.31	8.0.0	Fraud Information Gathering System (FIGS); Service requirements - Stage 0	Timothy Wright	R99
	01.33	7.0.0	Lawful Interception requirements for GSM	Bernie McKibben	R98
	01.33	8.0.0	Lawful Interception requirements for GSM	Bernie McKibben	R99
TS	01.61	8.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	Michael Walker	R97
GTS	02.09	3.1.0	Security Aspects	Per Christoffersson	Phase 1
ETS	02.09	4.5.0	Security Aspects	Per Christoffersson	Phase 2
ETS	02.09	5.2.0	Security Aspects	Per Christoffersson	Phase 2+
EN	02.09	6.1.0	Security Aspects	Per Christoffersson	R97
EN	02.09	7.1.0	Security Aspects	Per Christoffersson	R98
	02.09	8.0.0	Security Aspects	Per Christoffersson	R99
TS	02.31	7.1.1	Fraud Information Gathering System (FIGS) Service description - Stage 1	Timothy Wright	R98
	02.31	8.0.0	Fraud Information Gathering System (FIGS) Service description - Stage 1	Timothy Wright	R99
TS	02.32	7.1.1	Immediate Service Termination (IST); Service description - Stage 1	Timothy Wright	R98
	02.32	8.0.0	Immediate Service Termination (IST); Service description - Stage 1	Timothy Wright	R99
TS	02.33	7.3.0	Lawful Interception - Stage 1	Bernie McKibben	R98
	02.33	8.0.0	Lawful Interception - Stage 1	Bernie McKibben	R99
GTS	03.20	3.0.0	Security-related Network Functions	Sebastien Nguyen Ngoc	Phase 1 extension
GTS	03.20	3.3.2	Security-related Network Functions	Sebastien Nguyen Ngoc	Phase 1
ETS	03.20	4.4.1	Security-related Network Functions	Sebastien Nguyen Ngoc	Phase 2
	03.20	5.2.0	Security-related Network Functions	Sebastien Nguyen Ngoc	R96
TS	03.20	6.1.0	Security-related Network Functions	Sebastien Nguyen Ngoc	R97
TS	03.20	7.3.0	Security-related Network Functions	Sebastien Nguyen Ngoc	R98
	03.20	8.1.0	Security-related Network Functions	Sebastien Nguyen Ngoc	R99
	03.31	7.0.0	Fraud Information Gathering System (FIGS); Service description - Stage 2	Timothy Wright	R98
	03.31	8.0.0	Fraud Information Gathering System (FIGS); Service description - Stage 2	Timothy Wright	R99
TS	03.33	7.1.0	Lawful Interception - stage 2	Bernie McKibben	R98
	03.33	8.0.0	Lawful Interception - stage 2	Bernie McKibben	R99
	03.35	7.0.0	Immediate Service Termination (IST); Stage 2	Timothy Wright	R98
	03.35	8.0.0	Immediate Service Termination (IST); Stage 2	Timothy Wright	R99
	10.20	-	Lawful Interception requirements for GSM	Bernie McKibben	R99