Technical Specification Group Services and System Aspects **TSGS#09(00)0407**

Meeting #9, Kapolei, Hawaii, USA, 25-28 September 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

The TSG-SA WG3 meeting #14 was held in Oslo, Norway from the 1-4 August 2000. Dr Stefan Pütz (T-Mobil) chaired the meeting on the first day and Professor Michael Walker (Vodafone) chaired for the rest of the meeting. The secretary was Mr Maurice Pope from the MCC. The host was Telenor.

The TSG-SA WG3 meeting #15 was held in Washington DC, USA from the 12-14 September 2000. Professor Michael Walker (Vodafone) chaired the meeting and the secretary was Mr Maurice Pope from the MCC. A joint meeting with TIA TR-45 AHAG was held on the first day. The hosts were Lucent, Qualcomm and TIA.

The group has been focussing on completing Release 99 together with addressing feedback from other working groups. There was also a review of the work required for Release 2000 to which end SA3 has produced a number of new and revised work item descriptions.

Doc-1st-Level	Doc-2nd-Level	Work item title	Comment
SP-000408		Reports of SA WG3 meetings held since SA#8	For information to SA#9

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 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/

A press release is also available:

http://www.etsi.org/press/algo3gpp.htm

The evaluation results will now also be published as 3G TR 33.909.

2.2 Authentication Algorithm

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. Work has been proceeding in SAGE and algorithm publication is scheduled for November 2000.

2.3 Harmonisation of 3GPP/3GPP2 Authentication

A second joint meeting with AHAG was held during S3#15 (September 2000). SA3 and TIA TR-45 AHAG are working on procedures for joint control of the 3GPP specifications for authentication, which are contained in SA3 technical standards. The current recommendations for joint control as developed by both groups is presented to SA#9 for information. These recommendations will also be presented to TR-45 by AHAG. Approval of these procedures is planned at SA#10.

AHAG require certain provisions to be included in the Release 2000 specifications which are intended to enhance control of security by the home environment. These provisions are positive authentication reporting and authentication vector revocation. A new Work Item description is presented to SA#9 to cover this (see later).

Doc-1st-Level	Doc-2nd-Level	Work item title	Comment
SP-000419	S3-000591	Recommendations for joint control	For information to SA#9

2.4 Specifications/Reports

No specifications or reports are submitted to this meeting.

As reported above, due to the recent publication of the 3G confidentiality and integrity algorithm specifications (3G TS 35.20x series), the evaluation report in 3G TS 33.908 which was approved at SA#7 will now be published. A CR to update the evaluation report slightly is expected at SA#10.

SA3 has created two new technical reports in the following areas:

- Principles for network domain security (R00)
- Principles for IM subsystem security (R00)

These will result in the following new technical standards:

- Network domain security architecture (R00)
- IM subsystem security architecture (R00)

The first specifications on network domain security are expected to be submitted to SA#10 for approval. These first specifications on network domain security for R00 will supersede specifications on MAP security which were part of earlier versions of the R99 security architecture but were subsequently removed.

2.5 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. One functional modification to an informative annex in a Release 99 specification is also submitted for approval. The details are given below.

2.5.1 Security Architecture (33.102)

The following corrective CRs were agreed at SA WG3 meetings #14 and #15 and are presented to TSG SA #09 for approval.

Doc-1st-Level	Doc-2nd-Level	Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New
SP-000442	S3-000483	33.102	095	2	R99	F	Handling of emergency call	3.5.0	
SP-000442	S3-000460	33.102	105		R99	F	Length of CFN	3.5.0	
SP-000442	S3-000429	33.102	106		R99	F	Clarification on Sequence Numbers (SQN - SEQ)	3.5.0	
SP-000442	S3-000430	33.102	107		R99	F	Replace IMUI and TMUI with IMSI and TMSI	3.5.0	
SP-000442	S3-000431	33.102	108		R99	F	Replace Quintuplet by Quintet	3.5.0	
SP-000442	S3-000464	33.102	109		R99	F	Conversion function c2	3.5.0	
SP-000442	S3-000485	33.102	110		R99	F	Update terminology regarding VLR/SGSN	3.5.0	
SP-000442	S3-000536	33.102	111		R99	F	Start of ciphering	3.5.0	
SP-000442	S3-000537	33.102	112		R99	F	Removal of ME triggered authentication during RRC connection	3.5.0	
SP-000442	S3-000540	33.102	113		R99	F	Removal of EUIC	3.5.0	
SP-000442	S3-000545	33.102	114		R99	F	Removal of duplicate text on USIM toolkit secure messaging and addition of a reference to 02.48 and 03.48 instead.	3.5.0	
SP-000442	S3-000547	33.102	115		R99	F	Removal of secure authentication mechanism negotiation.	3.5.0	
SP-000442	S3-000548	33.102	116		R99	F	Removal of HE control of some aspects of security configuration	3.5.0	
SP-000442	S3-000550	33.102	117		R99	F	Specification of authentication vector handling in serving network nodes.	3.5.0	
SP-000442	S3-000552	33.102	118		R99	F	Update of References	3.5.0	
SP-000442	S3-000569	33.102	120		R99	F	Change of parameter value x regarding the capability of the USIM to store information on past successful authentication events	3.5.0	
SP-000442	S3-000603	33.102	123		R99	F	Clarification on condition on rejecting keys CK and IK	3.5.0	
SP-000442	S3-000615	33.102	124		R99	F	Clarifications on the START parameter handling	3.5.0	
SP-000442	S3-000616	33.102	125		R99	F	New FRESH at SRNC relocation	3.5.0	
SP-000442	S3-000617	33.102	126		R99	F	Addition of authentication parameter lengths	3.5.0	
SP-000442	S3-000620	33.102	127		R99	F	Clarifications on the COUNT parameters	3.5.0	
SP-000442	S3-000621	33.102	128		R99	F	Minor editorial changes	3.5.0	

The following corrective CR was agreed at SA WG3 meeting #15 and is presented to TSG SA #09 for approval.

Doc-1st-Level	Doc-2nd-Level	Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New
SP-000411	S3-000578	33.102	104	1	R99	F	Re-transmission of authentication request using the same quintet	3.5.0	

The following functional CR was agreed at SA WG3 meeting #15 and is presented to TSG SA #09 for approval.

Although this is presented as a Category "C" Release 1999 CR, SA WG3 request approval of this change. This CR provides a set of examples in an **Informative Annex**, which will provide the opportunity for operators to choose from this set of example schemes if they wish, in order to improve better interoperability and to reduce the number of different schemes to be supported by manufacturers. This CR was supported by all delegates (i.e. operators and manufacturers) represented at SA WG3 meeting #15.

Doc-1st-Level	Doc-2nd-Level	Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New
SP-000412	S3-000568	33.102	119		R99	C	Profiles for sequence number management	3.5.0	

2.5.2 Integration Guidelines (33.103)

The following corrective CR was agreed at SA WG3 meetings #14 and #15 and are presented to TSG SA #09 for approval.

Doc-1st-Level	Doc-2nd-Level	Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New
SP-000443	S3-000493	33.103	010		R99	F	Removal of Network Wide Confidentiality for R99 (clause 6)	3.3.0	

2.5.3 Algorithm Requirements (33.105)

The following corrective CR was agreed at SA WG3 meeting #14 and is presented to TSG SA #09 for approval.

Doc-1st-Level	Doc-2nd-Level	Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New
SP-000444	S3-000473	33.105	013		R99	F	Deletion of eUIC	3.4.0	

2.5.4 Anonymity Key Calculation during Re-synchronisation (33.102, 33.103, 33.105)

The following corrective CRs were agreed at SA WG3 meeting #15 and are presented to TSG SA #09 for approval.

Doc-1st-Level	Doc-2nd-Level	Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New
SP-000445	S3-000601	33.102	122		R99	F	Change of computation of the anonymity key in the re-synchronisation procedure	3.5.0	
SP-000445	S3-000612	33.103	012		R99	F	Computation of the anonymity key for re-synchronisation	3.3.0	
SP-000445	S3-000494	33.105	012		R99	F	Calculation of AK in re-synchronisation	3.4.0	
SP-000445	S3-000613	33.105	014		R99	F	Anonymity key computation during re-synchronisation	3.4.0	

2.5.5 Clarification on integrity and ciphering (33.102, 33.103)

The following corrective CRs were agreed at SA WG3 meeting #15 and are presented to TSG SA #09 for approval.

Doc-1st-Level	Doc-2nd-Level	Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New
SP-000446	S3-000573	33.102	121		R99	F	Clarifications on integrity and ciphering of radio bearers.	3.5.0	
SP-000446	S3-000586	33.103	011	1	R99	F	Correction to BEARER definition	3.3.0	

2.6 Release 2000

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

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

2.6.1 Revised Work Items

The following revised Work Items have been agreed by SA3 to be presented for approval in document SP-000420.

Doc-1st-Level	Doc-2nd-Level	Work item title	Rapporteur
SP-000420	S3-000606	Network domain security	Geir Koien
SP-000420	S3-000626	Access security for IP-based services	Krister Boman

2.6.2 New Work Items

The following new Work Items have been agreed by SA3 to be presented for approval in document SP-000421.

Doc-1st-Level	Doc-2nd-Level	Work item title	Rapporteur
SP-000421	S3-000488	UE triggered authentication during connections	Peter Howard
SP-000421	S3-000490	Enhanced home control of security by HE	Peter Howard
SP-000421	S3-000599	USIM toolkit security	Peter Howard
SP-000421	S3-000609	Location services security	Valtteri Niemi
SP-000421	S3-000610	VHE security	Colin Blanchard
SP-000421	S3-000611	Study on network-based denial of services attacks	Dan Brown & Rong Shi

3 Outlook for Future Meetings

With the stability of the work for Release 99, SA3 will now continue with the work for Release 2000. An ad hoc meeting will be held to progress work items concerning IM subsystem security and network domain security.

4 Planned Meetings of SA3

Title	Date	Location
S3 ad hoc on IM subsystem security and	8-9 November 2000	Munich, Germany

network domain security		
S3#16	28-30 November 2000	Jerusalem, Israel
S3#17	27 February - 1 March 2001	Sophia Antipolis, France
S3#18	21 or 22 - 24 May 2001	Location TBA

Annex 1 Documents Provided to SA#9

Tdoc	Title	Agenda
SP-000407	SA WG3 Status Report to TSG SA#09	7.3.1
SP-000408	Reports of SA WG3 meetings held since SA#08	7.3.1
SP-000411	1 Corrective CR to TS 33.102: Re-transmission of authentication request using the same quintet	7.3.3
SP-000412	1 Functional CR to TS 33.102: Profiles for sequence number management	7.3.3
SP-000418	Presentation slides of SA WG3 Status Report to TSG SA#09	7.3.1
SP-000419	Recommendation on joint AKA control	7.3.1
SP-000420	Revised work item descriptions	7.3.3
SP-000421	New work item descriptions	7.3.3
SP-000442	23 corrective CRs to 33.102	7.3.3
SP-000443	2 corrective CRs to 33.103	7.3.3
SP-000444	1 corrective CR to 33.105	7.3.3
SP-000445	CRs to 33.102, 33.103, 33.105 on anonymity key calculation during resynchronisation	7.3.3
SP-000446	CRs to 33.102, 33.103 to clarify that integrity and ciphering is applied to radio bearers	7.3.3

Annex 2 CRs Provided to SA#9

Annex 2.1 SA WG3 CRs at SA#9

Doc-1st-Level	Doc-2nd-Level	Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New
SP-000442	S3-000483	33.102	095	2	R99	F	Handling of emergency call	3.5.0	
SP-000411	S3-000578	33.102	104	1	R99	F	Re-transmission of authentication request using the same quintet	3.5.0	
SP-000442	S3-000460	33.102	105		R99	F	Length of CFN	3.5.0	
SP-000442	S3-000429	33.102	106		R99	F	Clarification on Sequence Numbers (SQN - SEQ)	3.5.0	
SP-000442	S3-000430	33.102	107		R99	F	Replace IMUI and TMUI with IMSI and TMSI	3.5.0	
SP-000442	S3-000431	33.102	108		R99	F	Replace Quintuplet by Quintet	3.5.0	
SP-000442	S3-000464	33.102	109		R99	F	Conversion function c2	3.5.0	
SP-000442	S3-000485	33.102	110		R99	F	Update terminology regarding VLR/SGSN	3.5.0	
SP-000442	S3-000536	33.102	111		R99	F	Start of ciphering	3.5.0	
SP-000442	S3-000537	33.102	112		R99	F	Removal of ME triggered authentication during RRC connection	3.5.0	
SP-000442	S3-000540	33.102	113		R99	F	Removal of EUIC	3.5.0	
SP-000442	S3-000545	33.102	114		R99	F	Removal of duplicate text on USIM toolkit secure messaging and addition of a reference to 02.48 and 03.48 instead.	3.5.0	
SP-000442	S3-000547	33.102	115		R99	F	Removal of secure authentication mechanism negotiation.	3.5.0	
SP-000442	S3-000548	33.102	116		R99	F	Removal of HE control of some aspects of security configuration	3.5.0	
SP-000442	S3-000550	33.102	117		R99	F	Specification of authentication vector handling in serving network nodes.	3.5.0	
SP-000442	S3-000552	33.102	118		R99	F	Update of References	3.5.0	
SP-000412	S3-000568	33.102	119		R99	C	Profiles for sequence number management	3.5.0	
SP-000442	S3-000569	33.102	120		R99	F	Change of parameter value x regarding the capability of the USIM to store information on past successful authentication events	3.5.0	
SP-000446	S3-000573	33.102	121		R99	F	Clarifications on integrity and ciphering of radio bearers.	3.5.0	
SP-000445	S3-000601	33.102	122		R99	F	Change of computation of the anonymity key in the re-synchronisation procedure	3.5.0	
SP-000442	S3-000603	33.102	123		R99	F	Clarification on condition on rejecting keys CK and IK	3.5.0	
SP-000442	S3-000615	33.102	124		R99	F	Clarifications on the START parameter handling	3.5.0	
SP-000442	S3-000616	33.102	125		R99	F	New FRESH at SRNC relocation	3.5.0	
SP-000442	S3-000617	33.102	126		R99	F	Addition of authentication parameter lengths	3.5.0	
SP-000442	S3-000620	33.102	127		R99	F	Clarifications on the COUNT parameters	3.5.0	
SP-000442	S3-000621	33.102	128		R99	F	Minor editorial changes	3.5.0	
SP-000443	S3-000493	33.103	010		R99	F	Removal of Network Wide Confidentiality for R99 (clause 6)	3.3.0	
SP-000446	S3-000586	33.103	011	1	R99	F	Correction to BEARER definition	3.3.0	
SP-000445	S3-000612	33.103	012		R99	F	Computation of the anonymity key for re-synchronisation	3.3.0	
SP-000445	S3-000494	33.105	012		R99	F	Calculation of AK in re-synchronisation	3.4.0	
SP-000444	S3-000473	33.105	013		R99	F	Deletion of eUIC	3.4.0	
SP-000445	S3-000613	33.105	014		R99	F	Anonymity key computation during re-synchronisation	3.4.0	

Annex 2.2 SMG10 CRs at SA#9

None.

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	3.1.0	Personalisation of GSM ME Mobile functionality specification - Stage 1	Oct 99	Sebastien Nguyen Ngoc	R99
TS	33.102	3.5.0	Security Architecture	Mar 00	Bart Vinck	R99
TS	33.103	3.3.0	Security Integration Guidelines	Oct 99	Colin Blanchard	R99
TS	33.105	3.4.0	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	3.0.0	ETSI SAGE 3GPP Standards Algorithms Task Force: Report on the evaluation of 3GPP standard confidentiality and integrity algorithms	Jun 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