3GPP TSG SA WG3 Security — S3#10 **S3-000029**

19-21 January, 2000

Antwerpen, Belgium

Source: **MCC**

Title: **SA WG3 extract of TSG SA #5 Draft Meeting Report**

Document for: **Information**

Agenda Item:

The following is an extract of the SA WG3 part of the TSG SA Meeting #6 Draft Report:

5.3 TSG SA WG3

5.3.1 Report from TSG SA WG3

TD SP-99583: The Report from SA WG3 to TSG SA (presentation slides) was presented by the SA WG3 Vice Chairman, Dr. Stefan Pütz.

5.3.2 Questions for advice and decisions from TSG SA WG3

TD SP-99553: This contains a liaison to TSG SA on MAP Security.

TD SP-99592: This contribution contains 4 Liaisons Statements from SA WG3 on:

- **MAP security:**

  A comment that the urgency of this work may be overestimated by SA WG3. It was also asked whether the MAP is the only type of signalling intended to be secured. It was explained that the intention is to start with MAP and then extend to other types of signalling. The CN could be impacted if this is intended to be included in Release 1999.

  It was suggested to call an ad-hoc meeting to discuss the way forward between network and security experts to ensure a solution is adopted which will be backward compatible in the future and is reasonable to implement in a short timescale.

  It was suggested that due to the cross border access on the MAP that can be expected, it may be better to set up a "Security Hooks" workshop or ad-hoc to look into including hooks into the system for future specification.

  It was concluded that in order to estimate the feasibility of having the necessary work available in time for Release 1999 without jeopardising the completion of the other work, a meeting between security and Core Network experts should be held. This meeting should study and decide on the feasibility, solutions and impact on inclusion in Release 1999. The backward compatible system evolution should also be taken into account in this decision, rather than a "quick fix" which may need re-design in the future. SA WG3 have proposed a meeting with CN experts in January 2000 to talk about this and believe it can be completed for Release 1999 in the March timescale for late inclusion. At the March 2000 meeting it can be decided if it has been achieved or should be included only into Release 2000. An small group was tasked to draft a document describing the way forward for the open security issues (see TD SP-99622).

TD SP-99622: Way forward for open Release 1999 security issues from the ad-hoc group on Open issues on security. The document was presented and the solution **approved** as a way forward by TSG SA.

- **TIA TR-45 AHAG**

  TR45 has adopted the 3GPP proposed Security algorithm. They have requirements which require study and SA WG3 have produced this liaison asking for a joint session with TR45 Security group at the SA WG3 meeting in April 2000. It was noted that there still may be a need to do some lobbying in TIA on some security issues.

- **Authentication failure message**

  This is a liaison informing N2 that a new mechanism for reporting authentication failure from VLR/SGSN to HLR is being specified in 3G TS 33.102. This was noted by TSG SA as for Information. It was reported that TSG CN had not received the liaison, and it was decided to include it in the meeting on MAP Security.

- **VHE/OSA security.**

  This liaison was also not received by CN and was added to the list for discussion between SA WG3 and TSG CN. The liaison statement was for information to TSG SA and was noted.

SA WG3 offered to assist in the review of all the relevant specifications for all the security work topics on completion of the tasks by the different TSGs, in order to ensure that SA WG3 security features are properly implemented in the Release 1999 specifications and to identify where corrective CRs are required.

The review of the ciphering algorithm is progressing on target and is expected to be complete for March 2000.

5.3.3 Approval of Release 1999 contributions from TSG SA WG3

Specifications:

3G TS 23.048, USIM toolkit security

- Transfer of GSM 03.48 v8.1.0 into 3G Release 1999
- Enhancements for Release 2000

3G TS 22.022, ME personalisation (now under SA WG3 control)

- Transfer of GSM 02.22 into 3G Release 1999
- Do we need this feature in Release 2000?

TD SP-99514: Liaison statement from TIA TR-45: This liaison was noted.

TD SP-99503: LS on emergency calls. The liaison was provided for information and was noted.

5.3.4 Approval of contributions from TSG SA WG3

The status of the approval of CRs from SA WG3 are given in Annex E, section E.3. The reported discussion is only for any CRs which were not approved or approved with important comments.

TD SP-99590: 3G TS 21.133: CR001 **Approved**.

TD SP-99584: 3G TS 33.102 CR022, CR025, CR026, CR027, CR030, CR032, CR033*, CR034*, CR035, CR036, CR037, CR038, CR039, CR040: **Approved**.

* The cover sheet of these CRs has the titles of CR033 and CR034 reversed. MCC were asked to ensure that the CR database reflects the actual CRs presented and not the cover sheet information.

3G TS 33.102 CR041 which appears on the list of CRs in TD SP-99584 was withdrawn. This subject will be added as an open item from SA WG3 for Release 1999 completion.

TD SP-99385: 3G TS 33.102 CR031 (Removal of alternative authentication mechanism described in Annex D): This was approved by SA WG3, but with an objection from Lucent technologies, so SA WG3 ask for Plenary decision on approval. There have been 2 authentication mechanisms in the specification since the start of 1999, the Annex D mechanism was proposed by Lucent Technologies. The criteria required to revert to the Annex D mechanism has not been reached and SA WG3 feel it should be removed. The Annex D mechanism is an alternative proposal to the 3GPP mechanism.

Lucent technologies reported that if the mechanism was not needed in the document as a fall back solution, then there was no objection to its removal. This was confirmed and the CR was **approved**.

TD SP-99587: 3G TS 33.105 CR004 and CR005: **Approved**.

TD SP-99589: 3G TR 33.902 CR001: **Approved**.

TD SP-99586: 3G TS 33.103 CR001, CR002 and CR004: **Approved**

TD SP-99588: 3G TS 33.106 CR001: Lawful interception requirements. It was confirmed that there was no impact on the work of TSG CN as the work is already complete for inclusion in Release 1999. **Approved**.

TD SP-99591: 3G TS 33.107 version 1.0.0: Lawful Interception Architecture and Functions was presented for approval. This was presented for immediate approval because LI will be a mandatory regulatory requirement for 3G systems. It was noted that slide 25 of the presentation contains erroneous specification number (should read 3G TS 33.107 in both cases). This had not been seen by SA WG2 and it was asked that it should be considered by SA WG2 at their next meeting.

The TSG CN Chairman asked if there was no impact on their work. This needs to be verified but little or no impact is expected. It was suggested that the document is taken for Information at this meeting and re-presented for approval in the March 2000 meeting after review by CN and SA WG2.

It was explained that the document is basically the equivalent to traditional fixed line and GSM access interception, but modified to include packet interception and additional requirements for 3G Networks.

After some discussion on the pros and cons to approval or delay until March 2000 the specification was **approved** and placed under TSG SA Change Control as version 3.0.0.

It is considered an exception to approve documents at their first appearance at a TSG meeting, which should only be done when there is no expected impact on other work and urgency requires it. In this case, concerned groups are expected to check the approved document for impacts.

E.3 CRs from SA WG3:

3GPP CRs

TSG SA Doc	SPEC	CR	rev	Current version	SUBJECT	TSG status	New version	Specification Title	cat
SP-99590	21.133	001		3.0.0	Data integrity of user traffic	approved	3.1.0	Security Threats and Requirements	C
SP-99584	33.102	022	1	3.2.0	Refinement of Enhanced User Identity Confidentiality	approved	3.3.0	Security Architecture	C
SP-99584	33.102	025		3.2.0	Length of KSI	approved	3.3.0	Security Architecture	C
SP-99584	33.102	026	1	3.2.0	Mobile IP security	approved	3.3.0	Security Architecture	B
SP-99584	33.102	027	1	3.2.0	Clarification of re-authentication during PS connections	approved	3.3.0	Security Architecture	C
SP-99584	33.102	030		3.2.0	Handling of the MS UEA and UIA capability information	approved	3.3.0	Security Architecture	C
SP-99585	33.102	031		3.2.0	Removal of alternative authentication mechanism described in annex D	approved	3.3.0	Security Architecture	C
SP-99584	33.102	032		3.2.0	Removal of network-wide encryption mechanism form application security section	approved	3.3.0	Security Architecture	F
SP-99584	33.102	033		3.2.0	Interoperation and intersystem handover/change between UTRAN and GSM BSS	approved	3.3.0	Security Architecture	C
SP-99584	33.102	034		3.2.0	Distribution of authentication data within one serving network domain	approved	3.3.0	Security Architecture	C
SP-99584	33.102	035		3.2.0	Authentication and key agreement	approved	3.3.0	Security Architecture	C
SP-99584	33.102	036		3.2.0	Sequence number management	approved	3.3.0	Security Architecture	C
SP-99584	33.102	037	1	3.2.0	Authentication and key agreement	approved	3.3.0	Security Architecture	C
SP-99584	33.102	038		3.2.0	Clarification on system architecture	approved	3.3.0	Security Architecture	C
SP-99584	33.102	039		3.2.0	Updated definitions and abbrviations	approved	3.3.0	Security Architecture	D
SP-99584	33.102	040		3.2.0	An authentication failure report mechanism from SN to HE	approved	3.3.0	Security Architecture	B
SP-99584	33.102	041		3.2.0	UIA and UEA identifications	withdrawn		Security Architecture	B
SP-99586	33.103	001	1	3.0.0	Refinement of Enhanced User Identity Confidentiality	approved	3.1.0	Security Integration Guidelines	C
SP-99586	33.103	002	1	3.0.0	Corrections to figure 1	approved	3.1.0	Security Integration Guidelines	D
SP-99586	33.103	004		3.0.0	Change length of KSI (and other miscellaneous corrections)	approved	3.1.0	Security Integration Guidelines	C
SP-99587	33.105	004		3.1.0	Time variant parameter for synchronisation of ciphering	approved	3.2.0	Cryptographic Algorithm requirements	D
SP-99587	33.105	005		3.1.0	Direction bit in f9	approved	3.2.0	Cryptographic Algorithm requirements	D
SP-99588	33.106	001		3.0.0	Lawful Interception Requirements	approved	3.1.0	Lawful interception requirements	C

Status of SA WG3 Specifications:

TS	21.133	Security Threats and Requirements	3.1.0	April 99	S3	Per Christoffersson	CR @ TSG#6
TS	22.022	Personalisation of GSM ME Mobile functionality specification - Stage 1	3.0.1	Oct 99	S3		
TS	33.102	Security Architecture	3.3.1	April 99	S3	Bart Vinck	CR @ TSG#6
TS	33.103	Security Integration Guidelines	3.1.0	Oct 99	S3	Colin Blanchard	CR @ TSG#6
TS	33.105	Cryptographic Algorithm requirements	3.2.0	June 99	S3	Takeshi Chickawaza	CR @ TSG#6
TS	33.106	Lawful interception requirements	3.1.0	June 99	S3	Berthold Wilhelm	CR @ TSG#6
TS	33.107	Lawful interception architecture and functions	3.0.0	Dec 99	S3	Berthold Wilhelm	New at TSG#6
TS	33.120	Security Objectives and Principles	3.0.0	April 99	S3	Tim Wright	
TR	33.900	Guide to 3G security	0.0.0	Dec 99	S3	Charles Brookson	Delayed until TSG#7
TR	33.901	Criteria for cryptographic Algorithm design process	3.0.0	June 99	S3	Gert Roelofsen	
TR	33.902	Formal Analysis of the 3G Authentication Protocol with Modified Sequence number Management	3.1.0	Oct 99	S3	Guenther Horn	CR @ TSG#6