3GPP TSG SA WG3 Security — S3#28
6 - 9 May 2003
Berlin, Germany

S3-030267

Technical Specification Group Services and System Aspects

Draft Report

Meeting #19, Birmingham, UK, 17-20 March 2003

Source: **Secretary TSG SA (Maurice Pope, MCC)**

Title: **Extract of Draft Report of TSG SA meeting #19, version 0.0.5**

Status: **For information**

[...]

7.3 TSG SA WG3

7.3.1 Report from TSG SA WG3 and review of progress

TD SP-030094 Status Report from SA WG3 to TSG SA#19. The status report of SA WG3 to TSG SA Plenary #19 was presented by the SA WG3 Chairman.

Slide 19: It was clarified that SA WG3 were asked to do an evaluation of security mechanisms, and it needed clarification what the evaluation was to be against (3GPP/SA WG3 requirements or IETF requirements. The TSG CN Chairman reported that the intention was to ensure that nothing introduced by 3GPP would weaken their security. The TSG CN Chairman agreed to send an e-mail to enable the channels for clarification of the security requirements from IETF to SA WG3.

Slide 22: It was clarified that the "joint meeting" with 3GPP2/AHAG was actually a co-located meeting with the group. The SA WG3 Chairman reported that these sessions consisted of 2 hours during the meeting where members of each group discussed interoperability issues with their security mechanisms.

Slide 15: GERAN Security - Uplink TDOA location method. It was clarified by the GERAN Chairman that GERAN had recognised that the proposal could have a security problem and therefore asked SA WG3 for advice on and analysis of this, rather than agreeing to the proposal at their meeting.

Slide 6: The ISIM/USIM issue had been discussed under the SA WG1 presentation, and agreed along the lines of the information from SA WG3 (i.e. ISIM is used if both ISIM and USIM exist on the UICC). It was further clarified by the SA WG1 Chairman that the CR had been discussed in SA WG1 (a revised CR taking this into account the agreements in TD SP-030174).

Slide 11: It was clarified that funding issues would be discussed under Liaisons in TD SP-030070 and TD SP-030074.

The SA WG3 Chairman reported that elections for SA WG3 Chairman and Vice-Chairmen's positions were due at the next SA WG3 meeting and that he did not intend to stand for the Chairmanship position this time.

The SA WG3 Chairman was thanked for his report, which was then noted. The SA WG3 Chairman was thanked for his work in Chairing the group since it's formation in the 3GPP Project. He thanked his SA WG3 management team for their good support during his term of office.

TD SP-030095 Draft report of SA WG3 meetings since TSG SA#18. The draft report of the last meeting of SA WG3 (meeting #27) was provided for information and was noted.

7.3.2 Questions for advice from TSG SA WG3

TD SP-030069 SA WG3 response on the "Additional Release 5 work needed for Policy Control and Subscription Control of Media". This was introduced by the SA WG3 Chairman and reports that no security features were considered necessary to protect this and other SIP messages of a similar nature. It was noted that no specific problems had been identified by SA WG3. The LS was then noted.

TD SP-030070 LS (from SA WG3) to SA on back up algorithms for UTRAN. TD SP-030074 was provided with a revised version of the attachment (Provisional work plan) to this LS.

It was clarified that the deployment of the second algorithm would be done and it would lie dormant unless needed and then "switched on". It was further clarified that the new algorithm would have the same (very low) possibility of compromise as the original, and therefore, theoretically, could be compromised before the original algorithm.

Considering the budget restrictions, the TSG SA Chairman thought that the only way this funding could be raised would be by reducing the MCC budget (and therefore support), by planning for the next budget year or by asking whether Operators would be interested in Sponsoring the development of the algorithm. It was considered unlikely that the funding could be found with the current budget. The SA WG3 Chairman responded that the issue was of interest to both Operators and Manufacturers, although he could provide a request to the GSMA. The SA WG3 Chairman was asked and agreed to write a letter to all the MRPs ~~asking for support of funding for this~~ outlining the budgetary constraints for the design of this backup algorithm activity. **It was clarified that any funding allocated would be administered by the OPs and the PCG, rather than through TSG SA.**

TD SP-030074 Provisional work plan for the design of the 3GPP confidentiality and integrity algorithms UEA2 and UIA2. This was provided as a revision to the attachment in TD SP-030070. **It was agreed that provided the funding was made available for the work, then this preliminary schedule and work plan was acceptable and was endorsed.**

TD SP-030071 LS (from SA WG3) on: "Requirement to allow IMS access by means of SIM". This was introduced by the SA WG3 Chairman and reports that SA WG3 have serious reservations about the increased security risks to the high-profile IMS service by using the reduced-level security available using SIM. There were also threats to system credibility raised, where the perceived security breach could affect the visited network operator, even though the user has a SIM subscription in his home network and is using his home network IMS service while roaming. It was also thought that the IETF would have to be informed if this is allowed as they had assumed 128-bit strength AKA would be used with their standards.

The SA WG3 Chairman reported that the CR provided at the last TSG SA meeting, which had been rejected awaiting the decision on SIM access to IMS, had been reviewed briefly again by SA WG3 and it had been recognised that more work would be needed on this before approval.

However, all other CRs had been prepared by the other groups, pending the agreement in TSG SA, and the SA WG3 CR would have to take into account these CRs as a mapping of the security requirements to the modified specifications.

A "straw poll" was held to find how many of those present would be in favour of SIM access to IMS based on the information received at the meeting on the impacts of allowing this. The result was that there was no strong desire in the room to introduce this new functionality into Release 5. **It was therefore concluded that SIM access to IMS would not be added as a Feature to Release 5. Therefore any CRs for SIM access to IMS in Release 5 that have been Approved, were now considered as Rejected.**

7.3.3 Approval of contributions from TSG SA WG3

CRs:

TD SP-030096 2 CRs to 33.108: Coding of ASN.1 parameters of the type OCTET STRING (Rel-5, Rel-6). These CRs were approved.

TD SP-030097 CR to 33.108: CS Section for 33.108 (Rel-6). This CR was approved.

TD SP-030098 CR to 33.108: Adjustments to the requirements on the delivery of the intercepted RT data over TCP (Rel-6). This CR was approved.

TD SP-030099 CR to 33.108: Incorrect ASN.1 object tree (Rel-5). This CR was approved.

TD SP-030100 CR to 33.203: Clarification of the use of ISIM and USIM for IMS access. This CR was approved.

TD SP-030101 CR to 33.203: Malicious UE bypassing the P-CSCF (Rel-5). It was explained that SA WG3 had recognised a severe security threat in the Rel-5 specifications and this CR had been created to add guidelines for the use of the mechanisms provided by the specifications. It was agreed that the "shall" in the bullets should be downgraded to "should". The CR was revised in TD SP-030185 which was approved.

TD SP-030102 CR to 33.203: Ensuring the deletion of unwanted SA's (Rel-5). This CR was approved.

TD SP-030103 CR to 33.203: Add protected port into Via header (Rel-5). This CR was approved.

TD SP-030104 2 CRs to 33.210: Za-interface and roaming agreements (Rel-5, Rel-6). These CRs were approved.

TD SP-030105 3 CRs to 33.210: Clarification to the re-keying aspects of network domain security (Rel-5, Rel-6). crs

TD SP-030111 1 CR to 33.203: Correction of the Port 2 definition for SA establishment. This CR was approved.

TD SP- 030149 2 CR to 33.108: Correction to implementation of CR 005 (Rel-5, Rel-6). This CR was approved.

WIDs:

TD SP-030106 WID: Lawful Interception in the 3GPP Rel-6 architecture. This WI description was approved.

TD SP-030107 Updated WID: Revised GERAN A/Gb mode security enhancements work item. This WI description was approved.

TD SP-030108 WID: Network Domain Security; Authentication Framework (NDS/AF). This WI description was approved.

TD SP-030109 Updated WID: 3GPP Generic User Profile Security. This WI description was approved.