SA3 Status Report to SA#27

Valtteri Niemi, SA3 Chairman

Contents

- **General aspects**
- **Status report on work items**
- **Actions expected from SA#26**

General aspects

Vice chairman of SA3 for many years, our respected colleague,

Michael Marcovici

passed away 2nd February 2005.

SA3 leadership

- **Chairman: Valtteri Niemi (Nokia)**
- **Secretary: Maurice Pope (MCC)**
- **Vice-chair**
  - **Peter Howard (Vodafone)**
- **Lawful interception (LI) sub-group**
  - **Chair: Brye Bonner (Motorola)**
  - **Vice Chair: Alex Leadbeater (BT)**
  - **Secretary: Rupert Thorogood (UK Home Office)**

Meetings since SA#25

- **SA3 plenary**
  - **SA3#37: Sophia Antipolis, France, 21-25 February 2005, hosted by ETSI**

- **Lawful interception sub-group**
  - **SA3-LI#16, Barcelona, Spain, 18-20 January 2005, hosted by EF3**

Next SA3 plenary meetings

- **SA3#38: Geneva, Switzerland, 26-29 April 2005, hosted by EF3 and Orange**
- **SA3#39: Toronto, Canada, 28 June- 1 July 2005, hosted by NAF**

Next SA3-LI meetings

- **LI#17: Sophia Antipolis, France, 5-7 April 2005**
- **LI#18: Toronto (tbc), 14-16 June 2005**

Statistics at SA3#37

- **36 delegates attended**
- **183 temporary documents handled including**
  - **21 incoming LSs**
  - **11 outgoing LSs**

Summary of SA3 input to SA#27

- **1 SA3-LI CR for approval**
- **39 SA3 CRs for approval**
- **1 TR for approval**
- **1 WID for approval**
- **1 LS for discussion and decision**
- **1 LS to OMA BAC for information**
- **Status report from SA3 Chairman (info)**
- **Draft report of previous SA3 meeting (info)**

Status report on work items

Lawful interception

- **One CR to 33.108 (Rel-7) (SP-050125):**
  - **Aligning comments in National-HI3-ASN1parameters with comments in National-HI2-ASN1parameters**

IMS security

- **TR 33.978 "Security aspects of early IMS" submitted for approval (SP-050136)**
  - **Valuable input was received from CN1 and all of their suggestions have been implemented**
- **One CR to 33.203 (Rel-6) (SP-050137):**
  - **Addition of reference to early IMS security TR**
- **Participation of SA3 delegates in workshop with ETSI TISPAN was guaranteed**
- **It was agreed that whatever solution is chosen for Fixed IMS Access should not reduce the level of security for the Existing 3GPP IMS Access.**
- **Approval of WID on Rel-7 IMS security enhancements postponed until outcome of TISPAN workshop is known**

Network domain security: MAP layer

- **Three Rel-6 CRs to 33.200 (SP-050138):**
  - **Correct specification of addresses used in TCAP-Handshake**
  - **Addition of TCAP-Handshake for MO-ForwardSM**
  - **Improving the robustness of the TCAP handshake mechanism**
- **Work on MAPsec gateway concept has started**
- **An LS sent to CN4 about MAPsec gateway solution**
  - **There is a plan to 'delete' the MAPsec Rel-4 NE-based solution from the 3GPP specs, or to make it clear in the gateway specifications that interworking with the MAPsec Rel-4 NE-based solution is not supported.**

UTRAN access security

- **Two recent research papers on GSM and UMTS security were reviewed**
- **It was concluded that no changes to UMTS specs are needed but a recommendation from GSMA could be useful**
  - **Email discussion started on the issue, outcome may be an LS to GSMA**

GERAN access security

- **Feasibility study work has started on Access Security Enhancements (WID approved in SA#26)**

GAA – Generic authentication architecture 1/2

- **Three Rel-6 CRs to 33.220 (SP-050139):**
  - **Key derivation function: character encoding**
  - **Bootstrapping timestamp (there is a conditionally approved CR from CN4 related to this)**
  - **Storage of B-TID in GBA_U NAF Derivation procedure**
- **One Rel-6 CR to TR 33.919 (SP-050140):**
  - **Correct the "Application guidelines to use GAA"**
- **Discussions on potential GAA enhancements in Rel-7 have started**

GAA - 2/2

- **Three Rel-6 CRs to 33.222 (SP-050141):**
  - **Keeping PSK TLS in 3GPP Rel-6**
  - **Clarification to TS 33.222**
  - **Clarify the GBA requirements for https supporting applications at Ua reference point**
- **An LS from SA3 to SA#27 (SP-050144) asking permission for further study on issue of https terminating in the UICC**
  - **An early deadline agreed for contributions to next SA3 meeting**

WLAN inter-working security

- **Ten Rel-6 CRs to TS 33.234 (SP-050142):**
  - **Wu Reference Point Description**
  - **Replacing PDGW with PDG**
  - **Clarification on EAP-AKA(SIM) description in 3GPP IP access authentication and authorization**
  - **Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation**
  - **Clarifying the status that can't be changed in the security requirement of WLAN-UE split**
  - **WLAN AN providing protection against IP address spoofing**
  - **Clarification on the handling of simultaneous sessions**
  - **Removal of editors' notes**
  - **Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages**
  - **Using OCSP to Check Validity of PDG Certificate in 3GPP IP Access**

MBMS security 1/3

- **14 out of 17 remaining open issues were solved (see SP-040868). The remaining issues are:**
  - **Consistency check with SA4 specs**
  - **Consistency check threats --> requirements --> solutions**
  - **Editorial check**
- **Several LS's sent out**

MBMS security 2/3

- **Eighteen Rel-6 CRs to 33.246 (SP-050143):**
  - **Storing SP payload after MSK message is verified**
  - **ME based MBMS key derivation for ME based MBMS key management**
  - **Correct the MSK verification message handling**
  - **Clarify MUK key synchronisation for MSK push procedure**
  - **Add missing parts of CR33 (SA3#36)**
  - **Annex D1: correction of the description of the GBA run**
  - **Alignment according to MIKEY related IETF work**
  - **Clarification of HTTP procedures**
  - **Usage of security policy payload**

MBMS security 3/3

- Clarification of MSK and MTK procedures
- MGV-F functionality related to MTK-ID upper limit
- Alignment to SA4 terminology
- Introduction of BM-SC subfunctions
- Removing IDi from MTK message
- MBMS download protection details
- Removal of editors' notes
- Protection of MBMS Service Announcement sent over MBMS bearer
- Introduction of missing abbreviation, Symbols and definitions

Security for voice group call services

- **An issue pointed out in an LS from GERAN 2 was reviewed and a reply was sent**

New Work Item agreed in SA3

- **Liberty Alliance and 3GPP Security Interworking (SP-050145)**
  - **The results will be a report (TR) on how an interworking between 3G security methods and the Liberty Alliance framework could be realised, and suggestions to optimise the interworking between LAP and GAA.**
  - **Planned completion:**
    - **SA#28 (June 2005) for information**
    - **SA#29 (September 2005) for approval.**

Actions expected from SA#27

Documents for approval

CRs for approval:

- **(SP-050125) One Rel-7 CR to 33.108**
- **(SP-050137) One Rel-6 CR to 33.203**
- **(SP-050138) Three Rel-6 CRs to 33.200**
- **(SP-050139) Three Rel-6 CRs to 33.220**
- **(SP-050140) One Rel-6 CR to TR 33.919**
- **(SP-050141) Three Rel-6 CRs to 33.222**
- **(SP-050142) Ten Rel-6 CRs to TS 33.234**
- **(SP-050143) Eighteen Rel-6 CRs to 33.246**
- **TR for approval: (SP-050136)**
  - **TR 33.978: "Security aspects of early IMS" v 2.0.0**
- **WID for approval: (SP-050145)**
  - **Liberty Alliance and 3GPP Security Interworking**

Documents for information

SP-050123: Status Report from SA WG3 to TSG SA #27

SP-050124: Draft Report of SA WG3 meeting #37

SP-050135: Reply LS (to OMA BAC) to 'Status of OMA Mobile Broadcast Services'