SA3 Status Report to SA#17
SP-020504

Professor Michael Walker, Vodafone Group
SA3 Chairman

SA3 Leadership

Chairman: Michael Walker (Vodafone)

Secretary: Maurice Pope (MCC)

Vice-chairs:

- **Michael Marcovici (Lucent)**
- **Valtteri Niemi (Nokia)**

LI sub-group chair:

- **Brye Bonner (Motorola)**

Meetings Held

- **SA3 Plenary**
  - **SA3#24: 9-12 July 2002**
  - **Helsinki, Finland**
  - **Report in SP-020505**
- **Lawful interception sub-group**
  - **LI#03/02: 4-6 June 2002**
  - **Budapest, Hungary**

SA3 General Status

- **Focus has been on completing IMS security architecture for Release 5**
- **New ciphering algorithm specifications for GSM, EDGE and GPRS have been produced**
- **Release 6 feasibility study on authentication framework to support NDS/IP evolution has been completed**
- **Five new Release 6 work items have been created**

Lawful Interception

- **Release 5 CRs**
  - **33.106 LI requirements**
    - **clarify interception handling requirements**
  - **33.107 LI architecture**
    - **clarify meaning of timestamp used in packet data records**
    - **add extra parameters to X3-interface for alignment with 33.108**
  - **33.108 LI handover interface specification**
    - **miscellaneous corrections**
- **Further IMS-related CRs are expected**

IMS Security (1)

- **Several corrections and clarifications made to the IMS security architecture (33.203)**
- **An annex is added which gives 3GPP-specific extension parameters to draft-ietf-sip-sec-agree**
- **Some clarifications are needed on SA lifetime but it was felt that further investigations were required before a CR could be approved**

IMS Security (2)

- IMS security architecture is dependant on some IETF work
  - draft-ietf-sip-digest-aka-03.txt:
    - Same status as SA#16
    - IETF last call completed
    - It is not an RFC yet but an RFC number already allocated (RFC 3310)
  - draft-ietf-sip-sec-agree-04.txt:
    - Two new versions since SA#16
    - The document is awaiting IESG/security review

IP Layer Network Domain Security

- New Release 6 work item on authentication framework to support NDS/IP evolution presented at SA#16
  - SA wanted to see result of feasibility work before deciding whether rest of the work should be carried out
  - Feasibility study (TR 33.910) presented for information
  - The TR will be updated and used as the justification for the rest of the work
- Updated NDS/IP work item which will consider extending protection to Iu, Iur, Iub, Iupc and Gb interfaces
  - Updated WID presented for approval

MAP Layer Network Domain Security (MAPsec)

- **The Ze interface part of MAPsec automatic key management is not complete**
- **LS sent to CN4 requesting an estimate on the timescales for completing the Ze interface specifications**
- **Decision on whether to remove automatic key management from the Release 5 spec will be taken after a response is received from CN4**
- **MAPsec automatic key management is also dependant on IETF draft-arkko-map-doi-07 which is awaiting IESG/security review before becoming an informational RFC**

GERAN Security

- Reply LS sent to GERAN on impact of moving LLC ciphering to the radio access network
- SA3#24 decided to hold an email discussion on the SA3 mailing list enhanced A/Gb mode security
- A summary of the email discussion has been agreed on the SA3 list and was presented at GERAN#11
  - This will be the basis for further discussion at SA3#25

Immediate Service Termination

- **Some corrections made to IST stage 2 (23.035) to correct the use of the IST command message and call termination indication parameter**
  - **An optimisation was introduced by CN4 into 29.002 in 1999 but not taken into account in 23.035**

A5/3 and GEA3

- New ciphering algorithms for GSM, EDGE and GPRS produced by ETSI SAGE
  - TS 55.216, TS 55.217, TS 55.218, TR 55.919 presented for approval
- Based on the KASUMI algorithm (TS 35.202)
- Current standards support 64 bit key but A5/3 and GEA3 allow for possible future enhancements to support longer keys (up to 128 bit)
- LS on introduction and adoption sent to GSMA TWG for forwarding to manufacturers
  - SA3 hope that equipment would be available from October 2004

Support for Subscriber Certificates

- **LS sent to SA2, SA1 (copy T2) on aspects of subscriber certificates**
  - **Answers were given to SA2 on architectural aspects**
  - **Guidance is asked from SA1 on service requirements for certificates to be issued to roaming subscribers by the visited network**
- **SA3 is currently working on the following open issues**
  - **Further elaboration of different usage cases and the need for so-called “proof of possession”**
  - **Compatibility with PKI solutions developed in other relevant standard fora, e.g. ETSI MCOM, WAP and IETF**
  - **Comparison with conventional “global PKI” approach**
  - **Implications on Lawful Interception**
  - **Review of different architectural solutions to support issuing of certificates**
  - **Trust issues; in particular, issues related to business relationships and resolution of disputes**

WLAN Interworking Security

- **New Rel-6 WID presented for approval**
- **Reply LS sent to SA1 answering questions on the trust model**
- **SA3 has reviewed draft TR on WLAN interworking from SA2 and sent comments via LS**
- **SA3 will use the material in the SA2 TR as the basis for a TS on WLAN interworking security**
- **MMAC HSWA and ETSI BRAN have been invited to the next SA3 meeting to discussion opportunities for co-operation on WLAN security**

New Release 6 Work Items

- **Support of the Presence Service Security Architecture**
- **3GPP Generic User Profile Security**
- **Release 6 User Equipment Management: Security aspects**
- **Security Aspects of Multimedia Broadcast/Multicast Service (MBMS)**
- **WLAN Interworking Security WID**

Future SA3 Meetings

- **SA3#25: 8-11 Oct 2002, Munich, Germany, hosted by Siemens**
- **SA3#26: 19-22 Nov 2002, location and host tbc**
- **SA3#27: 25-28 Feb 2003, location and host tbc**
- **SA3#28: 6-9 May 2003, location and host tbc**

- **LI #6: 24-26 Sep 2002, Helsinki, Finland**
- **LI #7: 12-14 Nov 2002, San Diego, USA**
- **LI #8: 18-20 Feb 2003, Paris, France**
- **LI #9: 13-15 May 2003, Sophia Antipolis, France**
- **LI #10: 16-18 Sep 2003, USA (tbc)**
- **LI #10: 18-20 Nov 2003, London**

Documents for information/approval

Documents for information/approval

- SP-020505 Report on SA3#24 – *for information*
- SP-020506 - *for approval*
  - TS 55.216: Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encryption Algorithm for GPRS. Document 1: A5/3 and GEA3 Specifications.
  - TS 55.217: Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encryption Algorithm for GPRS. Document 2: Implementors' Test Data.
  - TS 55.218: Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encryption Algorithm for GPRS. Document 3: Design Conformance Test Data.
  - TR 55.919: Design and Evaluation report.
- SP-020507 TR 33.910: Network Domain Security / Authentication Framework (NDS/AF); Feasibility Study to support NDS/IP evolution (Rel-6) – *for information*

CRs for approval

- SP-020583 Various Rel-5 CRs to 33.203 on IMS security (revised from SP-020508 and SP-020580)
- SP-020509 Rel-99/4/5 CRs to 23.035 on the use of the IST Command message and Call Termination Indication parameter
- SP-020510 Rel-5 CR to 33.106 to clarify interception capabilities
- SP-020511 Various Rel-5 CRs to 33.107 on LI architecture
- SP-020512 Rel-5 CR to 33.108 to correct inconsistencies

WIDs for approval

- **SP-020513 Revised WID: Network Domain Security; IP network layer security (NDS/IP) for Release 6**
- **SP-020514 Various new WIDs (Release 6):**
  - **Support of the Presence Service Security Architecture**
  - **3GPP Generic User Profile Security**
  - **Release 6 User Equipment Management: Security aspects**
  - **Security Aspects of Multimedia Broadcast/Multicast Service (MBMS)**
  - **WLAN Interworking Security WID**