SA3 Status Report to SA#15
SP-020106

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#22: 25-28 February 2002**
  - **Bristol, England**
  - **Hosted by Orange**
- **Ad-hocs**
  - **IMS security, NDS/IP and MAPsec, 31 January – 1 February 2002, Antwerp, Belgium, hosted by Alcatel**

(meeting reports are available in SP-020107)

- **Lawful interception sub-group**
  - **#1/02, 29-31 January 2002, Amsterdam, The Netherlands**

SA3 General Status

- **Focus has been on completing Rel-5 work (especially IMS security)**
- **Some maintenance of Rel-99 and Rel-4 specifications**
- **Some activity on new work areas for Rel-6**

Lawful Interception

- **Brye Bonner (Motorola) elected as chairperson of sub-group**
- **CRs to LI architecture 33.107 (Rel-99, Rel-4 and Rel-5)**
- **New handover interface specification (33.108) provided for information**
  - **Currently only covers PS domain (CS domain and IMS are for further study)**
  - **Should Annex G be moved to a regional version?**
- **Revised work item description presented for approval**

IP Multimedia Subsystem - #1

- **IMS security architecture 33.203 presented for approval (Rel-5)**
- **Integrity protection mechanism still open**
  - **Extended HTTP Digest defined for SIP or**
  - **A solution based on IPsec without IKE but SIP adopted**
- **33.203 will be presented to CN1 and CN4 on 8-9 April in Fort Lauderdale (TBC)**
- **Joint session with SA1 at SA3#23 on UE functionality split aspects (TBC)**

IP Multimedia Subsystem - #2

- **The stage 3 work based on 33.203 is dependant on various Internet Drafts not yet at RFC status**
  - **Encapsulating UMTS authentication in HTTP Digest (draft-niemi-sipping-digest-aka-00.txt)**
  - Security mechanism agreement for SIP sessions **(draft-arkko-sip-sec-agree-01.txt)**
    - **Potential fallback in 33.203 if this is not accepted**
  - **Extensions to RFC 2617 on HTTP Digest authentication (draft-undery-sip-auth-00.txt)**
  - **There are also various requirements drafts**

IP Multimedia Subsystem - #3

- **Security of SIP signalling between network nodes**
  - **SA3 solution is to use SIP-over-IPsec (according to NDS/IP 33.210)**
  - **IETF want to mandate SIP-over-TLS in all network nodes**
  - **SA3 consider this unnecessary for those 3GPP nodes that do not interface with non-3GPP nodes**

IP Network Layer Security (NDS/IP) - #1

- **The IP layer security architecture for network domain security (NDS/IP) is presented for approval as 33.210 (Rel-5)**
- **33.210 profiles IPsec and IKE for use in protecting 3GPP core network signalling**
- **Minimal changes from version presented for information at SA#14**

IP Network Layer Security (NDS/IP) - #2

- Referenced IETF work not yet at RFC status
  - The use of SCTP with IPsec (draft-ietf-ipsec-sctp-03.txt)
    - Relates to annex on IMS security only (Cx interface)
  - Use of AES algorithm is mentioned in editor's notes
    - 3DES/SHA-1 solution available now
    - AES modes have not yet been finalised by IETF
    - AES will be introduced when RFCs become available

MAP Security (MAPsec)

- A small CR was made to 33.200 Rel-4 to update the reference to the NIST standard used for encryption
- A single CR to add automatic key management for Rel-5 is presented for approval
  - Rationale for not splitting CR explained in a cover note
- CN4 will use 33.200 Rel-5 as the basis for the standardisation of the Ze interface between key administration centres and network elements
  - Joint session with CN4 was held at SA3#22
- Referenced Internet Drafts not yet at RFC status
  - The MAP Security Domain of Interpretation for ISAKMP (draft-arkko-map-doi-05.txt)

GERAN

- **Proposals from GERAN on the ciphering mechanism for Rel-5 were accepted by SA3**
  - **“COUNT” input to algorithm is composed of an 11-bit HFN and a 17-bit truncated GSM TDMA frame number**
  - **Rules for managing HFN**

UTRAN

- **RAN2 principles that were recently adopted to resolve outstanding issues in the UTRAN Rel-99 specifications were accepted by SA3**
- **Further work is required to understand whether it is needed to protect TM RLC mode SRBs in Rel-4 specifications**
- **A small CR to 33.102 Rel-99 to delete a message which has been removed from RAN2 Rel-99 specifications**

Immediate Service Termination

- **A CR to 43.035 Rel-4 was approved which corresponds to a Rel-99 CR which was not applied to Rel-4 by mistake**
- **The numbering of the stage 1 and stage 2 specifications will be corrected by MCC to reflect the fact that IST is independent of the radio access network**

Support for Subscriber Certificates

- **Initial contributions on this Rel-6 feature have been presented at SA3**
- **SA3 has clarified the scope of this work item in an LS to SA1**
- **A revised work item description is presented for approval**

Configuration of Ciphering

- **A CR to specify how terminals reject unciphered calls was rejected at SA#14**
- **SA#14 asked SA3 to consider USIM control, automatic calling devices and the need for AT command support**
- **CN1 have highlighted some other issues**
- **A new CR could not be approved at SA3#22**
- **There will be an email discussion to decided how to progress this feature in Rel-6**

New GSM Authentication Algorithm

- GSMA SG have suggested that Milenage is used as the basis for a new example GSM A3/A8
- SA3 endorsed this suggestion and recommended SAGE begin design and evaluation work
- SA3 suggest using Milenage in “GSM mode” which is already defined in 33.102
- The restriction on the use of Milenage needs to be relaxed to allow its use in GSM-only systems
  - Milenage is completely IPR-free

New GSM Encryption Algorithm

- **A new algorithm based on Kasumi is expected to be delivered May/June 2002**
- **Three modes of operation**
  - **A5/3 for GSM circuit-switched services**
  - **A variant of A5/3 for GSM EDGE**
  - **GEA3 for GSM GPRS**
  - **(UMTS f8 can be considered as a fourth mode of KASUMI)**

Other Topics (Rel-6) - #1

- **LSs sent on the following topics**
  - **User equipment management**
    - **New SA3 work item expected at SA#16**
  - **Location services enhancements**
    - **Joint session with SA1 at SA3#23 (TBC)**
  - **Presence service**
  - **Call trace**
- **Joint sessions/presentations at SA3#22**
  - **Open service access**
  - **Generic user profile**

Other Topics (Rel-6) - #2

- **In progress…**
  - **DRM**
    - **New SA3 work item expected at SA#16**
    - **Who should own the stage 2 specifications?**
  - **Push**
    - **Comments on stage 1 (TS 22.174) are being collected**
  - **Priority service**
    - **Comments on TR 22.950 are being collected**
    - **SA3 have concerns about PIN-based solutions**

Other Topics - #3

- In progress…
  - Multimedia messaging
    - Comments on TS 23.140 are being collected
    - SA3 have concerns about the use of HTTP basic authentication (cleartext password)
  - WLAN inter-working
    - Comments on TR 22.934 are being collected
    - Editor of SA1 TR will be invited to SA#24

Future SA3 Meetings

- SA3 IMS ad hoc: 8-9 Apr 2002, Fort Lauderdale, USA (TBC)
  - Joint session with CN1 and CN4 to present 33.203 (TBC)

- SA3#23: 14-17 May 2002, Victoria, Canada, hosted by AWS
  - Joint session with SA1 on location services and UE functionality split (TBC)
- SA3#24: 9-12 Jul 2002, Helsinki, Finland, hosted by Nokia
- SA3#25: 8-11 Oct 2002, Munich, Germany, hosted by Siemens

- LI #2/02: 9-11 Apr 2002, Orlando, USA
- LI #3/02: 4-6 Jun 2002, Budapest, Hungary (TBC)

Documents for information and approval

CRs - #1

- **SP-020108**
  - **CR to 33.102 Rel-99 to remove “TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)” from list of messages that need to be integrity protected**

CRs - #2

- SP-020109
  - CR to 33.107 on PDP context deactivation cause (Rel-5)
- SP-020160
  - CR to 33.107 on use of H.248 in setting up a bearer intercept point at the MGW (Rel-5)
- SP020161
  - 3 CRs to 33.107 on inter-SGSN RA update with active PDP context (R99, Rel-4, Rel-5)
- SP-020162
  - CR to 33.107 on addition of PDP context modification event and transferring the QoS information element across the X2 interface (Rel-5)

CRs - #3

- SP-020113
  - CR to 43.035 Rel-4 on IST for non-CAMEL subscribers
- SP-020114
  - CR to 33.200 Rel-4 on NIST special publication 800-38A updates on MEA-1 (MAP encryption)
- SP-020115
  - CR to 33.200 Rel-5 to add automatic key management (including cover note)

Documents for Information

- **SP-020118**
  - **TS 33.108: Handover interface for lawful interception (Rel-5)**

Documents for Approval

- **SP-020116**
  - **TS 33.203: Access Security for IP-based Services (Rel-5)**
- **SP-020117**
  - **TS 33.210: Network domain security; IP network layer security (Rel-5)**

WIs

- **SP-020119**
  - **Revised WI on support of subscriber certificates**
- **SP-020120**
  - **Revised WI on lawful interception**