SA3 status report to SA#16

Valtteri Niemi

Nokia Research Center

SA3 vice chairman

NOKIA

SA3 leadership

- SA3 chairman: Mike Walker (Vodafone)
- SA3 vice chairmen: Mike Marcovici (Lucent)

    Valtteri Niemi (Nokia)
- SA3 secretary: Maurice Pope (MCC)
- SA3 LI- subgroup chair: Brye Bonner (Motorola)

Meetings held

- SA3#23 in Victoria, Canada 14-17th May 2002
  - Hosted by AT&T Wireless and Rogers Wireless

- Ad hoc meeting (SA3#22bis) on IMS security, Ft. Lauderdale, Florida 8-9th April 2002
  - Joint sessions with both CN1 and CN4

- SA3 LI subgroup meetings
  - 9-11th April in Orlando, Florida
  - 4-6th June in Budapest, Hungary

SA3 general status

- Main focus on finalizing Rel. 5 work

- Some corrections on Rel. 99 and Rel. 4

- Rel. 6 work has started

NOKIA

Lawful interception

- Handover interface specification TS 33.108 presented for **approval** (SP-020357)
  - IMS part is now included
  - CS domain is covered by reference to ETSI and TIA specs
- Three CRs on 33.107 Rel. 5 (SP-020345)

NOKIA

IMS security

- An e-mail vote was organized to resolve the deadlock in the selection of IMS first-hop integrity protection mechanism
    - IPSEC/ESP – based solution was chosen by clear majority (18 against 6)
    - This implies a big CR to IMS security architecture 33.203 which moves the IPSEC mechanism from the Annex to main body (SP-020351)
- Eight other CRs against 33.203 Rel. 5 presented for **approval** (SP-020346-350 and SP-020352-354)
- Status of IETF specs on which stage 3 work is dependant
    - Draft-ietf-sip-digest-aka-03.txt: IETF last call finished without complications; it is not RFC yet but RFC number 3310 already allocated
    - Draft-ietf-sip-sec-agree-02.txt: Substantial comments were received in IETF last call; the current version addresses all the comments; IESG should decide soon about the way forward

IMS security (cont'd)

- An annex to 33.203 is still needed which gives the 3GPP-specific extension parameters to draft-ietf-sip-sec-agree. If the latter is never approved in IETF then a bigger CR is needed as a fall-back solution.

NOKIA

Network domain security: IP layer

- Two minor CRs against 33.210 Rel. 5 (SP-020355, SP-020356)

- For Rel. 6: New WID presented for approval:
  - Network domain security / Authentication framework (SP-020359)

NOKIA

MAP security

- The ball is handed over to CN4 who are to specify Ze-interface between MAPSEC Key Administration Center and MAP NEs

- MAPSEC TS 33.200 is dependant on IETF draft on MAPSEC DoI. IETF has required a security review of the draft before it can be accepted to become an informational RFC

Access security to CS/PS domains

- Four pairs of Rel. 99 / Rel. 4 correction CRs against 3G security architecture spec 33.102 presented for **approval** (SP-020340, SP-020342-344)

NOKIA

Immediate Service Termination

- Endorsement for changes in IST specification numbers is **requested**

NOKIA

Visibility and configurability of security

- A pair of Rel. 99 / Rel. 4 CRs against 33.102 presented for **approval** (SP-020341)
    - to clarify that ciphering indicator is not optional; it is mandatory

NOKIA

User Equipment Management

- A Rel. 99 / Rel. 4 CR pair against TS 22.022 "Personalisation of ME" spec presented for **approval** (SP-020339)
    - IMEI format corrected

© NOKIA   FILENAMs .PPT/ DATE / NN

NOKIA

Rel. 6 work with some progress

- Digital Rights Management (DRM) security:
  - WID presented for **approval** (SP-020358)

- Support for subscriber certificates

- Security aspects of WLAN interworking

- Push security

- LCS security
  - A joint session held with SA1

- Security aspects of UE split
  - A joint session held with SA1

- OSA security

- MBMS security

- Presence service

- GUP security

    FILENAMs .PPT/ DATE / NN

NOKIA

Future meetings

- SA3#24: 9-12th July 2002 in Helsinki (hosted by Nokia and Sonera)

- SA3#25: 8-11th October 2002 in Munich (hosted by Siemens)

- SA3#26: 19-22nd November 2002 (TBC)

- SA3 LI subgroup meeting in Sept./Oct. hosted by T-mobile (TBC)

NOKIA