SA3 Status Report to SA#18
SP-020697

Michael Walker, SA3 Chairman

SA3 Leadership

Chairman: Michael Walker (Vodafone)

Secretary: Maurice Pope (MCC)

Vice-chairs:

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

LI sub-group chair:

- Brye Bonner (Motorola)

Meetings Held

- SA3 Plenary
  - SA3#25: 8-11 October 2002
  - Munich, Germany
  - Report in SP-020698
- SA3 Plenary
  - SA3#26: 19-22 November 2002
  - Oxford, England
  - Report in SP-020698
- Lawful interception sub-group
  - LI#06/02: 24-26 September 2002
  - LI#07/02: 12-14 November 2002

Lawful Interception (1)

- Several essential changes to ensure that LI requirements are met in full
- Release 5 CRs
  - 33.107 LI architecture
    - timestamp can also be generated in HLR (SP-020702)
    - incorrect implementation of serving system report (SP-020703)
    - essential correction to LI events during inter-SGSN RAU (SP-020704)
  - 33.108 LI handover interface specification
    - essential correction to LI events during inter-SGSN RAU (SP-020704)
    - essential correction to Annex C1(SP-020705)
    - missing PDP context modification event (SP-020706)
    - Changes for US LI requirements (SP-020708)
- One Release 6 CR
  - 33.108
    - Several IRI (Intercept Related Information) records can be aggregated into one single file (SP-020707)

Lawful Interception (2)

- WID for LI in Rel-6 architecture
  - WID LI in Rel-6 Architecture (SP-020722)
- Members of the LI working group have requested that access to their input documents should be restricted because of fears that journalists and others may misuse them. After considerable discussion SA3 approve a liaison on the subject that asks for such documents to be protected by user name and password to permit access for 3GPP members only
  - LS to SA on change to Li subscription (SP-020699)

IMS Security (1)

- Several corrections and clarifications made to the IMS security architecture – notably on SA registration, lifetimes and handling in failure events
- Release 5 CRs
  - 33.203 IMS security architecture
    - Correction to IP-address acquisition in P-CSCF (SP- 020710)
    - Sending error response when P-CSCF receives unacceptable proposal (SP-020711)
    - Use of SAs in user authentication failure (SP-020712)
    - Clear editorial note (SP-020713)
    - Re-use and retransmission of RAND and AUTN (SP-020714)
    - Update of SIP security agreement syntax in App. H (SP-020715)
    - Registration and SA lifetimes (SP-020716)
    - TCP and UDP share same SA (SP-020760)
    - Indication that UE is no longer active in P-CSCF (SP-020761)

IMS Security (2)

- Release 5 CR
  - 33.203 IMS security architecture
    - Open issues on SA handling (SP-020717)
    - The issue was that CN1 did not implement an earlier SA3 CR on SA handling but instead implemented a different solution which was found to have a security problem. The CR aligns our spec with the CN1 solution and corrects a problem in the CN1 solution which has to be implemented at their next meeting

IMS Security (3)

- Use of SIM to access IMS services
  - Review was made of the technical feasibility of using a SIM to access IMS services. This was found to be technically possible.
  - Some members of SA3 expressed concern because the SIM was already reaching the end of its lifetime (in the sense that its security features needed upgrading) and the proposal would prolong its life
  - A CR was created in the event that SA approved the change in functionality to R5.
  - An LS on this topic is copied to TSG SA for information (SP-020811).
- Release 5 CR
  - 33.203 IMS security architecture
    - Allowing IMS access with SIM cards (SP- 020718)

IP Layer Network Domain Security NDS/IP

- TR 33.810 Network Domain Security:
  - Authentication Framework Feasibility Study
    - presented for approval (SP-020723)
  - New WID (SP-020722)
- Release 5 CRs
  - 33.210 Network Domain Security:
    - mandatory support for 3-DES encryption algorithm and removes references to AES (SP-020719)
- It was agreed that protection of RANAP over Iu is to be given the highest priority in Release, but security requirements for all UTRAN IP interfaces are to be studied
- Release 6 CRs
  - 33.210 Network Domain Security:
    - securing UTRAN/GERAN IP transport interfaces and specifically the Iu interface with NDS/IP mechs (SP-020720)

MAP Layer Network Domain Security (MAPsec)

- At the request of SA a reverse CR to change functionality by removing MAPsec automatic key management from 33.200 Release 5 was created in SA3#25 and approved in SA3#26
- Release 5 CR
  - 33.200 Network Domain Security:
    - removal of automatic key management R5 (SP020709)

UTRAN Security (1)

- **Reply LS sent to RAN2 on impact of re-use of COUNT-C values during handover**
- **Some CRs suggested by RAN2 to correct problems with START formula were reviewed, modified and approved**
  Release 99, 4 and 5 CRs to 33.102
  Correction to START formula (SP-020790)

UTRAN Security (2)

- Group release security study by e-mail concluded that it was not appropriate to introduce an additional security mechanisms to counter a denial of service attack at this stage. This is justified by the fact that denial of service has not been addressed and that a study of the vulnerability of UMTS to denial of service was needed. Proposals to be made at next meeting for R6 work item. RAN2 informed.
- It was agreed that work should begin on the provision of a second integrity and encryption algorithm as a replacement in case Kasumi is compromised. It should be stressed that S3 continues to have full confidence in Kasumi, the measure is merely a safeguard
  - LS to SA to approve design of new algorithm and forward to the PCC a request for funding (SP-020812)

GERAN Security (1)

- Corrections were made to allow USIM to access through GERAN only terminals
  - Release 5 CR to 33.102
    - USIM support in GERAN only terminals (SP-020700)
- The need to provide an encryption mechanism for ECSD and EGPRS was discussed and a way forward agreed
  - Release 6 CRs to 55.216, 55.217, 55.218, 55.219
    - EGPRS algorithms (SP-020721)

GERAN Security (2)

- GERAN A/Gb security enhancements were considered and a new WID approved
  - WID for R6
    - GERAN A/Gb security enhancements (SP-020820)

Support for Subscriber Certificates

- There was a wide ranging discussion of contributions on support for subscriber certificates covering architecture and trust, PKI , use of smart cards for subscriber digital signatures. The following was agreed:
  - The use of a smart card for subscriber digital signatures was necessary
  - SA3 should focus its work on subscriber certificates to 'bootstrapping' on SA3 defined mechanisms to establish secret keys for certificate management
  - Collaboration with and separation of roles between SA3, OMA, OASIS and W3C was needed – and SA3 favoured it having responsibility for co-ordination
  - Chairman to contact above groups and organise a joint workshop

WLAN Interworking Security

- A presentation to SA3#25 was given by Dr. Robert Hancock on behalf of ETSI/MMAC about their work in the area
- Work on TS 33.234 WLAN interworking security was progressed:
  - changes made to the requirements section to ensure statements only refer to security
  - Security features have been separated into those that could implemented within a ‘loose coupling’ (interworking) with UMTS and those that could best be provided within a ‘close coupling’ (integration)
  - Two proposals for identity confidentiality were considered
    - A simple approach based on the GSM TMSI method
    - An approach which uses PEAP to enhance EAP/SIM and EAP/AKA

  The first was adopted as a working hypothesis. This will be reviewed if PEAP is adopted to provide another security mechanism

Presence

- LSs to SA2 on architectural issues, including a security architecture, and use of HTTP
- A technical report TR 33.cde: Presence Service Security (Release 6) is being prepared.

Multimedia Broadcast/Multicast

- Principles for the security architecture and security requirements for MBMS are being etablished and discussed with/communicated to SA2, and a TR 33.cde: Security of Multimedia Broadcast/Multicast Service (Release 6) started
- S3 cannot progress on several issues until S2 develop and stabilise the MBMS Architecture. It was agreed that an ad-hoc meeting should be set up to discuss any results from S2 architecture work. It was agreed to try to join S2#30 in Milan on 24 February 2003. If this is not possible, then 24 February would be reserved in the S3 meeting #27 and invite experts from S2. A third option is to send some S3 delegates to S2#29 in January 2003.

G-MILENAGE

- The GSM version of MILENAGE has been delivered as an alternative for operators to the COMP 128 algorithms.
- It was clarified that the algorithm was partly sponsored by the GSMA. Ownership and distribution rights will be jointly shared between 3GPP and GSMA.
- The alleged attacks on Rijndael were not considered to pose any immediate threats. However, a replacement block cipher for MILENAGE may be considered to be developed next year, for backup reasons.
- Some bureaucracy regarding export control has to be finalized before deliveries can start.
  - TS 55.205 Specification of the G-MILENAGE-2G Algorithms: an Example Algorithm Set for the GSM Authentication and Key Generation Functions A3 and A8
  - Presented for approval (SP-020724)

Other Topics

- Extending MAP-based IST to PS services was considered but not progressed
- A review of Push stage 1 (TS 22.174v1.1.0) was made and comments sent to SA1
- No contributions on DRM, priority, location services user equipment functionality split, open service architecture, generic user profile (GUP), guide to 3G security or visibility and configurability of security

Other Topics

- FIGS specification numbering – it was agreed that the FIGS specification numbering should be modified as was done for IST. The SA3 agreed solution is described as follows:
  - withdraw 02.31 and 03.31 R99
  - create technically identical 22.031 and 23.031 R99
  - withdraw 42.031 and 43.031 Rel-4
  - create technically identical 22.031 and 43.031 Rel-4
  - create Rel-5 clones of the Rel-4 specs
- these changes should be reflected in updates to 01.01, 21.101, 41.102, 21.102, 41.103 and 21.103.
  - It has been checked that there are no cross references to the FIGS specifications from the CAMEL specs (22.078, 23.078 & 29.078).

Future SA3 Meetings

- SA3#27: 25-28 Feb 2003, Sophia Antipolis
- SA3#28: 6-9 May 2003, Berlin, European 'Friends of 3GPP'
- SA3#29: 15-18 July 2003, San Francisco (tbc), NA 'Friends of 3GPP' (tbc)
- S3#30, 7-10 October 2003, Italy (tbc)

- LI #7: 12-14 Nov 2002, San Diego, USA
- LI #8: 19-21 Feb 2003, Paris, France
- LI #9: 13-15 May 2003, Sophia Antipolis, France
- LI #10: 16-18 Sep 2003, USA (tbc)

Documents for information/approval

Documents for information/approval

- For Information:
  - SP-020697 Status report from SA WG3 to TSG SA#18
  - SP-020698 Reports of SA WG3 meetings #25 and #26
  - SP-020811 LS (from SA WG3) on Requirement to allow access to IMS by means of SIM
- For Approval:
  - SP-020723 Presentation of TR 33.810 version 2.0.0
  - SP-020724 Presentation of TR 55.205 version 1.0.0
  - SP-020699 LS on change to LI subscription
  - SP-020812 LS on second UMTS encryption/integrity algorithm

R5 CRs for approval (1)

- SP-020700 1 CR to 33.102 (Rel-5): USIM support in GERAN only terminals
- SP-020790 3 CRs to 33.102 (R99, Rel-4 and Rel-5): Correction to the START formula
- SP-020702 1 CR to 33.107 (Rel-5): Event Time
- SP-020703 1 CR to 33.107 (Rel-5): Incorrect implementation of the Serving System reporting
- SP-020704 2 CRs to 33.107 and 33.108 (Rel-5): Essential correction to the LI events generated during inter-SGSN RAU, when PDP context is active
- SP-020705 1 CR to 33.108 (Rel-5): Essential corrections to the Annex C.1 (ULIC)
- SP-020706 1 CR to 33.108 (Rel-5): Missing PDP Context Modification event
- SP-020708 1 CR to 33.108 (Rel-5): Changes to TS 33.108 for U.S. LI Requirements
- SP-020709 1 CR to 33.200 (Rel-5): Removal of Automatic Key Management from Release 5
- SP-020710 1 CR to 33.203 (Rel-5): Correction of IP address acquisition in P-CSCF
- SP-020711 1 CR to 33.203 (Rel-5): Sending error response when P-CSCF receives unacceptable proposal

R5 CRs for approval (2)

- SP-020712 1 CR to 33.203 (Rel-5): The use of SAs in user authentication failures
- SP-020713 1 CR to 33.203 (Rel-5): Clean up one Editor's note in 33.203
- SP-020714 1 CR to 33.203 (Rel-5): Re-use and re-transmission of RAND and AUTN
- SP-020715 1 CR to 33.203 (Rel-5): Update of SIP Security Agreement Syntax in Appendix H
- SP-020716 1 CR to 33.203 (Rel-5): Registration and SA lifetimes
- SP-020717 1 CR to 33.203 (Rel-5): Open issues in SA handling
- SP-020760 1 CR to 33.203 (Rel-5): TCP and UDP sharing same SA
- SP-020761 1 CR to 33.203 (Rel-5): Indication that UE is no longer active in P-CSCF
- SP-020718 1 CR to 33.203 (Rel-5): Allowing IMS access with SIM cards
- SP-020719 1 CR to 33.210 (Rel-5): Adding requirement to provide mandatory support for 3DES encryption in NDS/IP.Remove AES references and dependencies

R6 CRs for approval

- SP-020707 1 CR to 33.108 (Rel-6): Aggregation of IRI Records
- SP-020720 1 CR to 33.210 (Rel-6): Securing UTRAN/GERAN IP Transport interfaces and specifically the Iu interface with NDS/IP mechanisms
- SP-020721 4 CRs to 55.216, 55.217, 55.218 and 55.919 (Rel-6): EGPRS algorithm

WIDs for approval

- SP-020722 WID: Lawful Interception in the 3GPP Rel-6
- SP-020820 WID: GERAN A/Gb security enhancements