3GPP TSG-SA WG3 (Security)
Status Report to SA#14

17-20 December 2001

Kyoto, Japan

Maurice Pope

on behalf of

Professor Michael Walker

Chairman 3GPP TSG-SA WG3

Content of Presentation

- Report from TSG-SA WG3 and review of progress (AI 7.3.1)
- Questions for advice from TSG-SA WG3 (AI 7.3.2)
- Approval of contributions from TSG-SA WG3 (AI 7.3.3)

Report and Review of Progress in SA3 (AI 7.3.1)

- Contents for agenda item 7.3.1
  - General overview of progress
  - Meetings since SA#13
  - Lawful interception sub-group
  - A5/3 development
  - Presentation of documents for information
  - Meetings scheduled after SA#14

General Overview of Progress

- Several clarifications and corrections to various Rel-99/Rel-4 specifications
- Corrective Rel-4 CRs on MAP security
- Progress on Rel-5 work items
  - Rel-5 specifications and major Rel-5 changes to existing specifications presented to SA#14 for information (IMS security, IP network layer security and MAP security)
- In addition, SA3 has addressed feedback from other groups

Meetings Since SA#13

- S3-010606 – meeting reports for information
  - SA WG3 meeting #20, Sydney, Australia, 16-19 October 2001
  - Joint SA3/T3 meeting on ISIM, Sophia Antipolis, France, 26 November 2001
  - SA WG3 meeting #21, Sophia Antipolis, France, 27-30 November 2001

Lawful Interception Sub-Group

- The current chairperson, Rolf Schnitzler (D2 Vodafone), will resign at the end of this year
- A new chairman has not yet been elected
- Members are asked to consider providing suitable candidates for the chairmanship of this group

A5/3 Development

- Funding, ownership and distribution issues are now resolved
- The development work will start in ETSI SAGE in February 2002

TS 33.200, MAP Security (Rel-5) SP-010625

- Rel-5 MAPsec adds automatic key management by introducing Key Administration Centres (KAC) in PLMNs which communication with each other using Internet Key Exchange (IKE)
- Progress has been made on the IETF MAPsec Domain of Interpretation for the IKE – see 3GPP IETF dependencies and priorities document
- Proposed changes to TS 33.200 are presented to SA#14 for information
- Completion of the CR is expected at SA#15

TS 33.210, IP network layer security (Rel-5) SP-010623

- Specifies the use of IPsec/IKE to secure signalling within and between networks
- Covers IP based signalling within the core network including GTP, IMS signalling
- TS 33.210 is presented to SA#14 for information
- Presentation for approval is expected at SA#15

TS 33.203, Access Security for IP-based Services (Rel-5) SP-010624

- Authentication and session key agreement architecture
- Security mode establishment
- Two approaches for protecting access link (UE to P-CSCF) using IPsec or SIP-level protection
  - Only one approach will be included in final version
- Several dependencies on IETF documents - see 3GPP IETF dependencies and priorities document
- TS 33.203 is presented to SA#14 for information
- Presentation for approval is expected at SA#15

Meetings Scheduled after SA#14

- SA3 ad hocs, 31 January – 1 February 2002, Antwerp, Belgium
- SA3#22, 26 February – 1 March 2002, Bristol, UK
- SA3#23, 14-17 May 2002, Victoria, Canada
- SA3#24, 9-12 July 2002, Helsinki, Finland (TBC)
- SA3#25, 15-18 October 2002, Munich, Germany (TBC)

Questions for Advice from S3 (AI 7.3.2)

- SP-010604 – LS to SA from SA3
  - Security and privacy requirements of presence service

Approval of Contributions from SA3 (AI 7.3.3)

- Contents for agenda item 7.3.3
  - CRs to TS 21.133, Security Threats and Requirements
  - CRs to TS 33.102, Security Architecture
  - CRs to TS 33.107, Lawful Interception Architecture
  - CRs to TS 33.200, MAP Security
  - CRs to TS 35.201, UTRAN Security Algorithms
  - New and revised work item descriptions

CRs on TS 21.133, Security Threats and Requirements

- SP-010607
  - CRs to R99 and Rel-4 to align UICC definition with 3G vocabulary document TS 21.905

CRs to TS 33.102, Security Architecture (1/2)

- SP-010608
  - CRs to R99 and Rel-4 to make changes to Annex F which correspond to changes that were made to Annex C at SA#9
- SP-010609
  - CRs to R99 and Rel-4 to clarify sequence number management scheme in Annex C
- SP-010610
  - CRs to R99 and Rel-4 to clarify the use of the f5* function in the resynchronisation procedure

CRs to TS 33.102, Security Architecture (2/2)

- SP-010611
  - Rel-5 changes on visibility and configurability of security
  - Clarification that cipher indicator is mandatory
  - Specification to allow the user to be able to reject unciphered connections

CRs to TS 33.107, Lawful Interception Architecture

- SP-010612
  - CRs to Rel-4 and Rel-5 to clarify behaviour when an LEA requests interception of a target that is already being intercepted by another LEA
- SP-010613
  - CR to Rel-5 to align lawful interception specifications with recent changes to the Rel-5 IMS architecture
- SP-010614
  - CRs to R99, Rel-4 and Rel-5 to allow SMSs to be intercepted even when a delivery notification is not received

CRs to TS 33.107, Lawful Interception Architecture

- SP-010615
  - CRs to Rel-4 and Rel-5 to allow the LEA to obtain information about who initiated an intercepted PDP context

CRs to 33.200, MAP Security (Rel-4) (1/3)

- SP-010727 CRs on MAPsec protection profiles
  - CR014 was approved to remove DeleteSubscriberData from one of the protection groups as it is not considered to be a very sensitive message
  - CR018 to introduce a protection profile revision numbers to allow protection profiles to be modified rather than having to create new ones in future Releases of the specifications

CRs to TS 33.200, MAP Security (Rel-4) (2/3)

- SP-010618 CRs on MAPsec security association
  - CR016 introduces the concept of soft and hard security association expiry times to ease security association renewal procedures
  - CR019 clarifies that destination PLMN_ID and SPI belong to the security association

CRs to 33.200, MAP Security (Rel-4) (3/3)

- SP-010728
  - Clarifies the use of the “original component identifier” field in the MAPsec security header
- SP-010729
  - Clarifies that the security policy database should have an explicit entry for all PLMNs with which the network element is allowed to communicate
- SP-010616
  - Update to the specification of the MAP security encryption algorithm
- SP-010619
  - Removes sending PLMN_ID from the MAPsec header - companion CR to 29.002 approved at CN#14 (NP-010622)

CRs to 35.201, UTRAN Security Algorithms

- SP-010620
  - CRs to R99 and Rel-4 to correct the maximum input length for f8 and f9

New Work Item Description

- SP-010622
  - Support for subscriber certificates
    - Signalling procedures to issue temporary or long-term certificates to subscribers
    - Standard format of certificates and digital signatures, e.g re-using wireless PKI
    - Specifications are scheduled to be complete at SA#17

Revised Work Item Description

- SP-010621
  - Revision of lawful interception work item (SP-000309)
    - Include a description of the Rel-5 work to create a new specification TS 33.108
    - TS 33.108 is due for approval at SA#15