Technical Specification Group Services and System Aspects *TSGS#28(05)0255*
Meeting #28, Quebec, Canada, 6-8 June 2005

SA3 Status Report to SA#28

Valtteri Niemi, SA3 Chairman

Contents

- General aspects
- Status report on work items
- Actions expected from SA#28

General aspects

SA3 leadership

- Chairman: Valtteri Niemi (Nokia)
- Secretary: Michael Clayton (MCC)
- Vice-chair
  - Peter Howard (Vodafone)
- Elections of chairman and vice chairmen are to be held in next SA3 meeting

- Lawful interception (LI) sub-group
  - Chair: Brye Bonner (Motorola)
  - Vice Chair: Alex Leadbeater (BT)
  - Secretary: Rupert Thorogood (UK Home Office)

Meetings since SA#27

- **SA3 plenary**
  - **SA3#38: Geneva, Switzerland, 26-29 April 2005, hosted by EF3**

- **Lawful interception sub-group**
  - **SA3-LI#17, Sophia Antipolis, France, 5-7 April 2005, hosted by ETSI**

Next SA3 plenary meetings

- **SA3#39: Montreal, Canada, 28 June- 1 July 2005, hosted by NAF**
- **SA3#40: tbd, 13-16 September 2005, hosted by EF3 or ETSI (tbc), possibly co-located with ETSI TISPAN in Slovenia**
- **SA3#41: tbd, 15-18 November 2005, hosted by Qualcomm (tbc)**

Next SA3-LI meetings

- **LI#18: Toronto, Canada, 14-16 June 2005**
- **LI#19: Tbilisi, Georgia (tbc), 18-20 October 2005**

Statistics at SA3#38

- 38 delegates attended
- 137 temporary documents handled including
  - 13 incoming LSs
  - 9 outgoing LSs

Summary of SA3 input to SA#28

- 9 SA3-LI CR for approval
- 19 SA3 CRs for approval
- 2 WIDs for approval
- Status report Presentation SA3 Chairman (info)
- Status report from SA3 MCC (info)
- Draft report of previous SA3 meeting (info)

Status report on work items

Lawful interception 1/2

- One CR to 33.107 (Rel-6) (SP-050256):
  - Correction on the use of identities for I-WLAN lawful interception
- Two CRs to 33.107 (Rel-7) (SP-050257):
  - Clarifications for the usage of the notion of a service in distributed IP networks
  - Correlation for IMS interception
- One CR to 33.108 (Rel-6) (SP-050258):
  - Correction on IMS correlation
- Three CRs to 33.108 (Rel-7) (SP-050259):
  - Clarifications to the timing issue
  - Clarification pertaining to the filtering of SDP for IRI-only cases
  - Obsolete Import Statement in Annex B.6
- One CR pair to 33.108 (Rel-6 and Rel-7) (SP-050260):
  - Inconsistency in Annex B.5

Lawful interception 2/2

- **A new WID "Lawful Interception in the 3GPP Rel-7 architecture" (SP-050237)**

IMS security

- One CR to 33.203 (Rel-6) (SP-050261):
  - Description of 2xx Auth_Ok message
- One CR to 33.978 “Security aspects of early IMS” (Rel-6) (SP-050267)
  - Correction of use of 401 Unauthorized and 399 Warning headers
- A new WID: “Security Enhancements for Fixed Broadband Access to IMS” (SP-050238)
- An LS was received from TISPAN WG7 (Security):
  - it was taken into account for the WID
  - a joint meeting is now under preparation

Network domain security

- **Some progress on the work for MAPsec gateway concept**

UTRAN access security

- **A draft CR to 33.102 (Rel-5) was prepared about ”keystatus” parameter sent by CN node in Security Mode Command ; LS sent to RAN3 and CT1 to discuss the issue before submission to SA plenary**
- **An LS sent to GSMA Security group about two recent research papers on GSM and UMTS security: recommendations about network configurations included**
- **The work on new encryption and integrity algorithms UEA2/UIA2 has progressed according to the schedule. Funding is needed for external evaluation of the algorithms.**

GERAN access security

- **A baseline draft version of TR "Access Security Review" was agreed**

GAA – Generic authentication architecture 1/2

- **Two Rel-6 CRs to 33.220 (SP-050262):**
  - **Usage of USS for local policy enforcement in BSF**
  - **Correcting figure 4.4**
- **One Rel-7 CR to 33.220 (SP-050263):**
  - **GBA User Security Settings (GUSS) transfer optimisation**
- **One Rel-6 CR to 33.222 (SP-050264):**
  - **Removal of editor's note**

GAA - 2/2

- It was agreed to work tentatively on CRs to allow GBA for 2G SIM cards (currently only USIMs are supported); LS to SA1 is under preparation
- Email discussion ongoing to remove some inconsistencies in 33.222
- Issues around https terminating in the UICC:
  - An early deadline agreed for contributions to next SA3 meeting
  - Goal is to propose this for early implementation in Rel-7

WLAN inter-working security

- **Three Rel-6 CRs to TS 33.234 (SP-050265):**
  - **Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access**
  - **Terminate WLAN session by AAA server**
  - **Correction to the definition of the Wn Reference Point**

MBMS security 1/2

- **A couple of LS's sent to SA4 to resolve remaining issues in consistency between SA3 and SA4 specs**
- **A presentation about MBMS security was given in workshop on "Mobile Broadcast Service Standardization" (Den Haag, 23 May 2005)**

MBMS security 2/2

- Ten Rel-6 CRs to 33.246 (SP-050266):
  - MKI and authentication tag length in User Service Description
  - Clarification of Key domain ID in service announcement
  - Key usage clarification
  - Omitted MTK Update Error Message
  - Editorial corrections to TS 33.246
  - Clarifications on MBMS key management
  - Use of IMPI in MBMS
  - Clarification on CSB ID and SP payload use
  - MIME type adjustments according to LS S3-050192
  - Results of mapping the MBMS security requirements into security functions and mechanisms

Liberty-3GPP security interworking

- **A baseline draft version of TR “Liberty Alliance and 3GPP Security Interworking: Interworking of Liberty Alliance ID-FF, ID-WSF and Generic Authentication Architecture ” was agreed**

Actions expected from SA#28

Documents for approval 1/2

CRs for approval:

- (SP-050256) One CR to 33.107 (Rel-6)
- (SP-050257) Two CRs to 33.107 (Rel-7)
- (SP-050258) One CR to 33.108 (Rel-6)
- (SP-050259) Three CRs to 33.108 (Rel-7)
- (SP-050260) One CR pair to 33.108 (Rel-6/Rel7)
- (SP-050261) One CR to 33.203 (Rel-6)
- (SP-050262) Two Rel-6 CRs to 33.220
- (SP-050263) One Rel-7 CR to 33.220
- (SP-050264) One Rel-6 CR to 33.222
- (SP-050265) Three Rel-6 CRs to TS 33.234
- (SP-050266) Ten Rel-6 CRs to 33.246
- (SP-050267) One CR to 33.978 (Rel-6)

Documents for approval 2/2

WIDs for approval:

- **(SP-050237) Lawful Interception in the 3GPP Rel-7 architecture**
- **(SP-050238) Security Enhancements for Fixed Broadband Access to IMS**

Documents for information

SP-050255: Status Report presentationfrom SA WG3 to TSG SA #28

SP-050323: Status report of SA WG3 meeting #38

SP-050236: Draft Report of SA WG3 meeting #38