3GPP TSG SA WG3 Security — S3#37 **S3-050003**
21 - 25 February 2004
Sophia Antipolis, France

Source: **Chairman of 3GPP TSG-SA WG3**
Title: **Report from SA#26 plenary**
Document for: **Information**
Agenda Item: **4.2**

Dear SA3,

I am glad to inform you that SA3 matters were handled smoothly at the SA#26 plenary meeting in Athens, Greece, 13-16 December 2004. The main points with impact to SA3 are listed in the following:

1. It was agreed that the TR 33.878 "Security aspects of early IMS" is to be upgraded to 33.9xx series. Also, a CR adding a reference to 33.203 is expected from us to the next SA plenary. On the other hand, the TR was not yet put under change control. In particular, CN groups were asked to review (current version of) the TR. Note that this means we still work with pseudo-CRs in SA3#37 (in case further changes are needed).

2. Another point of advice we asked from SA#26 was about the fate of "tls-psk" in Release 6 (S3-041141). Based on the advice from the IETF coordination officer (and CN chairman) Stephen Hayes, it was decided to allow three more months to complete the work in IETF. More specifically, we should check in SA3#37 meeting whether the "tls-psk" draft has at least passed working group last call. Similar decisions had been done in CN plenary. As a consequence, the decision between our two alternative CRs was postponed to SA#27.

3. Our proposed CR against 33.200 "SMS fraud countermeasures" (S3-0401070) caused some discussion. It was explained that the address of the SMSC used in TCAP layer is not necessarily the same as the address included in MAP layer. It may even happen that the NDC parts of the two addresses do not match (see SP-040924 for description of the problem). Because of this, the comparison check of addresses in different layers was removed from the solution and a warning note was added to Measure-1. The updated CR SP-040921 was then approved. It was also noted that SA3 might build enhancements on top of the basic solution if needed.

1. All of our other CRs were accepted as proposed. Please note that one of the CRs to 33.234 (S3-041151) was actually done against the (old) version 6.0.0. This caused problems because there was a proposed change to an editor's note but the editor's note itself had been replaced by a "genuine" note already in version 6.1.0. Based on my advice, Maurice prepared a replacement CR (which does not include the change in the non-existing editor's note) against the (correct) version 6.2.1. This new CR was approved (SP-040891).

1. All three WIDs that we submitted were approved with no changes.

1. Our "Issue list to complete MBMS Security" (S3-041132) did not induce very much discussion. One comment was that it is expected that service announcements be typically carried over point-to-multipoint channels.

1. Issues of interest in SA1 area:
   - SA1 have created a TR 22.978 (v1.0.0) "All-IP Network (AIPN) Feasibility Study (Rel-7)" that contains several pages devoted to security and privacy issues (SP-040739).

1. Issues of interest in SA2 area:
   - A CR against TS 23.125 "IP flow based bearer level charging" containing generic statement of adding "adequate security" was approved (SP-040753).
   - ETSI TISPAN has proposed a second workshop on "IMS over Fixed Access". A reply LS was prepared in SP-040929 (cc also to SA3) in which SA plenary accepts the proposal and delegates organisation duties on 3GPP side to SA2 management.

1. Issues of interest in CN area:
    - An LS from CN1 to ETSI OCG EMTEL about “Support of eCall on UUS type 1 Supplementary Service” (SP-040716) should be noted by SA3 also because there may be connections to fraud potential.

2. Issues of interest in RAN area:
    - A workshop was arranged recently on long-term evolution of UTRAN. There are of course relevant security issues. Summary of requirements was created as an output from the workshop (SP-040914). The related study item is described in SP-040915 (WID) and SP-040916 (process description).The new TSG structure is going to be valid after next plenaries in March. The new TSG RAN contains old RAN WGs and T1. The new TSG CT contains old CN WGs added with T2 and T3. There is no direct impact on SA WGs.
    - Features that have been planned for Release 6 but not completed by now (e.g. MBMS) got three more months for completion of the work; see SP-040927 for list of these features. An explicit justification for keeping a feature in Release 6 has to be presented in SA#27 if work still needs to continue after March 2005.

Attached: my status report slides (SP-040848)

Best regards,

Valtteri Niemi
SA3 chairman

SA3 Status Report to SA#26

Valtteri Niemi, SA3 Chairman

Contents

- General aspects
- Status report on work items
- Actions expected from SA#26

General aspects

SA3 leadership

- **Chairman: Valtteri Niemi (Nokia)**
- **Secretary: Maurice Pope (MCC)**
- **Vice-chairs**
  - **Michael Marcovici (Lucent)**
  - **Peter Howard (Vodafone)**
- **Lawful interception (LI) sub-group**
  - **Chair: Brye Bonner (Motorola)**
  - **Vice Chair: vacant**
  - **Secretary: Rupert Thorogood (UK Home Office)**

Meetings since SA#25

- **SA3 plenary**
  - **SA3#35: Malta, 5-8 October 2004, hosted by EF3**
  - **SA3#36: Shenzhen, China, 23-26 November 2004, hosted by HuaWei**

- **Lawful interception sub-group**
  - **LI#4/2004, San Antonio, USA, 11-13 October 2004, hosted by NA Friends of 3GPP**

Next SA3 plenary meetings

- **SA3#37: Sophia Antipolis, France, 21-25 February 2005, hosted by ETSI**
- **SA3#38: Switzerland (tbc), 26-29 April 2005, hosted by Orange and EF3 (tbc)**
- **SA3#39: USA (tbc), 28 June- 1 July 2005, co-located with SA2, hosted by NAF (tbc)**

Next SA3-LI meetings

- **LI#1/2005: Barcelona, Spain (tbc), 18-20 January 2005**
- **LI#2/2005: Sophia Antipolis, France, 5-7 April 2005**

Statistics at SA3#35 / SA3#36

- **40 / 45 delegates attended**
- **200 / 266 temporary documents handled including**
  - **21 / 21 incoming LSs**
  - **13 / 12 outgoing LSs**

Summary of SA3 input to SA#26

- **12 SA3-LI CRs for approval**
- **78 SA3 CRs for approval**
- **1 TR for approval**
- **3 WIDs for approval**
- **1 LS for discussion and decision**

Status report on work items

Lawful interception (1/2)

- **Three CRs to 33.107 (Rel. 6) (SP-040850):**
  - **Lawful Interception for WLAN Interworking**
  - **33.107 Cleanup**
  - **Clarification on MMS interception**

Lawful interception (2/2)

- **One Rel. 5 / Rel. 6 pairs of CRs to 33.108 (SP-040851):**
  - **Correction to ULIC header**
- **Seven Rel. 6 CRs to 33.108 (SP-040851):**
  - **Correction on parameter GprsOperationErrorCode**
  - **Correction to the IMPORTS statements**
  - **Syntax Error in Annex B.3**
  - **Deleting CC from SIP message**
  - **Adding domain ID to HI3 CS domain module**
  - **Syntax Error in Annex B.3a**
  - **HI2 SIP Content clarification**

IMS security

- **One Rel-6 CR to 33.203 (SP-040854):**
  - **Editorial corrections**
- **TR 33.878 ì Security aspects of early IMSî submitted for approval (SP-040866)**
  - **Valuable input was received from SA2, CN1, CN3 and CN4**
  - **Advice from SA plenary is needed on whether the report**
    - **to be upgraded to 33.9xx series**
    - **to be referenced in TS 33.203**

    (current WID does not include these actions, see SP-040691)
- **Email discussion started for IMS security extensions (WID expected next time)**

Network domain security: MAP layer

- **One Rel. 6 CR to 33.200 (SP-040853):**
  - **SMS fraud countermeasures**
- **An LS received from GSMA proposing concept of MAPsec gateway**
  - **under study in SA3 for basis of Rel. 7 MAPsec work**

UTRAN access security

- **Three Rel. 6 CRs to 33.102 (SP-040852):**
  - **Correction of Abbreviation for USIM**
  - **Correction of TMUI to TMSI in a figure**
  - **Support of algorithms in UEs**
- **One WID for approval: Development of UEA2 and UIA2**
  - **ETSI SAGE has already started design work for UTRAN back-up algorithms**

GERAN access security

- **One Rel. 6 CR to 43.020 (SP-040862):**
  - **Clarifying the mandatory support of A5 algorithms within mobile stations**

    This CR mandates support of A5/1 and A5/3 while it prohibits support of A5/2
- **Proposed new WID: Access Security Enhancements (SP-040865)**
- **TR ì Feasibility Study on Generic Access to the A/Gb interfaceî was reviewed from security point of view**

Generic authentication architecture (GAA)

- **SA3 is specifying three stage 2 TSs and one TR**
  - **TR 33.919 Generic Authentication Architecture (GAA), which gives GAA overview (approved in SA#25)**
  - **TS 33.220 Generic Bootstrapping Architecture, which describes use of UMTS AKA protocol to establish shared secrets for various applications (approved in SA#23)**
  - **TS 33.221 Support for Subscriber Certificates, which describes subscriber certificate enrolment and delivery of certificates to UE (approved in SA#23)**
  - **TS 33.222 Access to Network Application Functions using HTTPS, which describes how bootstrapped shared secret (GBA) or subscriber certificate (SSC) is used for authentication in HTTP-based services (approved in SA#24)**

GAA ñ Generic authentication architecture

- **One Rel-6 CR to 33.919 (SP-040861):**
  - **Removal of unnecessary editor's notes**
- **Relations of GAA and Liberty have been studied**

GAA ñ Generic bootstrapping architecture (GBA) 1/2

- **Seventeen Rel-6 CRs to 33.220 (SP-040855):**
  - **BSF discovery using default domain method**
  - **Local validity condition set by NAF**
  - **GBA User Security Settings (GUSS) usage in GAA and Introduction of NAF groups**
  - **Details of USIM/ISIM selection in GAA**
  - **TLS profile for securing Zn' reference point**
  - **Optimization of the GBA_U key derivation procedure**
  - **Requirement on ME capabilities for GBA_U**
  - **Adding a note about replay protection**
  - **Complete the MAC modification for GBA_U**
  - **Removal of unnecessary editor's notes**
  - **Fetching of one AV only on each Zh run between BSF and HSS**
  - **Clean up of TS 33.220**

GAA ñ Generic bootstrapping architecture (GBA) 2/2

- New key management for ME based GBA keys
- Key derivation function
- Re-negotiation of keys
- No GUSS/USS update procedures in Release-6
- Clarify the number of NAF-specific keys stored in the UE per NAF-Id

GAA ñ Support for subscriber certificates

- **Two Rel. 6 CRs to 33.221 (SP-040856):**
  - **Visited network issuing subscriber certificates**
  - **Editorial correction**

GAA ñ Secure HTTP access to network application functions

- **Six Rel. 6 CRs to 33.222 (SP-040889):**
  - **GBA supported indication in PSK TLS**
  - **Adding Support for AES in the TLS Profile**
  - **Authorization flag transfer between AP and AS**
  - **Correction of inconsistencies within AP specification**
  - **TLS extensions support**
  - **Visited AS using subscriber certificates**
- **An LS submitted to SA plenary asking advice on whether to keep one option in Rel. 6 although the corresponding IETF draft is not yet an RFC**
  - **Two alternative CRs prepared on this issue (SP-040890)**

WLAN inter-working security 1/2

- **Twenty-two Rel-6 CRs to TS 33.234 (SP-040858):**
  - **Profile for PDG certificates in Scenario 3**
  - **Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces)**
    - **This CR is revised in SP-040891**
  - **Sending of W-APN identification**
  - **Clean up of not completed chapters**
  - **Correction of WLAN UE function split**
  - **Passing keying material to the WLAN-AN during the Fast re-authentication procedure**
  - **Clarification on Deletion of Temporary IDs**
  - **Clarification on Protecting Re-authentication ID in FAST/FULL Re-Authentication procedure**
  - **Assigning Remote IP Address to WLAN UE using IKEv2 configuration Payload**

WLAN inter-working security 2/2

- Tunnel Establishment Procedure
- Deletion of inconclusive text on A5/2 countermeasures
- Alignment of IPsec profile with RFC2406
- Control of simultaneous sessions in WLAN 3GPP IP access
- Completion of definition and abbreviations
- Fallback from re-authentication to full authentication
- Clarification on the use of IMSI in WLAN 3GPP IP access
- Clarification on the use of MAC addresses
- Clarifications and corrections on the use of pseudonyms
- Wn Reference Point Description
- Removal of word ì scenarioî
- Correction of WRAP to CCMP
- Removal of resolved editors' notes

MBMS security 1/3

- **A couple of contentious issues were solved**
  - **Mandatory support of GBA-U**
  - **Re-use of OMA DCF for download protection**
- **However, several open issues remain, see SP-040868**
- **Email discussions started on some issues**

MBMS security 2/3

- **Nineteen Rel. 6 CRs to 33.246 (SP-040859):**
  - **Deletion of MBMS keys stored in the ME**
  - **Clarification on key management**
  - **Clean up of MBMS TS**
  - **Traffic protection combinations**
  - **Clarifying ME and BM-SC capabilities**
  - **MBMS MTK Download transport**
  - **MBMS Transport of salt**
  - **SRTP index synchronisation within ME**
  - **Clarify the use of mandatory MIKEY features for MBMS**
  - **Protection of the Gmb reference point**

MBMS security 3/3

- Use of parallel MSKs and MTKs
- Scope of MBMS security
- Clarification of the format of MTK ID and MSK ID
- MTK update procedure for streaming services
- Clarification of MSK key management
- Modification of delivery of MIKEY RAND field in MSK updates
- OMA DRM DCF for protection of download services
- Shorter MKI
- Handling of MBMS identities and definition completion/modification. Specify how to identify the MUK and MRK

Feasibility Study on (U)SIM Security Reuse by Peripheral Devices

- **Two Rel. 6 CRs to 33.817 (SP-040860):**
  - **Bluetooth security and configuration considerations for Annex of TR 33.817**
  - **Terminology update to not rule out the use of the smart card for security enhancements**

Security for voice group call services

- **One Rel. 6 CR to 43.020 (SP-040862): Clarifications to VGCS/VBS ciphering mechanism**

Other SA3 work items

- **Generic user profile security**
  - **LSs exchanged with SA2 and CN4**
- **Selective Disabling of UE Capabilities**
  - **SA1 thought that SA3 have done work not requested in the WID. An LS was sent to SA1 explaining how the draft document corresponds to the WID**

Actions expected from SA#26

Documents for approval (1/3)

SP-040850 3 SA WG3 LI Group Rel-6 CRs to TS 33.107 (Rel-6)

SP-040851 9 SA WG3 LI Group CRs to TS 33.108 (Rel-5 and Rel-6)

SP-040852 3 CRs to 33.102 (Rel-6)

SP-040853 1 CR to 33.200: SMS fraud countermeasures (Rel-6)

SP-040854 1 CR to 33.203: Editorial corrections (Rel-6)

SP-040855 17 CRs to 33.220: (Rel-6)

SP-040856 2 CRs to 33.221: (Rel-6)

SP-040889 6 CRs to 33.222: (Rel-6)

SP-040867/SP-040890: Decision on a CR to 33.222: Removing/ Keeping PSK TLS from 3GPP Rel 6 (Rel-6)

SP-040858/SP-040891 22 CRs to 33.234: (Rel-6)

SP-040859 19 CRs to 33.246: (Rel-6)

SP-040860 2 CRs to 33.817: (Rel-6)

SP-040861 1 CR to 33.919: Removal of unnecessary editor's notes (Rel-6)

SP-040862 2 CRs to 43.020 (Rel-6)

Documents for approval (2/3)

SP-040866: Presentation of TR 33.878 î Security Aspects of Early IMSî version 1.0.0 to TSG SA

Documents for approval (3/3)

SP-040863: Work Item Description for Trust Requirements for Open Platforms in 3GPP

SP-040864: Work Item Description for Development of UEA2 and UIA2

SP-040865: Work Item Description for Access Security Enhancements

Documents for information

- **SP-040848 Report of SA WG3 activities to TSG SA Plenary**
- **SP-040849 Draft reports of SA WG3 meetings #35 and #36**
- **SP-040868 Issue list to complete MBMS Security**