

Technical Specification Group Services and System Aspects TSGS#26(04)0848

Meeting #26, Athens, Greece, 13-16 December 2004



SA3 Status Report to SA#26

Valtteri Niemi, SA3 Chairman

A GLOBAL INITIATIVE

Contents

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

General aspects



A GLOBAL INITIATIVE

SA3 leadership

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

Meetings since SA#25

ï SA3 plenary

ñ SA3#35: Malta, 5-8 October 2004, hosted by EF3

ñ SA3#36: Shenzhen, China, 23-26 November 2004, hosted by HuaWei

ï Lawful interception sub-group

ñ LI#4/2004, San Antonio, USA, 11-13 October 2004, hosted by NA Friends of 3GPP

Next SA3 plenary meetings

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

Next SA3-LI meetings

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

Statistics at SA3#35 / SA3#36

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

Summary of SA3 input to SA#26

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

Status report on work items



A GLOBAL INITIATIVE

Lawful interception (1/2)



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

A GLOBAL INITIATIVE

Lawful interception (2/2)

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

IMS security



- ï **One Rel-6 CR to 33.203 (SP-040854):**
 - ñ **Editorial corrections**
- ï **TR 33.878 `Security aspects of early IMS` submitted for approval (SP-040866)**
 - ñ **Valuable input was received from SA2, CN1, CN3 and CN4**
 - ñ **Advice from SA plenary is needed on whether the report**
 - ï **to be upgraded to 33.9xx series**
 - ï **to be referenced in TS 33.203****(current WID does not include these actions, see SP-040691)**
- ï **Email discussion started for IMS security extensions (WID expected next time)**

Network domain security: MAP layer

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

UTRAN access security



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

A GLOBAL INITIATIVE

GERAN access security

- ï **One Rel. 6 CR to 43.020 (SP-040862):**
 - ñ **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
- ï **Proposed new WID: Access Security Enhancements (SP-040865)**
- ï **TR ì Feasibility Study on Generic Access to the A/Gb interfaceî was reviewed from security point of view**

Generic authentication architecture (GAA)



- ï **SA3 is specifying three stage 2 TSs and one TR**
 - ñ **TR 33.919 Generic Authentication Architecture (GAA), which gives GAA overview (approved in SA#25)**
 - ñ **TS 33.220 Generic Bootstrapping Architecture, which describes use of UMTS AKA protocol to establish shared secrets for various applications (approved in SA#23)**
 - ñ **TS 33.221 Support for Subscriber Certificates, which describes subscriber certificate enrolment and delivery of certificates to UE (approved in SA#23)**
 - ñ **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)**

A GLOBAL INITIATIVE

GAA ñ Generic authentication architecture



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



A G L O B A L I N I T I A T I V E

GAA ñ Generic bootstrapping architecture (GBA) 1/2



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

GAA ñ Generic bootstrapping architecture (GBA) 2/2



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

A GLOBAL INITIATIVE

GAA ñ Support for subscriber certificates

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

GAA ñ Secure HTTP access to network application functions



- ï **Six Rel. 6 CRs to 33.222 (SP-040889):**
 - ñ **GBA supported indication in PSK TLS**
 - ñ **Adding Support for AES in the TLS Profile**
 - ñ **Authorization flag transfer between AP and AS**
 - ñ **Correction of inconsistencies within AP specification**
 - ñ **TLS extensions support**
 - ñ **Visited AS using subscriber certificates**
- ï **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**
 - ñ **Two alternative CRs prepared on this issue (SP-040890)**

WLAN inter-working security 1/2



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

A GLOBAL INITIATIVE

WLAN inter-working security 2/2



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

A GLOBAL INITIATIVE

MBMS security 1/3



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

A GLOBAL INITIATIVE

MBMS security 2/3



ï Nineteen Rel. 6 CRs to 33.246 (SP-040859):

- ñ Deletion of MBMS keys stored in the ME**
- ñ Clarification on key management**
- ñ Clean up of MBMS TS**
- ñ Traffic protection combinations**
- ñ Clarifying ME and BM-SC capabilities**
- ñ MBMS MTK Download transport**
- ñ MBMS Transport of salt**
- ñ SRTP index synchronisation within ME**
- ñ Clarify the use of mandatory MIKEY features for MBMS**
- ñ Protection of the Gmb reference point**

A GLOBAL INITIATIVE

MBMS security 3/3



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

A GLOBAL INITIATIVE

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



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

A GLOBAL INITIATIVE

Security for voice group call services



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

A GLOBAL INITIATIVE

Other SA3 work items



- ï Generic user profile security**
 - ñ LSs exchanged with SA2 and CN4**
- ï Selective Disabling of UE Capabilities**
 - ñ 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***

A GLOBAL INITIATIVE

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)**

A GLOBAL INITIATIVE

Documents for approval (2/3)



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

A GLOBAL INITIATIVE

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**

A GLOBAL INITIATIVE

Documents for information

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