

Source: Chairman of 3GPP TSG-SA WG3
Title: Report from SA#23 plenary
Document for: Information
Agenda Item: 4.2

Dear SA3,

I am glad to inform you that no problems were encountered with SA3 matters in the SA#23 plenary meeting in Phoenix 15-18 March 2004. The main points with impact to SA3 are listed in the following:

1. All our CR's were approved as submitted.
2. All our TS's and TR's submitted for approval (i.e. 33.220, 33. 221, 33.234, 33.310, 33.817) were approved and they are now under change control. One consequence of this is that these documents are progressed from now on by CR's instead of pseudo-CR's. In particular, more attention should be devoted to the correctness and completeness of information in cover sheets when preparing future CR's.
3. The three TS's that we submitted for information (i.e. 33.141, 33.222, 55.226) caused a few comments:
 - It was requested that OMA is kept aware of the work done for http-based services. I reminded SA of our earlier initiative for a joint workshop with OMA/SEC on the area of GAA. I also promised to check feasibility of such workshop again with OMA/SEC.
 - The specification manager felt that it is confusing to have 55.226 in release 6 unless also support for 128-bit keys in other relevant TS's is included in release 6. I reported that SA3 do not expect that all of the support for longer keys can be specified for release 6. SA plenary, however, requested that SA3 have another look at how much specification work is involved here. Based on our feedback, SA plenary would decide in June whether 55.226 would be approved for release 6 or for release 7.
4. As agreed in SA3#32, I raised the issue with the MMS security study done by GSMA. I reported that no workshop was held as a consequence of the study. I also explained that the most severe security concerns raised in the study report seem to fall into areas where OMA is responsible. My proposal was that further work on the area should follow the general work division between OMA and 3GPP agreed for MMS. Therefore, SA3 would continue work on MMS security only if security issues specific to the 3GPP cellular system are identified first. Also, we would naturally follow normal working procedures with a WID etc. SA did not challenge this proposal of way forward.
5. Issues of interest in SA1 area:
 - SA1 have moved all the WLAN interworking requirements into a single new TS 22.234 which was approved;
 - TR 22.949 Study on a Generalised Privacy Capability was approved.
6. Issues of interest in SA2 area:
 - The WLAN interworking stage 2 TS 23.234 was finally approved;
 - Several TR's were approved with non-negligible amount of text about security aspects: TR 23.877 Speech enabled services, TR 23.881 Interworking aspects and migration scenarios for IPv4 based IMS implementations, TR 23.976 Push architecture. On the other hand, TR 23.851 Network sharing contains an empty "Security aspects" section.
7. Issues of interest in SA4 area:

- TS 26.244 PSS: 3GPP file format (3GP) was approved. As we already have been informed by SA4, it contains substantial amount of security-related material, e.g. clauses about SRTP and encryption.
8. Issues of interest in SA5 area:
- TS 32.371 Security Management Concept and Requirements was presented for information. As you remember, we briefly reviewed an earlier version in SA3#32.
9. Issues of interest in CN area:
- CN, and subsequently SA, replied to LS from CN4 (on Relationship between 3GPP and Liberty Alliance related to GUP work), see SP-040181 and SP-040220. The original CN4 LS (SP-040021) is also cc:ied to SA3. SA#23 decided to ask PCG to pursue the negotiation of a collaboration agreement with Liberty Alliance.
10. Issues of interest in T area:
- As we already know, T3 is in schedule for providing USIM support for MBMS in release 6;
 - T3 is working on USSD message delivery and transfer to the USIM, including identifying secure mechanisms for all use cases.
11. Other issues:
- ETSI TC-TISPAN wants to utilize IMS for their NGN architecture, see SP-040150. SA#23 mandated SA2 to organize a workshop with TISPAN on the issue, see LS (SP-040218) that is also cc:ied to SA3;
 - Rel-6 content is going to be functionally frozen in September 2004 but specific exceptions may be listed at the same time. For these exceptional work items extra time may be allowed until December 2004;
 - New WID form was approved. It should be used for all NEW work items.

Best regards,

Valtteri Niemi
SA3 chairman

Technical Specification Group Services and System Aspects TSGS#23(04)0151

Meeting #23, Phoenix, USA, 15-18 March 2004



SA3 Status Report to SA#23

Valtteri Niemi, SA3 Chairman

A GLOBAL INITIATIVE

Contents

- **General aspects**
- **Status report on work items**
- **Actions expected from SA#23**

General aspects



A GLOBAL INITIATIVE

SA3 leadership

- **Chairman: Valteri 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: Burkhard Kubbutat (O2 Germany)**

Meetings since SA#22

- **SA3 plenary**
 - **SA3#32: Edinburgh, Scotland, UK, 9-13 February 2004, hosted by European Friends of 3GPP**
 - We tried out 4.5 day meeting schedule for first time
- **Lawful interception sub-group**
 - **LI#1/2004, Miami, USA, 27-29 January 2004**

Next SA3 plenary meetings

- **SA3#33: Beijing, China, 10-14 May 2004, hosted by Samsung**
- **SA3#34: North America, 6-9 July 2004, hosted by NA Friends of 3GPP**
- **SA3#35: Malta, 5-8 October 2004 (TBC)**
- **SA3#36: Shenzhen, China, 23-26 November 2004, hosted by HuaWei**

Next SA3-LI meetings

- **LI#2/2004: Roma, 14-16 April 2004 (TBC)**
- **LI#3/2004: Povoia de Varzim, 19-21 July 2004 (TBC)**
- **LI#4/2004: USA, 12-14 October 2004 (TBC)**

Statistics at SA3#32

- **44 delegates attended**
- **201 temporary documents handled including**
 - **24 incoming LSs**
 - **18 outgoing LSs**

Summary of SA3 input to SA#23

- 11 SA3-LI CRs for approval
- 3 SA3 CRs for approval
- 4 TSs for approval
- 3 TSs for information
- 1 TR for approval

Status report on work items



A GLOBAL INITIATIVE

Lawful interception (1/2)

- **Rel-5 CRs against 33.108 (with Rel-6 mirror CRs)**
 - **SP-040160: Implications of R5 onwards QoS parameters on ASN.1 module in 33.108**
 - **SP-040158: Correction on the description of "initiator" in "PDP Context Modification CONTINUE Record"**
 - **SP-040161: Syntax error in Annex B.4**

Lawful interception (2/2)

- **Rel-6 CRs against 33.108**
 - **SP-040155: Corrections to Tables 6.2, 6.7**
 - **SP-040156: Corrections to Correlation Number**
 - **SP-040157: Correction to Identifiers**
 - **SP-040162: Clarification on the use of IRI-END record in PS interception**
 - **SP-040159: Editorial Corrections**

IMS security

- **Two Rel-6 CRs against 33.203:**
 - **SP-040153: Addition of AES transform**
 - **SP-040154: Deploying TLS (sips:) for interoperation between IMS and non-IMS network**
- **An email discussion has been triggered by a proposed CR in CN1 (for Rel-5)**

Network domain security: IP layer

- **Sending IMSI over Gn/Gp endorsed by SA3 → LS sent to CN4**
- **One Rel-6 CR against 33.210:**
 - **SP-040153: Addition of AES transform**

Network domain security: authentication framework

- **TS 33.310 presented for approval (SP-040168)**
 - This specification provides a scalable entity authentication framework for 3GPP network nodes that are using NDS/IP (TS 33.210) for control plane security
- **Open issues**
 - CMPv2 is used for initial enrolment. It is still an internet draft but it is already widely supported and expected to received RFC status by June 2004 at latest

GERAN security



- **New attack on GSM security**
 - Work is continuing to address an attack on GSM security which was reported at Crypto 2003 conference in August
 - A mechanism based on “special RAND” parameter adopted as a working assumption but another proposal is under study also (email discussion ongoing)
 - CRs against 43.020 have been drafted but not submitted yet
- **A5/4 and GEA4**
 - A5/3 and GEA3 refer to 64 bit key versions of the KASUMI-based algorithms
 - SAGE has created 128-bit key versions named A5/4 and GEA4:
 - SP-040170: draft TS 55.226: Specification of the A5/4 Encryption Algorithms for GSM and ECSD, and the GEA4 Encryption Algorithm for GPRS (for information).
 - This is for Release 6 but introduction of the algorithms requires also changes to other specs. These changes are not expected for release 6.

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

Generic authentication architecture

- **SA3 is specifying three stage 2 TSs and one TR**
 - **TR 33.919 Generic Authentication Architecture (GAA), which describes how GAA is used**
 - **TS 33.220 Generic Bootstrapping Architecture, which describes use of UMTS AKA protocol to establish shared secrets for various applications**
 - **TS 33.221 Support for Subscriber Certificates, which describes subscriber certificate enrolment and delivery of certificates to UE**
 - **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**

GAA – System description

- **TR 33.919 was presented for information in SA#22 but it is not submitted for approval yet**
 - **The TR is a framework document which describes the building blocks of the GAA and the relationship between the TSs that specify the GAA**
 - **The TR is to be submitted for approval after all three TSs are also ready**

GAA – Generic bootstrapping architecture (GBA)

- **TS 33.220 presented for approval (SP-040175)**
 - **The GBA describes a mechanism to bootstrap authentication and key agreement for application security from the 3GPP AKA mechanism**
 - **Some minor open issues**

GAA – Support for subscriber certificates

- **TS 33.221 presented for approval (SP-040165)**
 - The SSC feature describes how the GBA can be used to support the subscriber certificate enrolment and delivery of certificates to UE
 - Open issues:
 - The charging mechanism and whether it needs to be standardized in 3GPP is FFS.
 - The usage of shared key TLS instead of HTTP Digest as a method for securing enrolment is FFS.

GAA – Secure HTTP access to network application functions

- SA3 is specifying how a bootstrapped shared secret (GBA) or subscriber certificate (SSC) can be used for authentication in HTTP-based services
- This feature is needed e.g. to secure Ut interface for presence service
- Draft TS 33.222 presented for information (SP-040166)

WLAN inter-working security

- **TS 33.234 presented for approval (SP-040167)**
 - This TS specifies authentication (using EAP-AKA and EAP-SIM), re-authentication and user identify privacy for WLAN scenario 2. It also specifies security for UE-initiated tunnels in WLAN scenario 3
 - Open issues:
 - WLAN-UE functional split
 - Visibility and configurability
- **LS sent to Bluetooth about termination point of EAP in split case; SA3 working assumption is to terminate EAP in the GSM/UMTS UE and not in TE**

MBMS security

- **Draft TS 33.246 was presented for information in SA#22.**
 - This TS defines a mechanism to allow a BM-SC to encrypt multicast data in such a way that only intended recipients can decrypt the data
- **Draft was progressed with several contributions**
- **Based on the feedback from SA#22 earlier SA3 compromise on key management was challenged by some companies.**
- **SA3 tries to build consensus using early deadline for MBMS contributions to S3#33 (4 weeks before meeting; hopefully discussion rounds can be carried out via email before the meeting)**

Presence security

- **TS 33.141 presented for information for second time (SP-040163)**
 - **TS 33.141 mainly covers HTTP-based Ut interface security between UE and presence list server**

Feasibility study on USIM re-use by peripheral devices

- **TR 33.817 presented for approval (SP-040169)**
 - This TR contains a feasibility study on the re-use of a single SIM, USIM, or ISIM by peripheral devices on local interfaces (e.g. Bluetooth) to access multiple networks (e.g. 3GPP, WLAN, etc.)
 - The TS considers possible updates to 3GPP specifications and the need for new specifications

Other SA3 work items

- **Security for voice group call service**
 - SA3 is specifying a ciphering solution for VGCS
 - This was progressed by several contributions
 - SA3 has liaised with T3 and GERAN2 on this topic
- **Generic user profile security**
 - SA3 agreed to adopt the Liberty Alliance Project ID-WSF security solutions as the basis for the GUP security work → LS sent to SA2 and CN4



***Actions expected from
SA#22***

A GLOBAL INITIATIVE

Documents for approval (1/2)

- **SP-040153 CR to 33.203 and 33.210: Addition of AES transform (Rel-6)**
- **SP-040154 CR to 33.203: Deploying TLS (sips:) for interoperation between IMS and non-IMS network (Rel-6)**
- **SP-040155 CR to 33.108: Corrections to Tables 6.2, 6.7 (Rel-6)**
- **SP-040156 CR to 33.108: Corrections to Correlation Number (Rel-6)**
- **SP-040157 CR to 33.108: Correction to Identifiers (Rel-6)**
- **SP-040158 2 CRs to 33.108: Correction on the description of "initiator" in "PDP Context Modification CONTINUE Record" (Rel-5 and Rel-6) SA WG3**
- **SP-040159 CR to 33.108: Editorial Corrections (Rel-6)**
- **SP-040160 2 CRs to 33.108: Implications of R5 onwards QoS parameters on ASN.1 module in 33.108. (Rel-5, Rel-6)**
- **SP-040161 2 CRs to 33.108: Syntax error in Annex B.4 (Rel-5, Rel-6)**
- **SP-040162 CR to 33.108: Clarification on the use of IRI-END record in PS interception (Rel-6)**

Documents for approval (2/2)



- **SP-040175 Draft TS 33.220 v 2.0.0 and presentation cover sheet**
- **SP-040165 Draft TS 33.221 v 2.0.0 and presentation cover sheet**
- **SP-040167 Draft TS 33.234 v 2.0.0 and presentation cover sheet**
- **SP-040168 Draft TS 33.310 v 2.0.0 and presentation cover sheet**
- **SP-040169 Draft TR 33.817 v 2.0.0 and presentation cover sheet**

A GLOBAL INITIATIVE

Documents for information

- **SP-040151 Report from SA WG3 Chairman to TSG SA#2**
- **SP-040152 Draft Report of SA WG3 meeting #32**
- **SP-040163 Draft TS 33.141 v 1.1.1 and presentation cover sheet**
- **SP-040166 Draft TS 33.222 v 1.0.0 and presentation cover sheet**
- **SP-040170 Draft TS 55.226 v 1.0.0 and presentation cover sheet**