SA3 Status Report to SA#25

Valtteri Niemi, SA3 Chairman

Contents

ï General aspects

ï Status report on work items

ï Actions expected from SA#25

General aspects

SA3 leadership

- ï Chairman: Valtteri 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: Burkhard Kubbutat (O2 Germany)
  - ñ Secretary: Rupert Thorogood (UK Home Office)

Meetings since SA#24

- SA3 plenary
  - SA3#34: Acapulco, Mexico,
    6-9 July 2004, hosted by NAF;
    included joint session with TR-45 AHAG
- Lawful interception sub-group
  - LI#3/2004, Povoa de Varzim, Portugal,
    19-20 July 2004, hosted by EF3;
    co-located with ETSI TC LI
- Joint SA3-SA4 meeting on MBMS security
  - Sophia Antipolis, France,
    23-24 August, 2004, hosted by EF3

Next SA3 plenary meetings

- SA3#35: Malta, 5-8 October 2004, hosted by EF3
- SA3#36: Shenzhen, China, 23-26 November 2004, hosted by HuaWei
- SA3#37: Sophia Antipolis, France (to be discussed), 21-25 February 2005, hosted by ETSI (TBC)

Next SA3-LI meetings

- **LI#4/2004: San Antonio, USA,
11-13 October 2004,
hosted by NA Friends of 3GPP,
co-located with TR45 LAES**

Statistics at SA3#34

ï 39 delegates attended

ï 239 temporary documents handled including:

ñ 21 incoming LSs

ñ 19 outgoing LSs

Summary of SA3 input to SA#25

ï 14 SA3-LI CRs for approval

ï 36 SA3 CRs for approval

ï 2 ì MCCî CRs to 33.102: Correction to mis-implementation of CR175: Rel4- definition

ï 1 TS for approval

ï 1 TR for approval

ï 1 WID for approval

Status report on work items

Lawful interception (1/2)

- Four CRs to 33.107 (Rel. 6) (SP-040616):
  - Correction on the use of session initiator parameter
  - ICE (Intercepting Control Elements), INE (Intercepting Network Elements) definition
  - Clarification to SMS interception
  - Replace SIP URL with SIP URI

Lawful interception (2/2)

- Ten Rel. 6 CRs to 33.108 (SP-040616):
  - Explanation concerning the Sequence Number
  - National ASN.1 parameter
  - Clarifying clause titles
  - Adding azimuth in location
  - Correction of the Subaddressing definitions
  - Correction to hi3DomainId definition
  - Correction of wrong use of abbreviations
  - Differences between subaddress sections in 33.108 and ETSI TS 101 671
  - Replace SIP URL with SIP URI
  - Corrections to References

IMS security

- One Rel-5/Rel-6 CR pair to 33.203 (SP-040618):
  - Deletion of old authentication vectors in S-CSCF after re-synchronization
- Two Rel-6 CRs to 33.203 (SP-040618):
  - Forwards compatibility to TLS based access security
  - SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network
  - IMS Service Profile is independent from Implicit Registration Set
- One WID: Security for early IMS:
  - Comments from SA#24 taken into account
  - SA3 has already created a draft TR

Network domain security: MAP layer

ï Contributions from SA#24 were discussed

ï There was a proposal for an alternative countermeasure against SMS fraud. Feasibility of it to be checked with CN4 and T2 (LS was sent).

ï MAPsec would provide wider protection

Network domain security: IP layer

- One proposed CR was discussed but postponed

Network domain security: authentication framework

ï One Rel-6 CR to 33.310 (SP-040623):

  ñ Splitting the Roaming CA into a SEG CA and an Interconnection CA

UTRAN access security

ï A response LS sent to RAN2 about re-authentication and key set change during inter-system handover.

ï A recent LS from T3 has triggered the following corrective action:

  ñ One CR has not been correctly implemented

  ñ New corrective CRs provided by SA3 leadership in SP-040627

GERAN access security

- Removal of mandatory A5/2 support from Rel-6:
  - SA1 replied algorithm selection is out of their scope
  - Ongoing AP to SA3 leadership: to find best way to reflect the changes for GSM Algorithm support in the specifications.

- New attack on GSM security
  - Decision about a mechanism based on ì special RANDî parameter was postponed out from Rel-6 and other mechanisms are still studied also. SA3 aims for decisions in early Rel-7 timeframe

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: submitted for approval in SA#25 (SP-040625)
  - 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 bootstrapping architecture (GBA)

- ï Eight Rel-6 CRs to 33.220 (SP-040619):
  - ñ Detailing of key lifetime
  - ñ Details of USIM/ISIM usage in GAA
  - ñ Generic Ua interface requirements
  - ñ B-TID generation
  - ñ Securing Zn reference point
  - ñ GBA User Security Settings
  - ñ Creation of GBA_U AV in the BSF
  - ñ Clarification of the definition of a default type of NAF-specific key
- ï There is need for further functional changes in the GBA_U work after September 2004.

GAA ñ Support for subscriber certificates

ï **Four CRs to 33.221 (SP-040620):**

- ñ **User security settings**
- ñ **Editorial cleanup**
- ñ **Cleanup of procedure descriptions**
- ñ **Removal of unnecessary editor's notes**

GAA ñ Secure HTTP access to network application functions

- Four CRs to 33.222 (SP-040621):
  - GBA User Security Settings
  - GBA supported indication and NAF hostname transfer in HTTP and in PSK TLS
  - Editorial clean-up of TS 33.222
  - Further modifications to TLS profile related text in 33.222

WLAN inter-working security 1/3

- **Nine Rel-6 CRs to TS 33.234 (SP-040622):**
  - **Two CRs to update references**
  - **Sending of temporary identities from WLAN UE**
  - **Clarification on fast re-authentication procedure**
  - **Correction of authentication procedure for WLAN UE split**
  - **Modification of mechanism to restrict simultaneous WLAN sessions**
  - **Wa interface security**
  - **Introduction of protected result indications**
  - **Tunnel authentication procedure in Wm interface**

WLAN inter-working security 2/3

ï **SA3 conclusions about WLAN/UICC issues:**

- ñ **USIM enhancements to support EAP in the UICC provide some improvements from both deployment and security perspectives. However, the balance between the needed standardization/implementation work and the benefits is not yet clear.**
- ñ **Not enough benefits were yet identified to justify postponing of Rel-6 WLAN security TS freeze date in order to specify these USIM enhancements. Some more studies are required to decide on the introduction of the EAP support in UICC.**

WLAN inter-working security 3/3

ï Effect of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces) to WLAN security TS:

  ñ discussed in break-out session and later in conference calls

  ñ Some CRs expected later as an outcome

ï A proposal to work on ì Trust Requirements for Open Platforms in WLAN-WWAN Interworkingî

  ñ Conference calls held to formulate a potential WID for release 7

  ñ To be discussed in next SA3 meeting

MBMS security 1/2

- Draft TS 33.246 is submitted for approval in SA#25 (SP-040624)
  - 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
- Open issues:
  - Exact details of the application layer joining and leaving are still to be determined (was discussed in the SA3-SA4 joint meeting).
  - The exact key derivation of MRK and MUK from the keys provided by GBA_U. SA3 are communicating with ETSI SAGE over the design of a key derivation function.
  - Exact details of the MIKEY messages that carry MSK and MTK from the BM-SC to the UE.
  - Exact details of SRTP use in MBMS
  - More details needed on the handling of MSKs and MTKs.
  - The protection of download data.

MBMS security 2/2

- Joint meeting between SA3 and SA4 was held 23-24 August (SP-040614).
  - Main purpose was information sharing; to identify gaps and overlaps in the specifications of the two groups
  - Several tentative agreements (e.g use of SRTP for streaming, order of FEC and encryption in streaming)

Presence security

- Four CRs to TS 33.141 (SP-040617)
  - ISIM used in GBA
  - Further modifications to TLS profile related text in 33.141
  - Editorial cleanup of TS 33.141
  - Clarification on Ut interface

Other SA3 work items

- Security for voice group call service
  - A CR to 43.020 (SP-040615): Introducing VGCS/VBS ciphering
- Generic user profile security
  - An LS sent (again) to SA2 & CN4 about GUP security progress, including proposed CRs to TS 23.240 and TS 29.240.
- Selective Disabling of UE Capabilities
  - Draft text was agreed that is going to be further improved inside SA3 first and later provided to SA1 for inclusion in their TR.

Stability of Rel-6 TSs:

ñ 33.246 (MBMS): Not considered ready, some functional changes may be necessary.

- 33.234 (WLAN-IW): Not considered ready, some functional changes may be necessary.
- 33.220 (GBA): Not considered ready, some functional changes may be necessary.
- 33.221 (Subscriber Certificates): It was generally agreed that this should be ready for functional freezing in September 2004.
- 33.222 (HTTPS-based services): It was generally agreed that this should be ready for functional freezing in September 2004.
- 33.141 (Presence): It was generally agreed that this should be ready for functional freezing in September 2004.
- 33.310 (NDS/AF): It was generally agreed that this should be ready for functional freezing in September 2004. The possible use of TLS will have no impact as it is not part of the 3GPP specifications.
- 33.203 (IMS): It was generally agreed that this should be ready for functional freezing in September 2004.

Actions expected from SA#25

Documents for approval (1/4)

SP-040615: CR to 43.020: Introducing VGCS/VBS ciphering (Rel-6)

SP-040616: SA WG3 LI Group Rel-6 CRs which were agreed by SA WG3 by e-mail (02/09/2004)

SP-040617: 4 CRs to 33.141: Various changes to Presence Security (Rel6)

SP-040618: 5 CRs to 33.203: Various changes to IMS Security (Rel-5 & Rel-6)

SP-040619 8 CRs to 33.220: GAA: Various changes to Generic Bootsrapping Architecture (Rel-6)

SP-040620 4 CRs to 33.221: GAA: Various changes to Subscriber Certificates (Rel-6)

SP-040621 4 CRs to 33.222: GBA: Various changes to Secure HTTP access (Rel-6)

Documents for approval (2/4)

SP-040622: 9 CRs to 33.234: Various changes to WLAN Interworking Security (Rel-6)

SP-040623: One CR to 33.310: Splitting the Roaming CA into a SEG CA and an Interconnection CA (Rel-6)

SP-040627: One Rel-4 / Rel- 5 CR pair to 33.102: Correction to mis-implementation of CR175: Rel4- definition

Documents for approval (3/4)

SP-040624: Presentation of Specification 33.246 version 2.0.0 to TSG SA

SP-040625: Presentation of TR 33.919 version 2.0.0 to TSG SA

Documents for approval (4/4)

SP-040626: Work Item Description: Security for early IMS

Documents for information

ï SP-040612 Report of SA WG3 activities to TSG SA Plenary

ï SP-040613 Draft report of SA WG3 meeting #34

ï SP-040614 Report of MBMS Ad-hoc meeting