SA3 Status Report to SA#24

Valtteri Niemi, SA3 Chairman

Contents

- General aspects
- Status report on work items
- Actions expected from SA#24

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: Burkhard Kubbutat (O2 Germany)
  - Secretary: Rupert Thorogood (UK Home Office)

Meetings since SA#23

- SA3 plenary
  - SA3#33: Beijing, China, 10-14 May 2004, hosted by Samsung
    - 4.5 day meeting
- Lawful interception sub-group
  - LI#2/2004, Rome, Italy, 14-16 April 2004

Next SA3 plenary meetings

- SA3#34: Acapulco, Mexico, 6-9 July 2004, hosted by NA Friends of 3GPP
- SA3#35: Malta, 5-8 October 2004, hosted by EF3
- SA3#36: Shenzhen, China, 23-26 November 2004, hosted by HuaWei

Next SA3-LI meetings

- LI#3/2004: Povoa de Varzim, 19-21 July 2004, hosted by EF3, includes joint meeting with ETSI TC LI
- LI#4/2004: USA, 11-13 October 2004, hosted by NA Friends of 3GPP, co-located with TR45 LAES

Statistics at SA3#33

- 47 delegates attended
- 248 temporary documents handled including
  - 26 incoming LSs
  - 16 outgoing LSs

Summary of SA3 input to SA#24

- 14 SA3-LI CRs for approval
- 28 SA3 CRs for approval
- 2 TSs for approval
- 2 TSs for information (second time)

Status report on work items

Lawful interception (1/2)

- One CR to 33.106 (Rel. 6)
  - Clarification on delivery of IRI and CC (SP-040396)
- Eight CRs to 33.107 (Rel. 6)
  - Correction on Network initiated Mobile Station Detach signalling flow (SP-040397)
  - TEL-URL missing in activation of LI in the CSCFs (SP-040398)
  - Correction on the use of session initiator parameter (SP-040399)
  - Correction to HLR interception event name (SP-040400)
  - Clarification for Push to talk over Cellular (SP-040401)
  - Adding an encryption parameter to IRI across X2 interface (SP-040402)
  - References (SP-040403)
  - Enhancements for the Functional Architecture chapter (SP-040404)

Lawful interception (2/2)

- One Rel. 5 CR to 33.108 (with Rel. 6 mirror)
  - WGS 84 coordinates length correction (SP-040406)
- Three Rel. 6 CRs to 33.108
  - Correction on interception identities in multi-media domain (SP-040405)
  - CR offering alignment to ETSI TS 101 671 (SP-040406)
  - Additional text for Definition and Acronym section (SP-040407)

IMS security

- Two Rel-6 CRs to 33.203:
  - SP-040372: Correction on IMS confidentiality protection
  - SP-040373: SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network

- Interim security for early IMS implementations:
  - LS was received from SA2
  - SA3 acknowledge the issue although regret that the full 33.203 solution had not been deployed in the market.
  - SA3 will study this further before next meeting and make a decision then based upon contributions.

Network domain security: IP layer

- **One Rel-6 CR to 33.210:**
  - **SP-040374: Diffie-Hellman groups in NDS/IP**

Network domain security: authentication framework

- **Three Rel-6 CRs to 33.310:**
  - **Removal of inconsistencies regarding SEG actions during IKE phase 1 (SP-040393)**
  - **Removal of unnecessary restriction on CA path length (SP-040394)**
  - **Correction of 'Extended key usage' extension in SEG Certificate profile (SP-040395)**

UTRAN access security

- One Rel-5 CR to 33.102 (with Rel-6 mirror)
  - Handling of key sets at inter-system change (to align with CN1) (SP-040370)
- One Rel-6 CR to 33.102
  - Clarification on Authentication re-attempt parameter (SP-040369)
- One Rel-4 CR to 33.105 “Cryptographic Algorithm requirements” (SP-040371)
  - Correction of inconsistencies in AK computation for re-synchronisation
  - This is proposed for Release 4 because Rel-5/Rel-6 do not exist !
  - SA3 proposes also to create Rel-5/Rel-6 versions

GERAN access security

- **New attack on GSM security**
  - **An LS sent to SA1 requesting removal of mandatory support of A5/2 (and addition of mandatory support of A5/3) in Rel-6 terminals.**
  - **A mechanism based on "special RAND" parameter is still the working assumption but "authenticated GSM cipher command mechanism" is still studied also.**
- **A5/4 and GEA4**
  - **A5/3 and GEA3 refer to 64 bit key versions of the KASUMI-based algorithms.**
  - **128-bit key versions were named A5/4 and GEA4 and corresponding draft TS was presented for information in SA#23.**
  - **SA3 proposes that work for A5/4 and GEA4 is moved to Release 7 in order that all related specifications can handle the 128-bit keys in the same Release.**

Generic authentication architecture (GAA)

- SA3 is specifying three stage 2 TSs and one TR
  - TR 33.919 Generic Authentication Architecture (GAA), which describes how GAA is used (for info in SA#22 and again in SA#24)
  - 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 (submitted for approval in SA#24)

GAA – System description

- TR 33.919 was presented for information in SA#22 but it is still not submitted for approval
  - 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)

- Nine Rel-6 CRs to 33.220:
  - Removal of Annex A (SP-040375)
  - NAF remove the security associations (SP-040376)
  - Removal of editors notes on Transaction Identifiers (SP-040377)
  - Introduction of a UICC-based Generic Bootstrapping Architecture (SP-040378)
  - Editorial corrections to TS 33.220 (SP-040379)
  - Support for NAF in visited network (SP-040380)
  - Editorial changes and clarifications to TS 33.220 (SP-040381)
  - Multiple key derivation mandatory (SP-040382)
  - NAF’s public hostname verification (SP-040383)

GAA – Support for subscriber certificates

- **One CR to 33.221 was proposed but approval postponed because SA#24 advice is needed first about correct referencing of OMA documents**

GAA – Secure HTTP access to network application functions

- Draft TS 33.222 presented for approval (SP-040368)
  - Draft progressed with several contributions
  - Internet draft about “preshared key TLS” added to IETF dependency list
- Open issues:
  - Some open issues related to preshared key TLS
  - Mandate of AES cipher suites as specified in RFC 3268
  - Inclusion of TLS extensions as specified in RFC 3546
  - Requirements for the Authentication Proxy architecture might be revisited after feasibility of preshared key TLS has been fully studied.
  - Transfer of further information elements in app. specific user profile in standardised format to AS
  - Changes in 33.220 about handling of app. specific user profiles may affect TS
  - Annex A may need to be revisited
  - The support of accessing an AS in the visited network is FFS in future release.

WLAN inter-working security

- Nine Rel-6 CRs to TS 33.234:
  - Profiling of IKEv2 and ESP for NAT traversal (SP-040384)
  - Sending of temporary identities from WLAN UE (SP-040385)
  - Extension of IKEv2 and IPsec profiles (SP-040386)
  - Support of EAP SIM and AKA in AAA server and WLAN UE (SP-040387)
  - Introduction of UE split alternative 2 in TS 33.234 (SP-040388)
  - Re-authentication failure notification to HSS (SP-040389)
  - Identity request procedure clarification (SP-040390)
  - WLAN mechanism to allow restrictions on simultaneous sessions (SP-040391)
  - Requirement on keeping WLAN access keys independent from 2G/3G access keys stored in USIM (SP-040392)

MBMS security 1/2

- Draft TS 33.246 was presented for information in SA#22 (December). Now it is presented for information second time (SP-040366).
  - 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
- A consensus was reached for key management architecture:
  - GBA method will be used (GBA_U + GBA_ME + MIKEY). If a terminal is to support MBMS, then it will need to support GBA_U.
  - There is both UICC-based solution and ME-based solution. Some companies objected to the keeping of both solutions and advocated the UICC-based solution only.
  - An LS was sent to SA1, T3, SA4 about the agreement

MBMS security 2/2

- Draft TS was progressed with several contributions on other issues (than the key management architecture).
- Open issues:
  - Details of app layer joining and leaving are still to be determined. Some input from SA4 is needed.
  - Derivation of MBMS keys from the keys provided by GBA_U. ETSI SAGE consulted for design of key derivation function.
  - Format of the delivery of MSKs still needs to be determined. It will be based on an extension of MIKEY. The exact combination of push/pull of MSK needs to be agreed.
  - Methods of protecting the data sent as part of an MBMS User Service are still open. SA3 has provided some possible solutions for SA4 to analyse and ensure that they fit with the SA4 requirements.

Presence security

- **TS 33.141 presented for approval (SP-040367)**
  - **TS 33.141 mainly covers HTTP-based Ut interface security between UE and presence list server**
- **Open issues:**
  - **Some dependencies with the ongoing work on Generic Bootstrapping Architecture (GBA).**
  - **ISIM support: If ISIM-only UICCs are allowed then it is ffs whether ISIM may be used in GAA**
  - **Decision on optional use of preshared key TLS and/or SSC**

Other SA3 work items

- Security for voice group call service
  - A proposed CR to 43.020 agreed in principle but some issues have to be checked still
  - SA3 has liased with several WGs on this topic
- Generic user profile security
  - An LS sent to SA2 & CN4

Actions expected from SA#24

Documents for approval (1/7)

CRs to 33.102:

- **SP-040369 CR to 33.102: Clarification on Authentication re-attempt parameter (Rel-6)**
- **SP-040370 2 CRs to 33.102: Handling of key sets at inter-system change (Rel-5, Rel-6)**

CR to 33.105:

- **SP-040371 CR to 33.105: Correction of inconsistencies in AK computation for re-synchronisation (Rel-4)**

CRs to 33.203:

- **SP-040372 CR to 33.203: Correction on IMS confidentiality protection (Rel-6)**
- **SP-040373 CR to 33.203: SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network (Rel-6)**

CR to 33.210:

- **SP-040374 CR to 33.210: Diffie-Hellman groups in NDS/IP (Rel-6)**

Documents for approval (2/7)

CRs to 33.220:

- **SP-040375 CR to 33.220: Removal of Annex A (Rel-6)**
- **SP-040376 CR to 33.220: NAF remove the security associations (Rel-6)**
- **SP-040377 CR to 33.220: Removal of editors notes on Transaction Identifiers (Rel-6)**
- **SP-040378 CR to 33.220: Introduction of a UICC-based Generic Bootstrapping Architecture (Rel-6)**
- **SP-040379 CR to 33.220: Editorial corrections to TS 33.220 (Rel-6)**
- **SP-040380 CR to 33.220: Support for NAF in visited network (Rel-6)**
- **SP-040381 CR to 33.220: Editorial changes and clarifications to TS 33.220 (Rel-6)**
- **SP-040382 CR to 33.220: Multiple key derivation mandatory (Rel-6)**
- **SP-040383 CR to 33.220: NAF's public hostname verification (Rel-6)**

Documents for approval (3/7)

CRs to 33.234:

- SP-040384 CR to 33.234: Profiling of IKEv2 and ESP for NAT traversal (Rel-6)
- SP-040385 CR to 33.234: Sending of temporary identities from WLAN UE (Rel-6)
- SP-040386 CR to 33.234: Extension of IKEv2 and IPsec profiles (Rel-6)
- SP-040387 CR to 33.234: Support of EAP SIM and AKA in AAA server and WLAN UE (Rel-6)
- SP-040388 CR to 33.234: Introduction of UE split alternative 2 in TS 33.234 (Rel-6)
- SP-040389 CR to 33.234: Re-authentication failure notification to HSS (Rel-6)
- SP-040390 CR to 33.234: Identity request procedure clarification (Rel-6)
- SP-040391 CR to 33.234: WLAN mechanism to allow restrictions on simultaneous sessions (Rel-6)
- SP-040392 CR to 33.234: Requirement on keeping WLAN access keys independent from 2G/3G access keys stored in USIM (Rel-6)

Documents for approval (4/7)

CRs to 33.310:

- **SP-040393 CR to 33.310: Removal of inconsistencies regarding SEG actions during IKE phase 1 (Rel-6)**
- **SP-040394 CR to 33.310: Removal of unnecessary restriction on CA path length (Rel-6)**
- **SP-040395 CR to 33.310: Correction of ‘Extended key usage’ extension in SEG Certificate profile (Rel-6)**

CR to 33.106 (LI Group):

- **SP-040396 CR to 33.106: Clarification on delivery of IRI and CC (Rel-6)**

Documents for approval (5/7)

CRs to 33.107 (LI Group):

- SP-040397 CR to 33.107: Correction on Network initiated Mobile Station Detach signalling flow (Rel-6)
- SP-040398 CR to 33.107: TEL-URL missing in activation of LI in the CSCFs (Rel-6)
- SP-040399 CR to 33.107: Correction on the use of session initiator parameter (Rel-6)
- SP-040400 CR to 33.107: Correction to HLR interception event name (Rel-6)
- SP-040401 CR to 33.107: Clarification for Push to talk over Cellular (Rel-6)
- SP-040402 CR to 33.107: Adding an encryption parameter to IRI across X2 interface (Rel-6)
- SP-040403 CR to 33.107: References (Rel-6)
- SP-040404 CR to 33.107: Enhancements for the Functional Architecture chapter (Rel-6)

Documents for approval (6/7)

CRs to 33.108 (LI Group):

- **SP-040405 CR to 33.108: Correction on interception identities in multi-media domain (Rel-6)**
- **SP-040406 2 CRs to 33.108: WGS 84 coordinates length correction (Rel-5, Rel-6)**
- **SP-040407 CR to 33.108: CR offering alignment to ETSI TS 101 671 (Rel-6)**
- **SP-040408 CR to 33.108: Additional text for Definition and Acronym section (Rel-6)**

Documents for approval (7/7)

- **SP-040175 Draft TS 33.141 v 2.0.0 and presentation cover sheet**
- **SP-040165 Draft TS 33.222 v 2.0.0 and presentation cover sheet**

Documents for information

- **SP-040363 Report from SA WG3 Chairman to TSG SA#24**
- **SP-040364 Draft Report of SA WG3 meeting #33**
- **SP-040365 Draft TR 33.919 and presentation cover sheet**
- **SP-040366 Draft TS 33.246 v 1.2.0 and presentation cover sheet**