SA3 (Security) Status Report to SA#22

Peter Howard, Vodafone

SA3 Vice Chairman

Contents

- **General aspects**
- **Status report on work items**
- **Actions expected from SA#22**

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)**

SA3 meetings since SA#21

- **SA3 plenary**
  - **SA3#30: Povoa de Varzim, Portugal, 6-10 October 2003, hosted by European Friends of 3GPP**
    - **Including joint session with CN1 on IMS**
  - **SA3#31: Munich, Germany, 18-21 November 2003, hosted by European Friends of 3GPP**
- **Lawful interception sub-group**
  - **LI#10: Jackson Hole, USA, 22-24 September 2003**
  - **LI#11: London, England, 18-20 November 2003**

Next SA3 plenary meetings

- **SA3#32: Edinburgh, Scotland, 9-13 February 2004, hosted by European Friends of 3GPP**
- **SA3#33: Beijing, China, 11-14 May 2004, hosted by Samsung**
- **SA3#34: Chicago, USA, 6-9 July 2004 (TBC)**
- **SA3#35: Europe, 5-8 October 2004 (TBC)**
- **SA3#36: China, 23-26 November 2004 (TBC)**

Next SA3-LI meetings

- **LI#12: USA, 27-29 January 2004 (TBC)**
- **LI#13: Europe, 14-16 April 2004 (TBC)**
- **LI#14: Europe, 20-22 July 2004 (TBC)**
- **LI#15: USA, 12-14 October 2004 (TBC)**

Statistics at SA3#30 and SA3#31

- **Around 50 delegates at each meeting**
- **334 temporary documents handled including**
  - **42 incoming LSs**
  - **19 outgoing LSs**

Summary of SA3 input to SA#22

- **10 SA3-LI CRs for approval**
- **18 SA3 CRs for approval**
- **5 TSs for information**
- **2 TRs for information**

Status report on work items

Lawful interception (1/2)

- **Rel-5 CR (with Rel-6 mirror CR)**
  - **SP-030592: Essential correction to ASN.1 coding for TCP-based transport of Intercept Related Information (IRI) in US annex of LI handover interface specification (33.108)**

Lawful interception (2/2)

- **Rel-6 CRs**
  - **SP-030589: Addition of references to related standards in LI requirements specification (33.106)**
  - **SP-030590: Clarification to LI architecture (33.107) on limitations of interception if MSISDN or IMEI is used instead of IMSI for PS domain interception**
  - **SP-030591: Completion of specification for intercept based on TEL URL in 33.107/33.108**
  - **SP-030593: Additions to LI handover interface (33.108) to support US requirement for dialled digit reporting**
  - **SP-030594: Additions to 33.108 on user packet data transfer in CS domain and management operations from ETSI TS 101 671 for backward compatibility reasons**
  - **SP-030595: Clarification to 33.108 on length of LI identifiers corresponding to changes in ETSI TS 101 671**

IMS security (1/4)

- **Rel-5 general status**
  - **Several open issues were resolved during a joint session with CN1 at SA3#30 which resulted in several stage 2 CRs being agreed by SA3**
    - **Corresponding stage 3 CRs were agreed at CN1#32**
  - **Specifications for SIP privacy are introduced, based on LSs from CN1 and SA2, to close gap with stage 3 specifications**

IMS security (2/4)

- **Rel-5 CRs (all have a Rel-6 mirror CR)**
  - **SP-030596: Clarification that the authentication response is calculated from RES and that RES is not sent in the clear**
  - **SP-030597: Minor clarifications to Security Association (SA) handling in P-CSCF**
  - **SP-030598: Addition of specification on how to use the transport layer with SIP**
  - **SP-030599: Clarification on the discard/rejection of SIP messages**
  - **SP-030600: Addition of specification on use of old SAs on pending transactions and behaviour of P-CSCF when old SA expires**

IMS security (3/4)

- **Rel-5 CRs (all except * have a Rel-6 mirror CR)**
  - **SP-030604: Clarification that the RAND sent to the UE is stored by the S-CSCF and subsequently sent to the HSS if there is a synchronization failure**
  - **SP-030605: When the S-CSCF challenges a new REGISTER while still waiting for a response to a previous challenge then the S-CSCF should abandon the previous challenge, and the P-CSCF should replace the old SA with the new one**
  - *** SP-030602: Specifications for SIP privacy are introduced to close gap with stage 3 specs**

IMS security (4/4)

- **Rel-6 CRs**
  - **SP-030601: Minor clarifications to improve readability**
  - **SP-030603: Minor correction to remove anti-replay requirement which was incorrectly added to confidentiality clause at SA#21**
- **Openness of IMS in Rel-6**
  - **SA3 is considering whether new mechanisms are needed to authenticate non-IMS clients**
    - **This is being progressed by email discussion**

UTRAN security

- **CRs to clarify handling of key set changes at inter-system change were postponed**
  - **More work needed at stage 3 level in CN1 and RAN2 before stage 2 CRs in SA3 can be agreed**

GERAN security

- New attack on GSM security
  - SA3 is working with GSMA security group to address an attack on GSM security reported at Crypto 2003 conference in August 2003
  - Manufacturers and operators have been asked to considered impact of various solutions (see S3-030682)
  - One specific solution has been discussed with involved 3GPP WGs and draft CRs have been developed
- A5/4 and GEA4
  - A5/3 and GEA3 refer to 64 bit key versions of the KASUMI-based algorithms
  - SAGE is developing 128-bit key versions named A5/4 and GEA4
  - The “delta” specification for A5/4 and GEA4 is expected to be ready in March 2004

GSM authentication algorithm

- **Rel-6 CR**
  - **SP-030606: Correction of references in GSM-MILENAGE Algorithm specification (55.205)**

Generic authentication architecture (GAA)

- **SA3 is specifying three stage 2 TSs and a TR**
  - **TR 33.919 GAA System Description, which describes the building blocks of the GAA**
  - **TS 33.220 Generic Bootstrapping Architecture, which specifies re-use of 3GPP AKA protocol to establish shared secrets for various applications**
  - **TS 33.221 Support for Subscriber Certificates, which specifies subscriber certificate enrolment and delivery of certificates to UE**
  - **TS 33.222 Access to Network Application Functions using HTTPS, which specifies how a bootstrapped shared secret (GBA) or subscriber certificate (SSC) is used for authentication in HTTP-based services**
- **Corresponding stage 3 specifications in CN1 (24.xxx) and CN4 (29.109)**

GAA – System description

- **TR 33.919 presented for information (SP-003582)**
  - **The GAA defines a generic architecture for authentication that can be used for a range of different applications**
  - **The TR is a framework document which describes the building blocks of the GAA and the relationship between the TSs that specify the GAA**
  - **Some further development of the TR is needed but there are no open issues**

GAA – Generic bootstrapping architecture

- **TS 33.220 presented for information (SP-030583)**
  - **The GBA describes a mechanism to bootstrap authentication and key agreement for application security from the 3GPP AKA protocol**
  - **Introduces new elements: Bootstrapping Server Function (BSF) and Network Application Function (NAF)**
- **Open issues**
  - **Management of profile in HSS and BSF**
  - **Need for new profile parameters in HSS**
  - **Key generation for NAF**
  - **Solution for CS domain**
  - **Method for NAF to initiate bootstrapping**
  - **Usage of GUP in GAA**

GAA – Support for subscriber certificates

- **TS 33.221 presented for information (SP-030584)**
  - **The SSC feature describes how the GBA can be used to support the subscriber certificate enrolment and delivery of certificates to UE**
- **Open issues**
  - **Charging mechanism and extent of standardisation**
  - **Applicability of other certificate profile specifications**
  - **Service discover of PKI portal**
  - **Use of shared key TLS to secure enrolment instead of HTTP Digest**
  - **Content type for HTTP response when delivering certificate chains**

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 has been progressed by several contributions but is not ready to present to SA for information**
- **Open issues**
  - **Decision needed on which variant(s) of TLS to use**
  - **Decision needed on what type of TLS authentication proxy to use**

WLAN inter-working security (1/2)

- **TS 33.234 presented for information (SP-030585)**
  - **This TS specifies authentication, link layer security and user identify privacy for WLAN scenario 2 and the establishment of security for UE-initiated tunnels in WLAN scenario 3**
- **Open issues**
  - **Security implications of WLAN-UE functionality split and simultaneous 3GPP/WLAN access**
  - **Specification of link layer security for scenario 2**
  - **Security mechanism for UE-initiated tunnel for scenario 3**
    - **Working assumption is to use EAP-AKA or EAP-SIM with IKEv2, but alternative solutions are kept in an annex**

WLAN inter-working security (2/2)

- **SA3#31 agreed LS on possible updates to Bluetooth SIM access profile for split WLAN-UE scenarios (S3-030780)**
  - **SA3 request authorisation from PCG to send liaisons to Bluetooth**

MBMS security

- **TS 33.246 presented for information (SP-030586)**
  - **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**
  - **It was agreed at SA3#31 that the MBMS keys can be held on the UICC or the ME in Rel-6 but this has not yet been incorporated into the TS**
  - **Exact way to use GBA to establish shared keys between UE and BM-SC**
  - **Mechanism for transport of MBMS keys to the UE (several proposals have been made)**
  - **Mechanism to protect traffic between BM-SC and UE**
  - **Harmonisation with OMA DRM**

Network domain security: authentication framework

- **TS 33.310 presented for information (SP-030587)**
  - **This specification provides a scalable entity authentication framework for 3GPP network nodes that are using NDS/IP (TS 33.210) for network domain control plane security**
- **Open issues**
  - **The specified enrolment protocol, CMPv2, is still an internet draft but it is already widely supported and expected to received RFC status by June 2004 at latest**
  - **Some further profiling of options may be needed to limit interoperability problems**
  - **Use of certificate issue name to restrict access to certain subnets is for further study**
  - **Specification of the public CRL interface is ffs**

Presence security

- **TS 33.141 presented for information (SP-030719)**
  - **SIP communications between watcher and server protected using IMS security (33.203) and NDS/IP (33.210)**
    - **Confidentiality protection added to 33.203 in Rel-6**
  - **TS 33.141 mainly covers HTTP-based Ut interface security between UE and presence list server**
- **Open issues**
  - **The TS will adopt the mechanisms considered for HTTP security from TS 33.222 but this has not yet been incorporated into TS 33.141**

Feasibility study on USIM re-use by peripheral devices

- **TR 33.817 presented for information (SP-030582)**
  - **This TR analyses various security threats and countermeasures to determine the feasibility of re-using 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 will consider 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 liased with T3 and GERAN2 on this topic**
- **Generic user profile security**
  - **SA3 is considering the use of Liberty Alliance specifications for the Rg interface**
- **Data rights management**
  - **SA3 has handled LSs from OMA and SA4 on a mechanism for carrying encrypted streams within PSS for DRM purposes**
  - **SA3 has agreed that 3GPP solution for MBMS security and OMA DRM solution should be aligned**

Other topics (1/2)

- **GPRS over-billing**
  - **SA3 is considering possible changes to the standards to address a recently publicised GPRS over-billing attack**
  - **This is being progressed by email discussion**
- **Liberty Alliance**
  - **A representative from Liberty Alliance gave an overview of their specifications at SA3#31**
  - **Possible synergies with GAA and GUP work in SA3**

Other topics (2/2)

- **MMS security**
  - **Presentations on a GSMA report on MMS security were given at SA3#30 and SA3#31**
  - **SA3 is considering possible updates to 3GPP specifications**
  - **A workshop may be arrange for early in the New Year**
- **OMA**
  - **The planned joint meeting/session with OMA security group has not yet been arranged**
  - **The scope will include SSC and MBMS**

Actions expected from SA#22

Actions expected

- **SA3 request authorisation from PCG to send liaisons to Bluetooth**

Documents for approval (1/2)

- **SP-030589: CR to 33.106: Correction to lawful interception references (Rel-6)**
- **SP-030590: CR to 33.107 MSISDN/IMEI clarification for GPRS interception (Rel-6)**
- **SP-030591: CRs to 33.107 and 33.108: Reporting TEL URL (Rel-6)**
- **SP-030592: CRs to 33.108: Correction to Annex G on TCP based transport (Rel-5 / Rel-6)**
- **SP-030593: CR to 33.108: LI Reporting of Dialed Digits (Rel-6)**
- **SP-030594: CRs to 33.108: CS Section for 33.108 - LI Management Operation and User data packet transfer (Rel-6)**
- **SP-030595: CR to 33.108 Alignment of Lawful Interception identifiers length to ETSI TS 101 671 (Rel-6)**
- **SP-030596: CRs to 33.203: Correcting the text on sending an authentication response (Rel-5 / Rel-6)**
- **SP-030597: CRs to 33.203: SA procedures (Rel-5 / Rel-6)**

Documents for approval (2/2)

- **SP-030598: CRs to 33.203: SA parameters and management (Rel-5 / Rel-6)**
- **SP-030599: CRs to 33.203: Reject or discard of messages (Rel-5 / Rel-6)**
- **SP-030600: CRs to 33.203: Correcting the SA handling procedures (Rel-5 / Rel-6)**
- **SP-030601: CR to 33.203: Terminology alignment (Rel-6)**
- **SP-030602: CR to 33.203: Introducing the SIP Privacy mechanism in Stage 2 specifications (Rel-5)**
- **SP-030603: CR to 33.203: Removing anti-replay requirement from Confidentiality clause (Rel-6)**
- **SP-030604: CRs to 33.203: Ensuring the correct RAND is used in synchronization failures (Rel-5 / Rel-6)**
- **SP-030605: CRs to 33.203: Network behaviour when a new REGISTER is challenged during an on going authentication (Rel-5 / Rel-6)**
- **SP-030606: CR to 55.205: Correction of reference (Rel-6)**

Documents for information

- **SP-030581: Reports of SA WG3 meetings since TSG SA#21**
- **SP-030582: Draft TR 33.919 version 1.0.0: Generic Authentication Architecture; System Description (Rel-6)**
- **SP-030583: Draft TS 33.220 version 1.0.0: Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (Rel-6)**
- **SP-030584: Draft TS 33.221 version 1.0.0: Generic Authentication Architecture (GAA); Support for Subscriber Certificates (Rel-6)**
- **SP-030585: Draft TS 33.234 version 1.0.0: Wireless Local Area Network (WLAN) Interworking Security (Rel-6)**
- **SP-030586: Draft TS 33.246 version 1.0.0: Security of Multimedia Broadcast/Multicast Service (Rel-6)**
- **SP-030587: Draft TS 33.310 version 1.0.0: Network Domain Security; Authentication Framework (Rel-6)**
- **SP-030588: Draft TR 33.817 version 1.0.0: Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Rel-6)**

Thank You!

Peter Howard, Vodafone

SA3 Vice Chairman