Technical Specification Group Services and System Aspects TSGS#19(03)0094

Meeting #19, Birmingham, UK, 17-20 March 2003

SA3 Status Report to SA#19
SP-020094

Michael Walker, SA3 Chairman

SA3 Leadership

Chairman: Michael Walker (Vodafone)

Secretary: Maurice Pope (MCC)

Vice-chairs:

- Valtteri Niemi (Nokia)
- Michael Marcovici (Lucent)

LI sub-group chair:

- Brye Bonner (Motorola)

Meetings Held

- SA3 Plenary
  - SA3#26: Sophia Antipolis, France, 25-28 February 2003
  - Report in SP-020095
- SA3 joint meetings
  - Joint SA2/SA3 meeting on MBMS: Milan, Italy, 24 February 2003
  - See SA2#30 meeting report
- Lawful interception sub-group
  - LI#01/03: Paris, France, 19-21 February 2003

Lawful Interception (1)

- Several essential changes to ensure that LI requirements are met
- Release 5/6 CRs on TS33.108 LI handover interface
  - Coding of ASN.1 parameters of type OCTET STRING (SP-030096)
    - Specifies the correct ordering of nibbles
  - Incorrect ASN.1 object tree (SP-020099)
    - Corrects a mistake in the ASN.1 object tree
- Release 6 CRs on TS33.108 LI handover interface
  - CS section (SP-030097)
    - In Rel-5 the circuit-switched part of the standard consists of a reference to ETSI TS 101 671. This is replaced in Rel-6 will a full text specification which has been updated for the 3GPP system.
  - Adjustments to the requirements on the delivery of the intercepted RT data over TCP (SP-030098)
    - Clarifies that when TCP is used as the transport protocol then the real time (RT) delivery of the result of the interception cannot be guaranteed

Lawful Interception (2)

- **Revised WID for LI in Rel-6 Architecture (SP-030106)**
  - **Presence service added to the list of Rel-6 study items**
  - **New dates added regarding the work plan**
    - **Rel-6 updates to LI specifications scheduled for approval at SA#22 (December 2003)**

IMS Security (1)

- Several corrections and clarifications made to the IMS security architecture
- Release 5 CRs on TS33.203 IMS security architecture
  - Clarification of the use of ISIM and USIM for IMS access (SP- 030100)
    - Specifies that ISIM is used if both ISIM and USIM exist on the UICC
  - Malicious UE bypassing the P-CSCF (SP-030101)
    - Recommends to use NDS/IP and IP traffic filtering to prevent a UE from bypassing the P-CSCF and I-CSCF to connect directly to the S-CSCF
  - Ensuring the deletion of unwanted SAs (SP-030102)
    - Clarifies that the P-CSCF should delete the Security Associations from an incomplete authentication when a subsequent authentication is completed
  - Add protected port into Via header (SP-030103)
    - Clarifies that the Port number must be included in the Via header of SIP messages for compliance with the SIP RFC and to ensure that the necessary information is available to establish a security association
  - Correction of the Port 2 definition for SA establishment (SP-030111)
    - A rule is added for selecting the source port number at the P-CSCF and a definition is added for the port numbers symbolic name

IMS Security (2)

- Use of SIM to access IMS services
  - A Rel-5 CR to TS33.203 was presented to SA#18 together with a corresponding LS highlighting security concerns
    - The CR was not approved at SA#18
  - A further LS to SA is presented to elaborate on the security concerns (SP-030071)
    - Describes security limitations with solution using conversion functions and solution using EAP-SIM
    - Identifies additional issues with SIM access to IMS

IMS Security (3)

- Other issues
  - Further work is needed to decide how to follow up the IMS security related conclusions from the IETF/3GPP workshop (26-27 January 2003)

Network Domain Security: IP layer (NDS/IP)

- **Several corrections and clarifications made to the NDS/IP specification**
- **Release 5/6 CRs on TS33.210 Network Domain Security: IP layer**
  - **Za interface and roaming agreements (SP-030104)**
    - **Clarifies that roaming agreements are not always needed for the Za interface because an operator can split his network into several security domains separated by inter-operator Za interfaces**
  - **Clarification on re-keying aspects (SP-030105)**
    - **Clarifies that the IPsec security associations (SA) should be re-keyed proactively, i.e. a new SA should be established before the old SA expires**

Network Domain Security: Authentication Framework (NDS/AF)

- **Revised WID: Network Domain Security: Authentication Framework (SP-030108)**
  - **The feasbility study (TR33.810) was completed at SA#18 so corresponding objectives are removed**
  - **The justification is improved based on the results of the feasibility study**
  - **It is added that the feasibility study will be used as the basis for the standardisation work**
  - **The expected completion date is brought forward by 3 months to March 2004**
- **New draft TS created**
  - **Sections on use cases, VPN establishment, cross-certification, operator / security gateway deregistration**
  - **Working assumption that cross certification will be done manually rather than using a bridge CA model**

UTRAN Security: Second Integrity and Encryption Algorithm

- **LS to SA on "Back up algorithms for UTRAN" (SP-030070)**
  - **The algorithm requirements specification sent to ETSI SAGE is attached to the LS as S3-030135**
  - **The attachment for the provisional work plan is incorrect – it is provided in a separate contribution (SP-030074)**
  - **The budget for the work is estimated to be 16 man months in case of no external evaluation. To cater for an external evaluation a further budget of 4 MM should be reserved.**
  - ***SA are asked to allocate the requested budget***
  - **In response to a question raised at SA#18, SA3 has not yet discussed possible implementation dates for the algorithm**
- **It is stressed again that SA3 continues to have full confidence in Kasumi; the measure is merely a safeguard**

GERAN Security (1)

- Two versions of A5/3 are defined
  - “GSM A5/3” and “EDGE A5/3”
- To clarify which version is used SA3 endorsed the following recommendation from GERAN
  - if the assigned channel combination in use contains at least one 8-PSK modulated channel, then only “EDGE A5/3” algorithm is used for all channels in the connection, irrespective of the modulation
  - conversely, if no 8-PSK channel is assigned, only the “GSM A5/3” algorithm shall be used

GERAN Security (2)

- **Revised WID: GERAN A/Gb security enhancements (SP-030107)**
  - **The errors in the date identified at SA#18 are corrected (“2002” -> “2003”)**

Policy Control and Subscription Control of Media

- Reply LS to SA and others on Policy Control and Subscription Control of Media (SP-030069)
  - SA3 studied the following issues relating to the use of the 488 message
    - Whether it causes denial of service problems
    - Whether the ability to deduce information about local operator policies using the 488 message is a security issue
  - The conclusion is that the use of the 488 message does not introduce new security requirements

Uplink TDOA location method

- SA3 studied a variant of the uplink TDOA location method where the GSM cipher key Kc is distributed to co-operating LMUs to increase accuracy and reduce data volume
- This increases the exposure of the Kc significantly
- A reply LS was sent to GERAN highlight the security issues
- Further co-operation with GERAN is needed if they decide to proceed with this approach

G-MILENAGE and A5/3

- **The approved specifications were published on the 3GPP server in December 2002**
  - **G-MILENAGE: TS55.203**
  - **A5/3 and GEA3: TS55.216, TS55.217, TS55.218 and TR55.919**
- **Update since SA3#27**
  - **A5/3 and GEA3 algorithms will be officially distributed by ETSI, GSMA and any organisational partners who wishes to distribute it**
    - **Distribution will be similar to the UMTS algorithms**
    - **Each beneficiary must sign a restricted usage undertaking and pay a corresponding administration fee**
  - **The distribution procedures for G-MILENAGE have yet to be formalised**

Generic User Profile

- Revised WID: Generic User Profile Security (SP-030109)
  - The dates in the work plan are updated
  - The new expected completion date is SA#21 (September 2003)

Support for Subscriber Certificates

- New draft TS created
- Progress was made to define an architecture for using the 3GPP AKA infrastructure to provide a secure way of issuing public key certificates to subscribers
- Candidate protocols are being considered for the various interfaces in the architecture, e.g.
  - HTTP Digest AKA is the preferred solution for exchanging AKA messages with the subscriber
  - PKCS#10 is being considered for certificate enrolment
  - DIAMETER is being considered for transporting key material and subscriber profile information
  - DIAMETER and MAP are being considered for exchanging AKA and subscriber profile information with the HSS
- A joint workshop with SA3, OMA, OASIS and W3C is being organised

WLAN Interworking Security

- Draft TS33.234 was progressed
  - Further information added on security threats and requirements
- An LS was sent to IEEE to request information about the expected completion date for the 802.11i standard
- SA2 were asked to comment on the implications of supporting Wi-Fi Protected Access WPA if the 802.11i standard is not ready in time
- Further clarification is needed on the WLAN-related conclusions from the IETF/3GPP workshop (26-27 January 2003)

Presence

- Draft TS33.xxx was progressed
  - Further information added on security requirements
- Working assumptions on security for HTTP access to the presence server
  - TLS will be taken as a “priority mechanism” for integrity and confidentiality protection of HTTP
  - Authentication should use the AKA architecture if possible

Multimedia Broadcast/Multicast

- Draft TS33.246 was progressed
  - Further information added on security requirements
- Joint meeting at SA2 plenary in Milan on 24 February
- SA3 agreed that encryption should be done on end-to-end between the UE and the multicast/broadcast service centre
  - Further information is needed on which protocols, media formats and codecs are to be supported before deciding which layer encryption should be applied at
  - Corresponding LS sent to SA4 (copy SA1 and SA2)
- An LS was sent to RAN2, GERAN and CN1 on how to avoid double encryption of MBMS bearers – this is desirable for a number of reasons
- Several approaches for how to do key management are being considered

Future SA3 Meetings

- SA3#28: 6-9 May 2003, Berlin, European ‘Friends of 3GPP’
- SA3#29: 15-18 July 2003, San Francisco, 3GPP2
  - Including joint meeting with 3GPP2
- SA3#30: 7-10 October 2003, European ‘Friends of 3GPP’(tbc)

- LI #9: 20-22 May 2003, Sophia Antipolis, France, European ‘Friends of 3GPP’
- LI #10: 23-25 September 2003, USA (host tbc)
- LI #11: 18-20 November 2003, London, UK, DTI

Documents for information/approval

Documents for Information/Approval

- **For Information:**
  - **SP-030094: Status report from SA WG3 to TSG SA#19**
  - **SP-030095: Report of SA WG3 meeting #27**
  - **SP-030069: LS (from SA WG3) on Additional Release 5 work needed for Policy Control and Subscription Control of Media**
  - **SP-030070: LS (from SA WG3) on Back up algorithms for UTRAN**
  - **SP-030071: LS (from SA WG3) on Requirement to allow IMS access by means of SIM**
  - **SP-030074: Provisional work plan for the design of the 3GPP confidentiality and integrity algorithms UEA2 and UIA2**

CRs for Approval

- SP-030096: 2 CRs to 33.108: Coding of ASN.1 parameters of the type OCTET STRING (Rel-5, Rel-6)
- SP-030097: CS Section for 33.108 (Rel-6)
- SP-030098: CR to 33.108: Adjustments to the requirements on the delivery of the intercepted RT data over TCP (Rel-6)
- SP-030099: CR to 33.108: Incorrect ASN.1 object tree (Rel-5, Rel-6)
- SP-030100: CR to 33.203: Clarification of the use of ISIM and USIM for IMS access (Rel-5)
- SP-030101: CR to 33.203: Malicious UE bypassing the P-CSCF (Rel-5)
- SP-030102: CR to 33.203: Ensuring the deletion of unwanted SA's (Rel-5)
- SP-030103: CR to 33.203: Add protected port into Via header (Rel-5)
- SP-030104: 2 CRs to 33.210: Za-interface and roaming agreements (Rel-5, Rel-6)
- SP-030105: 3 CRs to 33.210: Clarification to the re-keying aspects of network domain security (Rel-5, Rel-6)
- SP-030111: Correction of the Port 2 definition for SA establishment (Rel-5)
- SP-030149: 2 CR to 33.108: Correction to implementation of CR 005 (Rel-5, Rel-6)

WIDs for Approval

- **SP-030106: Revised WID: Lawful Interception in the 3GPP Rel-6**
- **SP-030107: Revised WID: GERAN A/Gb security enhancements**
- **SP-030108: Revised WID: Network Domain Security: Authentication Framework**
- **SP-030109: Revised WID: Generic User Profile Security**