Technical Specification Group Services and System Aspects *TSGS#21(03)0473*

Meeting #21, Frankfurt, Germany, 22-25 September 2003

SA3 Status Report to SA#21

Valtteri Niemi, SA3 Chairman

SA3 Leadership

Chairman: Valtteri Niemi (Nokia)

Secretary: Maurice Pope (MCC)

Vice-chairs:

- **Michael Marcovici (Lucent)**
- **Peter Howard (Vodafone)**

LI sub-group chair:

- **Brye Bonner (Motorola)**

Meetings Held

- **SA3 Plenary:**
  - **SA3#28: San Francisco, USA, 15-18 July 2003**
  - **Included joint session with 3GPP2 TSG-S WG4**
- **SA3 ad hoc meeting Antwerp, Belgium, 3-4 Sept:**
  - **About Generic Authentication Architecture and MBMS**
- **Lawful interception sub-group :**
  - **(LI#2/2003: Vienna, Austria, 20-22 May 2003)**

Lawful Interception

- **One Rel-6 CR (SP-030477) against TS 33.106 “Lawful Interception Requirements”**
- **One Rel-5 CR (SP-030478) and two Rel-6 CRs (SP-030479,480) against TS 33.107 “Lawful interception architecture and functions”**
- **Two Rel-5/Rel-6 CR pairs (SP-030509, SP-030482) and six Rel-6 CRs (SP-030508) against TS 33.108 “Handover interface for Lawful Interception”**

IMS Security

- **Three Rel-5 CRs (SP-030484,485,486) against TS 33.203 "Access security for IP-based services" result from liaison with CN1**
- **Two Rel-6 CRs (SP-030483,487) against 33.203:**
  - **Introducing Confidentiality Protection for IMS**
  - **Introducing Cipher key Expansion for IMS**
- **Scheduled a joint 1 ½ day session with CN1 to make sure that stages 2 & 3 are fully aligned before SA#22**

Network Domain Security: IP layer (NDS/IP)

- **Two pairs of Release 5/6 CRs against TS 33.210 ”Network Domain Security: IP layer”**
  - **Change of IKE profiling (SP-030488)**
    - **makes it possible to use NDS/IP in inter-domain case without a global DNS hierarchy**
  - **A reference upgraded from Internet draft to RFC (SP-030489)**

Network Domain Security: Authentication Framework (NDS/AF)

- **Draft TS**
  - **Has been progressed by several contributions**
  - **Is well in line to be submitted for information in SA#22**

UTRAN Security: unciphered IMEISV transfer (for "early UE handling")

- **Two Rel-5 CRs against 33.102 "Security architecture" were created based on the advice from SA2 (SP-030476) :**
  - **IMEISV retrieval before completion of security mode setup procedure**
  - **Mitigation against a man-in-the-middle attack associated with early UE handling**

UTRAN Security: other issues

- **One Rel-6 CR (SP-030475) against 33.102 "Security architecture": Clarification on the usage of the c3 conversion function**

GERAN Security

- **The algorithm names A5/3 and GEA3 refer to the 64-bit key versions of the KASUMI based algorithms**
- **The 128-bit key versions to be named A5/4 and GEA4 (following suggestion from CN1) → "delta" specifications to be created.**
- **One Rel-6 CR (SP-030490) against TS 55.216**
  - **Clarification on the usage of the Key length (restricts the key length to values 64 and 128)**

Support for Subscriber Certificates

- **Draft TS progressed with several contributions.**
- **LSs sent to CN1 & CN4 to query whether they can take over the needed stage 3 specification work.**
- **A joint meeting/session planned with OMA security group**
- **An ad hoc meeting was held 3rd Sept on Generic authentication architecture:**
  - **Bootstrapping shared secret keys from the AKA infrastructure is the core of the rel. 6 concept**
  - **The shared keys are used to deliver subscriber certificates, set up TLS tunnels etc.**

WLAN Interworking Security

- **Draft TS 33.234 was progressed by several contributions**
- **Implications of the trust relation between the Cellular Operator and the WLAN Access Provider are discussed over email**
- **Several LSs were sent**

Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces

- **A baseline draft TR has been created by supporting companies but not yet endorsed by SA3**
- **The work has been progressed by phone conferences**

Presence

- **Agreed to make a split between TS 33.203 (IMS access security) and Presence security**
  1) Create a new TS for Presence security and move relevant parts from the current draft Presence security TR to this new TS;
  2) Some parts of the draft Presence security TR moved to TS 33.203;
  3) Future services on top of IMS are candidates for creating an individual TS rather than updating the TS33.203 for each new application
- **Proxy functionality to be used as the TLS termination point (for protection of the Ut interface)**

Multimedia Broadcast/Multicast

- **Draft TS 33.246 progressed by several contributions**
- **Ad hoc meeting held 3-4 September**
  - **Reduced the number of key management schemes under consideration**

Future SA3 Meetings

- **SA3#30: 6-10 October 2003, Povoa, Portugal, EF3**
  - **Including joint meeting with CN1 about IMS security**
- **SA3#31: 18-21 November 2003, Munich (tbc), EF3**
- **LI #3/2003: 22-24 September 2003, Jackson Hole, USA, NAF3**
- **LI #4/2003: 18-20 November 2003, London, UK, DTI**

Documents for information/approval

Documents for Information/Approval

- **For Information:**
  - **Status report from SA WG3 to TSG SA#20 (SP-030473)**
  - **Draft Report of SA WG3 meeting #28 (SP-030474)**

CRs for Approval

Doc-1st-Level	Spec	CR	Phase	Subject	Cat	Version-Current	WG-Resp	Doc-2nd-Level
SP-030475	33.102	180	Rel-6	Clarification on the usage of the c3 conversion function	F	5.2.0	S3	S3-030465 rev (MCC re-edited using correct base Release version)
SP-030476	33.102	181	Rel-5	IMEISV retrieval before completion of security mode setup procedure	F	5.2.0	S3	S3-030478
SP-030476	33.102	182	Rel-5	Mitigation against a man-in-the-middle attack associated with early UE handling	C	5.2.0	S3	S3-030479 (e-mail)
SP-030477	33.106	005	Rel-6	References	D	5.1.0	S3	S3-030352
SP-030478	33.107	031	Rel-5	Missing QoS Parameter in IRI	F	5.5.0	S3	S3-030352
SP-030479	33.107	032	Rel-6	TEL URL for IMS interception identity	B	5.5.0	S3	S3-030352
SP-030479	33.107	033	Rel-6	Stereo delivery to LEMF	D	5.5.0	S3	S3-030352
SP-030508	33.108	017r1	Rel-6	Correct Abbreviations in TS 33.108	D	6.2.0	S3	S3-030352_rev
SP-030509	33.108	018r1	Rel-5	Syntax error in Annex B.3	F	5.4.0	S3	S3-030352_rev
SP-030509	33.108	019r1	Rel-6	Syntax error in Annex B.3	A	6.2.0	S3	S3-030352_rev
SP-030508	33.108	020r1	Rel-6	Inconsistency in Annex B.3	D	6.2.0	S3	S3-030352_rev
SP-030508	33.108	021r1	Rel-6	Data Link Establishment and Sending part for ROSE operation	F	6.2.0	S3	S3-030352_rev
SP-030508	33.108	022r1	Rel-6	Correction on the usage of Lawful Interception identifiers	F	6.2.0	S3	S3-030352_rev
SP-030508	33.108	023r1	Rel-6	Subscriber controlled input clarification	F	6.2.0	S3	S3-030352_rev
SP-030508	33.108	024r1	Rel-6	Field separator in subaddress	D	6.2.0	S3	S3-030352_rev
SP-030482	33.108	025	Rel-5	Reference errors in Annex G	F	5.4.0	S3	S3-030394
SP-030482	33.108	026	Rel-6	Reference errors in Annex G	A	6.2.0	S3	S3-030395
SP-030483	33.203	042	Rel-6	Introducing Cipher key Expansion for IMS	B	5.6.0	S3	S3-030375
SP-030484	33.203	043	Rel-5	Modification of the security association lifetime management	F	5.6.0	S3	S3-030442
SP-030485	33.203	044	Rel-5	Annex H in 33.203	F	5.6.0	S3	S3-030445
SP-030486	33.203	045	Rel-5	Security association handling, behaviour of SIP over TCP and re-authentication	F	5.6.0	S3	S3-030461
SP-030487	33.203	046	Rel-6	Introducing Confidentiality Protection for IMS	B	5.6.0	S3	S3-030455
SP-030488	33.210	011	Rel-5	Change of IKE profiling	F	5.4.0	S3	S3-030350
SP-030488	33.210	012	Rel-6	Change of IKE profiling	A	6.2.0	S3	S3-030354
SP-030489	33.210	013	Rel-5	Update draft-ietf-ipsec-sctp-03.txt reference to new standard RFC: RFC3554	F	5.4.0	S3	S3-030404
SP-030489	33.210	014	Rel-6	Update draft-ietf-ipsec-sctp-03.txt reference to new standard RFC: RFC3554	A	6.2.0	S3	S3-030405
SP-030490	55.216	002	Rel-6	Clarification on the usage of the Key length	F	6.1.0	S3	S3-030438

WIDs for Approval

- **WID for Key Management of group keys for Voice Group Call Services (SP-030491)**