3GPP TSG-SA WG3 (Security)

Report to SA Meeting # 5,

Kyongju, Korea

11-13 October 1999

Michael Walker

Chairman 3GPP TSG-SA WG3

Content of Presentation

- Summary of documents tabled by S3
- Status of deliverables - followed by approval
- Security features provided by S3 for R99
- Status of algorithm design
- 3GPP authentication as a candidate for TIA ESA
- Lawful interception
- Meeting schedule

Document List, 1

- SP-99477, Report of SA WG3 meeting #5, 3-6 Aug, Sophia Antipolis - *for information*
- SP-99478, Report of SA WG3 meeting #5bis, 25 Aug, Bonn - *for information*
- SP-99xxx Draft Report of SA WG3 meeting #6, 29 Sep - 1 Oct, Sophia Antipolis - *for information*
- SP-99426, Status of SA WG3 deliverables - *for information & discussion*

Document List, 2
CRs for Approval

- SP-99417, CRs to TS33.102, Security architecture - *for approval*
- SP-99418, CRs to TS33.105, Cryptographic algorithm requirements - *for approval*

Document List, 3
Specifications, Reports & LS for Approval

- SP-99424, TS33.103, Integration guidelines - *for approval*
- SP-99423, TR33.902, Formal analysis of security mechanisms - *for approval*
- SP-99xxx, LS to TIA TR-45 AHAG - *for approval*

Status of 3GPP Security Deliverables, 1

TS33.120	Security principles and objectives	Approved at SA#3	Stable
TS21.133	Security threats and requirements	Approved at SA#3.	CRs may be required at SA#6 to refine or clarify some security requirements.
TS33.102	Security architecture	Approved at SA#3. 11 CRs approved at SA#4. **CRs for approval at SA#5.**	More CRs expected at SA#6.

Status of 3GPP Security Deliverables, 2

TS33.103	Integration guidelines	For approval at SA#5.	CRs may be required at SA#6 to align with architecture.
TS33.105	Cryptographic algorithm requirements	Approved at SA#4. **CRs for approval at SA#5.**	CRs may be required at SA#6 to align with architecture.
TR33.901	Criteria for cryptographic algorithm design process	Approved at SA#4.	Stable.

Status of 3GPP Security Deliverables, 3

TS33.106	Lawful interception requirements	Approved at TSG-SA #4.	CRs expected at SA#6.
TS33.107	Lawful interception architecture and functions	Approval at SA#6 planned.	Originally planned for approval at SA#5.
TR33.900	Guide to 3G security	Approval at SA#6 planned.	Draft presented at S3#6.
TRxx.xxx	Formal analysis of security mechanisms	**For approval at SA#5.**	Additional analyses may be added.

TS33.102, Security Architecture, 1 CRs for Approval - 417

- modification of cipher/integrity key setting procedure
- reorganisation of document structure
- ***refinement and extension of integrity mechanism (including security mode control)***
- refinement and extension of MAP security
- ***addition of mechanisms for secure UMTS-GSM interoperation***

TS33.102, Security Architecture, 2 CRs for Approval - 417

- refinement of network-wide confidentiality
- addition of authentication management field to authentication request
- additional support for sequence number management
- clarifications on example window/list mechanisms for sequence number management

TS33.105, Cryptographic Algorithm Requirements - CRs for Approval - 418

- additional information on likely available resources for algorithms on USIM
- ***changes to integrity algorithm based on recommendations from SAGE***
- additional information on cipher keystream block length

Deliverables for Approval, 1

- TS33.103, Integration guidelines - 424
  - defines how elements in architecture are integrated into network nodes (AuC, MSC/VLR, SGSN, RNC, UE, USIM)
  - defines cryptographic functions required (including standard/proprietary, optional/mandatory)
  - defines data elements required (including length, lifetime, optional/mandatory)

Deliverables for Approval, 2

- TR33.902, Formal analysis of security mechanisms - 423
  - BAN-logic analysis of authentication and key agreement protocol
  - Temporal Logic of Actions (TLA) analysis of sequence number management mechanism

Security Features Provided by S3 - R99, 1

- User identity confidentiality
  - corrections possible early next year if there are problems integrating encrypted IMSI into other specs
- Access link integrity/ciphering
- Mutual Authentication and key agreement
- Visibility and configurability
- Core network signalling security
  - MAP over SS7 security addressed in R99

Security Features Provided by S3 - R99, 2

- Secure UMTS-GSM interoperation
  - corrections possible early next year (PS domain may be problematic)
- Network wide encryption mechanism
  - verification of hooks early next year may led to some corrections
- Terminal security
- Lawful interception

Security Features Provided by S3 - R99, 3 (as for GSM)

- Fraud Information Gathering System
- USIM application security
- Mobile Execution Environment
- Location services

Security Features Provided by S3 for R00

- Core network signalling security
  - INAP over SS7 and GTP security may slip into R00
  - Security of MAP over IP will be addressed in R00
- IP security
  - some support for mobile IP may be in release 99
  - detailed specification of security features will not be available until R00

Status of Algorithm Design

- Algorithm design based on MISTY block cipher from Mitsubishi
- IPR position
- Design process agreed at SA#4
- Terms of reference for external evaluators agreed
- Evaluators to be selected at S3#7 jointly with SAGE
- Evaluation period: 15 Nov - 13 Dec

3GPP Authentication Mechanisms as a Candidate for TIA TR-45 ESA

- 3GPP2 planning to select mechanism
- Four candidates: 3GPP, Certicom, CipherIT, Lucent
- Support of 3GPP candidate endorsed by S3#6
- S3 to carry 3GPP vote in straw poll this week
- LS to TIA TR-45 AHAG - *for approval and distribution this week*
- Decision before end Dec 99
- Lobbying in TIA required over next few months

Lawful Interception

- Approval of LI architecture has slipped to SA#6
- More regulator involvement required - only UK are Germany currently represented

Meeting Schedule

- *3-6 Aug 99, Sophia Antipolis, S3#5 (with SMG10)*
- *24 Aug 99, Bonn, Joint session on USIM at T3#7*
- *25 Aug 99, Bonn, S3#5bis*
- *29 Sep - 1 Oct 99, Sophia Antipolis, S3#6*
- 25 Oct 99, The Hague, Joint session with SAGE
- 26-27/28 Oct 99, The Hague, S3#7 (with SMG10 pre-SMG#30)
- 16-19 Nov 99, Sophia Antipolis, S3#8 (with SMG10)
- 7-9 Dec 99, Helsinki. S3#9 (extra day added)
- 19-21 Jan 2000, Location tba, S3#10 (new meeting)
- 22-24 Feb 2000, Location tba, S3#11 (new meeting)
- 11-13 Apr 2000, Location tba, S3#12 (new meeting)