SP-000267

3GPP TSG-SA WG3 (Security)

Status report to SA#8

26-28 June, 2000

Düsseldorf, Germany

Michael Walker

Chairman 3GPP TSG-SA WG3

Content of presentation

- Document list
- Report and review of progress in S3 (AI 6.3.1)
- Questions for advice from S3 (AI 6.3.2)
- Approval of contributions from S3 (AI 6.3.3)

Document list

- S3 meeting reports - *for information*
  - SP-000268 : Report of SA WG3 meeting #11
  - SP-000269 : Report of SA WG3 meeting #12
  - SP-000270 : Report of SA WG3 meeting #13
- CRs to TS 33.102, TS 33.103, TS 33.105 and TS 22.022- *for approval*

  SP-000271, SP- 000272, SP-000273, SP-000274
- R00+ security work items - *for information/approval*

Report and review of progress in S3 (AI 6.3.1)

- Meetings
- Confidentiality/integrity algorithms
- Authentication algorithm
- Harmonisation of 3GPP/3GPP2 authentication
- Open R99 security issues
- S3 technical specifications and reports
- Integration of security features into R99 specifications
- R00+ security work programme

S3 meeting reports

- S3#11, 22-24 January 2000, Mainz (before SA#7)
  - S3-approved report available in SP-000268 - *for information*
- S3#12, 11-14 April 2000, Stockholm
  (including joint meeting with TR-45 AHAG)
  - S3-approved report available in SP-000269 - *for information*
- S3#13, 23-26 May 2000, Yokohama
  - Draft report available in SP-000270 - *for information*
- Joint S3/CN meeting, 13-14 June 2000, Sophia

Meetings scheduled after SA#8

- S3#14, 01-04 Aug 2000, Oslo
- S3#15, 12-15 Sep 2000, Arlington, Virginia (tbc)
  (including joint meeting with TR-45 AHAG)
- S3#16, 27-30 Nov 2000, Israel (tbc)

Confidentiality & authentication algorithms

- SA#7 approved report on the work performed by SAGE task force on cipher
  - Published as 3G TR 33.908
- And approved algorithms for distribution to 3GPP partners
  - Publication of algorithm specifications and report on evaluation results was delayed for procedural reasons
- SA#7 approved the development of standard authentication algorithm and SAGE work plan tabled at SA#7
  - Funding approved by 3GPP in June 00
  - Target algorithm publication by end of Sep 00

Harmonisation of 3GPP/3GPP2 authentication

- First joint meeting with AHAG during S3#12 (Apr 00)
- Further joint meeting planned during S3#15 (Sep 00)
- S3 to propose that certain clauses in 3GPP specifications are considered for joint control as they contain the stage 2 description of the 3GPP AKA
  - LS to AHAG to be agreed at S3#14 in August
- Other issues / AHAG requirements on 3GPP AKA
  - Home control of AKA - the need for R00+ work items on this is being considered by S3
  - Support for global challenge at initial registration - AHAG are considering several proposals with varying impact on 3GPP AKA and intersystem operation

Open R99 security issues (1)

- Core network security (MAP application layer security)
  - Moved to early version of R00 at SA#7
  - CRs presented for approval to CN#8 to complete work
- Core network security (GTP, MAP-over IP, new interfaces/applications in R00, key management)
  - Two R00+ work items created - key management; everything else
- Enhanced user identity confidentiality
  - Moved to R00 at SA#7
  - No R00+ work items created - no support in S3
- Authentication failure reporting to HE
  - CRs presented for approval to CN#8 to complete R99 work
- Emergency calls handling
  - CR rejected at SA#7
  - New CR tabled at SA#8 (CR95 to 33.102 considered under AI 6.3.3)

Open R99 security issues (2)

- MS behaviour on network authentication token reject
  - CRs presented for approval to CN#8 to complete R99 work (issue resolved in N1)
- R00+ work items created for
  - Network-wide encryption
  - Rejection of unenciphered connections
  - UE triggered re-authentication during connections
  - 3G location services security
  - OSA security
- Further corrective CRs expected as security features continue to be integrated into other specifications; changes possible to
  - handover, sequence number management

S3 technical specifications and reports (1)

- TS 33.120: Security principles and objectives
  - approved at SA#3 - stable
- TS 21.133: Security threats and requirements
  - approved at SA#3; 1 CR at SA#6 - stable
- TS 33.102: Security architecture
  - approved at SA#3;
    - 11 CRs approved at SA#4,
    - 10 CRs approved at SA#5;
    - 15 CRs approved at SA#6;
    - 28 CRs approved at SA#7
  - **17 CRs presented for approval at SA#8**

S3 technical specifications and reports (2)

- TS 33.103: Integration guidelines
  - approved at SA#5; 3 CRs at SA#6; 1 CR at SA#7
  - **3 CRs at SA#8** - Alignment with TS 33.102
- TS 33.105: Cryptographic algorithm requirements
  - approved at SA#4; 3 CRs approved at SA#5; 2 CRs approved at SA#6; 4 CRs at SA#7
  - **1 CR at SA#8** - Alignment with TS 33.102
- TS 33.106: Lawful interception requirements
  - approved at TSG-SA#4; 1 CR approved at SA#6 - stable
- TS 33.107: Lawful interception architecture and functions
  - approved at SA#6 - stable

S3 technical specifications and reports (3)

- TR 33.900: Guide to 3G security
  - approval at SA#7 planned; postponed until SA#8
  - **Postponed until SA#9 - content immature**
- TR 33.901: Criteria for cryptographic algorithm design
  - approved at SA#4 - stable
- TR 33.902: Formal analysis of security mechanisms
  - Approved at SA#5; 1 CR approved at SA#6 - stable
- TS 22.022: ME personalisation
  - Under S3 control since SA#6
  - **1 CR at SA#8 -** Update to make specification applicable to 3GPP as well as GSM

S3 technical specifications and reports (4)

- TR 33.908: Report on confidentiality/integrity algorithm development
  - Approved at SA#7 - stable
- Publication of confidentiality/integrity algorithm specifications and evaluation has been delayed
  - TS 35.201: f6, f7 security algorithm specifications
  - TS 35.202: Kasumi algorithm specifications
  - TS 35.203: Implementation test data
  - TS 35.204: Design conformance test data
  - TR xx.xxx: Algorithm evaluation results

Integration of security into R99 specifications

- Need to ensure that S3 security features are properly integrated into the R99 specifications
- S3 is reviewing relevant specifications on
  - authentication and key agreement
  - confidentiality and integrity protection
  - secure 2G-3G inter-working - most CRs are expected to be in this area
  - others areas may follow
- S3 is identifying where corrective CRs are required with assistance of other WGs

R00+ security work programme

- Structured programme for R00+ security work items being created in conjunction with Security IGC in S2
  - 15 WI descriptions tabled at SA#8 (to be considered under AI 6.3.3)
  - further WI descriptions to be drafted at S3#14 on VHE, location
  - See latest R00+ project plan from S2
- Dependencies between WGs identified and timescales being agreed (e.g. joint meeting with CN, 13-14 June 2000)
- Security work item project phases
  - Requirements capture by S3
  - Security feature specification by S3
  - Feasibility study by S3 other WGs (optional)
  - Definition of security architecture by S3
  - Integration of security architecture by other WGs (optional)

Questions for advice from S3 (AI 6.3.2)

- No items

Approval of contributions from S3 (AI 5.3.3)

- CRs to TS 33.102 Security Architecture - 17
- CRs to TS 33.103 Integration Guidelines - 3
- CRs to TS 33.105 Cryptographic Algorithms Requirements Specification - 1
- CRs to TS 22.022 ME Personalisation - 1
- R00+ work item descriptions -15

CRs to TS 33.102 - *for approval (1)*

- SP-000271: CRs to TS 33.102 (Security Architecture)
  - CR097R1: Clarification on the meaning of the asterisk in Figure 18
  - CR103R2: Clarification of terminology in user domain
    - Replace UE with ME throughout
    - Clarification (see section 6.8.1.5) that USIM shall support 3GPP AKA and may support backwards compatibility with GSM by supporting GSM cipher key derivation function plus SIM-ME interface (GSM 11.11)

CRs to TS 33.102 - *for approval (2)*

- SP-000272: CRs to TS 33.102 (Security architecture)
  - CR080: Clarification on intersystem handover
    - hyperframe number handling
    - starting integrity protection
    - changing ciphering algorithm
    - ‘handover to UTRAN complete’ message not integrity protected
  - CR083: Clarification on authentication
    - changes due to incorrect implementation of CR037R1
    - MAC-S needs padding with zeros before input to f5 function
    - USIM does not store RAND for re-synchronisation
  - CR084: Changes to conversion functions for intersystem operation

CRs to TS 33.102 - *for approval (3)*

- SP-000272: CRs to TS 33.102 (Security Architecture)
  - CR088R2: The length of initial hyperframe number (START) is defined as 20 bits and the management of START values for CS /PS domains described in detail.
  - CR090: Values for the DIRECTION bit are defined for the confidentiality and integrity algorithms. The BEARER parameter is defined as the radio bearer since the logical channel identifier is not unique for one UE.
  - CR093: Removal of MAP application layer protection following decision at SA#7.
  - CR094: The requirement that the MSC/VLR or SGSN to update CK and IK at least every 24 hours removed.

CRs to TS 33.102 - *for approval (4)*

- SP-000272: CRs to TS 33.102 (Security Architecture)
  - CR095: Specifications on how emergency calls are handled are added.
  - CR096: Clarification that there is one initial hyperframe number per CN domain (CS and PS). Clarification that a new CK and IK resets the hyperframe number.
  - CR098: Replaces one instance of COUNT with COUNT-C.
  - CR100: Clarification of hyperframe number management by by using the START parameters in the description.

CRs to TS 33.102 - *for approval (5)*

- SP-000273: CRs to TS 33.102 (Security Architecture)
  - CR092: Removal of enhanced user identity confidentiality following decision at SA#7.
  - CR102: Removal of network-wide encryption specifications.
- SP-000274: CRs to TS 33.102 (Security Architecture)
  - CR089: A further sequence number generation scheme is defined which allows for a more static AuC database
  - CR091: The radio bearer identity is appended to the front of the message to be integrity protected.

CRs to TS 33.103 - *for approval*

- SP-000271: CRs to TS 33.103 v3.2.0 (Integration guidelines)
  - CR009: The sequence number length is defined as 48 bits.
- SP-000273: CRs to TS 33.103 v3.2.0 (Integration guidelines)
  - CR007: Removal of enhanced user identity confidentiality following decision at SA#7.
  - CR008: Removal of MAP application layer protection following decision at SA#7.

CRs to TS 33.105 - *for approval*

- SP-000271: CR to TS 33.105 v3.3.0 (Algorithm requirements)
  - CR011: Values for the DIRECTION bit are defined for the confidentiality and integrity algorithms. The BEARER parameter is defined as the radio bearer since the logical channel identifier is not unique for one UE.

CRs to TS 22.022 - *for approval*

- SP-000271: CR to TS 22.022 v3.1.0 (ME personalisation)
  - CR002: Update to make specification applicable to 3GPP

R00+ work item descriptions - *for information/approval (1)*

- R00+ security work item descriptions
  - SP-000296: Access security for IP multimedia services
  - SP-000297: Network based end-to-end security
  - SP-000298: User plane security
  - SP-000299: MAP application layer protection
  - SP-000300: Core network security
  - SP-000301: Key management for core network security
  - SP-000302: OSA security
  - SP-000303: MExE security
  - SP-000304: FIGs
  - SP-000305: Visibility and configurability of security

R00+ work item descriptions - *for information/approval (2)*

- R00+ security work item descriptions
  - SP-000306: Evolution of CS algorithms (A5/3 development and deployment)
  - SP-000307: Evolution of PS algorithms (GEA2 deployment)
  - SP-000308: GERAN security
  - SP-000309: Lawful interception architecture
  - SP-000310: General security enhancements