SA WG3#12 S3-000234

TSG SA#7
15-17 March, 2000 Madrid

SP-000042

3GPP TSG-SA WG3 (Security)

S3 status report to SA#7

15-17 March 2000

Dr. Stefan Pütz

Vice-chairman 3GPP TSG-SA WG3

T-Mobil

SA WG3#12 S3-000234

T-Mobil

Content of presentation

- Summary of documents tabled by S3
- Report and questions from S3 (AI 5.3.1)
- Review of S3's completion of R99 (AI 5.3.2)
- Approval of contributions from S3 (AI 5.3.3)

T-Mobil

Document list (1)

- Liaisons to SA plenary
  - SP-000005: LS to ETSI SAGE on delivery of algorithm specifications
  - SP-000076: LS to TR-45 on proposed procedures for joint control of 3GPP AKA
  - SP-000043: LS on MAP security status report
  - SP-000111: LS on MAP security
  - SP-000006: LS concerning EUIC status

Document list (2)

- SP-000049: General report from ETSI SAGE on the design, specification and evaluation of the standard 3GPP confidentiality and integrity algorithms - *for approval*
- SP-000118: ETSI SAGE work plan for algorithm design is available - *for information*
- SP-000121: Discussion paper on GPRS encryption - *for information*

Document list (3)

- CRs to TS 33.102 - *for approval*
  - SP-000112: Miscellaneous CRs to TS 33.102 (revision of SP-000046)
  - SP-000077: Miscellaneous CRs to TS 33.102
  - SP-000044: CR on MAP security

Document list (4)

- CRs to TS 33.103 - *for approval*
  - SP-000047: CR on alignment of integration guidelines (TS 33.103) with security architecture (TS 33.102)
- CRs to TS 33.105 - *for approval*
  - SP-000048: Miscellaneous CRs to TS 33.105
- CRs on EUIC - *for approval*
  - SP-000075: Miscellaneous CRs on EUIC (revision of SP-000045)

T-Mobil

Report and questions from S3 (AI 5.3.1)

- Meeting schedule
- Status of confidentiality/integrity algorithm
- Common authentication for 3GPP and 3GPP2
- Status of authentication algorithm
- Status of open R99 security issues
  (as identified during SA#6)

Meetings since SA#6

- S3 adhoc with N2 experts invited, 16 Jan 2000, Darmstadt
  - Report available in S3-000016 - *for information*
- S3#10, 19-21 Jan 2000, Antwerp
  - Report available in S3-000096 - *for information*
- S3#11, 22-24 Feb 2000, Mainz
  - Draft report available in S3-000218 - *for information*
- N2B adhoc with S3 experts invited, 2 Mar 2000, Kista

T-Mobil

Meetings schedule after SA#7

- S3#12, 11-14 Apr 2000, Stockholm
  (including joint meeting with TR-45 AHAG)
- S3#13, 23-25 May 2000, Tokyo
- S3#14, 01-03 Aug 2000, Oslo
- S3#15, 19-21 Sep 2000, location tbd
- S3#16, 27-30 Nov 2000, location tbd

Status of confidentiality/integrity algorithm (1)

- SP-000005: LS to ETSI SAGE on delivery of algorithm specifications - *for information*
  - Status of work done by ETSI SAGE Task Force
  - S3 chairman has received the specifications of the confidentiality and integrity algorithms including the underlying block cipher Kasumi
  - 'Report on the work performed by the Task Force' and 'Report on the evaluation results' formally endorsed by S3
  - Algorithm publication (including 'Report on the evaluation results') is delayed

T-Mobil

Status of confidentiality/integrity algorithm (2)

- SP-000049: General report from ETSI SAGE on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms
  - *for approval and publication as 3GPP TR*

Common authentication for 3GPP and 3GPP2

- TR-45 has adopted 3GPP authentication mechanism; approve global challenge but optional for HLR - *not yet officially confirmed*
- SP-000076: LS to TR-45 on proposed procedures for joint control of 3GPP AKA - *for information*
  - S3 acknowledges the need to define procedures to allow joint control of the 3GPP AKA specifications so that both S3 and TR-45 requirements may be addressed
  - Details on the exact procedures will be formulated at the joint S3/AHAG meeting to be held in April

T-Mobil

Status of authentication algorithm (1)

- Standard authentication algorithm is recommended to encourage a minimum level of security across all 3GPP networks
- Reduces the risk of some operators choosing a weak algorithm
- Standard algorithm will have operator-specific part
- Publication by end of Sep 2000
- Operator-specific algorithm can still be selected
- SA asked to approve the requirement for standard authentication algorithm

T-Mobil

Status of authentication algorithm (2)

- S3 intends to task ETSI SAGE to do the work for the algorithm, subject to the approval of funding
- ETSI SAGE work plan for algorithm design is available (SP-000118 - *for information*)
- Week 39 (end Sep 2000) is indicated for final specification delivery under condition that funding will be clarified by 20 Mar 2000
- Some extra funding is needed so that a Japanese partner can be included in Task Force

T-Mobil

Status of open R99 security issues (1)

- Authentication failure report indicator
- Network-wide encryption
- Encryption mandatory
- No valid key-set in MS
- 3G location services
- OSA
- MAP security
- Enhanced user identity confidentiality (EUIC)

- SP-99622 was not broadly accepted by all WGs

T-Mobil

Status of open R99 security issues (2)

- Authentication failure indicator
  - Necessary CRs are agreed on by N2
- Network-wide encryption
  - Hooks and extensions to be verified
- Encryption not mandatory
  - S3 intends to use same procedure as proposed for GPRS (contained in SP-000121 - *for information*)
- No valid key-set in MS - resolved
- 3G location services - same as for GSM
- OSA - no work performed

Status of open R99 security issues (3) MAP security

- SP-000111: LS on MAP Security - *for information*
  - 2G CN security has long been identified as a problem area which must be tackled in 3G
  - Short to medium term solution is required to address the very real threats that exist in today's signalling networks
  - It is necessary that 3GPP provides a solution in R99; no time to wait for IP
  - For those who doubt the severity of the attacks, demonstrations could be provided

Status of open R99 security issues (4) MAP security

- SP-000043: LS on MAP Security Status Report
  - Layer I (inter PLMN key transport mechanism)
    a) No standardisation for R'99
  - Layer II (intra PLMN key transport mechanism)
    a) Identification of suitable transport mechanisms
    b) Specification of PLMN internal O&M interfaces
    c) Liaison with S5 has been established
  - Layer III (MAP level)
    a) Most open issues have been resolved
    b) Work has been progressed by N2(B)
    c) N2 CRs specifying secure MAP messages withdrawn
    d) Agreed N2(B) work assumption is based on a more generic approach

Status of open R99 security issues (5) MAP security

- Layer II work can be completed by N2/S3 until SA#8
- Layer III work can be completed by S5/S3 until SA#8

- S3 requests an extension until SA#8 to complete work on MAP security

Status of open R99 security issues (6) EUIC

- SP-000006: LS concerning EUIC Status
  - Scope of feature
    - Registration/call set-up by encrypted IMSI (EMSI)
    - Paging by temporary encrypted IMSI (TEMSI) in case TMSI is lost
  - Attacks prevented
    - Active IMSI catching attacks
    - Eavesdropping (cleartext) IMSI paging messages
    - Active IMSI paging attacks
      (but not other identity probing attacks)

Status of open R99 security issues (7) EUIC

- Impact on all networks
  - Transport and storage of EMSIs and TEMSIs, especially in VLR/SGSN
- Work was progressed and more than 12 CRs have been prepared to accommodate the feature in N1, N2, R2, S2, S3, T3
- Unresolved issues
  - R2: Transport of XEMSI during initial access
  - N2: How to proceed in case TEMSI is lost by VLR/SGSN

Status of open R99 security issues (8) EUIC

- Extensions to cover IMSI paging are not completely supported by S3
- One objection to the agreement of CRs recorded (S3#11)
- Conclusion
  - Based on this information, a decision is needed on how to proceed further with EUIC
  - S3 proposes the following three options
    - The feature is included in R'99
    - The feature is included in R'99, but optional for ME
    - The feature is included in R'00
- Problems will occur due to the requirement of backward compatibility. This may prevent introduction in future releases.

T-Mobil

Review of S3's completion of R99 (AI 5.3.2)

- Status of S3 deliverables
- Integration of security features into R99 specifications

Status of S3 deliverables (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

Status of S3 deliverables (2)

- 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
  - CRs at SA#7
  - Main work has focused on
    - Open R99 security issues
    - Cipher/integrity/authentication mechanisms
    - Handling of authentication vectors
    - Interoperation scenarios
    - Conversion functions

Status of S3 deliverables (3)

- TS 33.102: Security architecture
  - Remaining issues
    - Terminology not in-line with other 3G specifications
    - Due to export restrictions there may be a need to allow weaker ciphering (effective key length shorter than 128 bit)
      - By shortening and extension functions
      - Further treatment at S3#12
    - Assignment of algorithm ID and existing algorithms
    - Clarifications to visibility and configurability

Status of S3 deliverables (4)

- TS 33.103: Integration guidelines
  - Approved at SA#5; 3 CRs approved at SA#6
  - CRs at SA#7
    - Alignment of TS 33.103 and 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
  - CRs at SA#7
    - Alignment of 33.105 with 33.102
      Clarification on cipher keys shorter than 128 bit

Status of S3 deliverables (5)

- TS33.106: Lawful interception requirements
  - Approved at TSG-SA#4; 1 CR approved at SA#6
  - Stable
- TS33.107: Lawful interception architecture and functions
  - Approved at SA#6
  - Stable

Status of S3 deliverables (6)

- TR33.900: Guide to 3G security
  - Approval at SA#7 planned
  - Postponed until SA#8
- TR33.901: Criteria for cryptographic algorithm design process
  - Approved at SA#4
  - Stable

Status of S3 deliverables (7)

- TR33.902: 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
  - Some editorial changes are necessary
  - Editor still required

Integration of security into R99 specifications

- Need to ensure that S3 security features are properly integrated into the R99 specifications
- S3 has started to identify affected specifications on
  - Authentication and key agreement
  - Confidentiality and integrity protection
  - Secure 2G-3G interworking
  - others areas may follow
- S3 is identifying where corrective CRs are required with assistance of other WGs

Approval of contributions from S3 (AI 5.3.3)

- CRs to TS 33.102
- CRs to TS 33.103
- CRs to TS 33.105
- CRs on EUIC

T-Mobil

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

- SP-000112: Miscellaneous CRs to TS 33.102 (revision of SP-000046)
  - CR043: Clarification that cipher/integrity keys should be deleted when their lifetime expires
  - CR044: Various clarifications on the use of the integrity mechanism to provide local authentication
  - CR048: Clarification that 3G authentication vectors cannot be re-used
  - CR049: Correction that home environment does not need to acknowledge reception of authentication failure report

T-Mobil

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

- CR050: Correction that the UE rather than the USIM shall trigger an authentication and key agreement when the cipher/integrity key lifetime has expired
- CR051: Clarification that the USIM contains a conversion function c3 for deriving the GSM cipher key from the 3G cipher/integrity keys
- CR052: Clarification that authentication failure reporting shall be initiated after an authentication failure in the serving network

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

- CR053: Correction that the plaintext IMSI rather then the encrypted IMSI is sent in the authentication data request procedure between serving network and home environment
- CR054: Clarification on GSM/3G interoperation scope
- CR055: Clarification that the generation of sequence numbers in the home environment does not have to safeguard user identity and location confidentiality
- CR056: Clarification that mechanisms and procedures for allocation and use of TMSI and P-TMSI are described in GSM 03.20 and 3G TS 23.060

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

- CR057: Editorial clarifications on cipher/integrity key setting
- CR058: Clarification that since a common RNC connection is used, simultaneous PS and CS connections must have common cipher/integrity preferences
- CR059: Clarification on the application of integrity protection, including exceptions when it is not mandatory to start integrity

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

- CR061: Functional modification to integrity mechanism to remove the requirement to trigger an authentication and key agreement when integrity check failures in UTRAN
- CR063: Clarification that the hyperframe number should be reset when new cipher/integrity keys are established
- CR071: Since integrity protection is mandatory a default key is used for emergency calls when no valid USIM is available or if authentication fails
- CR72: Clarification that ciphering is continued at intersystem handover and that integrity protection is started at handover from GSM BSS to UTRAN

CRs to TS 33.102 - *for approval (6)*

- CR74: Clarification that a mechanism to protect the cipher/integrity keys on the Iu interface is not provided
- CR76: Correction/enhancement of the cipher/integrity key lifetime control mechanism so that an authentication and key agreement can be triggered by the UE during a connection
- CR77: Clarification that an authentication can be performed during both CS and PS connections and that the new keys can be taken into use during the security mode procedure that follows authentication

CRs to TS 33.102 - *for approval (7)*

- CR79: A periodic local authentication procedure is added to guard against the stealing of capacity from the network

CRs to TS 33.102 - *for approval (8)*

- SP-000077: Miscellaneous CRs to TS 33.102
  - CR047: Interoperation scenarios between 3G and GSM are specified in more detail and clarifications are made
  - CR064: Conditions for distributing authentication vectors and security context data between serving network nodes are specified in detail
  - CR066: The ciphering mechanism is specified in more detail using descriptions from 33.105 and 25.301
  - CR067: The integrity mechanism is specified in more detail

CRs to TS 33.102 - *for approval (9)*

- SP-000044: CR on MAP Security
  - CR073: Further specification of the structure of the encrypted MAP messages is added

CRs to TS 33.103 - *for approval*

- SP-000047: Alignment of the integration guidelines (TS 33.103) with the security architecture (TS 33.102)

CRs to TS 33.105 - *for approval*

- SP-000048: Miscellaneous CRs to TS 33.105
  - CR006: Alignment of the authentication algorithm requirements specification with the security architecture
  - CR007: Alignment of the enhanced user identity confidentiality algorithm requirements specification with the security architecture
  - CR009: Correction that if the effective cipher key length is less that 128 bits then the effective key shall be repeated when forming a 128 bit CK data structure
  - CR010: Correction that integrity keys shorter than 128 bits are not allowed

CRs on EUIC - *for approval*

- SP-000075: Miscellaneous CRs on EUIC (revision of SP-000045)
  - CR33.102-045: Clarifications to the mechanism, addition of a new temporary identity for paging, addition of new procedures for requesting the last temporary identity for paging in the case that data is not available in the serving network (e.g. due to database failure)
  - CR33.103-005: Clarifications to the integration guidelines plus alignment of the integration guidelines with CR33.102-045
  - CR33.105-008: Clarifications to the algorithm requirements