3GPP TSG SA WG3 Security — S3#12 **S3-00231**

11-14 April, 2000

Stockholm, Sweden

Source: **SA WG3 Chairman**

Title: **SA WG3 "To-do list" for meeting #12**

Document for: **Discussion/Action**

Agenda Item:

point out from SA#7

- SP-000042, S3 status report to SA#7
- SP-000092, LS from SA2 to SA (cc CN, T, RAN) on EUIC (S2-000587)
- SP-000108, Proposal for the Release 2000 IGCs, Features, Building Blocks and Work Tasks v.0.7
- SP-000118, Work plan for the design of the 3GPP Authentication Algorithm (MCC Task Force)
- SP-000131, Status of Ciphering and Integrity Algorithm distribution
- SP-000156, LS from SA to GSMA, GSMA SG on 3G Authentication Algorithm
- SP-000169, Open Issues for Release 99 List

SMG10 (2G part)

1. GPRS encryption case:
   Check if S3-000156 was updated in SP-000060 as approved during S3#11?
   This wasn't the case because S1 CRs could not be updated from S3. This needs further treatment.
   Liaison from and with N1 (S3-000219). N1 sees the need for a separate new WI.
   Presentation at SMG#31bis
2. Attacks on A5/1
3. Design A5/3, requirement specification approval, funding
4. Design new A3/A8 (combined with 3GPP authentication algorithm)
5. 64 bit Kc
6. 96 bit Kc (WI on studying the impact on running GSM systems)

S3 (3G part)

7. Non technical issues but important
   - Agreement with TIA TR-45 AHAG on a common agenda for the joint session during S3#12
   - Clear view on the 3GPP requirements on the procedures to allow joint control of the 3GPP AKA specifications
8. Content and schedule of R00 security work (R00 security features)
9. Approval of 3G security guidelines
10. Integration of security into R99 specifications: identifying where corrective CRs are required
    - Authentication and key agreement, Confidentiality and integrity protection, Secure 2G-3G interworking, others?
11. Clarification of the clean-up procedure of specifications under control of S3
    (including use of abbreviations: US, ME, terminal; definition of what is meant by R98- and R99+, define what is R99 ME: GSM-only/GSM-UMTS-dual-mode/UMTS-only)
12. EUIC postponed to R00: review concept, review possibility of introduction in GSM, liaison with RAN needed on explanation of EUIC

13. MAP postponed to R00
    Co-ordination of further work on MAP security layer I + II, decision between S5 and N2 needed; assist in layer III work; review/new proposal for layer I + II (elaborate on IKE?); assist in layer I + II work
    LS to TC security on use of BEANO for MAP security
14. N/w encryption - further work required for R00
15. CRs are needed to remove MAP security, EUIC from the appropriate parts from R99 specs (v3.x.x) under S3 control?
16. CRs are needed to add MAP security, EUIC to the appropriate parts of R00 specs (v4.x.x) under S3 control?
17. Authentication failure notification: MS behaviour on authentication failure is still open; LS with N1
18. Integrity protection of emergency calls, LS with N1 is needed on that issue (33.102CR071)
19. Re-authentication during connection (N1), LS with N1 (response in S3-000218)
20. Standarized 3GPP authentication algorithm
    Clarification of funding (as soon as possible together with GSMA SG)
    LS to GSMA on funding of UMTS authentication algorithm (to avoid duplication of work) - was SP-000156 approved by SA?
21. Weaker encryption case
22. Conversion functions: design of c3 (S3-000207-33102-331-CR078), task on Siemens/Ericsson to clarify requirements
23. HE control over accepting non-ciphered connections (S3-000195)
24. Requirements in case of encryption not allowed: Check the status of cipher indicator, configurability as proposed by discussion paper on GPRS encryption (S3-000205)
25. Refinement of features on visibility and configurability (S3-000041CR042)
26. Iu-interface security
27. Profile of IPsec for GTP security
28. Clarification on the security mode set-up message (S3-000120CR060)
29. CR on 23.060 on notification of authentication failure to home environment needed
30. Finalisation of which messages are integrity protected (R2)
    Integration of integrity protection in UTRAN: Work completed in RAN2? (There is a problem applying integrity protection to all messages since some are very small and the overhead of adding a MAC and synchronisation information to each message is very significant.)
31. Provision of integrity protected handover complete Ack (R2)
32. Protection overhead for AMR information and other small messages (R2)
33. Cipher/integrity key handling in non-anchor MSC
34. S3 tdocs from S3#11 to be handled at S3#12:
    - S3-000127: CR065 to 33.102: Authentication and key agreement. (Rewrites section 6.3 for better presentation.)
    - S3-000130: CR068 to 33.102: Interoperation and intersystem handover/change between UTRAN and GSM BSS. (Does not fulfil S1 requirements. Is it superseded by S3-000208?)
    - S3-000131: CR069 to 33.102: Local authentication and connection establishment. (Re-writes section 6.4, but does not take into account approved CRs.)
    - S3-000132: CR070 to 33.102: User identity confidentiality. (Re-writes section 6.1 and 6.2, but does not take into account CR065 and TD S3-000197.)
    - S3-000164: LS from SMG9 to SA WG3 on new SIM toolkit feature: 'Auto-answer & Mute-ringing'
    - S3-000165: Response to T3-99-432, “LS on 'Clarification of the information storage in USIM'
35. Remaining work on LCS security?
36. Remaining work on OSA security?
37. Joint meetings/sessions with other TSG WGs (at least N1 and N4, R2/R3?)
    - to solve existing problems
    - agree on R00 work packages

TDs to handle:

- S2-000589 (= N4-000021)
- S3-000217 (= S5-000154 = N4-000023)