3GPP TSG SA WG3 Security — S3#10 **S3-000022**

19-21 January, 2000

Antwerpen, Belgium

Source: **Secretary**

Title: Report of TSG SA WG3 Meeting #9 - draft

Document for: **Approval**

Agenda Item:

3GPP TSG SA WG3 draft **S3-99xxx**

Meeting #9, Helsinki, 7-9 December, 1999

Source: **Secretary TSG SA WG3 (Ansgar Bergmann)**

Title: **Report of TSG SA WG3 Meeting #9 - draft**

Table of contents

1 Opening of the meeting; general

The meeting was chaired by S3 Vice Chairman Michael Markovici who thanked Nokia for hosting the group.

2 Approval of the Agenda

The agenda in S3-99500 was approved:

1 Opening of the meeting
2 Approval of the agenda
3 Registration and assignment of input documents
4 Approval of meeting reports
4.1 TSG-SA3 Meeting no. 8 (joint with SMG10)
5 Reports / Liaisons from other 3GPP and SMG groups
5.1 TSG-SA plenary
5.2 TSG-CN, TSG-RAN, TSG-T and WGs
5.3 SMG plenary
5.4 SMG STCs
5.5 3GPP partners and their bodies
5.6 Others (GSMA, GSM2000, T1P1, SAGE, TIA TR-45, etc.)
6 2G security issues
6.1 GPRS
7 Review 3G security project plan
8 3G security issues
8.1 Confidentiality/integrity algorithm
8.2 Authentication algorithm
8.3 Terminal security
8.4 GLR security
8.5 Presentation from TSG-S2 on mobile IP
9 Review of CRs to 3G TS 33.102, Security architecture
10 Review of CRs to 3G TS 33.103, Integration guidelines
11 Review of CRs to other 3G specifications
11.1 TS 33.106, Lawful interception requirements
11.2 TS 21.133, Security threats and requirements
11.3 TR 33.902, Formal analysis of security mechanisms
11.4 TS 33.105, Cryptographic algorithm requirements
11.5 TS 33.120, Security principles and objectives
11.6 TR 33.901, Criteria for cryptographic algorithm design process
12 Review of draft 3G specifications
12.1 TS 33.107, Lawful interception architecture
12.2 TR 33.900, Guide to 3G security
12.3 TS 33.048, Security mechanisms for the USIM application toolkit
13 Update 3G security project plan
14 Any other business
15 Approval of liaison statements, CRs and draft specifications
16 Future meetings dates and venues
17 Close of meeting

3 Registration of input documents and assignment of input documents to agenda items

See Annex A.

4 Approval of meeting reports

5 Reports / Liaisons from other 3GPP and SMG groups

5.1 TSG-SA plenary and WGs

S2-99E05, LS from S2:

✏ **CB to draft an answer.**

5.2 TSG-CN, TSG-RAN, TSG-T and WGs

T2-991036, a LS from T2 on MExE: postponed to next meeting.

T2-991082: Noted

5.3 SMG plenary

SMG#30bis did not work on S3/SMG10 related issues.

5.4 SMG STCs

No input received;

5.5 3GPP partners and their bodies

No input received.

5.6 Others (GSMA, GSM2000, T1P1, SAGE, TIA TR-45, etc.)

Neither GSMA not GSM2000 had a meeting between S3#8 and S3#9.

No information was received from T1P1 or SAGE.

Bart Vinck reported on TR-54 activities. See LS in S3-99xxx (to be provided by PH, draft is available).

✏ **CB to draft an answer.**

6 2G security issues

6.1 GPRS

Mike Walker has sent a letter to ETSI DG explaining that manufacturers had difficulties to get GEA2. Lucent reported at S3#9 that they still have not yet received the algorithm.

7 Review of 3G security project plan

See section 13.

8 3G security issues

8.1 Confidentiality/integrity algorithm

No input received.

8.2 Authentication algorithm

S3-99509 presents the cipher algorithm Shazam, which has been approved by TIA TR-45.AHAG. This document is presented to TSG SA WG#3 for information and consideration as a potential 3GPP and/or GPRS Block Cipher algorithm.

The document was noted.

S3-99523, source Vodafone, discusses authentication algorithm requirements. Preference is given to ask SAGE to specify a single algorithm with exchangeable building blocks rather than to ask SAGE to work out a framework and building blocks.

✎ **S3-99524 on the same issue, S3-99xxx to be prepared by PH.**

8.3 Terminal security

8.4 GLR security review

8.5 Presentation from S2 on mobile IP

The presentation in S3-99495 was given by Anders Hansmats. 3G 23.923 V1.2.0 was available as S3-99494.

9 Review of CRs to TS 3G 33.102

501, 503, 504: 504 gives a justification to the CRs on sequence numbering in 501 and 503, which affect to section 6.3 and annex F.

S3-99462, *Preliminary analysis on how to implement an authentication failure report mechanism,* source: Telenor, was presented by Geir Køien. This document proposes to introduce an authentication failure report from VLR to HLR and from SGSN to HLR in R99. The proposed mechanism uses a new MAP operation MAP_AUTHENTICATION_FAILURE_REPORT on the Gr and D-interface.

Clarifications at S3#9:

- Peter Howard reported that, as the last N2 of 1999 has already been held, a decision to include this feature, and also MAP security, in R99 would have to be taken by CN next week.
- It was reported that a similar feature is contained in 3GPP2.

The document raises some points for decision. Agreement in S3#9:

- Concerning the first point raised for decision, whether the feature should become a R99 feature, it was agreed that a LS and a CR should be written under the working assumption that the feature becomes a R99 feature.
- Concerning the second point raised for decision, whether to specify a minimum or a further going solution, it was clarified that a decision is not necessary, as the feature would allow implementation of further reactions of SN and HN.
- Concerning the third point raised for decision, whether the feature should be mandatory in a new MAP version, still networks would be able not to apply it.
- Concerning the forth point raised for decision, whether it is appropriate to implement the feature for GSM/GPRS specifications pre-dating UMTS, it was concluded to be unacceptable to add the feature to R98 or earlier releases.

✎ **Geir Køien to create corresponding CRs to the S3 specifications and a LS to CN2.**

512: this CR was approved.

516, and 501: 516 requests deletion of old AVs when a user leaves and then re-enters a VLR/SGSN. 501 just requests that any AV is only used once. Both proponents agree that a VLR/SGSN doesn't have to delete unused AVs after a location cancellation, but may keep them for some time, provided that there are mechanisms to guarantee that AVs are not too old. If these mechanisms are home environment specific, there is a risk of unnecessary conflict situations in the roaming case. It was concluded that the change of section 6.3.3 (last ttwo paragraphs on top of 6.3.3.1) is preferable to the change in 516; that 516 also corrects occurrences of "VLR" to become "VLR/SGSN".

513 and 501: There was a debate on the degree of specification and the requirements to be raised. It was agreed that it should be avoided that the serving network often tries to use an AV which is considered out of range by HE and USIM. On the other hand, it was agreed that to specify a certain generation method does not help to fulfil that requirement. What would be necessary would be a way for the SN to judge whether AVs are probably out of range.

✎ **Conclusion: 516 was withdrawn; there will be a revision of 501.**

517: This CR to 33.102 proposes to correct figure 14. It was recognized that a correction is needed; however, it should identify the parameters sent to the UMTS RAN / GSM BSS and the parameters sent to the mobile station MM sublayer.

✎ **To create a CR identifying in figure 14 the parameters sent to the UMTS RAN / GSM BSS and the parameters sent to the mobile station MM sub-layer.**

CR in 33.102 on UIA and UEA identifications:

- There should be means to negotiate "no encryption" between network and mobile.

- For certain MM and CM messages, integrity protection might not be applicable (emergency calls). This would probably be possible by the network not setting integrity protection or by using a specific "null" key.

There was a discussion whether ciphering should be mandatory if a USIM is provided; the dangers of non-ciphered packet sessions is even higher that for circuit oriented connections.

✎ **Input on security handling of USIM-less emergency calls is requested. Also whether ciphering should b mandatory in all other cases.**

It was questioned whether 33.102 should specify 4 bit identifiers for integrity and encryption algorithms at all.

➢ **Still, the CR in s3-99520 was accepted, however further contributions on the matter are possible.**

➢ **538, rev. of 503: This CR 33.102-036 impacting Annex F, Example uses of AMF, was approved.**

➢ **539, revising 531 and 502, CR 33.102-036: This CR, rewriting annex C of 33.102, was approved.**

540 (revising 532, which revised 501 and 513) is CR 33.102-037: This CR includes requirements on sequence number handling, removes description of any particular method of sequence number handling, improves efficiency of the re-synchronisation procedure, and corrects the notation.

✎ **This CR 33.102-037 in 540 has to be dealt with further.**

➢ **541, revising 421, CR 33.102-026r1, on Mobile IP security: Agreed.**

➢ **542, CR 33.102-031 on Removal of alternative authentication mechanism described in annex D: This CR was agreed with the exception of Lucent.**

Lucent gave the following statement:

begin quotation

> Lucent objects to the removal, at this time, of the 3G TS 33.102 Annex D “A mechanism for authentication based on a temporary key (based on TETRA)”. The reason that this authentication method has been originally approved by SA WG3 as an alternate method is listed in Annex D section 3 (D.3) : “..Serious operational difficulties are discovered with the SQN protocol. Those are problems implementing the protocol that may be discovered during early development or testing. ..”.
>
> Although the SQN is expected to be an effective authentication architecture for the 3GPP systems, it is our position that it is prudent to maintain this option in Annex D, until the effectiveness of the SQN architecture can be proven via field testing. It should be noted that maintaining this optional TETRA based authentication method in the document does not effect in any way the implementation of the primary AKA architecture based on SQN.

end quotation.

S3-99409, CR 33.102-030, *Handling of the MS UEA and UIA capability information:* Approved.

➢ **549, revising 492, and 550, rev. of 493: The LS was agreed, the CR is postponed to S3#10.**

10 Review of CRs to TS 3G 33.103

There will be the need to changes corresponding to the changes agreed on 33.102, but they would be editorial and can wait until SA#7.

11 Review of CRs to other 3G specifications

11.1 TS 3G 33.106

507 is an updated CR to 33.106, updating S3-99284. The approved version is 3.0.0, so a CR should be created based on that version.

✐ **CR 33.106-001 in S3-99522 was approved.**

11.2 TS 3G 21.133

It was commented that this specification contains references to other no more existing specifications. It seems that the initial sections could be deleted, as they only collect material from other specifications.

✐ **Charles Brookson to lead a review group on 21.133.**

11.3 CRs to TR 3G 33.902

➢ **505: This CR to 33.902 was approved.**

11.4 TS 3G 33.105

No input received.

11.5 TR 3G 33.120

No input received. The document is stable.

11.6 TR 3G 33.901

No input received. The document is stable.

11.7 TS 3G 22.022

This specification had recently been transferred to S3. A rapporteur is missing.

12 Review of draft 3G specifications

12.1 TS 3G 33.107

✎ **33.107 in S3-99508 was approved to be presented to SA for approval.**

12.2 TR 3G 33.900

✎ **525: to be discussed in the group on 21.133.**

12.3 TS 3G 33.048

✎ **A version will be available during S3#9.**

10 Review of CRs to TS 3G 33.103

There will be the need to changes corresponding to the changes agreed on 33.102, but they would be editorial and can wait until SA#7.

11 Review of CRs to other 3G specifications

11.1 TS 3G 33.106

507 is an updated CR to 33.106, updating S3-99284. The approved version is 3.0.0, so a CR should be created based on that version.

✎ **BW to create CR 33.106-001 (S3-99522).**

11.2 TS 3G 21.133

It was commented that this specification contains references to other no more existing specifications. It seems that the initial sections could be deleted, as they only collect material from other specifications.

✎ **Charles Brookson to lead a review group on 21.133.**

11.3 CRs to TR 3G 33.902

➢ **505: This CR to 33.902 was approved.**

11.4 TS 3G 33.105

No input received.

11.5 TR 3G 33.120

No input received. The document is stable.

11.6 TR 3G 33.901

No input received. The document is stable.

11.7 TS 3G 22.022

This specification had recently been transferred to S3. A rapporteur is missing.

12 Review of draft 3G specifications

12.1 TS 3G 33.107

✐ 508: Assigned to a subgroup led by Berthold Wilhelm.

12.2 TR 3G 33.900

✐ 525: to be discussed in the group on 21.133.

12.3 TS 3G 33.048

✐ A version will be available during S3#9.

✐ The revision of LS to AHAG etc in 463 was approved.

13 Update 3G security project plan

14 Any other business

15 Approval of liaison statements, CRs and draft specifications

16 Future meetings dates and venues

Close of meeting