3GPP TSG SA WG3 Security — S3#12 **S3-000230**

11-14 April, 2000

Stockholm, Sweden

Source: SA WG3 Chairman
Title: Notes on S3 presentation at SA#7
Document for: Information
Agenda Item:

Notes on S3 presentation at SA#7

Documents for approval

All documents were approved as presented in SP-000042 with the exception of CR33.102-71 (SP-000122). This CR was discussed together with SP-000122: The argumentation was as follows: Know IK does not improve the level of security of the appropriate call; emergency call should be as robust as possible; therefore fail of integrity check shall not end in releasing the appropriate connection; this means that different handling of emergency calls and non-emergency call is needed; but this provides no advantage compared to not applying integrity protection to emergency calls. Liaison with N1 is needed on this issue.
S3 was asked to clarify the terminology of R98- and R99+ used in S3 specifications (CR33.102-054).

3GPP cipher and integrity protection algorithm

TSG SA formally approved the 3GPP cipher and integrity protection algorithm.
The general report from ETSI SAGE on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithm (SP-000049) was approved and will be published as 3GPP TR.
A status of algorithm distribution/publication was given (SP-000131). An initial solution of distribution via non-disclosure agreements was set up in order to allow the distribution to start from 20 March. This does not lessen the need to publish the algorithm as soon as possible.

Standardized 3GPP authentication algorithm

The need to have a standardized UMTS authentication algorithm was approved. It was also approved that ETSI SAGE will be the group to do the work. Funding cannot be confirmed. The fact that this will cause a delay was accepted.

Open R99 security issues

1. MAP security
The status of MAP security in R99 as detailed in our liaison was noted. CN confirms that they will be able to produce the relevant CRs for introduction of MAP security layer III until CN#8. MAP security layer II was discussed and it was questioned if SA5 is the appropriate group to do the work. CN delegates argued that MAP security layer I + II may better fit into the scope of N2. Both groups could not confirm that the work will be completed until CN#8/SA#8. MAP security was moved into R00 with a target date for approval of CRs (at least CRs related to layer III) as June 2000 in order to have it available as soon as possible.
CRs are needed to remove MAP security from R99 (specifications v3.x.x) and introduce it in R00 (specifications v4.x.x).

2. Enhanced user identity confidentiality
Following the suggestion of S2 in SP-000092, EUIC was moved to R00.
CRs are needed to remove EUIC from R99 (specifications v3.x.x) and introduce it in R00 (specifications v4.x.x).

3. Authentication failure notification
The part on MAP specifications is completed. MS behaviour on authentication failure is still open.
Authentication failure notification was allowed for late introduction in R99 if completed by CN#8/SA#8.

Stefan Pütz
T-Mobil
S3 vice chair

20th March 2000