3GPP TSG SA WG3 Security — S3#13 **S3-000354**

23-26 May, 2000

Yokohama, Japan

Source: **S3 vice chair (Stefan Pütz)** – compiled by Vodafone Airtouch

Title: **Report on SMG#31bis**

Document for: **Information**

Agenda Item: **7.2**

EMAIL REPORT TO SMG10

> > Dear SMG10
>
> >
>
> > Please find below some notes on the achievements of
>
> > presenting the SMG10 status report at SMG#31bis.
>
> >
>
> > Best regards,
>
> > Stefan Puetz
>
> > T-Mobil
>
> >
>
> > <P-00-223.zip, P-00-237.zip>
>
> >
>
> >
>
> >
>
> > - begin of text-
>
> > Presenting the SMG10 status report (P-00-223.zip) at
>
> > SMG#31bis I asked for three issues to be endorsed by SMG.
>
> > I received the following results.
>
> >
>
> > 1) 'Rejection of unciphered GPRS calls for R00 onwards'
>
> > Discussion and arguments at SMG#31bis: requirement not clear,
>
> > no need for whole feature, no need for asking
>
> > SMG#31bis for endorsement, achievable without

> > standardization, no impact on standards, therefore no need to
> > standardize, not
> > more than we already have today, ...
> >
> > SMG10 was asked to produce a WI description for presentation
> > at SMG#32 in accordance with SMG1, SMG2, SMG3,
> > SMG9 (and counterparts in 3GPP respectively).
> >
> >
> > 2) 'GEA 2 mandatory in terminals and SGSN for R99 but not
> > before the end of 2002; optional for R98'
> > GPRS R98 does not really exist. The main releases are R97 and
> > R99. It will be very hard to justify changes
> > against R98.
> > SMG#31bis recognizes the need of an early implementation of
> > GEA2 algorithm in both terminals and networks.
> > GEA2 and negotiation capability mandatory from R99 onwards
> > and for equipment <type approved> after December
> > 31st 2002, if backward compatibility with releases prior to
> > R99 can be assured. Otherwise introduction in
> > releases prior to R99 will be ffs. Support optional for
> > network equipment, i.e. SGSN (because on the network
> > side anything is optional(?). See document drafted during
> > SMG#31bis (P-00-237, prepared from hand-written
> > slide).
> >
> >
> > 3) 'A5/3 ciphering algorithm requirements specification'
> > This issue was not directly related to the SMG#31bis agenda
> > item 4 'GPRS encryption' but was allowed for
> > presentation.
> > The intention was to present the document for approval. A
> > discussion raises on legal issues in the sections on
> > ownership and export control. An updated version shall be

> > presented for approval at SMG#32.

> >

> > SMG10 to separate technical and legal issues into two

> > documents; sections on ownership and export control will

> > only be supported if export situation is clarified and no

> > problems are to be expected (especially on supported

> > key length).

> > -end of text-

➢ >

EXTRACT FROM DRAFT SMG#31BIS REPORT WITH COMMENTS

3 SMG10 MATTERS

Stefan Pütz, vice chair 3GPP TSG-SA WG3, presented the SMG10 status report to SMG#31bis in ~~P00~~P-00-223 on behalf of the SMG10 Chairman Mike Walker, who was not able to attend the meeting.

3.1 MANDATORY PROVISION OF GPRS ENCRYPTION

SMG10 had proposed to SMG#31 to make ciphering mandatory for GPRS. At SMG#31, several companies had asked to send the CRs back to SMG10 for further review, also to present them at TSG CN WG1 and to present the results of SMG10 to SMG#31bis. This had been agreed by SMG#31.

Problems and reasons that had been mentioned by delegates in SMG#31 (cf. SMG#31 meeting report):

- possible compatibility problems;
- if the CR is approved as such it could prohibit free circulation of mobiles;
- consequences for specifications like 04.08 might have to be elaborated;
- possible contradictions to 02.09;
- possible contradictions of national regulation in some countries;
- possibilities of other solutions.

SMG10 had discussed the issue further and concluded that there are practical problems making encryption mandatory for GPRS connections. For R97/R98/R99 SMG10 is satisfied with the support of mandatory ciphering indicator in GPRS terminals in accordance with GSM 02.09/03.20 and 3G 22.101/33.102. For R00 ~~Instead~~ SMG10 proposed to SMG#31bis the following mechanism known as rejection of unciphered calls:

- by default, all terminals to reject non ciphered connections;

- the user to be given the possibility to accept non ciphered connections by changing a setting in the MS, either in the SIM or the ME. SMG10 suggests that both the SIM and the ME contains a parameter to accept or reject non ciphered connections, and that the SIM parameter, if present, shall override the ME parameter.

Decision of SMG#31bis:

- P-00-224, LS on GPRS ciphering, and P-00-225, LS on Introduction of rejection of non ciphered calls for GPRS, were noted by SMG#31bis.
- SMG10 is asked to prepare a work item description for enhanced aplicability of GPRS ciphering and a corresponding requirement description; these documents should be made available as soon as possible to the relevant groups, and also to SMG#32.

A work shop on GPRS ciphering will be convened on xxx add information when and where xxx.

Presence of a ciphering indicator: TSG SA WG3/SMG10 had drawn to the attention of CN1/SMG3 that GSM 02.09 mandates the presence of a ciphering indicator in the ME, and that GSM 03.20 mandates that, when a ciphered connection is established, non-ciphered frames are discarded by the ME and that, once a ciphered connection is established, it is not acceptable to the ME to turn it off. See P-00-224.

3.2 GEA II

~~xxx Add some information. xxx~~

SMG10 recommends that GEA 2 algorithm is deployed in GPRS systems as soon as possible in accordance with the following time scale.

- Mandatory in terminals and SGSN for R99 but not before the end of 2002.
- Optional for R98.

SMG sees the benefits of an early implementation of GEA2 algorithm in both terminals and networks.

- It is suggested that support of GEA2 and an appropriate negotiation mechanism be made mandatory "for all new R99 MEs <type approved> after december 2002".
- The negotiation mechanism shall be backward compatible with releases prior to R99. If it is not possible to make a backward compatible negotiation mechanism, the possibility of including it in earlier releases should be studied.
- Support of GEA2 in the network, i.e. SGSN, should be optional.
- The support of negotiation mechanism shall be mandatory in the network.

Decision of SMG#31bis:

- P-00-~~xxx~~ 237 was approved with the understanding that retrofitting of mobile stations already on the market based on the existing releases will not be required.

Support for multiple GPRS ciphering algorithms in GSM 04.08/TS 24.008: SA3/SMG10 had reviewed GSM 04.08/TS 24.008 and has found that the ME does not have the ability to

signal to the SGSN information about its GPRS ciphering capabilities other than whether it supports GEA/1. SMG10 request the ME to have the ability to signal its capabilities on 7 GPRS ciphering algorithms and suggests that the MS network capability information element be extended by a second octet and that part of the additional bits are used to indicate the capability to support GEA/2, …, GEA/7.

3.3 A5/3

P-00-226, LS on A5/3 (S3-000307) and P-00-227: *A5/3 requirement specification*, were noted by SGM#31bis.

Comments at SMG#31bis:

- The ownership of A5/3 might be subject to discussion in other fora.
- A separation of technical aspects from legal and ownership matters seems necessary.
- ~~LS from SMG2 WPA on possible double ciphering: SMG10 saw no problem, an answer will be sent from SMG10 to SMG2 WPA (something with CS2).~~
- SMG10/S3 might envisage to study a wider application of A5/3, e.g. for 3G.
- Treated for information, revised version of P-00-227 should be presented for approval at SMG#32.