3GPP TSG SA WG3 Security — S3#14 **S3-000440**

2-4 August, 2000

Oslo, Norway

3GPP TSG_CN **Tdoc NP-000366**
Plenary Meeting #8, Dusseldorf, Germany
21st – 23rd June 2000.

Source: **TSG CN**

Title: Proposed LS on Support of additional GPRS ciphering algorithms

To: **TSG S3, TSG N4**

Copy: **TSG N1, TSG SA**

Agenda item: **6.3**

Document for: **APPROVAL**

TSG CN has considered incoming LS from TSG N1 (Tdoc = NP-000213) related to the support of additional GPRS ciphering algorithms. The outcome in TSG CN is presented here.

TSG CN would like to inform TSG S3 that the TSG CN Plenary#8 has agreed a CR to TS 24.008 for R99, which can be in found Tdoc NP-000267. With this change, the R99 MS has ability to signal its capabilities on 7 GPRS ciphering algorithms (GEA1, GEA 2, GEA3 etc.) to the network in the "MS Network Capability" IE which has been extended for R99. TSG CN notes that the support for GEA/2 is mandatory for Release 99 from the end of 2002 onwards.

TSG CN would like to inform TSG S3 that the TSG CN Plenary#8 has decided not to approve the changes to TS 04.08 for GPRS release R98 and R97, which can be found in Tdoc NP-000303 and NP-000392. This would have led to functional enhancements to GPRS R98 and R97. TSG CN state that GPRS R98 and R97 releases are frozen and agreed guidelines exist for modifications to these releases (see attached NP99361).

TSG CN also agreed that the GPRS R98 and R97 releases should be kept consistent.

TSG CN note that GPRS ciphering information is also carried on GTP protocol on the Gn interface. TSG N4 is requested consider the agreed R99 CR to TS 24.008 and to support the capability requested by TSG S3 when developing any enhancements that may be necessary to R99 GTP protocol to support these capabilities. TSG N4 is requested that any enhancements to R99 be developed in a backwards compatible way to earlier GPRS releases.

3GPP TSG_CN
Plenary Meeting #8, Düsseldorf, Germany
21st – 23rd June 2000.

Tdoc NP-000213

Source: **TSG_N1**

Title: **LS on "GPRS ciphering "**

Agenda item: **4.1**

Document for: **INFORMATION**

3GPP TSG-CN-WG1, Meeting #12
Hawaii, USA, 22-26 May 2000

Tdoc N1-000806
Rev Tdoc N1-000799
Rev of N1-000778

To: TSG-S3, TSG CN
cc: SMG, TSG N4
Source: TSG-N1
Title: Reply to LS on "GPRS ciphering "
Date: 2000-05-26

Support for multiple GPRS ciphering algorithms in GSM 04.08/TS 24.008

N1 thanks S3 for their LS on "GPRS ciphering" in Tdoc S3-000690. From this document, TSG N1 note the following:

> **"Support for multiple GPRS ciphering algorithms in GSM 04.08/TS 24.008**
>
> "SA3/SMG10 has 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. **The ME must have the ability to signal its capabilities on 7 GPRS ciphering algorithms.** SA3/SMG10 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. SA3/SMG10/SMG10 believes changes should be carried out at least starting **from Release 98**, as we propose – and hope to be endorsed – that support for GEA/2 is optional in Release 98 and mandatory for Release 99 from end of 2002 onwards.
>
> *We urge CN1/SMG3 to resolve this issue. "*

N1 has discussed the topic "Support for multiple GPRS ciphering algorithms in GSM 04.08/TS 24.008".

N1 #12 has agreed TS 24.008 R99 which can be found attached to this LS. With this change, the Rel 99 MS has ability to signal its capabilities on 7 GPRS ciphering algorithms to the network in the "MS Network Capability" IE which has been extended R99. TSG N1 also has prepared the corresponding change to Rel 98, but would like to have this issue raised at the TSG CN plenary level to the address the issues raised by these functional changes to GPRS.

TSG N1 has concerns in introducing new functional requirements to GPRS Rel 98 at this late stage. TSG N1 note that GPRS ciphering information is also carried on GTP protocol on the Gn interface, and the impact of this to roaming needs to be considered by GTP experts (TSG N4) as this CR introduces inconsistencies between the TS 24.008 Rel 98 and GTP protocols in Rel 97/98. TSG N1 would like to highlight that this proposed enhancements introduces inconsistencies between GPRS Rel 97 and GPRS Rel 98. TSG N1 has concerns that this may complicate interworking

TSG S3 is requested to consider whether it would be acceptable to have these new functional enhancement to GPRS from Rel 99 onwards and not GPRS Rel 98, considering that the support is mandatory from December 2002.

3GPP TSG_CN#5 **NP-99361**
Meeting #5, Kyongju, Korea,
06-08 October 1999

Source: TSG-CN

Title: Liaison statement on freezing GSM Release 97 & Release 98

To: TSG-RAN, TSG-SA, TSG-T

cc: SMG, TSG-N WG1, TSG-N WG2

Introduction

TSG-N have noted the concern of TSG-N WG1 and TSG-WG2 that the number of change requests against GSM specifications (especially CAMEL and GPRS) for Release 97 & Release 98 is so high that implementers do not have a stable base for their work. We have to accept that after SMG#30 it will not be acceptable to change GSM Release 98 or earlier releases except to deal with serious technical errors.

Acceptable categories of change

TSG-N believe that only the following categories of change should be accepted:

(C1) Essential corrections, i.e. where a frequently occurring successful or unsuccessful case is not handled properly because there is some (as yet undetected) error or significant ambiguity in the specifications;

NB: C1 applies only to cases which are likely to occur frequently. It is too late to correct errors which occur only infrequently.

(C2) Corrections to incorrect implementation of earlier CRs or to the effect of two or more conflicting CRs;

(C3) Other CRs where the CR is actively supported by all relevant manufacturing companies.

A relevant manufacturing company is a company which manufactures equipment (network entities or mobile stations) which would be affected by the proposed change.

When a CR is presented for approval, the category into which it falls shall be identified. If this cannot be identified then the CR shall be automatically rejected.

If a change to Release 97 or earlier is accepted, it will in general be necessary to accept the corresponding CR(s) to later release(s).

Conclusion

TSG-RAN, TSG-SA & TSG-T are asked to apply the principles described above when they consider possible change requests to GSM Release 98 and earlier.