3GPP TSG SA WG3 Security — S3#26 **S3-020665**
19- 22 November 2002
Oxford, UK

3GPP TSG GERAN #12 **Tdoc GP-023213**
Sophia Antipolis, France **Agenda 6.2; 7.1.5.3**
18.-22. November 2002
Source: Nokia

ECSD and Ciphering

1. INTRODUCTION

Enhanced Circuit Switched Data (ECSD) was introduced as part of Release 99 specifications. A number of channel combinations were defined (ref. 05.02):

E-TCH/F + E-IACCH/F + E-FACCH/F + SACCH/TF
E-TCH/F + E-IACCH/F + E-FACCH/F + SACCH/M
E-TCH/F + E-IACCH/F + SACCH/M
E-TCH/FD + E-IACCH/F + SACCH/MD

Appropriately there was a need to modify the usage of A5 ciphering algorthim due to larger output blocks when using 8-PSK modulation (ref. 03.20v810 section C1.2):

"In the case of EDGE (Enhanced Data rate for GSM Evolution) the useful data are organized into longer blocks than 114 bits. According to GSM 05.03 the useful information in a block is included in 116 symbols which are numbered E(0) to E(115). Each symbol contains 3 bits, hence a block contains 348 useful information bits."

And further explanation is given in section C1.5 of 03.20:

"In EDGE the block size is greater than 114 bits. With EDGE a modification of the usage of the A5 algorithm is employed which produces BLOCK 1 and BLOCK2 which each contain 348 bits. The other parameters are not modified. The modified algorithm produces both blocks during a TDMA frame duration, i.e. 4.615 ms. The blocks are combined by bitwise modulo 2 addition with the plaintext data as explained in C.1.2."

In addition, a concept that would allow different modulations in different directions was specified enabling assymetrical channel combinations, for example TCH/F uplink and E-TCH/F downlink. And since this concept would allow different block sizes for up and downlink, the following was specified in 03.20 section C1.5:

"It is possible in EDGE that the plaintext data block for either uplink or downlink is shorter than 348 bits. In this case only the first part of the corresponding output parameter BLOCK is used in the bit-wise adition and the rest of the bits are discarded."

2. A POTENTIAL MISUNDERSTANDING FOR ECSD R99 IMPLEMENTATION

There seems to be two questions regarding the ciphering and ECSD:

1. In case of assymetrical configuration, what is the correct usage of A5 algorithm? To be more general, what is meant with “EDGE” in the quoted sections above?
2. What is the correct way to use the A5 for control channels associated to E-TCH channels? The control channels are GMSK modulated, therefore it could be unclear from the specification above on what is the right way of using the A5 algorithm.

On the first issue our opinion is that section C1.5 of 03.20 states that in case when the plaintext data block is shorter than 348 bits, then only the first part of the corresponding output parameter BLOCK is used, and the rest of the bits are discarded. Consequently our understanding of “EDGE” in the context of 03.20 is that it refers to channels that contain 8-PSK modulated channels in the assigned channel combination. For example in case when the assigned channel is asymmetrical then even for the GMSK modulated channels the output parameter BLOCK is 348 bits, and only the first part of the corresponding output is used and the rest of the bits are discarded.

On the second issues, based on the explanation above, it is logical to use the same principle for control channels. So in case when a data block corresponding to FACCH block would need to be cipered, then only first part of the output parameter BLOCK is used and the rest of the bits are discarded.

Nokia invites other companies to comment whether the specification is clear and if any CRs are needed.

3. ECSD AND A5/3

As described above, the specification of usage of A5 algorithm in ECSD Release 99 makes it possible to use the same ciphering module to derive the output parameter BLOCK for both GMSK and 8-PSK modulated channels. In case of ciphering of GMSK modulated channels the first part of the output is used and the rest is discarded.

3GPP is currently specifying new algorithm to be used for CS services in GSM, called A5/3. The GSM A5/3 algorithm produces two 114-bit keystream strings, one of which is used for uplink encryption/decryption and the other for downlink encryption/decryption (see figure 1). The EDGE A5/3 algorithm produces two 348-bit keystream strings, one of which is used for uplink encryption/decryption and the other for downlink encryption/decryption (see figure 2). Note that in the case of A5/3, the ciphering bit stream for the first 114 bits would be dependent on the mode (EDGE or GMSK) for both the uplink and the downlink.

It appears that the ciphering depends on the modulation used, since one of the constants used in the ciphering algorithm is different for “GSM mode” and “EDGE mode”! (From the SAGE’s A5/3 specification it appears that by “GSM mode” they mean GMSK channels, while by “EDGE mode” they mean 8-PSK). This principle will complicate the usage of ciphering in case of ECSD, since there would be a need to use in parallel two ciphering modules, one for each modulation. This is different from the way it has been specified for ECSD in R99 therefore answers to the following questions are needed:

1. In case of asymmetrical channels for ECSD, what would be the proper usage of A5/3?

2. In case of ECSD channels, what would be the proper usage of A5/3 for control channels using GMSK?

It appears that it is not possible to use “EDGE A5/3” algorithm for GMSK modulated channels, since there is a difference in the constant CA (see figures below). Our understanding is that the A5/3 mode would need to be changed whenever there is a change in modulation (i.e. signalling data over FACCH, or up and downlink asymmetry), and believe that this is an unnecessary complication. Therefore we would recommend to always use “EDGE A5/3” mode and abandon the “GSM A5/3” mode alltogether. This means that the algorithm would always produce two blocks of 348 bits, and in case of

GMSK only first part of 348 bits would be used and the rest of the bits is discarded. According to our understanding, there is not degradation in the security, since anyway the CA value could be known based on the detection of the modulation over the air interface, although this need to be confirmed by TSG SA WG3.

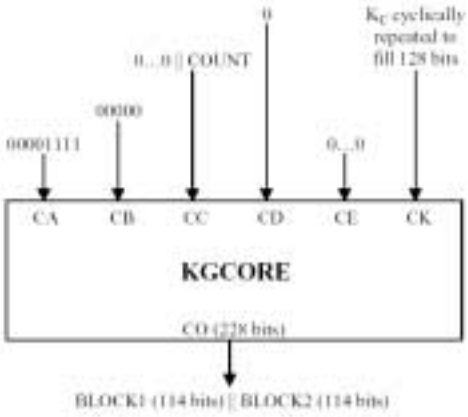

Figure 1. GSM A5/3 Keystream Generator Function

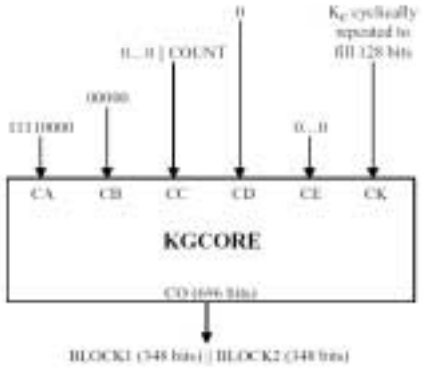

Figure 2. EDGE A5/3 Keystream Generator Function

4. CONCLUSION

This document presents two issues related to the ECSD and ciphering. The first one relates to the R99 specification where there seems to be a potential for misunderstanding. It is beneficial to get the feedback from TSG GERAN in order to decide whether a clarification CR is needed.

The second issue deals with the specification of new algorithm A5/3 and this document raises an issue with the usage of “GSM A5/3” and “EDGE A5/3” algorithms. Based on the understanding of the usage we believe that there is no need for GSM A5/3 and propose to abandon it altogether.