**3GPP TSG SA WG3 Security — S3#26** **S3-020693**
**19- 22 November 2002**
**Oxford, UK**

---

**3GPP TSG GERAN** **TSGG#12(02)3402**
**Meeting no 12** **Agenda item: 7.1.5.3**
**Sophia Antipolis, France**
**18 – 22 November 2002**

**Title:** **LS on ECSD and Ciphering**

**Source:** TSG GERAN

**To:** TSG SA WG3

**Cc:**

**Contact Person:**


**Name:** **Shkumbin Hamiti**
**Tel. Number:** +358504837349
**E-mail Address:** shkumbin.hamiti@nokia.com


**Attachments:** None

---

## 1. Overall Description:

Enhanced Circuit Switched Data (ECSD) was introduced as part of Release 99 specifications. A number of channel combinations were defined and the usage of A5 ciphering algorithm was modified due to larger output blocks when using 8-PSK modulation.

In addition, a concept that would allow different modulations in different directions was specified enabling asymmetrical 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 addition and the rest of the bits are discarded."

Consequently, our understanding of A5 usage in case of ECSD is that it applies to any channel combination that includes an 8-PSK channel. This means that the A5 usage specified for ECSD would be applicable to all channels in the channel combination, including GMSK modulated channels (as well as signalling blocks in associated control channels). For example in case when the assigned channel includes an E-TCH 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.

The A5/3 specification specifies two different algorithms to be used in GSM/EDGE:

- 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.
- 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.

It is our understanding that in the case of A5/3, the ciphering bit stream for the first 114 bits would be dependent on the mode (EDGE or GSM) for both the uplink and the downlink. 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 complicates the MS and BTS architecture due to a requirement to have a link from the modulation detection unit to the ciphering module. Note that this is different from the way it has been specified for ECSD in R99.

TSG GERAN thinks that the proper usage of the A5/3 would be so that if the assigned channel combination where 8-PSK modulated channel is used, then only "EDGE A5/3" algorithm is used for all channels in the connection, irrespective of the modulation.

## 2. ACTIONS:

1. TSG GERAN kindly asks TSG SA WG3 experts to specify the usage of the A5/3 according to the suggestion in this LS, specifically if the assigned channel combination where 8-PSK modulated channel is used, then only "EDGE A5/3" algorithm is used for all channels in the connection, irrespective of the modulation.

## 3. Date of Next TSG GERAN Meetings

| | |
|---|---|
| TSG GERAN WG2#12bis | 13-17 January, 2003 (St Paul de Vence, France) |
| TSG GERAN #13 | 03-07 February, 2003 (San Antonio, TX, USA) |