3GPP TSG SA WG3 Security — S3#11 **S3-000136**

Mainz, Germany, 22-24 February, 2000

Source: **Siemens Atea**

Title: **CRs on ciphering**

Document for: **Approval**

Agenda Item:

Introduction

The description of ciphering in 33.102, 25.301 and 33.105 was reviewed and the attached CR were drafted.

TS 25.301

TS 25.301 contains a more detailed description of ciphering that TS 33.102! It is suggested to transfer the detail in TS 25.301 to TS 33.102 and to delete it from TS 25.301 in order to avoid duplication. An important change is that the UE should not initialise HFN at random when the USIM has no valid START value available. Instead, AKA should be ran. After AKA, HFN can be initialised at 0.

In the event the removal of all detail from TS 25.301 is not acceptable, it is offered as an alternative that the proposed description (or part thereof) in TS 33.102 is included in 25.301.

TS 33.102

The existing clause 6.6 of TS 33.102 contains very few information ciphering. The new text started from the description in TS 33.105 and TS 25.301. The changes include:

1) Removal of the text in 6.3.3.1, the information is moved to 6.6.4.2 where it is discussed which cipher key is to be used;

2) Add description on the layer of ciphering in 6.6.2; text is taken from TS 25.301.

3) Add description of the ciphering method, taken from TS 33.105. The note is removed.

4) Add discussion on each of the input parameters in 6.6.4.

    1) The discussion for COUNT-C is most elaborated. The format of COUNT-C is first explained; the information comes from TS 25.301. Then it is explained how COUNT-C is initialised by means of the parameter START.

    2) Then CK is discussed. It is explained which CK needs to be used and how such a CK arrives at the location where it is applied (the UE or the RNC). The ciphering of the signalling data for simultaneous CS and PS services is discussed here.

    3) For purpose of the remaining input parameters is briefly described.

5) Furthermore, the table is replaced by a simple list, listing the values of the UEA that have a meaning in release '99.

TS 33.105

Changing TS 33.105 substantially is off course impossible, as it has already served its purpose: allowing SAGE to specify a cipher (and integrity) algorithm. The non-editorial changes relate what to do when the effective key length of the cipher and/or integrity key is smaller than 128.