3GPP TSG SA WG 3 (Security S3#14) **S3-000419**
1 - 4 August, 2000
Oslo, Norway

Source: **T-Mobil**

For: **Discussion**

Title: **Preparing the Use of BEANO as Confidentiality and Integrity Protection Algorithm for 3G Core Network Signalling Security**

For confidentiality and integrity protection of MAP-signalling messages, it is not very desirable that each pair of network operators uses its own security algorithm. Therefore, the block encryption algorithm BEANO (Block Encryption Algorithm for Network Operators) has been envisaged as a standard algorithm by S3, since that algorithm has been developed by ETSI SAGE for exactly that purpose.
However, the BEANO algorithm is now about four years old and has not been used since its development. There have been external and internal evaluations of BEANO, but these are not public, and neither is the algorithm itself[1].
On the other hand, it has been a guiding principle in the design of the 3G security architecture so far that all security algorithms used should be public, in order to enhance trust in the security of the overall system.
In order to prepare the use of BEANO as a confidentiality and integrity algorithm for core network signalling security, and to establish sufficient trust in BEANO, S3 should therefore consider the following steps:

1. Urgently request[2] from ETSI (which is the owner of BEANO) publication of the algorithm in case it is deployed for core network signalling security.
2. Acquire from ETSI the BEANO evaluation reports available by now.
3. Based on the evaluation reports, assess the suitability of BEANO for the envisaged purpose
4. If necessary, initiate another evaluation process of BEANO
5. Based on the results of the first four steps, select either BEANO or a standard off-the-shelf block encryption algorithm for core network signalling security

[1] The following documents exist in connection with BEANO:
- Requirements Specification for an encryption algorithm for operators of European public telecommunications networks; publicly available as ETSI Technical Report ETR 235
- Report on the specification, evaluation and usage of the PNO cipher BEANO; ETSI Technical Report, publicly available as DTR/SAGE-00008 (an ETR number could not be found on the ETSI server)
- Specification of the BEANO-Algorithm, Part 1: Algorithm Specification - confidential (no ETR no. available)
- Specification of the BEANO-Algorithm, Part 2: Design Conformance Test Data - confidential (no ETR No. available)
- Specification of the BEANO-Algorithm, Part 3: Algorithm Input/Output Test Data (Available on request from the BEANO Custodian, Mr. De Courcel)
- Specification of the BEANO-Algorithm, Part 4: Modes of Operation (Available on request from the BEANO Custodian, Mr. De Courcel)
- Evaluation Report of the BEANO-Algorithm, ETSI-SAGE internal document - confidential

[2] That request should probably come from SA plenary in order to have a chance of success