3GPP TSG SA WG 3 (Security S3#14) **S3-000420**
1 - 4 August, 2000
Oslo, Norway

Source: **T-Mobil**
For: **Discussion and Approval**

From: **3GPP TSG SA WG 3 (Security)**

To: **ETSI Secretariat**
Monsieur Pierre de Courcel
ETSI
F-062921 Sophia Antipolis Cedex, France

CC: **ETSI TC SEC**
ETSI SAGE

Request concerning use of the BEANO encryption algorithm

Dear Monsieur de Courcel,

3GPP TSG SA WG 3 (S3, for short) is the technical specification group within 3GPP dealing with the security aspects of 3G systems.
For Release 2000 of the UMTS system, confidentiality and integrity protection of signalling links within and between mobile network operator's networks by means of a cryptographic algorithm is planned. It is the understanding of S3, that the BEANO (Block Encryption Algorithm for Network Operators) algorithm has been designed by ETSI SAGE in 1996 for exactly that purpose. S3 would therefore like to ask ETSI as the owner of the BEANO algorithm to confirm that

- this understanding is correct, and that
- all involved 3GPP member companies can acquire the BEANO specifications from ETSI

Further, the ETSI secretariat is asked to clarify the exact conditions under which the BEANO specifications can be acquired, and whether the BEANO specifications and related evaluation reports can be published in case BEANO is used in 3G core network signalling security. Since by definition all 3G security algorithms shall be public, publication of BEANO is a prerequisite for its deployment in the 3G security architecture.

Thank you very much for your co-operation.

Yours sincerely,

(Chairman of 3GPP TSG SA WG 3)