



STACTIC W.P. 05/37

27TH ANNUAL MEETING – SEPTEMBER 2005

Addition to STACTIC Working Paper 05-26

by Ukraine

In our proposal we suggest to change the use of technical terms in NAFO/FC Doc. 05/3 stated:

‘It is also recommended that the Fisheries Commission approves the following encryption protocols for electronic data transmission:

- “Pretty Good Privacy” PGP
- “Digital Encryption Standard” DES‘

Our IT experts consider that such a use of the technical terms for electronic data transmission is not correct considering the electronic manual ‘An Introduction to Cryptography’ 2003 by PGP Corporation. We suggest the following version:

‘It is also recommended that the Fisheries Commission approves the following encryption software for electronic data transmission:

- “Pretty Good Privacy” PGP (using CAST, IDEA, Triple-DES, Twofish or AES (Rijndael) encryption algorithms with key 128 bit or stronger)
- WinZip 9.0 (using AES encryption algorithm with key 128 bit or stronger).’

These corrections will have no influence on the functioning of transmission and receiving of the encoded information and the system in general. STACTIC Working Paper 05/26 deals only with the proper use of the terminology.