



Sophia Antipolis, 24 July 1995

National Computer Centre
Oxford Road

MANCHESTER
United Kingdom

Our ref.: PMC\95126\GO\cad

Subject: Registration of cryptographic algorithms according ISO/IEC 9979;
Application for registration

Dear Madam, dear Sir,

The European Telecommunications Standards Institute (ETSI) would like to have its cryptographic algorithm BARAS registered according the rules given in ISO/IEC 9979.

The information required by the Standard in clause 7 is annexed to this letter.

A softcopy of that information is also attached to this letter.

The extended information for item f of the Annex is;

Name of organisation:	European Telecommunications Standards institute (ETSI)
Address to be registered:	F-06921 Sophia Antipolis
Principal contact in the organisation:	Mr. Karl Heinz Rosenbrock
Telephone number:	+33 92 94 42 00
Fax number:	+33 93 65 47 16
Address for correspondance:	ETSI Secretariat F-06921 Sophia Antipolis Cedex

Yours faithfully,

P.O. Karl Heinz Rosenbrock
Director

 A handwritten signature in black ink, appearing to read 'Fredo Jull', is written over a stylized, looped signature line. Below the signature, the name 'Fredo Jull' and the title 'Deputy Director' are printed in a bold, sans-serif font.

Fredo Jull
Deputy Director

Encl.

The information needed for the ISO registration of BARAS according to clause 7 of ISO/IEC 9979 is given below.

- a To be assigned by ISO ($\{\text{iso standard 9979 baras (11)}\}$)
- b BARAS
- c Confidentiality for Audio Visual Systems
- d Cryptographic interface parameters

The algorithm is an additive stream cipher algorithm with variable input size and output size.

The key length is 64 bits.

The Initializing Value size is 64 bits

- e Testwords

Testset 1

KEY: 00000000000000000000000000000000
00000000000000000000000000000000

IV: 00000000000000000000000000000000
00000000000000000000000000000000

First 256 bits of key-stream produced by additive stream cipher:

```
00101000100011010111110101010101
01001000010100011100001011000110
00010100010111111101111000111001
10001010110101001101011001010101
00111010001001010010001000010111
11000001100111101011001111101011
11000011011101000110100100111111
11101100111111010110100001110011
```

Testset 2

KEY: 11111111111111111111111111111111
11111111111111111111111111111111

IV: 11111111111111111111111111111111
11111111111111111111111111111111

First 256 bits of key-stream produced by additive stream cipher:

```
11110111011010010001010000110111
10100001101011110010111011001000
01101001111011100000010010010101
00100001001000100100001001001011
11100110011110101011010000100110
10111001110110001101101011110100
00010100100111100100011010010011
10000110001100111110100011101101
```

- f European Telecommunications Standards Institute (ETSI)

- g To be assigned by the Registration Authority (18 August 1995)
- h Not subject to national standards
- i The algorithm will be distributed by an ETSI custodian on the basis of a non-disclosure and restricted usage undertaking.
- j None
- k Not provided
- l Additive stream cipher
- m Not provided