3GPP TSG SA WG3 Security — S3#10 **S3-000027**

19-21 January, 2000

Antwerpen, Belgium

Source: **ETSI SAGE 3GPP Task Force**

Title: **Extension of shortened keys to full-length keys**

Document for: **Discussion**

Agenda Item:

LIASON STATEMENT

To:	3GPP TSG SA WG3
From:	ETSI SAGE 3GPP Task Force
Date:	28th December 1999
Topic:	Extension of shortened keys to full-length keys

The ETSI SAGE Task Force for the design of the 3GPP Confidentiality and Integrity Algorithms (SAGE TF 3GPP) requests 3GPP TSG SA3 to adopt the following recommendation.

If in the f8 or f9 algorithm a cryptographic key of fewer than 128 bits is to be used, then the full 128-bit key shall be obtained by repeating the shorter key as often as necessary (rather than by padding the short key with zeros, as is currently proposed).

To be precise: suppose that SK is a key with a length of n bits with n less than 128 and the key bits are denoted by

$$SK[\ 0\ ],\ SK[\ 1\ ],\ \ldots.,\ SK[\ n-1\ ].$$

If the 128 bit Confidentiality Key CK is derived from SK this should be done as follows:

$$CK[\ i\ ] = SK[\ i\ (\mathrm{mod}\ n)\ ] \text{ for } i = 0, 1, 2, \ldots, 127$$

Similarly, if the 128 bit Integrity Key IK is derived from SK this should be done as follows:

$$IK[\ i\ ] = SK[\ i\ (\mathrm{mod}\ n)\ ] \text{ for } i = 0, 1, 2, \ldots, 127.$$