3GPP TSG SA WG3 Security — S3#20 **S3-010574**

16 - 19 October, 2001

Sydney, Australia

From: **SA3**

To: **CN5**

Title: **LS to CN WG5: Comments on TS 29.198**

Contact: Peter Howard
Email. peter.howard@vodafone.com
Tel. +44 1635 676206

SA3 has the following comments on the cryptographic algorithm descriptions in TS 29.198. Note that SA3 has not conducted a security review of the full specification.

1. The algorithm descriptions do not constitute complete specifications. For example, for DES the exact mode of operation must be specified and for RSA-based digital signature the exact signature mechanism must be specified (e.g. by external reference to appropriate standards).

2. 56 bit DES and 512 bit RSA are both considered rather low-grade algorithms these days, and some people have expressed concerns about the strength of MD5. CN5 are asked to reconsider whether these algorithms should be supported in the OSA standard and to consider whether alternatives such as AES, DSA, SHA1 and RIPE-MD160 should be supported instead.

3. It was noticed that a description of DES with a 128 bit key is included. Although constructions of DES with a 128 bit key are technically possible, the two most common implementations of DES are "single DES" with a 56 bit key and "triple DES" with a (2x56 = 112) bit key. CN5 are asked to check whether they really intend to use DES with a 128 bit key, and if so to provide a complete specification or reference for the algorithm (see note below).

   NOTE: 8 parity bits are sometimes added to the 56 bit DES key. These parity bits have no cryptographic significance and are therefore ignored in the DES encryption process. This is often used to explain why it is sometimes incorrectly stated that DES keys are multiples of 64 bits.