3GPP TSG SA WG3 Security — S3#20 **S3-010561**

16 - 19 October, 2001

Sydney, Australia

Source:	**Vodafone**
Title:	**Draft LS to CN5 regarding comments on TS 29.198**
Document for:	**Email approval by 31st November 2001**
Agenda Item:	**-**

From:	**SA3**
To:	**CN5**
Copy:	
Title:	**Comments on TS 29.198**
Contact:	Peter Howard Email. peter.howard@vodafone.com Tel. +44 1635 676206

SA3 has reviewed TS 29.198 section 8.2.2.3 and would like to provide the following comments to CN5 regarding the algorithm descriptions:

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

2. SA3 have concerns that 56 bit DES and 512 bit RSA might not be secure enough for this particular application. In addition, there are concerns about the security of MD5. CN5 are asked to reconsider whether these algorithms should be supported in the OSA standard.

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[1].

---

[1] Note that 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.