3GPP TSG WG SA3 –Security SA3#16 **S3-000738**
28-30 November, 2000
Sophia Antipolis, France

Title: **Standardisation of security parameter bit ordering in USIM and AuC**

Source: **Vodafone**

For: **Email discussion**

Agenda:

It is clear that the bit ordering of security parameters is maintained on all interfaces between the USIM and the AuC. However, it seems that a consistent bit ordering within the AuC and within the USIM may not be maintained when the example authentication algorithm and/or sequence number management profile is used. If USIM and AuC suppliers do not agree on a consistent bit ordering, an AuC will potentially have to support different bit orderings for different USIMs. This seems undesirable.

It is proposed that this issue is discussed on the S3 mailing list so that working assumptions can be agreed as soon as possible. CRs should then be approved at the next S3 meeting.