3GPP TSG SA WG3 Security — S3#13 **S3-000374**

23-26 May, 2000

Yokohama, Japan

Source: **Vodafone Airtouch**

Title: **Proposed LS to N4 on replay protection for core network signalling messages**

Document for: **Approval**

Agenda Item: **12**

Source: **S3**[1]

To: **N4**

Title: **GTP signalling security**

In section 7 of 33.102 v3.4.0 on core network signalling security, a field is reserved in the layer III message structure for a time-varying parameter (TVP). This parameter is intended to be used as part of the integrity protection mechanism to provide *replay protection*. However, neither the length, type nor use of this field is specified. At least the length of this field must be determined to allow N4 to complete the stage 3 specifications in 29.002.

Please find attached a paper on replay protection for core network signalling security which recommends the use of time-stamps as TVPs for replay protection. It is further recommended to use protection mode 2 whenever possible as this makes replay attacks more difficult. As regards the size of TVPs, it is proposed that 32 bits is sufficient. This allows for a time-stamp based scheme with a maximum time resolution of 1 second and a maximum key lifetime of more than 100 years. The resolution of the clock must be agreed as a system parameter, the size of the time-window at the receiving node need not be standardised.

---

[1] Contact: Peter Howard, Vodafone Ltd; tel +44 1635 676206; email peter.howard@vf.vodafone.co.uk