3GPP TSG SA WG3 #21bis NDS/MAP ad hoc **Tdoc S3z020038**
Antwerp, Belgium
31st January – 1st February 2002

Source: **SA3 ad hoc**[1]

To: **CN4**

Title: **LS "MAP security issues"**

Contact: **Peter Howard, Vodafone Group R&D**
Email: Peter.Howard@vodafone.com

SA3 would like to thank CN4 and CN for their liaison statements on MAP security (N4-011449 and NP-010685).

In N4-011449 "LS on MAPsec error handling", CN4 highlighted the following issue:

> *MAP messages can be discarded at the MAP protocol level (e.g. if the TVP is out of an acceptable time window). It is however not possible to undo TCAP processing at the time when the message is processed on MAP level. This means that the dialogue cannot successfully be continued. This means that re-played messages could be used as the basis of a denial of service attack.*

SA3 understand that there are new denial of service possibilities introduced when adding security. However, these threats are much less severe that those threats that exist when no security is provided. The denial of service threat could be limited if the MAP application could close the TCAP dialogue immediately when the MAPsec message cannot be verified so that the TCAP dialogue is not left to time out. However, the CN4 LS seems to indicate that this is not possible and SA3 believe that the current denial of service possibilities are quite limited and therefore can be tolerated.

In N4-011449 CN4 also asked the following question:

> *CN4 is interested to know what is the maturity status of the SA3 TS 33.200 in order to plan future changes in the specifications under responsibility of CN4. Thus CN4 will appreciate that the final stable version of 3GPP TS 33.200 is send to us in a LS with the changes you foresee in CN4 specifications.*

SA3 would like to indicate that a draft CR to 33.200 was sent to SA#14 for information. This CR indicates the future changes that are planned to 33.200 for Release 5, i.e. the introduction of automatic security association establishment.

In NP-010685 "Liaison statement on Protocol Specification of the Ze-interface", CN identified the following actions on SA3:

Action 1: *SA3 are asked to consider sending an expert to the CN WG4 meeting in January/February 2002 to present the requirements for the protocol on the Ze interface.*

Unfortunately it has not been possible to send an SA3 expert to the CN4 meeting in Sophia Antipolis, France, 28 January – 1 February 2002.

Action 2: *SA3 are asked to consider extending their meeting in February/March 2002 to allow further joint discussion with CN4 experts on the protocol on the Ze interface.*

SA3 welcomes the proposal for CN4 experts to attend the SA3#22 meeting in Bristol, UK, 25-28 January 2002. SA3 believe that a half day joint session with CN4 experts can be accommodated

[1] This LS was approved by those delegates who attended the ad hoc meeting in Antwerp. It is subject to final approval on the SA3 email list

without extending the meeting. At present there are no constraints on the SA3#22 meeting schedule so CN4 experts are invited to indicate which date and time (morning or afternoon) they would prefer.