3GPP TSG SA WG3 Security — S3#22 **S3-020008**

25 - 28 February 2002

Bristol, UK

3GPP TSG CN WG4 Meeting #11 ***N4-011449***
Cancun, Mexico, 26th - 30th November 2001

Title: **DRAFT LS on MAPsec error handling**

Source: CN4
To: SA3
Cc:
Response to: LS (S3z010121) on MAPsec error handling from SA3

Contact Person:
Name: Ulrich Wiehe
Tel. Number: +49 6621 169 139
E-mail Address: ulrich.wiehe@icn.siemens.de

Attachments: NONE

---

1. Overall Description:

CN4 thank SA3 for their liaison on MAPsec error handling (S3z010121, N4-011348) and provide answers as follows:

- CN4 have checked the error handling for MAP secure transport messages in TS 29.002 and confirm that errors specific to MAPsec are rather generic. To be more specific the following MAPsec specific error information is returned to the sender of a protected MAP message:
  - "**encapsulatedAC-NotSupported**" if a MAP-dialogue opening message, which is not supported, is received in protected mode.
  - "**transportProtectionNotAdequate**" if a protected message is received, which should not be protected according to the SPD, and if an unprotected message is received, which should have been protected according to the SPD and fallback to unprotected mode is not allowed.
  - "**UnexpectedDataValue**" if an unexpected value is received in the Security Header e.g. an unknown SPI.
  - "**DataMissing**" if an optional parameter, which should be present, is missing; e.g. the protectedPayload.
  - "**Secure Transport Error**" if the application using secure transport returned an error. The parameter of the error indicates the protected payload, which carries the result of applying the protection function specified in 3G TS 33.200 to the encoding of the parameter of the original error

  CN4 believe that this is consistent with the SA3 flow provided in CR 33.200 007.

- 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.

CN4 will be pleased to check 3GPP TS 29.002 for consistency with the received SA3-flows and perform the corresponding changes in the mentioned specification.

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.

2. Actions:

CN4 kindly asks SA3 to send us the final stable version of 3GPP TS 33.200 with an indication of the impacts expected in specifications under responsibility of CN4.

3. Date of Next CN4 Meetings:

CN4#12	28 January – 1 February 2002, Sophia Antipolis, France
CN4#13	8 April – 12 April 2002, North America