3GPP TSG SA WG3 Security — S3#13 **S3-000339**

23-26 May, 2000

Yokohama, Japan

Source: **Ericsson**

Title: **MAP Security Layer III Open Items**

Document for: **Discussion**

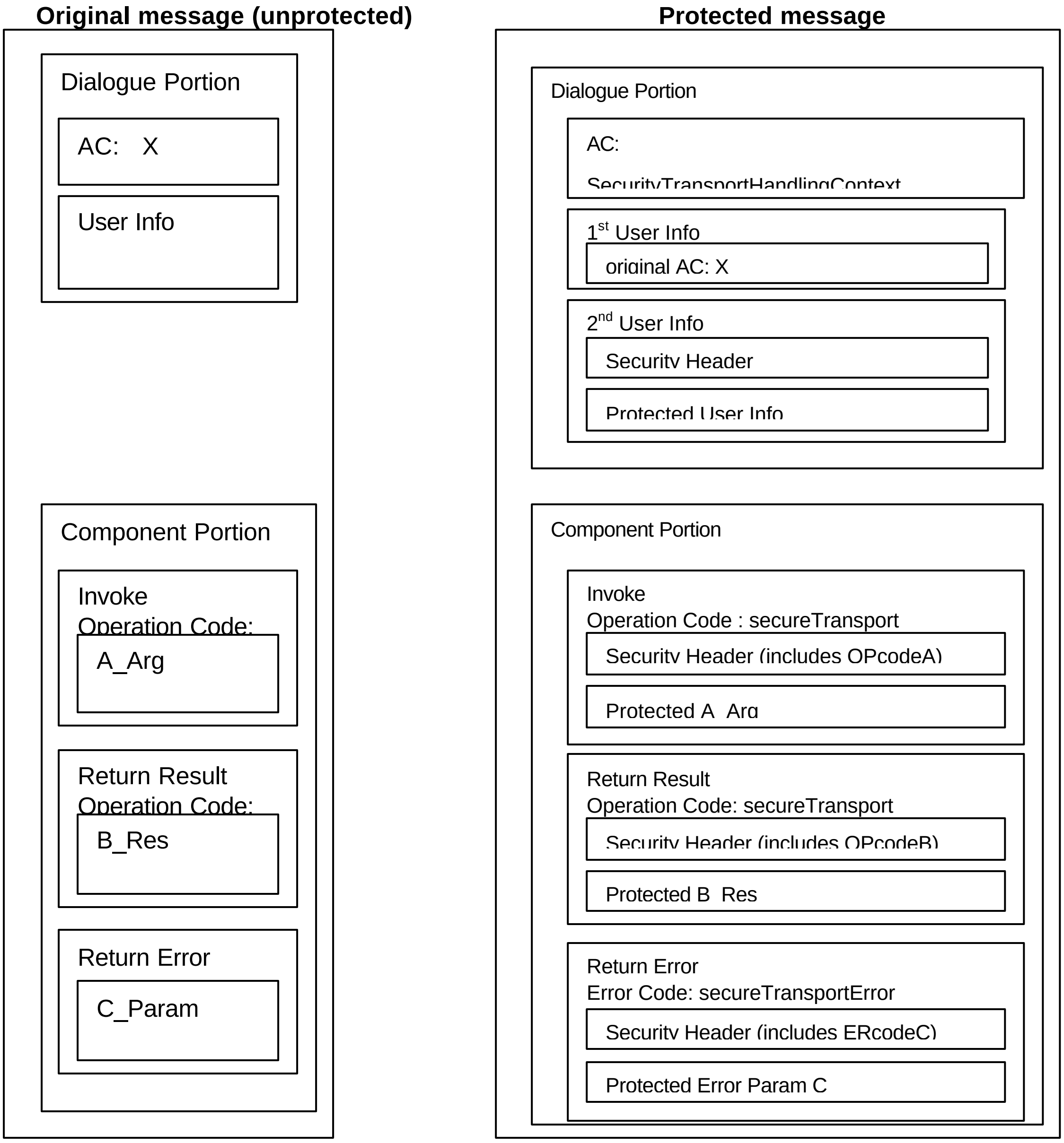
Agenda Item: **Ad-hoc MAP Security**

---

1. Introduction

At their last meeting in Charleston (27th-31st March), N4 agreed to follow the principles in Tdoc N2B-000394 for the incorporation of MAP Security Layer III at N4 specifications (mainly 29.002).

The structure of the protected message in comparison with the original message is as follows:



As it can be seen, it is proposed to protect each component of the message separately with the possibility to specify a different Protection Mode level at the Security Header of the different message components.

N4 is currently working in the introduction of MAP Security Layer III into their specifications and in order to meet June 00 deadline, corresponding CRs shall be presented and approved at their ongoing meeting (22nd-226th May).

However, S3 shall confirm that agreed principles at N4 are acceptable and still additional support and/or information shall be provided in order to make possible a complete successful implementation of MAP Security Layer III.

2. Open Items for a complete MAP Security Layer III specification

After a review of proposal in N2B-000394, the following open items have been identified:

- **Protection Mode 0:**

  The use of Protection Mode 0 as proposed in N2B-000394 implies that the protected MAP messages using the new AC for "SecurityTransportHandlingContext" can use Protection Mode 0 for some or all of the components in the MAP message to be protected.

  Protection Mode 0 offers no protection at all. Therefore, the layer III message body in Protection Mode 0 is identical to the original MAP message body in clear text.

  This implies the introduction of:

  a. Extra Headers:

  A MAP message protected using Protection Mode 0 will just introduce extra headers to the components protected in the form of additional ACs, User Info and Security Headers.

  b. Security risk with Protection Mode 1:

  Protection Mode 1 offers Integrity and Authenticity:

Cleartext||TVP||$E_{KSXY(i)}$(*Hash*(MAP Header||Security Header||Cleartext||TVP))

  With the following actions, an intruder catching a protected MAP message could potentially modify the clear text arguments in a MAP message component protected using Protection Mode 1:

  - Discard the Time Variant parameter (TVP),
  - Discard the Integrity Check hash function ($E_{KSXY(i)}$(*Hash*(MAP Header||Security Header||Cleartext||TVP),
  - Modify the Security Header to Protection Mode 0 and
  - Finally modify the clear text argument originally meant to be protected.

  For these reasons, it is recommended not to use Protection Mode 0 for protection of MAP messages with AC "SecurityTransportHandlingContext" (only Protection Mode 1 and 2 shall be used). The original MAP message shall be considered as offering Protection Mode 0 for MAP Security Layer III.

- **Encryption Algorithms and Keys:**

  MAP Security Layer III uses the distributed symetric keys agreed at Layers I and II for securely exchanging sensitive data between the NE of the operator/s by means of a symetric encryption algorithm.

  S3 shall agree on an specific set of encryption algorithms suitable to be used for encrypting MAP messages payload (performance in terms of computational time compsumtion and additional overheads shall be also considered).

  Specific characteristics and length of keys to be used with the selected algorithms shall be also agreed.

- **Detailed structure of protected payload:**

  N2B-000394 proposes S3 TS 33.102 to specify the detailed structure of protected payload, i.e. length and format of TVP and Integrity Check hash functions:

```
SecurityEnvelopeArg ::= SEQUENCE {
    securityHeader                  SecurityHeader,
    protectedPayload                ProtectedPayload              OPTIONAL
    }
    -- The protectedPayload carries the result of applying the
    -- encryption function specified in TS 33.102 to the encoding of the
    -- original operation's argument.
```

  Although TS 33.102 might not be the right place, the definition of data types and lengths for such parameters is extremely important to allow for a proper segmentation of the MAP message.

- **Further alignments between S3 and N4 specifications:**

  Once principles and open items for MAP Security Layer III are clarified and agreed, S3 shall update its specifications accordingly. N4 shall be also informed to work (or continue working) on the same principles, updating their specifications following S3 guidance.