**3GPP TSG-SA3 Meeting #15bis**
**(Ad-hoc on aSIP and NDS WIs)**
**Munich, 8th – 9th November 2000**

S3z000015

**Agenda Item:** -

**Source:** Ericsson

**Title:** Structure of Security Header for MAP Security

**Document for:** Discussion and decision

# 1 Introduction

This contribution tries to agree on a revised structure for the Security Header used for MAP Application Layer Security.

# 2 Background

MAP Security Header is a parameter added to secure MAP messages which carries information required by a receiving entity in order to extract the protected information from a securely transported MAP message.

The structure for this parameter as defined by S3 in 33.102 v3.4.0 during R99, is the following:

### *7.4.3 Structure of Security Header*

*The security header is a sequence of the following data elements and data types:*

- *Protection Mode (INTEGER)*
- *Key Identifier (INTEGER)*
- *Algorithm Identifier (Algorithm Identifier)*
- *Mode of Operation (INTEGER)*
- *Initialisation Vector (OCTET STRING OPTIONAL)*

*NOTE: Whether the Initialisation Vector is needed depends on the mode of operation of the encryption algorithm.*

S3 has progressed the work on MAP Application Layer Security as a WI for R00 and especially on the field of Key Management ($Z_A$ and $Z_B$ interfaces, former Layers I and II). As a consequence, the use of Security Associations for MAP Security has been agreed. MAP SAs are used to define the security parameters required to protect the traffic over the $Z_C$ interface (the SS7 network).

# 3 Revised Structure of Security Header

With the definition and use of Security Associations for MAP Application Layer Security, the structure of the Security Header needs to be revised.

Some of the parameters within the former structure of the Security Header are now included in the structure of the Security Association (Protection Mode, Key Identifier, Algorithm Identifier, Mode of Operation). Besides, the use of MAP-SAs require the introduction of additional parameters within the Security Header (e.g. Sending PLMN-Id).

The proposed (revised) structure of Security Header to be considered in 3GPP TR 33.800 on ‘Principles for Network Domain Security’ is as follows:

## 7.4.3 Structure of Security Header

~~NOTE: The content of the security header has yet to be finalised. Probably it will just contain the sending PLMN identity and an SPI identifying the MAP-SA used and per message related information like and Initialization Vector.~~

The Security Header is a sequence of the following data elements:

- **Sending PLMN-Id:**
  PLMN-Id is the ID number of the sending Public Land Mobile Network (PLMN). The value for the PLMN-Id is formed from the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the destination network.

- **Security Parameter Index (SPI):**
  SPI is an arbitrary 32-bit value that is used in combination with the sender's PLMNID to uniquely identify a MAP-SA.

- **Initialization Vector (IV):**
  Initialization vectors are used with block ciphers in chained mode to force an identical plaintext to encrypt to different cipher texts. Using IVs prevents launching a codebook attack against encrypted traffic. The issue is discussed in more detail in RFC 2406. IV has only local significance in the NE.

  NOTE: Whether the Initialisation Vector is needed depends on the mode of operation of the encryption algorithm.

- **Original Component identifier:**
  Identifies the type of component within the MAP operation that is being securely transported (Operation identified by operation code, Error defined by Error Code or User Information).