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

S3z000013

Agenda Item: -

Source: Ericsson

Title: General Structure of Secured MAP Operations

Document for: Discussion and decision

1 Introduction

This contribution tries to align S3 work with CN4 specifications including implementation of MAP Application Security Z_C interface (former Layer III).

In particular, this contribution tries to agree on the fact that S3 should focus on the definition of security mechanisms on a per-MAP Operation basis.

2 Background

A set of CRs implementing MAP Security Layer III (today's Z_C interface) has been recently agreed and incorporated in latest version of CN4 specifications. In particular, the information introduced by CR#148r4 on 29.002 is quite relevant for the shake of this contribution (basically includes the work progressed by CN4 during R99).

The principles followed by CN4 allows the protection of any MAP operation by encapsulating the information in the original operation (after execution of corresponding protection level) into a new defined MAP operation for secure MAP communication ("SecureTransportClassX").

The secure MAP operation, including the original information in protected mode, is performed (Request, Return Result/Error) in the course of a secure MAP dialogue established between the peer NEs wishing to communicate using secure MAP.

The idea is to reuse this "architecture" for the ongoing and future work in S3/CN4 as much as possible.

3 Structure of Secured MAP Operations

Given the implementation of Z_C interface proposed by CN4, it is Ericsson's understanding that S3, from a stage 2 specification perspective, should be focused on the definition of protection mechanisms on a per-MAP Operation basis; i.e. define which MAP operations require protection, what kind of protection (confidentiality/integrity) and how to apply this protection to the selected MAP operations.

These mechanims are then implemented in stage 3 specifications (29.002) where other implementation details of the MAP protocols are also taken into account.

Based on this assumption, Ericsson propose that the following 'Structure of Secure MAP Operations' appear in 3GPP TR 33.800 ('Principles for Network Domain Security'):

7.4 Security for MAP

[EDITOR: From Ericsson's S3-000556]

This subclause describes mechanisms for establishing secure signalling links between network nodes, in particular between SN-VLRs/SGSNs and HE-HLRs belonging to different network operators and communicating with MAP protocols. Such procedures may be incorporated into the roaming agreement establishment process.

7.4.1 ~~General Structure of Secured MAP Messages~~General Structure of Secured MAP Operations

Secured MAP ~~messages~~ operations are ~~transported~~ performed via the MAP protocol in the course of secured MAP dialogues~~, that means, they form the payload of a MAP message after the original MAP message header~~.

For Secured MAP ~~Messages~~operations, three levels of protection (or protection modes) are defined providing the following security features:

Protection Mode 0:	No Protection
Protection Mode 1:	Integrity, Authenticity
Protection Mode 2:	Confidentiality, Integrity, Authenticity

Secured MAP ~~messages~~ operations consists of a Security Header and the ~~Secured MAP Message Body~~ Protected Payload, that is the result of applying the corresponding protection mode to the original MAP operation payload~~protected by the symmetric encryption algorithm, using the symmetric session keys that were distributed as part of the MAP-SA~~. Secured MAP ~~Messages~~ operations have the following structure:

Security Header	~~Secured MAP Message Body~~Protected Payload

In all three protection modes, the security header is transmitted in cleartext.

~~Both parts of the Secured MAP message, security header and message body, will become part of the "new" MAP message body. Therefore, the complete "new" MAP messages take the following form in this proposal:~~

~~MAP Message Header~~	~~MAP Message Body~~

~~Secured MAP Message~~

~~MAP Message Header~~	~~Security Header~~	~~Secured MAP Message Body~~

~~Like the security header, the MAP message header is transmitted in cleartext.~~ In protection mode 2 providing confidentiality, the ~~Secured MAP Message Body~~protected payload is essentially the encrypted payload of the ~~"old"~~original MAP operation ~~message body~~. For integrity and authenticity in protection modes 1 and 2, an encrypted hash calculated on the ~~MAP message~~

~~header,~~ security header and the ~~"old"~~payload of the original MAP operation ~~message body~~ in cleartext is included in the ~~Secured MAP Message Body~~protected payload ~~in protection modes 1 and 2~~. In protection mode 0 no protection is offered, therefore the ~~Secured MAP Message Body~~protected payload is identical to the ~~"old"~~payload of the original MAP ~~message body~~operation ~~in cleartext in this case~~.

Summing up, the Secured MAP ~~Message~~ Operation is a sequence of data elements consisting of the MAP Message Header, the Security Header and the ~~Secured MAP Message Body~~protected payload. In the following subchapters, the contents of the ~~Secured MAP Message Body~~protected payload for the different protection modes and the security header will be specified in greater detail.

7.4.2 Format of Secured MAP Message Body

7.4.2.1 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the ~~Secured MAP message body~~protected payload in protection mode 0 is identical to the original MAP ~~message body~~operation payload in cleartext.

In case Protection Mode 0 is to be used, the mechanism shall also allow to perform the operation in cleartext, thus avoiding the extra load introduced by the Security Header.

7.4.2.2 Protection Mode 1

The ~~message body~~protected payload of Secured MAP ~~messages~~ operations in protection mode 1 takes the following form:

TVP||Cleartext|| $H_{KSXY(int)}$(TVP|| ~~MAP Header||~~Security Header||Cleartext)

where "Cleartext" is the ~~message body~~payload of the original MAP ~~message~~ operation in clear text. Therefore, in Protection Mode 1 the ~~Secured MAP Message Body~~protected payload is a concatenation of the following information elements:

- Time Variant Parameter TVP
- Cleartext
- Integrity Check Value

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function H with the integrity session key KS_{XY}(int) to the concatenation of Time Variant Parameter TVP, ~~MAP Header,~~ Security Header and Cleartext.

The TVP used for replay protection of Secured MAP ~~messages~~ operations is a 32 bit time-stamp. The receiving network entity will accept ~~a message~~an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

7.4.2.3 Protection Mode 2

The ~~Secured MAP Message Body~~protected payload in protection mode 2 takes the following form:

TVP|| $E_{KSXY(con)}$(Cleartext) || $H_{KSXY(int)}$(TVP|| ~~MAP Header||~~Security Header|| $E_{KSXY(con)}$(Cleartext))

where "Cleartext" is the original MAP ~~message~~ operation payload in clear text. ~~Message c~~Confidentiality is achieved by encrypting Cleartext with the confidentiality session key KS_{XY}(con). Authentication of origin and ~~message~~ integrity are achieved by applying the message authentication code (MAC) function H with the integrity session key KS_{XY}(int) to the concatenation of Time Variant Parameter TVP, ~~MAP Header,~~ Security Header and $E_{KSXY(con)}$(Cleartext).

The TVP used for replay protection of Secured MAP ~~messages~~ operations is a 32 bit time-stamp. The receiving network entity will accept ~~a message~~an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

It is further recommended the use of protection mode 2 whenever possible as this makes replay attacks more difficult.

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.

7.4.4 Mapping of MAP Messages and Modes of Protection

The network operator should be able to assign the mode of protection to each MAP message in order to adapt the level of protection according to its own security policy. Guidance may be obtained from the SS7 Signalling Protocols Threat Analysis [12].

It is foreseen that only a small set of MAP-PPs are standardised. However, the use of private MAP-PPs agreed offline between the operators shall be also allowed.