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

S3z000016

Agenda Item: -

Source: Ericsson

Title: Refinement of MAP Security Association for MAP Security

Document for: Discussion and decision

1 Introduction

This contribution proposes some changes in the previous agreed structure of MAP Security Association for MAP Security.

In particular the removal of "Encryption Key Version Number" and "MAC Key Version Number" parameters and the modification of the definition for "MAP Protection Profile" are proposed.

2 Background

S3 has progressed the work on MAP Application Layer Security as a WI for R00, 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).

So far, the structure of a MAP Security Association, as per 3GPP TR 33.800 ('Principles for Network Domain Security') is the following:

MAP Security Association

A MAP-SA encompasses the following parameters:

- ***Encryption Algorithm Identifier:***
  Identifies the encryption Algorithm used for MAP message protection.
- ***Encryption Key Version Number:***
  Version number of the encryption key to be used for MAP message protection.
- ***Encryption Key:***
  Encryption Key to be used for MAP message protection.
- ***MAC Algorithm Identifier:***
  Identifies the MAC Algorithm used for MAP message protection.
- ***MAC Key Version Number:***
  Version number of the MAC key to be used for MAP message protection.
- ***MAC Key:***
  MAC Key to be used for MAP message protection.
- ***MAP Protection Profile:***
  A MAP Protection Profile (MAP-PP), is an specification of how components in a MAP message over Z_C interface shall be protected. Indicates whether a MAP dialogue needs protection, and if so, indicates for every component of the dialogue the protection mode and mode of operation of the encryption algorithm to be used. In case protection is required, it shall also state whether fallback to unprotected mode is allowed.

- ***SA Lifetime:***
  Defines the actual duration of the SA.

As a result of the introduction of the MAP-SA concept in S3, the structure of the Security Header is affected. Refer to S3z000015 on 'Structure of Security Header for MAP Security' also presented to this meeting. In that document it is proposed to use the parameters "Sending-PLMN-Id" and "SPI" to uniquely identify the MAP-SA.

3 Refinement of MAP Security Association

3.1 Encryption and MAC Key Version Number

Before S3 agreed on the use of MAP-SAs, MAP Security specified secret key transport mechanisms at Layer I and II (today's Z_A and Z_B interfaces). Symmetric session keys were agreed between KACs and distributed to the NEs. The following approach was followed to start using the distributed Keys (33.102 v3.4.0, Chapter 7.3):

> *"In order to ensure that no network element starts enciphering with a key that not all potentially corresponding network elements have received yet, the following approach is suggested:*
>
> *The distribution of the session keys KS_{XY} in network X having initiated the Layer I message exchange should not begin before the Key Distribution Complete Message from the receiving network Y has been received by KAC_X in Layer I. As soon as a network element of X has received a session key KS_{XY}, it may start enciphering with this key."*

This made necessary that two set of keys were considered by the NEs; i.e. once a new session key was received by a NE, it was necessary to keep the old key until completion of distribution of new Key to the rest of NEs. During this time, two set keys were "alive" in the NE and it was required to differentiate them.

Both "Encryption Key Version Number" and "MAC Key Version Number" were used for this purpose.

With the use of MAP-SAs, the parameter "SPI" in the Security Header will be used along with "Sending-PLMN-Id" parameter to uniquely identify the MAP-SA and the specific key version to be used.

It is therefore proposed to remove these parameters from the structure of the MAP-SA.

3.2 MAP Protection Profile

As discussed in S3z000014 on 'Protection Profiles for MAP Security' also presented to this meeting, a new definition for the parameter "MAP-Protection Profile" is proposed.

That document, also propose to consider the indication on whether fallback to unprotected mode is allowed as a separate parameter within the MAP-SA.

It was also proposed there, to remove the mode of operation of the encryption algorithm from the definition of MAP-PP. In this contribution, Ericsson proposes to include this indication along within the definition of the Encryption/MAC algorithm identifiers (mind that the same applies to MAC algorithm for integrity protection).

3.3 Revised structure of MAP-SA

According to the changes proposed above, the structure of the MAP Security Association to be considered in 3GPP TR 33.800 on 'Principles for Network Domain Security' would be as follows:

7.2.1 Distribution of MAP-SA

A Security Association for Secure MAP message exchange (MAP-SA) is a set of policy and key(s) used to protect information. The MAP-SA conveys information about the security parameters to be used for MAP message protection when MAP messages are to be sent from Network A to Network B; i.e. a MAP-SA is a unidirectional SA (defined either for inbound or outbound traffic).

The agreement on a symmetric session key between two KACs for protection of the MAP message exchange between NEs belonging to their respective networks, is accomplished through the establishment of the MAP-SA.

A MAP-SA encompasses the following parameters:

- **Encryption Algorithm Identifier:**
  Identifies the encryption Algorithm and its mode of operation used for ~~MAP message~~confidentiality protection.

~~**Encryption Key Version Number:**~~
~~Version number of the encryption key to be used for MAP message protection.~~

- **Encryption Key:**
  Encryption Key to be used for ~~MAP message~~confidentiality protection.

- **MAC Algorithm Identifier:**
  Identifies the MAC Algorithm and its mode of operation used for ~~MAP message~~integrity protection.

~~**MAC Key Version Number:**~~
~~Version number of the MAC key to be used for MAP message protection.~~

- **MAC Key:**
  MAC Key to be used for ~~MAP message~~integrity protection.

~~**MAP Protection Profile:**~~
~~A MAP Protection Profile (MAP-PP), is an specification of how components in a MAP message over Z_C interface shall be protected. Indicates whether a MAP dialogue needs protection, and if so, indicates for every component of the dialogue the protection mode and mode of operation of the encryption algorithm to be used. In case protection is required, it shall also state whether fallback to unprotected mode is allowed.~~

- **MAP Protection Profile:**
  A MAP Protection Profile (MAP-PP), is an specification of how MAP operations over Z_C interface shall be protected. Indicates whether a MAP operation needs protection, and if so, indicates the protection mode to be used.

- **Fallback to Unprotected Mode Indicator:**
  In case protection is required, this parameter indicates whether fallback to unprotected mode is allowed.

- **SA Lifetime:**
  Defines the actual duration of the SA.

These parameters shall be transferred, in a secure manner, between the respective KACs of the co-operating networks at the Z_A interface.

The possibility to negotiate security attributes shall be provided to some extent, so that both communicating networks may arrange the encryption/MAC algorithms and parameters, the security policy or even the SA lifetime.