3GPP TSG SA WG3 Security — S3#17bis **S3z010005**
23rd April – 24th April
Madrid, Spain

Agenda Item: 7.5 – NDS session
Source: Ericsson
Title: MAP-SA Negotiation and Distribution Procedures
Document for: Discussion and decision

1. Scope and objectives

The main objective of this document is to define the mechanisms and flows for the transport of MAPSec SAs between the KAC and MAP-NEs at Ze interface.

A previous version of 3GPP TS 33.200 v0.3.1 (2001-01) proposed HTTP protocol to be used as transport protocol, and two different approaches: MAPSec SA PUSH procedures and MAPSec SA PULL procedures.

The following is proposed in this document:

1. A general description for the MAP-SA negotiation and distribution procedures,
2. A pure PULL approach to be used both at initiating and receiving side for the MAP-SA distribution procedures at Ze interface,
3. Selection and further development/refinement of the actual protocol at Ze interface shall be performed at CN4.

Additionally, KAC and NE functionality related to MAP Security (including Key Management) are specified.

2. Introduction

According to latest agreements in S3 and security architecture depicted in TS 33.200, a distinction between protocols carried by SS7 and IP based networks is made:

> ***"Native IP based protocols shall be protected at the network level by means of the IPSec protocols and SS7 based protocols are to be protected at the application level."***

The SAs negotiation for IPSec and MAPSec follows different strategies as well:

- For IPSec, the SA negotiation is performed by the same nodes that establish the secure communication (i.e. SEGs).
- For MAPSec, the SA negotiation is logically separated from the MAP nodes, and there is an entity in each network in charge of this task: the KAC. Every MAP-NE capable of setting secure MAP communications towards other MAP-NEs shall incorporate an IP interface to communicate with KAC.

The SAs negotiation shall be done in both cases (IPSec and MAPSec) through IP connectivity employing IKE with IPSec DOI and MAPSec DOI respectively.

The only SS7 protocol to be protected is the MAP protocol.

The proposed architecture in this case is shown in Figure 1.

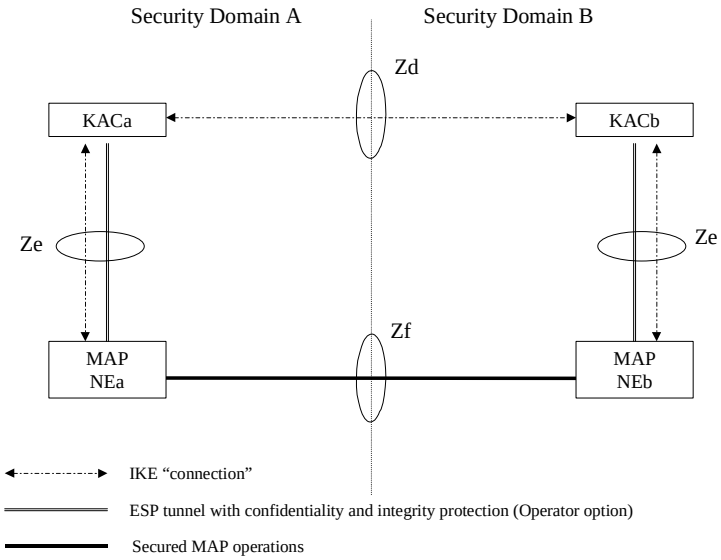

Figure 1. Security Architecture proposed for MAPSec

The following interfaces have been defined for MAPSec:

Zd (KAC-KAC): used to negotiate MAPSec SAs between MAP security domains. The traffic over Zd consists only of IKE negotiations, and employs the MAPSec DOI (being standardised). The SAs negotiated are valid for all the MAP nodes within the security domain.

Ze (KAC-NE): used for transport MAPSec SAs from the KAC to the MAP-NE. The MAP-NE and KAC might be able to establish and maintain an ESP tunnel between them in order to protect the SAs transmission.

Zf (NE-NE): used for MAPSec communication between nodes of the same or different security domain.

A previous version of TS 33.200, v0.3.1, proposed HTTP protocol as a candidate protocol for Ze interface, and two approaches are described to perform MAP-SA transport: PUSH and PULL approaches.

This document proposes that PULL approach is enough in order to perform all required tasks for MAP-SA distribution at Ze interface. The "RequestSA" procedure from a MAP-NE to the KAC is specified in this document. The flows for the MAP-SA negotiation and distribution process are also presented here as well as a description of the required functionality in the KAC and MAP-NEs.

Finally, this document also proposes that the selection and specification of the actual protocol at Ze interface should be performed at CN4 (protocollars).

3. MAP-SA Negotiation and Distribution Procedures

3.1. General Overview

Imagine a network scenario with two MAP-NEs at different Security Domains (NEa and NEb) willing to communicate using MAPSec. Figure 2 presents the proposed procedure for MAP-SA negotiation.

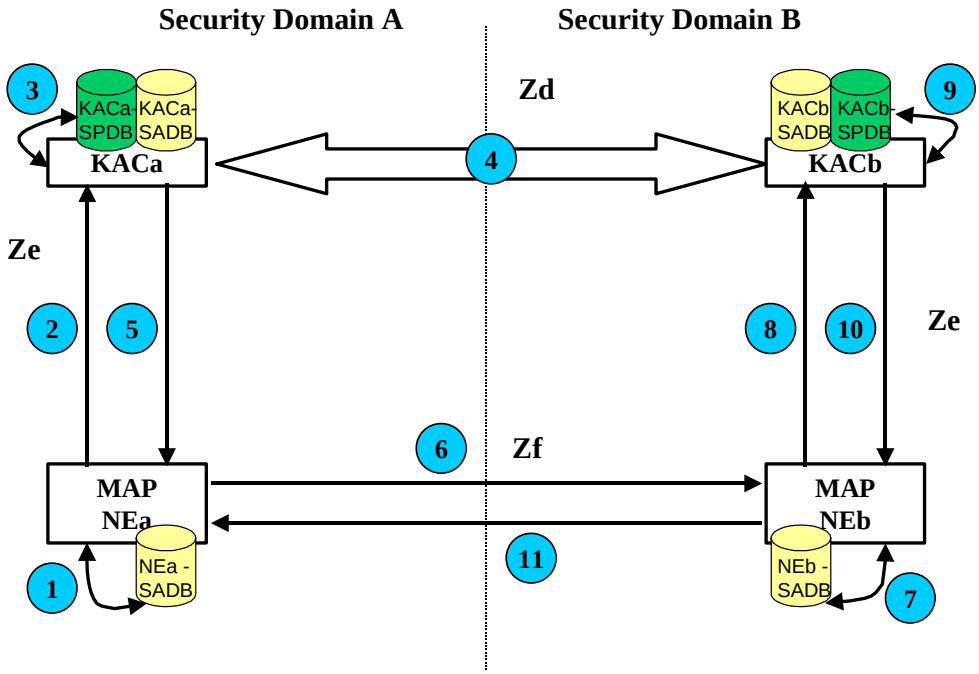

Figure 2. MAP-SA Negotiation and Distribution Procedure

According to the Figure 2, when MAP-NEa (NEa) from Security Domain A wishes to establish a secure communication with a MAP-NEb (NEb) of Security Domain B, the proposed process is the following:

1. NEa looks for a valid SA towards Security Domain B in its SADB. If it owns a valid SA, NEa starts the security protocol MAPSec (refer to step 6 below).
2. If NEa does not own a valid SA, then initiates a “RequestSA” procedure towards KACa, through Ze interface.
3. KACa looks into its SPDB and SADB and checks the action:
   - SPDB in KACa may indicate that communication towards Security Domain B does not need to be secured so KACa response to NEa MAP-SA request includes such indication (refer to step 5 below).

- SPDB in KACa may indicate that secure communication towards Security Domain B is required and KACa has a valid SA in its SADB for that purpose. KACa responds to NEa with the stored SA information (refer to step 5 below).
- SPDB in KACa may indicate that secure communication towards Security Domain B is required but KACa may not have a valid SA in its SADB for that purpose. KACa initiates a MAP-SA negotiation procedure with the KAC in Security Domain B, KACb (refer to step 4 below).

4. If KACa does not have a valid SA, KACa determines the appropriate KACb to negotiate SA according to SA end point, or domain identifier. KACa and KACb negotiate the SA through the Zd interface with IKE protocol using MAPSec DoI. KACb checks its SPDB to accept and complete the negotiation.
5. KACa responds to the “RequestSA” procedure initiated by NEa with a valid SA towards Security Domain B.

   This response to NEa might also indicate that secure communication towards Security Domain B is not required at that moment or that it has been impossible for KACa to provide a valid SA (e.g. problems during the SA negotiation with KACb, unavailability of KACb, etc …).
6. NEa stores information received and applies required actions:
   - NEa generates MAPSec traffic towards NEb.
   - NEa generated unprotected MAP traffic towards NEb.
   - NEa aborts MAP communication towards NEb and any other NE within Security Domain B. NEa shall reattempt the “RequestSA” procedure when a new MAP communication is to be established towards Security Domain where NEb resides.
7. When NEb receives traffic from NEa, it checks its SADB for a valid SA to process traffic from Security Domain A. If NEb already has a valid SA, NEb can then continue security protocol MAPSec (refer to step 11 below).
8. If NEb does not own a valid SA, then initiates a “RequestSA” procedure towards KACb, through Ze interface.
9. KACb looks for the already negotiated and stored SA information.
10. KACb responds to the “RequestSA” procedure initiated by NEb with a valid SA towards Security Domain A.

    This response to NEb might also indicate that secure communication towards Security Domain A is not required at that moment.
11. Finally, NEb can resume MAP communication towards NEa applying MAP Security depending on the content of the SA information received from KACb.

3.2. SA lifetime supervision at KAC and NEs

In order to improve processing time of the first message in a secure communication, the KACs and/or NEs might introduce the option to always maintain SAs alive.

With this option, KACs shall control the SA lifetime and negotiate a new SA before the SA in use expires in order to maintain continuously valid SAs for all or some preconfigured network domains. When a NE requests a SA, the KAC must answer with the recent one.

In a similar way and as a configuration option, NEs might supervise the SA lifetime

and request a new one before the SA in use expires.

The following considerations must be noticed:

- All nodes might try to update their SAs at the same time, so in order to prevent KAC from overload, SA requests from the NEs should be randomised.
- Two SAs can be valid during the same period of time; i.e. KAC might have negotiated a fresh SA before older one has expired.

3.3. Request SA Procedure

According to the MAP-SA negotiation and distribution procedure in figure 2, PULL approach is enough in order to perform SA distribution at Ze interface. Ericsson does not consider PUSH related mechanisms necessary (SubscribeSA, UnsubscribeSA or UpdateSA procedures as outlined in TS 33.200 v0.3.2).

The mechanism is outlined in more detail in Figure 3.

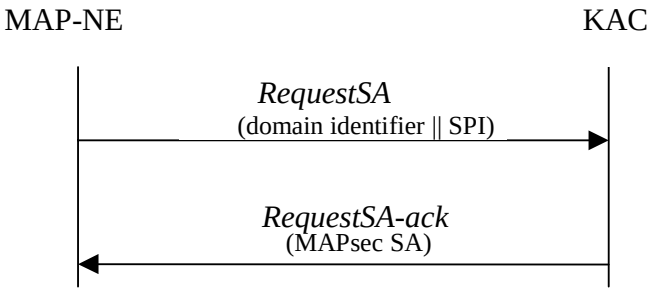

Figure 3. RequestSA procedure

The purpose of this procedure is to provide a MAP-NE with valid MAP-SA information to establish secure MAP communication with another MAP-NE.

The procedure is invoked by a MAP-NE when MAP communication towards another MAP-NE is to be initiated and no valid SA information is available at the MAP-NE SADB. Optionally, the procedure may also be initiated when the MAP-NE is configured to always maintain valid SAs.

The MAP-NE sends a *request SA* to the KAC; this message contains the domain identifier of the Security Domain the MAP-NE wishes to communicate with (i.e. destination PLMNid). In the event, the MAP-NE initiated the procedure with the purpose to refresh an existing SA (just expired or about to), the SPI (pair) of the SA being replaced shall be also included.

The answer from the KAC may include one of the following responses:

a) Valid SA information to secure MAP communication to and from the Security Domain identified in the request.

b) An indication that MAP communication towards/from that specific Security Domain does not need to be secured at that moment. This indication has a limited lifetime (also included in the response) to allow future changes in policy.

c) An error response informing that the KAC is not able to provide the MAP-NE with valid SA information at that moment.

In order to perform this procedure in a secure manner, the KAC and MAP-NE might be able to use IKE to negotiate, establish and maintain an ESP tunnel between them. Whether the tunnel is established is for the MAP-Security domain operator to decide.

This procedure does not allow notification from KAC to MAP-NEs. If SAs are compromised, additional measures shall be applied in order to abort new or secure communication in progress (e.g. MAP Policy).

3.3.1. MAP-SA Information

KACs take information in their SPDBs to negotiate an SA pair (for inbound and outbound traffic respectively). Each component of the MAP-SA pair will be uniquely identified by the PLMNid and an SPI. The MAP-SA information downloaded to the MAP-NE in the course of an "RequestSA" procedure includes the following parameters for each component of the SA pair:

- **Encryption Algorithm Identifier:**
  Identifies the encryption Algorithm and its mode of operation used for confidentiality protection.
- **Encryption Key:**
  Encryption Key to be used for confidentiality protection.
- **MAC Algorithm Identifier:**
  Identifies the MAC Algorithm and its mode of operation used for integrity protection.
- **MAC Key:**
  MAC Key to be used for integrity protection.
- **MAP Protection Profile reference:**
  This field gives a reference to the chosen MAP protection profile. A MAP Protection Profile (MAP-PP), is a specification of how MAP operations over Z_f interface shall be protected. Indicates whether a MAP operation needs protection, and if so, indicates the protection mode to be used. The MAP-NE associates this reference to the actual MAP-PP.
- **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. The expiry of the lifetime shall be given in absolute time.

In the event, the KAC response includes the indication that MAP communication towards/from a specific Security Domain does not need to be secured at that moment, all the fields in the SA information will contain a NULL value except SA-lifetime. The value here will be treated as in the case of a normal MAP-SA (i.e. the MAP-NE will initiate a new "RequestSA" procedure when the SA-lifetime parameter indicates so).

In the event, the KAC response includes the error indication that the KAC is not able to provide the MAP-NE with valid SA information at that moment, the MAP-NE will

abort the MAP communication towards the destination MAP-NE. The MAP-NE shall initiate a new “RequestSA” procedure next time a MAP message towards that security domain is required to be sent.

3.4. Protocol Selection for Ze interface

Ericsson is of the opinion that selection and further development/refinement of the actual protocol at Ze interface shall be performed at CN4 (an LS to inform them about this new task would be required).

4. Description of KAC and NE functionality

This section describes the main requirements for KACs and NEs according to the proposed MAP-SA negotiation and distribution procedures.

4.1. Properties and Tasks of KACs

KACs perform the following operations:

- Negotiate SAs for MAPSec with other KACs belonging to other network operators. This action is triggered either by request for a MAP-SA by a NE or by policy enforcement when MAP-SAs always should be available. MAP-SAs negotiation is performed at Zd interface using IKE protocol with MAPSec DoI.
- Perform refresh of MAP-SAs. Triggered internally by SA lifetime supervision, which is depending on the policies set by the operator and if, it is decided during the negotiation.
- Distribute MAP-SA information to requesting nodes belonging to the same security Domain as the KAC. This is done according to the ‘RequestSA” procedure outlined above.
- (Optional) KAC may be able to establish IPSec connections supporting IKE with IPSec DOI in order to secure transmission of MAP-SAs to the NEs within its security domain.

KACs are also responsible for the maintenance of the following databases:

- KAC-SPDB-MAP: Defines the scope, the security policy, in which MAP-SAs may be negotiated (allowed MAP-PPs, Algorithms, SA-lifetimes, value of “Fallback to unprotected Mode Indicator”). This database is updated on operator initiative in the framework of the roaming agreements.
- KAC-SADB-MAP: Contains actual MAP-SA information as result of the IKE negotiation.
- (Optional) KAC-SPDB-IP: Defines the scope, the security policy, in which IPSec-SAs may be negotiated at the Z_E interface.
- (Optional) KAC-SADB-IP: Containing IPSec-SAs for protection of IP traffic between the KAC and NEs over the Z_E interface.

4.2. Properties and Tasks of MAP-NEs

MAP-NEs perform the following operations:

- Request MAP-SA information to the KAC. This is done according to the "RequestSA" procedure outlined above.
- Supervise MAP-SA lifetimes to initiate new valid SA information once the SA in use has expired. Optionally, the MAP-NE might request new SAs before the previous SAs have expired.
- Secure MAP signalling (i.e. send/receive protected or unprotected messages) according to MAP-SA information received from the KAC.

MAP-NEs are responsible for the maintenance of the following databases:

- NE-SADB-MAP: A database in a NE containing MAP-SA information received from the KAC in the course of a "RequestSA" procedure. MAP-NEs shall control the SAs lifetime and the expired SAs shall be deleted of the database.
- (Optional) NE-SADB-IP: Containing IPSec-SAs for protection of IP traffic between the KAC and NEs over the Z_E interface.

5. Conclusion and Discussion

Ericsson believes that the proposal presented in this document set a solid and consistent basis for the specification of MAP-SA negotiation and distribution mechanisms.

S3 members are kindly asked to consider this proposal in order to be able to reach the following agreements:

1. Agreement on the general overview of the MAP-SA negotiation and distribution mechanisms (chapters 3.1 and 3.2).
2. Agreement on the principles of the "RequestSA" procedure (chapter 3.3).
3. Agreement on requesting CN4 to select and further develop/refine the actual protocol to be used at Ze interface (chapter 3.4) according to the requirements provided in this proposal. If this is agreed, a LS informing CN4 of such request shall be submitted as soon as possible.
4. Agreement on the basic functionality at the KAC and MAP-NEs in relation to MAP Security and Key Management (chapter 4.1. and 4.2).

If these agreements can be reached, the information in this proposal could be included in TS 33.200.