TSG-SA WG3 (Security) meeting #14 **S3-000432**
Oslo, 1st August – 4th August 2000

Agenda Item:

Source: Ericsson

Title: Key management for MAPSec(urity).

Document for: Discussion and decision

1 Introduction

This contribution proposes a key management solution for MAP Security (MAPSec). It discusses required functionality, applicability of IKE and IPSec, proposes Work Items and a time plan. The objective of this paper is to show that IKE based key management can be used, specs can be written in the required timeframe and that it gives an efficient solution from a management as well as implementation point of view.

As an outcome of the discussion we request a clear decision on the principles and the major mechanisms to be used for MAPSec key distribution.

2 Key Management Principles

The key management scheme proposed here follows the basic ideas in previous S3 work. Key Administration Centers (KAC) negotiate keys, algorithms etc to be used by all nodes in one network X when communication with nodes in another network Y (as described in 33.102 v3.4.0). In S3-000331 (Using IKE for Layer I of MAP Security) T-Mobil / T-Nova concludes that an IKE based solution is efficient and viable. In S3-000328 (Use of IPSec IKE for layer 2 key distribution) Motorola proposes the use of IKE and IPSec to protect the distribution of parameters from the KAC to the Network Elements. In another Ericsson contribution S3-000433 (Security Association for MAP Security) we propose to introduce Security Association for MAP security. This contribution expands these ideas into a complete key management architecture.

The key management is based on IP connectivity, which (according to our information) can be assumed to exist between all involved entities.

3 IKE Background

IKE, Internet Key Exchange, is a key management protocol used for dynamically creating security associations for IPSec but it may also be used for other protocols. It is based on ISAKMP, SKEME and Oakley and it consists of two phases: Phase 1 and Phase2. ISAKMP itself does not define any cryptographic algorithms or even what technique is used for establishing keys. Instead the protocol is very general in its design and can be used by different protocols for establishing security associations, SAs. ISAKMP defines five default types whereof IKE uses two of them: 1) Identity Protection Change where the key information is exchanged first and authentication information is sent next and 2) Aggressive Change where the key exchange and authentication payloads are sent all together.

In IKE terminology these two exchanges are called Main Mode and Aggressive Mode respectively and they are used in Phase 1 when the channel between two entities is secured. The Main Mode consists of six messages and the Aggressive Mode consists of three messages and is therefore faster but the identities are revealed. The Aggressive Mode may be used in situations like where the Initiator knows the policy of the Responder which would be the case if operators defined the policy in a roaming agreement.

In Phase 2, the Quick Mode, IKE defines the SAs for other protocols like e.g. IPSec and put the negotiated SAs in a database, the SADB.

Another important database is the SPD, Security Policy Database, which is used by IKE when negotiating SAs. The SPD may be located in e.g. a security gateway or even a KAC. There shall be policies defined for inbound and outbound traffic between two hosts. The policies define amongst other things cryptographic algorithms, key lengths, how many times Phase 2 negotiations can take place before the Phase 1 SAs have to be renegotiated etc. Furthermore the policy has to be set up for both Phase 1 and Phase 2. Today it does not exist any standard for how policies are defined so it is implementation specific. However it is an ongoing standardisation work in IETF for the standardisation of policies. Note that no matter what method is used for key management for MAPSec, is it IKE or any other key management protocol the policies have to be defined anyway. The selectors for looking up the policy for a connection are based on the source identity and the destination identity that in IPSec may be e.g. the IPv4 addresses but for MAPSec it is suggested to use PLMN identifications. In MAPSec additional information might be relevant for the selection of policies.

A vital component for ISAKMP to be able to define SAs in Phase 2 is the DOI, Domain of Interpretation, which defines different parameters like payload formats, exchange types, cryptographic algorithms etc. A DOI specification is a quite complex one and it is a time consuming process to define one from scratch. For this reason it is recommended in RFC2408 to customise an existing DOI rather than designing a new one. In the ISAKMP-header a 32-bit field is reserved for a DOI value which for IPSec takes the value one. IANA maintains all DOI values. It is recommended that new DOI's are RFC's.

Using IKE for MAPSec, Phase 1 of IKE shall be intact and a new DOI for MAPSec shall be defined which will be used by IKE in Phase 2. The design of this DOI shall customise the already existing DOI for IPSec such that it fulfils the requirements for MAPSec. This DOI must be registered with IANA. For a brief information the following shall be defined in a DOI:

1. A situation which is used to determine the required security services e.g. secrecy
2. The set of security policies that must be supported
3. A scheme for naming security information like cryptographic algorithms c.f. e.g. IPSec and Transform ID ESP_DES takes the value 2 etc
4. Security association attributes c.f. IPSec: SA Life Type, SA Life Duration, Key Length etc
5. Payload content e.g. SA payload, Identification Type Values (c.f. IPSec ID_IPV4_ADDR, ID_IPV6_ADDR etc which in the MAPSec case would be PLMNid)

Ericsson anticipates that it is possible to convert the existing IPSec DOI to a MAPSec DOI.

4 Key Management Architecture

4.1 Overview

Refer to figure 1 below. The Key Administration Center, KAC, of each operator is responsible for the establishment and maintenance of the security relationships valid for MAP based communications with other operators' networks. At establishment of a secured MAP connection the KAC uses the Internet Key Exchange protocol (IKE) to negotiate the relationship, the Security Associations (SA), one in each direction, with its counterpart of the operator in question.

The negotiated SAs are stored in a Security Association Database, KAC-SADB, associated with the KAC. There exists at least one pair of SA's regarding MAP communications between any pair of communicating networks. The validity of a SA is time limited, but automatic refresh of the SA can be agreed during the negotiation and will in that case be supervised by the KAC.

Any node of e.g. operator A that needs to secure its MAP communication with a node of operator B gets the currently valid SA to use from the KAC-SADB and stores it its own N-SADB. The node secures its MAP message as appropriate and sends it over the SS7 network to the destination node of operator B. In order for the receiving node to be able to understand the secured message it has to request the valid SA from the SADB of its own network (i.e. of operator B in this example).

The distribution of SA's between KAC and NE's can be protected by IPsec with use of IKE for local key management but there are other alternatives depending on the protocol used. It is proposed that the protection mechanism is left unspecified but that all NE's and the KAC optionally should support IKE/IPSec.

When the key management described above is used for applying MAPSec within one operators network the KAC should negotiate SA's with itself. This is obviously an exceptional case and has to be handled in a corresponding way.

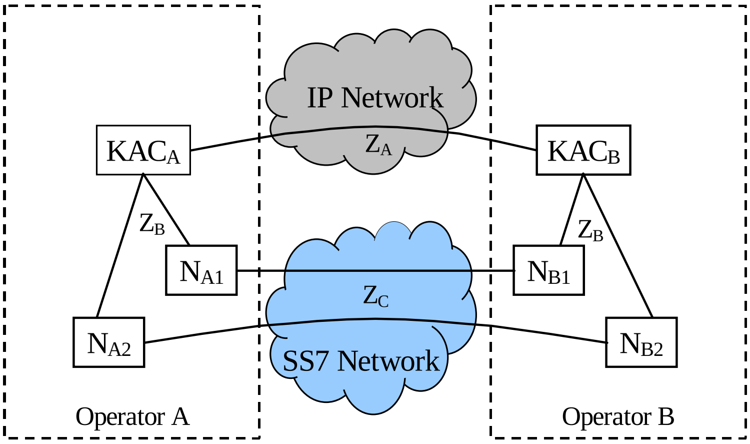

Figure 1. Architecture for MAP key management.

4.2 Definitions

4.2.1 Interfaces

In the proposed security architecture the notation Z_X is introduced to define an interface.

Z_A The inter-networks interface between two KACs. This interface is assumed to rely on IP transport and use IKE as application protocol.

Z_B The intra-network interface between the KAC and a node capable of external communications using secure MAP. The interface is assumed to rely on IP transport using e.g. LDAP or SNMP to distribute the SA information. IPsec might be used to secure the transfer.

Z_C The inter-networks interface between two nodes communicating by using secure MAP. The interface rely on SS7 transport and policing.

4.2.2 Security Associations and Protection Profiles

All SA's are unidirectional.

MAP-SA A MAP Security Association is an IKE negotiated collection of parameters controlling a secured MAP connection over Z_C.

IPSec-SA An IPsec Security Association is an IKE negotiated collection of parameters controlling an IPSec secured connection over Z_B.

MAP-PP A MAP Protection Profile is a specification of how components in a MAP message over Z_C shall be protected.

SPI Security Parameters Index is used to index a SA between two communicating entities.

4.2.3 Databases

The KAC and the NE's have to maintain several databases. These are

KAC-Z_A-SPD A database in the KAC, which defines the scope, the security policy, in which MAP-SA's may be negotiated.

KAC-Z_C-SADB A database in the KAC containing MAP-SA's and the corresponding MAP-PP.

KAC-Z_B-SPD (optional) A database which defines the scope, the security policy, in which IPSec-SA's may be negotiated.

KAC -Z_B-SADB (Optional) A database containing IPSec-SA's for protection of IP traffic between the KAC and NE's.

NE-Z_C-SADB A database in a NE containing MAP-SA's and corresponding MAP-PP's.

NE-Z_B-SADB (Optional) A database in a NE containing IPSec-SA's for protection of IP traffic between the NE and the KAC.

4.3 Functional description/discussion

4.3.1 The Key Administration Center

The KAC has the following functionality incorporated.

- Perform IKE negotiation to establish MAP-SAs with KACs belonging to other operators' networks. This action is triggered either by request for a MAP-SA by a NE or by policy enforcement when MAP-SA's always should be available.
- Perform refresh of MAP-SA's. Triggered internally by IKE SA lifetime supervision, which is depending on the policies set by the operator and if, it is decided during the negotiation.
- Maintain the KAC-Z_C-SADB of valid MAP-SA's and MAP-PP's. MAP-PP's entered and updated on operator initiative.
- Distribute valid MAP-SAs and MAP-PP's to requesting nodes belonging to the same network as the KAC. This is done according to the 'SA negotiation procedure' defined below. The trigger for distribution can be implemented in different ways, see discussion on the Z_B interface below.
- (Option) Perform IKE negotiation and establish IPSec protection with NE's in its own network.

4.3.2 Network Elements

The NE's have the following functionality incorporated.

- Secure MAP according to MAP-PP and MAP-SA for the network with which it communicates.
- Maintain the NE-Z_C-SADB of valid MAP-SA's and MAP-PP's distributed from the KAC.
- Supervise MAP_SA lifetimes in the NE-Zc_SADB.
- (Option) Perform IKE negotiation and establish IPSec protection with the KAC in its own network.

4.3.3 The Z_A Interface and Inter-network MAP-SA negotiation

To establish the MAP-SA for MAP security between two networks IKE with a MAP Domain of Interpretation (DOI) for ISAKMP is used. The MAP DOI has to be developed and it should contain the parameters that can be negotiated. The goal here is to use the IPSec DOI as a starting point and preferably only change interpretation and range of values for the parameters negotiated in and IPSec IKE negotiation.

The SA negotiation should allow for selection of a standard MAP-PP from a small set of standardised MAP-PP's or the use of a private MAP-PP agreed offline between the operators.

4.3.4 The Z_B Interface and MAP-SA distribution

The Z_B interface is used for distribution of MAP-SA's and related information. The principles for MAP-SA distribution could be based on the KAC PUSHing MAP-SA's to all NE's or NE's PULLing the MAP-SA's from the KAC on demand. Adoption of PUSH based distribution guarantees that if a MAP-SA has been negotiated between two networks then it will be available in a NE when required. The KAC can also have central control of updating of SA's when they expire. It also has to handle failures to push a MAP-SA to a NE by regularly trying to resend the SA. The major drawback is that PUSHing SA's will introduce a lot of unneccesary traffic. With a PULL based system only needed MAP-SA's will be distributed. This minimizes the traffic load. On the other hand the distribution must fullfill stricter time requirements.

In the case of adoption of the PUSH principle SNMP could be used to control and update the NE's databases (MIBs). If the PULL principle is adopted then LDAP can be used by the NE's to request information from the KAC. Another possibility in this case might be to the SA info an a AAA server and use the appropriate protocol to fetch the information.

Our initial evaluation favours a PULL based system using LDAP for SA distribution.

If a security mechanism over Z_B is needed than IKE/IPSec should be employed.

4.3.5 The Z_C Interface for MAPSec

The Z_C interface carries secured MAP traffic. The mechanisms to be used and the MAP formats are currently being defined in 29.002. To define the protection of a MAP component a security header is introduced. This header contains information which naturally would be part of the security association. We propose that the header format is changed to only contain the sending PLMN identity and an SPI identifying the MAP-SA used and per message related information like and IV.

4.3.5.1 MAPSec SA content

Today it is suggested to use a security header for MAPSec including parameters such as (note the similarities with IPSec and the IPSec DOI)

1. Sending PLMNid
2. Protection mode (no protection, integrity and authentication, integrity and authentication and confidentiality)
3. Encryption algorithm identifier (BEANO, DES, 3DES, IDEA etc)
4. Mode of operation (ECB, CBC etc)
5. Key version number for encryption algorithm key
6. MAC algorithm identifier (HMAC MD5, HMAC SHA-1 etc)
7. Key version number for hash algorithm key
8. Initialisation vector
9. Component identifier

The information in 2, 3, 4, 5, 6, and 7 together with the used keys should be contained in the SA. Ericsson anticipates that this structure may be mapped on the IPSec DOI such that it is customised to a MAPSec DOI. The protection mode may be compared with AH and ESP in IPSec. Also cryptographic algorithms are similar to what IPSec uses. However Ericsson suggests distinguishing DES_ECB and DEC_CBC by defining them as different algorithms rather than using the mode of operation parameter which is included in the MAP security header.

4.4 MAP-SA negotiation procedure

When a NE needs to communicate, using MAPSec, and it does not know of a valid MAP-SA to use for the receiving network, it contacts the KAC to get MAP-SA´s (inbound and outbound) defined. The following steps define the procedures involved.

1. The NE requests a valid MAP-SA from the KAC
2. The KAC checks its associated MAP-SADB to see if there already is stored valid SA's for MAP connections to the network in question. If the KAC finds stored (valid) MAP-SA´s, see step 7 below.
3. If the SADB does not contain valid MAP-SA's for the requested network, the KAC requests an IKE negotiation to establish them.
4. IKE checks if it has to perform phase 1 of the negotiation (if it has a valid ISAKMP-SA for the other KAC). If not see step 6.
5. The KAC contacts the KAC of the other network and starts phase 1 negotiations (main or aggressive mode depending on the policy set in the ISAKMP-SPD).
6. Then the KAC negotiates a new MAP-SA's by completing an 'IKE phase 2' procedure (quick mode) according to the policy it finds in its associated MAP-SPD.
7. The KAC forwards the MAP-SA to the requesting NE.
8. The node stores the received MAP-SA's and uses it for all communication towards the intended network until the MAP-SA's is no longer valid. (Then it all starts from 1 again.)

5 Deployment

An important aspect in defining the architecture described above has been to allow for a smooth introduction of MAP security. The main concerns being that

- A simple-to-introduce mechanism for trust distribution between operators is needed.
- Not all operators will introduce MAPSec at the same time
- Not all nodes within one operator's network will support MAPSec at the same time.
- A mixed environment of IPv4 and IPv6 may exist.
- Interoperability

Using IKE to negotiate SA's over Z_A allows for different methods to establish trust between the KAC's. In the first phase of deployment preshared keys, agreed upon bilaterally between operators, can be used while later, to automate and allow for simple refresh of trust, AAA based key or certificate distribution or a PKI infrastructure can be used. We propose not to standardise the trust establishment mechanism at the moment.

The use of MAP security will be controlled via the MAP Security Policy Database kept in the KAC. The database could indicate that MAP security should be used for signalling to/from another network while plain MAP should be used to/from another network. To allow for stepwise introduction of MAP security enabled NE's within one network we propose to allow mixed use of plain MAP and secured MAP. Thus the MAP Security Policy must be able to specify such behaviour.

IKE and IPSec are applicable both for IPv4 and IPv6. Other higher level protocols will be independent of the basic IP protocol used.

The solution is based on well-known protocols and simple procedures, which should guarantee interoperability.

6 Workplan/Issues

The main work items foreseen in the specification of the key management architecture proposed above are

- Write stage 2 description of MAPSec key management to be included in 33.102.
- Select algorithms to be supported by MAPSec.
- Write MAPSec Domain Of Interpretation for ISAKMP. Find out if it has to be an RFC.
- Agree on use of PUSH (or PULL) principle for KAC to NE distribution and on the protocol to use.
- Agree on (optional?) protection mechanism for Z_B
- Define database formats for MAP-SPD and MAP-SADB.
- Agree on standard profiles of MAP-PP
- Agree on use of SPI in and format of component headers.
- Update 29.002 to conform to use of MAP-SPD and MAP-SA info.
- Agree on standardisation strategy for trust distribution for IKE. This includes the time schedule and the mechanism to use.

First drafts of the stage 2 description of key management for MAPSec and the MAPsec DOI can be ready to review at the SA3#15 meeting in September.

7 Conclusions

The description of the key management for MAPSec above shows that

- The necessary functionality can be built on established protocols and software, which will enable a speedy implementation and deployment
- Key management procedures common between MAPSec and IPSec.
- IKE includes mechanisms for key refreshing, protection from Denial of Service attacks by using cookies, perfect forward secrecy, possibilities to use standard Diffie Hellman groups or define new ones, digital signatures to name a few.
- Facilitates stepwise deployment.
- Introduction of the PULL principle will minimise storage and communication requirements in the NE's.
- The introduction of SA's will lessen the overhead in MAPsec traffic.