TSG-SA WG3 (Security) meeting #15
Washington, September 12 – 15, 2000

S3-000627

Agenda Item: MAP Security

Source: Ericsson

Title: Update on MAPSec IKE

Document for: Discussion

---

1 Introduction

In this contribution we present some findings on what MAPSec DoI and IKE together with an alternative protocol for SA distribution from the KAC. The findings are focussed on differences between a MAPSec IKE and IPSec IKE and the respective DoI's.

2 MAPSec DoI for IKE

1.1 MAPSec Domain of Interpretation for ISAKMP

RFC2408: ISAKMP places the following significant requirements on a DoI definition:

- Define the interpretation for the Situation field
- Define the set of applicable security policies
- Define the syntax for DoI-specific SA Attributes (Phase II)
- Define the syntax for DoI-specific payload contents
- Define additional Key Exchange types, if necessary
- Define additional Notification Message types, if needed

IANA will not normally assign a DoI value without referencing some public specification, such as an Internet RFC. Without a DoI value assigned by IANA, the MAP SA negotiation over the interface Z_A is not possible. MAPSec DoI for ISAKMP draft *must* be written, since the new DoI is an essential part of the key management architecture.

The following sections define briefly the requirements for MAPSec DoI for ISAKMP.

1.1.1 MAPSec Situation Definition

Within ISAKMP, the Situation provides information that the responder can use to determine how to process incoming SA request. For the MAPSec DoI, the Situation field is always left empty.

1.1.2 MAPSec Security Policy Requirements

The MAPSec DoI does not impose specific security policy requirements on any implementation.

1.1.3 MAPSec Assigned Numbers

The following sections list the Assigned Numbers for the MAPSec DoI: protocol identifiers and transform identifiers.

MAPSec Protocol Identifier defines a value for the Security Protocol Identifier referenced in an ISAKMP Proposal Payload for the MAPSec DoI.

Protocol ID	Value
PROTO_MAPSEC	5

It is recommends that the chosen value should not overlap existing IPsec DoI values.

MAPSec Transform Identifier defines one(?) mandatory transform used to provide data confidentiality (The algorithms are just examples).

Transform ID	Value
RESERVED	0
MAPSEC_SHA1	1
MAPSEC_AES	2

It is recommended that operation mode (e.g. ECB, CBC) is combined to algorithms and not defined as a separate parameter. This will avoid configuration problems amongst other things.

1.1.4 MAPSec Security Association Attributes

The following attributes are needed (as discussed in earlier contributions)

- Protection Profile
- Authentication algorithm for integrity and authentication
- Encryption algorithm for confidentiality
- Encryption and authentication keys
- SA lifetime

1.1.5 MAPSec Payload Content

Defining different MAPSec payloads is outside the scope of this document. At least the following payloads require modifications or a redefinition:

- Security association payload
- Identification payload

1.1.6 MAPSec Key Exchange Requirements

MAPSec DoI does not introduce additional key exchange types.

2 Modifications to IKE

In Phase 1 there are no changes to main mode.

A new Phase 2 mode - the MAP mode, must be introduced. The MAP mode differs from the existing IKE quick mode in the following respects:

- Payloads included to the messages of MAP mode are the same as in Quick Mode but the contents of the payloads differ in the case SA payload and ID payloads.
- Either the identity is never sent or if sent it will be the PLMDID in fqdn or der_gn encoded form (or the key_id).

KEYMAT for MAPSec SA template (as in the present Quick mode)

3 Defining Policies and Structure of KAC-Z_A-SPD

The policy is described as in the RFC 2401 with following changes:

- The lifetime of the MAP SA is not defined as an amount of data transferred, but as lifetime in seconds.
- The generated MAP SA will not be used for processing inbound and outbound traffic in KACs and thus processing choices *discard*, *bypass IPsec* and *apply IPsec* are no applicable.
- The operator defines for which networks MAP SA's are negotiated.

The security policies for MAPSec key management are specified in the KACs' SPD by the network operator. The SPDs in the network elements are derived from the SPD of the KAC in the network. There can be no local security policy definitions for individual NEs.

The SPD can be implemented as a text file to ease the porting to different systems. Text-file based implementation is also easier to alter by possible third parties than a GUI interface. The SPD file contains the information required to implement the security policy and does not require a lot of memory. It can be easily cached to improve the performance of the system (real time requirements).

4 Accessing KAC-Z_C-SADB

HTTP has been suggested as a protocol for fetching MAP SA's from KAC_Z_c_SADB. The KAC should then run a standard WEB server with a standard HTTP database.