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

S3z000018

Agenda Item: -

Source: Ericsson

Title: MAP Security Domain of Interpretation for ISAKMP

Document for: Information

---

1 MAP Security Domain of Interpretation for ISAKMP

The two-tiered key management architecture defined by S3 for MAP Security uses IKE to negotiate MAP-SAs between KACs at Za interface. This requires the definition of a new Domain of Interpretation for MAP Security.

This paper presents to S3 a first draft of the “MAP Security Domain of Interpretation for ISAKMP”.

All S3 members (including those not present at the S3#15bis ad-hoc meeting) are kindly invited to review and comment on this proposal until November 10th. The intention is to submit a revised version to the San Diego IETF meeting if no serious objections are received.

Network Working Group J. Arkko
INTERNET-DRAFT Ericsson
Category: Informational October 2000

The MAP Security Domain of Interpretation for ISAKMP

Status of this Memo

Contents

1. Abstract

In the Global Mobile System (GSM) and Universal Mobile Telecommunication System (UMTS) networks, the MAP protocol plays a central role in the signaling communications between the Network Elements (NEs). The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges, payloads, and processing guidelines that occur within a given Domain of Interpretation (DOI). This document defines the MAP Security DOI (MAPSEC DOI), which instantiates ISAKMP for use with MAP when MAP uses ISAKMP to negotiate security associations.

2. Introduction

2.1. MAP

In the Global Mobile System (GSM) and Universal Mobile Telecommunication System (UMTS) networks, the MAP protocol plays a central role in the signaling communications between the Network Elements (NEs). User profiles, authentication, and mobility management are performed using MAP. MAP is an SS7 protocol and runs over the TCAP, SCCP, and MTP protocol layers, typically using dedicated PCM links.

The mobile networks are moving towards IP-based solutions, and completely IP based networks and new protocols such as SIP will in few years time replace MAP. However, MAP and SS7 signaling networks have to be supported during the transition time, and beyond, due to the need to retain legacy equipment in networks.

2.2. Requirements for a DOI

Within ISAKMP, a Domain of Interpretation is used to group related protocols using ISAKMP to negotiate security associations. Security protocols sharing a DOI choose security protocol and cryptographic transforms from a common namespace and share key exchange protocol identifiers. They also share a common interpretation of DOI-specific payload data content, including the Security Association and Identification payloads.

Overall, ISAKMP places the following requirements on a DOI definition:

- define the naming scheme for DOI-specific protocol identifiers
- 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 needed
- define additional Notification Message types, if needed

For instance, the IP Security DOI [IPDOI] describes the use of ISAKMP in the context of IP Security AH and ESP and the IP Compression protocols. The IP Security DOI also includes the details for how phase 1 authentication and protection of ISAKMP itself is performed between two IP nodes.

2.3. MAP Security

Due to the role of MAP in the authentication process of GSM phones, operators are concerned about its lack of cryptographic security support. For this reason a new protocol header has been developed to protect MAP messages, much in the same way as IPsec ESP protects IP packets. Also similarly, a key management mechanism is needed for MAP. The intention of the standardization entities working on MAP is to reuse an existing key management mechanism, namely ISAKMP, and parts of IKE and the IPsec DOI.

The reaons for wishing to reuse ISAKMP include the following:

- Avoiding the security and complexity pitfalls involved in new protocol design
- Benefits of using the same protocol that IP-based (especially IPv6) nodes already use for other purposes.

The use of IKE and IPsec DOI for MAP Security is possible since the networks employing MAP Security will always have also network-to-network IP connectivity even if MAP and SS7 are still used for the signaling.

The remainder of this document details the instantiation of these requirements for using the GSM MAP protocol and its security to provide authentication, integrity, and/or confidentiality for MAP messages sent between cooperating Network Elements.

For a description of the GSM and MAP architecture, see [???] and [???].

2.4. Network Architecture

The MAP Security protocol may provide confidentiality, integrity, and replay protection services to the MAP messages it transports. The purpose of the MAP Security header in the protocol is to provide enough information to determine the MAP SA and Protection Modes used in securing the MAP operation that follows the header.

Typically, two NEs belong to two different operator networks. The arrangement is shown in Figure 1.

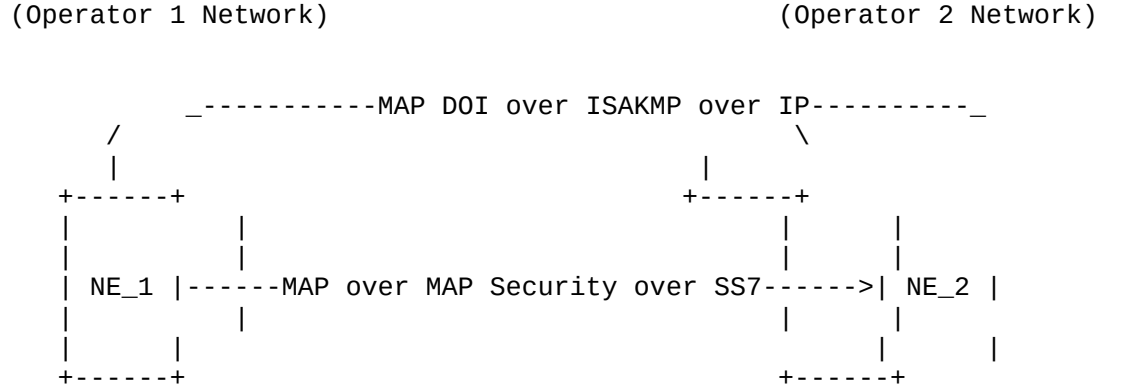

Figure 1. Simple network architecture for MAP Security

(Operator 1 Network) (Operator 2 Network)

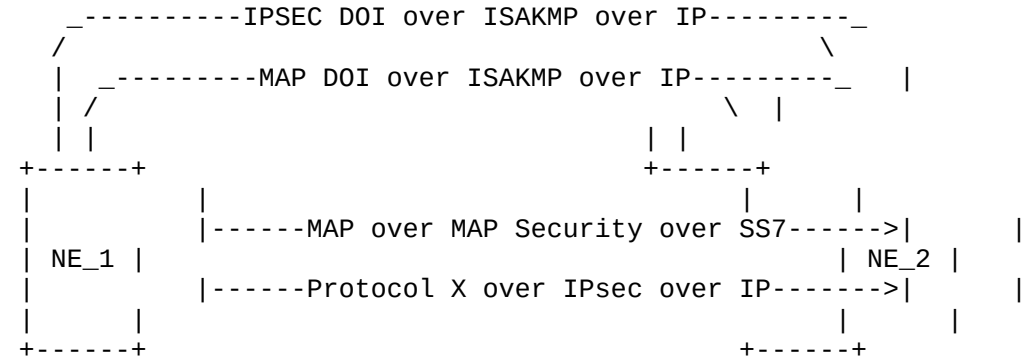

Figure 2. Use of IKE for two purposes.

One benefit of using IKE can be seen in Figure 2. As the network elements use both MAP and another, IP-based protocol X they can use ISAKMP/IKE to negotiate keys for both. In this case, IKE phase 1 needs to be run just once.

In an alternative network arrangement, the Network Elements do not have key management support or direct IP connections to other networks. In this case a Key Administration Center (KAC) handles the negotiations on the behalf of the NEs. This is shown in Figure 2.

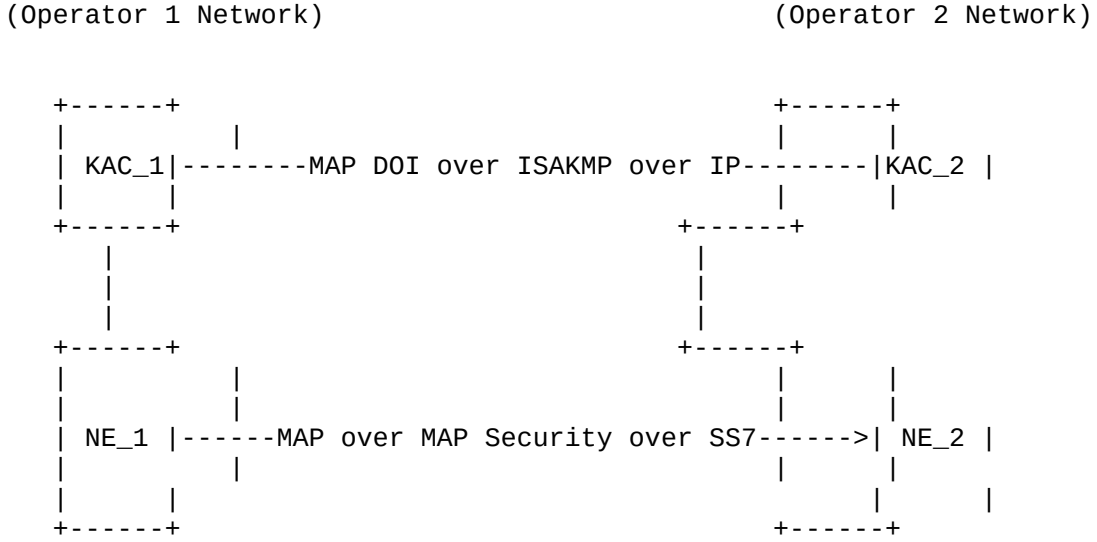

Figure 3. Complex network architecture for MAP Security

In this arrangement, the security of the communications between the NEs and the KAC is of great importance. Security mechanisms or transport protocols for that purpose are, however, not discussed in this document though as an example, IPsec/IKE, IPsec/KINK, MPLS VPNs [MPLS], or ATM Permanent Virtual Connections

could be used.

Only one SA (pair) needs to exist between two networks in this arrangement, even if there is a large number of NEs communicating to the NEs of the other network. (Note that MAP Security employs time stamps instead of sequence numbers, making the simultaneous use of the same SA in multiple NEs possible.)

2.5. Reuse of IPSEC DOI and IKE

The MAP DOI for ISAKMP is always used in devices that have IP connectivity to the peer device. There are no specific requirements set forth by the MAP Security or MAP protocols regarding the identification authentication of the communicating peers. Therefore, all IPSEC DOI definitions and IKE procedures regarding phase 1 of IKE are used unchanged in the MAPSEC DOI. Furthermore, the IKE procedures regarding phase 2 are used unchanged, with the following exceptions:

- Identity types used in phase 2 are different.
- SA payloads are different.
- The procedure for creating keys for MAP Security is different than that for IPsec.

Systems implementing the MAP Security DOI MUST support this DOI using ISAKMP/IKE.

2.6. Reuse of KKMP

The KINK protocol [KINK] uses centralized authenticatin from Kerberos to bypass IKE phase 1 and offer a faster alternative to IKE phase 2. KINK uses directly ISAKMP and IPSEC DOI payload formats, and therefore anything negotiable normally

Systems implementing the MAP Security DOI SHOULD support this DOI using KINK.

3. Terms and Definitions

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC 2119].

4. Definition

4.1 Naming Scheme

Within ISAKMP, all DOI’s must be registered with the IANA in the "Assigned Numbers" RFC [STD-2]. The IANA Assigned Number for the MAP Security DOI (MAPSEC DOI) is TBD (N). Within the MAP Security DOI, all well-known identifiers MUST be registered with the IANA under the MAPSEC DOI. Unless otherwise noted, all tables within this document refer to IANA Assigned Numbers for the MAPSEC DOI. See Section 6 for further information relating to the IANA registry for the MAPSEC DOI.

All multi-octet binary values are stored in network byte order.

4.2 MAPSEC Situation Definition

Within ISAKMP, the Situation provides information that can be used by the responder to make a policy determination about how to process the incoming Security Association request. For the MAPSEC DOI, the Situation field is a four (4) octet bitmask with the following values.

Situation	Value
SIT_IDENTITY_ONLY	0x01

4.2.1 SIT_IDENTITY_ONLY

The SIT_IDENTITY_ONLY type specifies that the security association will be identified by source identity information present in an associated Identification Payload. See Section 4.6.2 for a complete description of the various Identification types. All MAPSEC DOI implementations MUST support SIT_IDENTITY_ONLY by including an Identification Payload in at least one of the Phase I Oakley exchanges ([IKE], Section 5) and MUST abort any association setup that does not include an Identification Payload.

4.3 MAPSEC Security Policy Requirements

The MAPSEC DOI does not impose specific security policy requirements on any implementation. Host system policy issues are outside of the scope of this document.

However, the following sections touch on some of the issues that must be considered when designing an MAPSEC DOI host implementation. This section should be considered only informational in nature.

4.3.1 Protection Profiles

In order to make it possible to establish as small number of SAs as possible in large meshed operator network, and to limit the protection to the most critical MAP messages, the concept of MAP protection profiles has been introduced.

For instance, one profile could mandates the use of MAP Security for all MAP messages, while another could require the use of MAP Security only for all messages containing mobile terminal authentication vectors, and no security for other messages.

These actual profiles are numbered and standardized by the 3GPP [PROF] and are not listed here.

During the IKE phase 2 negotiations between two nodes or networks, they agree on a common protection profile and create a single SA (pair) between themselves. The SA is then either used or not used for individual MAP messages, based on the standardized rules in the particular selected profile.

Note that this is in contrast to the mechanisms used in the IPSEC DOI, where several SA (pairs) may be negotiated, one for each different class of traffic.

4.3.2 Key Management Issues

It is expected that many systems choosing to implement ISAKMP will strive to provide a protected domain of execution for a combined IKE key management daemon. On protected-mode multiuser operating systems, this key management daemon will likely exist as a separate privileged process.

In such an environment, a formalized API to introduce keying material into the TCP/IP kernel may be desirable. The IP Security architecture does not place any requirements for structure or flow between a host TCP/IP kernel and its key management provider.

4.3.3 Static Keying Issues

Static keying is not supported in MAP Security.

4.3.4 Host Policy Issues

It is not realistic to assume that the transition to MAP Security will occur overnight. Host systems must be prepared to implement flexible policy lists that describe which systems they desire to speak securely with and which systems they require speak securely to them. Some notion of proxy firewall addresses may also be required.

A minimal approach is probably a static list of Public Land Mobile Network Identities (PLMN IDs). A PLMN ID is constructed by concatenating the Mobile Country Code (MCC) and by the Mobile Network Code (MNC).

4.3.5 Certificate Management

Host systems implementing a certificate-based authentication scheme will need a mechanism for obtaining and managing a database of certificates.

Secure DNS is to be one certificate distribution mechanism, however the pervasive availability of secure DNS zones, in the short term, is doubtful for many reasons. What’s far more likely is that hosts will

need an ability to import certificates that they acquire through secure, out-of-band mechanisms, as well as an ability to export their own certificates for use by other systems.

However, manual certificate management should not be done so as to preclude the ability to introduce dynamic certificate discovery mechanisms and/or protocols as they become available.

4.4 MAPSEC Assigned Numbers

The following sections list the Assigned Numbers for the MAPSEC DOI: Protocol Identifiers, MAPSEC Transform Identifiers, Security Association Attribute Type Values, ID Payload Type Values, and Notify Message Type Values.

4.4.1 MAPSEC DOI Number

This number is TBD.

4.4.1 MAPSEC Security Protocol Identifier

The ISAKMP proposal syntax was specifically designed to allow for the simultaneous negotiation of multiple Phase II security protocol suites within a single negotiation. As a result, the protocol suites listed below form the set of protocols that can be negotiated at the same time. It is a host policy decision as to what protocol suites might be negotiated together.

The following table lists the values for the Security Protocol Identifiers referenced in an ISAKMP Proposal Payload for the MAPSEC DOI.

Protocol ID	Value
RESERVED	0
PROTO_ISAKMP	1
PROTO_MAPSEC_MAPSEC	TBD

4.4.1.1 PROTO_ISAKMP

The PROTO_ISAKMP type specifies message protection required during Phase I of the ISAKMP protocol. The specific protection mechanism used for the MAPSEC DOI is described in [IKE]. All implementations within the MAPSEC DOI MUST support PROTO_ISAKMP.

NB: ISAKMP reserves the value one (1) across all DOI definitions.

This is exactly as it is in the IPSEC DOI.

4.4.1.2 PROTO_MAPSEC_MAPSEC

The PROTO_MAPSEC_MAPSEC type specifies the use of the MAP Security to protect MAP messages.

4.4.2 MAPSEC ISAKMP Transform Identifiers

As part of an ISAKMP Phase I negotiation, the initiator's choice of Key Exchange offerings is made using some host system policy description. The actual selection of Key Exchange mechanism is made using the standard ISAKMP Proposal Payload. The following table lists the defined ISAKMP Phase I Transform Identifiers for the Proposal Payload for the MAPSEC DOI.

Transform	Value
RESERVED	0
KEY_IKE	1

Implementor's note: This is exactly as it is in the IPSEC DOI.

4.4.2.1 KEY_IKE

The KEY_IKE type specifies the hybrid ISAKMP/Oakley Diffie-Hellman key exchange (IKE) as defined in the [IKE] document. All implementations within the MAPSEC DOI MUST support KEY_IKE.

4.4.3 MAPSEC Transform Identifiers

The following table lists the defined MAPSEC AES Transform Identifier this this transform in the MAPSEC DOI.

Transform ID	Value
RESERVED	0-1
MAPSEC_AES	TBD
MAPSEC_BLOWFISH	TBD
MAPSEC_NULL	TBD

4.4.3.1 MAPSEC_AES

The MAPSEC_AES type specifies a generic MAP Security transform using AES. The actual protection suite is determined in concert with an associated SA attribute list

All implementations within the MAPSEC DOI MUST support this transform.

4.4.3.2 MAPSEC_BLOWFISH

The MAPSEC_BLOWFISH type specifies a generic MAP Security transform using BLOWFISH. The actual protection suite is determined in concert with an associated SA attribute list

All implementations within the MAPSEC DOI SHOULD support this transform,

and it is provided in this specification mainly as a fallback option in case security problems in AES are later discovered.

4.4.3.3 MAPSEC_NULL

The MAPSEC_NULL type specifies a generic MAP Security transform using no encryption. The actual protection suite is determined in concert with an associated SA attribute list. In case both the encryption and the authentication algorithms are NULL, no MAPSEC shall be run between the two nodes.

All implementations within the MAPSEC DOI MUST support this transform.

4.5 MAPSEC Security Association Attributes

The following SA attribute definitions are used in Phase II of an IKE negotiation. Attribute types can be either Basic (B) or Variable-Length (V). Encoding of these attributes is defined in the base ISAKMP specification.

Attributes described as basic MUST NOT be encoded as variable. Variable length attributes MAY be encoded as basic attributes if their value can fit into two octets. See [IKE] for further information on attribute encoding in the MAPSEC DOI. All restrictions listed in [IKE] also apply to the MAPSEC DOI.

Implementor’s note: In general, the attributes describe here behave exactly as the corresponding ones in the IPSEC DOI. The attributes Encapsulation Mode, Compression Dictionary Size, and Compression Private Algorithm are not supported by MAPSEC DOI.

Attribute Types

class	value	type
SA Life Type	1	B
SA Life Duration	2	V
Group Description	3	B
Encapsulation Mode	4	B
Authentication Algorithm	5	B
Key Length	6	B
Key Rounds	7	B
Compress Dictionary Size	8	B
Compress Private Algorithm	9	V
MAP Protection Profile	TBD	B

Class Values

SA Life Type
SA Duration

Specifies the time-to-live for the overall security association. When the SA expires, all keys negotiated under the association (AH or ESP) must be renegotiated. The life type values are:

RESERVED	0
seconds	1

Values 3-61439 are reserved to IANA. Values 61440-65535 are for private use. For a given Life Type, the value of the Life Duration attribute defines the actual length of the component lifetime -- in number of seconds.

If unspecified, the default value shall be assumed to be 28800 seconds (8 hours).

An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.

See Section 4.5.4 for additional information relating to lifetime notification.

Implementor’s note: The semantics and values for these attributes are exactly as they are in the IPSEC DOI, except that kilobyte lifetimes are not supported.

Group Description

Specifies the Oakley Group to be used in a PFS QM negotiation. For a list of supported values, see Appendix A of [IKE].

Implementor’s note: The semantics and values for these attributes are exactly as they are in the IPSEC DOI.

Authentication Algorithm

RESERVED 0
HMAC-MD5 1
HMAC-SHA 2
DES-MAC 3
KPDK 4

Values 5-61439 are reserved to IANA. Values 61440-65535 are for private use.

There is no default value for Auth Algorithm, as it must be specified to correctly identify the applicable transform.

Implementor's note: The semantics and values for these attributes are exactly as they are in the IPSEC DOI except that only HMAC_SHA1 and NULL are mandatory for all MAP Security implementations.

Key Length

RESERVED 0

There is no default value for Key Length, as it must be specified for transforms using ciphers with variable key lengths. For fixed length ciphers, the Key Length attribute MUST NOT be sent.

Implementor's note: The semantics and values for this attributes is exactly as it is in the IPSEC DOI.

Key Rounds

RESERVED 0

There is no default value for Key Rounds, as it must be specified for transforms using ciphers with varying numbers of rounds.

Implementor's note: The semantics and values for this attributes is exactly as it is in the IPSEC DOI.

MAP Protection Profile

The value of this attribute is as defined in section [PROF].

4.5.1 Required Attribute Support

To ensure basic interoperability, all implementations MUST be prepared to negotiate all of the following attributes.

SA Life Type
SA Duration
Auth Algorithm
MAP Protection Profile

4.5.2 Attribute Parsing Requirement (Lifetime)

To allow for flexible semantics, the MAPSEC DOI requires that a conforming ISAKMP implementation MUST correctly parse an attribute list that contains multiple instances of the same attribute class, so long as the different attribute entries do not conflict with one

another. Currently, the only attributes which requires this treatment are Life Type and Duration.

If conflicting attributes are detected, an ATTRIBUTES-NOT-SUPPORTED Notification Payload SHOULD be returned and the security association setup MUST be aborted.

Implementor's note: This is exactly as it is in the IPSEC DOI.

4.5.3 Attribute Negotiation

If an implementation receives a defined MAPSEC DOI attribute (or attribute value) which it does not support, an ATTRIBUTES-NOT-SUPPORT SHOULD be sent and the security association setup MUST be aborted, unless the attribute value is in the reserved range.

If an implementation receives an attribute value in the reserved range, an implementation MAY chose to continue based on local policy.

Implementor's note: This is exactly as it is in the IPSEC DOI.

4.5.4 Lifetime Notification

When an initiator offers an SA lifetime greater than what the responder desires based on their local policy, the responder has three choices: 1) fail the negotiation entirely; 2) complete the negotiation but use a shorter lifetime than what was offered; 3) complete the negotiation and send an advisory notification to the initiator indicating the responder's true lifetime. The choice of what the responder actually does is implementation specific and/or based on local policy.

To ensure interoperability in the latter case, the MAPSEC DOI requires the following only when the responder wishes to notify the initiator: if the initiator offers an SA lifetime longer than the responder is willing to accept, the responder SHOULD include an ISAKMP Notification Payload in the exchange that includes the responder's IPSEC SA payload. Section 4.6.3.1 defines the payload layout for the RESPONDER-LIFETIME Notification Message type which MUST be used for this purpose.

Implementor's note: This is exactly as it is in the IPSEC DOI.

4.6 MAP Security Payload Content

The following sections describe those ISAKMP payloads whose data representations are dependent on the applicable DOI.

4.6.1 Identification Payload Content

The Identification Payload is used to identify the initiator of the Security Association. The identity of the initiator SHOULD be used by the responder to determine the correct host system security policy requirement for the association.

During Phase I negotiations, the ID port and protocol fields MUST be set to zero or to UDP port 500. If an implementation receives any other values, this MUST be treated as an error and the security association setup MUST be aborted. This event SHOULD be auditable.

The following diagram illustrates the content of the Identification

Payload.

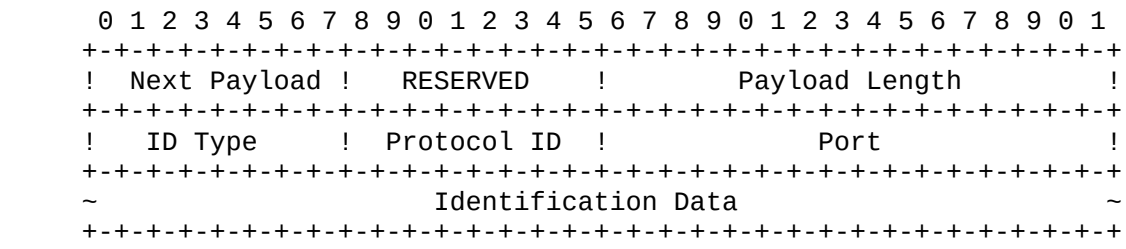

Figure 2: Identification Payload Format

The Identification Payload fields are defined as follows:

- Next Payload (1 octet) - Identifier for the payload type of the next payload in the message. If the current payload is the last in the message, this field will be zero (0).
- RESERVED (1 octet) - Unused, must be zero (0).
- Payload Length (2 octets) - Length, in octets, of the identification data, including the generic header.
- Identification Type (1 octet) - Value describing the identity information found in the Identification Data field.
- Protocol ID (1 octet) - Value specifying an associated IP protocol ID (e.g. UDP/TCP). A value of zero means that the Protocol ID field should be ignored.
- Port (2 octets) - Value specifying an associated port. A value of zero means that the Port field should be ignored.
- Identification Data (variable length) - Value, as indicated by the Identification Type.

4.6.1.1 Identification Type Values

The legal Identification Type field values in phase 1 are as defined in the IPSEC DOI. However, phase 2 identities should MUST conform to the following. The table lists the assigned values for the Identification Type field found in the Identification Payload.

ID Type	Value
RESERVED	0
ID_KEY_ID	11

For types where the ID entity is variable length, the size of the ID entity is computed from size in the ID payload header.

4.6.1.1.1 ID_KEY_ID

The ID_KEY_ID type specifies an opaque byte stream. In MAPSEC DOI, the contents of the data MUST be the the PLMN ID of the initiating or responding party.

4.6.2 IPSEC Notify Message Types

The IPSEC DOI Notify Message types are used in phase 1. In phase

2, the types in this document are used instead. (Implementor's note: the phase 2 types are exactly similar to those in IPSEC DOI.)

ISAKMP defines two blocks of Notify Message codes, one for errors and one for status messages. ISAKMP also allocates a portion of each block for private use within a DOI. The IPSEC DOI defines the following private message types for its own use.

Notify Messages - Status Types	Value
RESPONDER-LIFETIME	24576
REPLAY-STATUS	24577
INITIAL-CONTACT	24578

Notification Status Messages MUST be sent under the protection of an ISAKMP SA in a separate Informational Exchange or as a payload in any Quick Mode exchange.

Nota Bene: a Notify payload is fully protected only in Quick Mode, where the entire payload is included in the HASH(n) digest.

Implementation Note: the ISAKMP protocol does not guarantee delivery of Notification Status messages when sent in an ISAKMP Informational Exchange. To ensure receipt of any particular message, the sender SHOULD include a Notification Payload in a defined Main Mode or Quick Mode exchange which is protected by a retransmission timer.

4.6.2.1 RESPONDER-LIFETIME

The RESPONDER-LIFETIME status message may be used to communicate the MAPSEC SA lifetime chosen by the responder.

When present, the Notification Payload MUST have the following format:

- Payload Length - set to length of payload + size of data (var)
- DOI - set to IPSEC DOI (1)
- Protocol ID - set to selected Protocol ID from chosen SA
- SPI Size - set to four (4) (one MAP Security SPI)
- Notify Message Type - set to RESPONDER-LIFETIME (Section 4.6.2)
- SPI - set to the sender's inbound MAP Security SPI
- Notification Data - contains an ISAKMP attribute list with the responder's actual SA lifetime(s)

Implementation Note: saying that the Notification Data field contains an attribute list is equivalent to saying that the Notification Data field has zero length and the Notification Payload has an associated attribute list.

4.6.2.2 REPLAY-STATUS

The REPLAY-STATUS status message may be used for positive confirmation of the responder's election on whether or not he is to perform anti-replay detection.

When present, the Notification Payload MUST have the following format:

- Payload Length - set to length of payload + size of data (4)
- DOI - set to IPSEC DOI (1)
- Protocol ID - set to selected Protocol ID from chosen SA

- o SPI Size - set to four (4) (one MAP Security SPI)
- o Notify Message Type - set to REPLAY-STATUS
- o SPI - set to the sender's inbound MAP Security SPI
- o Notification Data - a 4 octet value:
  0 = replay detection disabled
  1 = replay detection enabled

4.7 MAPSEC Key Exchange Requirements

The MAPSEC DOI introduces no additional Key Exchange types.

5. Security Considerations

This entire memo pertains to the Internet Key Exchange protocol ([IKE]), which combines ISAKMP ([ISAKMP]) and Oakley ([OAKLEY]) to provide for the derivation of cryptographic keying material in a secure and authenticated manner. Specific discussion of the various security protocols and transforms identified in this document can be found in the associated base documents and in the cipher references.

6. IANA Considerations

This document contains many "magic" numbers to be maintained by the the standardization bodies. In the case of the MAPSEC DOI, the 3GPP handles the assignment of numbers instead of IANA. This section explains the criteria to be used by the 3GPP to assign additional numbers in each of these lists. All values not explicitly defined in previous sections are reserved to 3GPP.

6.1 MAPSEC Situation Definition

The Situation Definition is a 32-bit bitmask which represents the environment under which the IPSEC SA proposal and negotiation is carried out. Requests for assignments of new situations must be accompanied by an RFC which describes the interpretation for the associated bit.

The upper two bits are reserved for private use amongst cooperating systems.

6.2 MAPSEC Security Protocol Identifiers

The Security Protocol Identifier is an 8-bit value which identifies a security protocol suite being negotiated. Requests for assignments of new security protocol identifiers must be accompanied by an RFC which describes the requested security protocol. [AH] and [ESP] are examples of security protocol documents.

The values 249-255 are reserved for private use amongst cooperating systems.

6.3 MAPSEC ISAKMP Transform Identifiers

The ISAKMP Transform Identifier is an 8-bit value which identifies a key exchange protocol to be used for the negotiation. Requests for assignments of new ISAKMP transform identifiers must be accompanied by an RFC which describes the requested key exchange protocol. [IKE] is an example of one such document.

The values 249-255 are reserved for private use amongst cooperating systems.

6.4 MAPSEC MAP Security Transform Identifiers

The MAP Security Transform Identifier is an 8-bit value which identifies a particular algorithm to be used to provide security protection for MAP messages. Requests for assignments of new transform identifiers must be accompanied by an RFC which describes how to use the algorithm within the framework.

The values 249-255 are reserved for private use amongst cooperating systems.

6.5 MAPSEC Security Association Attributes

The MAPSEC Security Association Attribute consists of a 16-bit type and its associated value. MAPSEC SA attributes are used to pass miscellaneous values between ISAKMP peers. Requests for assignments of new MAPSEC SA attributes must be accompanied by an Internet Draft which describes the attribute encoding (Basic/Variable-Length) and its legal values. Section 4.5 of this document provides an example of such a description.

The values 32001-32767 are reserved for private use amongst cooperating systems.

6.6 MAPSEC Identification Type

The MAPSEC Identification Type is an 8-bit value which is used as a discriminant for interpretation of the variable-length Identification Payload. Requests for assignments of new Identification Types must be accompanied by an RFC which describes how to use the identification type.

The values 249-255 are reserved for private use amongst cooperating systems.

6.7 MAPSEC Notify Message Types

The MAPSEC Notify Message Type is a 16-bit value taken from the range of values reserved by ISAKMP for each DOI. There is one range for error messages (8192-16383) and a different range for status messages (24576-32767). Requests for assignments of new Notify Message Types must be accompanied by an Internet Draft which describes how to use the identification type.

The values 16001-16383 and the values 32001-32767 are reserved for private use amongst cooperating systems.

6.8 MAPSEC Protection Profiles

The MAPSEC Protection Profile values are 8-bit values used for in decisions regarding actual protection of individual MAP messages. The values are defined [PROF] and new values must be accompanied by a 3GPP contribution which describes the semantics of the profile.

The values 249-255 are reserved for private use amongst cooperating systems.

7. Key Derivation for MAP Security

7.1 IKE

MAP Security requires two sets of keys, one for each direction, just as in the case of IPSEC SAs. Both need authentication and encryption keys. For one direction of an SA, these two keys are taken from the key material as follows (see also Figure 4.)

- The authentication key is taken first and then the encryption key.

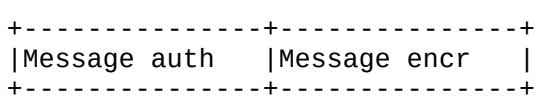

Figure 4. Use of derived key material for MAPSEC

Furthermore, it is possible that the Key Administration Centers (KACs) are used. Then just one key is negotiated on the behalf of whole set of NEs. Note that MAP Security uses timestamps instead of sequence numbers in order to prevent replay attacks, so the same SAs can be used by multiple senders.

If PFS is not needed, and KE payloads are not exchanged, the new keying material is defined as

```
    KEYMAT = prf(SKEYID_d, protocol | SPI | Ni_b | Nr_b).
```

If PFS is desired and KE payloads were exchanged, the new keying material is defined as

```
    KEYMAT = prf(SKEYID_d, g(qm)^xy | protocol | SPI | Ni_b | Nr_b)
```

The referenced symbols are defined as follows:

- prf is the negotiated, keyed pseudo-random function-- often a keyed hash function-- used to generate a deterministic output that appears pseudo-random.
- SKEYID_d is defined by IKE [IKE].
- g(qm)^xy is the shared secret from the ephemeral Diffie-Hellman exchange of this Quick Mode.
- "protocol" and "SPI" are from the ISAKMP Proposal Payload that contained the negotiated Transform.
- Ni_b indicates the body of the initiator’s Nonce payload from IKE [IKE].
- Nr_b indicates the body of the responder’s Nonce payload from IKE [IKE].

A single SA negotiation results in two security assocations-- one inbound and one outbound. Different SPIs for each SA (one chosen by the initiator, the other by the responder) guarantee a different key for each direction. The SPI chosen by the destination of the SA is used to derive KEYMAT for that SA.

For situations where the amount of keying material desired is greater than that supplied by the prf, KEYMAT is expanded by feeding the results of the prf back into itself and concatenating results until the required keying material has been reached. In other words,

```
KEYMAT = K1 | K2 | K3 | ...
where
  K1 = prf(SKEYID_d, [ g(qm)^xy | ] protocol | SPI | Ni_b | Nr_b)
  K2 = prf(SKEYID_d, K1 | [ g(qm)^xy | ] protocol | SPI | Ni_b |
  Nr_b)
  K3 = prf(SKEYID_d, K2 | [ g(qm)^xy | ] protocol | SPI | Ni_b |
  Nr_b)
  etc.
```

This keying material (whether with PFS or without, and whether derived directly or through concatenation) MUST be used with the negotiated SA.

7.2 KINK

In KINK, during the establishment of SAs the initiator and responder each provide random nonces that add entropy to the KDC supplied session key in order to derive the SA keying material (KEYMAT).

```
  KEYMAT = prf(Secret, Ni [ | Nr ])
```

where

- o prf is as presented in section 7.1.

- o Secret is the secret derived fro the Kerberos ticket. It is as defined in KINK [KINK].

- o Ni and and Nr are the nonces of the initiator and responder, respectively.

The function is initially called with the session key found in the service ticket used for Secret and is called recursively with the resulting KEYMAT until it has generated proper number of bits. Rules regarding the optionality of the Nr are as defined in KINK [KINK].

8. Open Issues

The exact nature of the MAP Security header and its placement between the MAP and the TCAP layers is still under discussion in 3GPP's S3 group. The exact list of required algorithms, size of IV fields, and so on may change.

9. Intellectual property rights

Ericsson has patent applications which may cover parts of this technology. Should such applications become actual patents and be determined to cover parts of this specification, Ericsson intends to provide licensing when implementing, using or distributing the technology under openly specified, reasonable, non-discriminatory terms.

10. Acknowledgments

This document is derived from the work done by Rolf Blom, David Castellanos Zamora, Krister Boman, Anders Liljekvist and others at Ericsson, and Tatu Ylonen and others at SSH Communications Security Corp.

11. References

[AH] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[ARCH] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[DEFLATE] Pereira, R., "IP Payload Compression Using DEFLATE", RFC 2394, August 1998.

[ESP] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[ESPCBC] Pereira, R., and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[ESPNULL] Glenn, R., and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

[DES] Madson, C., and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[HMACMD5] Madson, C., and R. Glenn, "The Use of HMAC-MD5 within ESP

and AH", RFC 2403, November 1998.

[HMACSHA] Madson, C., and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[IKE] Harkins, D., and D. Carrel, D., "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[IPCOMP] Shacham, A., Monsour, R., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 2393, August 1998.

[ISAKMP] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[IPSDOI] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[KINK] M. Froh, M. Hur, D. McGrew, S. Medvinsky, M. Thomas, J. Vilhuber, "Kerberized Internet Negotiation of Keys (KINK)", draft-ietf-kink-kink-00.txt, Cybersafe, Motorola, Cisco. Work In Progress, September 2000

[LZS] Friend, R., and R. Monsour, "IP Payload Compression Using LZS", RFC 2395, August 1998.

[OAKLEY] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

[PROF] N.N. "MAP Protection Profiles". Work In Progress, 3GPP, 2000.

[MPLS] E. Rosen, Y. Rekhter, "BGP/MPLS VPNs", RFC 2547, March 1999.

[X.501] ISO/IEC 9594-2, "Information Technology - Open Systems Interconnection - The Directory: Models", CCITT/ITU Recommendation X.501, 1993.

[X.509] ISO/IEC 9594-8, "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework", CCITT/ITU Recommendation X.509, 1993.

12. Author’s Address

Jari Arkko
Oy LM Ericsson Ab
02420 Jorvas
Finland

Phone: +358 40 5079256
EMail: jari.arkko@ericsson.com

Full Copyright Statement