

13 September, 2001

Sophia Antipolis, France

Source: Ericsson

Title: MAPSEC Version 03 and Status

Document for: MAPSEC, R5

Agenda Item: TBD

1. Introduction

This contribution reports on the latest modifications and status of the MAPSEC DOI, the automatic key management feature for 3GPP R5 release.

2. Modifications

A new version, 03, of the Internet Draft appears in the IETF directories soon. In this version the following modifications have been done:

- A number of editorial modifications, such as those reported in [Alcatel].
- Attribute numbers have been selected so that they are less likely to collide with future IPsec numbers.
- The relationship between IKE and MAPSEC DOI has been clarified in view of the possible future descendants of IKE. MAPSEC DOI is assigned a new port, and does not share the same port with IPsec/IKE.
- The use of the identity types in Phase 2 has been clarified such that only the MAPSEC specific identities may be used.
- The rules for using Situation field have been clarified to apply only to Phase 2.
- The notifications which are relevant for MAPSEC DOI have been clarified.

3. Discussion Items

Out of the suggestions made in [Alcatel], all have been adopted except for the use of SHA1 for MAPSEC itself (not Phase 2). The use of AES-CBC-MAC was already agreed upon by the SA3 Phoenix meeting, so this was also reflected in the DOI document. We've set the Phase 1 integrity algorithm to be AES CBC MAC as well.

Suggestions made in [Alcatel2] and even earlier by Siemens have already been incorporated earlier.

While the MAPSEC DOI has been mentioned a couple of times in various discussions, it hasn't really been discussed and no IETF input has been given to it during this period.

4. IETF and IKE Situation

The IETF Security directors Steven Bellovin, Marcus Leech, and Jeff Schiller published a statement [Bellovin] in the beginning of August. The position statement refers to the complexity of the IKE protocol, and asks for a temporary freeze on the development of new features to IKE, until its options are cut down or a replacement protocol has been developed. This statement was widely publicised and caused extensive discussion in the IETF, even fear of similar security problems such as those experienced in the WEP protocol. However, the directors later clarified their statement by noting that they do not know of serious security vulnerabilities, would like to cut down the number of options in the protocol in order to simplify analysis, the freeze has been public knowledge in the relevant working groups for almost a year already, the statement refers only to IKE and not IPsec in general, and that they allow current major IETF work items to proceed including extensions that affect IKE (such as NAT traversal or IPsec Remote Access).

At the same time, discussions have arisen in IETF around the so called Son-of-IKE protocol. This is also an effort that has been in place for some time. At the time this is being written, we do not know if this is a better documented IKE, simply cut-down version of the current IKE with options such as Revised Public Key Encryption or Aggressive Mode taken away, or if it is a completely new protocol. Nor is it clear when this effort will be completed.

The question that is relevant for 3GPP, however, is whether this affects somehow our MAPSEC DOI development. As the MAPSEC DOI is the work item of the 3GPP and intended only as an Informational RFC, the discussion in the Working Groups does not really affect it. However, the IETF Security directors still have to accept the document as not being in conflict with existing IETF work items. The question mark, however, is if the directors consider MAPSEC DOI as a "New IKE feature". Ericsson would like to argue the following:

- 3GPP networks need this functionality now. They do not have a possibility to wait – possibly many years – for a new key management protocol.
- Given that we are not changing IKE, MAPSEC DOI shouldn't really be seen as a new feature. It should rather be seen as introducing new "client" protocols for IKE, beyond the current AH and ESP.
- We should ensure that MAPSEC DOI can easily be moved on top of a new key management protocol, should one be widely adopted in the future. Further SA3 work on this matter is encouraged. Preliminary analysis indicates that this should be the case, given the possibility of defining new "security protocols" and parameters specific to them.
- We should ensure that implementations of MAPSEC DOI do not come too mixed up with IKE implementations. Even if code reuse is desired and used, the protocols should be seen as separate in terms of port number they run on, management of "magic number" spaces, and should e.g. be implemented as separate "daemons" in order to minimize the danger of a hole in one side of the implementation or protocol affecting the other.

In any case, it seems prudent to check the issue with the IETF Security directors.

5. Conclusions

Requested modifications to the MAPSEC DOI have been made and a new document version exists. The SA3 is kindly requested to review the document and once it feels the document is stable enough, to decide that it shall be sent forward to the editorial publishing process in order to gain an Informational RFC status. Ericsson proposes that all comments be received to the Sophia meeting in September, or few weeks thereafter, so that the document can be submitted to the RFC Editor before the SA3 Sydney meeting.

Ericsson undertakes to contact IETF Security directors to check that there are no effects of the IKE development freeze on MAPSEC DOI.

SA3 is encouraged to ensure that the MAPSEC DOI can easily be moved on top of new key management protocols, should such be available in the future.

6. References

- [Alcatel] Alcatel, „Comments on MAPsec DOI –02 Internet Draft“, S3-010254 (S3-010338). May 2001.
- [Alcatel2] Alcatel, „Comments on draft-arkko-map-doi-01.txt“, S3-010223 (S3-010337). April, 2001.
- [Bellovin] S. Bellovin, M. Leech, J. Schiller. „Position Statement on IKE development“, <http://www.vpnc.org/ietf-ipsec/mail-archive/msg01078.html>. August 2001.

Network Working Group
INTERNET-DRAFT
Category: Informational
<draft-arkko-map-doi-03.txt>
September 2001

J. Arkko
R. Blom
Ericsson
10

The MAP Security Domain of Interpretation for ISAKMP

Status of this Memo

This document is an Internet Draft and is in full conformance with all provisions of Section 10 of RFC2026 [Bra96]. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and working groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

To learn the current status of any Internet Draft, please check the "lid-abstracts.txt" listing contained in the Internet Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Australia), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

The distribution of this memo is unlimited. It is filed as <draft-arkko-map-doi-01.txt>, and expires August 15, 2001. Please send comments to the authors.

Contents

1. Abstract
2. Terms and Definitions
3. Introduction
 - 3.1. MAP
 - 3.2. Requirements for a DOI
 - 3.3. MAP Security
 - 3.4. Network Architecture
 - 3.5. Reuse of IPSEC DOI and IKE
4. Definition

- 4.1 Naming Scheme
- 4.2 MAPSEC Situation Definition
 - 4.2.1 SIT_IDENTITY_ONLY
- 4.3 MAPSEC Policy Requirements
- 4.4 MAPSEC Assigned Numbers
 - 4.4.1 MAPSEC DOI Number
 - 4.4.1.1 MAPSEC Security Protocol Identifier
 - 4.4.1.1.1 PROTO_MAPSEC
 - 4.4.2 MAPSEC Transform Identifiers
- 4.5 MAPSEC Security Association Attributes
 - 4.5.1 Required Attribute Support
 - 4.5.2 Attribute Negotiation
 - 4.5.3 Lifetime Matching
- 4.6 MAP Security Payload Content
 - 4.6.1 Identification Payload Content
 - 4.6.2 Notify Message Types
- 4.7 MAPSEC Key Exchange Requirements
- 5. Security Considerations
- 6. IANA Considerations
 - 6.1 MAPSEC Situation Definition
 - 6.2 MAPSEC Security Protocol Identifiers
 - 6.3 MAPSEC MAP Security Transform Identifiers
 - 6.4 MAPSEC Security Association Attributes
 - 6.5 MAPSEC Identification Type
- 7. Key Derivation for MAP Security
- 8. Modification History
- 9. Intellectual property rights
- 10. Acknowledgments
- 11. References
- 12. Author's Address

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 document defines the MAP Security Domain of Interpretation (MAPSEC DOI), which instantiates ISAKMP for use with MAP. This new DOI is essentially an exact copy of how IKE works, except that it negotiates other protocols than AH and ESP in Phase 2 and runs on another port number.

2. 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].

3. Introduction

3.1. 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 exchange, 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.

3.2. 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:

- o define the naming scheme for DOI-specific protocol identifiers
- o define the interpretation for the Situation field
- o define the set of applicable security policies
- o define the syntax for DOI-specific SA Attributes (Phase II)
- o define the syntax for DOI-specific payload contents
- o define additional Key Exchange types, if needed
- o 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.

This document defines the MAPSEC Domain of Interpretation. This new DOI is essentially an exact copy of how IKE works, except that it negotiates other protocols than AH and ESP in Phase 2. Also, MAPSEC DOI uses only a subset of all the features in IKE. MAPSEC DOI is separated from IKE as a new DOI rather than an extension of the current one in order to allow the two protocols to have different port numbers, name spaces, and change control in the future. Given that a subset of IKE is used unchanged, this gives also the possibility of updating MAPSEC DOI to use a new protocol later, should IKE be developed further or replaced by new protocols.

This document version specifies only the Phase 2 of ISAKMP/IKE. Therefore, this document leaves the specification of the Phase 1 details for the IP Security DOI [IPDOI]. For the sake of completeness, this document explains all issues related to the Phase 2, though in many cases it just refers to e.g. parts of the IKE RFC or the IP Security DOI.

It is envisioned that future development in algorithms, security protocols, and policy representation will be fast. Therefore, this specification defines only the framework for the MAPSEC Phase 2, and leaves the authentication algorithm, MAPSEC transform, and the definition of a policy element called the protection profile to the 3GPP Technical Specifications that are applicable at any current time. This ensures that this document does not have to be modified upon the development of a new authentication algorithm, for instance.

3.3. 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 reasons for wishing to reuse ISAKMP include the following:

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

The remainder of this document details the instantiation of these

requirements for using the GSM MAP protocol and its security to provide protection for MAP messages sent between cooperating Network Elements (NEs).

For a description of the MAP protocol, see [MAP].

3.4. Network Architecture

The MAP Security protocol and its key management part provides authentication, 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.

MAPSEC DOI and IKE are used to set up Security Associations for nodes implementing MAPSEC. While the MAP protocol usually runs over SS7, the MAPSEC DOI and IKE are always run over IP. It is therefore assumed that nodes or networks implementing MAPSEC always have IP connectivity in addition to the SS7 connectivity.

The network architectures where the MAPSEC DOI can be run include but are not limited to the one defined by 3GPP [NDSEC]. In the 3GPP architecture the MAPSEC is typically run between two different network operators, and the same SAs are shared by a number of NEs.

It is possible that the nodes using MAPSEC DOI and IKE also have some other, IP traffic to protect. The MAPSEC DOI allows a single Phase 1 IKE to be used for the negotiation of both MAP and IP traffic protection using different Phase 2 exchanges and DOI identifiers.

As in IKE, the MAPSEC DOI allows only symmetric Security Associations to be set up. That is, a pair of SAs is always created for the incoming and outgoing directions. These SAs differ only with respect to the keys, SPIs, and peer identities but all other parameters including the algorithms will have the same values.

3.5. Reuse of IPSEC DOI and IKE

For Phase 1, all IPSEC DOI definitions [IPSDOI] and IKE procedures [ISAKMP, IKE] MUST be used unchanged in the MAPSEC DOI, including the way that peers are authenticated. However, the MAP Security DOI relaxes the full implementation requirements. The following

exceptions to the full requirements are used:

- o All MAPSEC DOI communications shall run on port TBD instead of the standard IKE port 500. This applies to both Phase 1 and 2.
- o Support for Perfect Forward Secrecy (PFS) is not required. An implementation that receives a Phase 2 negotiation request with PFS on MAY decline the negotiation.
- o Only one identity type, ID_FQDN, MUST be implemented for phase 1. Other identity types specified in [IPSDOI] SHOULD be implemented.
- o Only the AES encryption [AESESP] and AES CBC MAC [AESMAC] algorithms MUST be implemented as ISAKMP encryption and hash operations.
- o Only IPv6 is mandatory. [??? - this is currently being discussed by the SA2 and SA3.]

Implementor's note: IKE [IKE] specifies that all implementations MUST support authentication through pre-shared secrets and SHOULD support public key based authentication. All implementations also MUST support Main Mode. Note also that IKE allows the deletion of an existing SA, which all implementations of this DOI MUST be able to handle.

Furthermore, the IKE procedures regarding phase 2 are used unchanged, with the following exceptions:

- o Identity types used in phase 2 are different.
- o SA payloads are different.
- o There are no MAPSEC-specific phase 2 notifications.
- o The procedure for creating keys for MAP Security is different than that for IPsec.

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. The MAPSEC DOI also makes use of several numbers defined by the 3GPP Technical Specification [NDSEC].

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

4.2 MAPSEC Situation Definition

Within ISAKMP, the Situation field 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 in Phase 1 is handled as specified by the IPSEC DOI [IPSDOI]. In Phase 2, the Situation field is a four (4) octet bitmask with the following value.

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 two Identification Payloads in the Phase 2 exchange, and MUST abort any association setup that fails to do so.

4.3 MAPSEC Policy Requirements

The policy requirements for nodes implementing the MAPSEC DOI are beyond the scope of this document. However, it is required that systems be able to specify their policies with respect to the MAP traffic in terms of so called Protection Profiles as defined in [NDSEC]. These Protection Profiles indicate the need for a particular kind of protection based on the type of the MAP message. For the purposes of this document a Protection Profile is a 16 bit number that is agreed upon during the SA negotiation.

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	0-1
PROTO_MAPSEC	TBD

4.4.1.2 PROTO_MAPSEC

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

4.4.2 MAPSEC Transform Identifiers

The following table lists the reserved MAPSEC Transform Identifiers.

Transform ID -----	Value -----
RESERVED	0-1

Actual MAP Transform Identifiers are defined in the 3GPP Technical Specification [NDSEC], which currently specifies only one, the use of AES in stream cipher mode. All implementations within the MAPSEC DOI MUST support that 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: The attributes described here behave exactly as the corresponding ones in the IPSEC DOI, unless specified explicitly otherwise. For the purposes of reusing IPsec DOI code, parameters not used by MAPSEC DOI have the type reserved (values 4, 8, and 9).

Attribute Types

class	value	type
SA Life Type	1	B
SA Life Duration	2	V
Group Description	3	B
RESERVED	4	-
Authentication Algorithm	5	B
Key Length	6	B
Key Rounds	7	B
RESERVED	8	-
RESERVED	9	-
MAP Protection Profile	100	B

Class Values

SA Life Type
SA Duration

Specifies the time-to-live for the overall security association. When the SA expires, the SA MUST be renegotiated. MAPSEC messages using the expired SA MUST no longer be either sent or accepted as input. The life type values are:

RESERVED	0
seconds	1
RESERVED	2

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.

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 0-4

This specification only lists the reserved values. Actual Authentication Algorithm values are defined in the 3GPP Technical Specification [NDSEC], which currently defines only one, the use of AES in CBC MAC mode. That authentication algorithm MUST be supported by all MAPSEC and MAPSEC DOI implementations.

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

Implementor's note: The first five values are reserved by the IPSEC DOI.

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. The definition of MAPSEC transforms in the 3GPP Technical Specifications such as [NDSEC] MUST specify if the use of Key Length is necessary and what the legal values are.

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 attribute is exactly as it is in the IPSEC DOI.

MAP Protection Profile

The value of this attribute is a 16-bit entity as defined in [NDSEC].

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
- Authentication Algorithm
- Key Length
- MAP Protection Profile

4.5.2 Attribute Negotiation

If an implementation receives a defined MAPSEC DOI attribute (or attribute value) which it does not support, an ATTRIBUTES-NOT-SUPPORTED 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 choose to continue based on local policy.

Implementor's note: This is exactly as it is in the IPSEC DOI. However, there are no special lifetime attribute parsing requirements as only time-based lifetimes are supported.

4.5.3 Lifetime Matching

Offered and locally acceptable SA lifetimes must match exactly under MAPSEC in order for the responder to select an SA.

Implementor's note: This is simplified from the IPSEC DOI which required notifications. In the MAPSEC DOI lifetime notifications are not defined and hence not used.

4.6 MAP Security Payload Content

The SA Payloads that the Initiator and the Responder exchange control the Security Associations that actually get installed. The attributes discussed above are a part of the SA Payloads. For a definition of a

MAPSEC SA, see [NDSEC].

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.

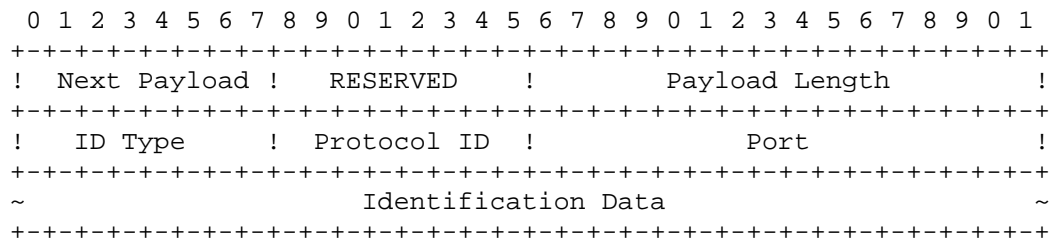


Figure 2: Identification Payload Format

The Identification Payload fields are defined as follows:

- o 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).
- o RESERVED (1 octet) - Unused, must be zero (0).
- o Payload Length (2 octets) - Length, in octets, of the identification data, including the generic header.
- o Identification Type (1 octet) - Value describing the identity

information found in the Identification Data field.

- o 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. In the MAPSEC DOI, value of zero MUST always be used in Phase 2.

- o Port (2 octets) - Value specifying an associated port. A value of zero means that the Port field should be ignored. In the MAPSEC DOI, value of zero MUST always be used in Phase 2.
- o Identification Data (variable length) - Value, as indicated by the Identification Type.

The legal Identification Type field values in Phase 1 are as defined in the IPSEC DOI. However, Phase 2 identities MUST conform to the following. The table lists the assigned values for the Identification Type field found in the Identification Payload. (Values from 0 to 11 are reserved by the IPsec DOI for the purposes of code reuse.)

ID Type	Value
-----	-----
RESERVED	0-11
ID_PLMN_ID	12

In MAPSEC DOI, the ID_PLMN_ID type specifies PLMN ID of the Initiator or the Responder. The PLMN ID MUST be represented as defined in section 17.7.8 of [MAP], i.e. be a three octet data item with the Mobile Country Code (MCC) followed by the Mobile Network Code (MNC). The size of the PLMN ID MUST correspond to the size in the ID payload header.

4.6.2 Notify Message Types

There are no DOI-specific Notify Message types for the MAPSEC DOI in Phase 2.

Note however, Phase 1 uses of course standard ISAKMP and IPSEC DOI notifications that are defined in section 3.14.1 of [ISAKMP] and section 4.6.3 of [IPSDOI], respectively. Even Phase 2 of the MAPSEC DOI uses standard ISAKMP notifications.

(Implementor's note: The reason why MAPSEC DOI doesn't need the same Phase 2 DOI-specific notifications is the following. MAPSEC does not allow turning replay protection on or off which makes the use of REPLAY-STATUS unnecessary. Responder lifetimes are required to be exactly the same as the initiator lifetimes, which makes the use

of RESPONDER-LIFETIME unnecessary. INITIAL-CONTACT notification on the other hand is used exclusively in Phase 1, and is therefore applicable also for MAPSEC DOI in Phase 1.)

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. (IANA will still define the DOI numbers, including the DOI number for this DOI.)

6.1 MAPSEC Situation Definition

The Situation Definition is a 32-bit bitmask which represents the environment under which the MAPSEC SA proposal and negotiation is carried out. Requests for assignments of new situations must be accompanied by a 3GPP Technical Specification 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 a 3GPP Technical Specification which describes the requested security protocol.

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

6.3 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 a 3GPP Technical Specification which describes how to use the algorithm within the framework.

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

6.4 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 a 3GPP Technical Specification 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.

Requests for new values for existing attributes must be accompanied also by a 3GPP Technical Specification. Such specifications describe the semantics of the new values.

6.5 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 a 3GPP Technical Specification which describes how to use the identification type.

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

7. Key Derivation for MAP Security

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

The keys are derived using exactly the same procedure as in section 5.5 of RFC 2409 [IKE].

Implementor's note: The same procedure is used in order to ease specification and implementation, but it should be noted that one of the parameters to the derivation process, protocol, is the constant PROTO_MAPSEC and does not vary in negotiations.

8. Modification History

The following modifications have been made to the -01 and -02 versions of this draft:

- o Section 3.5 now specify a profile for the use of IKE. Since the -02 version, Main Mode has been mandated, and SA deletion has become mandatory.
- o All MAPSEC-specific phase 2 notifications have been removed for simplicity.
- o AES-MAC has been specified instead of HMAC_SHA1. Note that Phase 1 has been specified to use AES and SHA1 since no RFC exists yet to define the use of AES-MAC for IKE Phase 1.
- o Some formatting modifications have been made.
- o Attribute parsing requirements were simplified since only a single kind of lifetimes are supported.
- o MAP_BLOWFISH has been removed since 3GPP hasn't defined it.
- o MAP_NULL has been removed and protection profiles are expected to be used instead to signify that no security is needed.
- o Rules for assigning new numbers within this DOI have been clarified. Since -02, it has also been made clear which numbers are defined in this document (such as the attribute numbers) and which ones are defined in the 3GPP Technical Specifications (such as the protection profile numbers).
- o Kerberized Internet Negotiation of Keys (KINK) is no longer referenced in this document.
- o Since version -02, ISAKMP protocol and transform identifiers have been removed from this document, and the introduction clarified to state that this document involves only the definition of Phase 2 elements.
- o Since version -02, the MAPSEC transform, Authentication Algorithm, and Protection Profile values have been left to be defined by 3GPP Technical Specifications.
- o References have been completed in version -02.
- o The format of the PLMN Id has been specified in -02.
- o In version -02, there are no longer private use value

space for attribute values.

- o In version -02, the size of the protection profile entity has been specified to be 16 bit.
- o Version -02 no longer copies the key derivation text from IKE, but references it.
- o Version -02 no longer describes the network architectures other than pointing to the 3GPP specifications and noting that other architectures are also possible.
- o In version -02 the mandated notification message types have been clarified.

- o Port and protocol fields in the Identity payload have been mandated to be always zero for MAPSEC since version -02.
- o The use of several key lengths in the context of e.g. AES has been clarified in -02.
- o Section 4.3 has been replaced by a brief policy comment since version -02. Possible future requirement to always implement certificate handling may have to be accompanied by clear specifications on how certificate management has to be performed by MAPSEC DOI nodes.
- o References to the IPSEC DOI, ISAKMP, and IKE requirements have been clarified to be relevant for Phase 1 only in section 3.5 and 4.6.2.
- o In version -03, the rules regarding notifications inherited from IPsec DOI and ISAKMP have been clarified.
- o In version -03, several editorial modifications have been made.
- o In version -03, the attribute numbers in MAPSEC DOI have been assigned values that are further beyond the are currently used by IPsec. This has been done in order to facilitate code reuse by allowing the same header files to be used for both MAPSEC DOI and IPSEC DOI.
- o In version -03, the use of certain type of identities in Phase 2 has been clarified to be a MUST.
- o In version -03, it has been clarified that any Situation field rules specified here apply only to Phase 2.
- o PFS support has been made optional.
- o Phase 1 has been clarified to use AES CBC MAC, not SHA1 in order to streamline all 3GPP protocols to use AES-based protocols.
- o References to the [NDSEC] have been updated to note the latest algorithms.
- o In view of the situation regarding new IKE extensions in IETF, the relationship of the MAPSEC DOI to IKE has been clarified. It has also been assigned to run on a different port than IKE.

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 the SA3 group of 3GPP. The authors wish to thank in particular David Castellanos-Zamora, Krister Boman, Anders Liljekvist, Eeva Munter and others at Ericsson, and Tatu Ylonen and others at SSH Communications Security Corp, Marc Blommaert, Dirk Kroeselberg, and Ulrich Wiehe at Siemens, and Olivier Paridaens at Alcatel. This document is also currently undergoing review of the SA3 group.

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.
- [ESP] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.
- [IKE] Harkins, D., and D. Carrel, D., "The Internet Key Exchange (IKE)", RFC 2409, November 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.
- [OAKLEY] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.
- [NDSEC] 3rd Generation Partnership Project, Technical Specification Group SA3, Security "Network Domain Security; MAP Application Layer Security (Release 4)", 3GPP TS 33.200, (Work In Progress), January, 2001.

- [MPLS] E. Rosen, Y. Rekhter, "BGP/MPLS VPNs", RFC 2547, March 1999.
- [MAP] 3rd Generation Partnership Project, Technical Specification Group Core Network, "Mobile Application Part (MAP) Specification (Release 4)", 3GPP TS 29.002, September, 2000.
- [AESESP] S. Frankel, S. Kelly, R. Glenn, "The AES Cipher Algorithm and Its Use With IPsec", draft-ietf-ipsec-ciph-aes-cbc-01.txt. Work In Progress, IETF, November 2000.

[AESMAC] M. Dworkin. "Recommendation for Block Cipher Modes of Operation". NIST Special Publication 800-XX, July 2001.

12. Authors' Addresses

Jari Arkko
Oy LM Ericsson Ab
02420 Jorvas
Finland

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

Rolf Blom
Ericsson Radio Systems AB
SE-16480 Stockholm
Sweden

Phone: +46 8 58531707
EMail: rolf.blom@era.ericsson.se

Full Copyright Statement

Copyright (C) The Internet Society (1998). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for

copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

