

Content Requirements for ISAKMP Notify Messages

Status of This Memo

This document is an Internet Draft and is in full conformance with all provisions of [Section 10 of \[RFC2026\]](#). 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>.

Comments on this document should be sent to the IETF IPsec WG discussion list (ipsec@lists.tislabs.com).

Abstract

The ISAKMP and DOI RFCs [RFC2408, [RFC2407](#)] specify error and status message types for use in ISAKMP NOTIFY messages, but in some cases do not specify that any additional clarifying data be carried in the messages. In these cases, it is difficult to determine which SA corresponds to the received NOTIFY message. While the DOI RFC specifies content and formats for additional data in the currently defined IPSEC status messages, no such requirements are currently specified for ISAKMP NOTIFY messages. This document provides content and format recommendations for those messages.

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

Table of Contents

1. Overview	3
1.1 Requirements Terminology	3
1.2 Reader Prerequisites	4
1.3 Document Organization	4
1.4 Backwards Compatibility	4
2. General Formatting Considerations	4
3. ISAKMP NOTIFY Error Messages	7
3.1 INVALID-PAYLOAD-TYPE	7
3.2 DOI-NOT-SUPPORTED	8
3.3 SITUATION-NOT-SUPPORTED	9
3.4 INVALID-COOKIE	9
3.5 INVALID-MAJOR-VERSION	10
3.6 INVALID-MINOR-VERSION	10
3.7 INVALID-EXCHANGE-TYPE	11
3.8 INVALID-FLAGS	11
3.9 INVALID-MESSAGE-ID	12
3.10 INVALID-PROTOCOL-ID	12
3.11 INVALID-SPI	13
3.12 INVALID-TRANSFORM-ID	13
3.13 ATTRIBUTES-NOT-SUPPORTED	14
3.14 NO-PROPOSAL-CHOSEN	15
3.15 BAD-PROPOSAL-SYNTAX	15
3.16 PAYLOAD-MALFORMED	16
3.17 INVALID-KEY-INFORMATION	16
3.18 INVALID-ID-INFORMATION	17
3.19 INVALID-CERT-ENCODING	17
3.20 INVALID-CERTIFICATE	18
3.21 CERT-TYPE-UNSUPPORTED	18
3.22 INVALID-CERT-AUTHORITY	19
3.23 INVALID-HASH-INFORMATION	19
3.24 AUTHENTICATION-FAILED	20
3.25 INVALID-SIGNATURE	20
3.26 ADDRESS-NOTIFICATION	21
3.27 NOTIFY-SA-LIFETIME	21
3.28 CERTIFICATE-UNAVAILABLE	22
3.29 UNSUPPORTED-EXCHANGE-TYPE	22
3.30 UNEQUAL-PAYLOAD-LENGTHS	23
4. ISAKMP Notify Status messages	23
4.1 CONNECTED	24
4.2 RESPONDER-LIFETIME	24
4.3 REPLAY-STATUS	25

4.4 INITIAL-CONTACT	25
5. Security Considerations	26
6. Editors' Addresses	26
7. References	27
8. Acknowledgements	27
9. Full Copyright Statement	27

[1. Overview](#)

The ISAKMP and DOI RFCs [RFC2408, [RFC2407](#)] specify error and status message types for use in ISAKMP NOTIFY messages, but in some cases do not specify that any additional clarifying data be carried in the messages. In many cases, it is difficult to determine which SA corresponds to the received NOTIFY message. Such determination requires that additional information be placed in the notification data section of the NOTIFY payload. While the DOI RFC specifies content and formats for additional data in the currently defined IPSEC status messages, no content or formatting requirements are currently specified for ISAKMP NOTIFY messages.

Many of the ISAKMP NOTIFY messages may apply to either phase 1 or phase 2 negotiations. In some cases, the context of the message makes clear what transaction it refers to, e.g. if the NOTIFY message pertains to the ISAKMP (phase 1) SA upon which it is received. However, there are cases in which ambiguities may arise. For example, there may be multiple phase 2 SAs negotiated using a single phase 1 SA, and these may be simultaneously under negotiation. A NOTIFY message received via the parent phase 1 SA may apply to any of the phase 2 SAs, but the receiver may not be able to determine which.

In order to be truly useful, NOTIFY messages must, at minimum, allow the receiver to determine which transaction the message corresponds to. As indicated above, in some cases this information may be entirely derived from information contained in the ISAKMP header (cookies and message ID). However, in many cases, and in particular with respect to phase 2 negotiations, the correct context cannot be ascertained without additional information. In some of those cases, the relevant information may be carried in the predefined notify payload fields. In others, this is not enough, and in such cases additional information may be carried in the notify payload data field.

In addition to the need to determine which SA a NOTIFY message

corresponds to, it would also be useful to know more precisely what problem was encountered. For example, an INVALID-PAYLOAD message would be far more useful if one could determine exactly which payload was at issue. Such additional data would be very useful when diagnosing error conditions, and also would provide useful information for auditing purposes. This document provides content and format recommendations for ISAKMP NOTIFY messages which are aimed at providing the additional granularity required to make these messages truly useful.

[1.1](#) Requirements Terminology

Kelly, Kivinen

Expires May, 2001

[Page 3]

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

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 [\[RFC2119\]](#).

[1.2](#) Reader Prerequisites

[\[RFC2407\]](#), [\[RFC2408\]](#), and [\[RFC2409\]](#) are prerequisites to understanding the material presented here. While not strictly necessary, reader familiarity with [\[RFC2401\]](#), [\[RFC2402\]](#), [\[RFC2406\]](#), and with general IP security concepts will further facilitate understanding.

[1.3](#) Document Organization

In the following section is a discussion of general format considerations for all notify messages. Following that, the NOTIFY messages are presented in 2 sections: ISAKMP error messages, and ISAKMP status messages. It is possible that a later revision of this document will address IPSEC error/status messages, but some of those NOTIFY message types are currently addressed in [\[RFC2407\]](#).

Within each section, messages are detailed in individual subsections. Following the example of [\[RFC2407\]](#), each message payload is detailed field-by-field. Where appropriate, additional information regarding the circumstances under which each message arises, along with relative payload variations under those circumstances, is included.

[1.4](#) Backwards Compatibility

The IPsec DOI [[RFC2407](#)] document defines some notification types, along with the data contained in the associated notification data fields. Those definitions do not conform with the definitions in this document. In the interest of backwards compatibility, pains have been taken to accommodate these differences in the definitions offered in this document.

When new use of notification data is defined in any document that uses the IPsec DOI ([RFC 2407](#)), regardless of the key exchange protocol the usage MUST follow the generic format described in this document (i.e. the attribute list encoding of the notification data). These new types may be either allocated from IANA or from the private use range.

[2.](#) General Formatting Considerations

The ISAKMP notify payload contains a number of fields meant to convey contextual information regarding the event precipitating the message. Following is an enumeration of the notify payload fields:

(payload type/length fields omitted)

- o Domain of Interpretation (4 octets) - Identifies the DOI under which this notification is taking place.
- o Protocol-Id (1 octet) - Specifies the protocol identifier for the current notification. Examples might include ISAKMP, IPSEC ESP, IPSEC AH, OSPF, TLS, etc.
- o SPI Size (1 octet) - Length in octets of the SPI as defined by the Protocol-Id.
- o Notify Message Type (2 octets) - Specifies the type of notification message.
- o SPI (variable length) - Security Parameter Index. The receiving entity's SPI. The length of this field is determined by the SPI Size field.
- o Notification Data (variable length) - Informational or error data transmitted in addition to the Notify Message Type.

In many cases, the information contained in the notify payload is insufficient to fully identify the session or transaction for which the error(s) occurred, and in these cases the Notification Data field MAY be used to convey additional information. In order to provide for uniform processing of the notification data field, class attributes are defined below for ISAKMP NOTIFY messages, and notification data MUST be encoded using these attributes.

Attribute encoding is discussed in [[RFC2408](#)], and that discussion is not repeated here, except for the following notes. Attribute encoding types are either Basic (B) or Variable-length (V). Encoding of these attributes is defined in the [[RFC2408](#)] as Type/Value (Basic) and Type/Length/Value (Variable-length). Attributes described as Basic MUST NOT be encoded as Variable. Variable attributes MAY be encoded as basic attributes if their value can fit into two octets.

Attribute Classes

Type Description	Value	Encoding Type
Type of Offending Payload	3	B
Offending Payload Data	4	V
Error Position Offset	5	B

Kelly, Kivinen

Expires May, 2001

[Page 5]

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

Error Text Describing the Problem	6	V
Error Text Language	7	V
Message Id of the Offending Negotiation	8	V
Exchange Type of Negotiation	9	B
Invalid Flag Bits	10	B
Suggested Proposal	11	V
Notification Attribute Version	12	B

Values 131-16383 are reserved to IANA. Values 16384-32767 are for private use among mutually consenting parties. Values 0, 1, and 2 are reserved for backwards compatibility, and MUST not be used in any other notifications than RESPONDER-LIFETIME and REPLAY-

STATUS. The RESPONDER-LIFETIME notification data is an attributes list containing attributes of class 1 and 2. The REPLAY-STATUS notification data is a 32-bit integer containing the values 0 or 1 (meaning the first 2 bytes are 0, thus decoding as an attribute class of 0). Note that when the attribute class of 0 is detected, the rest of the data does not conform to format of an attribute list.

Attribute Type Descriptions

Type of Offending Payload

Payload type of the offending payload encoded as a 16 bit integer.

Offending Payload Data

Offending payload data including the generic header. Note that next payload type in the notify payload itself points to the next payload beyond the notification data. Likewise, the next payload type in the offending payload contains the value placed there by the original sender, and does not reference any payloads within the notify message.

Error Position Offset

Byte offset of the error position from the beginning of the offending payload. Presence of this attribute implies the presence of the offending payload data attribute. That is, when this attribute is present, there MUST also be a corresponding offending payload attribute.

Error Text Describing the Problem

Text describing the problem. (ISO-10646 UTF-8 encoding).

Error Text Language

Error text language tag (as defined in [RFC 1766](#)). When this attribute is present, there MUST also be a corresponding error text attribute.

Message Id of the Offending Negotiation

Message id of the offending negotiation encoded has 4 byte value.

Exchange Type of Negotiation

Exchange type of the offending negotiation. Encoded as 16 bit integer.

Invalid Flag Bits

Invalid flags (valid flags are masked out) Encoded as 16 bit integer.

Suggested Proposal

Optional proposal suggestion to be used in case of failed negotiation due to policy mismatch.

Notification Attribute Version

Indicates the version of this document from which encodings were derived. MUST be the first attribute in the notification data if notification data is included, and MUST contain the value 0x0001. Because this attribute is always first, it can be used as a magic cookie, i.e. if the notification data begins with bytes 0x80, 0x0C, 0x00, 0x01, then it most likely follows the formatting guidelines described in this document.

Note that implementations may not recognize some or all of these attributes, and in some cases, inclusion of some attributes within specific notify messages will be optional. In such cases, implementations MUST ignore unrecognized attributes.

[3. ISAKMP NOTIFY Error Messages](#)

This section contains NOTIFY error messages which are usually specific to ISAKMP (phase 1) Security Associations (SAs). Some of these messages may also apply to the negotiation of IPsec (phase 2) SAs. In such cases, provision is made for use of the appropriate SPI (and other) values. These NOTIFY message types are defined in [\[RFC2408\]](#).

[3.1 INVALID-PAYLOAD-TYPE](#)

that an unrecognized or invalid payload type was received.

Phase: 1 or 2

Differentiators: Cookies vs SPI,
Subject payload (and/or type)
Message ID

Payloads: All

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

- o Payload Length - set to length of payload + size of data (var)
- o DOI - set to the current DOI if available, or set to zero (0) to indicate ISAKMP DOI.
- o Protocol ID - set to selected Protocol ID from chosen SA if available; set to zero (0) to indicate ISAKMP SA.
- o SPI Size - set to either zero (0) or sixteen (16)
- o Notify Message Type - set to INVALID-PAYLOAD-TYPE
- o SPI - set to empty or to the ISAKMP cookies for the failed negotiation.
- o Notification Data - SHOULD contain the type of the offending payload, and MAY contain the offending payload, the message ID associated with the payload, and error text describing the problem.

[3.2](#) DOI-NOT-SUPPORTED

The DOI-NOT-SUPPORTED error message may be used to communicate that an unrecognized or unsupported DOI value was received.

Phase: 1 or 2

Differentiators: Cookies vs SPI, Protocol ID,
subject DOI, message ID

Payloads: SA

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to 0 (ISAKMP DOI)
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to either zero (0) or sixteen (16)
- o Notify Message Type - set to DOI-NOT-SUPPORTED
- o SPI - set to empty or to the ISAKMP cookies for the failed negotiation.

- o Notification Data - SHOULD contain the offending payload and the message ID associated with the payload. It MAY also contain the error position offset, and error text describing the problem.

[3.3](#) SITUATION-NOT-SUPPORTED

The SITUATION-NOT-SUPPORTED error message may be used to communicate that an unrecognized or unsupported situation value was received.

Phase: 1 or 2
Differentiator: Cookies vs SPI, Protocol ID,
offending payload, message ID
Payloads: SA

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to ISAKMP DOI
- o Protocol ID - set to zero (0)
- o SPI Size - set to either zero (0) or sixteen (16)
- o Notify Message Type - set to SITUATION-NOT-SUPPORTED
- o SPI - set to empty or to the ISAKMP cookies for the failed negotiation.
- o Notification Data - SHOULD contain the offending payload and the message ID associated with the payload. It MAY also contain the error position offset, and error text describing the problem.

[3.4](#) INVALID-COOKIE

The INVALID-COOKIE error message may be used to communicate that an invalid ISAKMP cookie was received. Invalid cookies are those cookies for which there is no matching SA. This message applies to a few different situations:

- o one of the cookies in the pair is not valid
- o neither of the cookies in the pair are valid

Phase: 1 or 2
Differentiator: Cookies, message ID
invalid cookie(s) in SPI field
Payloads: ISAKMP header

When present, the Notification Payload MUST have the following

format:

- o Payload Length - set to length of payload + size of data
- o DOI - set to 0 (ISAKMP DOI)
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to sixteen (16)
- o Notify Message Type - set to INVALID-COOKIE
- o SPI - set to the ISAKMP cookies for the failed negotiation.
- o Notification Data - SHOULD contain the message ID of the offending negotiation, and MAY contain error text describing the problem.

[3.5](#) INVALID-MAJOR-VERSION

The INVALID-MAJOR-VERSION error message may be used to communicate that this portion of the ISAKMP version is invalid or unsupported.

Phase: 1 or 2
Differentiator: Cookies, message ID
invalid version
Payloads: ISAKMP header

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to 0 (ISAKMP DOI)
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to sixteen (16)
- o Notify Message Type - set to INVALID-MAJOR-VERSION
- o SPI - set to the ISAKMP cookies for the failed negotiation.
- o Notification Data - SHOULD contain the message ID of the offending negotiation, and MAY contain error text describing the problem.

[3.6](#) INVALID-MINOR-VERSION

The INVALID-MINOR-VERSION error message may be used to communicate that this portion of the ISAKMP version is invalid or unsupported.

Phase: 1 or 2
Differentiator: Cookies, message ID,
invalid version
Payloads: ISAKMP header

When present, the Notification Payload MUST have the following

format:

- o Payload Length - set to length of payload + size of data
- o DOI - set to 0 (ISAKMP DOI)
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to sixteen (16)
- o Notify Message Type - set to INVALID-MINOR-VERSION
- o SPI - set to the ISAKMP cookies for the failed negotiation.
- o Notification Data - SHOULD contain the message ID of the offending negotiation, and MAY contain error text describing the problem.

[3.7](#) INVALID-EXCHANGE-TYPE

The INVALID-EXCHANGE-TYPE error message may be used to communicate that that an unrecognized or invalid ISAKMP exchange type was received.

Phase: 1 or 2
Differentiator: Cookies, message ID
invalid exchange type in notify data
Payloads: ISAKMP header

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to 0 (ISAKMP DOI)
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to sixteen (16)

- o Notify Message Type - set to INVALID-EXCHANGE-TYPE
- o SPI - set to the ISAKMP cookies for the failed negotiation.
- o Notification Data - SHOULD contain the message ID of the offending negotiation and the invalid exchange type, and MAY contain error text describing the problem.

[3.8](#) INVALID-FLAGS

The INVALID-FLAGS error message may be used to communicate that one or more of the received ISAKMP header flags were unrecognized or invalid. Cases where flags are invalid include the following:

- o The encryption bit is unset/set when it should/shouldn't be
- o The commit bit is unset/set when it should/shouldn't be
- o The auth-only bit is unset/set when it should/shouldn't be

Kelly, Kivinen

Expires May, 2001

[Page 11]

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

Phase: 1 or 2
 Differentiator: Cookies, message ID
 invalid flags
 Payloads: ISAKMP header

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to 0 (ISAKMP DOI)
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to sixteen (16)
- o Notify Message Type - set to INVALID-FLAGS
- o SPI - set to the ISAKMP cookies for the failed negotiation.
- o Notification Data - SHOULD contain the message ID of the offending negotiation and the invalid exchange type, invalid flags attribute having only the invalid flags bits set (i.e valid bits are masked off), and MAY contain error text describing the problem.

[3.9](#) INVALID-MESSAGE-ID

The INVALID-MESSAGE-ID error message may be used to communicate that the message ID in the received message is unrecognized or invalid.

Phase: 1 or 2
Differentiator: Cookies, message ID
Payloads: ISAKMP header

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to 0 (ISAKMP DOI)
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to sixteen (16)
- o Notify Message Type - set to INVALID-MESSAGE-ID
- o SPI - set to the ISAKMP cookies for the failed negotiation.
- o Notification Data - SHOULD contain the message ID of the offending negotiation, and MAY contain error text describing the problem.

[3.10](#) INVALID-PROTOCOL-ID

The INVALID-PROTOCOL-ID error message may be used to communicate that an invalid or unsupported protocol ID was received as part of a

Kelly, Kivinen

Expires May, 2001

[Page 12]

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

proposal payload.

Phase: 1 or 2
Differentiator: message ID, proposal payload
Payloads: Proposal

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to zero (0)
- o Notify Message Type - set to INVALID-PROTOCOL-ID
- o SPI - empty
- o Notification Data - SHOULD contain the offending SA payload, error offset position, and the message ID from the offending negotiation. It MAY contain error text describing the problem.

[3.11](#) INVALID-SPI

The INVALID-SPI error message may be used to communicate that an invalid SPI was received as part of a proposal payload.

Phase: 1 or 2
Differentiator: Cookies, message ID, offending payload, protocol ID
Payloads: Proposal

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to PROTO_ISAKMP, PROTO_IPSEC_ESP, or PROTO_IPSEC_AH
- o SPI Size - set to size of subject SPI
- o Notify Message Type - set to INVALID-SPI
- o SPI - set to the invalid SPI
- o Notification Data - SHOULD contain the offending SA payload, error offset position, and the message ID from the offending negotiation. It MAY contain error text describing the problem.

[3.12](#) INVALID-TRANSFORM-ID

The INVALID-TRANSFORM-ID error message may be used to communicate that an invalid or unrecognized (unimplemented?) transform was received as part of a proposal.

Phase: 1 or 2
Differentiator: Cookies, message ID, SPI
Payloads: Transform

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to zero (0)

- o Notify Message Type - set to INVALID-TRANSFORM-ID
- o SPI - empty
- o Notification Data - SHOULD contain the offending SA payload, error offset position, and the message ID from the offending negotiation. It MAY contain error text describing the problem.

3.13 ATTRIBUTES-NOT-SUPPORTED

The ATTRIBUTES-NOT-SUPPORTED error message may be used to communicate that unrecognized or unsupported attributes were received as part of a proposal. Currently, this message may result from one of the following events:

- o unacceptable group in IKE new-group-mode negotiation
- o conflicting lifetime attributes are detected
- o invalid or unsupported SA attributes are received

Phase: 1 or 2
 Differentiator: Cookies, message ID, SPI, attributes
 Payloads: SA

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to selected Protocol ID from subject SA
- o SPI Size - set to either zero (0) or four (4)(one IPSEC SPI)
- o Notify Message Type - set to ATTRIBUTES-NOT-SUPPORTED
- o SPI - set to empty or to the target entity's IPsec SPI; if present, the SPI MUST be from the same proposal payload contains the offending transform.
- o Notification Data - SHOULD contain the offending SA payload, error offset position, and the message ID from the offending negotiation. It MAY contain error text describing the problem.

3.14 NO-PROPOSAL-CHOSEN

The NO-PROPOSAL-CHOSEN error message may be used to communicate that none of the received proposals are acceptable to the responder.

Phase: 1 or 2
Differentiator: Cookies, message ID
Payloads: SA

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

- o Payload Length - set to length of payload + size of data (4)
- o DOI - set to DOI of received packet
- o Protocol ID - set to selected Protocol ID from subject SA
- o SPI Size - set to sixteen (16)
- o Notify Message Type - set to NO-PROPOSAL-CHOSEN
- o SPI - set to ISAKMP cookies
- o Notification Data - SHOULD contain the message ID of the offending negotiation, and MAY contain error text describing the problem. MAY also contain a proposal suggestion.

[3.15](#) BAD-PROPOSAL-SYNTAX

The BAD-PROPOSAL-SYNTAX error message may be used to communicate that a received proposal is improperly formed. This message may be precipitated by the following events (among others):

- o a reserved field in a proposal payload does not contain zero (0)
- o a reserved field in a transform payload does not contain zero (0)
- o responder returns SA payload containing multiple proposals
- o responder returns multiple (or no) transforms
- o initiator attempts to negotiate multiple quick mode SAs but responder only answers to one of them.

Phase: 1 or 2
Differentiator: Cookies, message ID, proposal/transform payload
Payloads: Generic Payload Header, Proposal, Transform

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to PROTO_ISAKMP

- o SPI Size - set to zero (0) or sixteen (16)
- o Notify Message Type - set to BAD-PROPOSAL-SYNTAX
- o SPI - empty or ISAKMP cookies
- o Notification Data - SHOULD contain the offending SA payload, error offset position, and the message ID from the offending negotiation. It MAY contain error text describing the problem.

[Note: There's an ambiguity here due to overloading this error type. It would be resolved by adding a BAD-TRANSFORM-SYNTAX error, and only using this one for proposals. Alternatively, we could add an identifier to this message to distinguish between the two cases]

[3.16](#) PAYLOAD-MALFORMED

The PAYLOAD-MALFORMED error message may be used to communicate that a malformed payload was received. This includes proposals, transforms, or attributes that are syntactically incorrect.

Phase: 1 or 2
Differentiator: Cookies, message ID, malformed payload
Payloads: Generic Payload Header, Proposal, Transform

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to ISAKMP DOI (0)
- o Protocol ID - set to selected Protocol ID from subject SA if available, else set to protocol PROTO_ISAKMP
- o SPI Size - set to zero (0), two (2), four (4) or sixteen (16)
- o Notify Message Type - set to PAYLOAD-MALFORMED
- o SPI - If protocol ID is PROTO_ISAKMP, contains the cookies; otherwise, contains SPI associated with Protocol ID if applicable, or nothing.
- o Notification Data - SHOULD contain the type of the offending payload, the payload data, the error position offset, and the message ID of the offending negotiation. It MAY contain error text describing the problem.

[Note: This overlaps with BAD-PROPOSAL-SYNTAX...]

[3.17](#) INVALID-KEY-INFORMATION

The INVALID-KEY-INFORMATION error message may be used to communicate

that the key exchange payload is not the correct size.

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

Phase: 1 or 2
Differentiator: Cookies, message ID, KE payload
Payloads: Key Exchange

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to ISAKMP DOI (0)
- o Protocol ID - set to selected Protocol ID from subject SA if available, else set to protocol PROTO_ISAKMP
- o SPI Size - set to zero (0), two (2), four (4) or sixteen (16)
- o Notify Message Type - set to INVALID-KEY-INFORMATION
- o SPI - If protocol ID is PROTO_ISAKMP, contains the cookies; otherwise, contains SPI associated with Protocol ID if applicable, or nothing.
- o Notification Data - SHOULD contain the offending payload, the error position offset, and the message ID of the offending negotiation. It MAY contain error text describing the problem.

[3.18](#) INVALID-ID-INFORMATION

The INVALID-ID-INFORMATION error message may be used to communicate that the identification type of the ID payload is not supported.

Phase: 1 or 2
Differentiator: Cookies, message ID, SPI, ID payload
Payloads: ID

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to selected Protocol ID from subject SA if phase 2, else set to protocol PROTO_ISAKMP
- o SPI Size - set to zero (0), two (2), four (4) or sixteen (16)
- o Notify Message Type - set to INVALID-ID-INFORMATION
- o SPI - If protocol ID is PROTO_ISAKMP, contains the cookies;

- otherwise, contains SPI associated with Protocol ID if applicable, or nothing.
- o Notification Data - SHOULD contain the offending payload, the error position offset, and the message ID of the offending negotiation. It MAY contain error text describing the problem.

3.19 INVALID-CERT-ENCODING

Kelly, Kivinen

Expires May, 2001

[Page 17]

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

The INVALID-CERT-ENCODING error message may be used to communicate that the encoding of a received certificate payload is not valid.

Phase: 1 or 2
Differentiator: Cookies, message ID, SPI, CERT payload
Payloads: Certificate, Certificate Request

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to either zero (0) or sixteen (16)
- o Notify Message Type - set to INVALID-CERT-ENCODING
- o SPI - set to empty or to the ISAKMP cookies
- o Notification Data - SHOULD contain the offending certificate payload, error position offset, and Message ID. It MAY contain error text describing the problem.

3.20 INVALID-CERTIFICATE

The INVALID-CERTIFICATE error message may be used to communicate that the data in a certificate payload is invalid or improperly formatted.

Phase: 1 or 2
Differentiator: Cookies, message ID, SPI, CERT payload
Payloads: Certificate

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to either zero (0) or sixteen (16)
- o Notify Message Type - set to INVALID-CERTIFICATE
- o SPI - set to empty or to the ISAKMP cookies
- o Notification Data - SHOULD contain the offending certificate payload, error position offset, and Message ID. It MAY contain error text describing the problem.

3.21 CERT-TYPE-UNSUPPORTED

The CERT-TYPE-UNSUPPORTED error message may be used to communicate that the encoding of a received certificate payload is not supported.

Kelly, Kivinen

Expires May, 2001

[Page 18]

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

Phase: 1 or 2
 Differentiator: Cookies, message ID, SPI, CERT payload
 Payloads: Certificate Request

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to either zero (0) or sixteen (16)
- o Notify Message Type - set to CERT-TYPE-UNSUPPORTED
- o SPI - set to empty or to the ISAKMP cookies
- o Notification Data - SHOULD contain the offending certificate request payload, error position offset, and Message ID. It MAY contain error text describing the problem.

3.22 INVALID-CERT-AUTHORITY

The INVALID-CERT-AUTHORITY error message may be used to communicate that the Certificate Authority in a certificate request payload is invalid or improperly formatted.

Phase: 1
 Differentiator: Cookies, message ID, SPI, CERT-REQ payload

Payloads: Certificate Request

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to either zero (0) or sixteen (16)
- o Notify Message Type - set to INVALID-CERT-AUTHORITY
- o SPI - set to empty or to the ISAKMP cookies
- o Notification Data - SHOULD contain the offending certificate request payload, error position offset, and Message ID. It MAY contain error text describing the problem.

[3.23](#) INVALID-HASH-INFORMATION

The INVALID-HASH-INFORMATION error message may be used to communicate that the hash size is incorrect.

Phase: 1 or 2

Kelly, Kivinen

Expires May, 2001

[Page 19]

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

Differentiator: Cookies, message ID, SPI, hash payload

Payloads: Hash

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to selected Protocol ID from chosen SA or PROTO_ISAKMP
- o SPI Size - set to either zero (0), four (4), or sixteen (16)
- o Notify Message Type - set to INVALID-HASH-INFORMATION
- o SPI - set to empty, the target entity's IPsec SPI, or the ISAKMP cookies
- o Notification Data - SHOULD contain the offending hash payload error position offset, and Message ID. It MAY contain error text describing the problem.

[3.24 AUTHENTICATION-FAILED](#)

The AUTHENTICATION-FAILED error message may be used to communicate that the authentication operation (hash) produced an incorrect result.

Phase: 1 or 2
Differentiator: Cookies, message ID, SPI
Payloads: Hash, Signature

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to selected Protocol ID from chosen SA or PROTO_ISAKMP
- o SPI Size - set to either zero (0), four (4), or sixteen (16)
- o Notify Message Type - set to AUTHENTICATION-FAILED
- o SPI - set to empty, the target entity's IPsec SPI, or the ISAKMP cookies
- o Notification Data - SHOULD contain the Message ID of the offending payload. It MAY contain error text describing the problem.

[3.25 INVALID-SIGNATURE](#)

The INVALID-SIGNATURE error message may be used to communicate that

the signature is the wrong size.

NOTE: If signature verification fails, AUTHENTICATION-FAILED is sent.

Phase: 1
Differentiator: Cookies
Payloads: Signature

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet

- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to sixteen (16)
- o Notify Message Type - set to INVALID-SIGNATURE
- o SPI - set to the ISAKMP cookies
- o Notification Data - SHOULD contain the offending ID payload and the associated message ID. It MAY contain error text describing the problem.

[3.26](#) ADDRESS-NOTIFICATION

The ADDRESS-NOTIFICATION error message may be used to communicate that an invalid address was received in the ID payload.

Phase: 1 or 2
 Differentiator: Cookies, message ID, SPI, address info?
 Payloads: ID

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to selected Protocol ID from chosen SA or PROTO_ISAKMP
- o SPI Size - set to either zero (0), four (4), or sixteen (16)
- o Notify Message Type - set to ADDRESS-NOTIFICATION
- o SPI - set to empty, the target entity's IPsec SPI, or the ISAKMP cookies
- o Notification Data - SHOULD contain the offending ID payload and the associated message ID. It MAY contain error text describing the problem.

[3.27](#) NOTIFY-SA-LIFETIME

The NOTIFY-SA-LIFETIME message may be used to communicate that a lifetime attribute list is incorrectly formatted. I.e. only life type attribute but no life duration etc.

Phase: 1

Differentiator: Cookies, message ID

Payloads: Transform

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to selected Protocol ID from chosen SA
- o SPI Size - set to four (4) or sixteen (16)
- o Notify Message Type - set to NOTIFY-SA-LIFETIME
- o SPI - set to the target entity's IPsec SPI, or the ISAKMP cookies
- o Notification Data - SHOULD contain the offending payload and the message ID associated with the payload. It MAY also contain the error position offset, and error text describing the problem.

[3.28](#) CERTIFICATE-UNAVAILABLE

The CERTIFICATE-UNAVAILABLE error message may be used to communicate that the requested certificate is unavailable.

Phase: 1 or 2

Differentiator: Cookies, message ID, SPI, CERT-REQ payload

Payloads: Certificate Request

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to zero (0) or sixteen (16)
- o Notify Message Type - set to CERTIFICATE-UNAVAILABLE
- o SPI - set to empty or to the ISAKMP cookies
- o Notification Data - SHOULD contain the subject certificate request payload and the associated message ID. MAY contain error text describing the problem.

[3.29](#) UNSUPPORTED-EXCHANGE-TYPE

The UNSUPPORTED-EXCHANGE-TYPE error message may be used to communicate that the requested exchange type is not supported.

Phase: 1 or 2
Differentiator: Cookies, message ID, SPI, exchange type
Payloads: ISAKMP header

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to 0
- o Protocol ID - set to PROTO_ISAKMP
- o SPI Size - set to sixteen (16)
- o Notify Message Type - set to UNSUPPORTED-EXCHANGE-TYPE
- o SPI - set to ISAKMP cookies
- o Notification Data - SHOULD contain the message ID of the offending negotiation and the offending exchange type. MAY contain error text describing the problem.

[3.30](#) UNEQUAL-PAYLOAD-LENGTHS

The UNEQUAL-PAYLOAD-LENGTHS error message may be used to communicate that the message length in the ISAKMP header does not match the sum of the actual payload lengths. It may also be used when data attributes overflow their encapsulating payload boundaries.

Phase: 1 or 2
Differentiator: Cookies, message ID, SPI

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet or zero (0)
- o Protocol ID - set to PROTO_ISAKMP or selected Protocol ID from chosen SA
- o SPI Size - set to four (4) or (16)
- o Notify Message Type - set to UNEQUAL-PAYLOAD-LENGTHS
- o SPI - set to the target entity's IPsec SPI or the ISAKMP cookies
- o Notification Data - SHOULD contain the type of the offending payload. It MAY contain the offending payload, the associated message ID, the error position offset, and error text describing the problem.

[4.](#) ISAKMP Notify Status messages

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

This section contains NOTIFY status messages which are specific to ISAKMP, or phase 1 Security Associations (SAs). These NOTIFY message types are defined in [\[RFC2408\]](#).

[4.1](#) CONNECTED

The CONNECTED status message may be used to communicate that the IPSEC protocol (phase 2) SA has been established.

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to PROTO_ISAKMP or selected Protocol ID from chosen SA
- o SPI Size - set to zero (0), four (4) or sixteen (16)
- o Notify Message Type - set to CONNECTED
- o SPI - set to the selected SPI
- o Notification Data - empty

[4.2](#) RESPONDER-LIFETIME

The RESPONDER-LIFETIME message may be used to communicate that a lifetime which is shorter than the one requested will be enforced. This notification is defined in the DOI, and is included here only because it does NOT follow the notification data formatting specifications defined in this document.

Phase: 1 or 2
Differentiator: Cookies, message ID,
Payloads: Transform

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to selected Protocol ID from chosen SA
- o SPI Size - set to four (4) or sixteen (16)
- o Notify Message Type - set to RESPONDER-LIFETIME

- o SPI - set to the target entity's IPsec SPI, or the ISAKMP cookies
- o Notification Data - contains an ISAKMP attribute list with the responder's actual SA lifetime

WARNING: the attribute classes for the ISAKMP attribute list are

defined in the ISAKMP DOI document ([RFC2407](#)). This message type is included here for completeness.

[4.3](#) REPLAY-STATUS

The REPLAY-STATUS message may be used for positive confirmation of the responder's election on whether or not he is to perform anti-replay detection. This notification is defined in the DOI, and is included here only because it does NOT follow the notification data formatting specifications defined in this document.

Phase: 2
 Differentiator: Cookies vs SPI
 Payloads: Transform

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

- o Payload Length - set to length of payload + size of data
- o DOI - set to DOI of received packet
- o Protocol ID - set to selected Protocol ID from chosen SA
- o SPI Size - set to four (4) or sixteen (16)
- o Notify Message Type - set to REPLAY-STATUS
- o SPI - set to the target entity's IPsec SPI, or the ISAKMP cookies
- o Notification Data - a 4 octet value:
 - 0 = replay detection disabled
 - 1 = replay detection enabled

WARNING: This message type is defined in the ISAKMP DOI document ([RFC2407](#)). This message type is included here for completeness.

[4.4](#) INITIAL-CONTACT

The INITIAL-CONTACT status message may be used when one side wishes

to inform the other that this is the first SA being established with the remote system. This notification is defined in the DOI, and is included here only because it does NOT follow the notification data formatting specifications defined in this document.

Phase: 1
Differentiator: Cookies
Payloads: None

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

- o Payload Length - set to length of payload + size of data

Kelly, Kivinen

Expires May, 2001

[Page 25]

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

- o DOI - set to DOI of received packet
- o Protocol ID - set to selected Protocol ID from chosen SA
- o SPI Size - sixteen (16)
- o Notify Message Type - set to INITIAL-CONTACT
- o SPI - set to ISAKMP cookies
- o Notification Data - <not included>

WARNING: This message type is defined in the ISAKMP DOI document ([RFC2407](#)). This message type is included here for completeness.

[5.](#) Security Considerations

In general, accepting unauthenticated NOTIFY messages renders an implementation susceptible to numerous attacks, both passive and active. In such cases, there is no assurance whatsoever that these messages are not being sent by an attacker intent upon mounting a simple denial of service attack, or perhaps a more sophisticated attack. Hence, applications MUST NOT rely upon information provided by such unprotected exchanges.

Furthermore, the inclusion of variable notification payloads within unprotected messages presents a significant denial of service opportunity to a hostile adversary. Thus, implementations which choose to inspect unprotected notification data are well advised to limit the amount of processing expended upon such packets.

In cases where received payloads are copied into notification data, if the original payload was encrypted, the resulting notify message

MUST be encrypted with at least the same level of protection that the original payload had. Otherwise, numerous attacks are possible.

6. Editors' Addresses

Scott Kelly
RedCreek Communications
3900 Newpark Mall Road
Newark, CA 94560
USA
email: skelly@redcreek.com
Telephone: +1 (510) 745-3969

Tero Kivinen
SSH Communications Security Corp
Fredrikinkatu 42
FIN-00100 HELSINKI
Finland
E-mail: kivinen@ssh.fi

Kelly, Kivinen

Expires May, 2001

[Page 26]

Internet Draft

[draft-ietf-ipsec-notifymsg-04.txt](#)

November, 2000

The IPSec working group can be contacted via the IPSec working group's mailing list (ipsec@lists.tislabs.com) or through its chairs:

Robert Moskowitz
rgm@icsa.net
International Computer Security Association

Theodore Y. Ts'o
tytso@MIT.EDU
Massachusetts Institute of Technology

7. References

- [RFC2401] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998.
- [RFC2402] Kent, S., and R. Atkinson, "IP Authentication Header", [RFC 2402](#), November 1998.
- [RFC2406] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998.

- [RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", [RFC 2407](#), November 1998.
- [RFC2408] Maughhan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", [RFC 2408](#), November 1998.
- [RFC2409] Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", [RFC 2409](#), November 1998.
- [RFC-2119] Bradner, S., "Key Words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[8](#). Acknowledgements

The editors would like to acknowledge all the helpful comments received from numerous members of the IPsec working group, including S. Frankel of NIST, T. Zegman of Checkpoint, D. Mason of Network Associates, V. Smyslov of Trustworks, and A. Potluri of TRI.

[9](#). 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.