Internet Engineering Task Force
IP Security Working Group
Internet Draft
Expires August 2003

John Shriver
Sockeye Networks

February 27, 2003

IPsec DOI Textual Conventions MIB

<draft-ietf-ipsec-doi-tc-mib-07.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its 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/1id-abstracts.txt

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

This document is a submission to the IETF Internet Protocol Security (IPsec) Working Group. Please send comments on this document to the working group mailing list (ipsec@lists.tislabs.com).

Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document defines textual conventions for the constants used in MIBs for the IPsec protocols. In particular, it documents those numbers whose assignments are managed by the IANA, with new assignments being made over time. The textual conventions provide IPsec-related MIBs with clearer documentation, and insulate them from having to track new assignments by the IANA.

The MIB documented by this document will become a separate living document maintained by the IANA, and will be the document of record for these assignments.

Table of Contents

1. Introduction

This memo defines textual conventions for use in monitoring, status, and configuration MIBs for IPsec. It includes a MIB module that defines those textual conventions.

2. The SNMPv2 Network Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Objects in the MIB are defined using the mechanisms defined in the SMI.

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

3. Discussion

The IPsec architecture [SECARCH] defines protocols for dynamic key management. These are based on the Internet Security Association and Key Management Protocol [ISAKMP].

ISAKMP defines the concept of Domains of Interpretation (DOI). The IPsec architecture has defined the Internet IP Security Domain of Interptetation for ISAKMP [IPDOI].

The IPsec architecture defines the Internet Key Exchange [IKE]. The use of this protocol is indicated by one of the constants in the IPsec DOI.

This MIB defines textual conventions for the constants defined in ISAKMP, the IPsec DOI, and IKE.

These are defined in a seperate MIB for two reasons.

o There will be variables with a syntax corresponding to these textual conventions in numberous MIBs that will be defined for the IPsec architecture.

o All of the numbers defined in these textual conventions are in "magic number" spaces that are managed by the IANA.

If these conventions were part of the relevant MIBs, those MIBs would be constantly out of date. By placing them in a seperate MIB, that MIB can be maintained by the IANA simultaneously with assigning new values.

4. MIB Definitions

```
IPSEC-ISAKMP-IKE-DOI-TC DEFINITIONS ::= BEGIN

IMPORTS
-- delete next line before release
   experimental,
```

```
      MODULE-IDENTITY, Unsigned32         FROM SNMPv2-SMI
   -- uncomment next line before release
   -- mib-2                               FROM RFC1213-MIB
      TEXTUAL-CONVENTION                  FROM SNMPv2-TC;

   ianaIPsecIsakmpIkeDoiTcMib MODULE-IDENTITY
      LAST-UPDATED "200302271543Z"
      ORGANIZATION "Sockeye Networks"
      CONTACT-INFO "John Shriver
                   Sockeye Networks
                   52 Second Ave., Suite 100
                   Waltham, MA  02451

                   Phone:
                   +1-781-693-7067

                   E-mail:
                   jshriver+ietf@sockeye.com"

      DESCRIPTION  "The MIB module which defines the textual conventions
                   used in IPsec MIBs.  This includes Internet DOI
                   numbers defined in RFC 2407, ISAKMP numbers defined
                   in RFC 2408, and IKE numbers defined in RFC 2409.

                   These Textual Conventions are defined in a separate
                   MIB module since they are protocol numbers managed
                   by the IANA.  Revision control after publication
                   will be under the authority of the IANA.

                   Copyright (C) The Internet Society (2003). This
                   version of this MIB module is part of RFC XXXX; see
                   the RFC itself for full legal notices."
      REVISION     "200302271543Z"
   -- replace XXX in next line before release
      DESCRIPTION  "Initial revision, published as RFC XXXX."

   -- replace xxx in next line before release, uncomment before release
   -- ::= { mib-2 xxx }
   -- delete next line before release
      ::= { experimental 100 }

   -- The first group of textual conventions are based on definitions
   -- in the IPsec DOI, RFC 2407.

   IpsecDoiSituation ::= TEXTUAL-CONVENTION
       DISPLAY-HINT "x"
       STATUS      current
```

```
       DESCRIPTION "The IPsec DOI Situation provides information that
                   can be used by the responder to make a policy
                   determination about how to process the incoming
                   Security Association request.

                   It is a four (4) octet bitmask, with the following
                   values:

                   sitIdentityOnly            0x01
                   sitSecrecy                 0x02
                   sitIntegrity               0x04

                   The upper two bits (0x80000000 and 0x40000000) are
                   reserved for private use amongst cooperating
                   systems."
       REFERENCE   "RFC 2407 sections 4.2 and 6.2"
       SYNTAX      Unsigned32 (0..4294967295)
       -- The syntax is not BITS, because we want the representation
       -- to be the same here as it is in the ISAKMP/IKE protocols.


   IpsecDoiSecProtocolId ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "These are the IPsec DOI values for the Protocol-Id
                   field in an ISAKMP Proposal Payload, and in all
                   Notification Payloads.

                   They are also used as the Protocol-ID In the
                   Notification Payload and the Delete Payload.

                   The values 249-255 are reserved for private use
                   amongst cooperating systems."
       REFERENCE   "RFC 2407 section 4.4.1"
       SYNTAX      INTEGER {
                       reserved(0),         -- reserved in DOI
                       protoIsakmp(1),      -- message protection
                                            -- required during Phase I
                                            -- of the IKE protocol
                       protoIpsecAh(2),     -- IP packet authentication
                                            -- via Authentication Header
                       protoIpsecEsp(3),    -- IP packet confidentiality
                                            -- via Encapsulating
                                            -- Security Payload
                       protoIpcomp(4)       -- IP payload compression
                   }

   IpsecDoiTransformIdent ::= TEXTUAL-CONVENTION
```

```
       STATUS      current
       DESCRIPTION "The values of the IPsec DOI ISAKMP Transform
                   Identifier which identify a key exchange protocol
                   to be used for the negotiation.  It is used in the
                   Transform-Id field of an IKE Phase I Transform
                   Payload.

                   The values 249-255 are reserved for private use
                   amongst cooperating systems."
       REFERENCE   "RFC 2407 sections 4.4.2 and 6.3"
       SYNTAX      INTEGER {
                       reserved(0),        -- reserved in DOI
                       keyIke(1)           -- the hybrid ISAKMP/Oakley
                                           -- Diffie-Hellman key
                                           -- exchange
                   }

   IpsecDoiAhTransform ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "The values of the IPsec DOI AH Transform Identifier
                   which identify a particular algorithm to be
                   used to provide integrity protection for AH.  It is
                   used in the Tranform-ID field of a ISAKMP Transform
                   Payload for the IPsec DOI, when the Protocol-Id of
                   the associated Proposal Payload is 2 (AH).

                   The values 249-255 are reserved for private use
                   amongst cooperating systems."
       REFERENCE   "RFC 2407 sections 4.4.3 and 6.4,
                   IANA,
                   RFC 2857"
       SYNTAX      INTEGER {
                       reserved(0),        -- reserved in DOI
                       reserved1(1),       -- reserved
                       ahMd5(2),           -- generic AH transform
                                           -- using MD5
                       ahSha(3),           -- generic AH transform
                                           -- using SHA-1
                       ahDes(4),           -- generic AH transform
                                           -- using DES
                       ahSha256(5),        -- generic AH transform
                                           -- using SHA-256
                       ahSha384(6),        -- generic AH transform
                                           -- using SHA-384
                       ahSha512(7),        -- generic AH transform
                                           -- using SHA-512
                       ahRipemd(8)         -- generic AH transform
```

```
                                           -- using HMAC-RIPEMD-160-96
                                           -- RFC 2857
                   }

   IpsecDoiEspTransform ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "The values of the IPsec DOI ESP Transform Identifier
                   which identify a particular algorithm to be used to
                   provide secrecy protection for ESP.  It is used in
                   the Tranform-ID field of a ISAKMP Transform Payload
                   for the IPsec DOI, when the Protocol-Id of the
                   associated Proposal Payload is 2 (AH), 3 (ESP),
                   and 4 (IPCOMP).

                   The values 249-255 are reserved for private use
                   amongst cooperating systems."
       REFERENCE   "RFC 2407 sections 4.4.4 and 6.5,
                   IANA"
       SYNTAX      INTEGER {
                       none(0),            -- reserved in DOI, used
                                           -- in MIBs to reflect no
                                           -- encryption used
                       espDesIv64(1),      -- DES-CBC transform defined
                                           -- in RFC 1827 and RFC 1829
                                           -- using a 64-bit IV
                       espDes(2),          -- generic DES transform
                                           -- using DES-CBC
                       esp3Des(3),         -- generic triple-DES
                                           -- transform
                       espRc5(4),          -- RC5 transform
                       espIdea(5),         -- IDEA transform
                       espCast(6),         -- CAST transform
                       espBlowfish(7),     -- BLOWFISH transform
                       esp3Idea(8),        -- reserved for triple-IDEA
                       espDesIv32(9),      -- DES-CBC transform defined
                                           -- in RFC 1827 and RFC 1829
                                           -- using a 32-bit IV
                       espRc4(10),         -- reserved for RC4
                       espNull(11),        -- no confidentiality
                                           -- provided by ESP
                       espAes(12)          -- NIST AES transform
                   }

   IpsecDoiAuthAlgorithm ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "The ESP Authentication Algorithm used in the IPsec
                   DOI as a SA Attributes definition in the Transform
```

```
                        Payload of Phase II of an IKE negotiation.  This
                        set of values defines the AH authentication
                        algorithm, when the associated Proposal Payload has
                        a Protocol-ID of 2 (AH).  This set of values
                        defines the ESP authentication algorithm, when the
                        associated Proposal Payload has a Protocol-ID
                        of 3 (ESP).

                        Unused values <= 61439 are reserved to IANA.

                        Values 61440-65535 are for private use.

                        In a MIB, a value of 0 indicates that ESP
                        has been negotiated without authentication."
       REFERENCE        "RFC 2407 section 4.5,
                        RFC 2407 section 4.4.3.1,
                        RFC 1826,
                        IANA,
                        RFC 2857"
       SYNTAX           INTEGER {
                            none(0),              -- reserved in DOI, used
                                                  -- in MIBs to reflect no
                                                  -- encryption used
                            hmacMd5(1),           -- hashed MAC using MD5
                            hmacSha(2),           -- hashed MAC using SHA-1
                            desMac(3),            -- DES MAC
                            kpdk(4),              -- RFC 1826
                                                  -- Key/Pad/Data/Key
                            hmacSha256(5),        -- hashed MAC using SHA-256
                            hmacSha384(6),        -- hashed MAC using SHA-384
                            hmacSha512(7),        -- hashed MAC using SHA-512
                            hamcRipemd(8)         -- hashed MAC using
                                                  -- RIPEMD-160-96
                        }

   IpsecDoiIpcompTransform ::= TEXTUAL-CONVENTION
       STATUS           current
       DESCRIPTION      "The IPsec DOI IPCOMP Transform Identifier is an
                        8-bit value which identifies a particular algorithm
                        to be used to provide IP-level compression before
                        ESP.  It is used in the Tranform-ID field of a ISAKMP
                        Transform Payload for the IPsec DOI, when the
                        Protocol-Id of the associated Proposal Payload
                        is 4 (IPCOMP).

                        The values 1-47 are reserved for algorithms for which
                        an RFC has been approved for publication.
```

```
                    The values 48-63 are reserved for private use amongst
                    cooperating systems.

                    The values 64-255 are reserved for future expansion."
       REFERENCE    "RFC 2407 sections 4.4.5 and 6.6,
                    RFC 3051"
       SYNTAX       INTEGER {
                        reserved(0),        -- reserved in DOI
                        ipcompOui(1),       -- proprietary compression
                                            -- transform
                        ipcompDeflate(2),   -- "zlib" deflate algorithm
                        ipcompLzs(3),       -- Stac Electronics LZS
                        ipcompLzjh(4)       -- ITU-T V.44 packet method
                    }

   IpsecDoiEncapsulationMode ::= TEXTUAL-CONVENTION
       STATUS       current
       DESCRIPTION "The Encapsulation Mode used as an IPsec DOI
                    SA Attributes definition in the Transform Payload
                    of a Phase II IKE negotiation.  This set of
                    values defines encapsulation modes used for AH,
                    ESP, and IPCOMP when the associated Proposal Payload
                    has a Protocol-ID of 3 (ESP).

                    Unused values <= 61439 are reserved to IANA.

                    Values 61440-65535 are for private use."
       SYNTAX       INTEGER {
                        reserved(0),        -- reserved in DOI
                        tunnel(1),
                        transport(2)
                    }

   IpsecDoiIdentType ::= TEXTUAL-CONVENTION
       STATUS       current
       DESCRIPTION "The IPsec DOI Identification Type is an 8-bit value
                    which is used in the ID Type field as a discriminant
                    for interpretation of the variable-length
                    Identification Payload.

                    The values 249-255 are reserved for private use
                    amongst cooperating systems."
       REFERENCE    "RFC 2407 sections 4.4.5, 4.6.2.1, and 6.9"
       SYNTAX       INTEGER {
                        reserved(0),        -- reserved in DOI
                        idIpv4Addr(1),      -- a single four (4) octet
                                            -- IPv4 address
```

```
                       idFqdn(2),          -- fully-qualified domain
                                           -- name string
                       idUserFqdn(3),      -- fully-qualified username
                                           -- string
                       idIpv4AddrSubnet(4),
                                           -- a range of IPv4 addresses,
                                           -- represented by two
                                           -- four (4) octet values,
                                           -- where the first is an
                                           -- address and the second
                                           -- is a mask
                       idIpv6Addr(5),      -- a single sixteen (16)
                                           -- octet IPv6 address
                       idIpv6AddrSubnet(6),
                                           -- a range of IPv6 addresses,
                                           -- represented by two
                                           -- sixteen (16) octet values,
                                           -- where the first is an
                                           -- address and the second
                                           -- is a mask
                       idIpv4AddrRange(7), -- a range of IPv4 addresses,
                                           -- represented by two
                                           -- four (4) octet values,
                                           -- where the first is the
                                           -- beginning IPv4 address
                                           -- and the second is the
                                           -- ending IPv4 address
                       idIpv6AddrRange(8), -- a range of IPv6 addresses,
                                           -- represented by two
                                           -- sixteen (16) octet values,
                                           -- where the first is the
                                           -- beginning IPv6 address
                                           -- and the second is the
                                           -- ending IPv6 address
                       idDerAsn1Dn(9),     -- the binary DER encoding of
                                           -- ASN1 X.500
                                           -- DistinguishedName
                       idDerAsn1Gn(10),    -- the binary DER encoding of
                                           -- ASN1 X.500 GeneralName
                       idKeyId(11)         -- opaque byte stream which
                                           -- may be used to pass
                                           -- vendor-specific
                                           -- information
                   }

   -- The second group of textual conventions are based on defintions
   -- the ISAKMP protocol, RFC 2408.
```

```
   IsakmpDOI ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "These are the domain of interpretation values for
                   the ISAKMP Protocol.  They are a 32-bit value
                   used in the Domain of Interpretation field of the
                   Security Association Payload.

                   Unused values <= 4294967295 are reserved to
                   the IANA."
       REFERENCE   "RFC 2048 section 3.4."
       SYNTAX      INTEGER {
                       isakmp(0),          -- generic ISAKMP SA in
                                           -- Phase 1, which can be
                                           -- used for any protocol
                                           -- in Phase 2
                       ipsecDOI(1)         -- the IPsec DOI as
                                           -- specified in RFC 2407
                   }

   IsakmpCertificateEncoding ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "These are the values for the types of
                   certificate-related information contained in the
                   Certificate Data field of a Certificate Payload.
                   They are used in the Cert Encoding field of the
                   Certificate Payload.

                   Values 11-255 are reserved."
       REFERENCE   "RFC 2408 section 3.9"
       SYNTAX      INTEGER {
                       pkcs7(1),           -- PKCS #7 wrapped
                                           -- X.509 certificate
                       pgp(2),             -- PGP Certificate
                       dnsSignedKey(3),    -- DNS Signed Key
                       x509Signature(4),   -- X.509 Certificate:
                                           -- Signature
                       x509KeyExchange(5), -- X.509 Certificate:
                                           -- Key Exchange
                       kerberosTokens(6),  -- Kerberos Tokens
                       crl(7),             -- Certificate Revocation
                                           -- List (CRL)
                       arl(8),             -- Authority Revocation
                                           -- List (ARL)
                       spki(9),            -- SPKI Certificate
                       x509Attribute(10)   -- X.509 Certificate:
                                           -- Attribute
                   }
```

```
   IsakmpExchangeType ::= TEXTUAL-CONVENTION
       --
       -- When revising IsakmpExchangeType, consider revising
       -- IkeExchangeType as well.
       --
       STATUS      current
       DESCRIPTION "These are the values used for the exchange types in
                   the ISAKMP header.

                   Values up to 31 are reserved for future
                   DOI-independent assignment for ISAKMP.

                   The values 240-255 are reserved for private use
                   amongst cooperating systems."
       REFERENCE   "RFC 2408 section 3.1"
       SYNTAX      INTEGER {
                       reserved(0),
                       base(1),             -- base mode
                       identityProtect(2), -- identity protection
                       authOnly(3),         -- authentication only
                       aggressive(4),       -- aggressive mode
                       informational(5)     -- informational
                   }

   IsakmpNotifyMessageType ::= TEXTUAL-CONVENTION
       --
       -- If you change this, you probably want to
       -- change IkeNotifyMessageType.
       --
       STATUS      current
       DESCRIPTION "These are the values for the types of notification
                   messages.  They are used as the Notify Message Type
                   field in the Notification Payload.

                   This textual convention merges the types
                   for error types (in the range 1-16386) and for
                   notification types (in the range 16384-65535).

                   The values 16001-16383 are reserved for private use
                   as error types amongst cooperating systems.

                   The values 24576-32767 are reserved for use in
                   each DOI.  Each DOI should have a clone of this
                   textual convention adding local values.

                   The values 32768-40958 are reserved for private use
                   as notification types amongst cooperating systems."
```

```
       REFERENCE    "RFC 2408 section 3.14.1"
       SYNTAX       INTEGER {

                        -- Values defined for errors in ISAKMP
                        --
                        reserved(0),        -- reserved in DOI
                        invalidPayloadType(1),
                        doiNotSupported(2),
                        situationNotSupported(3),
                        invalidCookie(4),
                        invalidMajorVersion(5),
                        invalidMinorVersion(6),
                        invalidExchangeType(7),
                        invalidFlags(8),
                        invalidMessageId(9),
                        invalidProtocolId(10),
                        invalidSpi(11),
                        invalidTransformId(12),
                        attributesNotSupported(13),
                        noProposalChosen(14),
                        badProposalSyntax(15),
                        payloadMalformed(16),
                        invalidKeyInformation(17),
                        invalidIdInformation(18),
                        invalidCertEncoding(19),
                        invalidCertificate(20),
                        certTypeUnsupported(21),
                        invalidCertAuthority(22),
                        invalidHashInformation(23),
                        authenticationFailed(24),
                        invalidSignature(25),
                        addressNotification(26),
                        notifySaLifetime(27),
                        certificateUnavailable(28),
                        unsupportedExchangeType(29),
                        unequalPayloadLengths(30),

                        -- values defined for errors in IPsec DOI
                        -- (none)

                        -- values defined for notification in ISAKMP
                        --
                        connected(16384)

                        -- values defined for notification in
                        -- each DOI (clone this TC)
                    }
```

```
   -- The third group of textual conventions are based on defintions
   -- the IKE key exchange protocol, RFC 2409.

   IkeExchangeType ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "These are the values used for the exchange types in
                   the ISAKMP header.

                   The values 32-239 are DOI-specific, these values are
                   for the IPsec DOI used by IKE.

                   The values 240-255 are reserved for private use
                   amongst cooperating systems."
       REFERENCE   "RFC 2409 Appendix A"
       SYNTAX      INTEGER {
                       reserved(0),
                       base(1),            -- base mode
                       mainMode(2),        -- main mode
                       authOnly(3),        -- authentication only
                       aggressive(4),      -- aggressive mode
                       informational(5),   -- informational
                       reservedDontUse(6), -- reserved, not to be used
                       quickMode(32),      -- quick mode
                       newGroupMode(33)    -- new group mode
                   }

   IkeEncryptionAlgorithm ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "Values for encryption algorithms negotiated
                   for the ISAKMP SA by IKE in Phase I.  These are
                   values for SA Attrbute type Encryption
                   Algorithm (1).

                   Unused values <= 65000 are reserved to IANA.

                   Values 65001-65535 are for private use among
                   mutually consenting parties."
       REFERENCE   "RFC 2409 appendix A,
                   IANA"
       SYNTAX      INTEGER {
                       reserved(0),        -- reserved in IKE
                       desCbc(1),          -- RFC 2405
                       ideaCbc(2),
                       blowfishCbc(3),
                       rc5R16B64Cbc(4),    -- RC5 R16 B64 CBC
                       tripleDesCbc(5),    -- 3DES CBC
                       castCbc(6),
```

```
                            aesCbc(7)
                        }

   IkeHashAlgorithm ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "Values for hash algorithms negotiated
                   for the ISAKMP SA by IKE in Phase I.  These are
                   values for SA Attrbute type Hash Algorithm (2).

                   Unused values <= 65000 are reserved to IANA.

                   Values 65001-65535 are for private use among
                   mutually consenting parties."
       REFERENCE   "RFC 2409 appendix A,
                   IANA"
       SYNTAX      INTEGER {
                       reserved(0),         -- reserved in IKE
                       md5(1),              -- RFC 1321
                       sha(2),              -- FIPS 180-1
                       tiger(3),
                       sha256(4),
                       sha384(5),
                       sha512(6)
                   }

   IkeAuthMethod ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "Values for authentication methods negotiated
                   for the ISAKMP SA by IKE in Phase I.  These are
                   values for SA Attrbute type Authentication
                   Method (3).

                   Unused values <= 65000 are reserved to IANA.

                   Values 65001-65535 are for private use among
                   mutually consenting parties."
       REFERENCE   "RFC 2409 appendix A,
                   IANA"
       SYNTAX      INTEGER {
                       reserved(0),         -- reserved in IKE
                       preSharedKey(1),
                       dssSignatures(2),
                       rsaSignatures(3),
                       encryptionWithRsa(4),
                       revisedEncryptionWithRsa(5),
                       reservedDontUse6(6), -- not to be used
                       reservedDontUse7(7), -- not to be used
```

```
                        ecdsaSignatures(8)
                    }

   IkeGroupDescription ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "Values for Oakley key computation groups for
                   Diffie-Hellman exchange negotiated for the ISAKMP
                   SA by IKE in Phase I.  They are also used in Phase II
                   when perfect forward secrecy is in use.  These are
                   values for SA Attrbute type Group Description (4).

                   Unused values <= 32767 are reserved to IANA.

                   Values 32768-65535 are for private use among
                   mutually consenting parties."
       REFERENCE   "RFC 2409 appendix A,
                   IANA"
       SYNTAX      INTEGER {
                       none(0),             -- reserved in IKE, used
                                            -- in MIBs to reflect that
                                            -- none of the predefined
                                            -- groups are used
                       modp768(1),          -- default 768-bit MODP group
                       modp1024(2),         -- alternate 1024-bit MODP
                                            -- group
                       ec2nGF155(3),        -- EC2N group on Galois
                                            -- Field GF[2^155]
                       ec2nGF185(4),        -- EC2N group on Galois
                                            -- Field GF[2^185]
                       ec2nGF163Random(6),  -- EC2N group on Galois
                                            -- Field GF[2^163],
                                            -- random seed
                       ec2nGF163Koblitz(7),
                                            -- EC2N group on Galois
                                            -- Field GF[2^163],
                                            -- Koblitz curve
                       ec2nGF283Random(8),  -- EC2N group on Galois
                                            -- Field GF[2^283],
                                            -- random seed
                       ec2nGF283Koblitz(9),
                                            -- EC2N group on Galois
                                            -- Field GF[2^283],
                                            -- Koblitz curve
                       ec2nGF409Random(10),
                                            -- EC2N group on Galois
                                            -- Field GF[2^409],
                                            -- random seed
```

```
                       ec2nGF409Koblitz(11),
                                           -- EC2N group on Galois
                                           -- Field GF[2^409],
                                           -- Koblitz curve
                       ec2nGF571Random(12),
                                           -- EC2N group on Galois
                                           -- Field GF[2^571],
                                           -- random seed
                       ec2nGF571Koblitz(13)
                                           -- EC2N group on Galois
                                           -- Field GF[2^571],
                                           -- Koblitz curve
                   }

   IkeGroupType ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "Values for Oakley key computation group types
                   negotiated for the ISAKMP SA by IKE in Phase I.
                   They are also used in Phase II when perfect forward
                   secrecy is in use.  These are values for SA Attribute
                   type Group Type (5)."
       REFERENCE   "RFC 2409 appendix A"
       SYNTAX      INTEGER {
                       reserved(0),        -- reserved in IKE
                       modp(1),            -- modular eponentiation

                                           -- group
                       ecp(2),             -- elliptic curve group over
                                           -- Galois Field GF[P]
                       ec2n(3)             -- elliptic curve group over
                                           -- Galois Field GF[2^N]
                   }

   IkePrf ::= TEXTUAL-CONVENTION
       DISPLAY-HINT "d"
       STATUS      current
       DESCRIPTION "Values for Pseudo-Random Functions used with
                   with the hash algorithm negotiated for the ISAKMP SA
                   by IKE in Phase I.  There are currently no
                   pseudo-random functions defined, the default HMAC is
                   always used.  These are values for SA Attribute type
                   PRF (13).

                   Unused values <= 65000 are reserved to IANA.

                   Values 65001-65535 are for private use among
                   mutually consenting parties."
```

```
       REFERENCE   "RFC 2409 appendix A"
       SYNTAX      Unsigned32 (0..65535)

   IkeNotifyMessageType ::= TEXTUAL-CONVENTION
       STATUS      current
       DESCRIPTION "These are the values for the types of notification
                   messages.  They are used as the Notify Message Type
                   field in the Notification Payload.

                   This textual convention merges the types
                   for error types (in the range 1-16386) and for
                   notification types (in the range 16384-65535).

                   This textual convention is a merge of values
                   defined by ISAKMP with the additional values
                   defined in the IPsec DOI.

                   The values 16001-16383 are reserved for private use
                   as error types amongst cooperating systems.

                   The values 32001-32767 are reserved for private use
                   as notification types amongst cooperating systems."
       REFERENCE   "RFC 2408 section 3.14.1 and RFC 2407 sections 4.6.3
                   and 6.10"
       SYNTAX      INTEGER {

                       -- Values defined for errors in ISAKMP
                       --
                       unknown(0),         -- reserved in DOI
                                           -- used for unknown in MIBs
                       invalidPayloadType(1),
                       doiNotSupported(2),
                       situationNotSupported(3),
                       invalidCookie(4),
                       invalidMajorVersion(5),
                       invalidMinorVersion(6),
                       invalidExchangeType(7),
                       invalidFlags(8),
                       invalidMessageId(9),
                       invalidProtocolId(10),
                       invalidSpi(11),
                       invalidTransformId(12),
                       attributesNotSupported(13),
                       noProposalChosen(14),
                       badProposalSyntax(15),
                       payloadMalformed(16),
                       invalidKeyInformation(17),
```

```
                         invalidIdInformation(18),
                         invalidCertEncoding(19),
                         invalidCertificate(20),
                         certTypeUnsupported(21),
                         invalidCertAuthority(22),
                         invalidHashInformation(23),
                         authenticationFailed(24),
                         invalidSignature(25),
                         addressNotification(26),
                         notifySaLifetime(27),
                         certificateUnavailable(28),
                         unsupportedExchangeType(29),
                         unequalPayloadLengths(30),

                         -- values defined for errors in IPsec DOI
                         -- (none)

                         -- values defined for notification in ISAKMP
                         -- (none)

                         -- values defined for notification in IPsec
                         -- DOI
                         responderLifetime(24576),
                                             -- used to communicate IPsec
                                             -- SA lifetime chosen by the
                                             -- responder

                         replayStatus(24577),
                                             -- used for positive
                                             -- confirmation of the
                                             -- responder's election on
                                             -- whether or not he is to
                                             -- perform anti-replay
                                             -- detection

                         initialContact(24578)
                                             -- used when one side wishes
                                             -- to inform the other that
                                             -- this is the first SA being
                                             -- established with the
                                             -- remote system
                     }
   END
```

5. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

6. Acknowledgements

Thanks are extended to Tim Jenkins for his cooperation in developing this MIB.

7. Revision History

This section will be removed before publication.

February 3, 1999. Initial release as draft-shriver-doi-tc-mib-00.txt, due to issues as to whether the MIB was an IPsec or IPsecond work item.

March 22, 1999. Released as draft-ietf-ipsec-doi-tc-mib-00.txt. Added IsakmpDOI textual convention.

October 13, 1999. Use real number in experimental branch. Added IsakmpExchangeType and IkeExchangeType. Split IkeNotifyMessageType off of IsakmpNotifyMessageType, and removed IPsec DOI values from the latter. Corrected latest values of IkeAuthMethod, there had been some "number grabbing" in Internet-Drafts, now tracking the IKE Internet-Draft. Cleaned up references.

October 15, 1999. Removed stray comma in MIB.

June 13, 2000. Enforced consistent capitalization of IPsec.

November 22, 2000. Updated with the recent IANA assignments, particularly for AES, also from RFC 2857. Removed any numbers assigned only in the IKE Internet-Draft, since those cannot go in an RFC, and this is going out first.

October 3, 2001. Some changes in descriptions from readers' comments. For those variables defined as enumerations, where the protocol defines the value 0 as reserved, but the MIBs use the value 0 to indicate none, change the naming to none, and properly document the dual meaning.

November 29, 2001. Added missing status "connected" in IsakmpNotifyMessageType.

February 27, 2003. Catch up with changes in RFC authoring requirements. Add some new values that appear to have been assigned by the IANA. Change MIB name to ianaIPsecIsakmpIkeDoiTcMib, to make it clear that this is IANA-maintained.

8. Normative References

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

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

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

[RFC2578] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999

[RFC2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999

[RFC2580] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999

9. Informative References

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

[RFC3410] Case, J., Mundy, R., Partain, D. and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

10. Security Considerations

Since this MIB defines only textual conventions, there are no security considerations. Security considerations exist only when managed objects are defined with these textual conventions.

11. IANA Considerations

This document is the MIB definitions corresponding to a group of "magic numberes" that are maintained by the IANA. The IANA will maintain the MIB in this document as they assign new values of these magic numbers.

This MIB will be maintained in the same manner as the IANAifType-MIB.

12. Author's Address

John Shriver
Sockeye Networks
52 Second Ave., Suite 100
Waltham, MA 02451

Phone: +1-781-693-7067
E-mail: jshriver+ietf@sockeye.com

13. Full Copyright Statement

Expires August 2003