IPSP
Internet-Draft
Intended status: Informational
Expires: April 22, 2007

M. Baer
Sparta, Inc.
R. Charlet
Self
W. Hardaker
Sparta, Inc.
R. Story
Revelstone Software
C. Wang
ARO/North Carolina State University

October 19, 2006

IPsec Security Policy IPsec Action MIB
draft-ietf-ipsp-ipsecaction-mib-02.txt

Status of this Memo

Copyright Notice

Abstract

This document defines an SMIv2 Management Information Base (MIB) module for configuring IPsec actions for the security policy database (SPD) of a device that uses the IPsec Security Policy Database Configuration MIB for configuring the IPSec protocol actions on that device. The IPsec Action MIB integrates directly with the IPsec Security Policy Database Configuration MIB and it is meant to work within the framework of an action referenced by that MIB.

Table of Contents

1. Introduction

This document defines a MIB module for configuration of an IPsec action within the IPsec security policy database (SPD). This module works within the framework of the IPsec Security Policy Database Configuration MIB (IPSEC-SPD-MIB) [RFCZZZZ]. It can be referenced as an action by the IPSEC-SPD-MIB and is used to configure IPsec SA's [RFC2401] that are created for network traffic between devices.

The companion document [RFCZZZZ], documents the IPsec Security Policy Database Configuration MIB (IPSEC-SPD-MIB). For information surrounding the configuration of IKE and its parameters, see the companion document [RFCYYYY] which documents the IPsec Security Policy IKE Action MIB.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. The Internet-Standard 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. 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].

4. Relationship to the DMTF Policy Model

The Distributed Management Task Force has created an object oriented model of IPsec policy information known as the IPsec Policy Model White Paper [IPPMWP]. The "IPsec Configuration Policy Model" (IPCP) [RFC3585] is based in large part on the DMTF's IPsec policy model. The IPCP document describes a model for configuring IPsec. This MIB module is a task specific derivation (i.e. an SMIv2 instantiation) of the IPCP's IPsec configuration model for use over SNMPv3. This MIB

includes the necessary transform, negotiation, and IPsec action information required to create an IPsec SA within the IPsec Policy framework.

5. MIB Module Overview

The MIB module describes the necessary information to implement IPsec actions and their associated Security Associations referred to by the IPsec Security Policy Database Configuration MIB. A basic understanding of IPsec processing, of the IPsec Configuration Policy Model and of how actions fit in to the framework of the IPSEC-SPD-MIB are required to use this MIB properly. When referring to an action in this MIB from the IPSEC-SPD-MIB, the filters within the IPSEC-SPD-MIB that are associated to the action are limited to those that are supported by IPsec [RFC2401] and this MIB.

6. MIB definition

The following MIB Module imports from: [RFC2578], [RFC2579], [RFC2580], [RFC3289], [RFC3411], [RFC4001].

```
IPSEC-IPSECACTION-MIB DEFINITIONS ::= BEGIN


IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, Integer32,
    Unsigned32
                                    FROM SNMPv2-SMI
                                         -- [rfc2578]

    TEXTUAL-CONVENTION, RowStatus, TruthValue, TimeStamp,
    StorageType
                                    FROM SNMPv2-TC
                                         -- [rfc2579]

    MODULE-COMPLIANCE, OBJECT-GROUP
                                    FROM SNMPv2-CONF
                                         -- [rfc2580]

    SnmpAdminString                 FROM SNMP-FRAMEWORK-MIB
                                         -- [rfc3411]

    InetAddressType, InetAddress
                                    FROM INET-ADDRESS-MIB
                                         -- [rfc4001]
```

```
       spdActions, SpdIPPacketLogging, SpdAdminStatus
                                       FROM IPSEC-SPD-MIB
                                            -- [rfcZZZZ]

       IfDirection
                                       FROM DIFFSERV-MIB
                                            -- [rfc3289]
       ;

   --
   -- module identity
   --

   ipsaMIB MODULE-IDENTITY
       LAST-UPDATED "200610170000Z"    -- 17 October 2006
       ORGANIZATION "IETF IP Security Policy Working Group"
       CONTACT-INFO "Michael Baer
                     P.O. Box 72682
                     Davis, CA 95617
                     Phone: +1 530 902 3131
                     Email: baerm@tislabs.com

                     Ricky Charlet
                     Email: rcharlet@alumni.calpoly.edu

                     Wes Hardaker
                     Sparta, Inc.
                     P.O. Box 382
                     Davis, CA  95617
                     Phone: +1 530 792 1913
                     Email: hardaker@tislabs.com

                     Robert Story
                     Revelstone Software
                     PO Box 1812
                     Tucker, GA 30085
                     Phone: +1 770 617 3722
                     Email: rstory@sparta.com

                     Cliff Wang
                     ARO/North Carolina State University
                     4300 S. Miami Blvd.
                     RTP, NC 27709
                     E-Mail: cliffwangmail@yahoo.com"
       DESCRIPTION
        "The MIB module defines IPsec actions for managing IPsec
         Security Policy.
```

```
   -- Revision History

       REVISION     "200610170000Z"    -- 17 October 2006
       DESCRIPTION  "Initial version, published as RFC XXXX."
       -- RFC-editor assigns XXXX

       ::= { spdActions 1 }

   --
   -- groups of related objects
   --

   ipsaConfigObjects         OBJECT IDENTIFIER
        ::= { ipsaMIB 1 }
   ipsaNotificationObjects   OBJECT IDENTIFIER
        ::= { ipsaMIB 2 }
   ipsaConformanceObjects    OBJECT IDENTIFIER
        ::= { ipsaMIB 3 }

   --
   -- Textual Conventions
   --

   IpsecDoiEncapsulationMode ::= TEXTUAL-CONVENTION
       DISPLAY-HINT "d"
       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.
                    Currently assigned values at the time of this
                    writing:

                        reserved(0),        -- reserved in DOI
                        tunnel(1),
                        transport(2)

                    Values 61440-65535 are for private use."
       SYNTAX      Unsigned32 (0..65535)
```

```
   IpsecDoiIpcompTransform ::= TEXTUAL-CONVENTION
       DISPLAY-HINT "d"
       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.
                   Currently assigned values at the time of this
                   writing:

                       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

                   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      Unsigned32 (0..255)

   IpsecDoiAuthAlgorithm ::= TEXTUAL-CONVENTION
       DISPLAY-HINT "d"
       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.
                   Currently assigned values at the time of this
                   writing:
```

```
                    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

                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      Unsigned32 (0..65535)


IpsecDoiEspTransform ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    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).

                Currently assigned values at the time of this
                writing:

                    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

                The values 249-255 are reserved for private use
                amongst cooperating systems."
    REFERENCE   "RFC 2407 sections 4.4.4 and 6.5,
                IANA"
    SYNTAX      Unsigned32 (0..255)

IpsecDoiIdentType ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    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.

                Currently assigned values at the time of this
                writing:

                    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 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      Unsigned32 (0..255)

    IpsaCredentialType ::= TEXTUAL-CONVENTION
        STATUS   current
        DESCRIPTION
            "IpsaCredentialType identifies the type of credential
             contained in a corresponding IpsaIdentityFilter object."
        SYNTAX      INTEGER { reserved(0),
                              unknown(1),
                              sharedSecret(2),
                              x509(3),
                              kerberos(4) }

    IpsaIdentityFilter ::=  TEXTUAL-CONVENTION
        STATUS   current
        DESCRIPTION
            "IpsaIdentityFilter contains a string encoded Identity Type
```

```
            value to be used in comparisons against an IKE Identity
            payload.  Wherever this TC is used, there SHOULD be an
            accompanying column which uses the IpsecDoiIdentType TC to
            specify the type of data in this object.

            See the IpsecDoiIdentType TC for the supported identity
            types available.  Note that the IpsecDoiIdentType TC
            sepcifies how to encode binary values, while this object
            will contain human readable string versions."
        SYNTAX      OCTET STRING (SIZE(1..256))

    --
    -- Preconfigured Action Table
    --

    ipsaSaPreconfiguredActionTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF IpsaSaPreconfiguredActionEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table is a list of non-negotiated IPsec actions (SAs)
             that can be performed and contains or indicates the data
             necessary to create such an SA."
        ::= { ipsaConfigObjects 1 }

    ipsaSaPreconfiguredActionEntry OBJECT-TYPE
        SYNTAX      IpsaSaPreconfiguredActionEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "One entry in the ipsaSaPreconfiguredActionTable."
        INDEX       { ipsaSaPreActActionName, ipsaSaPreActSADirection }
        ::= { ipsaSaPreconfiguredActionTable 1 }

    IpsaSaPreconfiguredActionEntry ::= SEQUENCE {
        ipsaSaPreActActionName                SnmpAdminString,
        ipsaSaPreActSADirection               IfDirection,
        ipsaSaPreActActionDescription         SnmpAdminString,
        ipsaSaPreActActionLifetimeSec         Unsigned32,
        ipsaSaPreActActionLifetimeKB          Unsigned32,
        ipsaSaPreActDoActionLogging           TruthValue,
        ipsaSaPreActDoPacketLogging           SpdIPPacketLogging,
        ipsaSaPreActDFHandling                INTEGER,
        ipsaSaPreActActionType                IpsecDoiEncapsulationMode,
        ipsaSaPreActAHSPI                     Integer32,
        ipsaSaPreActAHTransformName           SnmpAdminString,
        ipsaSaPreActAHSharedSecretName        SnmpAdminString,
        ipsaSaPreActESPSPI                    Integer32,
```

```
        ipsaSaPreActESPTransformName          SnmpAdminString,
        ipsaSaPreActESPEncSecretName          SnmpAdminString,
        ipsaSaPreActESPAuthSecretName         SnmpAdminString,
        ipsaSaPreActIPCompSPI                 Integer32,
        ipsaSaPreActIPCompTransformName       SnmpAdminString,
        ipsaSaPreActPeerGatewayIdName         SnmpAdminString,
        ipsaSaPreActLastChanged               TimeStamp,
        ipsaSaPreActStorageType               StorageType,
        ipsaSaPreActRowStatus                 RowStatus
    }

    ipsaSaPreActActionName OBJECT-TYPE
        SYNTAX      SnmpAdminString (SIZE(1..32))
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This object contains the name of this
             SaPreconfiguredActionEntry."
        ::= { ipsaSaPreconfiguredActionEntry 1 }

    ipsaSaPreActSADirection OBJECT-TYPE
        SYNTAX      IfDirection
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This object indicates whether a row applies to egress
             or ingress SAs"
        ::= { ipsaSaPreconfiguredActionEntry 2 }


    ipsaSaPreActActionDescription OBJECT-TYPE
        SYNTAX      SnmpAdminString
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "An administratively assigned string which can be used
             to describe what the action does."
        DEFVAL { "" }
        ::= { ipsaSaPreconfiguredActionEntry 3 }

    ipsaSaPreActActionLifetimeSec OBJECT-TYPE
        SYNTAX      Unsigned32
        UNITS       "seconds"
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaSaPreActActionLifetimeSec specifies how long in seconds
             the security association derived from this action is used.
```

```
            The default lifetime is 8 hours.

            Note: the actual lifetime of the preconfigured SA will be
            the lesser of the value of this object and of the value of
            the MaxLifetimeSecs property of the associated transform.

            A value of 0 indicates no time limit on the lifetime
            of the SA."
        DEFVAL      { 28800 }
        ::= { ipsaSaPreconfiguredActionEntry 4 }

    ipsaSaPreActActionLifetimeKB OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaSaPreActActionLifetimeKB specifies how long the
            security association derived from this action is used.
            After this value in KiloBytes has passed through the
            security association, this SA SHOULD be destroyed.

            Note: the actual lifetime of the preconfigured SA will be
            the lesser of the value of this object and of the value of
            the MaxLifetimeKB property of the associated transform.

            The default value, '0', indicates no kilobyte limit."
        DEFVAL      { 0 }
        ::= { ipsaSaPreconfiguredActionEntry 5 }

    ipsaSaPreActDoActionLogging OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaSaPreActDoActionLogging specifies whether or not an
            audit message SHOULD be logged when a preconfigured SA is
            created."
        DEFVAL { false }
        ::= { ipsaSaPreconfiguredActionEntry 6 }

    ipsaSaPreActDoPacketLogging OBJECT-TYPE
        SYNTAX      SpdIPPacketLogging
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaSaPreActDoPacketLogging specifies whether or not an
            audit message SHOULD be logged and if there is logging, how
            many bytes of the packet to place in the notification."
```

```
        DEFVAL { -1 }
        ::= { ipsaSaPreconfiguredActionEntry 7 }

    ipsaSaPreActDFHandling OBJECT-TYPE
        SYNTAX     INTEGER {
                     copy(1),      -- indicates copy the DF bit from the
                                   -- internal to external IP header.
                     set(2),       -- set the DF bit in the external IP
                                   -- header to 1.
                     clear(3)      -- clear the DF bit in the external IP
                                   -- header to 0.
                   }
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object specifies how to process the DF bit in packets
             sent through the preconfigured SA.  This object is not used
             for transport SAs."
        DEFVAL { copy }
        ::= { ipsaSaPreconfiguredActionEntry 8 }

    ipsaSaPreActActionType OBJECT-TYPE
        SYNTAX      IpsecDoiEncapsulationMode
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object specifies the encapsulation mode to use for the
             preconfigured SA: tunnel or transport mode."
        DEFVAL { 1 }
        ::= { ipsaSaPreconfiguredActionEntry 9 }

    ipsaSaPreActAHSPI OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object represents the SPI value for the AH SA."
        ::= { ipsaSaPreconfiguredActionEntry 10 }

    ipsaSaPreActAHTransformName OBJECT-TYPE
        SYNTAX      SnmpAdminString (SIZE(0..32))
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object is the name of the AH transform to use as an
             index into the AHTransformTable.  A zero length value
             indicates no transform of this type is used."
        ::= { ipsaSaPreconfiguredActionEntry 11 }
```

```
   ipsaSaPreActAHSharedSecretName OBJECT-TYPE
       SYNTAX      SnmpAdminString(SIZE(0..32))
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "This object contains a name value to be used as an index
            into the ipsaCredentialTable which holds the pertinent
            keying information for the AH SA."
       ::= { ipsaSaPreconfiguredActionEntry 12 }

   ipsaSaPreActESPSPI OBJECT-TYPE
       SYNTAX      Integer32
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "This object represents the SPI value for the ESP SA."
       ::= { ipsaSaPreconfiguredActionEntry 13 }

   ipsaSaPreActESPTransformName OBJECT-TYPE
       SYNTAX      SnmpAdminString (SIZE(0..32))
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "This object is the name of the ESP transform to use as an
            index into the ESPTransformTable.  A zero length value
            indicates no transform of this type is used."
       ::= { ipsaSaPreconfiguredActionEntry 14 }

   ipsaSaPreActESPEncSecretName OBJECT-TYPE
       SYNTAX      SnmpAdminString(SIZE(0..32))
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "This object contains a name value to be used as an index
            into the ipsaCredentialTable which holds the pertinent
            keying information for the encryption algorithm of the ESP
            SA."
       ::= { ipsaSaPreconfiguredActionEntry 15 }

   ipsaSaPreActESPAuthSecretName OBJECT-TYPE
       SYNTAX      SnmpAdminString(SIZE(0..32))
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "This object contains a name value to be used as an index
            into the ipsaCredentialTable which holds the pertinent
            keying information for the authentication algorithm of the
            ESP SA."
```

```
        ::= { ipsaSaPreconfiguredActionEntry 16 }

    ipsaSaPreActIPCompSPI OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object represents the SPI value for the IPComp SA."
        ::= { ipsaSaPreconfiguredActionEntry 17 }

    ipsaSaPreActIPCompTransformName OBJECT-TYPE
        SYNTAX      SnmpAdminString (SIZE(0..32))
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object is the name of the IPComp transform to use as
             an index into the IPCompTransformTable.  A zero length
             value indicates no transform of this type is used."
        ::= { ipsaSaPreconfiguredActionEntry 18 }

    ipsaSaPreActPeerGatewayIdName OBJECT-TYPE
        SYNTAX      SnmpAdminString (SIZE(0..32))
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object indicates the peer id name of the peer
             gateway.  This object can be used to look up the peer
             gateway address in the ipsaPeerIdentityTable.

             This object is only used when initiating a tunnel SA, and
             is not used for transport SAs.  If ipsaSaPreActActionType
             specifies tunnel mode and this object is empty, the peer
             gateway is determined from the source or destination of the
             packet."
         DEFVAL { "" }
        ::= { ipsaSaPreconfiguredActionEntry 19 }

    ipsaSaPreActLastChanged  OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of sysUpTime when this row was last modified or
             created either through SNMP SETs or by some other external
             means.

             If this row has not been modified since the last
             re-initialization of the network management subsystem, this
```

```
            object SHOULD have a zero value."
        ::= { ipsaSaPreconfiguredActionEntry 20 }

    ipsaSaPreActStorageType OBJECT-TYPE
        SYNTAX      StorageType
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "The storage type for this row.  Rows in this table which
             were created through an external process MAY have a storage
             type of readOnly or permanent.

             For a storage type of permanent, none of the columns have
             to be writable."
        DEFVAL { nonVolatile }
        ::= { ipsaSaPreconfiguredActionEntry 21 }

    ipsaSaPreActRowStatus OBJECT-TYPE
        SYNTAX      RowStatus
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object indicates the conceptual status of this row.

             The value of this object has no effect on whether other
             objects in this conceptual row can be modified.

             If active, this object MUST remain active if it is
             referenced by an active row in another table.  An attempt
             to set it to anything other than active while it is
             referenced by an active row in another table MUST result in
             an inconsistentValue error."
        ::= { ipsaSaPreconfiguredActionEntry 22 }

    --
    -- AH transform definition table
    --


    ipsaAhTransformTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF IpsaAhTransformEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table lists all the AH transforms which can be used to
             build IPsec proposals."
        ::= { ipsaConfigObjects 2 }
```

```
   ipsaAhTransformEntry OBJECT-TYPE
       SYNTAX      IpsaAhTransformEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "This entry contains the attributes of one AH transform."
       INDEX       { ipsaAhTranName }
       ::= { ipsaAhTransformTable 1 }

   IpsaAhTransformEntry ::= SEQUENCE {
       ipsaAhTranName                    SnmpAdminString,
       ipsaAhTranMaxLifetimeSec          Unsigned32,
       ipsaAhTranMaxLifetimeKB           Unsigned32,
       ipsaAhTranAlgorithm               IpsecDoiAuthAlgorithm,
       ipsaAhTranReplayProtection        TruthValue,
       ipsaAhTranReplayWindowSize        Unsigned32,
       ipsaAhTranLastChanged             TimeStamp,
       ipsaAhTranStorageType             StorageType,
       ipsaAhTranRowStatus               RowStatus
   }

   ipsaAhTranName OBJECT-TYPE
       SYNTAX      SnmpAdminString (SIZE(1..32))
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "This object contains the name of this AH transform.  This
           row
            will be referred to by an ipsaIpsecTransformsEntry."
       ::= { ipsaAhTransformEntry 1 }

   ipsaAhTranMaxLifetimeSec OBJECT-TYPE
       SYNTAX      Unsigned32
       UNITS       "seconds"
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "ipsaAhTranMaxLifetimeSec specifies how long in seconds the
            security association derived from this transform SHOULD be
            used.

            A value of 0 indicates that the default lifetime of
            8 hours SHOULD be used."
       ::= { ipsaAhTransformEntry 2 }

   ipsaAhTranMaxLifetimeKB OBJECT-TYPE
       SYNTAX      Unsigned32
       MAX-ACCESS  read-create
```

```
        STATUS      current
        DESCRIPTION
            "ipsaAhTranMaxLifetimeKB specifies how long in kilobytes the
             security association derived from this transform SHOULD be
             used."
        ::= { ipsaAhTransformEntry 3 }

    ipsaAhTranAlgorithm OBJECT-TYPE
        SYNTAX      IpsecDoiAuthAlgorithm
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object specifies the AH algorithm for this transform."
        ::= { ipsaAhTransformEntry 4 }

    ipsaAhTranReplayProtection OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaAhTranReplayProtection indicates whether or not anti
             replay service is to be provided by this SA."
        ::= { ipsaAhTransformEntry 5 }

    ipsaAhTranReplayWindowSize OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaAhTranReplayWindowSize indicates the size, in bits, of
             the replay window to use if replay protection is true for
             this transform.  The window size is assumed to be a power
             of two.  If Replay Protection is false, this value can be
             ignored."
        ::= { ipsaAhTransformEntry 6 }

    ipsaAhTranLastChanged OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of sysUpTime when this row was last modified or
             created either through SNMP SETs or by some other external
             means.

             If this row has not been modified since the last
             re-initialization of the network management subsystem, this
             object SHOULD have a zero value."
```

```
        ::= { ipsaAhTransformEntry 7 }

    ipsaAhTranStorageType OBJECT-TYPE
        SYNTAX      StorageType
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "The storage type for this row.  Rows in this table which
             were created through an external process MAY have a storage
             type of readOnly or permanent.

             For a storage type of permanent, none of the columns have
             to be writable."
        DEFVAL { nonVolatile }
        ::= { ipsaAhTransformEntry 8 }

    ipsaAhTranRowStatus OBJECT-TYPE
        SYNTAX      RowStatus
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object indicates the conceptual status of this row.

             The value of this object has no effect on whether other
             objects in this conceptual row can be modified.

             If active, this object MUST remain active if it is
             referenced by an active row in another table.  An attempt
             to set it to anything other than active while it is
             referenced by an active row in another table MUST result in
             an inconsistentValue error."
        ::= { ipsaAhTransformEntry 9 }


    --
    -- ESP transform definition table
    --


    ipsaEspTransformTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF IpsaEspTransformEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table lists all the ESP transforms which can be used
             to build IPsec proposals"
        ::= { ipsaConfigObjects 3 }
```

```
   ipsaEspTransformEntry OBJECT-TYPE
       SYNTAX      IpsaEspTransformEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "This entry contains the attributes of one ESP transform."
       INDEX       { ipsaEspTranName }
       ::= { ipsaEspTransformTable 1 }

   IpsaEspTransformEntry ::= SEQUENCE {
       ipsaEspTranName                         SnmpAdminString,
       ipsaEspTranMaxLifetimeSec               Unsigned32,
       ipsaEspTranMaxLifetimeKB                Unsigned32,
       ipsaEspTranCipherTransformId            IpsecDoiEspTransform,
       ipsaEspTranCipherKeyLength              Unsigned32,
       ipsaEspTranCipherKeyRounds              Unsigned32,
       ipsaEspTranIntegrityAlgorithmId         IpsecDoiAuthAlgorithm,
       ipsaEspTranReplayPrevention             TruthValue,
       ipsaEspTranReplayWindowSize             Unsigned32,
       ipsaEspTranLastChanged                  TimeStamp,
       ipsaEspTranStorageType                  StorageType,
       ipsaEspTranRowStatus                    RowStatus
   }

   ipsaEspTranName OBJECT-TYPE
       SYNTAX      SnmpAdminString (SIZE(1..32))
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "The name of this particular espTransform be referred to by
            an ipsaIpsecTransformsEntry."
       ::= { ipsaEspTransformEntry 1 }

   ipsaEspTranMaxLifetimeSec OBJECT-TYPE
       SYNTAX      Unsigned32
       UNITS       "seconds"
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "ipsaEspTranMaxLifetimeSec specifies how long in seconds the
            security association derived from this transform SHOULD be
            used.

            A value of 0 indicates that the default lifetime of
            8 hours SHOULD be used."
       ::= { ipsaEspTransformEntry 2 }

   ipsaEspTranMaxLifetimeKB OBJECT-TYPE
```

```
        SYNTAX      Unsigned32
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaEspTranMaxLifetimeKB specifies how long in kilobytes
             the security association derived from this transform is
             used."
        ::= { ipsaEspTransformEntry 3 }

    ipsaEspTranCipherTransformId OBJECT-TYPE
        SYNTAX      IpsecDoiEspTransform
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object specifies the transform ID of the ESP cipher
             algorithm."
        ::= { ipsaEspTransformEntry 4 }


    ipsaEspTranCipherKeyLength OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object specifies, in bits, the key length for
             the ESP cipher algorithm."
        ::= { ipsaEspTransformEntry 5 }

    ipsaEspTranCipherKeyRounds OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object specifies the number of key rounds for
             the ESP cipher algorithm."
        ::= { ipsaEspTransformEntry 6 }

    ipsaEspTranIntegrityAlgorithmId OBJECT-TYPE
        SYNTAX      IpsecDoiAuthAlgorithm
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object specifies the ESP integrity algorithm ID."
        ::= { ipsaEspTransformEntry 7 }

    ipsaEspTranReplayPrevention OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-create
```

```
        STATUS      current
        DESCRIPTION
            "ipsaEspTranReplayPrevention indicates whether or not
             anti-replay service is to be provided by this SA."
        ::= { ipsaEspTransformEntry 8 }

    ipsaEspTranReplayWindowSize OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaEspTranReplayWindowSize indicates the size, in bits, of
             the replay window to use if replay protection is true for
             this transform.  The window size is assumed to be a power
             of two.  If Replay Protection is false, this value can be
             ignored."
        ::= { ipsaEspTransformEntry 9 }

    ipsaEspTranLastChanged OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of sysUpTime when this row was last modified or
             created either through SNMP SETs or by some other external
             means.

             If this row has not been modified since the last
             re-initialization of the network management subsystem, this
             object SHOULD have a zero value."
        ::= { ipsaEspTransformEntry 10 }

    ipsaEspTranStorageType OBJECT-TYPE
        SYNTAX      StorageType
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "The storage type for this row.  Rows in this table which
             were created through an external process MAY have a storage
             type of readOnly or permanent.

             For a storage type of permanent, none of the columns have
             to be writable."
        DEFVAL { nonVolatile }
        ::= { ipsaEspTransformEntry 11 }

    ipsaEspTranRowStatus OBJECT-TYPE
        SYNTAX      RowStatus
```

```
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object indicates the conceptual status of this row.

             The value of this object has no effect on whether other
             objects in this conceptual row can be modified.

             If active, this object MUST remain active if it is
             referenced by a row in another table.  An attempt to set it
             to anything other than active while it is referenced by an
             active row in another table MUST result in an
             inconsistentValue error."
        ::= { ipsaEspTransformEntry 12 }


    --
    -- IP compression transform definition table
    --

    ipsaIpcompTransformTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF IpsaIpcompTransformEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table lists all the IP compression transforms which
             can be used to build IPsec proposals during negotiation of
             a phase 2 SA."
        ::= { ipsaConfigObjects 4 }

    ipsaIpcompTransformEntry OBJECT-TYPE
        SYNTAX      IpsaIpcompTransformEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This entry contains the attributes of one IP compression
             transform."
        INDEX       { ipsaIpcompTranName }
        ::= { ipsaIpcompTransformTable 1 }

    IpsaIpcompTransformEntry ::= SEQUENCE {
        ipsaIpcompTranName                      SnmpAdminString,
        ipsaIpcompTranMaxLifetimeSec            Unsigned32,
        ipsaIpcompTranMaxLifetimeKB             Unsigned32,
        ipsaIpcompTranAlgorithm                 IpsecDoiIpcompTransform,
        ipsaIpcompTranDictionarySize            Unsigned32,
        ipsaIpcompTranPrivateAlgorithm          Unsigned32,
        ipsaIpcompTranLastChanged               TimeStamp,
```

```
        ipsaIpcompTranStorageType               StorageType,
        ipsaIpcompTranRowStatus                 RowStatus
    }

    ipsaIpcompTranName OBJECT-TYPE
        SYNTAX      SnmpAdminString (SIZE(1..32))
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "The name of this ipsaIpcompTransformEntry."
        ::= { ipsaIpcompTransformEntry 1 }

    ipsaIpcompTranMaxLifetimeSec OBJECT-TYPE
        SYNTAX      Unsigned32
        UNITS       "seconds"
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaIpcompTranMaxLifetimeSec specifies how long in seconds
             the security association derived from this transform SHOULD
             be used.

             A value of 0 indicates that the default lifetime of
             8 hours SHOULD be used."
        ::= { ipsaIpcompTransformEntry 2 }

    ipsaIpcompTranMaxLifetimeKB OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaIpcompTranMaxLifetimeKB specifies how long in kilobytes
             the security association derived from this transform SHOULD
             be used."
        ::= { ipsaIpcompTransformEntry 3 }

    ipsaIpcompTranAlgorithm OBJECT-TYPE
        SYNTAX      IpsecDoiIpcompTransform
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaIpcompTranAlgorithm specifies the transform ID of the
             IP compression algorithm."
        ::= { ipsaIpcompTransformEntry 4 }

    ipsaIpcompTranDictionarySize OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-create
```

```
        STATUS      current
        DESCRIPTION
            "If the algorithm in ipsaIpcompTranAlgorithm requires a
             dictionary size configuration parameter, then this is the
             place to put it.  This object specifies the log2 maximum
             size of the dictionary for the compression algorithm."
        ::= { ipsaIpcompTransformEntry 5 }

    ipsaIpcompTranPrivateAlgorithm OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "If ipsaIpcompTranPrivateAlgorithm has a value other zero,
             then it is up to the vendors implementation to determine
             the meaning of this field and substitute a data compression
             algorithm in place of ipsaIpcompTranAlgorithm."
        ::= { ipsaIpcompTransformEntry 6 }

    ipsaIpcompTranLastChanged OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of sysUpTime when this row was last modified or
             created either through SNMP SETs or by some other external
             means.

             If this row has not been modified since the last
             re-initialization of the network management subsystem, this
             object SHOULD have a zero value."
        ::= { ipsaIpcompTransformEntry 7 }

    ipsaIpcompTranStorageType OBJECT-TYPE
        SYNTAX      StorageType
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "The storage type for this row.  Rows in this table which
             were created through an external process MAY have a storage
             type of readOnly or permanent.

             For a storage type of permanent, none of the columns have
             to be writable."
        DEFVAL { nonVolatile }
        ::= { ipsaIpcompTransformEntry 8 }

    ipsaIpcompTranRowStatus OBJECT-TYPE
```

```
        SYNTAX      RowStatus
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object indicates the conceptual status of this row.

             The value of this object has no effect on whether other
             objects in this conceptual row can be modified.

             If active, this object MUST remain active if it is
             referenced by an active row in another table.  An attempt
             to set it to anything other than active while it is
             referenced by an active row in another table MUST result in
             an inconsistentValue error."
        ::= { ipsaIpcompTransformEntry 9 }

    --
    -- Credential Table
    --

    ipsaCredentialTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF IpsaCredentialEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A table of credential values.  Example of Credentials are
             shared secrets, certificates or kerberos tickets."
        ::= { ipsaConfigObjects 5 }

    ipsaCredentialEntry OBJECT-TYPE
        SYNTAX      IpsaCredentialEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A row in the ipsaCredentialTable."
        INDEX   { ipsaCredName }
        ::= { ipsaCredentialTable 1 }

    IpsaCredentialEntry ::= SEQUENCE {
            ipsaCredName                SnmpAdminString,
            ipsaCredType                IpsaCredentialType,
            ipsaCredCredential          OCTET STRING,
            ipsaCredSize                Integer32,
            ipsaCredMngName             SnmpAdminString,
            ipsaCredRemoteID            OCTET STRING,
            ipsaCredAdminStatus         SpdAdminStatus,
            ipsaCredLastChanged         TimeStamp,
            ipsaCredStorageType         StorageType,
```

```
        ipsaCredRowStatus           RowStatus
    }

    ipsaCredName OBJECT-TYPE
        SYNTAX      SnmpAdminString(SIZE(1..32))
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This object represents the name for an entry in this table."
        ::= { ipsaCredentialEntry 1 }

    ipsaCredType OBJECT-TYPE
        SYNTAX      IpsaCredentialType
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object represents the type of the credential for this
             row."
        ::= { ipsaCredentialEntry 2 }

    ipsaCredCredential OBJECT-TYPE
        SYNTAX      OCTET STRING (SIZE(0..1024))
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object represents the credential value.

             If the size of the credential is greater than 1024, the
             credential MUST be configured via the ipsaCredSegmentTable.

             For credential type where the disclosure of the credential
             would compromise the credential (e.g. shared secrets), when
             this object is accessed for reading, it MUST return a null
             length (0 length) string and MUST NOT return the configured
             credential."
        ::= { ipsaCredentialEntry 3 }

    ipsaCredSize OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This value represents the size of the credential.

             If this value is greater than 1024, the ipsaCreCredential
             column will return an empty (0 length) string. In this
             case, the value of the credential is retrived from the
             ipsaCredSegmentTable.
```

```
            For credential type where the disclosure of the credential
            would compromise the credential (e.g. shared secrets), when
            this object is accessed for reading, it MUST return a value
            of 0 and MUST NOT return the size credential."
        ::= { ipsaCredentialEntry 4 }

    ipsaCredMngName OBJECT-TYPE
        SYNTAX      SnmpAdminString (SIZE(0..32))
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This value is used as an index into the
             ipsaIpsecCredMngServiceTable.  For IDs that have no
             credential management service, this value is left blank."
        ::= { ipsaCredentialEntry 5 }

    ipsaCredRemoteID OBJECT-TYPE
        SYNTAX      OCTET STRING(SIZE(0..256))
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object represents the Identification (e.g. user name)
             of the user of the key information on the remote site.  If
             there is no ID associated with this credential, the value
             of this object SHOULD be the null string."
        ::= { ipsaCredentialEntry 6 }

    ipsaCredAdminStatus OBJECT-TYPE
        SYNTAX      SpdAdminStatus
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "Indicates whether this credential is considered
             active.  Rows with a disabled status MUST NOT be used for
             any purpose, including IKE or IPSEC processing.

             For credentials whose size does not exeeced the maximum
             size for the ipsaCredCredential, it MAY be set to enabled
             during row creation. For larger credentials, it SHOULD be
             left as disabled until all rows have been uploaded to the
             ipsaCredSegmentTable."
        DEFVAL { disabled }
        ::= { ipsaCredentialEntry 7 }

    ipsaCredLastChanged  OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
```

```
        DESCRIPTION
            "The value of sysUpTime when this row was last modified or
             created either through SNMP SETs or by some other external
             means.

             If this row has not been modified since the last
             re-initialization of the network management subsystem, this
             object SHOULD have a zero value."
        ::= { ipsaCredentialEntry 8 }

    ipsaCredStorageType OBJECT-TYPE
        SYNTAX      StorageType
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "The storage type for this row.  Rows in this table which
             were created through an external process MAY have a storage
             type of readOnly or permanent.

             For a storage type of permanent, none of the columns have
             to be writable."
        DEFVAL { nonVolatile }
        ::= { ipsaCredentialEntry 9 }

    ipsaCredRowStatus OBJECT-TYPE
        SYNTAX      RowStatus
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This object indicates the conceptual status of this row.

             The value of this object has no effect on whether other
             objects in this conceptual row can be modified.

             If active, this object MUST remain active if it is
             referenced by an active row in another table.  An attempt
             to set it to anything other than active while it is
             referenced by an active row in another table MUST result in
             an inconsistentValue error."
        ::= { ipsaCredentialEntry 10 }


    --
    -- Credential Segement Value Table
    --

    ipsaCredentialSegmentTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF IpsaCredentialSegmentEntry
```

```
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A table of credential segments.  This table is used for
             credentials which are larger than the maximum size allowed
             for ipsaCredCredential."
        ::= { ipsaConfigObjects 6 }

    ipsaCredentialSegmentEntry OBJECT-TYPE
        SYNTAX      IpsaCredentialSegmentEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A row in the ipsaCredentialSegmentTable."
        INDEX   { ipsaCredName, ipsaCredSegIndex }
        ::= { ipsaCredentialSegmentTable 1 }

    IpsaCredentialSegmentEntry ::= SEQUENCE {
            ipsaCredSegIndex                Integer32,
            ipsaCredSegValue                OCTET STRING,
            ipsaCredSegLastChanged          TimeStamp,
            ipsaCredSegStorageType          StorageType,
            ipsaCredSegRowStatus            RowStatus
    }

    ipsaCredSegIndex OBJECT-TYPE
        SYNTAX      Integer32 (1..65535)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This object represents the segment number for this segment.

             By default, each segment will be 1024 octets. However, when
             this table is accessed using a context of 'ipsa4096',
             'ipsa8192' or 'ipsa16384' a segment size of 4096, 8192 or
             16384 (respectively) will be used instead.

             The number of rows which need to be retrieved or set can be
             calculated by obtaining the value of the ipsaCredSize
             column from the corresponding ipsaCredentialTable row and
             dividing it by the segment size."
        ::= { ipsaCredentialSegmentEntry 1 }

    ipsaCredSegValue OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
```

```
            "This object represents one segment of the credential.

             By default, each complete segment will be 1024 octets. (The
             last row for a given credential might be smaller, if the
             credential size is not a multiple of the segment size).

             An implementation MAY optionally support segment sizes of
             256, 4096, 8192 or the full object size when this table is
             is accessed using a context of 'ipsaCred256',
             'ipsaCred4096', 'ipsaCred8192' or 'ipsaCredFull'
             (respectively).

             The number of rows which need to be retrieved or set can be
             calculated by obtaining the value of the ipsaCredSize
             column from the corresponding ipsaCredentialTable row and
             dividing it by the segment size."
        ::= { ipsaCredentialSegmentEntry 2 }

    ipsaCredSegLastChanged  OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of sysUpTime when this credential was last
             modified or created either through SNMP SETs or by some
             other external means. Note that the last changed type will
             be the same for all segemnts of the credential.

             If this row has not been modified since the last
             re-initialization of the network management subsystem, this
             object SHOULD have a zero value."
        ::= { ipsaCredentialSegmentEntry 3 }

    ipsaCredSegStorageType OBJECT-TYPE
        SYNTAX      StorageType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The storage type for this row.  This object is
             read-only. Rows in this table have the same value as the
             ipsaCrendStorageType for the corresponding row in the
             ipsaCredentialTable.

             For a storage type of permanent, none of the columns have
             to be writable."
        DEFVAL { nonVolatile }
        ::= { ipsaCredentialSegmentEntry 4 }
```

```
   ipsaCredSegRowStatus OBJECT-TYPE
       SYNTAX      RowStatus
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "This object indicates the conceptual status of this row.

            The segment of this object has no effect on whether other
            objects in this conceptual row can be modified.

            If active, this object MUST remain active if it is
            referenced by an active row in another table.  An attempt
            to set it to anything other than active while it is
            referenced by an active row in another table MUST result in
            an inconsistentValue error."
       ::= { ipsaCredentialSegmentEntry 5 }

   --
   -- Peer Identity Table
   --

   ipsaPeerIdentityTable OBJECT-TYPE
       SYNTAX      SEQUENCE OF IpsaPeerIdentityEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "PeerIdentity is used to represent the identities that are
            used for peers to identify themselves in IKE phase I/II
            negotiations.  PeerIdentityTable aggregates the table
            entries that provide mappings between identities and their
            addresses."
       ::= { ipsaConfigObjects 7 }

   ipsaPeerIdentityEntry OBJECT-TYPE
       SYNTAX      IpsaPeerIdentityEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "peerIdentity matches a peer's identity to its address."
       INDEX { ipsaPeerIdName, ipsaPeerIdPriority }
       ::= { ipsaPeerIdentityTable 1 }

   IpsaPeerIdentityEntry ::= SEQUENCE {
       ipsaPeerIdName                          SnmpAdminString,
       ipsaPeerIdPriority                      Integer32,
       ipsaPeerIdType                          IpsecDoiIdentType,
       ipsaPeerIdValue                         IpsaIdentityFilter,
       ipsaPeerIdAddressType                   InetAddressType,
```

```
        ipsaPeerIdAddress                       InetAddress,
        ipsaPeerIdCredentialName                SnmpAdminString,
        ipsaPeerIdLastChanged                   TimeStamp,
        ipsaPeerIdStorageType                   StorageType,
        ipsaPeerIdRowStatus                     RowStatus
    }

    ipsaPeerIdName OBJECT-TYPE
        SYNTAX      SnmpAdminString (SIZE(1..32))
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This is an administratively assigned value that, together
             with ipsaPeerIdPriority, uniquely identifies an entry in
             this table."
        ::= { ipsaPeerIdentityEntry 1 }

    ipsaPeerIdPriority OBJECT-TYPE
        SYNTAX      Integer32 (0..2147483647)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This object, along with ipsaPeerIdName, uniquely identifies
             an entry in this table.  The priority also indicates the
             ordering of peer gateways from which to initiate or accept
             SAs.  The priority value is ordered from low to high.  For
             example, a row with a priority of 0 is used before a row
             with a priority of 1, a 1 before a 2, etc...."
        ::= { ipsaPeerIdentityEntry 2 }

    ipsaPeerIdType       OBJECT-TYPE
        SYNTAX      IpsecDoiIdentType
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaPeerIdType is an enumeration identifying the type of the
             Identity value."
        ::= { ipsaPeerIdentityEntry 3 }

    ipsaPeerIdValue     OBJECT-TYPE
        SYNTAX      IpsaIdentityFilter
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "ipsaPeerIdValue contains an Identity filter to be used to
             match against the identity payload in an IKE request, or
             blank otherwise.  If this value matches the value in the
             identity payload, the credential for the peer can be found
```

```
            using the ipsaPeerIdCredentialName as an index into the
            credential table."
        ::= { ipsaPeerIdentityEntry 4 }

    ipsaPeerIdAddressType OBJECT-TYPE
        SYNTAX      InetAddressType
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "The property ipsaPeerIdAddressType specifies the format of
            the ipsaPeerIdAddress property value."
        ::= { ipsaPeerIdentityEntry 5 }

    ipsaPeerIdAddress OBJECT-TYPE
        SYNTAX      InetAddress
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "The property PeerAddress specifies the IP address of the
            peer.  The format is specified by the
            ipsaPeerIdAddressType."
        ::= { ipsaPeerIdentityEntry 6 }

    ipsaPeerIdCredentialName OBJECT-TYPE
        SYNTAX      SnmpAdminString (SIZE(0..32))
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This value is used as an index into the ipsaCredentialTable
            to look up the actual credential value and other credential
            information.  For peer IDs that have no associated
            credential information, this value is left blank."
        ::= { ipsaPeerIdentityEntry 7 }

    ipsaPeerIdLastChanged OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of sysUpTime when this row was last modified or
            created either through SNMP SETs or by some other external
            means.

            If this row has not been modified since the last
            re-initialization of the network management subsystem, this
            object SHOULD have a zero value."
        ::= { ipsaPeerIdentityEntry 8 }
```

```
   ipsaPeerIdStorageType OBJECT-TYPE
       SYNTAX      StorageType
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "The storage type for this row.  Rows in this table which
            were created through an external process MAY have a storage
            type of readOnly or permanent.

            For a storage type of permanent, none of the columns have
            to be writable."
       DEFVAL { nonVolatile }
       ::= { ipsaPeerIdentityEntry 9 }

   ipsaPeerIdRowStatus OBJECT-TYPE
       SYNTAX      RowStatus
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
           "This object indicates the conceptual status of this row.

            The value of this object has no effect on whether other
            objects in this conceptual row can be modified.

            If active, this object MUST remain active if it is
            referenced by an active row in another table.  An attempt
            to set it to anything other than active while it is
            referenced by an active row in another table MUST result in
            an inconsistentValue error."
       ::= { ipsaPeerIdentityEntry 10 }

   --
   --
   -- Notification objects information
   --
   --

   ipsaNotificationVariables OBJECT IDENTIFIER ::=
      { ipsaNotificationObjects 1 }

   ipsaNotifications OBJECT IDENTIFIER ::=
      { ipsaNotificationObjects 0 }


   --
   --
   -- Conformance information
   --
```

```
   --

   ipsaCompliances OBJECT IDENTIFIER
       ::= { ipsaConformanceObjects 1 }
   ipsaGroups OBJECT IDENTIFIER
       ::= { ipsaConformanceObjects 2 }

   --
   -- Compliance statements
   --
   --

   ipsaIPsecCompliance MODULE-COMPLIANCE
       STATUS      current
       DESCRIPTION
           "The compliance statement for SNMP entities that include an
            IPsec MIB implementation and supports IPsec actions.

            There are a number of INDEX objects that cannot be
            represented in the form of OBJECT clauses in SMIv2, but for
            which we have the following compliance requirements,
            expressed in OBJECT clause form in this description clause:

            -- OBJECT ipsaPeerIdAddressType
            -- SYNTAX InetAddressType { ipv4(1), ipv6(2) }
            -- DESCRIPTION
            -- Only support for global IPv4 and IPv6 address
            -- types is required.
            --
            -- OBJECT ipsaPeerIdAddress
            -- SYNTAX InetAddress (SIZE(4|16))
            -- DESCRIPTION
            -- Only support for global IPv4 and IPv6 address
            -- types is required.
            --"
       MODULE -- This Module
           MANDATORY-GROUPS { ipsaPreconfiguredGroup, ipsaSharedGroup }

           OBJECT      ipsaSaPreActLastChanged
           MIN-ACCESS  not-accessible
           DESCRIPTION
                "This object is optional so as not to impose an undue
                 burden on resource-constrained devices."

           OBJECT      ipsaAhTranLastChanged
           MIN-ACCESS  not-accessible
           DESCRIPTION
                "This object is optional so as not to impose an undue
```

```
                burden on resource-constrained devices."

            OBJECT      ipsaEspTranLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
                 "This object is optional so as not to impose an undue
                  burden on resource-constrained devices."

            OBJECT      ipsaIpcompTranLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
                 "This object is optional so as not to impose an undue
                  burden on resource-constrained devices."

            OBJECT      ipsaPeerIdLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
                 "This object is optional so as not to impose an undue
                  burden on resource-constrained devices."

            OBJECT      ipsaCredLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
                 "This object is optional so as not to impose an undue
                  burden on resource-constrained devices."

            OBJECT      ipsaCredSegLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
                 "This object is optional so as not to impose an undue
                  burden on resource-constrained devices."


        ::= { ipsaCompliances 1 }

    --
    --
    -- Compliance Groups Definitions
    --

    ipsaPreconfiguredGroup OBJECT-GROUP
        OBJECTS {
            ipsaSaPreActActionDescription,
            ipsaSaPreActActionLifetimeSec, ipsaSaPreActActionLifetimeKB,
            ipsaSaPreActDoActionLogging, ipsaSaPreActDoPacketLogging,
            ipsaSaPreActDFHandling, ipsaSaPreActActionType,
            ipsaSaPreActAHSPI, ipsaSaPreActAHTransformName,
            ipsaSaPreActAHSharedSecretName, ipsaSaPreActESPSPI,
```

```
            ipsaSaPreActESPTransformName, ipsaSaPreActESPEncSecretName,
            ipsaSaPreActESPAuthSecretName, ipsaSaPreActIPCompSPI,
            ipsaSaPreActIPCompTransformName,
            ipsaSaPreActPeerGatewayIdName, ipsaSaPreActLastChanged,
            ipsaSaPreActStorageType, ipsaSaPreActRowStatus
        }
        STATUS current
        DESCRIPTION
            "This group is the set of objects that support preconfigured
             IPsec actions.  These objects are from The Preconfigured
             Action Table.  This group also includes objects from the
             shared tables: Peer Identity Table, Credential Table,
             Credential Management Service Table and the AH, ESP, and
             IPComp Transform Tables."
        ::= { ipsaGroups 1 }

    ipsaSharedGroup OBJECT-GROUP
        OBJECTS {
            ipsaAhTranMaxLifetimeSec, ipsaAhTranMaxLifetimeKB,
            ipsaAhTranAlgorithm, ipsaAhTranReplayProtection,
            ipsaAhTranReplayWindowSize, ipsaAhTranLastChanged,
            ipsaAhTranStorageType, ipsaAhTranRowStatus,

            ipsaEspTranMaxLifetimeSec, ipsaEspTranMaxLifetimeKB,
            ipsaEspTranCipherTransformId, ipsaEspTranCipherKeyLength,
            ipsaEspTranCipherKeyRounds, ipsaEspTranIntegrityAlgorithmId,
            ipsaEspTranReplayPrevention, ipsaEspTranReplayWindowSize,
            ipsaEspTranLastChanged, ipsaEspTranStorageType,
            ipsaEspTranRowStatus,

            ipsaIpcompTranDictionarySize, ipsaIpcompTranAlgorithm,
            ipsaIpcompTranMaxLifetimeSec, ipsaIpcompTranMaxLifetimeKB,
            ipsaIpcompTranPrivateAlgorithm, ipsaIpcompTranLastChanged,
            ipsaIpcompTranStorageType, ipsaIpcompTranRowStatus,

            ipsaCredType, ipsaCredCredential, ipsaCredMngName,
            ipsaCredSize, ipsaCredRemoteID, ipsaCredAdminStatus,
            ipsaCredLastChanged, ipsaCredStorageType, ipsaCredRowStatus,

            ipsaCredSegValue, ipsaCredSegLastChanged,
            ipsaCredSegStorageType, ipsaCredSegRowStatus,

            ipsaPeerIdValue, ipsaPeerIdType, ipsaPeerIdAddress,
            ipsaPeerIdAddressType, ipsaPeerIdCredentialName,
            ipsaPeerIdLastChanged, ipsaPeerIdStorageType,
            ipsaPeerIdRowStatus
        }
        STATUS current
```

```
        DESCRIPTION
            "This group includes objects from tables expected
             to be shared by other modules: Peer Identity Table,
             Credential Table, Credential Management Service Table and
             the AH, ESP, and IPComp Transform Tables."
        ::= { ipsaGroups 2 }


    END
```

7. Security Considerations

7.1. Introduction

This document defines a MIB module used to configure IPsec policy services. Since IPsec provides network security services, all of its configuration data (e.g. this entire MIB) SHOULD be as secure or more secure than any of the security services IPsec provides. There are two main threats you need to protect against when configuring IPsec devices.

1. Malicious Configuration: This MIB configures network security services. If an attacker has SET access to any part of this MIB, the network security services configured by this MIB SHOULD be considered broken. The network data sent through the associated gateway should no longer be considered as protected by IPsec (i.e., it is no longer confidential or authenticated). Therefore, only the official administrators SHOULD be allowed to configure a device. In other words, administrators' identities SHOULD be authenticated and their access rights checked before they are allowed to do device configuration. The support for SET operations to the IPSEC-IPSECACTION MIB in a non-secure environment, without proper protection, will invalidate the security of the network traffic affected by the IPSEC-IPSECACTION-MIB.

2. Disclosure of Configuration: In general, malicious parties SHOULD NOT be able to read security configuration data while the data is in network transit. An attacker reading the configuration data may be able to find misconfigurations in the MIB that enable attacks to the network or to the configured node. Since this entire MIB is used for security configuration, it is highly RECOMMENDED that only authorized administrators are allowed to view data in this MIB. In particular, malicious users SHOULD be prevented from reading SNMP packets containing this MIB's data. SNMP GET data SHOULD be encrypted when sent across the network.

Also, only authorized administrators SHOULD be allowed SNMP GET access to any of the MIB objects.

SNMP versions prior to SNMPv3 do not include adequate security. Even if the network itself is secure (e.g. by using IPsec), earlier versions of SNMP have virtually no control as to who on the secure network is allowed to access (i.e. read/change/create/delete) the objects in this MIB module.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see [RFC3410], section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to GET or SET (change/create/delete) them.

Therefore, when configuring data in the IPSEC-IPSECACTION-MIB, you SHOULD use SNMP version 3. The rest of this discussion assumes the use of SNMPv3. This is a real strength, because it allows administrators the ability to load new IPsec configuration on a device and keep the conversation private and authenticated under the protection of SNMPv3 before any IPsec protections are available. Once initial establishment of IPsec configuration on a device has been achieved, it would be possible to set up IPsec SAs to then also provide security and integrity services to the configuration conversation. This may seem redundant at first, but will be shown to have a use for added privacy protection below.

7.2. Protecting against unauthenticated access

The current SNMPv3 User Security Model provides for key based user authentication. Typically, keys are derived from passwords (but are not required to be), and the keys are then used in HMAC algorithms (currently MD5 and SHA-1 HMACs are defined) to authenticate all SNMP data. Each SNMP device keeps a (configured) list of users and keys. Under SNMPv3 user keys may be updated as often as an administrator cares to have users enter new passwords. But Perfect Forward Secrecy for user keys in SNMPv3 is not yet provided by standards track documents, although RFC2786 defines an experimental method of doing so.

7.3. Protecting against involuntary disclosure

While sending IPsec configuration data to a Policy Enforcement Point (PEP), there are a few critical parameters which MUST NOT be observed by third parties. Specifically, except for public keys, keying information MUST NOT be allowed to be observed by third parties. This include IKE Pre-Shared Keys and possibly the private key of a public/private key pair for use in a PKI. Were either of those parameters to be known to a third party, they could then impersonate the device to other IKE peers. Aside from those critical parameters, policy administrators have an interest in not divulging any of their policy configuration. Any knowledge about a device's configuration could help an unfriendly party compromise that device. SNMPv3 offers privacy security services, but at the time this document was written, the only standardized encryption algorithm supported by SNMPv3 is the DES encryption algorithm. Support for other (stronger) cryptographic algorithms is in the works and may be done as you read this (e.g. AES [RFC3826]). When configure IPsec policy using this MIB, policy administrators SHOULD use a privacy security service that is at least as strong as the desired IPsec policy. E.G., If an administrator were to use this MIB to configure an IPsec connection that utilizes a 3DES algorithms, the SNMP communication configuring the connection SHOULD be protected by an algorithm as strong or stronger than the 3DES algorithm.

7.4. Bootstrapping your configuration

Most vendors will not ship new products with a default SNMPv3 user/password pair, but it is possible. If a device does ship with a default user/password pair, policy administrators SHOULD either change the password or configure a new user, deleting the default user (or at a minimum, restrict the access of the default user). Most SNMPv3 distributions should, hopefully, require an out-of-band initialization over a trusted medium, such as a local console connection.

8. IANA Considerations

Only one IANA consideration exist for this document. The consideration is the node number allocation of the IPSEC-IPSECACTION-MIB under the IPSEC-SPD-MIB MIB's spdActions node.

9. Acknowledgments

Many other people contributed thoughts and ideas that influenced this MIB module. Some special thanks are in order for the following

people:

Lindy Foster	(Sparta, Inc.)
John Gillis	(ADC)
Jamie Jason	(Intel Corporation)
Roger Hartmuller	(Sparta, Inc.)
David Partain	(Ericsson)
Lee Rafalow	(IBM)
Jon Saperia	(JDS Consulting)
John Shriver	(Internap Network Services Corporation)
Eric Vyncke	(Cisco Systems)

10. References

10.1. Normative References

[RFCZZZZ] Baer, M., Charlet, R., Hardaker, W., Story, R., and C. Wang, "IPsec Security Policy Database Configuration MIB", January 2004.

[RFCYYYY] Baer, M., Charlet, R., Hardaker, W., Story, R., and C. Wang, "IPsec Security Policy IKE Action MIB", January 2004.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2401] Kent, S. and R. Atkinson, "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.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

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

[RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

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

[RFC3289] Baker, F., Chan, K., and A. Smith, "Management Information Base for the Differentiated Services Architecture", RFC 3289, May 2002.

[RFC3585] Jason, J., Rafalow, L., and E. Vyncke, "IPsec Configuration Policy Information Model", RFC 3585, August 2003.

[RFC4001] Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", RFC 4001, February 2005.

10.2. Informative References

[IPPMWP] Lortz, V. and L. Rafalow, "IPsec Policy Model White Paper", More Info http://www.dmtf.org/specs/cim.html, November 2000.

[RFC3826] Blumenthal, U., Maino, F., and K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model", RFC 3826, June 2004.

Authors' Addresses

Michael Baer
Sparta, Inc.
P.O. Box 72682
Davis, CA 95617
US

Email: baerm@tislabs.com

Ricky Charlet
Self

Email: rcharlet@alumni.calpoly.edu

Wes Hardaker
Sparta, Inc.
P.O. Box 382
Davis, CA 95617
US

Phone: +1 530 792 1913
Email: hardaker@tislabs.com

Robert Story
Revelstone Software
PO Box 1812
Tucker, GA 30085
US

Email: rstory@sparta.com

Cliff Wang
ARO/North Carolina State University
4300 S. Miami Blvd
RTP, NC 27709
US

Email: cliffwangmail@yahoo.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).