

# YANG Data Model for Internet Protocol Security (IPSec)

draft-tran-ipecme-yang-ipsec-00

K. Tran, Ericsson

# Goals

- YANG data model for configuring and monitoring IPSec
  - IPSec
  - IKE
  - IKEv2

# Relationship with Other Modules

- An independent tree

# Architecture

## Configuration and State Data

```
+---rw ipsec
| +---rw access-list*
|     [name sequence-number]
|   + ...
|   +---rw security-association
|     | +---rw ipsec-sa* [name]
|     | + ...
|     +---rw proposal
|       | +---rw ipsec-proposal* [name]
|       | + ...
|       +---rw policy
|         +---rw ipsec-policy* [name]
|         + ...
+---rw ike
| +---rw proposal* [name]
| | + ...
| +---rw policy* [name]
| + ...
+---rw ikev2
| +---rw proposal* [name]
| | + ...
| +---rw policy* [name]
| + ...
+---ro ipsec-state
| +---ro ...
+---ro ike-state
| +---ro ...
+---ro ikev2-state
  +---ro ...
```

## RPC

```
rpcs:
+---x clear-ipsec-group
| +---ro input
|   +---ro alarm-hold-down?
|                                     uint8
|   +---ro ipsec-policy-name?
|                                     leafref
+---x clear-ike-group
| +---ro input
|   +---ro proposal?                 leafref
+---x clear-ikev2-group
  +---ro input
    +---ro proposal?                 leafref
```

# Configuration for IPSec

```

+--rw ipsec
|  +--rw access-list*
|  |      [name sequence-number]
|  |  + ...
|  |  +--rw security-association
|  |  |  +--rw ipsec-sa* [name]
|  |  |  + ...
|  |  +--rw proposal
|  |  |  +--rw ipsec-proposal* [name]
|  |  |  + ...
|  |  +--rw policy
|  |  |  +--rw ipsec-policy* [name]
|  |  |  + ...

```

```

+--rw name
+--rw sequence-number
+--rw (protocol)?
|  +--:(number)
|  |  +--rw number?
|  |  |  +--rw (argument)?
|  |  |  |  +--:(source-ip-address)
|  |  |  |  |  +--rw source-ipv4-address
|  |  |  |  +--:(any)
|  |  |  |  |  +--rw source-any?
|  |  |  +--:(source-ipv4-address)
|  |  |  |  +--rw source-ipv4-address?
|  |  |  +--:(any)
|  |  |  |  +--rw any?
|  |  |  +--:(tcp)
|  |  |  |  +--rw tcp?
|  |  |  +--:(udp)
|  |  |  |  +--rw udp?
|  |  |  +--:(dest-address)?
|  |  +-- ...

```

```

+--rw name
+--rw anti-replay-window?
+--rw ip-comp?
+--rw in
|  +--rw ah
|  |  +--rw spi?
|  |  |  +--rw (authentication-
|  |  |  |  algorithm)?
|  |  |  |  +--:(hmac-aes-xcbc)
|  |  |  |  |  +--rw hmac-aes-xcbc
|  |  |  |  |  |  +--rw key-str?
|  |  |  |  +--:(hmac-md5-96)
|  |  |  |  |  +--rw hmac-md5-96
|  |  |  |  |  |  +--rw key-str?
|  |  |  |  +--:(hmac-sha1-96)
|  |  |  |  |  +--rw hmac-sha1-96
|  |  |  |  |  |  +--rw key-str?
|  |  |  |  +--:(key-string)
|  |  |  |  |  +--rw key-string
|  |  |  |  |  |  +--rw key-str?
|  |  +--rw esp
|  |  |  + ...
+--rw out
+ ...

```

```

+--rw name                string
+--rw ah?                 ike-integrity-algorithm-t
+--rw esp
|  +--rw authentication?  ike-integrity-algorithm-t
|  +--rw encryption?     ike-encryption-algorithm-t
+--rw ip-comp?           empty
+--rw lifetime
|  +--rw kbytes?          uint32
|  +--rw seconds?        yub32

```

```

+--rw name                string
+--rw anti-replay-window? uint32
+--rw perfect-forward-secrecy
|  +--rw dh-group?       diffie-hellman-group-t
+--rw seq* [seq-id]
|  +--rw seq-id          uint32
+--rw proposal?

```

# Configuration for IKE

```
+--rw ipsec
| ...
+--rw ike
| +--rw proposal* [name]
| | ...
| +--rw keepalive? empty
| +--rw policy* [name]
| | ...
```

```
+--rw name string
+--rw dh-group diffie-hellman-group-t
+--rw encryption
| +--rw algorithm? ike-encryption-algorithm-t
+--rw lifetime uint32
+--rw authentication
| +--rw algorithm? ike-integrity-algorithm-t
| +--rw prehard-key? empty
| +--rw rsa-signature? empty
```

```
+--rw name string
+--rw mode
| +--rw aggressive? empty
| +--rw main? empty
+--rw connection-type connection-type-t
+--rw pre-shared-key union
+--rw validate-certificate-identity? empty
+--rw seq* [seq-id]
| +--rw seq-id uint32
| +--rw proposal?
+--rw identity
+--rw local
| +--rw (identity)?
| | +--rw:(ipv4-address)
| | | +--rw ipv4-address? inet:ipv4-address
| | +--rw:(ipv6-address)
| | | +--rw ipv6-address? inet:ipv6-address
| | +--rw:(fqdn-string)
| | | +--rw fqdn-string? string
| | +--rw:(rfc822-address-string)
| | | +--rw rfc822-address-string? string
| | +--rw:(dnX509)
| | | +--rw dnX509?
+--rw remote
| ...
```

# Configuration for IKEv2

```
+--rw ipsec
| ...
+--rw ike
| ...
+--rw ikev2
| +--rw proposal* [name]
| | ...
| +--rw policy* [name]
| | ...
```

```
+--rw name string
+--rw dh-group diffie-hellman-group-t
+--rw encryption
| +--rw algorithm? ike-encryption-algorithm-t
+--rw pseudo-random-function pseudo-random-function-t
+--rw authentication
| +--rw algorithm? ike-integrity-algorithm-t
```

```
+--rw name string
+--rw authentication
| +--rw preshared-key? empty
| +--rw rsa-signature? empty
+--rw lifetime uint32
+--rw address-collision
| +--rw aaa? empty
+--rw connection-type connection-type-t
+--rw pre-shared-key? union
+--rw validate-certificate-identity? empty
+--rw seq* [seq-id]
| +--rw seq-id uint32
| +--rw proposal?
+--rw identity
+--rw local
| +--rw (identity)?
| +--rw:(ipv4-address)
| | +--rw ipv4-address? inet:ipv4-address
| +--rw:(ipv6-address)
| | +--rw ipv6-address? inet:ipv6-address
| +--rw:(fqdn-string)
| | +--rw fqdn-string? inet:domain-name
| +--rw:(rfc822-address-string)
| | +--rw rfc822-address-string? string
| +--rw:(dnX509)
| | +--rw dnX509? string
+--rw remote
| ...
```

# Operational States for IPsec

```
+---rw
| ...
+---ro ipsec-state
  +---ro policy*
    | +---ro name?                string
    | +---ro anti-replay-window?  uint32
    | +---ro perfect-forward-secrecy?  diffie-hellman-group-t
    | +---ro seq*
    |   +---ro seq-id?            uint32
    |   +---ro proposal-name?     string
  +---ro proposal*
    | +---ro name?                string
    | +---ro ah?                  ike-integrity-algorithm-t
    | +---ro esp
    | | +---ro authentication?    ike-integrity-algorithm-t
    | | +---ro encryption?       ike-encryption-algorithm-t
    | +---ro ip-comp?            empty
    | +---ro lifetime
    |   +---ro kbytes?           uint32
    |   +---ro seconds?         uint32
  +---ro hold-down?            uint32
+---ro sa*
  +---ro name?                string
  +---ro anti-replay-window?  uint16
  +---ro ip-comp?            empty
  +---ro spi?                uint32
  +---ro description?        string
  +---ro authentication-algorithm?  ike-integrity-algorithm-t
  +---ro encryption-algorithm?  ike-encryption-algorithm-t
```



# Operational States for IKE

```
+-rw
| ...
+-ro ipsec-state
| ...
+-ro ike-state
| +-ro proposal*
| | +-ro name?          string
| | +-ro lifetime?     uint32
| | +-ro encryption?   ike-encryption-algorithm-t
| | +-ro dh-group?     diffie-hellman-group-t
| | +-ro authentication? ike-integrity-algorithm-t
| +-ro policy*
|   +-ro name?          string
|   +-ro description?   string
|   +-ro mode?          enumeration
|   +-ro connection-type? connection-type-t
|   +-ro local-identity? inet:ipv4-address-no-zone
|   +-ro remote-identity? inet:ipv4-address-no-zone
|   +-ro pre-shared-key? string
|   +-ro seq?           uint32
|   +-ro proposal?     string
```

# Operational States for IKEv2

```
+--rw
| ...
+--ro ipsec-state
| ...
+--ro ike-state
| ...
+--ro ikev2-state
  | +--ro proposal*
  | | +--ro name?                string
  | | +--ro pseudo-random-function? pseudo-random-function-t
  | | +--ro authentication?      ike-integrity-algorithm-t
  | | +--ro encryption?          ike-encryption-algorithm-t
  | | +--ro dh-group              diffie-hellman-group-t
  | +--ro policy*
  |   +--ro name?                  string
  |   +--ro description?           string
  |   +--ro mode?                  enumeration
  |   +--ro connection-type?      connection-type-t
  |   +--ro local-identity?        inet:ipv4-address-no-zone
  |   +--ro remote-identity?       inet:ipv4-address-no-zone
  |   +--ro pre-shared-key?        string
  |   +--ro seq?                   uint32
  |   +--ro proposal?              string
```

# RPC Operations

rpcs:

```
+---x clear-ipsec-group
|  +--ro input
|    +--ro alarm-hold-down?    uint8
|    +--ro ipsec-policy-name?  leafref
+---x clear-ike-group
|  +--ro input
|    +--ro proposal?           leafref
+---x clear-ikev2-group
|  +--ro input
|    +--ro proposal?           leafref
```

# Comparison

## draft-tran-ipsecme-yang-ipsec

```
+--rw ipsec
| +--rw access-list* [name sequence-number]
| | +--rw name string
| | +--rw description? String
| | +--rw sequence-number uint32
| | +--rw (protocol)?
| | ...
| +--rw alarms
| | +--rw hold-down? uint8
| +--rw qos
| | +--rw policy* [name]
| | ...
| +--rw redundancy
| | ...
| +--rw security-association
| | +--rw ipsec-sa* [name]
| | ...
| +--rw proposal
| | +--rw ipsec-proposal* [name]
| | ...
| +--rw policy
| | +--rw ipsec-policy* [name]
| | ...
+--rw ike
| +--rw proposal* [name]
| | ...
| +--rw keepalive? empty
| +--rw policy* [name]
| | ...
+--rw ikev2
| +--rw proposal* [name]
| | ...
| +--rw policy* [name]
| | ...
+--ro ipsec-state
| +--ro proposal*
| | ...
| +--ro policy*
| | ...
| +--ro sa*
+--ro ike-state
| +--ro proposal*
| | ...
| +--ro policy*
| | ...
+--ro ikev2-state
+--ro proposal*
| ...
+--ro policy*
+ ...
```

## draft-wang-ipsecme-ike-yang

```
+--rw ike-global-configuration
| ...
+--rw ipsec-proposal
| ...
+--rw ike-proposal
| ...
+--rw ike-peer
| ...
+--rw ipsec-policy
| +--rw policy-entries*
| | [policy-name sequence-number]
| | ...
| +--rw policy-template-entries*
| | [policy-name sequence-number]
| | ...
+--rw ipsec-interface-map
| ...
+--ro ike-sa
| ...
+--ro ipsec-sa
| ...
```

# Next Steps

- Solicit comments
- Plan to coordinate
  - draft-tran-ipecme-yang-ipsec
  - draft-wang-ipsec-ipsec-yang
  - draft-wang-ipsec-ike-yang
- Tangential topics
  - draft-chen-rtgwg-key-table-yang
  - draft-acee-rtg-key-chain-yang