IETF 93 Prague, CZ
Key Chain Yang Data Model

Acee Lindem, Cisco
Yingzhen Qu, Cisco
Derek Yeung, Cisco
Helen Chen, Ericsson
Jeffery Zhang, Juniper
Yi Yang, Cisco

Requirements

- Provide model definition for industry defacto standard key-chain
- Base model for protocol authentication import for (OSPF, ISIS, and others to follow)
- Support graceful key/algorithm rollover.
- Provide containers for key-chain entries and authentication protocols.

Model Structure

- Global List of key-chains
- Each key-chain has list of keys (reusable container)
  - Send/Accept Lifetime or Send and Accept Lifetime
    - Lifetime (reusable container) supports multiple specification options
  - Algorithm (reusable container)
  - Key

Operational State

- Along with the configuration state
- Key string is omitted
- Includes an indication of whether a key chain entry is valid for sending or acceptance.

Key-Chain Data Model

```
+--rw key-chains
        +--rw key-chain-list* [name]
           +--rw name                      string
           +--ro name-state?                 String
        +--rw key-chain-entry* [key-id]
             +--rw key-id                    uint64
             +--ro key-id-state?               uint64
             +--rw key-string
             |  ..
             +--rw lifetime
             |  +--rw (lifetime)?
             |        ..
             +--ro lifetime-state
             |  +--ro send-lifetime
             | |  ..
             |  +--ro send-valid?         boolean
             |  +--ro accept-lifetime
             |  |         ..
             |  +--ro accept-valid?       boolean
             +--rw crypto-algorithm
             |  +--rw (algorithm)?
             |     ..
             +--ro crypto-algorithm-state
                +--ro (algorithm)?
                  …
```

Summary

- Reusable authentication/encryption policy
- Being used in ISIS and OSPF data models
- Can be extended through augmentation

WG adoption?!