IETF 96 Berlin, Germany
Key Chain Yang Data Model

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

Changes Since IETF 95

- Added “replay-protection-only” algorithm for BFD

- Changed module name from ietf-routing-key-chain back to ietf-key-chain

New Crypto Algorithm

```
feature replay-protection-only {
    description
        "Provide replay-protection without any
         authentication as required by protocols
         such as Bidirectional Forwarding Detection
         (BFD).";
  }
```


```
+--ro crypto-algorithm-state
     +--ro (algorithm)?
        +--:(hmac-sha-1-12) {crypto-hmac-sha-1-12}?
        |  +--ro hmac-sha1-12?          empty
        +--:(aes-cmac-prf-128) {aes-cmac-prf-128}?
        |  +--ro aes-cmac-prf-128?      empty
        +--:(md5)
        |  +--ro md5?                   empty
        +--:(sha-1)
        |  +--ro sha-1?                 empty
        +--:(hmac-sha-1)
        |  +--ro hmac-sha-1?            empty
        +--:(hmac-sha-256)
        |  +--ro hmac-sha-256?          empty
        +--:(hmac-sha-384)
        |  +--ro hmac-sha-384?          empty
        +--:(hmac-sha-512)
        |  +--ro hmac-sha-512?          empty
        +--:(clear-text) {clear-text}?
        |  +--ro clear-text?            empty
        +--:(replay-protection-only) {replay-protection-only}?
           +--ro replay-protection-only?   empty
```

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

Current Status

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

Next Steps

- Possible Operational State updates

- Functionality complete, ready for WGLC