

# IETF 94 Yokohama, Japan

## 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

# Key Encryption

- AES Key Wrap Encryption

+--rw aes-key-wrap {aes-key-wrap}?

+--rw enable? boolean

+--ro aes-key-wrap-state {aes-key-wrap}?

+--ro enable? boolean

# New Crypto Algorithm

- feature aes-cmac-prf-128 {  
    description  
        "Support for AES Cipher based  
Message  
        Authentication Code Pseudo  
Random  
        Function."  
    }

module: ietf-key-chain

+--rw key-chains

+--rw key-chain-list\* [name]

| +--rw name string

| +--ro name-state? string

| +--rw accept-tolerance {accept-tolerance}?

| | +--rw duration? uint32

| +--ro accept-tolerance-state

| | +--ro duration? uint32

| +--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

| +--rw **crypto-algorithm**

+--rw **AES-KW {AES-KW}?**

| +--rw **enable? boolean**

+--ro **AES-KW-state {AES-KW}?**

+--ro **enable? boolean**

# Summary

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