YANG Data Model for RFC 7210 Key Table

draft-chen-rtgwg-key-table-yang-00

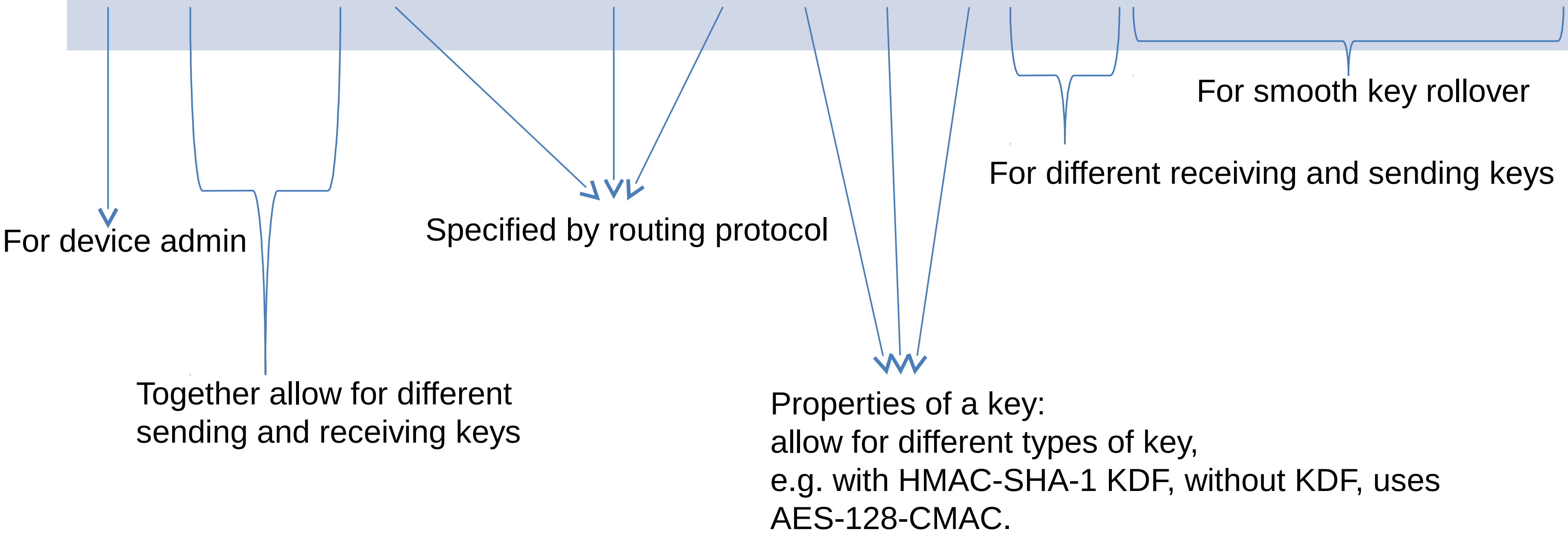
Goals

- YANG data model for configuring cryptographic keys for routing protocols
  - Based on key table defined in RFC 7210
    - Conceptual key database
    - Accommodates different key management implementations
    - Accommodates different routing protocols
    - Accommodates different security protocols
- Inter-operable key management solution that uses NETCONF and key-table YANG model

RFC 7210 Key Table

- A database of keys
- Heterogeneous deployments

Admin Key Name	Local Key Name	Peer Key Name	Peers	Interfaces	Protocol	Protocol Specific Info	KDF	AlgID	Key	Direction	Send Lifetime Start	Send Lifetime End	Accept Lifetime Start	Accept Lifetime End



For smooth key rollover

For different receiving and sending keys

For device admin

Specified by routing protocol

Together allow for different sending and receiving keys

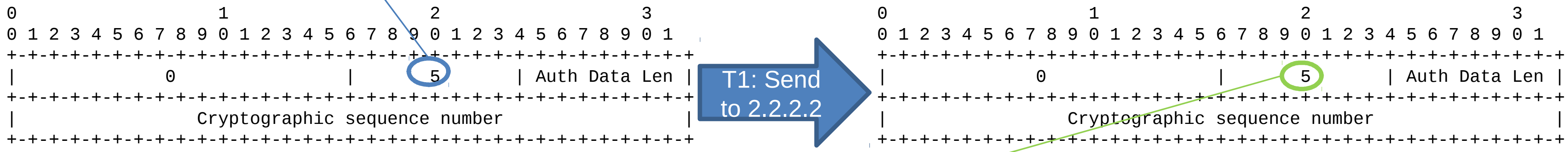
Properties of a key:
allow for different types of key,
e.g. with HMAC-SHA-1 KDF, without KDF, uses AES-128-CMAC.

OSPF Authentication (RFC 2328 Appendix D.3)

Also applies to RIPv2 and IS-IS

Router ID 1.1.1.1

Admin Key Name	Local Key Name	Peer Key Name	Peers	Interfaces	Protocol	Protocol Specific Info	KDF	AlgID	Key	Direction	Send Lifetime Start	Send Lifetime End	Accept Lifetime Start	Accept Lifetime End
k1	5	5	2.2.2.2	all	ospf	NA	none	hmac …	0x0..	both	T1	T2	T1 + 1	T2- 1
k2	7	7	2.2.2.2	all	ospf	NA	none	hmac …	0x1..	both	T5	T6	T5 + 1	T6 - 1



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              0                |       5       | Auth Data Len |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Cryptographic sequence number                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

T1: Send to 2.2.2.2

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              0                |       5       | Auth Data Len |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Cryptographic sequence number                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Router ID 2.2.2.2

Admin Key Name	Local Key Name	Peer Key Name	Peers	Interfaces	Protocol	Protocol Specific Info	KDF	AlgID	Key	Direction	Send Lifetime Start	Send Lifetime End	Accept Lifetime Start	Accept Lifetime End
L1	5	5	1.1.1.1	all	ospf	NA	none	hmac …	0x0..	both	T1	T2	T1 + 1	T2 - 1
L2	7	7	1.1.1.1	all	ospf	NA	none	hmac	0x1..	both	T5	T6	T5 + 1	T6 - 1

RSVP Authentication (RFC 2747)

Router ID 1.1.1.1

Admin Key Name	Local Key Name	Peer Key Name	Peers	Interfaces	Protocol	Protocol Specific Info	KDF	AlgID	Key	Direction	Send Lifetime Start	Send Lifetime End	Accept Lifetime Start	Accept Lifetime End
A1	15		2.2.2.2	all	rsvp	NA	none	aes …	0x0..	in	T1	T2	T1 + 1	T2- 1
A2	17		2.2.2.2	all	rsvp	NA	none	aes …	0x1..	in	T5	T6	T5 + 1	T6 - 1
B1		19	2.2.2.2	all	rsvp	NA	none	aes …	0x2..	out	T1	T2	T1 + 1	T2 - 1
B2		21	2.2.2.2	all	rsvp	NA	none	aes …	0x3..	out	T5	T6	T5 + 1	T6 - 1

```
+-------------+-------------+-------------+-------------+
|    Flags    | 0 (Reserved)|                           |
+-------------+-------------+                           +
|                            21                         |
+-------------+-------------+-------------+-------------+
|                    Sequence Number                    |
|                                                       |
+-------------+-------------+-------------+-------------+
|                                                       |
+                                                       +
|                                                       |
+                 Keyed Message Digest                  |
|                                                       |
+                                                       +
|                                                       |
+-------------+-------------+-------------+-------------+
```

T5: Send to 2.2.2.2

```
+-------------+-------------+-------------+-------------+
|    Flags    | 0 (Reserved)|                           |
+-------------+-------------+                           +
|                            21                         |
+-------------+-------------+-------------+-------------+
|                    Sequence Number                    |
|                                                       |
+-------------+-------------+-------------+-------------+
|                                                       |
+                                                       +
|                                                       |
+                 Keyed Message Digest                  |
|                                                       |
+                                                       +
|                                                       |
+-------------+-------------+-------------+-------------+
```

Router ID 2.2.2.2

Admin Key Name	Local Key Name	Peer Key Name	Peers	Interfaces	Protocol	Protocol Specific Info	KDF	AlgID	Key	Direction	Send Lifetime Start	Send Lifetime End	Accept Lifetime Start	Accept Lifetime End
p1	19		1.1.1.1	all	rsvp	NA	none	aes …	0x2..	in	T1	T2	T1 + 1	T2 - 1
p2	21		1.1.1.1	all	rsvp	NA	none	aes …	0x3..	in	T5	T6	T5 + 1	T6 - 1

Key Table YANG Model

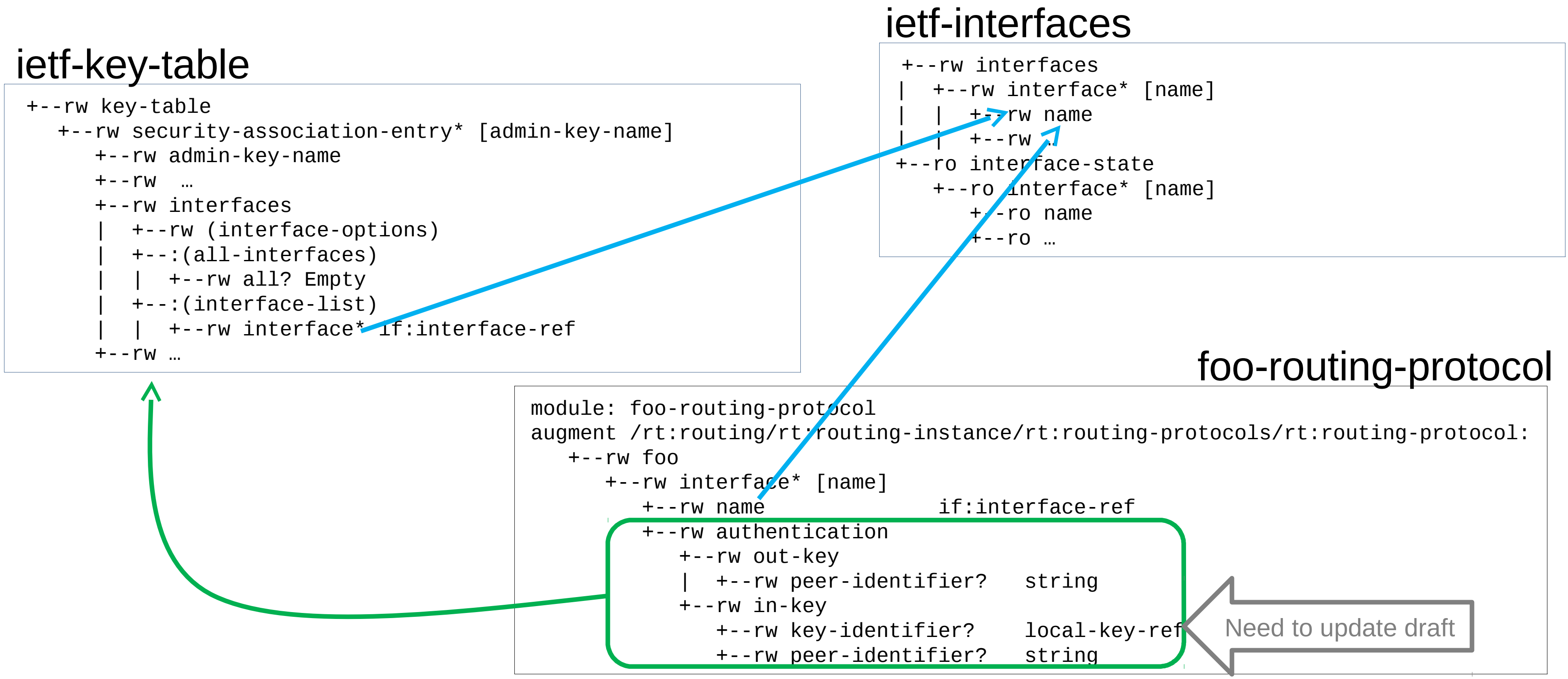
Admin Key Name	Local Key Name	Peer Key Name	Peers	Interfaces	Protocol	Protocol Specific Info	KDF	AlgID	Key	Direction	Send Lifetime Start	Send Lifetime End	Accept Lifetime Start	Accept Lifetime End

```
  +--rw security-association-entry* [admin-key-name]
     +--rw admin-key-name string
     +--rw local-key-name string
     +--rw peer-key-name string
     +--rw peers
     +--rw interfaces
     |  +--rw (interface-options)
     |  +--:(all-interfaces)
     |  |  +--rw all? Empty
     |  +--:(interface-list)
     |  |  +--rw interface* if:interface-ref
     +--rw protocol identityref
     +--rw protocol-specific-info
     +--rw kdf key-derivation-function-type
     +--rw alg-id cryptographic-algorithm-type
     +--rw key yang:hex-string
     +--rw direction enumeration
     +--rw send-lifetime-start lifetime-type
     +--rw send-lifetime-end lifetime-type
     +--rw accept-lifetime-start lifetime-type
     +--rw accept-lifetime-end lifetime-type
```

Defined as containers (i.e. YANG placeholder) and left for routing protocols to augment

Relationship with Other Modules

- An independent tree
  - Does not augment from key-chain module
- Links to ietf-interfaces
- Routing protocols link to this module



ietf-key-table

```
+--rw key-table
   +--rw security-association-entry* [admin-key-name]
      +--rw admin-key-name
      +--rw  …
      +--rw interfaces
      |  +--rw (interface-options)
      |  +--:(all-interfaces)
      |  |  +--rw all? Empty
      |  +--:(interface-list)
      |  |  +--rw interface* if:interface-ref
      +--rw …
```

ietf-interfaces

```
 +--rw interfaces
 |  +--rw interface* [name]
 |  |  +--rw name
 |  |  +--rw …
+--ro interface-state
   +--ro interface* [name]
      +--ro name
      +--ro …
```

foo-routing-protocol

```
module: foo-routing-protocol
augment /rt:routing/rt:routing-instance/rt:routing-protocols/rt:routing-protocol:
   +--rw foo
      +--rw interface* [name]
         +--rw name                if:interface-ref
         +--rw authentication
            +--rw out-key
            |  +--rw peer-identifier?   string
            +--rw in-key
               +--rw key-identifier?    local-key-ref
               +--rw peer-identifier?   string
```

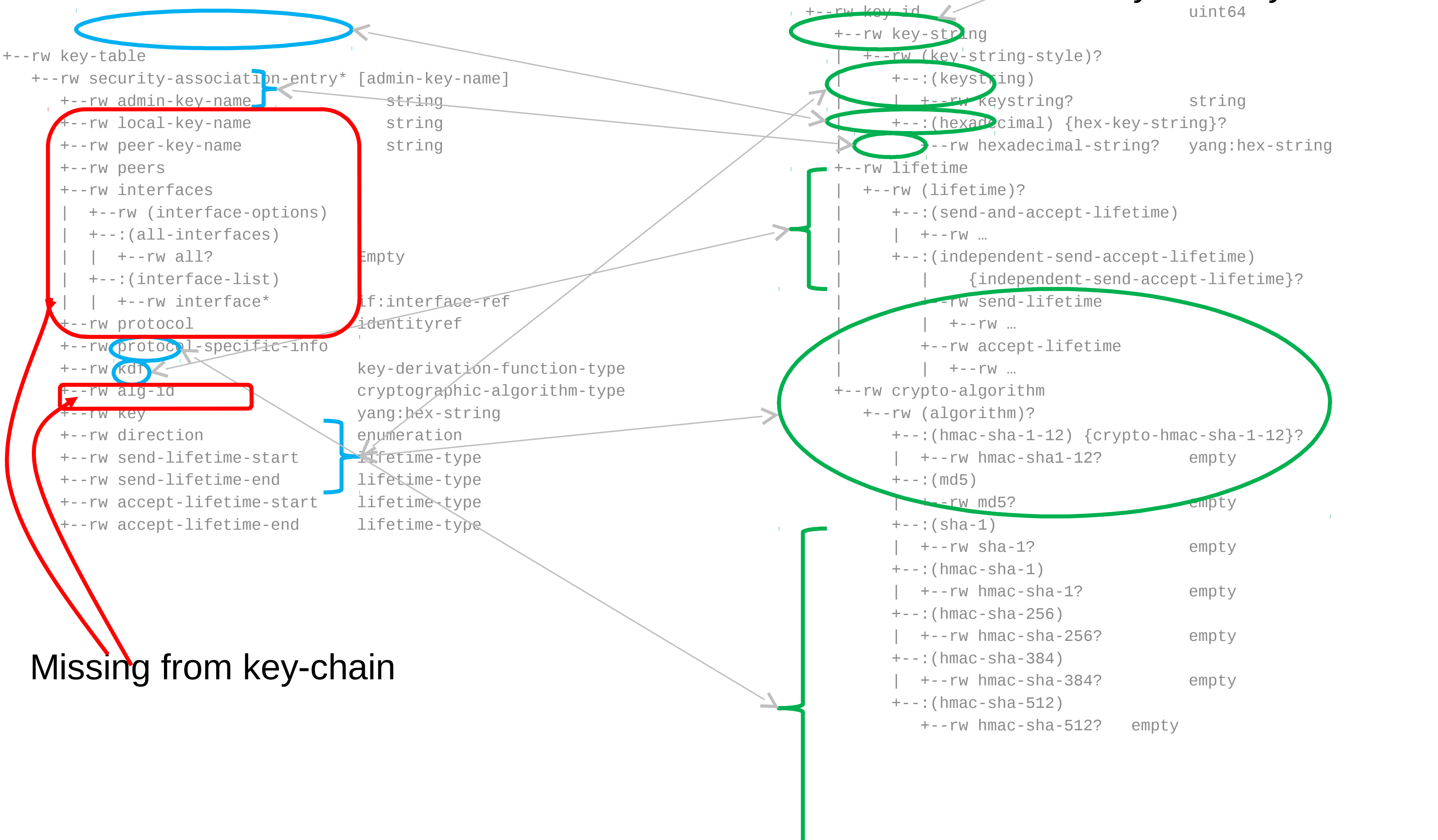
Need to update draft

Comparison: Configuration

key-table

key-chain

Extra layer in key-chain



```
+--rw key-table
   +--rw security-association-entry* [admin-key-name]
      +--rw admin-key-name                string
      +--rw local-key-name                string
      +--rw peer-key-name                 string
      +--rw peers
      +--rw interfaces
      |  +--rw (interface-options)
      |  +--:(all-interfaces)
      |  |  +--rw all?                   Empty
      |  +--:(interface-list)
      |  |  +--rw interface*             if:interface-ref
      +--rw protocol                     identityref
      +--rw protocol-specific-info
      +--rw kdf                          key-derivation-function-type
      +--rw alg-id                       cryptographic-algorithm-type
      +--rw key                          yang:hex-string
      +--rw direction                    enumeration
      +--rw send-lifetime-start          lifetime-type
      +--rw send-lifetime-end            lifetime-type
      +--rw accept-lifetime-start        lifetime-type
      +--rw accept-lifetime-end          lifetime-type
```

```
+--rw key-chains
   +--rw key-chain-list* [name]
      +--rw name                                       string
      +--rw accept-tolerance {accept-tolerance}?
      |  +--rw duration?                               uint32
      +--rw key-chain-entry* [key-id]
         +--rw key-id                                  uint64
            +--rw key-string
            |  +--rw (key-string-style)?
            |     +--:(keystring)
            |     |  +--rw keystring?                  string
            |     +--:(hexadecimal) {hex-key-string}?
            |        +--rw hexadecimal-string?   yang:hex-string
            +--rw lifetime
            |  +--rw (lifetime)?
            |     +--:(send-and-accept-lifetime)
            |     |  +--rw …
            |     +--:(independent-send-accept-lifetime)
            |        |    {independent-send-accept-lifetime}?
            |        +--rw send-lifetime
            |        |  +--rw …
            |        +--rw accept-lifetime
            |        |  +--rw …
            +--rw crypto-algorithm
               +--rw (algorithm)?
                  +--:(hmac-sha-1-12) {crypto-hmac-sha-1-12}?
                  |  +--rw hmac-sha1-12?             empty
                  +--:(md5)
                  |  +--rw md5?                      empty
                  +--:(sha-1)
                  |  +--rw sha-1?                    empty
                  +--:(hmac-sha-1)
                  |  +--rw hmac-sha-1?               empty
                  +--:(hmac-sha-256)
                  |  +--rw hmac-sha-256?             empty
                  +--:(hmac-sha-384)
                  |  +--rw hmac-sha-384?             empty
                  +--:(hmac-sha-512)
                     +--rw hmac-sha-512?    empty
```

Missing from key-chain

Mapping

KeyTable	OSPF
Admin Key Name	N/A
LocalKeyName	OSPF KeyID
PeerKeyName	N/A, SHOULD equal LocalKeyName
Peers	KeyChainName or empty
Interfaces	For nonempty Peers, MUST equal “all” For empty Peers, specifies interfaces
Protocol	OSPF (register with IANA) [used only for lookup]
ProtocolSpecificInfo	N/A, empty
KDF	MUST be “None”
AlgID	{register with IANA}
Key	Key
Direction	MUST be “both”
SendLifetimeStart	Use as start value
SendLifetimeEnd	Use as end value
AcceptLifetimeStart	For systems with a single “accept tolerance” value, N/A For systems with two “accept tolerance” values, set tolerance to difference(SendLifetimeEnd,AcceptLifetimeEnd
AcceptLifetimeEnd	For systems with a single “accept tolerance” value, set tolerance to difference(SendLifetimeEnd,AcceptLifetimeEnd For systems with two “accept tolerance” values, set tolerance to difference(SendLifetimeEnd,AcceptLifetimeEnd

Comparison Summary

key-table

- An conceptual database of security associations (keys)
- Defines all attributes included in RFC 7210
- Supports multiple security deployments
- Does not have operational state yet
  - Can be added

key-chain

- An abstraction of an implementation
- Defines a subset of attributes in RFC 7210
- Supports a particular security deployment
- Replicates some configuration data

Summary

- Introduce a key-table YANG model
  - Based on RFC 7210
  - Conceptual database of keys
  - Map to different implementations
  - Support different routing protocols
  - Support different security protocols
- Introduce an inter-operable solution to manage keys
  - NETCONF
  - key-table YANG model

Next Steps

- What does WG want to standardize?
  - Overlapping topics
    - draft-chen-rtgwg-key-table-yang
    - draft-acee-rtg-key-chain-yang
  - Tangential
    - draft-tran-ipecme-yang-ipsec
    - draft-wang-ipsec-ipsec-yang
    - draft-wang-ipsec-ike-yang

Questions/Comments

OSPF YANG Model

```
|    |     +--rw authentication
|    |        +--rw (auth-type-selection)?
|    |           +--:(auth-ipsec) {ospfv3-authentication-ipsec}?
|    |           |  +--rw sa?                  string
|    |           +--:(auth-trailer-key-chain)
|    |           |  +--rw key-chain?        key-chain:key-chain-ref
|    |           +--:(auth-trailer-key)
|    |              +--rw key?              string
|    |              +--rw crypto-algorithm
|    |              +--rw (algorithm)?
|    |                  +--:(hmac-sha-1-12) {crypto-hmac-sha-1-12}?
|    |                  |  +--rw hmac-sha1-12?   empty
|    |                  +--:(md5)
|    |                  |  +--rw md5?            empty
|    |                  +--:(sha-1)
|    |                  |  +--rw sha-1?          empty
|    |                  +--:(hmac-sha-1)
|    |                  |  +--rw hmac-sha-1?     empty
|    |                  +--:(hmac-sha-256)
|    |                  |  +--rw hmac-sha-256?   empty
|    |                  +--:(hmac-sha-384)
|    |                  |  +--rw hmac-sha-384?   empty
|    |                  +--:(hmac-sha-512)
|    |                     +--rw hmac-sha-512?   empty
```

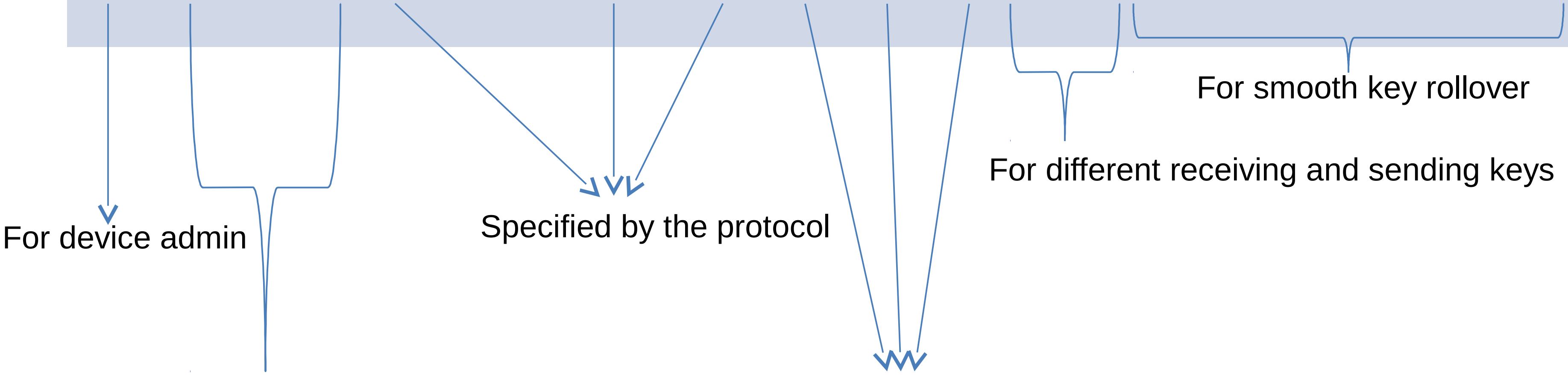
ISIS YANG model

```
|  +--rw (authentication-type)?
|  |  +--:(key-chain) {key-chain}?
|  |  |  +--rw key-chain?      key-chain:key-chain-ref
|  |  +--:(password)
|  |     +--rw key?            string
|  |     +--rw (algorithm)?
|  |        +--:(hmac-sha1-12)
|  |        |     ...
|  |        +--:(hmac-sha1-20)
|  |        |     ...
|  |        +--:(md5)
|  |        |     ...
|  |        +--:(sha-1)
|  |        |     ...
|  |        +--:(hmac-sha-1)
|  |        |     ...
|  |        +--:(hmac-sha-256)
|  |        |     ...
|  |        +--:(hmac-sha-384)
|  |        |     ...
|  |        +--:(hmac-sha-512)
|  |              ...
```

RFC 7210 Key Table

- A single database
- Heterogeneous deployment

Admin Key Name	Local Key Name	Peer Key Name	Peers	Interfaces	Protocol	Protocol Specific Info	KDF	AlgID	Key	Direction	Send Lifetime Start	Send Lifetime End	Accept Lifetime Start	Accept Lifetime End



For smooth key rollover

For different receiving and sending keys

For device admin

Specified by the protocol

Together allow for different sending and receiving keys

Properties of a key:
allow for different types of key,
e.g. with HMAC-SHA-1 KDF, without KDF, uses AES-128-CMAC.