Proposal for Refactoring the Keystore Model

draft-ietf-netconf-keystore-04
draft-kwatsen-netconf-crypto-types-00
draft-kwatsen-netconf-trust-anchors-00

NETCONF WG
IETF 101 (London)

History

- The Keystore module was primarily modeled after the “Keychain Access” Mac OS X utility, albeit without any encryption to protect the private keys
  - In fact, the module was originally called “keychain”, but was later changed to deconflict from the “key-chain” module used by routers
- The primary goal is to centralize the configuration of trust anchors
  - e.g., the same set of trust anchors for authenticating NBI clients could be used once for the configuration of a NETCONF server and again for the configuration of a RESTCONF server
- Centralizing the configuration of private keys was added primarily to eliminate needing to have the same YANG everywhere

History (Cont.)

- But then it was noted that it is uncommon for implementations to centralize private keys this way
- Thus the top-level “keys” ‘container’ was converted to a couple ‘grouping’s, and all the client-server modules were updated accordingly
- But then this raises the question, why call it a "keystore" when it no longer stores keys?

Proposal

- Since the remaining protocol-accessible configuration is solely for trust anchors, renaming the module to “trust-anchors” makes sense.

- However, the module also defines the groupings used for private keys, which has nothing to do with “trust anchors”, and thus should be moved to another module.

- Seeing how this module would define a number of crypto-related identities and typedefs, this module could be called “ietf-crypto-types”.

Similar to other “types” modules

- For example:
  - ietf-yang-type (RFC 6991)
  - ietf-inet-types (RFC 6991)
  - ietf-routing-types (RFC 8294)

- It seems that its time has come
  - Needed now as we’re beginning to define data models for configuring Security

Current contents ieft-crypto-types

- Identities for Hashing Algorithms (e.g. sha-256)
- Identities for Key Algorithms (e.g. secp256r1)
- Typedefs for ASN.1 structures (e.g. x509, cms)
- Groupings for private keys and their associated certificates
- A notification for certificate expirations

Just what’s needed to support the various client/server drafts.

Issues

- Crypto is a big area; it seems like the current ietf-crypto-types module might be just scratching the surface
  - In the interest of time, it would be good to publish just the subset needed immediately, but need to know the end-game now so as to ensure correctness.
- Should ietf-crypto-types be refactored further?
  - the two groupings for configuring private keys seem like they might be better off somewhere else
  - the notification could be pulled out or deleted
  - the ASN.1 typedefs could be factored out (e.g. ietf-asn1-types)

Options

1. Keep ietf-keystore as is
   - well, maybe rename it, but to what?

2. Switch to ietf-trust-anchors and ietf-crypto-types
   - with no more refactoring

3. Get advice from Security Area first
   - what does the “end game” look like?
   - for the parts needed now, how do they look?

4. Anything else?