NETCONF Over TLS

RFC 5539bis

http://tools.ietf.org/html/draft-ietf-netconf-rfc5539bis-01

Motivation

- Alternate transport for platforms that do not support SSH; e.g., embedded systems
- Define a standards-based mechanism for generating NETCONF usernames from X.509 certificates or pre-shared keys

Remaining Work

- Harmonize with draft-ietf-netmod-snmp-cfg
- Add overview of data model
- Add example configuration
- Possible further clarifications
- Editorial improvements
- 2nd WG last call

Ex1: map cert to user-name

```
<netconf-config xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-tls">
  <tls>
    <cert-maps>
      <cert-map>
        <key>foo</key>
        <fingerprint>                          <!-- why this container? -->
          <sha1>de:ad:be:ef</sha1>
        </fingerprint>
        <specified>admin</specified>    <!-- user-name? -->
      </cert-map>
    </cert-maps>
  </tls>
</netconf-config>
```

Ex2: get user-name from cert

```
<netconf-config xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-tls">
  <tls>
    <cert-maps>
      <cert-map>
        <key>fum</key>
        <fingerprint>
          <sha1>de:ad:be:ef</sha1>
        </fingerprint>
        <from-certificate>rfc822Name</from-certificate>
      </cert-map>
    </cert-maps>
  </tls>
</netconf-config>
```

Ex3: Map PSK to user-name

```
<netconf-config xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-tls">
  <tls>
    <psk-maps>
      <psk-map>
        <psk-identity>a8gc8]klh59</psk-identity>
        <user-name>admin</user-name>
        <valid-not-before>2013-01-01T00:00:00-00:00</valid-not-before>
        <valid-not-after>2014-01-01T00:00:00-00:00</valid-not-after>
      </psk-map>
    </psk-maps>
  </tls>
</netconf-config>
```

Harmonize with draft-ietf-netmod-snmp-cfg

The SNMP configuration document uses a simpler data model to map certs to security names:

```
+--rw cert-to-security-name [id]
   +--rw id                                  uint32
   +--rw fingerprint?                        tls-fingerprint
   +--rw map-type?                           identityref
   +--rw cert-specified-security-name?       admin-string
```

The NC over TLS solution is less extensible and does not even fit on this slide.

Clarifications

- Is the top netconf-config the proper top?
- Should authenticating with X.509 certificates be optional?
- Others?