NETCONF Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 6, 2018

K. Watsen
Juniper Networks

March 5, 2018

YANG Data Model for Global Trust Anchors
draft-kwatsen-netconf-trust-anchors-00

Abstract

This document defines a YANG data model for configuring global sets of X.509 certificates and SSH host-keys that can be referenced by other data models for trust. While the SSH host-keys are uniquely for the SSH protocol, the X.509 certificates may be used for multiple uses, including authenticating protocol peers and verifying signatures.

Editorial Note (To be removed by RFC Editor)

This draft contains many placeholder values that need to be replaced with finalized values at the time of publication. This note summarizes all of the substitutions that are needed. No other RFC Editor instructions are specified elsewhere in this document.

Artwork in this document contains shorthand references to drafts in progress. Please apply the following replacements:

- "XXXX" --> the assigned RFC value for this draft

Artwork in this document contains placeholder values for the date of publication of this draft. Please apply the following replacement:

- "2018-03-05" --> the publication date of this draft

The following Appendix section is to be removed prior to publication:

- Appendix A. Change Log

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Table of Contents

1. Introduction

This document defines a YANG data model for configuring global sets of X.509 certificates and SSH host-keys that can be referenced by other data models for trust. While the SSH host-keys are uniquely for the SSH protocol, the X.509 certificates may be used for multiple

uses, including authenticating protocol peers and verifying signatures.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Tree Diagram Notation

Tree diagrams used in this document follow the notation defined in [I-D.ietf-netmod-yang-tree-diagrams].

2. Tree Diagram

The following tree diagram provides an overview of the "ietf-trust-anchors" module.

```
module: ietf-trust-anchors
  +--rw trust-anchors
     +--rw pinned-certificates* [name]
     |  +--rw name                  string
     |  +--rw description?          string
     |  +--rw pinned-certificate* [name]
     |     +--rw name    string
     |     +--rw data    binary
     +--rw pinned-host-keys* [name]
        +--rw name               string
        +--rw description?       string
        +--rw pinned-host-key* [name]
           +--rw name    string
           +--rw data    binary
```

3. Example Usage

The following example illustrates configured data.

```
<trust-anchors xmlns="urn:ietf:params:xml:ns:yang:ietf-trust-anchors">

 <!-- Manufacturer's trust root CA certs -->
 <pinned-certificates>
   <name>manufacturers-root-ca-certs</name>
   <description>
     Certificates built into the device for authenticating
     manufacturer-signed objects, such as TLS server certificates,
```

```
        vouchers, etc..  Note, though listed here, these are not
        configurable; any attempt to do so will be denied.
      </description>
      <pinned-certificate>
        <name>Manufacturer Root CA cert 1</name>
        <data>base64encodedvalue==</data>
      </pinned-certificate>
      <pinned-certificate>
        <name>Manufacturer Root CA cert 2</name>
        <data>base64encodedvalue==</data>
      </pinned-certificate>
    </pinned-certificates>

    <!-- pinned netconf/restconf client certificates -->
    <pinned-certificates>
      <name>explicitly-trusted-client-certs</name>
      <description>
        Specific client authentication certificates for explicitly
        trusted clients.  These are needed for client certificates
        that are not signed by a pinned CA.
      </description>
      <pinned-certificate>
        <name>George Jetson</name>
        <data>base64encodedvalue==</data>
      </pinned-certificate>
    </pinned-certificates>

    <!-- pinned netconf/restconf server certificates -->
    <pinned-certificates>
      <name>explicitly-trusted-server-certs</name>
      <description>
        Specific server authentication certificates for explicitly
        trusted servers.  These are needed for server certificates
        that are not signed by a pinned CA.
      </description>
      <pinned-certificate>
        <name>Fred Flintstone</name>
        <data>base64encodedvalue==</data>
      </pinned-certificate>
    </pinned-certificates>

    <!-- trust anchors (CA certs) for authenticating clients -->
    <pinned-certificates>
      <name>deployment-specific-ca-certs</name>
      <description>
        Trust anchors (i.e. CA certs) that are used to authenticate
        client connections.  Clients are authenticated if their
        certificate has a chain of trust to one of these configured
```

```
        CA certificates.
      </description>
      <pinned-certificate>
        <name>ca.example.com</name>
        <data>base64encodedvalue==</data>
      </pinned-certificate>
    </pinned-certificates>

    <!-- trust anchors for random HTTPS servers on Internet -->
    <pinned-certificates>
      <name>common-ca-certs</name>
      <description>
        Trusted certificates to authenticate common HTTPS servers.
        These certificates are similar to those that might be
        shipped with a web browser.
      </description>
      <pinned-certificate>
        <name>ex-certificate-authority</name>
        <data>base64encodedvalue==</data>
      </pinned-certificate>
    </pinned-certificates>

    <!-- pinned SSH host keys -->
    <pinned-host-keys>
      <name>explicitly-trusted-ssh-host-keys</name>
      <description>
        Trusted SSH host keys used to authenticate SSH servers.
        These host keys would be analogous to those stored in
        a known_hosts file in OpenSSH.
      </description>
      <pinned-host-key>
        <name>corp-fw1</name>
        <data>base64encodedvalue==</data>
      </pinned-host-key>
    </pinned-host-keys>

  </trust-anchors>
```

4. YANG Module

This YANG module imports modules defined in [RFC6536]. This module uses data types defined in [RFC2315], [RFC4253], [RFC5280], and [ITU.X690.1994].

```
<CODE BEGINS> file "ietf-trust-anchors@2018-03-05.yang"
module ietf-trust-anchors {
  yang-version 1.1;
```

```
     namespace "urn:ietf:params:xml:ns:yang:ietf-trust-anchors";
     prefix "ta";

     import ietf-netconf-acm {
       prefix nacm;
       reference
         "RFC 6536: Network Configuration Protocol (NETCONF) Access
          Control Model";
     }

     organization
      "IETF NETCONF (Network Configuration) Working Group";

     contact
      "WG Web:   <http://tools.ietf.org/wg/netconf/>
       WG List:  <mailto:netconf@ietf.org>

       Author:   Kent Watsen
                 <mailto:kwatsen@juniper.net>";


     description
      "This module defines a data model for configuring global
       trust anchors used by other data models.  The data model
       actually enables the configuration of sets of trust
       anchors.  This data model supports configuring trust
       anchors for both X.509 certificates and SSH host keys.

       This data model does not support the configuring trust
       anchors for SSH client keys, or pinning of the client
       keys themselves, as the ability to do so is already
       supported by ietf-system in RFC 7317.


       Copyright (c) 2018 IETF Trust and the persons identified
       as authors of the code. All rights reserved.

       Redistribution and use in source and binary forms, with
       or without modification, is permitted pursuant to, and
       subject to the license terms contained in, the Simplified
       BSD License set forth in Section 4.c of the IETF Trust's
       Legal Provisions Relating to IETF Documents
       (http://trustee.ietf.org/license-info).

       This version of this YANG module is part of RFC XXXX; see
       the RFC itself for full legal notices.";

     revision "2018-03-05" {
```

```
       description
        "Initial version";
       reference
        "RFC XXXX: YANG Data Model for Global Trust Anchors";
     }

     // Identities


     // typedefs

     typedef pinned-certificates {
       type leafref {
         path "/ta:trust-anchors/ta:pinned-certificates/ta:name";
       }
       description
         "This typedef enables importing modules to easily define a
          reference to pinned-certificates.  Use of this type also
          impacts the YANG tree diagram output.";
     }

     typedef pinned-host-keys {
       type leafref {
         path "/ta:trust-anchors/ta:pinned-host-keys/ta:name";
       }
       description
         "This typedef enables importing modules to easily define a
          reference to pinned-host-keys.  Use of this type also
          impacts the YANG tree diagram output.";
       reference
         "I-D.ietf-netmod-yang-tree-diagrams: YANG Tree Diagrams";
     }


     // protocol accessible nodes

     container trust-anchors {
       nacm:default-deny-write;
       description
         "Contains sets of X.509 certificates and SSH host keys.";

       list pinned-certificates {
         key name;
         description
           "A list of pinned certificates.  These certificates can be
            used by a server to authenticate clients, or by a client to
            authenticate servers.   Each list of pinned certificates
            SHOULD be specific to a purpose, as the list as a whole
```

```
           may be referenced by other modules.  For instance, a
           NETCONF server's configuration might use a specific list
           of pinned certificates for when authenticating NETCONF
           client connections.";
        leaf name {
          type string;
          description
            "An arbitrary name for this list of pinned certificates.";
        }
        leaf description {
          type string;
          description
            "An arbitrary description for this list of pinned
             certificates.";
        }
        list pinned-certificate {
          key name;
          description
            "A pinned certificate.";
          leaf name {
            type string;
            description
              "An arbitrary name for this pinned certificate. The
               name must be unique across all lists of pinned
               certificates (not just this list) so that leafrefs
               from another module can resolve to unique values.";
          }
          leaf data {
            type binary;
            mandatory true;
            description
              "An X.509 v3 certificate structure as specified by RFC
               5280, Section 4 encoded using the ASN.1 distinguished
               encoding rules (DER), as specified in ITU-T X.690.";
            reference
              "RFC 5280:
                 Internet X.509 Public Key Infrastructure Certificate
                 and Certificate Revocation List (CRL) Profile.
               ITU-T X.690:
                  Information technology - ASN.1 encoding rules:
                  Specification of Basic Encoding Rules (BER),
                  Canonical Encoding Rules (CER) and Distinguished
                  Encoding Rules (DER).";
          }
        }
      }

      list pinned-host-keys {
```

```
        key name;
        description
          "A list of pinned host keys.  These pinned host-keys can
           be used by clients to authenticate SSH servers.  Each
           list of pinned host keys SHOULD be specific to a purpose,
           so the list as a whole may be referenced by other modules.
           For instance, a NETCONF client's configuration might
           point to a specific list of pinned host keys for when
           authenticating specific SSH servers.";
        leaf name {
          type string;
          description
            "An arbitrary name for this list of pinned SSH host keys.";
        }
        leaf description {
          type string;
          description
            "An arbitrary description for this list of pinned SSH host
             keys.";
        }
        list pinned-host-key {
          key name;
          description
            "A pinned host key.";
          leaf name {
            type string;
            description
              "An arbitrary name for this pinned host-key. Must be
               unique across all lists of pinned host-keys (not just
               this list) so that a leafref to it from another module
               can resolve to unique values.";
          }
          leaf data {
            type binary;
            mandatory true;
            description
              "The binary public key data for this SSH key, as
               specified by RFC 4253, Section 6.6, i.e.:

                  string    certificate or public key format
                            identifier
                  byte[n]   key/certificate data.";
            reference
              "RFC 4253: The Secure Shell (SSH) Transport Layer
                         Protocol";
          }
        }
      }
```

```
    }

  }
<CODE ENDS>
```

5. Security Considerations

TBD

6. IANA Considerations

6.1. The IETF XML Registry

This document registers one URI in the IETF XML registry [RFC3688]. Following the format in [RFC3688], the following registration is requested:

```
URI: urn:ietf:params:xml:ns:yang:ietf-trust-anchors
Registrant Contact: The NETCONF WG of the IETF.
XML: N/A, the requested URI is an XML namespace.
```

6.2. The YANG Module Names Registry

This document registers one YANG module in the YANG Module Names registry [RFC6020]. Following the format in [RFC6020], the the following registration is requested:

```
name:         ietf-trust-anchors
namespace:    urn:ietf:params:xml:ns:yang:ietf-trust-anchors
prefix:       ta
reference:    RFC XXXX
```

7. Acknowledgements

The authors would like to thank for following for lively discussions on list and in the halls (ordered by last name):

8. References

8.1. Normative References

[ITU.X690.1994]
International Telecommunications Union, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, 1994.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, DOI 10.17487/RFC2315, March 1998, <https://www.rfc-editor.org/info/rfc2315>.

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253, January 2006, <https://www.rfc-editor.org/info/rfc4253>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, DOI 10.17487/RFC6536, March 2012, <https://www.rfc-editor.org/info/rfc6536>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

8.2. Informative References

[I-D.ietf-netmod-yang-tree-diagrams] Bjorklund, M. and L. Berger, "YANG Tree Diagrams", draft-ietf-netmod-yang-tree-diagrams-06 (work in progress), February 2018.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Appendix A. Change Log

TBD

Author's Address

Kent Watsen
Juniper Networks

EMail: kwatsen@juniper.net