NETCONF Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 10, 2019

K. Watsen
Watsen Networks
G. Wu
Cisco Systems
L. Xia
Huawei

March 9, 2019

YANG Groupings for SSH Clients and SSH Servers
draft-ietf-netconf-ssh-client-server-09

Abstract

This document defines three YANG modules: the first defines groupings for a generic SSH client, the second defines groupings for a generic SSH server, and the third defines common identities and groupings used by both the client and the server. It is intended that these groupings will be used by applications using the SSH protocol.

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.

This document contains references to other drafts in progress, both in the Normative References section, as well as in body text throughout. Please update the following references to reflect their final RFC assignments:

- I-D.ietf-netconf-trust-anchors

- I-D.ietf-netconf-keystore

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

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

- "YYYY" --> the assigned RFC value for I-D.ietf-netconf-trust-anchors

- "ZZZZ" --> the assigned RFC value for I-D.ietf-netconf-keystore

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

o "2019-03-09" --> the publication date of this draft

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

o 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/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 10, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 3
2. Terminology 4
3. The SSH Client Model 4
  3.1. Tree Diagram 4
  3.2. Example Usage 5
  3.3. YANG Module 8
4. The SSH Server Model 13
  4.1. Tree Diagram 13

4.2. Example Usage 14
4.3. YANG Module 17
5. The SSH Common Model 22
5.1. Tree Diagram 24
5.2. Example Usage 25
5.3. YANG Module 25
6. Security Considerations 35
7. IANA Considerations 36
7.1. The IETF XML Registry 36
7.2. The YANG Module Names Registry 37
8. References 37
8.1. Normative References 37
8.2. Informative References 38
Appendix A. Change Log 40
A.1. 00 to 01 40
A.2. 01 to 02 40
A.3. 02 to 03 40
A.4. 03 to 04 40
A.5. 04 to 05 41
A.6. 05 to 06 41
A.7. 06 to 07 41
A.8. 07 to 08 41
A.9. 08 to 09 41
Acknowledgements 42
Authors' Addresses 42

1. Introduction

This document defines three YANG 1.1 [RFC7950] modules: the first defines a grouping for a generic SSH client, the second defines a grouping for a generic SSH server, and the third defines identities and groupings common to both the client and the server. It is intended that these groupings will be used by applications using the SSH protocol [RFC4252], [RFC4253], and [RFC4254]. For instance, these groupings could be used to help define the data model for an OpenSSH [OPENSSH] server or a NETCONF over SSH [RFC6242] based server.

The client and server YANG modules in this document each define one grouping, which is focused on just SSH-specific configuration, and specifically avoids any transport-level configuration, such as what ports to listen on or connect to. This affords applications the opportunity to define their own strategy for how the underlying TCP connection is established. For instance, applications supporting NETCONF Call Home [RFC8071] could use the "ssh-server-grouping" grouping for the SSH parts it provides, while adding data nodes for the TCP-level call-home configuration.

The modules defined in this document use groupings defined in [I-D.ietf-netconf-keystore] enabling keys to be either locally defined or a reference to globally configured values.

The modules defined in this document optionally support [RFC6187] enabling X.509v3 certificate based host keys and public keys.

2. Terminology

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.

3. The SSH Client Model

3.1. Tree Diagram

This section provides a tree diagram [RFC8340] for the "ietf-ssh-client" module that does not have groupings expanded.

```
module: ietf-ssh-client

  grouping ssh-client-grouping
    +---u client-identity-grouping
    +---u server-auth-grouping
    +---u transport-params-grouping
    +---u keepalives-grouping
  grouping client-identity-grouping
    +-- ssh-client-identity
       +-- username?            string
       +-- (auth-type)
          +--:(password)
          |  +-- password?      string
          +--:(public-key)
          |  +-- public-key
          |     +---u client-identity-grouping
          +--:(certificate)
             +-- certificate {sshcmn:ssh-x509-certs}?
                +---u client-identity-grouping
  grouping server-auth-grouping
    +-- ssh-server-auth
       +-- pinned-ssh-host-keys?   ta:pinned-host-keys-ref
       |       {ta:ssh-host-keys}?
       +-- pinned-ca-certs?        ta:pinned-certificates-ref
       |       {sshcmn:ssh-x509-certs,ta:x509-certificates}?
       +-- pinned-server-certs?    ta:pinned-certificates-ref
               {sshcmn:ssh-x509-certs,ta:x509-certificates}?
  grouping transport-params-grouping
    +-- ssh-transport-params {ssh-client-transport-params-config}?
       +---u transport-params-grouping
  grouping keepalives-grouping
    +-- ssh-keepalives {ssh-client-keepalives}?
       +-- max-wait?       uint16
       +-- max-attempts?   uint8
```

3.2. Example Usage

This section presents two examples showing the ssh-client-grouping populated with some data. These examples are effectively the same except the first configures the client identity using a local key while the second uses a key configured in a keystore. Both examples are consistent with the examples presented in Section 3 of [I-D.ietf-netconf-trust-anchors] and Section 3.2 of [I-D.ietf-netconf-keystore].

The following example configures the client identity using a local key:

```
========== NOTE: '\\' line wrapping per BCP XX (RFC XXXX) ===========

<ssh-client
   xmlns="urn:ietf:params:xml:ns:yang:ietf-ssh-client"
   xmlns:algs="urn:ietf:params:xml:ns:yang:ietf-ssh-common">

  <!-- how this client will authenticate itself to the server -->
  <ssh-client-identity>
    <username>foobar</username>
    <public-key>
      <local-definition>
        <algorithm xmlns:ct="urn:ietf:params:xml:ns:yang:ietf-crypto\
\-types">ct:rsa2048</algorithm>
        <private-key>base64encodedvalue==</private-key>
        <public-key>base64encodedvalue==</public-key>
      </local-definition>
    </public-key>
  </ssh-client-identity>

  <!-- which host-keys will this client trust -->
  <ssh-server-auth>
    <pinned-ssh-host-keys>explicitly-trusted-ssh-host-keys</pinned-s\
\sh-host-keys>
  </ssh-server-auth>

  <ssh-transport-params>
    <host-key>
      <host-key-alg>algs:ssh-rsa</host-key-alg>
    </host-key>
    <key-exchange>
      <key-exchange-alg>
        algs:diffie-hellman-group-exchange-sha256
      </key-exchange-alg>
    </key-exchange>
    <encryption>
      <encryption-alg>algs:aes256-ctr</encryption-alg>
      <encryption-alg>algs:aes192-ctr</encryption-alg>
      <encryption-alg>algs:aes128-ctr</encryption-alg>
      <encryption-alg>algs:aes256-cbc</encryption-alg>
      <encryption-alg>algs:aes192-cbc</encryption-alg>
      <encryption-alg>algs:aes128-cbc</encryption-alg>
    </encryption>
    <mac>
      <mac-alg>algs:hmac-sha2-256</mac-alg>
      <mac-alg>algs:hmac-sha2-512</mac-alg>
    </mac>
  </ssh-transport-params>
```

```
     <ssh-keepalives>
       <max-wait>30</max-wait>
       <max-attempts>3</max-attempts>
     </ssh-keepalives>

   </ssh-client>
```

The following example configures the client identity using a key from the keystore:

```
   ========== NOTE: '\\' line wrapping per BCP XX (RFC XXXX) ===========

   <ssh-client
      xmlns="urn:ietf:params:xml:ns:yang:ietf-ssh-client"
      xmlns:algs="urn:ietf:params:xml:ns:yang:ietf-ssh-common">

     <!-- how this client will authenticate itself to the server -->
     <ssh-client-identity>
       <username>foobar</username>
       <public-key>
         <keystore-reference>ex-rsa-key</keystore-reference>
       </public-key>
     </ssh-client-identity>

     <!-- which host-keys will this client trust -->
     <ssh-server-auth>
       <pinned-ssh-host-keys>explicitly-trusted-ssh-host-keys</pinned-s\
   \sh-host-keys>
     </ssh-server-auth>

     <ssh-transport-params>
       <host-key>
         <host-key-alg>algs:ssh-rsa</host-key-alg>
       </host-key>
       <key-exchange>
         <key-exchange-alg>
           algs:diffie-hellman-group-exchange-sha256
         </key-exchange-alg>
       </key-exchange>
       <encryption>
         <encryption-alg>algs:aes256-ctr</encryption-alg>
         <encryption-alg>algs:aes192-ctr</encryption-alg>
         <encryption-alg>algs:aes128-ctr</encryption-alg>
         <encryption-alg>algs:aes256-cbc</encryption-alg>
         <encryption-alg>algs:aes192-cbc</encryption-alg>
         <encryption-alg>algs:aes128-cbc</encryption-alg>
       </encryption>
       <mac>
```

```
        <mac-alg>algs:hmac-sha2-256</mac-alg>
        <mac-alg>algs:hmac-sha2-512</mac-alg>
      </mac>
    </ssh-transport-params>

    <ssh-keepalives>
      <max-wait>30</max-wait>
      <max-attempts>3</max-attempts>
    </ssh-keepalives>

  </ssh-client>
```

3.3. YANG Module

This YANG module has normative references to [I-D.ietf-netconf-trust-anchors], and [I-D.ietf-netconf-keystore].

```
<CODE BEGINS> file "ietf-ssh-client@2019-03-09.yang"
module ietf-ssh-client {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-ssh-client";
  prefix "sshc";

  import ietf-ssh-common {
    prefix sshcmn;
    revision-date 2019-03-09; // stable grouping definitions
    reference
      "RFC XXXX: YANG Groupings for SSH Clients and SSH Servers";
  }

  import ietf-trust-anchors {
    prefix ta;
    reference
      "RFC YYYY: YANG Data Model for Global Trust Anchors";
  }

  import ietf-keystore {
    prefix ks;
    reference
      "RFC ZZZZ:
         YANG Data Model for a Centralized Keystore Mechanism";
  }

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

  contact
   "WG Web:   <http://datatracker.ietf.org/wg/netconf/>
```

```
     WG List:  <mailto:netconf@ietf.org>
     Author:   Kent Watsen <mailto:kent+ietf@watsen.net>
     Author:   Gary Wu <mailto:garywu@cisco.com>";

   description
    "This module defines reusable groupings for SSH clients that
     can be used as a basis for specific SSH client instances.

     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.

     Copyright (c) 2019 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 "2019-03-09" {
     description
      "Initial version";
     reference
      "RFC XXXX: YANG Groupings for SSH Clients and SSH Servers";
   }

   // Features

   feature ssh-client-transport-params-config {
     description
       "SSH transport layer parameters are configurable on an SSH
        client.";
   }

   feature ssh-client-keepalives {
     description
       "Per socket SSH keepalive parameters are configurable for
        SSH clients on the server implementing this feature.";
   }
```

```
   // Groupings

   grouping ssh-client-grouping {
     description
       "A reusable grouping for configuring a SSH client without
        any consideration for how an underlying TCP session is
        established.";
     uses client-identity-grouping;
     uses server-auth-grouping;
     uses transport-params-grouping;
     uses keepalives-grouping;
   }

   grouping client-identity-grouping {
     description
       "A reusable grouping for configuring a SSH client identity.";
     container ssh-client-identity {
       description
         "The credentials used by the client to authenticate to
          the SSH server.";
       leaf username {
         type string;
         description
           "The username of this user.  This will be the username
            used, for instance, to log into an SSH server.";
       }
       choice auth-type {
         mandatory true;
         description
           "The authentication type.";
         leaf password {
           type string;
           description
             "A password to be used for client authentication.";
         }
         container public-key {
           uses ks:local-or-keystore-asymmetric-key-grouping;
           description
             "A locally-defined or referenced asymmetric key pair
              to be used for client authentication.";
           reference
             "RFC ZZZZ:
               YANG Data Model for a Centralized Keystore Mechanism";
         }
         container certificate {
           if-feature sshcmn:ssh-x509-certs;
           uses ks:local-or-keystore-end-entity-cert-with-key-grouping;
           description
```

```
             "A locally-defined or referenced certificate
              to be used for client authentication.";
           reference
             "RFC ZZZZ
               YANG Data Model for a Centralized Keystore Mechanism";
         }
       } // auth-type
     } // client-identity
   } // client-identity-grouping

   grouping server-auth-grouping {
     description
       "A reusable grouping for configuring SSH server
        authentication.";
     container ssh-server-auth {
       must 'pinned-ssh-host-keys or pinned-ca-certs or '
            + 'pinned-server-certs';
       description
         "Trusted server identities.";
       leaf pinned-ssh-host-keys {
         if-feature "ta:ssh-host-keys";
         type ta:pinned-host-keys-ref;
         description
           "A reference to a list of SSH host keys used by the
            SSH client to authenticate SSH server host keys.
            A server host key is authenticated if it is an exact
            match to a configured SSH host key.";
         reference
           "RFC YYYY: YANG Data Model for Global Trust Anchors";
       }
       leaf pinned-ca-certs {
         if-feature sshcmn:ssh-x509-certs;
         if-feature "ta:x509-certificates";
         type ta:pinned-certificates-ref;
         description
           "A reference to a list of certificate authority (CA)
            certificates used by the SSH client to authenticate
            SSH server certificates.  A server certificate is
            authenticated if it has a valid chain of trust to
            a configured CA certificate.";
         reference
           "RFC YYYY: YANG Data Model for Global Trust Anchors";
       }

       leaf pinned-server-certs {
         if-feature sshcmn:ssh-x509-certs;
         if-feature "ta:x509-certificates";
         type ta:pinned-certificates-ref;
```

```
        description
          "A reference to a list of server certificates used by
           the SSH client to authenticate SSH server certificates.
           A server certificate is authenticated if it is an
           exact match to a configured server certificate.";
        reference
          "RFC YYYY: YANG Data Model for Global Trust Anchors";
      }
    } // server-auth
  } // server-auth-grouping

  grouping transport-params-grouping {
    description
      "A reusable grouping for configuring a SSH transport
       parameters.";
    container ssh-transport-params {
      if-feature ssh-client-transport-params-config;
      description
        "Configurable parameters of the SSH transport layer.";
      uses sshcmn:transport-params-grouping;
    }
  } // transport-params-grouping

  grouping keepalives-grouping {
    description
      "A reusable grouping for configuring SSH client keepalive
       parameters.";
    container ssh-keepalives {
      if-feature "ssh-client-keepalives";
      description
        "Configures the keep-alive policy, to proactively test the
         aliveness of the SSH server.  An unresponsive TLS server is
         dropped after approximately max-wait * max-attempts seconds.";
      leaf max-wait {
        type uint16 {
          range "1..max";
        }
        units seconds;
        default 30;
        description
         "Sets the amount of time in seconds after which if no data
          has been received from the SSH server, a TLS-level message
          will be sent to test the aliveness of the SSH server.";
      }
      leaf max-attempts {
        type uint8;
        default 3;
        description
```

```
          "Sets the maximum number of sequential keep-alive messages
          that can fail to obtain a response from the SSH server
          before assuming the SSH server is no longer alive.";
       }
     }
   } // keepalives-grouping

 }
 <CODE ENDS>
```

4. The SSH Server Model

4.1. Tree Diagram

This section provides a tree diagram [RFC8340] for the "ietf-ssh-server" module that does not have groupings expanded.

```
module: ietf-ssh-server

  grouping ssh-server-grouping
    +---u server-identity-grouping
    +---u client-auth-grouping
    +---u transport-params-grouping
    +---u keepalives-grouping
  grouping server-identity-grouping
    +-- ssh-server-identity
       +-- host-key* [name]
          +-- name?                string
          +-- (host-key-type)
             +--:(public-key)
             |  +-- public-key
             |     +---u server-identity-grouping
             +--:(certificate)
                +-- certificate {sshcmn:ssh-x509-certs}?
                   +---u server-identity-grouping
  grouping client-auth-grouping
    +-- ssh-client-cert-auth {sshcmn:ssh-x509-certs}?
       +-- pinned-ca-certs?       ta:pinned-certificates-ref
       |       {ta:x509-certificates}?
       +-- pinned-client-certs?   ta:pinned-certificates-ref
               {ta:x509-certificates}?
  grouping transport-params-grouping
    +-- ssh-transport-params {ssh-server-transport-params-config}?
       +---u transport-params-grouping
  grouping keepalives-grouping
    +-- ssh-keepalives {ssh-server-keepalives}?
       +-- max-wait?       uint16
       +-- max-attempts?   uint8
```

4.2. Example Usage

This section presents two examples showing the ssh-server-grouping populated with some data. These examples are effectively the same except the first configures the server identity using a local key while the second uses a key configured in a keystore. Both examples are consistent with the examples presented in Section 3 of [I-D.ietf-netconf-trust-anchors] and Section 3.2 of [I-D.ietf-netconf-keystore].

The following example configures the server identity using a local key:

```
========== NOTE: '\\' line wrapping per BCP XX (RFC XXXX) ===========

<ssh-server xmlns="urn:ietf:params:xml:ns:yang:ietf-ssh-server"
            xmlns:algs="urn:ietf:params:xml:ns:yang:ietf-ssh-common">

  <!-- which host-keys will this SSH server present -->
  <ssh-server-identity>
    <host-key>
      <name>deployment-specific-certificate</name>
      <public-key>
        <local-definition>
          <algorithm xmlns:ct="urn:ietf:params:xml:ns:yang:ietf-cryp\
\to-types">ct:rsa2048</algorithm>
          <private-key>base64encodedvalue==</private-key>
          <public-key>base64encodedvalue==</public-key>
        </local-definition>
      </public-key>
    </host-key>
  </ssh-server-identity>

  <!-- which client-certs will this SSH server trust -->
  <ssh-client-cert-auth>
    <pinned-ca-certs>explicitly-trusted-client-ca-certs</pinned-ca-c\
\erts>
    <pinned-client-certs>explicitly-trusted-client-certs</pinned-cli\
\ent-certs>
  </ssh-client-cert-auth>

  <ssh-transport-params>
    <host-key>
      <host-key-alg>algs:ssh-rsa</host-key-alg>
    </host-key>
    <key-exchange>
      <key-exchange-alg>
        algs:diffie-hellman-group-exchange-sha256
```

```
        </key-exchange-alg>
      </key-exchange>
      <encryption>
        <encryption-alg>algs:aes256-ctr</encryption-alg>
        <encryption-alg>algs:aes192-ctr</encryption-alg>
        <encryption-alg>algs:aes128-ctr</encryption-alg>
        <encryption-alg>algs:aes256-cbc</encryption-alg>
        <encryption-alg>algs:aes192-cbc</encryption-alg>
        <encryption-alg>algs:aes128-cbc</encryption-alg>
      </encryption>
      <mac>
        <mac-alg>algs:hmac-sha2-256</mac-alg>
        <mac-alg>algs:hmac-sha2-512</mac-alg>
      </mac>
    </ssh-transport-params>

  </ssh-server>
```

The following example configures the server identity using a key from the keystore:

```
========== NOTE: '\\' line wrapping per BCP XX (RFC XXXX) ===========

<ssh-server xmlns="urn:ietf:params:xml:ns:yang:ietf-ssh-server"
            xmlns:algs="urn:ietf:params:xml:ns:yang:ietf-ssh-common">

  <!-- which host-keys will this SSH server present -->
  <ssh-server-identity>
    <host-key>
      <name>deployment-specific-certificate</name>
      <public-key>
        <keystore-reference>ex-rsa-key</keystore-reference>
      </public-key>
    </host-key>
  </ssh-server-identity>

  <!-- which client-certs will this SSH server trust -->
  <ssh-client-cert-auth>
    <pinned-ca-certs>explicitly-trusted-client-ca-certs</pinned-ca-c\
\erts>
    <pinned-client-certs>explicitly-trusted-client-certs</pinned-cli\
\ent-certs>
  </ssh-client-cert-auth>

  <ssh-transport-params>
    <host-key>
      <host-key-alg>algs:ssh-rsa</host-key-alg>
    </host-key>
    <key-exchange>
      <key-exchange-alg>
        algs:diffie-hellman-group-exchange-sha256
      </key-exchange-alg>
    </key-exchange>
    <encryption>
      <encryption-alg>algs:aes256-ctr</encryption-alg>
      <encryption-alg>algs:aes192-ctr</encryption-alg>
      <encryption-alg>algs:aes128-ctr</encryption-alg>
      <encryption-alg>algs:aes256-cbc</encryption-alg>
      <encryption-alg>algs:aes192-cbc</encryption-alg>
      <encryption-alg>algs:aes128-cbc</encryption-alg>
    </encryption>
    <mac>
      <mac-alg>algs:hmac-sha2-256</mac-alg>
      <mac-alg>algs:hmac-sha2-512</mac-alg>
    </mac>
  </ssh-transport-params>

</ssh-server>
```

4.3. YANG Module

This YANG module has normative references to [I-D.ietf-netconf-trust-anchors] and [I-D.ietf-netconf-keystore] and informative references to [RFC4253] and [RFC7317].

```
<CODE BEGINS> file "ietf-ssh-server@2019-03-09.yang"
========== NOTE: '\\' line wrapping per BCP XX (RFC XXXX) ===========

module ietf-ssh-server {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-ssh-server";
  prefix "sshs";

  import ietf-ssh-common {
    prefix sshcmn;
    revision-date 2019-03-09; // stable grouping definitions
    reference
      "RFC XXXX: YANG Groupings for SSH Clients and SSH Servers";
  }

  import ietf-trust-anchors {
    prefix ta;
    reference
      "RFC YYYY: YANG Data Model for Global Trust Anchors";
  }

  import ietf-keystore {
    prefix ks;
    reference
      "RFC ZZZZ:
         YANG Data Model for a Centralized Keystore Mechanism";
  }

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

  contact
   "WG Web:   <http://datatracker.ietf.org/wg/netconf/>
    WG List:  <mailto:netconf@ietf.org>
    Author:   Kent Watsen <mailto:kent+ietf@watsen.net>
    Author:   Gary Wu <mailto:garywu@cisco.com>";

  description
   "This module defines reusable groupings for SSH servers that
    can be used as a basis for specific SSH server instances.

    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.

       Copyright (c) 2019 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 "2019-03-09" {
       description
        "Initial version";
       reference
        "RFC XXXX: YANG Groupings for SSH Clients and SSH Servers";
     }

     // Features

     feature ssh-server-transport-params-config {
       description
         "SSH transport layer parameters are configurable on an SSH
          server.";
     }

     feature ssh-server-keepalives {
       description
         "Per socket SSH keepalive parameters are configurable for
          SSH servers on the server implementing this feature.";
     }


     // Groupings

     grouping ssh-server-grouping {
       description
         "A reusable grouping for configuring a SSH server without
          any consideration for how underlying TCP sessions are
          established.";
```

```
      uses server-identity-grouping;
      uses client-auth-grouping;
      uses transport-params-grouping;
      uses keepalives-grouping;
    }

    grouping server-identity-grouping {
      description
        "A reusable grouping for configuring an SSH server identity.";
      container ssh-server-identity {
        description
          "The list of host-keys the SSH server will present when
           establishing a SSH connection.";
        list host-key {
          key name;
          min-elements 1;
          ordered-by user;
          description
            "An ordered list of host keys the SSH server will use to
             construct its ordered list of algorithms, when sending
             its SSH_MSG_KEXINIT message, as defined in Section 7.1
             of RFC 4253.";
          reference
            "RFC 4253: The Secure Shell (SSH) Transport Layer
                       Protocol";
          leaf name {
            type string;
            description
              "An arbitrary name for this host-key";
          }
          choice host-key-type {
            mandatory true;
            description
              "The type of host key being specified";
            container public-key {
              uses ks:local-or-keystore-asymmetric-key-grouping;
              description
                "A locally-defined or referenced asymmetric key pair
                 to be used for the SSH server's host key.";
              reference
                "RFC ZZZZ: YANG Data Model for a Centralized
                           Keystore Mechanism";
            }
            container certificate {
              if-feature sshcmn:ssh-x509-certs;
              uses
                ks:local-or-keystore-end-entity-cert-with-key-grouping;
              description
```

```
                 "A locally-defined or referenced end-entity
                  certificate to be used for the SSH server's
                  host key.";
               reference
                 "RFC ZZZZ: YANG Data Model for a Centralized
                            Keystore Mechanism";
             }
           }
         }
       } // server-identity
     } // server-identity-grouping


     grouping client-auth-grouping {
       description
         "A reusable grouping for configuring a SSH client
          authentication.";
       container ssh-client-cert-auth {
         if-feature sshcmn:ssh-x509-certs;
         description
           "A reference to a list of pinned certificate authority (CA)
            certificates and a reference to a list of pinned client
            certificates.

            Note: password and public-key based client authentication
                  are not configured in this YANG module as they are
                  expected to be configured by the ietf-system module
                  defined in RFC 7317.";
         reference
           "RFC 7317: A YANG Data Model for System Management";
         leaf pinned-ca-certs {
           if-feature "ta:x509-certificates";
           type ta:pinned-certificates-ref;
           description
             "A reference to a list of certificate authority (CA)
              certificates used by the SSH server to authenticate
              SSH client certificates.  A client certificate is
              authenticated if it has a valid chain of trust to
              a configured pinned CA certificate.";
           reference
             "RFC YYYY: YANG Data Model for Global Trust Anchors";
         }
         leaf pinned-client-certs {
           if-feature "ta:x509-certificates";
           type ta:pinned-certificates-ref;
           description
             "A reference to a list of client certificates used by
              the SSH server to authenticate SSH client certificates.
```

```
              A clients certificate is authenticated if it is an
              exact match to a configured pinned client certificate.";
            reference
              "RFC YYYY: YANG Data Model for Global Trust Anchors";
          }
        }
      } // client-auth-grouping


      grouping transport-params-grouping {
        description
          "A reusable grouping for configuring a SSH transport
           parameters.";
        container ssh-transport-params {
          if-feature ssh-server-transport-params-config;
          description
            "Configurable parameters of the SSH transport layer.";
          uses sshcmn:transport-params-grouping;
        }
      } // transport-params-grouping


      grouping keepalives-grouping {
        description
          "A reusable grouping for configuring SSH server keepalive
           parameters.";
        container ssh-keepalives {
          if-feature "ssh-server-keepalives";
          description
            "Configures the keep-alive policy, to proactively test the
             aliveness of the SSL client.  An unresponsive SSL client is
             dropped after approximately max-wait * max-attempts seconds\
    \.";
          leaf max-wait {
            type uint16 {
              range "1..max";
            }
            units seconds;
            default 30;
            description
             "Sets the amount of time in seconds after which if no data
              has been received from the SSL client, a SSL-level message
              will be sent to test the aliveness of the SSL client.";
          }
          leaf max-attempts {
            type uint8;
            default 3;
            description
```

```
            "Sets the maximum number of sequential keep-alive messages
            that can fail to obtain a response from the SSL client
            before assuming the SSL client is no longer alive.";
          }
        }
      } // keepalives-grouping

    }
    <CODE ENDS>
```

5. The SSH Common Model

The SSH common model presented in this section contains identities and groupings common to both SSH clients and SSH servers. The transport-params-grouping can be used to configure the list of SSH transport algorithms permitted by the SSH client or SSH server. The lists of algorithms are ordered such that, if multiple algorithms are permitted by the client, the algorithm that appears first in its list that is also permitted by the server is used for the SSH transport layer connection. The ability to restrict the algorithms allowed is provided in this grouping for SSH clients and SSH servers that are capable of doing so and may serve to make SSH clients and SSH servers compliant with security policies.

[I-D.ietf-netconf-crypto-types] defines six categories of cryptographic algorithms (hash-algorithm, symmetric-key-encryption-algorithm, mac-algorithm, asymmetric-key-encryption-algorithm, signature-algorithm, key-negotiation-algorithm) and lists several widely accepted algorithms for each of them. The SSH client and server models use one or more of these algorithms. The SSH common model includes four parameters for configuring its permitted SSH algorithms, which are: host-key-alg, key-exchange-alg, encryption-alg and mac-alg. The following tables are provided, in part, to define the subset of algorithms defined in the crypto-types model used by SSH and, in part, to ensure compatibility of configured SSH cryptographic parameters for configuring its permitted SSH algorithms ("sshcmn" representing SSH common model, and "ct" representing crypto-types model which the SSH client/server model is based on):

sshcmn:host-key-alg	ct:signature-algorithm
dsa-sha1	dsa-sha1
rsa-pkcs1-sha1	rsa-pkcs1-sha1
rsa-pkcs1-sha256	rsa-pkcs1-sha256
rsa-pkcs1-sha512	rsa-pkcs1-sha512
ecdsa-secp256r1-sha256	ecdsa-secp256r1-sha256
ecdsa-secp384r1-sha384	ecdsa-secp384r1-sha384
ecdsa-secp521r1-sha512	ecdsa-secp521r1-sha512
x509v3-rsa-pkcs1-sha1	x509v3-rsa-pkcs1-sha1
x509v3-rsa2048-pkcs1-sha256	x509v3-rsa2048-pkcs1-sha1
x509v3-ecdsa-secp256r1-sha256	x509v3-ecdsa-secp256r1-sha256
x509v3-ecdsa-secp384r1-sha384	x509v3-ecdsa-secp384r1-sha384
x509v3-ecdsa-secp521r1-sha512	x509v3-ecdsa-secp521r1-sha512

Table 1 The SSH Host-key-alg Compatibility Matrix

sshcmn:key-exchange-alg	ct:key-negotiation-algorithm
diffie-hellman-group14-sha1	diffie-hellman-group14-sha1
diffie-hellman-group14-sha256	diffie-hellman-group14-sha256
diffie-hellman-group15-sha512	diffie-hellman-group15-sha512
diffie-hellman-group16-sha512	diffie-hellman-group16-sha512
diffie-hellman-group17-sha512	diffie-hellman-group17-sha512
diffie-hellman-group18-sha512	diffie-hellman-group18-sha512
ecdh-sha2-secp256r1	ecdh-sha2-secp256r1
ecdh-sha2-secp384r1	ecdh-sha2-secp384r1

Table 2 The SSH Key-exchange-alg Compatibility Matrix

sshcmn:encryption-alg	ct:symmetric-key-encryption-algorithm
aes-128-cbc	aes-128-cbc
aes-192-cbc	aes-192-cbc
aes-256-cbc	aes-256-cbc
aes-128-ctr	aes-128-ctr
aes-192-ctr	aes-192-ctr
aes-256-ctr	aes-256-ctr

Table 3 The SSH Encryption-alg Compatibility Matrix

sshcmn:mac-alg	ct:mac-algorithm
hmac-sha1	hmac-sha1
hmac-sha1-96	hmac-sha1-96
hmac-sha2-256	hmac-sha2-256
hmac-sha2-512	hmac-sha2-512

Table 4 The SSH Mac-alg Compatibility Matrix

As is seen in the tables above, the names of the "sshcmn" algorithms are all identical to the names of algorithms defined in [I-D.ietf-netconf-crypto-types]. While appearing to be redundant, it is important to realize that not all the algorithms defined in [I-D.ietf-netconf-crypto-types] are supported by SSH. That is, the algorithms supported by SSH are a subset of the algorithms defined in [I-D.ietf-netconf-crypto-types]. The algorithms used by SSH are redefined in this document in order to constrain the algorithms that may be selected to just the ones used by SSH.

Features are defined for algorithms that are OPTIONAL or are not widely supported by popular implementations. Note that the list of algorithms is not exhaustive. As well, some algorithms that are REQUIRED by [RFC4253] are missing, notably "ssh-dss" and "diffie-hellman-group1-sha1" due to their weak security and there being alternatives that are widely supported.

5.1. Tree Diagram

The following tree diagram [RFC8340] provides an overview of the data model for the "ietf-ssh-common" module.

```
module: ietf-ssh-common

  grouping transport-params-grouping
    +-- host-key
    |  +-- host-key-alg*   identityref
    +-- key-exchange
    |  +-- key-exchange-alg*   identityref
    +-- encryption
    |  +-- encryption-alg*   identityref
    +-- mac
       +-- mac-alg*   identityref
```

5.2. Example Usage

This following example illustrates how the transport-params-grouping appears when populated with some data.

```
<transport-params
  xmlns="urn:ietf:params:xml:ns:yang:ietf-ssh-common"
  xmlns:algs="urn:ietf:params:xml:ns:yang:ietf-ssh-common">
  <host-key>
    <host-key-alg>algs:x509v3-rsa2048-sha256</host-key-alg>
    <host-key-alg>algs:ssh-rsa</host-key-alg>
  </host-key>
  <key-exchange>
    <key-exchange-alg>
      algs:diffie-hellman-group-exchange-sha256
    </key-exchange-alg>
  </key-exchange>
  <encryption>
    <encryption-alg>algs:aes256-ctr</encryption-alg>
    <encryption-alg>algs:aes192-ctr</encryption-alg>
    <encryption-alg>algs:aes128-ctr</encryption-alg>
    <encryption-alg>algs:aes256-cbc</encryption-alg>
    <encryption-alg>algs:aes192-cbc</encryption-alg>
    <encryption-alg>algs:aes128-cbc</encryption-alg>
  </encryption>
  <mac>
    <mac-alg>algs:hmac-sha2-256</mac-alg>
    <mac-alg>algs:hmac-sha2-512</mac-alg>
  </mac>
</transport-params>
```

5.3. YANG Module

This YANG module has normative references to [RFC4253], [RFC4344], [RFC4419], [RFC5656], [RFC6187], and [RFC6668].

```
<CODE BEGINS> file "ietf-ssh-common@2019-03-09.yang"
module ietf-ssh-common {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-ssh-common";
  prefix "sshcmn";

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

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

```
       Author:   Kent Watsen <mailto:kent+ietf@watsen.net>
       Author:   Gary Wu <mailto:garywu@cisco.com>";

     description
      "This module defines a common features, identities, and
       groupings for Secure Shell (SSH).

       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.

       Copyright (c) 2019 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 "2019-03-09" {
       description
        "Initial version";
       reference
        "RFC XXXX: YANG Groupings for SSH Clients and SSH Servers";
     }

     // features

     feature ssh-ecc {
       description
         "Elliptic Curve Cryptography is supported for SSH.";
       reference
         "RFC 5656: Elliptic Curve Algorithm Integration in the
                    Secure Shell Transport Layer";
     }

     feature ssh-x509-certs {
       description
         "X.509v3 certificates are supported for SSH per RFC 6187.";
       reference
```

```
        "RFC 6187: X.509v3 Certificates for Secure Shell
                   Authentication";
    }

    feature ssh-dh-group-exchange {
      description
        "Diffie-Hellman Group Exchange is supported for SSH.";
      reference
        "RFC 4419: Diffie-Hellman Group Exchange for the
                   Secure Shell (SSH) Transport Layer Protocol";
    }

    feature ssh-ctr {
      description
        "SDCTR encryption mode is supported for SSH.";
      reference
        "RFC 4344: The Secure Shell (SSH) Transport Layer
                   Encryption Modes";
    }

    feature ssh-sha2 {
      description
        "The SHA2 family of cryptographic hash functions is
         supported for SSH.";
      reference
        "FIPS PUB 180-4: Secure Hash Standard (SHS)";
    }

    // identities

    identity public-key-alg-base {
      description
        "Base identity used to identify public key algorithms.";
    }

    identity ssh-dss {
      base public-key-alg-base;
      description
        "Digital Signature Algorithm using SHA-1 as the
         hashing algorithm.";
      reference
        "RFC 4253:
           The Secure Shell (SSH) Transport Layer Protocol";
    }

    identity ssh-rsa {
      base public-key-alg-base;
      description
```

```
        "RSASSA-PKCS1-v1_5 signature scheme using SHA-1 as the
         hashing algorithm.";
      reference
        "RFC 4253:
           The Secure Shell (SSH) Transport Layer Protocol";
    }

    identity ecdsa-sha2-nistp256 {
      base public-key-alg-base;
      if-feature "ssh-ecc and ssh-sha2";
      description
        "Elliptic Curve Digital Signature Algorithm (ECDSA) using the
         nistp256 curve and the SHA2 family of hashing algorithms.";
      reference
        "RFC 5656: Elliptic Curve Algorithm Integration in the
                   Secure Shell Transport Layer";
    }

    identity ecdsa-sha2-nistp384 {
      base public-key-alg-base;
      if-feature "ssh-ecc and ssh-sha2";
      description
        "Elliptic Curve Digital Signature Algorithm (ECDSA) using the
         nistp384 curve and the SHA2 family of hashing algorithms.";
      reference
        "RFC 5656: Elliptic Curve Algorithm Integration in the
                   Secure Shell Transport Layer";
    }

    identity ecdsa-sha2-nistp521 {
      base public-key-alg-base;
      if-feature "ssh-ecc and ssh-sha2";
      description
        "Elliptic Curve Digital Signature Algorithm (ECDSA) using the
         nistp521 curve and the SHA2 family of hashing algorithms.";
      reference
        "RFC 5656: Elliptic Curve Algorithm Integration in the
                   Secure Shell Transport Layer";
    }

    identity x509v3-ssh-rsa {
      base public-key-alg-base;
      if-feature ssh-x509-certs;
      description
        "RSASSA-PKCS1-v1_5 signature scheme using a public key stored
         in an X.509v3 certificate and using SHA-1 as the hashing
         algorithm.";
      reference
```

```
        "RFC 6187: X.509v3 Certificates for Secure Shell
                   Authentication";
    }

    identity x509v3-rsa2048-sha256 {
      base public-key-alg-base;
      if-feature "ssh-x509-certs and ssh-sha2";
      description
        "RSASSA-PKCS1-v1_5 signature scheme using a public key stored
         in an X.509v3 certificate and using SHA-256 as the hashing
         algorithm.  RSA keys conveyed using this format MUST have a
         modulus of at least 2048 bits.";
      reference
        "RFC 6187: X.509v3 Certificates for Secure Shell
                   Authentication";
    }

    identity x509v3-ecdsa-sha2-nistp256 {
      base public-key-alg-base;
      if-feature "ssh-ecc and ssh-x509-certs and ssh-sha2";
      description
        "Elliptic Curve Digital Signature Algorithm (ECDSA)
         using the nistp256 curve with a public key stored in
         an X.509v3 certificate and using the SHA2 family of
         hashing algorithms.";
      reference
        "RFC 6187: X.509v3 Certificates for Secure Shell
                   Authentication";
    }

    identity x509v3-ecdsa-sha2-nistp384 {
      base public-key-alg-base;
      if-feature "ssh-ecc and ssh-x509-certs and ssh-sha2";
      description
        "Elliptic Curve Digital Signature Algorithm (ECDSA)
         using the nistp384 curve with a public key stored in
         an X.509v3 certificate and using the SHA2 family of
         hashing algorithms.";
      reference
        "RFC 6187: X.509v3 Certificates for Secure Shell
                   Authentication";
    }

    identity x509v3-ecdsa-sha2-nistp521 {
      base public-key-alg-base;
      if-feature "ssh-ecc and ssh-x509-certs and ssh-sha2";
      description
        "Elliptic Curve Digital Signature Algorithm (ECDSA)
```

```
          using the nistp521 curve with a public key stored in
          an X.509v3 certificate and using the SHA2 family of
          hashing algorithms.";
       reference
         "RFC 6187: X.509v3 Certificates for Secure Shell
                    Authentication";
     }

     identity key-exchange-alg-base {
       description
         "Base identity used to identify key exchange algorithms.";
     }

     identity diffie-hellman-group14-sha1 {
       base key-exchange-alg-base;
       description
         "Diffie-Hellman key exchange with SHA-1 as HASH and
          Oakley Group 14 (2048-bit MODP Group).";
       reference
         "RFC 4253: The Secure Shell (SSH) Transport Layer Protocol";
     }

     identity diffie-hellman-group-exchange-sha1 {
       base key-exchange-alg-base;
       if-feature ssh-dh-group-exchange;
       description
         "Diffie-Hellman Group and Key Exchange with SHA-1 as HASH.";
       reference
         "RFC 4419: Diffie-Hellman Group Exchange for the
                    Secure Shell (SSH) Transport Layer Protocol";
     }

     identity diffie-hellman-group-exchange-sha256 {
       base key-exchange-alg-base;
       if-feature "ssh-dh-group-exchange and ssh-sha2";
       description
         "Diffie-Hellman Group and Key Exchange with SHA-256 as HASH.";
       reference
         "RFC 4419: Diffie-Hellman Group Exchange for the
                    Secure Shell (SSH) Transport Layer Protocol";
     }

     identity ecdh-sha2-nistp256 {
       base key-exchange-alg-base;
       if-feature "ssh-ecc and ssh-sha2";
       description
         "Elliptic Curve Diffie-Hellman (ECDH) key exchange using the
          nistp256 curve and the SHA2 family of hashing algorithms.";
```

```
      reference
        "RFC 5656: Elliptic Curve Algorithm Integration in the
                   Secure Shell Transport Layer";
    }

    identity ecdh-sha2-nistp384 {
      base key-exchange-alg-base;
      if-feature "ssh-ecc and ssh-sha2";
      description
        "Elliptic Curve Diffie-Hellman (ECDH) key exchange using the
         nistp384 curve and the SHA2 family of hashing algorithms.";
      reference
        "RFC 5656: Elliptic Curve Algorithm Integration in the
                   Secure Shell Transport Layer";
    }

    identity ecdh-sha2-nistp521 {
      base key-exchange-alg-base;
      if-feature "ssh-ecc and ssh-sha2";
      description
        "Elliptic Curve Diffie-Hellman (ECDH) key exchange using the
         nistp521 curve and the SHA2 family of hashing algorithms.";
      reference
        "RFC 5656: Elliptic Curve Algorithm Integration in the
                   Secure Shell Transport Layer";
    }

    identity encryption-alg-base {
      description
        "Base identity used to identify encryption algorithms.";
    }

    identity triple-des-cbc {
      base encryption-alg-base;
      description
        "Three-key 3DES in CBC mode.";
      reference
        "RFC 4253: The Secure Shell (SSH) Transport Layer Protocol";
    }

    identity aes128-cbc {
      base encryption-alg-base;
      description
       "AES in CBC mode, with a 128-bit key.";
      reference
       "RFC 4253: The Secure Shell (SSH) Transport Layer Protocol";
    }
```

```
identity aes192-cbc {
  base encryption-alg-base;
  description
    "AES in CBC mode, with a 192-bit key.";
  reference
    "RFC 4253: The Secure Shell (SSH) Transport Layer Protocol";
}

identity aes256-cbc {
  base encryption-alg-base;
  description
    "AES in CBC mode, with a 256-bit key.";
  reference
    "RFC 4253: The Secure Shell (SSH) Transport Layer Protocol";
}

identity aes128-ctr {
  base encryption-alg-base;
  if-feature ssh-ctr;
  description
    "AES in SDCTR mode, with 128-bit key.";
  reference
    "RFC 4344: The Secure Shell (SSH) Transport Layer Encryption
               Modes";
}

identity aes192-ctr {
  base encryption-alg-base;
  if-feature ssh-ctr;
  description
    "AES in SDCTR mode, with 192-bit key.";
  reference
    "RFC 4344: The Secure Shell (SSH) Transport Layer Encryption
               Modes";
}

identity aes256-ctr {
  base encryption-alg-base;
  if-feature ssh-ctr;
  description
    "AES in SDCTR mode, with 256-bit key.";
  reference
    "RFC 4344: The Secure Shell (SSH) Transport Layer Encryption
       Modes";
}

identity mac-alg-base {
  description
```

```
         "Base identity used to identify message authentication
          code (MAC) algorithms.";
     }

     identity hmac-sha1 {
       base mac-alg-base;
       description
         "HMAC-SHA1";
       reference
         "RFC 4253: The Secure Shell (SSH) Transport Layer Protocol";
     }

     identity hmac-sha2-256 {
       base mac-alg-base;
       if-feature "ssh-sha2";
       description
         "HMAC-SHA2-256";
       reference
         "RFC 6668: SHA-2 Data Integrity Verification for the
                    Secure Shell (SSH) Transport Layer Protocol";
     }

     identity hmac-sha2-512 {
       base mac-alg-base;
       if-feature "ssh-sha2";
       description
         "HMAC-SHA2-512";
       reference
         "RFC 6668: SHA-2 Data Integrity Verification for the
                    Secure Shell (SSH) Transport Layer Protocol";
     }

     // groupings

     grouping transport-params-grouping {
       description
         "A reusable grouping for SSH transport parameters.";
       reference
         "RFC 4253: The Secure Shell (SSH) Transport Layer Protocol";
       container host-key {
         description
           "Parameters regarding host key.";
         leaf-list host-key-alg {
           type identityref {
             base public-key-alg-base;
           }
           ordered-by user;
           description
```

```
             "Acceptable host key algorithms in order of descending
              preference.  The configured host key algorithms should
              be compatible with the algorithm used by the configured
              private key.  Please see Section 5 of RFC XXXX for
              valid combinations.

              If this leaf-list is not configured (has zero elements)
              the acceptable host key algorithms are implementation-
              defined.";
           reference
             "RFC XXXX: YANG Groupings for SSH Clients and SSH Servers";
         }
       }
       container key-exchange {
         description
           "Parameters regarding key exchange.";
         leaf-list key-exchange-alg {
           type identityref {
             base key-exchange-alg-base;
           }
           ordered-by user;
           description
            "Acceptable key exchange algorithms in order of descending
             preference.

             If this leaf-list is not configured (has zero elements)
             the acceptable key exchange algorithms are implementation
             defined.";
         }
       }
       container encryption {
         description
           "Parameters regarding encryption.";
         leaf-list encryption-alg {
           type identityref {
             base encryption-alg-base;
           }
           ordered-by user;
           description
            "Acceptable encryption algorithms in order of descending
             preference.

             If this leaf-list is not configured (has zero elements)
             the acceptable encryption algorithms are implementation
             defined.";
         }
       }
       container mac {
```

```
        description
          "Parameters regarding message authentication code (MAC).";
        leaf-list mac-alg {
          type identityref {
            base mac-alg-base;
          }
          ordered-by user;
          description
            "Acceptable MAC algorithms in order of descending
             preference.

             If this leaf-list is not configured (has zero elements)
             the acceptable MAC algorithms are implementation-
             defined.";
        }
      }

    } // transport-params-grouping

  }
  <CODE ENDS>
```

6. Security Considerations

The YANG modules defined in this document are designed to be accessed via YANG based management protocols, such as NETCONF [RFC6241] and RESTCONF [RFC8040]. Both of these protocols have mandatory-to-implement secure transport layers (e.g., SSH, TLS) with mutual authentication.

The NETCONF access control model (NACM) [RFC8341] provides the means to restrict access for particular users to a pre-configured subset of all available protocol operations and content.

Since the modules defined in this document define only groupings, these considerations are primarily for the designers of other modules that use these groupings.

There are a number of data nodes defined in the YANG modules that are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) to these data nodes without proper protection can have a negative effect on network operations. These are the subtrees and data nodes and their sensitivity/vulnerability:

/: The entire data tree defined by all the modules defined in this draft are sensitive to write operations. For instance, the

addition or removal of references to keys, certificates, trusted anchors, etc., can dramatically alter the implemented security policy. However, no NACM annotations are applied as the data SHOULD be editable by users other than a designated 'recovery session'.

Some of the readable data nodes in the YANG modules may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, or notification) to these data nodes. These are the subtrees and data nodes and their sensitivity/vulnerability:

/client-auth/password: This node in the 'ietf-ssh-client' module is additionally sensitive to read operations such that, in normal use cases, it should never be returned to a client. The only time this node should be returned is to support backup/restore type workflows. However, no NACM annotations are applied as the data SHOULD be writable by users other than a designated 'recovery session'.

Some of the RPC operations in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control access to these operations. These are the operations and their sensitivity/vulnerability:

NONE

7. IANA Considerations

7.1. The IETF XML Registry

This document registers three URIs in the "ns" subregistry of the IETF XML Registry [RFC3688]. Following the format in [RFC3688], the following registrations are requested:

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

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

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

7.2. The YANG Module Names Registry

This document registers three YANG modules in the YANG Module Names registry [RFC6020]. Following the format in [RFC6020], the following registrations are requested:

```
name:         ietf-ssh-client
namespace:    urn:ietf:params:xml:ns:yang:ietf-ssh-client
prefix:       sshc
reference:    RFC XXXX

name:         ietf-ssh-server
namespace:    urn:ietf:params:xml:ns:yang:ietf-ssh-server
prefix:       sshs
reference:    RFC XXXX

name:         ietf-ssh-common
namespace:    urn:ietf:params:xml:ns:yang:ietf-ssh-common
prefix:       sshcmn
reference:    RFC XXXX
```

8. References

8.1. Normative References

[I-D.ietf-netconf-crypto-types]
Watsen, K. and H. Wang, "Common YANG Data Types for Cryptography", draft-ietf-netconf-crypto-types-02 (work in progress), October 2018.

[I-D.ietf-netconf-keystore]
Watsen, K., "YANG Data Model for a Centralized Keystore Mechanism", draft-ietf-netconf-keystore-08 (work in progress), March 2019.

[I-D.ietf-netconf-trust-anchors]
Watsen, K., "YANG Data Model for Global Trust Anchors", draft-ietf-netconf-trust-anchors-03 (work in progress), March 2019.

[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>.

[RFC4344] Bellare, M., Kohno, T., and C. Namprempre, "The Secure Shell (SSH) Transport Layer Encryption Modes", RFC 4344, DOI 10.17487/RFC4344, January 2006, <https://www.rfc-editor.org/info/rfc4344>.

[RFC4419] Friedl, M., Provos, N., and W. Simpson, "Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol", RFC 4419, DOI 10.17487/RFC4419, March 2006, <https://www.rfc-editor.org/info/rfc4419>.

[RFC5656] Stebila, D. and J. Green, "Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer", RFC 5656, DOI 10.17487/RFC5656, December 2009, <https://www.rfc-editor.org/info/rfc5656>.

[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>.

[RFC6187] Igoe, K. and D. Stebila, "X.509v3 Certificates for Secure Shell Authentication", RFC 6187, DOI 10.17487/RFC6187, March 2011, <https://www.rfc-editor.org/info/rfc6187>.

[RFC6668] Bider, D. and M. Baushke, "SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol", RFC 6668, DOI 10.17487/RFC6668, July 2012, <https://www.rfc-editor.org/info/rfc6668>.

[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>.

[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>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

8.2. Informative References

[OPENSSH] Project, T. O., "OpenSSH", 2016, <http://www.openssh.com>.

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

[RFC4252] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol", RFC 4252, DOI 10.17487/RFC4252, January 2006, <https://www.rfc-editor.org/info/rfc4252>.

[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>.

[RFC4254] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Connection Protocol", RFC 4254, DOI 10.17487/RFC4254, January 2006, <https://www.rfc-editor.org/info/rfc4254>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC7317] Bierman, A. and M. Bjorklund, "A YANG Data Model for System Management", RFC 7317, DOI 10.17487/RFC7317, August 2014, <https://www.rfc-editor.org/info/rfc7317>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8071] Watsen, K., "NETCONF Call Home and RESTCONF Call Home", RFC 8071, DOI 10.17487/RFC8071, February 2017, <https://www.rfc-editor.org/info/rfc8071>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

Appendix A. Change Log

A.1. 00 to 01

- o Noted that '0.0.0.0' and '::' might have special meanings.
- o Renamed "keychain" to "keystore".

A.2. 01 to 02

- o Removed the groupings 'listening-ssh-client-grouping' and 'listening-ssh-server-grouping'. Now modules only contain the transport-independent groupings.
- o Simplified the "client-auth" part in the ietf-ssh-client module. It now inlines what it used to point to keystore for.
- o Added cipher suites for various algorithms into new 'ietf-ssh-common' module.

A.3. 02 to 03

- o Removed 'RESTRICTED' enum from 'password' leaf type.
- o Added a 'must' statement to container 'server-auth' asserting that at least one of the various auth mechanisms must be specified.
- o Fixed description statement for leaf 'trusted-ca-certs'.

A.4. 03 to 04

- o Change title to "YANG Groupings for SSH Clients and SSH Servers"
- o Added reference to RFC 6668
- o Added RFC 8174 to Requirements Language Section.
- o Enhanced description statement for ietf-ssh-server's "trusted-ca-certs" leaf.
- o Added mandatory true to ietf-ssh-client's "client-auth" 'choice' statement.
- o Changed the YANG prefix for module ietf-ssh-common from 'sshcom' to 'sshcmn'.
- o Removed the compression algorithms as they are not commonly configurable in vendors' implementations.

- o Updating descriptions in transport-params-grouping and the servers's usage of it.

- o Now tree diagrams reference ietf-netmod-yang-tree-diagrams

- o Updated YANG to use typedefs around leafrefs to common keystore paths

- o Now inlines key and certificates (no longer a leafref to keystore)

A.5. 04 to 05

- o Merged changes from co-author.

A.6. 05 to 06

- o Updated to use trust anchors from trust-anchors draft (was keystore draft)

- o Now uses new keystore grouping enabling asymmetric key to be either locally defined or a reference to the keystore.

A.7. 06 to 07

- o factored the ssh-[client|server]-groupings into more reusable groupings.

- o added if-feature statements for the new "ssh-host-keys" and "x509-certificates" features defined in draft-ietf-netconf-trust-anchors.

A.8. 07 to 08

- o Added a number of compatibility matrices to Section 5 (thanks Frank!)

- o Clarified that any configured "host-key-alg" values need to be compatible with the configured private key.

A.9. 08 to 09

- o Updated examples to reflect update to groupings defined in the keystore -09 draft.

- o Add SSH keepalives features and groupings.

- o Prefixed top-level SSH grouping nodes with 'ssh-' and support mashups.

- o Updated copyright date, boilerplate template, affiliation, and folding algorithm.

Acknowledgements

The authors would like to thank for following for lively discussions on list and in the halls (ordered by last name): Andy Bierman, Martin Bjorklund, Benoit Claise, Mehmet Ersue, Balazs Kovacs, David Lamparter, Alan Luchuk, Ladislav Lhotka, Radek Krejci, Tom Petch, Juergen Schoenwaelder, Phil Shafer, Sean Turner, Michal Vasko, and Bert Wijnen.

Authors' Addresses

Kent Watsen
Watsen Networks

EMail: kent+ietf@watsen.net

Gary Wu
Cisco Systems

EMail: garywu@cisco.com

Liang Xia
Huawei

EMail: frank.xialiang@huawei.com