Common YANG Data Types for Cryptography
draft-ietf-netconf-crypto-types-13

Abstract

This document defines four YANG modules for types useful to cryptographic applications. The modules defined include:

- ietf-crypto-types
- iana-symmetric-algs
- iana-asymmetric-algs
- iana-hash-algs

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:

- "2019-11-20" --> the publication date of this draft

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

- Appendix B. Change Log
Internet-Draft  Common YANG Data Types for Cryptography  November 2019

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 May 23, 2020.

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.  The Crypto Types Module .....................................  4
   2.1.  Tree Diagram .............................................  4
   2.2.  YANG Module .............................................  6
   2.3.  Examples ................................................  24
3.  The Symmetric Algorithms Module .............................  28
   3.1.  Tree Diagram .............................................  28
   3.2.  YANG Module .............................................  28
   3.3.  Examples ................................................  32
1. Introduction

This document defines four YANG 1.1 [RFC7950] modules for types useful to cryptographic applications. The modules defined include:

4. The Asymmetric Algorithms Module
   4.1. Tree Diagram
   4.2. YANG Module
   4.3. Examples

5. The Hash Algorithms Module

5.1. Tree Diagram
5.2. YANG Module
5.3. Examples

6. Security Considerations
   6.1. Support for Algorithms
   6.2. No Support for CRMF
   6.3. Access to Data Nodes

7. IANA Considerations
   7.1. The IETF XML Registry
   7.2. The YANG Module Names Registry

8. References
   8.1. Normative References
   8.2. Informative References

Appendix A. Change Log
   A.1. I-D to 00
   A.2. 00 to 01
   A.3. 01 to 02
   A.4. 02 to 03
   A.5. 03 to 04
   A.6. 04 to 05
   A.7. 05 to 06
   A.8. 06 to 07
   A.9. 07 to 08
   A.10. 08 to 09
   A.11. 09 to 10
   A.12. 10 to 11
   A.13. 11 to 12
   A.14. 12 to 13

Acknowledgements
Authors' Addresses
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 when, and only when, they appear in all capitals, as shown here.

2. The Crypto Types Module

2.1. Tree Diagram

This section provides a tree diagram [RFC8340] for the "ietf-crypto-types" module. Only "grouping" statements are represented, as tree diagrams have no means to represent identities or typedefs.

module: ietf-crypto-types

grouping symmetric-key-grouping
    +++ algorithm isa:symmetric-algorithm-type
    +++ key-format? identityref
    +++ (key-type)
        +--:(key)
            |  +-- key? binary
            +--:(hidden-key)
                +-- hidden-key? empty

grouping public-key-grouping
    +++ algorithm isa:asymmetric-algorithm-type
    +++ public-key-format? identityref
    +++ public-key binary

grouping asymmetric-key-pair-grouping
    +++ algorithm isa:asymmetric-algorithm-type
    +++ public-key-format? identityref
    +++ public-key binary
--- private-key-format?       identityref
--- (private-key-type)
|   ---:(private-key)
|     |   --- private-key?       binary
|     +---:(hidden-private-key)
|           |   --- hidden-private-key? empty

grouping trust-anchor-cert-grouping
--- cert?                     trust-anchor-cert-cms
|   ---n certificate-expiration
|     +-- expiration-date        yang:date-and-time

grouping trust-anchor-certs-grouping
--- cert*                     trust-anchor-cert-cms
|   ---n certificate-expiration
|     +-- expiration-date        yang:date-and-time

grouping end-entity-cert-grouping
--- cert?                     end-entity-cert-cms
|   ---n certificate-expiration
|     +-- expiration-date        yang:date-and-time

grouping end-entity-certs-grouping

--- cert*                     end-entity-cert-cms
|   ---n certificate-expiration
|     +-- expiration-date        yang:date-and-time

grouping asymmetric-key-pair-with-cert-grouping
--- algorithm
     |     iasa:asymmetric-algorithm-type
--- public-key-format?       identityref
--- public-key               binary
--- private-key-format?      identityref
--- (private-key-type)
     |     ---:(private-key)
     |     |     --- private-key?       binary
     |     +---:(hidden-private-key)
     |     |     +-- hidden-private-key? empty
--- cert?                     end-entity-cert-cms
|   ---n certificate-expiration
|     +-- expiration-date        yang:date-and-time

---w generate-certificate-signing-request
     |     ---w input
     |     |     +----w subject       binary
     |     |     +----w attributes?   binary
     +--ro output
2.2. YANG Module

This module has normative references to [RFC2404], [RFC3565], [RFC3686], [RFC4106], [RFC4253], [RFC4279], [RFC4309], [RFC4494], [RFC4543], [RFC4868], [RFC5280], [RFC5652], [RFC5656], [RFC6187], [RFC6991], [RFC7919], [RFC8268], [RFC8332], [RFC8341], [RFC8422], [RFC8446], and [ITU.X690.2015].

This module has an informational reference to [RFC2986], [RFC3174], [RFC4493], [RFC5915], [RFC6125], [RFC6234], [RFC6239], [RFC6507], [RFC8017], [RFC8032], [RFC8439].

<CODE BEGINS> file "ietf-crypto-types@2019-11-20.yang"

module ietf-crypto-types {

++-ro certificate-signing-request    binary
+--- algorithm
   |   iasa:asymmetric-algorithm-type
+--- public-key-format?    identityref
+--- public-key    binary
+--- private-key-format?    identityref
+--- (private-key-type)
   |   +++:(private-key)
   |     |   ++- private-key?    binary
   |   +++:(hidden-private-key)
   |     |   +++ hidden-private-key?    empty
+--- certificates
   |   +++ certificate*    [name]
   |     |     -- name?    string
   |     |     ++ cert?    end-entity-cert-cms
   |     |     ++-n certificate-expiration
   |     |       ++ expiration-date    yang:date-and-time
++-x generate-certificate-signing-request
   ++-w input
   |   +++-w subject    binary
   |   +++-w attributes?    binary
++-ro output
   ++-ro certificate-signing-request    binary

Watsen & Wang             Expires May 23, 2020                  [Page 5]

Internet-Draft   Common YANG Data Types for Cryptography   November 2019
yang-version 1.1;
namespace "urn:ietf:params:xml:ns:yang:ietf-crypto-types";
prefix ct;

import ietf-yang-types {
  prefix yang;
  reference
    "RFC 6991: Common YANG Data Types";
}

import ietf-netconf-acm {
  prefix nacm;
  reference
    "RFC 8341: Network Configuration Access Control Model";
}

//import iana-hash-algs {
//  prefix iha;
//  reference
//    "RFC XXXX: Common YANG Data Types for Cryptography";
//}

import iana-symmetric-algs {
  prefix isa;
  reference
    "RFC XXXX: Common YANG Data Types for Cryptography";
}

import iana-asymmetric-algs {
  prefix iasa;
  reference
    "RFC XXXX: Common YANG Data Types for Cryptography";
}
description
"This module defines common YANG types for cryptographic applications.

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 (https://trustee.ietf.org/license-info).

This version of this YANG module is part of RFC XXXX (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself for full legal notices.

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 (RFC 2119) (RFC 8174) when, and only when, they appear in all capitals, as shown here."

revision 2019-11-20 {
    description
        "Initial version";
    reference
        "RFC XXXX: Common YANG Data Types for Cryptography";
}

/*****************
/*  Features  */
*****************/

feature "one-asymmetric-key-format" {
    description
        "Indicates that the server supports the
feature "one-symmetric-key-format" {
    description
    "Indicates that the server supports the
    'one-symmetric-key-format' identity."
}

feature "encrypted-one-symmetric-key-format" {
    description
    "Indicates that the server supports the
    'encrypted-one-symmetric-key-format' identity."
}

feature "encrypted-one-asymmetric-key-format" {
    description
    "Indicates that the server supports the
    'encrypted-one-asymmetric-key-format' identity."
}

/********************
/* Identities for Key Format Structures */
/********************

/*** base key formats ****/

identity key-format-base {
    description "Base key-format identity for all keys.";
}

identity public-key-format {
    base "key-format-base";
    description "Base key-format identity for public keys.";
}

identity private-key-format {
    base "key-format-base";
    description "Base key-format identity for private keys.";
}

identity symmetric-key-format {
    base "key-format-base";
    description "Base key-format identity for symmetric keys.";
}

/**** for private keys ****/
identity rsa-private-key-format {
  base "private-key-format";
  description
    "Indicates that the private key value is encoded as an RSAPrivateKey (from RFC 3447).";
  reference
    "RFC 3447: PKCS #1: RSA Cryptography Specifications Version 2.2";
}

identity ec-private-key-format {
  base "private-key-format";
  description
    "Indicates that the private key value is encoded as an ECPrivateKey (from RFC 5915)";
  reference
    "RFC 5915: Elliptic Curve Private Key Structure";
}

identity one-asymmetric-key-format {
  if-feature "one-asymmetric-key-format";
  base "private-key-format";
  description
    "Indicates that the private key value is encoded as a OneAsymmetricKey structure (RFC 6031).";
    // FIXME: DER encoded ASN.1, etc...or flex PEM?
  reference
    "RFC 5958: Asymmetric Key Packages";
}

identity encrypted-one-asymmetric-key-format {
  if-feature "encrypted-one-asymmetric-key-format";
  base "private-key-format";
  description
    "Indicates that the private key value is encoded as a OneAsymmetricKey structure (RFC 5958).";
    // FIXME: DER encoded ASN.1, etc...or flex PEM?
  reference
    "RFC 5652: Cryptographic Message Syntax (CMS)
    RFC 5958: Asymmetric Key Packages";
}

/*** for public keys ****/

identity ssh-public-key-format {

"Indicates that the public key value is encoded as an SSH public key, as described by RFC 4716."
reference
"RFC 4716: The Secure Shell (SSH) Public Key File Format";
}

identity subject-public-key-info-format {
    base "public-key-format";
    description
        "Indicates that the public key value is encoded as a SubjectPublicKeyInfo structure, as described in RFC 5280.";
    // FIXME: DER encoded ASN.1, etc...
    reference
        "RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile";
}

/*** for symmetric keys ****/

identity octet-string-key-format {
    base "symmetric-key-format";
    description
        "Indicates that the key is encoded as a raw octet string.";
    // FIXME
    // Knowing that it is an "OctetString" isn't really helpful.
    // Knowing the length of the octet string would be helpful,
    // as it relates to the algorithm's block size. We may want
    // to only (for now) use "one-symmetric-key-format" for
    // symmetric keys...were the usability issues Juergen
    // mentioned before only apply to asymmetric keys?
}

identity one-symmetric-key-format {
    if-feature "one-symmetric-key-format";
    base "symmetric-key-format";
identity encrypted-one-symmetric-key-format {
  if-feature "encrypted-one-symmetric-key-format";
  base "symmetric-key-format";
  description
    "Indicates that the symmetric key value is encoded
    as an EncryptedData structure (RFC 5652) containing
    OneSymmetricKey (RFC 6031).";
  // FIXME: DER encoded ASN.1, etc...or flex PEM?
  reference
    "RFC 5652": Cryptographic Message Syntax (CMS)
    "RFC 6031": Cryptographic Message Syntax (CMS)
    Symmetric Key Package Content Type";
}

typedef x509 {
  type binary;
  description
    "A Certificate structure, as specified in RFC 5280,
    encoded using 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:
typedef crl {
    type binary;
    description
        "A CertificateList structure, as specified in RFC 5280,
        encoded using 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:"
}


Internet-Draft Common YANG Data Types for Cryptography November 2019

typedef cms {
    type binary;
    description
        "A ContentInfo structure, as specified in RFC 5652,
        encoded using ASN.1 distinguished encoding rules (DER),
        as specified in ITU-T X.690."
    reference
        "RFC 5652:
        Cryptographic Message Syntax (CMS)
        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).";
typedef data-content-cms {
    type cms;
    description
        "A CMS structure whose top-most content type MUST be the
data content type, as described by Section 4 in RFC 5652.";
    reference
        "RFC 5652: Cryptographic Message Syntax (CMS)";
}

typedef signed-data-cms {
    type cms;
    description
        "A CMS structure whose top-most content type MUST be the
signed-data content type, as described by Section 5 in
RFC 5652.";
    reference
        "RFC 5652: Cryptographic Message Syntax (CMS)";
}

typedef enveloped-data-cms {
    type cms;
    description
        "A CMS structure whose top-most content type MUST be the
enveloped-data content type, as described by Section 6
in RFC 5652.";
    reference
        "RFC 5652: Cryptographic Message Syntax (CMS)";
}

typedef digested-data-cms {
    type cms;
    description
        "A CMS structure whose top-most content type MUST be the
digested-data content type, as described by Section 7
in RFC 5652.";
    reference
        "RFC 5652: Cryptographic Message Syntax (CMS)";
}

typedef encrypted-data-cms {
type cms;
description
"A CMS structure whose top-most content type MUST be the encrypted-data content type, as described by Section 8 in RFC 5652.";
reference
"RFC 5652: Cryptographic Message Syntax (CMS);"
}
typedef authenticated-data-cms {
type cms;
description
"A CMS structure whose top-most content type MUST be the authenticated-data content type, as described by Section 9 in RFC 5652.";
reference
"RFC 5652: Cryptographic Message Syntax (CMS);"
}

/***************************************************/
/*   Typedefs for structures related to            */
/* RFC 4253                                       */
/***************************************************/
typedef ssh-host-key {
type binary;
description
"The binary public key data for an 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";
}

/***************************************************/
/*   Typedefs for ASN.1 structures related to      */
/* RFC 5280                                       */
/***************************************************/
typedef trust-anchor-cert-x509 {
  type x509;
  description
    "A Certificate structure that MUST encode a self-signed root certificate.";
}

typedef end-entity-cert-x509 {
  type x509;
  description
    "A Certificate structure that MUST encode a certificate that is neither self-signed nor having Basic constraint CA true.";
}

/*******************************************************************************/
/*   Typedefs for ASN.1 structures related to RFC 5652 */
/*******************************************************************************/

typedef trust-anchor-cert-cms {
  type signed-data-cms;
  description
    "A CMS SignedData structure that MUST contain the chain of X.509 certificates needed to authenticate the certificate presented by a client or end-entity.

    The CMS MUST contain only a single chain of certificates. The client or end-entity certificate MUST only authenticate to last intermediate CA certificate listed in the chain.

    In all cases, the chain MUST include a self-signed root certificate. In the case where the root certificate is itself the issuer of the client or end-entity certificate, only one certificate is present.

    This CMS structure MAY (as applicable where this type is used) also contain suitably fresh (as defined by local policy) revocation objects with which the device can verify the revocation status of the certificates.";
}
This CMS encodes the degenerate form of the SignedData structure that is commonly used to disseminate X.509 certificates and revocation objects (RFC 5280)."

reference
"RFC 5280:
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile."

}

typedef end-entity-cert-cms {
type signed-data-cms;
description
"A CMS SignedData structure that MUST contain the end entity certificate itself, and MAY contain any number of intermediate certificates leading up to a trust anchor certificate. The trust anchor certificate MAY be included as well.

The CMS MUST contain a single end entity certificate. The CMS MUST NOT contain any spurious certificates.

This CMS structure MAY (as applicable where this type is used) also contain suitably fresh (as defined by local policy) revocation objects with which the device can verify the revocation status of the certificates.

This CMS encodes the degenerate form of the SignedData structure that is commonly used to disseminate X.509 certificates and revocation objects (RFC 5280)."

reference
"RFC 5280:
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile."

}

typedef ssh-public-key-type { // DELETE?
type binary;
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.";
grouping symmetric-key-grouping {
  description "A symmetric key and algorithm.";
  leaf algorithm {
    type isa:symmetric-algorithm-type;
    mandatory true;
    description "The algorithm to be used when generating the key.";
    reference "RFC CCCC: Common YANG Data Types for Cryptography";
  }
  leaf key-format {
    nacm:default-deny-write;
    when "./key or ./encrypted-key"; // FIXME: forward ref?!
    type identityref {
      base symmetric-key-format;
    }
    description "Identifies the symmetric key's format.";
  }
  choice key-type {
    mandatory true;
    description "Choice between key types.";
    leaf key {
      nacm:default-deny-all;
      type binary;
      must "./key-format";
      description "The binary value of the key. The interpretation of
      the value is defined by 'key-format'. For example, FIXME.";
      reference "RFC XXXX: FIXME";
    }
    leaf hidden-key {
      nacm:default-deny-write;
      type empty;
      description
"A permanently hidden key. How such keys are created

is outside the scope of this module."

}
}
}

grouping public-key-grouping {
    description
        "A public key and its associated algorithm."
    leaf algorithm {
        nacm:default-deny-write;
        type iasa:asymmetric-algorithm-type;
        mandatory true;
        description
            "Identifies the key's algorithm."
        reference
            "RFC CCCC: Common YANG Data Types for Cryptography"
    }
    leaf public-key-format {
        nacm:default-deny-write;
        when ".../public-key"
        type identityref {
            base public-key-format;
        }
        description "Identifies the key's format."
    }
    leaf public-key {
        nacm:default-deny-write;
        type binary;
        must ".../public-key-format"
        mandatory true;
        description
            "The binary value of the public key. The interpretation
            of the value is defined by 'public-key-format' field."
    }
}

grouping asymmetric-key-pair-grouping {
    description
        "A private key and its associated public key and algorithm.";
    uses public-key-grouping;
leaf private-key-format {
    nacm:default-deny-write;
    when "../private-key or ../encrypted-private-key";
    // FIXME: forward ref?!
    type identityref {
        base private-key-format;
    }
    description "Identifies the key's format."
}

choice private-key-type {
    mandatory true;
    description
        "Choice between key types."
    leaf private-key {
        nacm:default-deny-all;
        type binary;
        must "../private-key-format";
        description
            "The value of the binary key. The key's value is
            interpreted by the 'private-key-format' field."
    }
    leaf hidden-private-key {
        nacm:default-deny-write;
        type empty;
        description
            "A permanently hidden key. How such keys are created
            is outside the scope of this module."
    }
}

grouping trust-anchor-cert-grouping {
    description
        "A trust anchor certificate, and a notification for when
        it is about to (or already has) expire."
    leaf cert {
        nacm:default-deny-write;
        type trust-anchor-cert-cms;
        description
            "The binary certificate data for this certificate."
        reference
}
notification certificate-expiration {
    description
        "A notification indicating that the configured certificate is either about to expire or has already expired. When to send notifications is an implementation specific decision, but it is RECOMMENDED that a notification be sent once a month for 3 months, then once a week for four weeks, and then once a day thereafter until the issue is resolved.";
    leaf expiration-date {
        type yang:date-and-time;
        mandatory true;
        description
            "Identifies the expiration date on the certificate.";
    }
}

grouping trust-anchor-certs-grouping {
    description
        "A list of trust anchor certificates, and a notification for when one is about to (or already has) expire.";
    leaf-list cert {
        nacm:default-deny-write;
        type trust-anchor-cert-cms;
        description
            "The binary certificate data for this certificate.";
        reference
            "RFC YYYY: Common YANG Data Types for Cryptography";
    }
}

notification certificate-expiration {
    description
        "A notification indicating that the configured certificate is either about to expire or has already expired. When to send notifications is an implementation specific decision, but it is RECOMMENDED that a notification be sent once a month for 3 months, then once a week for four weeks, and then once a day thereafter until the issue is resolved.";
    leaf expiration-date {
        type yang:date-and-time;
mandatory true;
description
  "Identifies the expiration date on the certificate."
};
}
}

grouping end-entity-cert-grouping {
description
  "An end entity certificate, and a notification for when
  it is about to (or already has) expire. Implementations
  SHOULD assert that, where used, the end entity certificate
  contains the expected public key."
leaf cert {
nacm:default-deny-write;
type end-entity-cert-cms;
description
  "The binary certificate data for this certificate."
reference
  "RFC YYYY: Common YANG Data Types for Cryptography"
}
notification certificate-expiration {

description
  "A notification indicating that the configured certificate
  is either about to expire or has already expired. When to
  send notifications is an implementation specific decision,
  but it is RECOMMENDED that a notification be sent once a
  month for 3 months, then once a week for four weeks, and
  then once a day thereafter until the issue is resolved."
leaf expiration-date {
type yang:date-and-time;
mandatory true;
description
  "Identifies the expiration date on the certificate."
}
}

grouping end-entity-certs-grouping {
description
  "A list of end entity certificates, and a notification for
when one is about to (or already has) expire.

leaf-list cert {
  nacm:default-deny-write;
  type end-entity-cert-cms;
  description
  "The binary certificate data for this certificate."
  reference
  "RFC YYYY: Common YANG Data Types for Cryptography"
}

notification certificate-expiration {
  description
  "A notification indicating that the configured certificate
  is either about to expire or has already expired. When to
  send notifications is an implementation specific decision,
  but it is RECOMMENDED that a notification be sent once a
  month for 3 months, then once a week for four weeks, and
  then once a day thereafter until the issue is resolved."
  leaf expiration-date {
    type yang:date-and-time;
    mandatory true;
    description
    "Identifies the expiration date on the certificate."
  }
}

grouping asymmetric-key-pair-with-cert-grouping {
  description
  "A private/public key pair and an associated certificate.

  Implementations SHOULD assert that certificates contain
  the matching public key."
  uses asymmetric-key-pair-grouping;
  uses end-entity-cert-grouping;
  action generate-certificate-signing-request {
    nacm:default-deny-all;
    description
    "Generates a certificate signing request structure for
    the associated asymmetric key using the passed subject
    and attribute values. The specified assertions need
    to be appropriate for the certificate's use. For
    example, an entity certificate for a TLS server
SHOULD have values that enable clients to satisfy
RFC 6125 processing.

input {
  leaf subject {
    type binary;
    mandatory true;
    description "The 'subject' field per the CertificationRequestInfo
    structure as specified by RFC 2986, Section 4.1
    encoded using the ASN.1 distinguished encoding
    rules (DER), as specified in ITU-T X.690.";
    reference "RFC 2986:
      PKCS #10: Certification Request Syntax
      Specification Version 1.7.
    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)."
  }
leaf attributes {
  type binary;
  description "The 'attributes' field from the structure
  CertificationRequestInfo as specified by RFC 2986,
  Section 4.1 encoded using the ASN.1 distinguished
  encoding rules (DER), as specified in ITU-T X.690.";
  reference "RFC 2986:
    PKCS #10: Certification Request Syntax
    Specification Version 1.7.
    ITU-T X.690:
    Information technology - ASN.1 encoding rules:
    Specification of Basic Encoding Rules (BER),
    Canonical Encoding Rules (CER) and Distinguished

output {
  leaf certificate-signing-request {
type binary;
mandatory true;
description
"A CertificationRequest structure as specified by
RFC 2986, Section 4.2 encoded using the ASN.1
distinguished encoding rules (DER), as specified
in ITU-T X.690."
reference
"RFC 2986:
   PKCS #10: Certification Request Syntax
   Specification Version 1.7.
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).";

// generate-certificate-signing-request
} // asymmetric-key-pair-with-cert-grouping

grouping asymmetric-key-pair-with-certs-grouping {
   description
   "A private/public key pair and associated certificates.
   Implementations SHOULD assert that certificates contain
   the matching public key.";
   uses asymmetric-key-pair-grouping;
   container certificates {
      nacm:default-deny-write;
      description
      "Certificates associated with this asymmetric key.
      More than one certificate supports, for instance,
      a TPM-protected asymmetric key that has both IDevID
      and LDevID certificates associated."
      list certificate {
         key "name";
         description
         "A certificate for this asymmetric key."
         leaf name {
            type string;
            description
            "An arbitrary name for the certificate. If the name
            matches the name of a certificate that exists
independently in <operational> (i.e., an IDevID), then the 'cert' node MUST NOT be configured.
}
uses end-entity-cert-grouping;
}
} // certificates
action generate-certificate-signing-request {
    nacm:default-deny-all;
    description "Generates a certificate signing request structure for the associated asymmetric key using the passed subject and attribute values. The specified assertions need to be appropriate for the certificate's use. For example, an entity certificate for a TLS server SHOULD have values that enable clients to satisfy RFC 6125 processing."
    input {
        leaf subject {
            type binary;
            mandatory true;
            description "The 'subject' field per the CertificationRequestInfo structure as specified by RFC 2986, Section 4.1 encoded using the ASN.1 distinguished encoding rules (DER), as specified in ITU-T X.690."
            reference "RFC 2986":
            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)."
        }
        leaf attributes {
            type binary;
            description "The 'attributes' field from the structure CertificationRequestInfo as specified by RFC 2986, Section 4.1 encoded using the ASN.1 distinguished encoding rules (DER), as specified in ITU-T X.690."
            reference "RFC 2986":
            ITU-T X.690:
                Information technology - ASN.1 encoding rules:
2.3. Examples

2.3.1. The "asymmetric-key-pair-with-certs-grouping" Grouping

The following example module illustrates the use of both the "symmetric-key-grouping" and the "asymmetric-key-pair-with-certs-grouping" groupings defined in the "ietf-crypto-types" module.

module ex-crypto-types-usage {
  yang-version 1.1;

output {
  leaf certificate-signing-request {
    type binary;
    mandatory true;
    description "A CertificationRequest structure as specified by [RFC 2986, Section 4.2] encoded using the ASN.1 distinguished encoding rules (DER), as specified in ITU-T X.690."
    reference "RFC 2986:
      PKCS #10: Certification Request Syntax
      Specification Version 1.7.
    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).";
  }
} // generate-certificate-signing-request
} // asymmetric-key-pair-with-certs-grouping

<CODE ENDS>
namespace "http://example.com/ns/example-crypto-types-usage";
prefix "ectu";

import ietf-crypto-types {
    prefix ct;
    reference
}

organization
"Example Corporation";

contact
"Author: YANG Designer <mailto:yang.designer@example.com>";

description
"This module illustrates the grouping defined in the crypto-types draft called 'asymmetric-key-pair-with-certs-grouping'.";

revision "1001-01-01" {
    description
    "Initial version";
    reference
    "RFC ?????: Usage Example for RFC XXXX";
}

container symmetric-keys {
    description
    "A container of symmetric keys.";
    list symmetric-key {
        key name;
        description
        "A symmetric key";
        leaf name {
            type string;
            description
            "An arbitrary name for this key.";
        }
        uses ct:symmetric-key-grouping;
    }
}
Given the above example usage module, the following example illustrates some configured keys.

```
<symmetric-keys
  xmlns="http://example.com/ns/example-crypto-types-usage"
  <symmetric-key>
    <name>ex-symmetric-key</name>
    <algorithm>aes-256-cbc</algorithm>
    <key-format>ct:octet-string-key-format</key-format>
    <key>base64encodedvalue==</key>
  </symmetric-key>
  <symmetric-key>
    <name>ex-hidden-symmetric-key</name>
    <algorithm>aes-256-cbc</algorithm>
    <hidden-key/>
  </symmetric-key>
</symmetric-keys>

<asymmetric-keys
  xmlns="http://example.com/ns/example-crypto-types-usage"
  <asymmetric-key>
2.3.2. The "generate-certificate-signing-request" Action

The following example illustrates the "generate-certificate-signing-request" action with the NETCONF protocol.

REQUEST
2.3.3. The "certificate-expiration" Notification

The following example illustrates the "certificate-expiration" notification with the NETCONF protocol.

<notification
 xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0"
 <eventTime>2018-05-25T00:01:00Z</eventTime>
 <keys xmlns="http://example.com/ns/example-crypto-types-usage">
   <key>
     <name>locally-defined key</name>
     <certificates>
       <certificate>
         <name>my-cert</name>
       </certificate>
     </certificates>
   </key>
 </keys>
</notification>
3. The Symmetric Algorithms Module

3.1. Tree Diagram

This section provides a tree diagram [RFC8340] for the "iana-symmetric-algs" module. Only the "container" statement is represented, as tree diagrams have no means to represent "typedef" statements.

module: iana-symmetric-algs
  +--ro supported-symmetric-algorithms
    +--ro supported-symmetric-algorithm* [algorithm]
      +--ro algorithm symmetric-algorithm-type

3.2. YANG Module

This module has normative references to FIXME...

<CODE BEGINS> file "iana-symmetric-algs@2019-11-20.yang"

module iana-symmetric-algs {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:iana-symmetric-algs";

  prefix isa;

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

  contact
    "WG Web:  <http://datatracker.ietf.org/wg/netconf/>"
This module defines a typedef for symmetric algorithms, and a container for a list of symmetric algorithms supported by the server.

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 (https://trustee.ietf.org/license-info).

This version of this YANG module is part of RFC XXXX (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself for full legal notices.

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 (RFC 2119) (RFC 8174) when, and only when, they appear in all capitals, as shown here.

revision 2019-11-20 {
  description
    "Initial version";
  reference
    "RFC XXXX: Common YANG Data Types for Cryptography";
}

// Typedefs

typedef symmetric-algorithm-type {
  type enumeration {
    enum aes-128-cbc {


value 1;
  description
    "Encrypt message with AES algorithm in CBC mode with
    a key length of 128 bits."
  reference
    "RFC 3565: Use of the Advanced Encryption Standard (AES)
    Encryption Algorithm in Cryptographic Message Syntax
    (CMS)"
};

enum aes-192-cbc {
  value 2;
  description
    "Encrypt message with AES algorithm in CBC mode with
    a key length of 192 bits"
  reference
    "RFC 3565: Use of the Advanced Encryption Standard (AES)
    Encryption Algorithm in Cryptographic Message Syntax
    (CMS)"
};

enum aes-256-cbc {
  value 3;
  description
    "Encrypt message with AES algorithm in CBC mode with
    a key length of 256 bits"
  reference
    "RFC 3565: Use of the Advanced Encryption Standard (AES)
    Encryption Algorithm in Cryptographic Message Syntax
    (CMS)"
};

enum aes-128-ctr {
  value 4;
  description
    "Encrypt message with AES algorithm in CTR mode with
    a key length of 128 bits"
  reference
    "RFC 3686: Using Advanced Encryption Standard (AES) Counter
    Mode with IPsec Encapsulating Security Payload (ESP)"
};

enum aes-192-ctr {
  value 5;
  description
    "Encrypt message with AES algorithm in CTR mode with
    a key length of 192 bits"
  reference
    "RFC 3686: Using Advanced Encryption Standard (AES) Counter
Mode with IPsec Encapsulating Security Payload (ESP);

} enum aes-256-ctr {
    value 6;
    description
        "Encrypt message with AES algorithm in CTR mode with a key length of 256 bits";
    reference
        "RFC_3686:
        Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP)";
}

enum des3-cbc-sha1-kd {
    value 7;
    description
        "Encrypt message with 3DES algorithm in CBC mode with sha1 function for key derivation";
    reference
        "RFC_3961:
        Encryption and Checksum Specifications for Kerberos 5";
}

enum rc4-hmac {
    value 8;
    description
        "Encrypt message with rc4 algorithm";
    reference
        "RFC_4757:
        The RC4-HMAC Kerberos Encryption Types Used by Microsoft Windows";
}

enum rc4-hmac-exp {
    value 9;
    description
        "Encrypt message with rc4 algorithm that is exportable";
    reference
        "RFC_4757:
        The RC4-HMAC Kerberos Encryption Types Used by Microsoft Windows";
}
}
description
   "A typedef enumerating various symmetric key algorithms."
}

// Protocol-accessible Nodes

<CODE ENDS>

3.3. Examples

The following example illustrates the "supported-symmetric-algorithms" "container" statement with the NETCONF protocol.

<supported-symmetric-algorithms
   xmlns="urn:ietf:params:xml:ns:yang:iana-symmetric-algs">
   <supported-symmetric-algorithm>
      <algorithm>aes-128-cbc</algorithm>
   </supported-symmetric-algorithm>
   <supported-symmetric-algorithm>
      <algorithm>aes-256-cbc</algorithm>
   </supported-symmetric-algorithm>
</supported-symmetric-algorithms>
4. The Asymmetric Algorithms Module

4.1. Tree Diagram

This section provides a tree diagram [RFC8340] for the "iana-asymmetric-algs" module. Only the "container" statement is represented, as tree diagrams have no means to represent "typedef" statements.

4.2. YANG Module

This module has normative references to FIXME...

<CODE BEGINS> file "iana-asymmetric-algs@2019-11-20.yang"

module iana-asymmetric-algs {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:iana-asymmetric-algs";
  prefix iasa;

  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:  Wang Haiguang <wang.haiguang.shieldlab@huawei.com>";

  description
    "This module defines a typedef for asymmetric algorithms, and
     a container for a list of asymmetric algorithms supported by
     the server."
typedef asymmetric-algorithm-type {
    type enumeration {
        enum rsa1024 {
            value 1;
            description "The RSA algorithm using a 1024-bit key.";
            reference "RFC 8017: PKCS #1: RSA Cryptography Specifications Version 2.2.";
        }
        enum rsa2048 {  
            value 2;
            description "The RSA algorithm using a 2048-bit key.";
            reference "RFC 8017: PKCS #1: RSA Cryptography Specifications Version 2.2.";
        }
    }
}

value 2;

description
"The RSA algorithm using a 2048-bit key.";

reference
"RFC 8017:
   PKCS #1: RSA Cryptography Specifications Version 2.2.";
}

enum rsa3072 {
    value 3;

description
"The RSA algorithm using a 3072-bit key.";

reference
"RFC 8017:
   PKCS #1: RSA Cryptography Specifications Version 2.2.";
}

enum rsa4096 {
    value 4;

description
"The RSA algorithm using a 4096-bit key.";

reference
"RFC 8017:
   PKCS #1: RSA Cryptography Specifications Version 2.2.";
}

enum rsa7680 {
    value 5;

description
"The RSA algorithm using a 7680-bit key.";

reference
"RFC 8017:
   PKCS #1: RSA Cryptography Specifications Version 2.2.";
}

enum rsa15360 {
    value 6;

description
"The RSA algorithm using a 15360-bit key.";

reference
"RFC 8017:
   PKCS #1: RSA Cryptography Specifications Version 2.2.";
}

enum secp192r1 {
    value 7;

description
  "The asymmetric algorithm using a NIST P192 Curve.";
reference
  "RFC 6090:
  Fundamental Elliptic Curve Cryptography Algorithms.
  RFC 5480:
  Elliptic Curve Cryptography Subject Public Key Information.";
}
enum secp224r1 {
  value 8;
  description
  "The asymmetric algorithm using a NIST P224 Curve.";
  reference
  "RFC 6090:
  Fundamental Elliptic Curve Cryptography Algorithms.
  RFC 5480:
  Elliptic Curve Cryptography Subject Public Key Information.";
}
enum secp256r1 {
  value 9;
  description
  "The asymmetric algorithm using a NIST P256 Curve.";
  reference
  "RFC 6090:
  Fundamental Elliptic Curve Cryptography Algorithms.
  RFC 5480:
  Elliptic Curve Cryptography Subject Public Key Information.";
}
enum secp384r1 {
  value 10;
  description
  "The asymmetric algorithm using a NIST P384 Curve.";
  reference
  "RFC 6090:
  Fundamental Elliptic Curve Cryptography Algorithms.
  RFC 5480:
  Elliptic Curve Cryptography Subject Public Key Information.";
} enum secp521r1 {
    value 11;
    description
        "The asymmetric algorithm using a NIST P521 Curve."
    reference
        "RFC 6090:
         Fundamental Elliptic Curve Cryptography Algorithms.
RFC 5480:
         Elliptic Curve Cryptography Subject Public Key
         Information.";
}
enum x25519 {
    value 12;
    description
        "The asymmetric algorithm using a x.25519 Curve."
    reference
        "RFC 7748:
         Elliptic Curves for Security.";
}
enum x448 {
    value 13;
    description
        "The asymmetric algorithm using a x.448 Curve."
    reference
        "RFC 7748:
         Elliptic Curves for Security.";
}
}
description
    "A typedef enumerating various asymmetric key algorithms.";
}

// Protocol-accessible Nodes

container supported-asymmetric-algorithms {
    config false;
    description
        "A container for a list of supported asymmetric algorithms.
        How algorithms come to be supported is outside the scope
4.3.  Examples

The following example illustrates the "supported-asymmetric-algorithms" "container" statement with the NETCONF protocol.

```xml
<supported-asymmetric-algorithms
  xmlns="urn:ietf:params:xml:ns:yang:iana-asymmetric-algs">
  <supported-asymmetric-algorithm>
    <algorithm>rsa2048</algorithm>
  </supported-asymmetric-algorithm>
  <supported-asymmetric-algorithm>
    <algorithm>secp256r1</algorithm>
  </supported-asymmetric-algorithm>
</supported-asymmetric-algorithms>
```

5.  The Hash Algorithms Module

5.1.  Tree Diagram

This section provides a tree diagram [RFC8340] for the "iana-hash-algs" module. Only the "container" statement is represented, as tree diagrams have no means to represent "typedef" statements.

```
module: iana-hash-algs
  +--ro supported-hash-algorithms
    +--ro supported-hash-algorithm* [algorithm]
      +--ro algorithm   hash-algorithm-type
```
5.2. YANG Module

This module has normative references to FIXME...

<CODE BEGINS> file "iana-hash-algs@2019-11-20.yang"

module iana-hash-algs {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:iana-hash-algs";
  prefix iha;

  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: Wang Haiguang <wang.haiguang.shieldlab@huawei.com>"

  description
    "This module defines a typedef for hash algorithms, and
    a container for a list of hash algorithms supported by
    the server.

    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

    This version of this YANG module is part of RFC XXXX
    (https://www.rfc-editor.org/info/rfcXXXX); see the RFC
    itself for full legal notices.

    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 (RFC 2119)
    (RFC 8174) when, and only when, they appear in all
    capitals, as shown here."

  revision 2019-11-20 {
typedef hash-algorithm-type {
    type enumeration {
        enum sha1 {
            value 1;
            status obsolete;
            description "The SHA1 algorithm.";
            reference "RFC 3174: US Secure Hash Algorithms 1 (SHA1).";
        }
        enum sha-224 {
            value 2;
            description "The SHA-224 algorithm.";
            reference "RFC 6234: US Secure Hash Algorithms.";
        }
        enum sha-256 {
            value 3;
            description "The SHA-256 algorithm.";
            reference "RFC 6234: US Secure Hash Algorithms.";
        }
        enum sha-384 {
            value 4;
            description "The SHA-384 algorithm.";
            reference "RFC 6234: US Secure Hash Algorithms.";
        }
        enum sha-512 {
            value 5;
        }
    }
}
enum shake-128 {
  value 6;
  description
    "The SHA3 algorithm with 128-bits output.";
  reference
    "RFC 6234: US Secure Hash Algorithms.";
}

enum shake-224 {
  value 7;
  description
    "The SHA3 algorithm with 224-bits output.";
  reference
    "National Institute of Standards and Technology, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, DOI 10.6028/NIST.FIPS.202, August 2015.";
}

enum shake-256 {
  value 8;
  description
    "The SHA3 algorithm with 256-bits output.";
  reference
    "National Institute of Standards and Technology, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, DOI 10.6028/NIST.FIPS.202, August 2015.";
}

enum shake-384 {
  value 9;
  description
    "The SHA3 algorithm with 384-bits output.";
  reference
    "National Institute of Standards and Technology,
enum shake-512 {
  value 10;
  description
    "The SHA3 algorithm with 384-bits output.";
  reference
    "National Institute of Standards and Technology,
    SHA-3 Standard: Permutation-Based Hash and
    Extendable-Output Functions, FIPS PUB 202, DOI
    10.6028/NIST.FIPS.202, August 2015.";
}

A typedef enumerating various hash key algorithms.

// Protocol-accessible Nodes

container supported-hash-algorithms {
  config false;
  description
    "A container for a list of supported hash algorithms. How algorithms come to be supported is outside the scope of this module.";
  list supported-hash-algorithm {
    key algorithm;
    description
      "A lists of hash algorithms supported by the server.";
    leaf algorithm {
      type hash-algorithm-type;
      description
        "An hash algorithms supported by the server.";
    }
  }
}
5.3. Examples

The following example illustrates the "supported-hash-algorithms" "container" statement with the NETCONF protocol.

```xml
<supported-hash-algorithms
  xmlns="urn:ietf:params:xml:ns:yang:iana-hash-algs">
  <supported-hash-algorithm>
    <algorithm>sha-256</algorithm>
  </supported-hash-algorithm>
  <supported-hash-algorithm>
    <algorithm>sha-512</algorithm>
  </supported-hash-algorithm>
</supported-hash-algorithms>
```

6. Security Considerations

6.1. Support for Algorithms

In order to use YANG identities for algorithm identifiers, only the most commonly used RSA key lengths are supported for the RSA algorithm. Additional key lengths can be defined in another module or added into a future version of this document.

This document limits the number of elliptical curves supported. This was done to match industry trends and IETF best practice (e.g., matching work being done in TLS 1.3). If additional algorithms are needed, they can be defined by another module or added into a future version of this document.

6.2. No Support for CRMF

This document uses PKCS #10 [RFC2986] for the "generate-certificate-signing-request" action. The use of Certificate Request Message Format (CRMF) [RFC4211] was considered, but it was unclear if there
was market demand for it. If it is desired to support CRMF in the future, a backwards compatible solution can be defined at that time.

6.3. Access to Data Nodes

The YANG module in this document defines "grouping" statements that 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 module in this document only define groupings, these considerations are primarily for the designers of other modules that use these groupings.

There are a number of data nodes defined by the grouping statements that are writable/creatable/deletable (i.e., config true, which is the default). Some of 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:

*: All of the data nodes defined by all the groupings are considered sensitive to write operations. For instance, the modification of a public key or a certificate can dramatically alter the implemented security policy. For this reason, the NACM extension "default-deny-write" has been applied to all the data nodes defined by all the groupings.

Some of the readable data nodes in the YANG module 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:

/private-key: The "private-key" node defined in the "asymmetric-
key-pair-grouping" grouping is additionally sensitive to read operations such that, in normal use cases, it should never be returned to a client. For this reason, the NACM extension "default-deny-all" has been applied to it here.

Some of the 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:

*: All of the "action" statements defined by groupings SHOULD only be executed by authorized users. For this reason, the NACM extension "default-deny-all" has been applied to all of them. Note that NACM uses "default-deny-all" to protect "RPC" and "action" statements; it does not define, e.g., an extension called "default-deny-execute".

generate-certificate-signing-request: For this action, it is RECOMMENDED that implementations assert channel binding [RFC5056], so as to ensure that the application layer that sent the request is the same as the device authenticated when the secure transport layer was established.

7. IANA Considerations

7.1. The IETF XML Registry

This document registers four URIs in the "ns" subregistry of the IETF XML Registry [RFC3688]. Following the format in [RFC3688], the following registrations are requested:
Registrant Contact: The NETCONF WG of the IETF.
XML: N/A, the requested URI is an XML namespace.

Registrant Contact: The NETCONF WG of the IETF.
XML: N/A, the requested URI is an XML namespace.

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 four YANG modules in the YANG Module Names registry [RFC6020]. Following the format in [RFC6020], the the following registrations are requested:

name:       ietf-crypto-types
prefix:     ct
reference:  RFC XXXX

name:       iana-symmetric-algs
prefix:     isa
reference:  RFC XXXX

name:       iana-asymmetric-algs
prefix:     iasa
reference:  RFC XXXX

name:       iana-hash-algs
prefix:     iha
reference:  RFC XXXX

8. References
8.1. Normative References


Internet-Draft  Common YANG Data Types for Cryptography  November 2019


8.2. Informative References


Appendix A. Change Log

A.1. I-D to 00

- Removed groupings and notifications.
- Added typedefs for identityrefs.
- Added typedefs for other RFC 5280 structures.
- Added typedefs for other RFC 5652 structures.
o Added convenience typedefs for RFC 4253, RFC 5280, and RFC 5652.

A.2. 00 to 01

o Moved groupings from the draft-ietf-netconf-keystore here.

A.3. 01 to 02

o Removed unwanted "mandatory" and "must" statements.

o Added many new crypto algorithms (thanks Haiguang!)

o Clarified in asymmetric-key-pair-with-certs-grouping, in certificates/certificate/name/description, that if the name MUST NOT match the name of a certificate that exists independently in <operational>, enabling certs installed by the manufacturer (e.g., an IDevID).

A.4. 02 to 03

o renamed base identity 'asymmetric-key-encryption-algorithm' to 'asymmetric-key-algorithm'.

o added new 'asymmetric-key-algorithm' identities for secp192r1, secp224r1, secp256r1, secp384r1, and secp521r1.


o for all -cbc and -ctr identities, renamed base identity 'symmetric-key-encryption-algorithm' to 'encryption-algorithm'.

o for all -ccm and -gcm identities, renamed base identity 'symmetric-key-encryption-algorithm' to 'encryption-and-mac-algorithm' and renamed the identity to remove the "enc-" prefix.

o for all the 'signature-algorithm' based identities, renamed from 'rsa-*' to 'rsassa-*'.

o removed all of the "x509v3-" prefixed 'signature-algorithm' based identities.
o added 'key-exchange-algorithm' based identities for 'rsaes-oaep' and 'rsaes-pkcs1-v1_5'.

o renamed typedef 'symmetric-key-encryption-algorithm-ref' to 'symmetric-key-algorithm-ref'.

o renamed typedef 'asymmetric-key-encryption-algorithm-ref' to 'asymmetric-key-algorithm-ref'.

o added typedef 'encryption-and-mac-algorithm-ref'.

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

A.5. 03 to 04

o ran YANG module through formatter.

A.6. 04 to 05

o fixed broken symlink causing reformatted YANG module to not show.

A.7. 05 to 06

o Added NACM annotations.

o Updated Security Considerations section.

o Added 'asymmetric-key-pair-with-cert-grouping' grouping.

o Removed text from 'permanently-hidden' enum regarding such keys not being backed up or restored.

o Updated the boilerplate text in module-level "description" statement to match copyeditor convention.

o Added an explanation to the 'public-key-grouping' and 'asymmetric-key-pair-grouping' statements as for why the nodes are not mandatory (e.g., because they may exist only in <operational>).
o Added 'must' expressions to the 'public-key-grouping' and 'asymmetric-key-pair-grouping' statements ensuring sibling nodes are either all exist or do not all exist.

o Added an explanation to the 'permanently-hidden' that the value cannot be configured directly by clients and servers MUST fail any attempt to do so.

o Added 'trust-anchor-certs-grouping' and 'end-entity-certs-grouping' (the plural form of existing groupings).

o Now states that keys created in <operational> by the *-hidden-key actions are bound to the lifetime of the parent 'config true' node, and that subsequent invocations of either action results in a failure.

A.8. 06 to 07

o Added clarifications that implementations SHOULD assert that configured certificates contain the matching public key.

o Replaced the 'generate-hidden-key' and 'install-hidden-key' actions with special 'crypt-hash' -like input/output values.

A.9. 07 to 08

o Removed the 'generate-key and 'hidden-key' features.

o Added grouping symmetric-key-grouping

o Modified 'asymmetric-key-pair-grouping' to have a 'choice' statement for the keystone module to augment into, as well as replacing the 'union' with leafs (having different NACM settings).

A.10. 08 to 09

o Converting algorithm from identities to enumerations.

A.11. 09 to 10

o All of the below changes are to the algorithm enumerations defined in ietf-crypto-types.

o Add in support for key exchange over x.25519 and x.448 based on RFC 8418.

o Add in SHAKE-128, SHAKE-224, SHAKE-256, SHAKE-384 and SHAKE 512
Revise/add in enum of signature algorithm for x25519 and x448

Add in des3-cbc-sha1 for IPSec

Add in sha1-des3-kd for IPSec

Add in definit for rc4-hmac and rc4-hmac-exp. These two algorithms have been deprecated in RFC 8429. But some existing draft in i2nsf may still want to use them.

Add x25519 and x448 curve for asymmetric algorithms

Add signature algorithms ed25519, ed25519-cts, ed25519ph

Add signature algorithms ed448, ed448ph

Add in rsa-sha2-256 and rsa-sha2-512 for SSH protocols (rfc8332)

**A.12.** 10 to 11

- Added a "key-format" identity.

- Added symmetric keys to the example in Section 2.3.

**A.13.** 11 to 12

- Removed all non-essential (to NC/RC) algorithm types.

- Moved remaining algorithm types each into its own module.

- Added a 'config false' "algorithms-supported" list to each of the algorithm-type modules.

**A.14.** 12 to 13

- Added the four features: "[encrypted-]one-[a]symmetric-key-format", each protecting a 'key-format' identity of the same name.

- Added 'must' expressions asserting that the 'key-format' leaf exists whenever a non-hidden key is specified.

- Improved the 'description' statements and added 'reference'
statements for the 'key-format' identities.

- Added a questionable forward reference to "encrypted-*" leafs in a couple 'when' expressions.
- Did NOT move "config false" alg-supported lists to SSH/TLS drafts.

Acknowledgements

The authors would like to thank for following for lively discussions on list and in the halls (ordered by last name): Martin Bjorklund, Nick Hancock, Balazs Kovacs, Juergen Schoenwaelder, Eric Voit, and Liang Xia.

Authors' Addresses

Kent Watsen
Watsen Networks

EMail: kent+ietf@watsen.net

Wang Haiguang
Huawei

EMail: wang.haiguang.shieldlab@huawei.com