Internet Engineering Task Force (IETF)
Request for Comments: 8177
Category: Standards Track
ISSN: 2070-1721

A. Lindem, Ed.
Cisco Systems
Y. Qu
Huawei
D. Yeung
Arrcus, Inc
I. Chen
Jabil
J. Zhang
Juniper Networks

June 2017

YANG Data Model for Key Chains

Модель данных YANG для цепочек ключей

Аннотация

Этот документ описывает модель данных YANG для цепочек ключей. Такие цепочки широко применяются для аутентификации протоколов маршрутизации и в других приложениях, требующих симметричных ключей. Цепочка ключей - это список из одного или нескольких элементов, содержащих Key ID, строку ключа, сроки действия для отправки и восприятия, связанный алгоритм проверки подлинности и шифрования. За счёт подобающего перекрытия сроков действия для отправки и восприятия нескольких элементов цепочки ключей строки ключей и алгоритмы можно аккуратно обновлять. Представление в модели данных YANG позволяет автоматизировать распространение ключей.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке http://www.rfc-editor.org/info/rfc8177.

Оглавление

[1] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Этот документ описывает модель данных YANG [YANG-1.1] для цепочек ключей. Цепочки широко применяются для аутентификации в протоколах маршрутизации, а также в других приложениях, которым нужны симметричные ключи. Цепочка ключей - это список из одного или нескольких элементов, содержащих Key ID, строку ключа, сроки действия для отправки и восприятия, связанный алгоритм проверки подлинности и шифрования. За счёт подобающего перекрытия сроков действия для отправки и восприятия нескольких элементов цепочки ключей строки ключей и алгоритмы можно аккуратно обновлять. Представление в модели данных YANG позволяет автоматизировать распространение ключей.

В некоторых приложениях протоколы не используют напрямую элементы цепочки ключей, а применяют функцию вывода ключей для создания краткосрочного ключа из элементов цепочки (например, первичные ключи в [TCP-AO]).

1.1. Уровни требований

Ключевые слова **должно** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [KEYWORDS] [KEYWORDS-UPD] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

1.2. Диаграммы деревьев

Упрощённое графическое представление полного дерева данных дано в параграфе 3.3 с использованием приведённых ниже обозначений.

- Квадратные скобки [и] содержат в себе ключи. Их не следует путать с ключами цепочек.
- Фигурные скобки { и } содержат имена необязательных функций, делающие соответствующий узел условным.
- В сокращениях перед именами узлов rw указывает данные конфигурации (read-write), ro - данные состояния (read-only), -x - операции RPC или действия, -n - уведомления.
- После имени узла символ ? Указывает необязательный узел, ! - контейнер с присутствием, * - list или leaf-list.
- Круглые скобки включают узлы choice и case, а узлы case помечаются также двоеточием (:).
- Три точки (…) указывают пропущенное содержимое субдерева (ветви).

2. Постановка задачи

Этот документ описывает модель данных YANG [YANG-1.1] для цепочек ключей. Цепочки ключей реализованы и развёрнуты большинством производителей сетевого оборудования. Создание стандартной модели YANG будет способствовать автоматическому распространению ключей и их неразрушающей смене (rollover). Это поможет улучшить защищенность инфраструктуры ядра маршрутизации в соответствии с рекомендациями [IAB-REPORT].

Цепочка ключей - это список из одного или нескольких элементов, содержащих Key ID, строку ключа, сроки действия для отправки и восприятия, связанный алгоритм проверки подлинности и шифрования. Цепочка может применяться любой службой или приложением, где нужна проверка подлинности или шифрование с симметричными ключами. По сути, цепочка ключей является многократно применяемой политикой , на которую можно указывать при возникновении необходимости. Цепочки ключей были реализованы большинством производителей сетевого оборудования и развёрнуты во многих сетях.

Концептуальное представление таблицы криптоключей описано в [CRYPTO-KEYTABLE]. Таблица включает ключи со сроками их действия и алгоритмами. Кроме того, в таблицу включается критерий выбора и она предназначена для модели развёртывания, где сведения о приложениях и службах, требующих аутентификации или шифрования, проникают в базу данных о ключах. Модель YANG для цепочки ключей, описанная здесь, не включает критериев выбора и не поддерживает эту модель развёртывания. Однако модель и не исключает этого. В [YANG-CRYPTO-KEYTABLE] описаны дополнения к модели YANG для цепочки ключей в поддержку критериев выбора.

2.1. Применимость

Другие модули YANG могут ссылаться на имена цепочек в модуле YANG ietf-key-chain для приложений аутентификации и шифрования. Предоставлен тип YANG для упрощения ссылок на имя цепочки ключей без указания полного выражения YANG XPath[1].

2.2. Аккуратная смена ключей с использованием цепочек

Цепочки ключей могут служить для аккуратного обновления строки ключа и/или алгоритма, используемых приложением для аутентификации или шифрования. Для аккуратной смены ключа получатель **может** воспринимать любые ключи с пригодным сроком действия, а отправитель **может** передавать ключ с последним (свежим) сроком действия. Один из вариантов смены ключа описан ниже.

1. Цепочка с новым ключом распространяется всем маршрутизаторам и другим сетевым устройствам в домене этой цепочки. Срок восприятия нового ключа следует устанавливать так, чтобы ключ был пригоден в период смены ключа (rollover). Срок действия для передачи следует устанавливать в будущем, чтобы обеспечить обновление ключей на всех маршрутизаторах домена. Он не оказывает непосредственного влияния на передаваемые ключи.
2. Проверяется получение новой цепочки всеми сетевыми устройствами и примерная синхронизация их часов. Системные часы устройств в административном домене обычно синхронизированы, например, по протоколу сетевого времени (Network Time Protocol или NTP) [NTP-PROTO]). Эту процедуру можно автоматизировать.

[1] XML Path Language - язык путей XML.

3. Когда срок передачи нового ключа станет действительным, сетевые устройства использующего цепочку домена будут использовать этот новый ключ для передачи.

4. В некий будущий момент в домене может быть распространена новая цепочка с удаленным старым ключом, однако эту процедуру можно отложить до следующего обновления ключа. В этом случае цепочка ключей всегда будет содержать два ключа - текущий и будущий (в процессе обновления) или текущий и предыдущий (между обновлениями).

Поскольку последний (свежий) срок действия ключа для передачи определён как срок действия ключа с самым поздним началом применения (start-time), указание срока действия «всегда» (always) будет мешать описанному выше методу смены ключей. Возможны иные конфигурации и варианты использования ключей, но это выходит за рамки документа.

3. Устройство модели для цепочек ключей

Модуль ietf-key-chain содержит список из одного или нескольких ключей с индексом Key ID. Для некоторых приложений (например, OSPFv3 [OSPFV3-AUTH]) Key ID применяется для указания используемой цепочки ключей. Кроме Key ID каждый ключ включает строку ключа и криптографический алгоритм, а также может включать срок действия для передачи и восприятия ключа (по умолчанию ключи действительны всегда).

Отметим, что разные сроки действия для передачи и восприятия могут указываться в разных элементах. Ключ для передачи может иметь действительное значение send-lifetime и непригодное значение accept-lifetime (например, end-time = start-time). Ключ, применяемый для восприятия может иметь действительное значение accept-lifetime и непригодное значение send-lifetime.

Из-за различий в реализации цепочек ключей у разных производителей некоторые элементы данных являются необязательными. Идентификаторы криптоалгоритмов предоставляются для многократного использования при настройке унаследованной аутентификации и шифрования без цепочек ключей.

Цепочка ключей указывается уникальным в масштабе сетевого устройства именем. Другим модулям **следует** применять определение типа (typedef) из key-chain-ref при необходимости указать настроенную цепочку ключей.

3.1. Рабочее состояние цепочки ключей

Рабочее состояние ключей включено в одно дерево с конфигурацией цепочки, соответствующее архитектуре NMDA [NMDA]. В рабочем состоянии поддерживается временная метка последнего изменения цепочки ключей, а также пригодность цепочки для передачи и восприятия.

3.2. Свойства модели

Для обработки различий между реализациями разных производителей используются операторы feature. Например, не все производители поддерживают настройку допустимого отклонения при восприятии или шестнадцатеричные строки для ключей. Свойства (feature) также применяются для поддержки требований безопасности (например, алгоритмов TCP-AO [TCP-AO-ALGORITHMS]), ещё не реализованных производителями или реализованных только одним из них.

Обычно элемент с достаточными правами может читать и сохранять конфигурацию устройства, включающую содержимое этой модели. Для предотвращения ненужного просмотра и хранения ключей в открытом виде (cleartext) модель поддерживает функцию (feature) aes-key-wrap (см. 5. Вопросы безопасности).

3.3. Дерево модели для цепочки ключей

```
+--rw key-chains
   +--rw key-chain* [name]
      |  +--rw name                        string
      |  +--rw description?                string
      |  +--rw accept-tolerance {accept-tolerance}?
      |  |  +--rw duration?   uint32
      |  +--ro last-modified-timestamp?   yang:date-and-time
      |  +--rw key* [key-id]
      |     +--rw key-id                     uint64
      |     +--rw lifetime
      |     |  +--rw (lifetime)?
      |     |     +--:(send-and-accept-lifetime)
      |     |     |  +--rw send-accept-lifetime
      |     |     |     +--rw (lifetime)?
      |     |     |        +--:(always)
      |     |     |        |  +--rw always?            empty
      |     |     |        +--:(start-end-time)
      |     |     |           +--rw start-date-time?
      |     |     |           |       yang:date-and-time
      |     |     |           +--rw (end-time)?
      |     |     |              +--:(infinite)
      |     |     |              |  +--rw no-end-time?       empty
      |     |     |              +--:(duration)
      |     |     |              |  +--rw duration?          uint32
      |     |     |              +--:(end-date-time)
      |     |     |                 +--rw end-date-time?
      |     |     |                         yang:date-and-time
      |     |     +--:(independent-send-accept-lifetime)
      |     |        |   {independent-send-accept-lifetime}?
      |     |        +--rw send-lifetime
      |     |        |  +--rw (lifetime)?
      |     |        |     +--:(always)
      |     |        |     |  +--rw always?            empty
```

```
      |      |         |     +--:(start-end-time)
      |      |         |        +--rw start-date-time?
      |      |         |        |       yang:date-and-time
      |      |         |        +--rw (end-time)?
      |      |         |           +--:(infinite)
      |      |         |           |  +--rw no-end-time?       empty
      |      |         |           +--:(duration)
      |      |         |           |  +--rw duration?          uint32
      |      |         |           +--:(end-date-time)
      |      |         |              +--rw end-date-time?
      |      |         |                      yang:date-and-time
      |      |         +--rw accept-lifetime
      |      |            +--rw (lifetime)?
      |      |               +--:(always)
      |      |               |  +--rw always?            empty
      |      |               +--:(start-end-time)
      |      |                  +--rw start-date-time?
      |      |                  |       yang:date-and-time
      |      |                  +--rw (end-time)?
      |      |                     +--:(infinite)
      |      |                     |  +--rw no-end-time?       empty
      |      |                     +--:(duration)
      |      |                     |  +--rw duration?          uint32
      |      |                     +--:(end-date-time)
      |      |                        +--rw end-date-time?
      |      |                                yang:date-and-time
      |      +--rw crypto-algorithm identityref
      |      +--rw key-string
      |      |  +--rw (key-string-style)?
      |      |     +--:(keystring)
      |      |     |  +--rw keystring?            string
      |      |     +--:(hexadecimal) {hex-key-string}?
      |      |        +--rw hexadecimal-string?   yang:hex-string
      |      +--ro send-lifetime-active?     boolean
      |      +--ro accept-lifetime-active?   boolean
      +--rw aes-key-wrap {aes-key-wrap}?
         +--rw enable?   boolean
```

4. Модель YANG Key Chain

```
<CODE BEGINS> file "ietf-key-chain@2017-06-15.yang"
module ietf-key-chain {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-key-chain";
  prefix key-chain;

  import ietf-yang-types {
    prefix yang;
  }
  import ietf-netconf-acm {
    prefix nacm;
  }

  organization
    "IETF RTGWG - Routing Area Working Group";
  contact
    "WG Web:   <https://datatracker.ietf.org/group/rtgwg>
     WG List:  <mailto:rtgwg@ietf.org>

     Editor: Acee Lindem
             <mailto:acee@cisco.com>
             Yingzhen Qu
             <mailto:yingzhen.qu@huawei.com>
             Derek Yeung
             <mailto:derek@arrcus.com>
             Ing-Wher Chen
             <mailto:Ing-Wher_Chen@jabail.com>
             Jeffrey Zhang
             <mailto:zzhang@juniper.net>";

  description
    "Этот модуль YANG задаёт базовые данные конфигурации для
     цепочек ключей. Предполагается, что производители будут
     расширять модуль своими параметрами цепочек ключей.

     Авторские права (Copyright (c) 2017) принадлежат IETF Trust и
     лицам, указанным как авторы. Все права защищены.

     Распространение и применение модуля в исходной или двоичной
     форме с изменениями или без таковых разрешено в соответствии с
     лицензией Simplified BSD License, изложенной в параграфе 4.c
     IETF Trust's Legal Provisions Relating to IETF Documents
     (https://trustee.ietf.org/license-info).

     Эта версия модуля YANG является частью RFC 8177, где правовые
     аспекты приведены более полно.";
```

```
reference "RFC 8177";

revision 2017-06-15 {
  description
    "Исходный выпуск RFC";
  reference "RFC 8177: YANG Data Model for Key Chains";
}

feature hex-key-string {
  description
    "Поддержка шестнадцатеричных строк для ключей.";
}

feature accept-tolerance {
  description
    "Поддержка допуска или предела для восприятия.";
}

feature independent-send-accept-lifetime {
  description
    "Поддержка независимых сроков действия для передачи
     и восприятия.";
}

feature crypto-hmac-sha-1-12 {
  description
    "Поддержка 12-байтовых дайджестов TCP HMAC-SHA-1.";
}

feature cleartext {
  description
    "Поддержка алгоритма cleartext (НЕ РЕКОМЕНДУЕТСЯ).";
}

feature aes-cmac-prf-128 {
  description
    "Поддержка псевдослучайной функции AES Cipher-based MAC.";
}

feature aes-key-wrap {
  description
    "Поддержка AES Key Wrap.";
}

feature replay-protection-only {
  description
    "Обеспечивает защиту от повторного использования без
     аутентификации, требуемую такими протоколами как BFD.";
}
identity crypto-algorithm {
  description
    "Базовое отождествление опций криптографического алгоритма.";
}

identity hmac-sha-1-12 {
  base crypto-algorithm;
  if-feature "crypto-hmac-sha-1-12";
  description
    "Алгоритм HMAC-SHA1-12.";
}

identity aes-cmac-prf-128 {
  base crypto-algorithm;
  if-feature "aes-cmac-prf-128";
  description
    "Алгоритм AES-CMAC-PRF-128. Требуется RFC 5926 для функций
     вывода ключей TCP-AO.";
}

identity md5 {
  base crypto-algorithm;
  description
    "Алгоритм MD5.";
}

identity sha-1 {
  base crypto-algorithm;
  description
    "Алгоритм SHA-1.";
}

identity hmac-sha-1 {
  base crypto-algorithm;
  description
    "Алгоритм аутентификации HMAC-SHA-1.";
```

```
  }

  identity hmac-sha-256 {
    base crypto-algorithm;
    description
      "Алгоритм аутентификации HMAC-SHA-256.";
  }

  identity hmac-sha-384 {
    base crypto-algorithm;
    description
      "Алгоритм аутентификации HMAC-SHA-384.";
  }

  identity hmac-sha-512 {
    base crypto-algorithm;
    description
      "Алгоритм аутентификации HMAC-SHA-512.";
  }

  identity cleartext {
    base crypto-algorithm;
    if-feature "cleartext";
    description
      "Открытый текст (cleartext).";
  }

  identity replay-protection-only {
    base crypto-algorithm;
    if-feature "replay-protection-only";
    description
      "Обеспечивает защиту от повторного использования без
       аутентификации, требуемую такими протоколами как BFD.";
  }

  typedef key-chain-ref {
    type leafref {
      path
      "/key-chain:key-chains/key-chain:key-chain/key-chain:name";
    }
    description
      "Применяется моделями данных для ссылки на настроенные
       цепочки ключей.";
  }

  grouping lifetime {
    description
      "Key lifetime specification.";
    choice lifetime {
      default "always";
      description
        "Опции задания срока действия для передачи и восприятия";
      case always {
        leaf always {
          type empty;
          description
            "Ключ действителен всегда.";
        }
      }
      case start-end-time {
        leaf start-date-time {
          type yang:date-and-time;
          description
            "Время начала.";
        }
        choice end-time {
          default "infinite";
          description
            "Время окончания для передачи.";
          case infinite {
            leaf no-end-time {
              type empty;
              description
                "Время завершения срока действия не ограничено.";
            }
          }
          case duration {
            leaf duration {
              type uint32 {
                range "1..2147483646";
              }
              units "seconds";
              description
                "Срок действия ключа в секундах.";
            }
          }
```

```
            case end-date-time {
              leaf end-date-time {
                type yang:date-and-time;
                description
                  "Время завершения.";
              }
            }
          }
        }
      }

    container key-chains {
      description
        "Все настроенные цепочки ключей имеются на устройстве.";
      list key-chain {
        key "name";
        description
          "Список цепочек ключей.";
        leaf name {
          type string;
          description
            "Имя цепочки ключей.";
        }
        leaf description {
          type string;
          description
            "Описание цепочки ключей.";
        }
        container accept-tolerance {
          if-feature "accept-tolerance";
          description
            "Отклонение для срока действия при восприятии (секунды).";
          leaf duration {
            type uint32;
            units "seconds";
            default "0";
            description
              "Диапазон отклонения в секундах.";
          }
        }
        leaf last-modified-timestamp {
          type yang:date-and-time;
          config false;
          description
            "Временная сетка последнего обновления цепочки ключей.";
        }
        list key {
          key "key-id";
          description
            "Один ключ в цепочке.";
          leaf key-id {
            type uint64;
            description
              "Уникальный числовой идентификатор ключа.";
          }
          container lifetime {
            description
              "Срок действия ключа.";
            choice lifetime {
              description
                "Варианты задания срока действия при передаче
                 и восприятии.";
              case send-and-accept-lifetime {
                description
                  "Сроки действия передачи и восприятия одинаковы.";
                container send-accept-lifetime {
                  description
                    "Одно значение срока для восприятия и передачи.";
                  uses lifetime;
                }
              }
              case independent-send-accept-lifetime {
                if-feature "independent-send-accept-lifetime";
                description
                  "Независимые сроки действия восприятия и передачи.";
                container send-lifetime {
                  description
                    "Отдельный срок действия для передачи.";
                  uses lifetime;
                }
                container accept-lifetime {
                  description
                    "Отдельный срок действия для восприятия.";
                  uses lifetime;
                }
```

```
            }
          }
        }
        leaf crypto-algorithm {
          type identityref {
            base crypto-algorithm;
          }
          mandatory true;
          description
            "Криптоалгоритм, связанный с ключом.";
        }
        container key-string {
          description
            "The key string.";
          nacm:default-deny-all;
          choice key-string-style {
            description
              "Стили строк ключей";
             case keystring {
               leaf keystring {
                type string;
                description
                  "Строка ключа в формате ASCII.";
               }
            }
            case hexadecimal {
              if-feature "hex-key-string";
              leaf hexadecimal-string {
                type yang:hex-string;
                description
                  "Ключ в форме шестнадцатеричной строки. По сравнению
                   обеспечивает большую энтропию при том же числе
                   октетов в строке. Кроме того, препятствует применению
                   общеизвестных слов и чисел.";
              }
            }
          }
        }
        leaf send-lifetime-active {
          type boolean;
          config false;
          description
            "Срок действия передачи для ключа активной цепочки.";
           }
        leaf accept-lifetime-active {
          type boolean;
          config false;
          description
            "Срок действия восприятия для ключа активной цепочки.";
        }
      }
    }
    container aes-key-wrap {
      if-feature "aes-key-wrap";
      description
        "Шифрование AES Key Wrap для строк ключей. Строки кодируются
         в шестнадцатеричной форме с применением листа
         hex-key-string.";
      leaf enable {
        type boolean;
        default "false";
        description
          "Включает шифрование AES Key Wrap.";
      }
    }
  }
}
<CODE ENDS>
```

5. Вопросы безопасности

Заданный этим документом модуль YANG определяет схему для данных, предназначенную для доступа через сеть с использованием протоколов управления, таких как NETCONF [NETCONF] или RESTCONF [RESTCONF]. Нижним уровнем NETCONF служит защищённый транспорт с обязательной поддержкой SSH (Secure Shell) [NETCONF-SSH]. Нижним уровнем RESTCONF служит протокол HTTPS с обязательной поддержкой защиты на транспортном уровне (TLS) [TLS].

Модель доступа к конфигурации сети (NACM – Network Configuration Access Control Model) [NETCONF-ACM] обеспечивает возможность разрешить доступ лишь определённых пользователей NETCONF или RESTCONF к заранее заданному подмножеству операций NETCONF или RESTCONF и содержимого. Строки ключей по умолчанию недоступны и требуются правила доступа NETCONF [NETCONF-ACM] для их настройки или извлечения.

Строки ключей могут зашифрованы с использованием алгоритма AES Key Wrap [AES-KEY-WRAP]. Ключ шифрования ключей AES (key-encryption key или KEK) не включён в модель YANG и должен задаваться или выводиться независимо от конфигурации цепочки ключей. При использовании шифрования AES требуется также свойство hex-key-string, поскольку зашифрованные ключи будут содержать символы, которые невозможно представить встроенным типом

YANG string [YANG-1.1]. **Рекомендуется** шифровать строки ключей с помощью ключа шифрования AES для предотвращение извлечения и сохранения строк ключей в открытом виде. Эта рекомендация не зависит от защиты доступа, обеспечиваемой моделью NACM [NETCONF-ACM].

В свойства (feature) модели YANG включён алгоритм cleartext. Его использование **не рекомендуется** за исключением случаев, когда у устройства и приложения нет иных вариантов (например, унаследованное сетевое устройство, которое должно аутентифицировать пакеты с интервалом 10 мсек или меньше для множества партнёров BFD [BFD]). Ключи, применяемые с алгоритмом cleartext, считаются незащищённые и такой ключ **не следует** применять в тоже время для более защищённого алгоритма.

Алгоритмы MD5 и SHA-1 тоже сочтены небезопасными ([Dobb96a], [Dobb96b], [SHA-SEC-CON]) и применять из **не рекомендуется**. Следует ограничивать их использование развёртываниями, где нужна совместимость с прежними версиями.

Реализациям, с ключами, предоставляемыми с помощью этой модели, следует хранить ключи с использованием имеющегося опыта защиты (best current security practice).

6. Взаимодействие с IANA

Этот документ регистрирует URI в реестре IETF XML Registry" [XML-REGISTRY] в формате [XML-REGISTRY].

```
URI: urn:ietf:params:xml:ns:yang:ietf-key-chain
Registrant Contact: The IESG.
XML: N/A, запрашиваемый URI является пространством имён XML.
```

Этот документ регистрирует модуль YANG в реестре YANG Module Names [YANG-1.0].

```
name: ietf-key-chain
namespace: urn:ietf:params:xml:ns:yang:ietf-key-chain
prefix: key-chain
reference: RFC 8177
```

7. Литература

7.1. Нормативные документы

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

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

[NETCONF] 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, <http://www.rfc-editor.org/info/rfc6241>.

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

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

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

[TLS] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

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

[YANG-1.0] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <http://www.rfc-editor.org/info/rfc6020>.

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

7.2. Дополнительная литература

[AES-KEY-WRAP] Housley, R. and M. Dworkin, "Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm", RFC 5649, DOI 10.17487/RFC5649, September 2009, <http://www.rfc-editor.org/info/rfc5649>.

[BFD] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <http://www.rfc-editor.org/info/rfc5880>.

[CRYPTO-KEYTABLE] Housley, R., Polk, T., Hartman, S., and D. Zhang, "Database of Long-Lived Symmetric Cryptographic Keys", RFC 7210, DOI 10.17487/RFC7210, April 2014, <http://www.rfc-editor.org/info/rfc7210>.

[Dobb96a] Dobbertin, H., "Cryptanalysis of MD5 Compress", Technical Report Presented at the Rump Session of EuroCrypt '96, May 1996.

[Dobb96b] Dobbertin, H., "The Status of MD5 After a Recent Attack", CryptoBytes, Vol. 2, No. 2, Summer 1996.

[IAB-REPORT] Andersson, L., Davies, E., and L. Zhang, "Report from the IAB workshop on Unwanted Traffic March 9-10, 2006", RFC 4948, DOI 10.17487/RFC4948, August 2007, <http://www.rfc-editor.org/info/rfc4948>.

[NMDA] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture", Work in Progress[1], draft-ietf-netmod-revised-datastores-02, May 2017.

[NTP-PROTO] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <http://www.rfc-editor.org/info/rfc5905>.

[OSPFV3-AUTH] Bhatia, M., Manral, V., and A. Lindem, "Supporting Authentication Trailer for OSPFv3", RFC 7166, DOI 10.17487/RFC7166, March 2014, <http://www.rfc-editor.org/info/rfc7166>.

[SHA-SEC-CON] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, DOI 10.17487/RFC6194, March 2011, <http://www.rfc-editor.org/info/rfc6194>.

[TCP-AO] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <http://www.rfc-editor.org/info/rfc5925>.

[TCP-AO-ALGORITHMS] Lebovitz, G. and E. Rescorla, "Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)", RFC 5926, DOI 10.17487/RFC5926, June 2010, <http://www.rfc-editor.org/info/rfc5926>.

[YANG-CRYPTO-KEYTABLE] Chen, I., "YANG Data Model for RFC 7210 Key Table", Work in Progress, draft-chen-rtg-key-table-yang-00, March 2015.

Приложение A. Примеры

A.1. Простая цепочка с одним, всегда пригодным ключом

```
<?xml version="1.0" encoding="utf-8"?>
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <key-chains xmlns="urn:ietf:params:xml:ns:yang:ietf-key-chain">
    <key-chain>
      <name>keychain-no-end-time</name>
      <description>
        A key chain with a single key that is always valid for
        transmission and reception.
      </description>
      <key>
        <key-id>100</key-id>
        <lifetime>
          <send-accept-lifetime>
            <always/>
          </send-accept-lifetime>
        </lifetime>
        <crypto-algorithm>hmac-sha-256</crypto-algorithm>
        <key-string>
          <keystring>keystring_in_ascii_100</keystring>
        </key-string>
      </key>
    </key-chain>
  </key-chains>
</data>
```

A.2. Цепочка ключей с разными сроками действия

```
<?xml version="1.0" encoding="utf-8"?>
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <key-chains xmlns="urn:ietf:params:xml:ns:yang:ietf-key-chain">
    <key-chain>
      <name>keychain2</name>
      <description>
        A key chain where each key contains a different send time
        and accept time and a different algorithm illustrating
        algorithm agility.
      </description>
      <key>
        <key-id>35</key-id>
        <lifetime>
          <send-lifetime>
            <start-date-time>2017-01-01T00:00:00Z</start-date-time>
            <end-date-time>2017-02-01T00:00:00Z</end-date-time>
          </send-lifetime>
          <accept-lifetime>
            <start-date-time>2016-12-31T23:59:55Z</start-date-time>
            <end-date-time>2017-02-01T00:00:05Z</end-date-time>
          </accept-lifetime>
        </lifetime>
        <crypto-algorithm>hmac-sha-256</crypto-algorithm>
        <key-string>
          <keystring>keystring_in_ascii_35</keystring>
        </key-string>
```

[1]Опубликовано в RFC 8342. *Прим. перев.*

```
        </key>
        <key>
          <key-id>36</key-id>
          <lifetime>
            <send-lifetime>
              <start-date-time>2017-02-01T00:00:00Z</start-date-time>
              <end-date-time>2017-03-01T00:00:00Z</end-date-time>
            </send-lifetime>
            <accept-lifetime>
              <start-date-time>2017-01-31T23:59:55Z</start-date-time>
              <end-date-time>2017-03-01T00:00:05Z</end-date-time>
            </accept-lifetime>
          </lifetime>
          <crypto-algorithm>hmac-sha-512</crypto-algorithm>
          <key-string>
            <hexadecimal-string>fe:ed:be:af:36</hexadecimal-string>
          </key-string>
        </key>
      </key-chain>
    </key-chains>
  </data>
```

A.3. Цепочка с независимыми сроками для передачи и восприятия

```
  <?xml version="1.0" encoding="utf-8"?>
  <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <key-chains xmlns="urn:ietf:params:xml:ns:yang:ietf-key-chain">
      <key-chain>
        <name>keychain2</name>
        <description>
          A key chain where each key contains different send times
          and accept times.
        </description>
        <key>
          <key-id>35</key-id>
          <lifetime>
            <send-lifetime>
              <start-date-time>2017-01-01T00:00:00Z</start-date-time>
              <end-date-time>2017-02-01T00:00:00Z</end-date-time>
            </send-lifetime>
            <accept-lifetime>
              <start-date-time>2016-12-31T23:59:55Z</start-date-time>
              <end-date-time>2017-02-01T00:00:05Z</end-date-time>
            </accept-lifetime>
          </lifetime>
          <crypto-algorithm>hmac-sha-256</crypto-algorithm>
          <key-string>
            <keystring>keystring_in_ascii_35</keystring>
          </key-string>
        </key>
        <key>
          <key-id>36</key-id>
          <lifetime>
            <send-lifetime>
              <start-date-time>2017-02-01T00:00:00Z</start-date-time>
              <end-date-time>2017-03-01T00:00:00Z</end-date-time>
            </send-lifetime>
            <accept-lifetime>
              <start-date-time>2017-01-31T23:59:55Z</start-date-time>
              <end-date-time>2017-03-01T00:00:05Z</end-date-time>
            </accept-lifetime>
          </lifetime>
          <crypto-algorithm>hmac-sha-256</crypto-algorithm>
          <key-string>
            <hexadecimal-string>fe:ed:be:af:36</hexadecimal-string>
          </key-string>
        </key>
      </key-chain>
    </key-chains>
  </data>
```

Участник работы

Yi Yang
SockRate
Email: yi.yang@sockrate.com

Благодарности

Спасибо Brian Weis за обсуждение вопросов безопасности.

Спасибо Ines Robles за комментарии к обзору Routing Directorate QA.

Спасибо Ladislav Lhotka за комментарии к обзору YANG Doctor.

Спасибо Martin Bjorklund за дополнительные комментарии к обзору YANG Doctor.

Спасибо Tom Petch за комментарии в IETF last call.

Спасибо Matthew Miller за комментарии при обзоре Gen-ART.

Спасибо Vincent Roca за комментарии при обзоре Security Directorate.

Спасибо Warren Kumari, Ben Campbell, Adam Roach, Benoit Claise за комментарии при обзоре IESG.

Адреса авторов

Acee Lindem (editor)
Cisco Systems
301 Midenhall Way
Cary, NC 27513
United States of America
Email: acee@cisco.com

Yingzhen Qu
Huawei
Email: yingzhen.qu@huawei.com

Derek Yeung
Arrcus, Inc
Email: derek@arrcus.com

Ing-Wher Chen
Jabil
Email: Ing-Wher_Chen@jabil.com

Jeffrey Zhang
Juniper Networks
10 Technology Park Drive
Westford, MA 01886
United States of America
Email: zzhang@juniper.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru