Internet Engineering Task Force (IETF)
Request for Comments: 8366
Category: Standards Track
ISSN: 2070-1721

K. Watsen
Juniper Networks
M. Richardson
Sandelman Software
M. Pritikin
Cisco Systems
T. Eckert
Huawei

May 2018

A Voucher Artifact for Bootstrapping Protocols

Ваучер для протоколов начальной загрузки

Аннотация

Этот документ задаёт стратегию защищённого связывания заявителя (pledge) с владельцем с использованием артефакта, напрямую или опосредованного подписанного изготовителем. Этот артефакт называется ваучером (voucher). В документе задан формат ваучера как определённого на языке YANG документа JSON, который подписан с использованием структуры CMS[1]. Возможны и другие форматы, производные от YANG. Артефакт ваучера обычно создаёт производитель (или уполномоченный производителем орган подписи MASA[2]). Документ определяет лишь артефакт ваучера, оставляя протоколы доступа к ваучерам другим документам.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[3] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[4]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8366.

Оглавление

[1]Cryptographic Message Syntax - синтаксис криптографических сообщений.
[2]Manufacturer Authorized Signing Authority.
[3]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[4]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Этот документ задаёт стратегию защищённого связывания устройства-кандидата (заявителя) с владельцем с помощью артефакта, подписанного напрямую или опосредованно изготовителем (уполномоченным этим производителем агнетом MASA). Этот артефакт называется ваучером.

Артефакт ваучера является документом JSON [RFC8259], соответствующим модели данных YANG [RFC7950], закодированным по правилам [RFC8259] и подписанным с использованием (по умолчанию) структуры CMS [RFC5652].

Основным назначением ваучера является защищённый перенос сертификата pinned-domain-cert, который заявитель может использовать для аутентификации последующих взаимодействий. Ваучер может быть полезен в разных случаях, но основным здесь является поддержка защищённых механизмов начальной загрузки. Назначение владения важно для механизмов начальной загрузки, чтобы заявитель мог аутентифицировать сеть, которая пытается получить контроль над ним.

Срок действия ваучером может меняться. В некоторых протоколах начальной загрузки ваучеры могут включать одноразовые значения (nonce), тогда как другие протоколы могут явно задавать срок действия. Для поддержки длительных сроков действия этот документ рекомендует использовать краткосрочные ваучера с механизмом программного обновления (параграф 6.1. Обновление вместо отзыва).

Этот документ задаёт лишь артефакт ваучера, оставляя другим документам описание протоколов для работы с ваучерами. Протоколы для работы с определенным здесь артефактом ваучера включают [ZERO-TOUCH], [SECUREJOIN], [KEYINFRA].

2. Терминология

Artifact — артефакт
: Здесь представляет ваучер как созданный экземпляр в форме подписанной структуры.

Domain - домен
: Набор сущностей (объектов) или инфраструктура с единым административным управлением. Целью протокола начальной загрузки является обнаружением заявителем домена и присоединение к нему.

Imprint - принятие отпечатка
: Процесс, где устройство получает криптографический ключевой материал для отождествления и доверия к будущим взаимодействиям с сетью. Этот термин взят из работы Конрада Лоренца (Konrad Lorenz) по биологии утят: «в критический период утёнок будет предполагать, что все, похожее на утку-мать, фактически является его матерью» [Stajano99theresurrecting]. Эквивалентом для устройства является получение отпечатка (fingerprint) сертификата корневого удостоверяющего центра сети. Устройство, принявшее отпечаток от злоумышленника, постигнет судьба, похожая на судьбу утёнка, принявшего волка за мать. Термин imprinting применяется в психологии и этологии [imprinting].

Join Registrar (Coordinator) - регистратор присоединения (координатор)
: Представитель домена, настроенный (возможно, автономно) для принятия решений о присоединении новых устройств к домену. Администратор домена взаимодействует с регистратором присоединения (и координатором) для управления этим процессом. Обычно регистратор размещается «внутри» домена. Для простоты в документе используется просто «регистратор».

MASA (Manufacturer Authorized Signing Authority) - уполномоченный изготовителем агент подписи
: сущность, которая (для целей этого документа) подписывает ваучеры для продукции изготовителя (заявителей). В некоторых протоколах начальной загрузки MASA может присутствовать в Internet и быть частью процесса начальной загрузки, а в других протоколах MASA является автономной службой, которая не играет активной роли в процессе начальной загрузки.

Owner - владелец
: Сущность, управляющая секретным ключом сертификата pinned-domain-cert, содержащегося в ваучере.

Pledge - заявитель
: Устройство, пытающееся найти домен и безопасно присоединиться к нему. При поставке заявитель доверяет лишь уполномоченным представителям изготовителя.

Registrar - регистратор
: См. join registrar.

TOFU (Trust on First Use) - доверие при первом использовании
: Когда устройство-заявитель не принимает решений о защите, а просто доверяет первой сущности из домена, с которым оно соединяется. Термин применяется как в [RFC7435]. Называется также моделью воскресающего утёнка (resurrecting duckling).

Voucher - ваучер
: Подписанное заявление службы MASA, указывающее заявителю криптографическое отождествление домена, которому следует доверять.

3. Уровни требований

Ключевые слова **необходимо** (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 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

4. Типы ваучеров

Ваучер является криптографически защищённым заявлением для устройства, разрешающим бесконтактный (zero-touch) отпечаток (imprint) для регистратора домена. Конкретные сведения, предоставляемые ваучером, зависят от

применяемого варианта начальной загрузки. Ваучер может сообщать регистратору присоединения и заявителю указанные ниже сведения.

Assertion Basis - основы контроля
Указывает метод защиты отпечатка (отличается от подписи ваучера, которая защищает сам ваучер). Это может включать подтверждённую изготовителем проверку владения, обеспеченные операции ведения журнала или зависимость от поведения конечной точки заявителя, такого как защищённый корень доверия для измерений. Этот документ нормативно задаёт лишь некоторые методы, оставляя другие будущим работам.

Authentication of Join Registrar - аутентификация регистратора
Указывает способ проверки заявителем подлинности регистратора. Этот документ задаёт механизм закрепления сертификата домена. Закрепление симметричного, необработанного (raw) ключа, данных CN-ID или DNS-ID (как задано в [RFC6125]) оставлено для будущих работ.

Anti-Replay Protections - защита от повторов
Сведения на основе времени или одноразового значения nonce для ограничения срока действия ваучера или числа попыток начальной загрузки.

Можно выполнить множество сценариев начальной загрузки с использованием разных комбинаций этих сведений. Все сценарии связаны с основной угрозой MiTM[1]-атак, когда регистратор получает управление заявителем. Приведённые ниже комбинации задают «тип» ваучера.

	Assertion		***Registrar ID***			***Validity***	
Тип ваучера	***Logged***	***Verified***	***Trust Anchor***	***CN-ID или DNS-ID***		***RTC***	***Nonce***
Audit - аудит	X		X				X
Nonceless Audit - аудит без Nonce	X		X			X	
Owner Audit - аудит владельца	X	X	X			X	X
Owner ID - идентификатор владельца		X	X		X	X	
Bearer out-of-scope - носитель вне области действия	X			шаблон		необязательно	

Примечание. Все типы ваучеров включают pledge ID serial-number (не показан для экономии места).

Audit Voucher - ваучер аудита
Ваучер аудита назван так из-за механизмов журнальных записей, которые регистратор проверяет на предмет соблюдения локальной политики. Регистратор смягчает действия MiTM-регистраторов, проверяя их присутствие по записям журнала. Это не позволяет предотвратить MiTM, но обеспечивает механизм отклика, который препятствует использованию враждебных регистраторов. Преимуществом этой формы является то, что службе MASA не требуется знать фактического владельца.

Nonceless Audit Voucher - ваучер аудита без Nonce
Ваучер аудита без проверки срока действия. Отличается от обычного Audit Voucher тем, что его можно выпускать заранее для поддержки разделения сети или обеспечения удалённого развертывания.

Ownership Audit Voucher - ваучер аудита владения
Ваучер аудита с подтверждением службой MASA того, что регистратор является полномочным владельцем. Служба MASA смягчает действия MiTM-регистраторов, отвергая создание Audit Voucher для несанкционированных регистраторов. Регистратор применяет аудит в дополнение к MASA. Это обеспечивает идеальный вариант совместного принятия решений и применения правил производителем и владельцем.

Ownership ID Voucher - ваучер идентификатора владения
Ваучер с включением идентификатора CN-ID или DNS-ID. Служба MASA смягчает действия MiTM-регистраторов, идентифицируя конкретного регистратора (через WebPKI), уполномоченного владеть заявителем.

Bearer Voucher - ваучер носителя
Ваучер с включением шаблона идентификатора регистратора. Поскольку идентификатор регистратора не указан, этот тип ваучера должен считаться секретным и требующим защиты от раскрытия, поскольку любой «носитель» ваучера может указать владение заявителем. Публикация ваучера носителя без nonce фактически превращает указанного заявителя в устройство TOFU с минимальным смягчением действий MiTM-регистраторов. Этот тип ваучеров не рассматривается в документе.

5. Артефакт ваучера

Основным назначением ваучера является защищённая привязка заявителя к владельцу. Ваучер сообщает заявителю , какой объект следует считать его владельцем.

Этот документ задаёт ваучер, являющийся документом JSON, представляющим экземпляр модуля YANG, определённого в параграфе 5.3, который по умолчанию имеет подпись CMS. Формат описан здесь как практическая основа для некоторых применений (таких как NETCONF), но больше для чёткой демонстрации того, как ваучеры выглядят на практике. Описание служит также для утверждения (validate) модели данных YANG.

Предполагается определение в будущих работах новых отображений ваучеров с кратким представлением двоичных объектов (Concise Binary Object Representation или CBOR) из JSON и замена контейнера подписи CMS на JOSE[2] или COSE[3]. Допустимы также форматы XML и ASN.1.

Этот документ задаёт тип носителя (media type) и расширение имён файлов для типа JSON с кодированием CMS. В будущих документах для других форматов будут заданы дополнительные типы носителей. Сигнализация осуществляется в форме MIME Content-Type заголовка HTTP Accept или более простых методов, таких как использование расширений имён файлов при передаче ваучеров на устройствах USB.

5.1. Диаграмма дерева

Ниже представлено верхний уровень дерева документа с ваучером на основе нотации [RFC8340]. Каждый узел дерева полностью описан в модуле YANG, заданном в параграфе 5.3. Модуль YANG.

[1]Man-in-The-Middle - перехват и изменение данных с участием человека.
[2]JSON Object Signing and Encryption - подписание и шифрование объектов JSON.
[3]CBOR Object Signing and Encryption - подписание и шифрование объектов CBOR.

```
   module: ietf-voucher

     yang-data voucher-artifact:
         +---- voucher
            +---- created-on                       yang:date-and-time
            +---- expires-on?                      yang:date-and-time
            +---- assertion                        enumeration
            +---- serial-number                    string
            +---- idevid-issuer?                   binary
            +---- pinned-domain-cert               binary
            +---- domain-cert-revocation-checks?   boolean
            +---- nonce?                           binary
            +---- last-renewal-date?               yang:date-and-time
```

5.2. Примеры

Этот параграф содержит иллюстративные примеры ваучеров с кодированием по правилам [RFC8259].

Ниже приведён пример эфемерного ваучера (с использованием nonce). MASA генерирует такой ваучер с использованием типа утверждения logged, зная, что это подходит для подающего запрос заявителя.

```
   {
     "ietf-voucher:voucher": {
       "created-on": "2016-10-07T19:31:42Z",
       "assertion": "logged",
       "serial-number": "JADA123456789",
       "idevid-issuer": "base64encodedvalue==",
       "pinned-domain-cert": "base64encodedvalue==",
       "nonce": "base64encodedvalue=="
     }
   }
```

Ниже приведён пример неэфемерного ваучера (без nonce). Хотя срок действия этого ваучера истекает через две недели, его, предположительно, можно продлить на срок до года. MASA генерирует такой ваучер с использованием типа утверждения verified, который должен подходить для всех заявителей.

```
   {
     "ietf-voucher:voucher": {
       "created-on": "2016-10-07T19:31:42Z",
       "expires-on": "2016-10-21T19:31:42Z",
       "assertion": "verified",
       "serial-number": "JADA123456789",
       "idevid-issuer": "base64encodedvalue==",
       "pinned-domain-cert": "base64encodedvalue==",
       "domain-cert-revocation-checks": true,
       "last-renewal-date": "2017-10-07T19:31:42Z"
     }
   }
```

5.3. Модуль YANG

Приведённый ниже модуль YANG [RFC7950] формально описывает структуру ваучера в форме документа JSON.

```
<CODE BEGINS> file "ietf-voucher@2018-05-09.yang"
module ietf-voucher {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-voucher";
  prefix vch;

  import ietf-yang-types {
    prefix yang;
    reference "RFC 6991: Common YANG Data Types";
  }
  import ietf-restconf {
    prefix rc;
    description
      "Этот оператор импорта присутствует лишь для доступа к
       расширению yang-data, определённому в RFC 8040.";
    reference "RFC 8040: RESTCONF Protocol";
  }

  organization
    "IETF ANIMA Working Group";
  contact
    "WG Web:   <https://datatracker.ietf.org/wg/anima/>
     WG List:  <mailto:anima@ietf.org>
     Author:   Kent Watsen
               <mailto:kwatsen@juniper.net>
     Author:   Max Pritikin
               <mailto:pritikin@cisco.com>
     Author:   Michael Richardson
               <mailto:mcr+ietf@sandelman.ca>
     Author:   Toerless Eckert
               <mailto:tte+ietf@cs.fau.de>";
  description
    "Модуль задаёт формат для ваучера, который создаётся изготовителем
     устройства-заявителя или делегируется агенту MASA для защищённого
     связывания заявителя с владельцем, чтобы заявитель мог организовать
     защищённое соединение с сетевой инфраструктурой владельца.
```

```
    Ключевые слова ДОЛЖНО, НЕДОПУСТИМО, ТРЕБУЕТСЯ, НУЖНО, НЕ НУЖНО,
    СЛЕДУЕТ, НЕ СЛЕДУЕТ, РЕКОМЕНДУЕТСЯ, НЕ РЕКОМЕНДУЕТСЯ, МОЖНО,
    НЕОБЯЗАТЕЛЬНО в этом документе трактуются в соответствии с
    BCP 14 (RFC 2119) (RFC 8174) тогда и только тогда, когда они
    указаны заглавными буквами, как показано здесь.

    Авторские права (Copyright (c) 2018) 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 8366, где правовые
    аспекты приведены более полно.";

  revision 2018-05-09 {
    description
      "Исходный выпуск";
    reference "RFC 8366: Voucher Profile for Bootstrapping Protocols";
  }

  // Оператор верхнего уровня
  rc:yang-data voucher-artifact {
    uses voucher-artifact-grouping;
  }

  // Группировка, определённая для будущих дополнений

  grouping voucher-artifact-grouping {
    description
      "Группировка для использования и расширения в будущем.";
    container voucher {
      description
        "Ваучер связывает заявителя с владельцем(pinned-domain-cert).";
      leaf created-on {
        type yang:date-and-time;
        mandatory true;
        description
          "Дата создания ваучера. Этот узел предназначен, прежде всего,
           для человека и систем аудита. В будущем на основе этого узла
           МОГУТ задаваться требования к проверке.";
      }
      leaf expires-on {
        type yang:date-and-time;
        must 'not(../nonce)';
        description
          "Срок действия ваучера. Узел необязателен и не все заявители
           поддерживают ограничение срока (например, при отсутствии
           надёжных часов).

           При наличии этого поля заявители ДОЛЖНЫ гарантировать, что
           указанное время ещё не наступило. Заявители без точных часов
           не соответствуют этому требованию.

           В expires-on НЕДОПУСТИМО указывать время после истечения
           срока действия любого из сертификатов в pinned-domain-cert.";
      }
      leaf assertion {
        type enumeration {
          enum verified {
            description
              "Указывает позитивный результат проверки владения агентом
               MASA (например, через канал продаж).";
          }
          enum logged {
            description
              "Указывает, что ваучер был выпущен после минимальной
               проверки прав владения или управления. Выпуск был записан
               в журнал для обнаружения возможных проблем безопасности
               (например, получатели ваучеров могут убедиться сами, что
               в журнале нет неожиданных ваучеров). Это похоже на
               незащищённое доверие при первом использовании (TOFU), но
               с ведением журнала для обнаружения неожиданных событий.";
          }
          enum proximity {
            description
              "Указывает, что ваучер был выпущен после проверки агентом
               MASA подтверждения близости, представленного устройством
               и целевым доменом. Выпуск был записан в журнал для
               обнаружения возможных проблем безопасности. Это сильнее,
               чем просто запись в журнал, поскольку требует проверки
               взаимодействия заявителя и владельца, но все равно
```

```
            зависит от анализа журнала для обнаружения неожиданных
            событий.";
        }
      }
      mandatory true;
      description
        "Утверждение (assertion) - это заявление MASA о способе
         проверки владельца. Это позволяет заявителю более подробно
         проверить правила. Заявители ДОЛЖНЫ гарантировать пригодность
         утверждения в соответствии с локальными правилами до
         начала обработки ваучера.";
    }
    leaf serial-number {
      type string;
      mandatory true;
      description
        "Порядковый номер оборудования. При обработке ваучера
         заявитель ДОЛЖЕН подтвердить соответствие своего порядкового
         номера этому значению. При несовпадении заявителю НЕДОПУСТИМО
         обрабатывать этот ваучер.";
    }
    leaf idevid-issuer {
      type binary;
      description
        "СТРОКА ОКТЕТОВ идентификатора ключа агентства (Authority
         Key Identifier), определённого в параграфе 4.2.1.1 RFC 5280,
         из сертификата IDevID заявителя. Лист необязателен,
         поскольку некоторые порядковые номера уже уникальны в
         сфере действия MASA. Включение статистически уникального
         идентификатора ключа обеспечивает статистически уникальную
         идентификацию оборудования. При обработке ваучера заявитель
         ДОЛЖЕН гарантировать соответствие IDevID Authority Key
         этому значению. При несовпадении обработка ваучера
         НЕДОПУСТИМА.

         При выпуске ваучера агент MASA ДОЛЖЕН обеспечить в этом поле
         порядковый номер, который в остальном неуникален в рамках
         действия MASA.";
    }
    leaf pinned-domain-cert {
      type binary;
      mandatory true;
      description
        "Структура сертификата X.509 v3, заданная RFC 5280, с
         кодированием DER (Distinguished Encoding Rules) в
         соответствии с ITU-T X.690.

         Этот сертификат используется заявителем для доверия к
         инфраструктуре открытых ключей (Public Key Infrastructure)
         для проверки сертификата домена, представленного заявителю
         независимо протоколом начальной загрузки. Сертификат домена
         ДОЛЖЕН включать этот сертификат в свою цепочку сертификации.
         Это МОЖЕТ быть сертификат конечного объекта, в том числе
         самоподписанный.";
      reference
        "RFC 5280:
           Internet X.509 Public Key Infrastructure Certificate
           and Certificate Revocation List (CRL) Profile.
         ITU-T X.690:
            Information technology - ASN.1 encoding rules:
            Specification of Basic Encoding Rules (BER),
            Canonical Encoding Rules (CER) and Distinguished
            Encoding Rules (DER).";
    }
    leaf domain-cert-revocation-checks {
      type boolean;
      description
        "Указание заявителю, что он ДОЛЖЕН (true) или ему НЕДОПУСТИМО
         (false) проверять статус отзыва для прикреплённого доменного
         сертификата. Если это поле не задано, используется обычное
         поведение PKIX для проверки сертификата домена.";
    }
    leaf nonce {
      type binary {
        length "8..32";
      }
      must 'not(../expires-on)';
      description
        "Значение, которое заявитель может применять в некоторых
         протоколах начальной загрузки для предотвращения повторов
         (anti-replay). Узел необязателен, поскольку его применяют
         не все протоколы начальной загрузки.

         При наличии листа заявитель ДОЛЖЕН сравнить представленное
         значение nonce с другим значением, которое случайно создано
         заявителем и передано серверу начальной загрузки в начальном
```

```
            сообщении. При несовпадении заявителю НЕДОПУСТИМО
            обрабатывать этот ваучер.";
        }
        leaf last-renewal-date {
          type yang:date-and-time;
          must '../expires-on';
          description
            "Финальная дата возможности продления ваучера с точки зрения
            MASA. Информативное поле, не обрабатываемое заявителем.

            После создания ваучера могут возникнуть обстоятельства,
            меняющие срок его действия. Например, производитель может
            связывать срок действия с контрактами на поддержку, которые
            могут продлеваться и расторгаться.";
        }
      } // end voucher
    } // end voucher-grouping
}
<CODE ENDS>
```

5.4. Формат CMS для артефакта ваучера

Развитием PKCS#7 в IETF является CMS [RFC5652]. Подписанный CMS ваучер, как принято по умолчанию, включает структуру ContentInfo с содержимым ваучера. Тип eContentType 40 указывает, что содержимое является ваучером в кодировке JSON.

Подпись является структурой CMS SignedData, как указано в параграфе 5.1 [RFC5652], закодированной в соответствии с ASN.1 DER[1], как указано в ITU-T X.690 [ITU.X690.2015].

Для улучшения совместимости параграф 8.3 в этом документе регистрирует тип носителя application/voucher-cms+json и расширение имён файлов .vcj.

Структура CMS **должна** включать структуру signerInfo, описанную в параграфе 5.1 [RFC5652], с подписью содержимого, использующей секретный ключ, которому доверяет получатель. Обычно получателем является заявитель, а подписывающей стороной - MASA. Другим возможным вариантом является формат подписанного запроса ваучера от заявителя или регистратора к агенту MASA. В этом документе подписывающей стороной считается MASA.

Отметим, что в параграфе 5.1 [RFC5652] рассматривается проверка объекта CMS, который на деле является объектом PKCS7 (cmsVersion=1). Промежуточные системы, такие как регистраторы инфраструктуры удалённых защищённых ключей начальной загрузки (Bootstrapping Remote Secure Key Infrastructures или BRSKI), которым может потребоваться оценка вайчера «на лету», **должны** быть готовы к этому устаревшему формату. Сигнализация не требуется, поскольку изготовителю известны возможности заявителя и он будет применять для каждого заявителя нужный формат.

В структуру CMS **следует** включать все сертификаты ведущие к сертификату привязки доверия, известной получателю (включая его). Включение привязки доверия необычно для многих приложений, но третья сторона не может точно проверить транзакцию без этой привязки.

Структура CMS **может** также включать объекты отзыва для любых промежуточных удостоверяющих центров (certificate authority или CA) между эмитентом ваучера и известной получателю привязкой доверия. Однако применение CRL и других механизмов проверки не рекомендуется, поскольку маловероятна способность заявителя выполнить online-проверку и наличие у него доверенного источника времени. Как описано ниже, использование краткосрочных ваучеров и/или представленное заявителем значение nonce обеспечивает гарантию актуальности ваучера.

6. Соображения по устройству

6.1. Обновление вместо отзыва

Сроки действия ваучеров могут меняться. В некоторых протоколах начальной загрузки ваучеры могут создаваться и сразу же применяться, а в других решениях может проходить достаточно много времени между созданием и использованием ваучера. В случаях отложенного применения ваучера заявитель должен гарантировать пригодность утверждений, сделанных при создании ваучера.

Артефакты отзыва обычно применяются для проверки действительности утверждений, таких как сертификаты PKIX, web-маркеры, «ваучеры». При таком подходе потенциально долгосрочные утверждения сочетаются с частой проверкой статуса отзыва, чтобы убедиться в фактической действительности утверждений. Однако это усложняет решения, поскольку требует дополнительных протоколов и кода для распространения и обработки отзывов.

Для устранения недостатков аннулирования этот документ рекомендует применять упрощённое продление краткосрочных безотзывных ваучеров. Вместо выпуска долгосрочного ваучера, где лист expires-on указывает далёкое будущее, предполагается, что агент MASA выдаёт краткосрочные ваучеры, где лист expires-on указывает сравнительно близкое время вместе с обещанием (поле last-renewal-date) при необходимости повторно выдать ваучер. Важно подчеркнуть, что, несмотря на серьёзные проверки при первом выпуске ваучера (Вы тот, за кого себя выдаёте? Заявитель действительно принадлежит вам?), повторный выпуск ваучеров следует упрощать, поскольку он, вероятно, лишь обновляет срок действия ваучера. При таком подходе имеется лишь один артефакт, и нужен лишь один путь кода - у заявителя нет возможности пропустить проверку статуса отзыва ваучера, например, по причине недоступности ответчика OCSP.

Хотя этот документ рекомендует краткосрочные ваучеры, артефакт ваучера не препятствует созданию долгосрочных, однако метод отзыва в документе не описан.

Отметим, что ваучер может быть подписан цепочкой промежуточных CA, ведущих к сертификату привязки доверия, известной заявителю. Хотя сам ваучер является безотзывным, его можно аннулировать, отозвав сертификат одного из промежуточных CA.

[1]Distinguished Encoding Rules - правила отличительного кодирования.

6.2. Ваучер на одного заявителя

Описанное здесь решение изначально предполагало применение одного ваучера для множества заявителей и использованием списка регулярных выражений для представления диапазонов серийных номеров. Однако было установлено, что блокировка обновления ваучера, применимого для множества устройств, будет чрезмерной, если нужно блокировать владение лишь одним заявителем. Поэтому формат ваучера поддерживает лишь один серийный номер.

7. Вопросы безопасности

7.1. Точность часов

Злоумышленник может использовать просроченный ваучер для получения контроля над устройством, которое не понимает времени (не имеет часов). Устройство не может доверять NTP как эталону времени, поскольку атакующий может контролировать поток NTP.

Имеется три варианта защиты: 1) устройство должны убедиться, что время ещё не достигло значения, указанного в поле expires-on, 2) устройство без доступа к часам может применять nonce для получения эфемерных ваучеров, 3) могут применяться ваучеры с неограниченным сроком действия, которые будут включаться в журнал аудита, информируя о защитном решении.

Этот документ задаёт формат ваучера, содержащий значения времени для срока действия, обработка которых требует точных часов. Производители, планирующие выпускать ваучеры с указанием срока действия, должны гарантировать наличие в устройстве часов, точно установленных при отгрузке, и принять меря предотвращения подделки часов. Если точность часов обеспечить невозможно, не следует выпускать ваучеры с ограниченным сроком действия.

7.2. Защита ваучера с помощью HSM

В соответствии с рекомендациями параграфа 6.1. Обновление вместо отзыва для MASA в качестве службы подписи ваучеров **рекомендуется** защищать секретный ключ MASA, применяемый для подписи ваучеров, защищать с помощью аппаратного модуля (hardware security module или HSM).

7.3. Проверка сертификата домена при подписи

Если сертификат домена скомпрометирован, злоумышленник может воспользоваться остающимися ваучерами этого домена. Очевидно, что администратор домена должен инициировать отзыв любых сертификатов отождествления домена (как в обычных решениях PKI). Предполагается также контакт с MASA, чтобы указать необходимость блокировки обновления остающихся ваучеров (предположительно, краткосрочных). Протоколам распространения ваучеров **рекомендуется** проверять отзыв сертификатов отождествления домена до подписания ваучеров.

7.4. Вопросы безопасности модуля YANG

Заданный здесь модуль YANG определяет схему для данных, которые инкапсулируются в тип носителя с подписью CMS, как описано в разделе 5 [RFC5652]. Таким образом смоделированные в YANG данные будут защищены от изменения.

Реализациям следует помнить, что подписанные данные лишь защищены от внешнего изменения, но остаются видимыми. Возможное раскрытие информации влияет не только на безопасность, но и на приватность. В частности, злоумышленники могут собирать такие сведения, как принадлежность устройств организации, точки распространения списков отзыва (CRL Distribution Point) и ссылки на ответчики OCSP (OCSP Responder URL), применяемые для проверки ваучеров. Когда сохранение приватности важно, данные с подписью CMS **следует** защищать путём передачи через защищённый транспорт с взаимной аутентификацией (например, TLS [RFC5246]) или инкапсуляции в тип enveloped-data (раздел 6 в [RFC5652]), но детали этого выходят за рамки документа.

Использование YANG для задания структур данных с помощью оператора yang-data является сравнительно новым и отличается от традиционного применения YANG для определения API с доступом по протоколам управления сетью, таким как NETCONF [RFC6241] и RESTCONF [RFC8040]. Поэтому приведённые здесь рекомендации не соответствуют шаблону, заданному в параграфе 3.7 [YANG-GUIDE].

8. Взаимодействие с IANA

8.1. Реестр IETF XML

Этот документ регистрирует URI в реестре IETF XML Registry [RFC3688]

```
URI: urn:ietf:params:xml:ns:yang:ietf-voucher
Registrant Contact: The ANIMA WG of the IETF.
XML: N/A, запрошенный URI является пространством имён XML.
```

8.2. Реестр YANG Module Names

Этот документ регистрирует модуль YANG в реестре YANG Module Names [RFC6020]

```
name:         ietf-voucher
namespace:    urn:ietf:params:xml:ns:yang:ietf-voucher
prefix:       vch
reference:    RFC 8366
```

8.3. Реестр Media Types

Этот документ регистрирует новый тип носителя в реестре Media Types [RFC6838]

```
Type name:  application
Subtype name:  voucher-cms+json
Required parameters:  нет
```

```
   Optional parameters:  нет
   Encoding considerations: ваучеры JSON с подписью CMS и кодированием ASN.1/DER.
   Security considerations: см. раздел 7
   Interoperability considerations: формат предназначен для широкой совместимости.
   Published specification:  RFC 8366
   Applications that use this media type: системы автоматических «отпечатков» ANIMA, 6tisch, NETCONF.
   Fragment identifier considerations:  нет
   Additional information:
      Deprecated alias names for this type:  нет
      Magic number(s):  нет
      File extension(s):  .vcj
      Macintosh file type code(s):  нет
   Person and email address to contact for further information:
      IETF ANIMA WG
   Intended usage:  LIMITED
   Restrictions on usage:  нет
   Author:  ANIMA WG
   Change controller:  IETF
   Provisional registration? (standards tree only):  нет
```

8.4. Реестр SMI Security for S/MIME CMS Content Type

Агентство IANA зарегистрировало идентификатор OID в реестре SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1).

Десятичное значение	*Описание*	*Документ*
40	id-ct-animaJSONVoucher	RFC 8366

9. Литература

9.1. Нормативные документы

[ITU.X690.2015] International Telecommunication Union, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1, August 2015, <https://www.itu.int/rec/T-REC-X.690/>.

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

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

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

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

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

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

9.2. Дополнительная литература

[imprinting] Wikipedia, "Wikipedia article: Imprinting", February 2018, <https://en.wikipedia.org/w/index.php?title=Imprinting_(psychology)&oldid=825757556>.

[KEYINFRA] Pritikin, M., Richardson, M., Behringer, M., Bjarnason, S., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", Work in Progress[1], draft-ietf-anima-bootstrapping-keyinfra-12, March 2018.

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

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

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure ping X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

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

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <https://www.rfc-editor.org/info/rfc6838>.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <https://www.rfc-editor.org/info/rfc7435>.

[1]Опубликовано в RFC 8995. *Прим. перев.*

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

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

[SECUREJOIN] Richardson, M., "6tisch Secure Join protocol", Work in Progress, draft-ietf-6tisch-dtsecurity-secure-join-01, February 2017.

[Stajano99theresurrecting] Stajano, F. and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks", 1999, <https://www.cl.cam.ac.uk/research/dtg/www/files/publications/public/files/tr.1999.2.pdf>.

[YANG-GUIDE] Bierman, A., "Guidelines for Authors and Reviewers of YANG Data Model Documents", Work in Progress[1], draft-ietf-netmod-rfc6087bis-20, March 2018.

[ZERO-TOUCH] Watsen, K., Abrahamsson, M., and I. Farrer, "Zero Touch Provisioning for Networking Devices", Work in Progress[2], draft-ietf-netconf-zerotouch-21, March 2018.

Благодарности

Авторы благодарны за обсуждение William Atwood, Toerless Eckert, Sheng Jiang (по фамилиям в алфавитном порядке).

Russ Housley представил обновление PKCS7 на CMS (RFC 5652) вместе с детальной структурой CMS.

Адреса авторов

Kent Watsen
Juniper Networks
Email: kwatsen@juniper.net

Michael C. Richardson
Sandelman Software
Email: mcr+ietf@sandelman.ca
URI: http://www.sandelman.ca/

Max Pritikin
Cisco Systems
Email: pritikin@cisco.com

Toerless Eckert
Huawei USA - Futurewei Technologies Inc.
2330 Central Expy
Santa Clara 95050
United States of America
Email: tte+ietf@cs.fau.de, toerless.eckert@huawei.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Опубликовано в RFC 8407. *Прим. перев.*
[2]Опубликовано в RFC 8572. *Прим. перев.*