Internet Engineering Task Force (IETF)
Request for Comments: 9608
Updates: 5280
Category: Standards Track
ISSN: 2070-1721

R. Housley
Vigil Security
T. Okubo
DigiCert
J. Mandel
AKAYLA, Inc.

June 2024

No Revocation Available for X.509 Public Key Certificates

Расширение для указания недоступности отзыва сертификатов открытых ключей X.509

Аннотация

Сертификаты открытых ключей X.509v3 описаны в RFC 5280. В Internet всё шире применяются краткосрочные сертификаты и удостоверяющие центры (Certification Authority или CA), выпускающие такие сертификаты не публикуют сведений об отзыве, поскольку сроки действия сертификатов меньше времени, требуемого на обнаружение и распространение сведений об отзыве. У некоторых долгосрочных сертификатов открытых ключей X.509v3 срок действия не ограничен и они тоже не отзываются. Данная спецификация определяет расширение сертификата noRevAvail, чтобы полагающаяся на сертификат сторона могла легко определить, что CA не публикует сведений об отзыве и обновить алгоритм проверки пути сертификации, заданный в RFC 5280, чтобы пропускать проверку отзыва при наличии в сертификате расширения noRevAvail.

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.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9608.

Оглавление

1. Введение

Краткосрочные сертификаты открытых ключей X.509v3 [RFC5280] все шире применяются в Internet. Например, среда автоматического управления сертификатами (Automatic Certificate Management Environment или ACME) [RFC8555] обеспечивает простой способ получения краткосрочных сертификатов. Во многих случаях удостоверяющие центры (CA) не предоставляют сведений об отзыве краткосрочных сертификатов. Это обусловлено тем, что срок их действия меньше времени, требуемого для обнаружения и распространения сведений об отзыве. В результате отзыв краткосрочных сертификатов, служащих для проверки подлинности или управления ключами, становится ненужным и

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

бессмысленным. С другой стороны, отзыв сертификатов, связанных с долгосрочными подписями (например, для документов или программного кода), позволяет получить важные сведения о моментах обнаружения компрометации.

Некоторые сертификаты открытых ключей X.509v3 имеют неограниченный срок действия и никогда не отзываются. Например, фабрика может включать сертификат IDevID [IEEE802.1AR] для привязки назначенного устройству идентификатора к установленному при производстве открытому ключу. Идентификатор может включать модель и серийный номер устройства, которые никогда не меняются. Для указания того, что для сертификата не задан срок действия, в поле notAfter периода действия сертификата устанавливается значение 99991231235959Z [RFC5280].

Данная спецификация задаёт расширение сертификата noRevAvail, позволяющее доверяющей стороне легко понять, что CA не публикует сведений об отзыве сертификата конечного субъекта, и обновляет алгоритм проверки пути сертификации [RFC5280], чтобы проверка отзыва не выполнялась при наличии в сертификате расширения noRevAvail.

Отметим, что расширение сертификата noRevAvail обеспечивает функциональность, похожую на расширение ocsp-nocheck [RFC6960]. Последнее подходит лишь для включения в сертификаты, выпущенные для респондентов протокола Online-статуса сертификатов (Online Certificate Status Protocol или OCSP), тогда как расширение noRevAvail можно применять в любом сертификате конечного субъекта, для которого CA не публикует сведений об отзыве. Чтобы не нарушать экосистему OCSP, разработчикам не следует считать расширение noRevAvail заменой ocsp-nocheck и оно может включаться в сертификаты для ответчиков OCSP, как дополнение к ocsp-nocheck.

1.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (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.

1.2. ASN.1

Сертификаты X.509 создаются с помощью ASN.1 [X.680] по базовым (Basic Encoding Rules или BER) и отличительным (Distinguished Encoding Rules или DER) правилам кодирования [X.690].

1.3. История

В 1988 г. сертификат X.509v1 был определён CCITT [X.509-1988].

В 1997 г. сертификат X.509v3 и сертификат атрибута был определён ITU-T [X.509-1997].

В 1999 г. IETF впервые было предложено использовать сертификаты X.509v3 в Internet [RFC2459].

В 2000 г. определено (ITU-T) расширение noRevAvail для использования сертификатами атрибутов [X.509-2000].

В 2002 г. впервые задан профиль сертификата атрибута (IETF) для использования в Internet [RFC3281] и этот профиль включал поддержку расширения noRevAvail.

В 2019 г., опубликовано обновление ITU-T Recommendation X.509 [X.509-2019].

В связи с расширяющимся применением в Internet краткосрочных сертификатов недавнее техническое исправление (Technical Corrigendum) для ITU-T Recommendation X.509 [X.509-2019-TC2] позволяет применять расширение noRevAvail для сертификатов открытых ключей и атрибутов.

2. Расширение сертификата noRevAvail

Расширение noRevAvail, заданное в [X.509-2019-TC2], позволяет CA указать недоступность сведений об отзывае для этого сертификата.

Это расширение **недопустимо** включать в сертификаты открытых ключей CA.

Соответствующие спецификации CA **должны** включать это расширение в сертификаты, для которых не будут публиковаться сведения об отзыве. При наличии расширения соответствующий спецификации CA **должен** помечать расширение как некритическое (non-critical).

```
name           id-ce-noRevAvail
OID            { id-ce 56 }
syntax         NULL (i.e. '0500'H is the DER encoding)
criticality    MUST be FALSE
```

Полагающаяся на сертификат сторона, не понимающая это расширение, может получить список отзыва сертификатов (Certificate Revocation List или CRL) от CA, но в этом CRL не будет записей для сертификатов с таким расширением.

3. Другие расширения сертификатов X.509

В сертификаты CA **недопустимо** включать расширение noRevAvail. В сертификаты с noRevAvail **недопустимо** включать расширения, указывающие репозитории CRL или местоположение ответчиков OCSP. При наличии noRevAvail в сертификате:

- **недопустимо** включать в него расширение с cA BOOLEAN = TRUE (см. параграф 4.2.1.9 в [RFC5280]);
- **недопустимо** включать в него расширение CRL Distribution Points (см. параграф 4.2.1.13 в [RFC5280]);
- **недопустимо** включать в него расширение Freshest CRL (см. параграф 4.2.1.15 в [RFC5280]);
- при наличии расширения Authority Information Access **недопустимо** включать в него id-ad-ocsp accessMethod (см. параграф 4.2.2.1 в [RFC5280]).

При нарушении любого из условий принимающая сертификат сторона **должна** считать его недействительным.

4. Проверка пути сертификации

В параграфе 6.1.3 [RFC5280] описана обработка сертификата в рамках процедур проверки пути сертификации. В частности, в п. (a)(3) сказано:

> В настоящий момент сертификат не отозван. Это можно определить из соответствующего CRL (параграф 6.3), сведений о состоянии или автономных (out-of-band) механизмов.

При наличии заданного здесь расширения noRevAvail или расширения ocsp-nocheck [RFC6960] п. (a)(3) пропускается, а ином случае выполняется определение статуса отзыва сертификата.

5. Модуль ASN.1

В этом разделе представлен модуль ASN.1 [X.680] для расширения сертификата noRevAvail с использованием соглашений [RFC5912] и [RFC6268].

```
<CODE BEGINS>
  NoRevAvailExtn
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0)
      id-mod-noRevAvail(110) }

  DEFINITIONS IMPLICIT TAGS ::=
  BEGIN

  IMPORTS
    EXTENSION
    FROM PKIX-CommonTypes-2009  -- RFC 5912
      { iso(1) identified-organization(3) dod(6) internet(1)
        security(5) mechanisms(5) pkix(7) id-mod(0)
        id-mod-pkixCommon-02(57) } ;

  -- Расширение сертификата noRevAvail

  ext-noRevAvail EXTENSION ::= {
    SYNTAX NULL
    IDENTIFIED BY id-ce-noRevAvail
    CRITICALITY { FALSE } }

  -- noRevAvail Certificate Extension OID

  id-ce OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) ds(5) 29 }

  id-ce-noRevAvail OBJECT IDENTIFIER ::= { id-ce 56 }

  END
<CODE ENDS>
```

6. Вопросы безопасночти

К этом документу применим одноимённый раздел [RFC5280].

При наличии в сертификате расширения noRevAvail проверки отзыва сертификата обходятся. Правила и практика CA **должны** гарантировать включение noRevAvail лишь в те сертификаты, где оно необходимо, поскольку некорректное использование или ошибочная конфигурация могут привести к доверию получающей стороны к отозванному сертификату. При обнаружении такого некорректного использования единственно возможным средством исправления является отзыв CA.

Некоторые приложения могут зависеть от сведений об отзыве или предполагать их доступность. Отсутствие таких сведений может потребовать изменения приложения или его настроек для обеспечения надлежащей безопасности и функциональности приложения.

Отсутствие сведений об отзыве ограничивает возможности принимающей сертификат стороны в плане обнаружения компрометации ключевого материала конечного субъекта или вредоносных сертификатов. Это также ограничивает возможности обнаружения CA, не обеспечивающих практику безопасности, правила выпуска сертификатов и контроль операций, заданные в политике сертификата (Certificate Policy или CP) или заявлении о практике сертификации (Certification Practices Statement или CPS) [RFC3647].

Поскольку отсутствие сведений об отзыве может ограничивать возможности обнаружения скомпрометированного ключевого материала и вредоносных сертификатов, принимающим сертификаты сторонам нужна уверенность в том, что CA следует практике безопасности, реализует правила выпуска сертификатов и надёжно управляет операциями. Доверяющие стороны могут оценивать надёжность CA, отслеживает их производительность и наблюдать за возможностями реагирования на инциденты.

6.1. Краткосрочные сертификаты

Для краткосрочных сертификатов сведения об отзыва не предоставляются, поскольку срок действия сертификата меньше времени, требуемого для обнаружения и распространения таких сведений. При некорректном использовании noRevAvail в сертификатах с недостаточно коротким сроком действия возникает возможность использования скомпрометированных секретных ключей. Поэтому важно до реализации расширения noRevAvail тщательно оценить и установить подходящие сроки действия сертификатов.

6.2. Долгосрочные сертификаты

Для некоторых долгосрочных сертификатов сведения об отзыва не предоставляются, поскольку срок действия сертификата никогда не заканчивается. Например, сертификаты IDevID [IEEE802.1AR] включаются в устройства при производстве и служат для получения сертификатов LDevID [IEEE802.1AR] в рабочей среде. В этом случае необходимо выбирать криптографические алгоритмы, которые считаются безопасными в течение предполагаемого срока использования устройств. Если применяется расширение noRevAvail, у CA не будет возможности уведомить доверяющие стороны о компрометации установленного при производстве ключевого материала.

7. Взаимодействие с IANA

Агентство IANA выделило приведённый в таблице 1 идентификатор объекта (OID) для модуля ASN.1 (раздел 5) в реестре SMI Security for PKIX Module Identifier (1.3.6.1.5.5.7.0).

Таблица 1.

Десятичное значение	***Описание***
110	id-mod-noRevAvail

8. Литература

8.1. Нормативные документы

[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>.

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

[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>.

[X.509-2019-TC2] ITU-T, "Information Technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks -- Technical Corrigendum 2", ITU-T Recommendation X.509-2019/Cor.2-2023, October 2023, <https://www.itu.int/rec/T-REC-X.509-202310-I!Cor2>.

[X.680] ITU-T, "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.680>.

[X.690] ITU-T, "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 8825-1-2021, February 2021, <https://www.itu.int/rec/T-REC-X.690>.

8.2. Дополнительная литература

[IEEE802.1AR] IEEE, "IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity", IEEE 802.1AR-2018, DOI 10.1109/IEEESTD.2018.8423794, 2 August 2018, <https://ieeexplore.ieee.org/document/8423794>.

[RFC2459] Housley, R., Ford, W., Polk, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, DOI 10.17487/RFC2459, January 1999, <https://www.rfc-editor.org/info/rfc2459>.

[RFC3281] Farrell, S. and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, DOI 10.17487/RFC3281, April 2002, <https://www.rfc-editor.org/info/rfc3281>.

[RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, DOI 10.17487/RFC3647, November 2003, <https://www.rfc-editor.org/info/rfc3647>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <https://www.rfc-editor.org/info/rfc5912>.

[RFC6268] Schaad, J. and S. Turner, "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)", RFC 6268, DOI 10.17487/RFC6268, July 2011, <https://www.rfc-editor.org/info/rfc6268>.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol — OCSP", RFC 6960, DOI 10.17487/RFC6960, June 2013, <https://www.rfc-editor.org/info/rfc6960>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/info/rfc8555>.

[X.509-1988] CCITT, "The Directory - Authentication Framework", CCITT Recommendation X.509-1988, November 1988, <https://www.itu.int/rec/T-REC-X.509-198811-S>.

[X.509-1997] ITU-T, "Information technology -- Open Systems Interconnection -- The Directory: Authentication framework", ITU-T Recommendation X.509-1997, August 1997, <https://www.itu.int/rec/T-REC-X.509-199708-S>.

[X.509-2000] ITU-T, "Information Technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509-2000, March 2000, <https://www.itu.int/rec/T-REC-X.509-200003-S>.

[X.509-2019] ITU-T, "Information Technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509-2019, October 2019, <https://www.itu.int/rec/T-REC-X.509-201910-I>.

Благодарности

Большое спасибо Erik Anderson за его усилия по созданию расширения сертификатов noRevAvail для использования с сертификатами открытых ключей конечных субъектов и сертификатами атрибутов.

Большое спасибо Corey Bonnell, Hendrik Brockhaus, Tim Hollebeek, Mike Ounsworth, Seo Suchan, Carl Wallace, Éric Vyncke, Paul Wouters (указаны в алфавитном порядке) за рецензиии и полезные комментарии.

Адреса авторов

Russ Housley
Vigil Security, LLC
Herndon, Virginia
United States of America
Email: housley@vigilsec.com

Tomofumi Okubo
DigiCert, Inc.
Fairfax, Virginia
United States of America
Email: tomofumi.okubo+ietf@gmail.com

Joseph Mandel
AKAYLA, Inc.
Tacoma, Washington
United States of America
Email: joe@akayla.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru