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

Abstract

X.509v3 public key certificates are profiled in RFC 5280. Short-lived certificates are seeing greater use in the Internet. The Certification Authority (CA) that issues these short-lived certificates do not publish revocation information because the certificate lifespan that is shorter than the time needed to detect, report, and distribute revocation information. Some long-lived X.509v3 public key certificates never expire, and they are never revoked. This specification defines the noRevAvail certificate extension so that a relying party can readily determine that the CA does not publish revocation information for the certificate, and it updates the certification path validation algorithm defined in RFC 5280 so that revocation checking is skipped when the noRevAvail certificate extension is present.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9608.

Table of Contents

1. Introduction

X.509v3 public key certificates [RFC5280] with short validity periods are seeing greater use in the Internet. For example, Automatic Certificate Management Environment (ACME) [RFC8555] provides a straightforward way to obtain short-lived certificates. In many cases, no revocation information is made available for short-lived certificates by the Certification Authority (CA). This is because short-lived certificates have a validity period that is shorter than the time needed to detect, report, and distribute revocation information. As a result, revoking a short-lived certificate that is used for authentication or key management is unnecessary and pointless. On the other hand, revoking a certificate associated with a long-lived signature, such as document signing or code signing, provides some important information about when a compromise was discovered.

Some long-lived X.509v3 public key certificates never expire, and they are never revoked. For example, a factory might include an IDevID certificate [IEEE802.1AR] to bind the factory-assigned device identity to a factory-installed public key. This identity might include the manufacturer, model, and serial number of the device, which never change. To indicate that a certificate has no well-defined expiration date, the notAfter date in the certificate validity period is set to "99991231235959Z" [RFC5280].

This specification defines the noRevAvail certificate extension so that a relying party can readily determine that the CA does not publish revocation information for the end-entity certificate, and it updates the certification path validation algorithm defined in [RFC5280] so that revocation checking is skipped when the noRevAvail certificate extension is present.

Note that the noRevAvail certificate extension provides similar functionality to the ocsp-nocheck certificate extension [RFC6960]. The ocsp-nocheck certificate extension is appropriate for inclusion only in certificates issued to Online Certificate Status Protocol (OCSP) responders, whereas the noRevAvail certificate extension is appropriate in any end-entity certificate for which the CA will not publish revocation information. To avoid disruption to the OCSP ecosystem, implementers should not think of the noRevAvail certificate extension a substitute for the ocsp-nocheck certificate extension; however, the noRevAvail certificate extension could be included in certificates issued to OCSP responders in addition to the ocsp-nocheck certificate extension.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all

capitals, as shown here.

1.2. ASN.1

X.509 certificates are generated using ASN.1 [X.680], using the Basic Encoding Rules (BER) and the Distinguished Encoding Rules (DER) [X.690].

1.3. History

In 1988, CCITT defined the X.509v1 certificate [X.509-1988].

In 1997, ITU-T defined the X.509v3 certificate and the attribute certificate [X.509-1997].

In 1999, the IETF first profiled the X.509v3 certificate for use in the Internet [RFC2459].

In 2000, ITU-T defined the noRevAvail certificate extension for use with attribute certificates [X.509-2000].

In 2002, the IETF first profiled the attribute certificate for use in the Internet [RFC3281], and this profile included support for the noRevAvail certificate extension.

In 2019, ITU-T published an update to ITU-T Recommendation X.509 [X.509-2019].

With greater use of short-lived certificates in the Internet, the recent Technical Corrigendum to ITU-T Recommendation X.509 [X.509-2019-TC2] allows the noRevAvail certificate extension to be used with public key certificates as well as attribute certificates.

2. The noRevAvail Certificate Extension

The noRevAvail extension, defined in [X.509-2019-TC2], allows a CA to indicate that no revocation information will be made available for this certificate.

This extension MUST NOT be present in CA public key certificates.

Conforming CAs MUST include this extension in certificates for which no revocation information will be published. When present, conforming CAs MUST mark this extension as non-critical.

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

A relying party that does not understand this extension might be able to find a Certificate Revocation List (CRL) from the CA, but the CRL will never include an entry for the certificate containing this extension.

3. Other X.509 Certificate Extensions

Certificates for CAs MUST NOT include the noRevAvail extension. Certificates that include the noRevAvail extension MUST NOT include certificate extensions that point to CRL repositories or provide locations of OCSP responders. If the noRevAvail extension is present in a certificate, then:

* The certificate MUST NOT also include the basic constraints certificate extension with the cA BOOLEAN set to TRUE; see Section 4.2.1.9 of [RFC5280].

* The certificate MUST NOT also include the CRL Distribution Points certificate extension; see Section 4.2.1.13 of [RFC5280].

* The certificate MUST NOT also include the Freshest CRL certificate extension; see Section 4.2.1.15 of [RFC5280].

* The Authority Information Access certificate extension, if present, MUST NOT include an id-ad-ocsp accessMethod; see Section 4.2.2.1 of [RFC5280].

If any of the above are violated in a certificate, then the relying party MUST consider the certificate invalid.

4. Certification Path Validation

Section 6.1.3 of [RFC5280] describes basic certificate processing within the certification path validation procedures. In particular, Step (a)(3) says:

> At the current time, the certificate is not revoked. This may be determined by obtaining the appropriate CRL (Section 6.3), by status information, or by out-of-band mechanisms.

If the noRevAvail certificate extension specified in this document is present or the ocsp-nocheck certificate extension [RFC6960] is present, then Step (a)(3) is skipped. Otherwise, revocation status determination of the certificate is performed.

5. ASN.1 Module

This section provides an ASN.1 module [X.680] for the noRevAvail certificate extension, and it follows the conventions established in [RFC5912] and [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) } ;

-- noRevAvail Certificate Extension

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. Security Considerations

The Security Considerations in [RFC5280] are relevant.

When the noRevAvail certificate extension is included in a certificate, all revocation checking is bypassed. CA policies and practices MUST ensure that the noRevAvail certificate extension is included only when appropriate, as any misuse or misconfiguration could result in a relying party continuing to trust a revoked certificate. When such misuse is discovered, the only possible remediation is the revocation of the CA.

Some applications may have dependencies on revocation information or assume its availability. The absence of revocation information may require modifications or alternative configuration settings to ensure proper application security and functionality.

The absence of revocation information limits the ability of relying parties to detect compromise of end-entity keying material or malicious certificates. It also limits their ability to detect CAs that are not following the security practices, certificate issuance policies, and operational controls that are specified in the Certificate Policy (CP) or the Certification Practices Statement (CPS) [RFC3647].

Since the absence of revocation information may limit the ability to detect compromised keying material or malicious certificates, relying parties need confidence that the CA is following security practices, implementing certificate issuance policies, and properly using operational controls. Relying parties may evaluate CA reliability, monitor CA performance, and observe CA incident response capabilities.

6.1. Short-Lived Certificates

No revocation information is made available for short-lived certificates because the certificate validity period is shorter than the time needed to detect, report, and distribute revocation information. If the noRevAvail certificate extension is incorrectly used for a certificate validity period that is not adequately short, it creates a window of opportunity for attackers to exploit a compromised private key. Therefore, it is crucial to carefully assess and set an appropriate certificate validity period before implementing the noRevAvail certificate extension.

6.2. Long-Lived Certificates

No revocation information is made available for some long-lived certificates that contain information that never changes. For example, IDevID certificates [IEEE802.1AR] are included in devices at the factory, and they are used to obtain LDevID certificates [IEEE802.1AR] in an operational environment. In this case, cryptographic algorithms that are expected to remain secure for the expected lifetime of the device need to be chosen. If the noRevAvail certificate extension is used, the CA has no means of notifying the relying party about compromise of the factory-installed keying material.

7. IANA Considerations

IANA has assigned the following object identifier (OID) for the ASN.1 module (see Section 5) within the "SMI Security for PKIX Module Identifier" (1.3.6.1.5.5.7.0) registry:

Decimal	Description
110	id-mod-noRevAvail

Table 1

8. References

8.1. Normative References

[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. Informative References

[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>.

Acknowledgements

Many thanks to Erik Anderson for his efforts to make the noRevAvail certificate extension available for use with public key end-entity certificates as well as attribute certificates.

Many thanks to (in alphabetical order) Corey Bonnell, Hendrik Brockhaus, Tim Hollebeek, Mike Ounsworth, Seo Suchan, Carl Wallace, ric Vyncke, and Paul Wouters for their review and insightful comments.

Authors' Addresses

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