Workgroup: Network Working Group
Internet-Draft:
draft-housley-lamps-norevavail-01
Published: 6 October 2023
Intended Status: Standards Track
Expires: 8 April 2024
Authors: R. Housley Vigil Security
T. Okubo DigiCert
J. Mandel SecureG

No Revocation Available for Short-lived X.509 Public Key Certificates

Abstract

Short-lived X.509v3 public key certificates as profiled in RFC 5280 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 The Certification Authority (CA) that issues these short-lived certificates do not publish revocation information because the certificate lifespan that is shorter than the time needed to detect, report, and distribute revocation information. 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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 April 2024.

Copyright Notice

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 short-lived certificates is unnecessary and pointless. 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.

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 an 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 that include the noRevAvail extension **MUST NOT** include certificate extensions that point to Certificate Revocation List (CRL) repositories or provide locations of Online Certificate Status Protocol (OCSP) Responders. If the noRevAvail extension is present in a certificate, then:

- 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].

4. 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(TBD) }

  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>
```

5. Security Considerations

The Security Considerations in [RFC5280] are relevant.

The precondition for applying this mechanism securely is that the certificate validity period is shorter than the time needed to detect, report and distribute revocation information. If the certificate validity period 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.

When the noRevAvail certificate extension is included in a certificate, all revocation checking is bypassed, even if the CRL Distribution Points, Freshest CRL, or Authority Information Access (pointing to an OCSP Responder) certificate extensions are present.

CA policies and practices **MUST** ensure that the noRevAvail is included only when appropriate, as any misuse or misconfiguration could result in a relying party continuing to trust a revoked certificate.

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.

Since the absence of revocation information may limit the ability to detect compromised 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, monitoring CA performance, and observe CA incident response capabilities.

6. IANA Considerations

For the ASN.1 Module in Section 4, IANA is requested to assign an object identifier (OID) for the module identifier. The OID for the module should be allocated in the "SMI Security for PKIX Module Identifier" registry (1.3.6.1.5.5.7.0).

7. Acknowledgements

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

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/rfc/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/rfc/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/rfc/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.509-201910-I>.

[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

[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/rfc/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/rfc/rfc3281>.

[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/rfc/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/rfc/rfc6268>.

[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/rfc/rfc8555>.

[X.509-1988] CCITT, "Series X: Data Communication Networks: Directory -- 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>.

Authors' Addresses

Russ Housley
Vigil Security, LLC
Herndon, VA,
United States of America

Email: housley@vigilsec.com

Tomofumi Okubo
DigiCert, Inc.
Fairfax, VA,
United States of America

Email: tomofumi.okubo+ietf@gmail.com

Joseph Mandel
SecureG Inc.
Tacoma, WA,
United States of America

Email: joe.mandel@secureg.io