

Network Working Group
Internet-Draft
Updates: 5280 (if approved)
Intended status: Standards Track
Expires: 4 April 2026

C. Bonnell
DigiCert, Inc.
伊藤 忠彦 (T. Ito)
SECOM CO., LTD.
大久保 智史 (T. Okubo)
Penguin Securities Pte. Ltd.
1 October 2025

Clarification to processing Key Usage values during CRL validation
draft-ietf-lamps-keyusage-crl-validation-02

Abstract

RFC 5280 defines the profile of X.509 certificates and certificate revocation lists (CRLs) for use in the Internet. This profile requires that certificates which certify keys for signing CRLs contain the key usage extension with the cRLSign bit asserted. Additionally, RFC 5280 defines steps for the validation of CRLs. While there is a requirement for CRL validators to verify that the cRLSign bit is asserted in the keyUsage extension of the CRL issuer's certificate, this document clarifies the requirement for relying parties to also verify the presence of the keyUsage extension in the CRL issuer's certificate. This check remediates a potential security issue that arises when relying parties accept a CRL which is signed by a certificate with no keyUsage extension, and therefore does not explicitly have the cRLSign bit asserted.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at <https://CBonnell.github.io/ietf-lamps-keyusage-crl-validation-clarification/draft-ietf-lamps-keyusage-crl-validation.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-ietf-lamps-keyusage-crl-validation/>.

Source for this draft and an issue tracker can be found at <https://github.com/CBonnell/lamps-keyusage-crl-validation-clarification>.

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 4 April 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Conventions and Definitions	3
3. The risk of trusting CRLs signed with non-certified keys . .	3
4. Checking the presence of the keyUsage extension	4
5. Security Considerations	5
6. IANA Considerations	5
7. Normative References	5
Acknowledgments	6
Authors' Addresses	6

1. Introduction

[RFC5280] defines the profile of X.509 certificates and certificate revocation lists (CRLs) for use in the Internet. Section 4.2.1.3 of [RFC5280] requires CRL issuer certificates to contain the keyUsage extension with the cRLSign bit asserted. However, the CRL validation algorithm specified in Section 6.3 of [RFC5280] does not explicitly include a corresponding check for the presence of the keyUsage certificate extension. This document updates [RFC5280] to require that check.

Section 3 describes the security concern that motivates this update.

Section 4 updates the CRL validation algorithm to resolve this concern.

2. Conventions and Definitions

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.

3. The risk of trusting CRLs signed with non-certified keys

In some Public Key Infrastructures, entities are delegated by Certification Authorities to sign CRLs. CRLs whose scope encompasses certificates that have not been signed by the CRL issuer are known as "indirect CRLs".

Certification Authorities delegate the issuance of CRLs to other entities by issuing to the entity a certificate that asserts the `cRLSign` bit in the `keyUsage` extension. The Certification Authority will then sign certificates that fall within the scope of the indirect CRL by including the `crlDistributionPoints` extension and specifying the distinguished name ("DN") of the CRL issuer in the `cRLIssuer` field of the corresponding distribution point.

The CRL issuer signs CRLs that assert the `indirectCRL` boolean within the `issuingDistributionPoint` extension.

Applications which consume CRLs follow the validation algorithm as specified in Section 6.3 of [RFC5280]. In particular, Section 6.3.3 contains the following step for CRL validation:

(f) Obtain and validate the certification path for the issuer of the complete CRL. The trust anchor for the certification path MUST be the same as the trust anchor used to validate the target certificate. If a `keyUsage` extension is present in the CRL issuer's certificate, verify that the `cRLSign` bit is set.

This step does not explicitly specify a check for the presence of the `keyUsage` extension itself.

Additionally, the certificate profile in [RFC5280] does not require the inclusion of the `keyUsage` extension in a certificate if the certified public key is not used for verifying the signatures of other certificates or CRLs. Section 4.2.1.3 of [RFC5280] says:

Conforming CAs MUST include this extension in certificates that contain public keys that are used to validate digital signatures on other public key certificates or CRLs.

The allowance for the issuance of certificates without the keyUsage extension and the lack of a check for the inclusion of the keyUsage extension during CRL verification can manifest in a security issue. A concrete example is described below.

1. The Certification Authority signs an end-entity CRL issuer certificate to subject X that certifies key A for signing CRLs by explicitly including the keyUsage extension and asserting the cRLSign bit in accordance with Section 4.2.1.3 of [RFC5280].
2. The Certification Authority signs one or more certificates that include the crlDistributionPoints extension with the DN for subject X included in the cRLIssuer field. This indicates that the CRL-based revocation information for these certificates will be provided by subject X.
3. The Certification Authority signs an end-entity certificate to subject X that certifies key B. This certificate contains no key usage extension, as the certified key is not intended to be used for signing CRLs and could be a “mundane” certificate of any type (e.g., S/MIME, document signing certificate where the corresponding private key is stored on the filesystem of the secretary’s laptop, etc.).
4. Subject X signs a CRL using key B and publishes the CRL at the distributionPoint specified in the crlDistributionPoints extension of the certificates signed in step 2.
5. Relying parties download the CRL published in step 4. The CRL validates successfully according to Section 6.3.3 of [RFC5280], as the CRL issuer DN matches, and the check for the presence of the cRLSign bit in the keyUsage extension is skipped because the keyUsage extension is absent.

4. Checking the presence of the keyUsage extension

To remediate the security issue described in Section 3, this document specifies the following amendment to step (f) of the CRL algorithm as found in Section 6.3.3 of [RFC5280].

OLD:

(f) Obtain and validate the certification path for the issuer of the complete CRL. The trust anchor for the certification path MUST be the same as the trust anchor used to validate the target certificate. If a keyUsage extension is present in the CRL issuer's certificate, verify that the cRLSign bit is set.

NEW:

(f) Obtain and validate the certification path for the issuer of the complete CRL. The trust anchor for the certification path MUST be the same as the trust anchor used to validate the target certificate. If the version of the CRL issuer's certificate is version 3 (v3), then verify that the keyUsage extension is present and verify that the cRLSign bit is set.

This change ensures that the CRL issuer's key is certified for CRL signing. However, this check is not performed if the CRL issuer's key is certified using a version 1 (v1) or version 2 (v2) X.509 certificate, as these versions do not have an extensions field where the key usage extension can be included.

5. Security Considerations

If a Certification Authority has signed certificates to be used for CRL verification but do not include the keyUsage extension in accordance with Section 4.2.1.3 of [RFC5280], then relying party applications that have implemented the modified verification algorithm as specified in this document will be unable to verify CRLs signed by the CRL issuer in question.

It is strongly RECOMMENDED that Certification Authorities include the keyUsage extension in certificates to be used for CRL verification to ensure that there are no interoperability issues where updated applications are unable to verify CRLs.

If it is not possible to update the profile of CRL issuer certificates, then the policy management authority of the affected Public Key Infrastructure SHOULD update the subject naming requirements to ensure that certificates to be used for different purposes contain unique DNSs.

6. IANA Considerations

This document has no IANA actions.

7. 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>>.

Acknowledgments

The authors would like to thank the participants on the LAMPS Working Group mailing list for their insightful feedback and comments. In particular, the authors extend sincere appreciation to Carl Wallace, David Hook, John Gray, Michael St. Johns, Mike Ounsworth, Russ Housley, Serge Mister, and Tomas Gustavsson for their reviews and suggestions, which greatly improved the quality of this document.

Authors' Addresses

Corey Bonnell
DigiCert, Inc.
Email: corey.bonnell@digicert.com

Tadahiko Ito
SECOM CO., LTD.
Email: tadahiko.ito.public@gmail.com

Additional contact information:

伊藤 忠彦
SECOM CO., LTD.

Tomofumi Okubo
Penguin Securities Pte. Ltd.
Email: tomofumi.okubo+ietf@gmail.com

Additional contact information:

大久保 智史

Penguin Securities Pte. Ltd.