Stream:	Internet Engineering Task Force (IETF)		
RFC:	10007		
Updates:	5280		
Category:	Standards Track		
Published:	June 2026		
ISSN:	2070-1721		
Authors:	C. Bonnell	伊藤 忠彦 (T. Ito)	大久保 智史 (T. Okubo)
	DigiCert, Inc.	セコム株式会社 *(SECOM CO., LTD.)*	*Penguin Securities Pte. Ltd.*

RFC 10007
Clarification to Processing Key Usage Values During Certificate Revocation List (CRL) Validation

Abstract

RFC 5280 defines the profile of X.509 certificates and Certificate Revocation Lists (CRLs) for use in the Internet. Section 4.2.1.3 of RFC 5280 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 RFC 5280 does not explicitly include a corresponding check for the presence of the `keyUsage` certificate extension. This document updates RFC 5280 to require that check.

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/rfc10007.

Copyright Notice

Table of Contents

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 (Section 6.3 of [RFC5280]) 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 (CAs) to sign CRLs. CRLs whose scope encompasses certificates that have not been signed by the CRL issuer are known as "indirect CRLs".

Applications that consume CRLs follow the validation algorithm as specified in Section 6.3 of [RFC5280]. In particular, Section 6.3.3 of [RFC5280] 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 key usage 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.

Similarly, the certificate profile in Section 4 of [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.

CAs can 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 CA will then sign certificates that fall within the scope of the indirect CRL by including the `crlDistributionPoints` extension (Section 4.2.1.13 of [RFC5280]) 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.

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 CA 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 CA 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 CA 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, a document signing certificate where the corresponding private key is stored on the file system of the secretary's laptop, etc.).
4. Subject `X` signs a CRL using key `B` and publishes the CRL at the `distributionPoint` field 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 specified 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 key usage 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 key usage 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 CA 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 **RECOMMENDED** that CAs 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 DNs.

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/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>.

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, Deb Cooley, John Gray, Michael StJohns, Mike Ounsworth, Mohamed Boucadair, 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
セコム株式会社

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

Additional contact information:

大久保 智史
Penguin Securities Pte. Ltd.