LAMPS
Internet-Draft
Intended status: Informational
Expires: 6 December 2025

P. Liu, Ed.
Pengcheng Laboratory
R. Fu, Ed.
China Unicom
R. Chen, Ed.
China Mobile
X. Liu, Ed.
Y. Zhang, Ed.
Pengcheng Laboratory

4 June 2025

Certificate Status Information Mechanism Description Updates to RFC 5280 draft-liu-lamps-mechanism-updates-to-rfc-5280-07

Abstract

The updates to RFC 5280 described in this document provide alignment with the 2013 specification for the X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP [RFC6960].

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 6 December 2025.

Copyright Notice

Table of Contents

1. Introduction

This document updates the "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC5280] to provide alignment with the 2013 specification for the X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP [RFC6960].

2. Requirements Language

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. Updates to RFC 5280

This section provides updates to several paragraphs of RFC 5280 [RFC5280]. For clarity, if the entire section is not replaced, then the original text and the replacement text are shown.

3.1. Update in “Overview of Approach” (Section 3.)

This update provides references for OCSP

OLD:

* CAs are responsible for indicating the revocation status of the certificates that they issue. Revocation status information may be provided using the Online Certificate Status Protocol (OCSP) [RFC2560], certificate revocation lists (CRLs), or some other mechanism. In general, when revocation status information is provided using CRLs, the CA is also the CRL issuer. However, a CA may delegate the responsibility for issuing CRLs to a different entity.

NEW:

* CAs are responsible for indicating the revocation status of the certificates that they issue. Revocation status information may be provided using the Online Certificate Status Protocol (OCSP) [RFC6960], certificate revocation lists (CRLs), or some other mechanism. In general, when revocation status information is provided using CRLs, the CA is also the CRL issuer. However, a CA may delegate the responsibility for issuing CRLs to a different entity.

3.2. Update in “Operational Protocols” (Section 3.4)

This update provides references for OCSP

OLD:

* Operational protocols are required to deliver certificates and CRLs (or status information) to certificate-using client systems. Provisions are needed for a variety of different means of certificate and CRL delivery, including distribution procedures based on LDAP, HTTP, FTP, and X.500. Operational protocols supporting these functions are defined in other PKIX specifications. These specifications may include definitions of message formats and procedures for supporting all of the above operational environments, including definitions of or references to appropriate MIME content types.

NEW:

* Operational protocols are required to deliver certificates and status information (CRLs or OCSP or other out-of-band means etc.,) to certificate-using client systems. Provisions are needed for a variety of different means of certificate and CRL or OCSP or out-of-band status delivery, including distribution procedures based on LDAP, HTTP, FTP, and X.500. Operational protocols supporting these functions are defined in other PKIX specifications. These specifications may include definitions of message formats and procedures for supporting all of the above operational environments, including definitions of or references to appropriate MIME content types.

3.3. Update in “Authority Information Access” (Section 4.2.2.1)

This update provides references for OCSP

OLD:

* The id-ad-ocsp OID is used when revocation information for the certificate containing this extension is available using the Online Certificate Status Protocol (OCSP) [RFC2560].

When id-ad-ocsp appears as accessMethod, the accessLocation field is the location of the OCSP responder, using the conventions defined in [RFC2560].

NEW:

* The id-ad-ocsp OID is used when revocation information for the certificate containing this extension is available using the Online Certificate Status Protocol (OCSP) [RFC6960].

When id-ad-ocsp appears as accessMethod, the accessLocation field is the location of the OCSP responder, using the conventions defined in [RFC6960].

3.4. Update in “CRL and CRL Extensions Profile” (Section 5)

This update provides references for OCSP

OLD:

* CRL issuers issue CRLs. The CRL issuer is either the CA or an entity that has been authorized by the CA to issue CRLs. CAs publish CRLs to provide status information about the certificates they issued. However, a CA may delegate this responsibility to another trusted authority.

NEW:

* CRL issuers issue CRLs. The CRL issuer is either the CA or an entity that has been authorized by the CA to issue CRLs and OCSP response. CAs publish CRLs or OCSP response to provide status information about the certificates they issued. However, a CA may delegate this responsibility to another trusted authority.

3.5. Update in “Basic Certificate Processing” (Section 6.1.3)

This update provides references for OCSP

OLD:

* (3) 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.

NEW:

* (3) At the current time, the certificate is not revoked. This may be determined by obtaining the appropriate CRL (Section 6.3), or by status information from OCSP [RFC6960], or by out-of-band mechanisms, such as Certificate Transparency.

3.6. Update in “Internationalized Names in Distinguished Names” (Section 7.1)

This update provides references for OCSP

OLD:

* Representation of internationalized names in distinguished names is covered in Sections 4.1.2.4, Issuer Name, and 4.1.2.6, Subject Name. Standard naming attributes, such as common name, employ the DirectoryString type, which supports internationalized names through a variety of language encodings. Conforming implementations MUST support UTF8String and PrintableString. RFC 3280 required only binary comparison of attribute values encoded in UTF8String, however, this specification requires a more comprehensive handling of comparison. Implementations may encounter certificates and CRLs with names encoded using TeletexString, BMPString, or UniversalString, but support for these is OPTIONAL.

NEW:

* Representation of internationalized names in distinguished names is covered in Sections 4.1.2.4, Issuer Name, and 4.1.2.6, Subject Name. Standard naming attributes, such as common name, employ the DirectoryString type, which supports internationalized names through a variety of language encodings. Conforming implementations MUST support UTF8String and PrintableString. RFC 3280 required only binary comparison of attribute values encoded in UTF8String, however, this specification requires a more comprehensive handling of comparison. Implementations may encounter certificates and CRLs or OCSP response with names encoded using TeletexString, BMPString, or UniversalString, but support for these is OPTIONAL.

3.7. Update in “Internationalized Domain Names in GeneralName ” (Section 7.2)

This update provides references for OCSP

OLD:

* Internationalized Domain Names (IDNs) may be included in certificates and CRLs in the subjectAltName and issuerAltName extensions, name constraints extension, authority information access extension, subject information access extension, CRL distribution points extension, and issuing distribution point extension. Each of these extensions uses the GeneralName type; one choice in GeneralName is the dNSName field, which is defined as type IA5String.

NEW:

* Internationalized Domain Names (IDNs) may be included in certificates and CRLs or OCSP response in the subjectAltName and issuerAltName extensions, name constraints extension, authority information access extension, subject information access extension, CRL distribution points extension, and issuing distribution point

extension, TBSRequest field. Each of these extensions or fields uses the GeneralName type; one choice in GeneralName is the dNSName field, which is defined as type IA5String.

3.8. Update in “Internationalized Electronic Mail Addresses” (Section 7.5)

This update provides references for OCSP

OLD:

* Electronic Mail addresses may be included in certificates and CRLs in the subjectAltName and issuerAltName extensions, name constraints extension, authority information access extension, subject information access extension, issuing distribution point extension, or CRL distribution points extension. Each of these extensions uses the GeneralName construct; GeneralName includes the rfc822Name choice, which is defined as type IA5String. To accommodate email addresses with internationalized domain names using the current structure, conforming implementations MUST convert the addresses into an ASCII representation.

NEW:

* Electronic Mail addresses may be included in certificates and CRLs or OCSP response in the subjectAltName and issuerAltName extensions, name constraints extension, authority information access extension, subject information access extension, issuing distribution point extension, or CRL distribution points extension, or TBSRequest field. Each of these extensions or fields uses the GeneralName construct; GeneralName includes the rfc822Name choice, which is defined as type IA5String. To accommodate email addresses with internationalized domain names using the current structure, conforming implementations MUST convert the addresses into an ASCII representation.

3.9. Update in “Informative References” (Section 11.2)

This update provides references for OCSP

OLD:

* [RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

NEW:

* [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, June 2013.

4. IANA Considerations

This memo includes no request to IANA.

5. Security Considerations

There is no more security concerns. OCSP including GeneralName elements was updated in 2013, the related updates to RFC 5280 described in this document provide alignment with the 2013 specification for the "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP" [RFC6960].

6. References

6.1. 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>.

[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>.

6.2. Informative References

[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>.

[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/rfc/rfc6960>.

Authors' Addresses

Penghui Liu (editor)
Pengcheng Laboratory
No.2 Xingke 1 Street
Shenzhen
518055
China
Email: liuph@pcl.ac.cn

Yu Fu (editor)
China Unicom
No.1 Zhonghe Street
Beijing
100000
China
Email: fuy186@chinaunicom.cn

Meiling Chen (editor)
China Mobile
No.32 Xuanwumen West Street
Beijing
100000
China
Email: chenmeiling@chinamobile.com

Xiang Liu (editor)
Pengcheng Laboratory
No.2 Xingke 1 Street
Shenzhen
518055
China
Email: liux15@pcl.ac.cn

Yu Zhang (editor)
Pengcheng Laboratory
No.2 Xingke 1 Street
Shenzhen
518055
China
Email: zhangy08@pcl.ac.cn