Network Working Group
Internet-Draft
Intended status: Experimental
Expires: August 9, 2019

M. Pala
CableLabs

February 5, 2019

Online Certificate Status Protocol - Version 2 (OCSPv2)
draft-pala-ocspv2-00

Abstract

With the increase number of protocols and applications that rely on digital certificates to authenticate either the communication channel (TLS) or the data itself (PKIX), the need for providing an efficient revocation system is paramount. Although the Online Certificate Status Protocol (OCSP) allows for efficient lookup of the revocation status of a certificate, the distribution of this information via HTTP (or very rarely) HTTPS is not particularly efficient for high volume websites without incurring in high distribution costs (e.g., CDN).

In particular, this specification defines a new set of messages (i.e., OCSPv2 Request and OCSPv2 Response) that address the inefficiencies of OCSPv1 by (a) providing range-based responses to optimize (reduce) the number of pre-computed responses required by a CA, and (b) allowing the inclusion of other (certificate chain) responses in the same response for round-trip and caching optimization.

The deployment of OCSPv2 to validate the status of a certificate is meant to lower the costs of providing revocation services and increase the efficiency of the service, thus allowing for short-lived responses (i.e., hours instead of days).

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 August 9, 2019.

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

Introduction

3. Limitations of previous versions of OCSPv1

Explains the limitations of OCSPv1 when it comes to efficiency.

4. Protocol Overview

Provides a description of the protocol with particular emphasis on the different approach (range vs. one-by-one).

5. The OCSPv2 Request

The OCSPv2 Request.

6. The OCSPv2 Response

The OCSPv2 Response.

7. IANA Considerations

No special considerations for IANA.

8. Security Considerations

Several security considerations need to be explicitly considered for the system administrators and application developers to understand the weaknesses of the overall architecture.

9. Acknowledgments

The authors would like to thank everybody who provided insightful comments and helped in the definition of the deployment considerations. Last but not least, the authors would like to thank all the people that expressed interest in implementing support for this proposal.

10. 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>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC4501] Josefsson, S., "Domain Name System Uniform Resource Identifiers", RFC 4501, DOI 10.17487/RFC4501, May 2006, <https://www.rfc-editor.org/info/rfc4501>.

[RFC5019] Deacon, A. and R. Hurst, "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments", RFC 5019, DOI 10.17487/RFC5019, September 2007, <https://www.rfc-editor.org/info/rfc5019>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[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>.

[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>.

Author's Address

Massimiliano Pala
CableLabs
858 Coal Creek Cir
Louisville, CO 80027
USA

Email: director@openca.org
URI: http://www.linkedin.com/in/mpala