Network Working Group
Internet-Draft
Intended status: Experimental
Expires: May 17, 2018

M. Pala
CableLabs

November 13, 2017

# OCSP over DNS (ODIN)
# draft-pala-odin-03

## 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 how to distribute OCSP responses over DNS and how to define OCSP-over-DNS URLs in certificates. The use of the DNS system to distribute such information is meant to lower the costs of providing revocation services (by leveraging the distributed nature of DNS cache) and increase the availability of revocation information (by providing an additional access method for revocation information retrieval).

## 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 May 17, 2018.

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

With the increasing number of highly available and highly utilized websites that require secure communications to protect the flow of information from the server to the client and the raising number of devices (IoT) that require strong authentication capabilities, the

need for a low-cost efficient approach to revocation information availability is crucial. The OCSP-over-DNS approach allows clients to determine the revocation status of digital certificates by optimizing the delivery mechanism for revocation information distribution to the client. This transport protocol can be used in lieu of or in addition to other PKIX endorsed transport mechanisms such as HTTP. This specification addresses the problem of providing a highly-available distributed system for OCSP responses [RFC6960].

This document defines the DNS records to be used for OCSP data publication and the definition of additional URLs for the AuthorityInfoAccess (AIA) extension in certificates.

## 3. Overview of existing solutions

Currently there are three main options to retrieve the revocation information associated with a digital certificates:

- by retrieving the freshest CRL
- by querying an OCSP responder for a freshly computed response
- by retrieving a pre-signed OCSP response from a web site (typically a content distribution network or CDN)
- by verifying pre-computed OCSP responses embedded (stapled) during the TLS negotiation (only in the TLS case, though)

All of these methods are based on the ability from the application to extract URLs out of the CRL (CrlDistributionPoint) or of the OCSP responder (AuthorityInfoAccess) from the certificate and query (almost uniquely via HTTP/HTTPS, although supported protocols might include LDAP and FTP) the corresponding server to retrieve the required data.

## 4. Scope Statement

This document focuses only on the definition of the required options for providing OCSP responses over DNS as an alternative transport protocol. The reliability and accessibility of DNS records (e.g., issues related to TCP vs. UDP DNS responses) are out of the scope of this document.

## 5. Protocol Overview

In order to validate a certificate using OCSP-over-DNS, the client should check the certificate for a DNS-based OCSP URI ("dns://") and then retrieve the OCSP response from the DNS. After this point, all

procedures are to be performed according to the OCSP protocol as defined in [RFC5019]. In particular, clients using OCSP-over-DNS, SHOULD:

1. Lookup the OCSP URI provided in the AIA of the certificate to be checked. The format of the URI comprises the id-ad-ocsp identifier and a base URL where the scheme (‘‘dns://’’) is used. The format of the full URI is discussed in Section 7.

2. Retrieve the DNS record carrying the required OCSP response.

## 6. The OCSP Resource Record (OCSPRR)

The OCSP DNS resource record (RR) is used to distribute a certificate’s revocation status to clients. The contents of the OCSP RR record are described in Section 6.1.

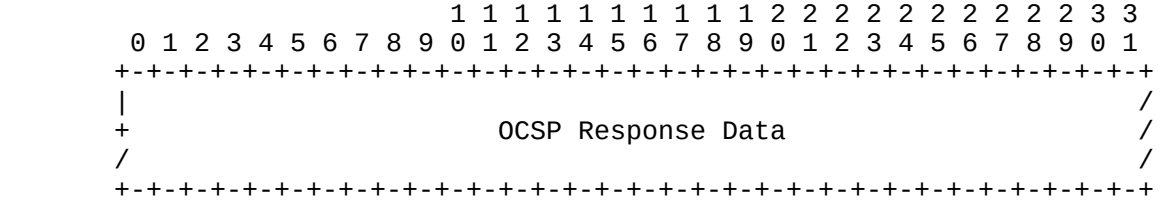
The type value for the OCSP RR type is defined in Section 6.2.

The OCSP RR is class independent.

The OCSP RR Time to Live (TTL) should not exceed the validity period of the OCSP response that is contained in the record.

### 6.1. The OCSP RDATA Wire Format

The RDATA for an OCSP RR consists of a single field which carries the DER encoded OCSP response for the identified certificate.




The OCSP response should contain only one response that refers to the certificate which contains that URL. Following this schema, the OCSP DNS URIs within the AIA extension SHOULD be unique for each certificate issued by a single CA.

### 6.2. The OCSP RRType

This document uses a new DNS RR type, OCSP, whose value (TBD) was allocated by IANA from the Resource Record (RR) TYPEs subregistry of the Domain Name System (DNS) Parameters registry.

### 6.3. Time Validity

The time validity should reflect the frequency of updates in revocation information (i.e., the TTL should not be set to expire after the OCSP response expiration). In practice, as an operational matter, operators SHOULD ensure that the records are published in a way that the TTL is low enough that they expire from caches before the OCSP response expiration.

## 7. Specifying DNS URLs for OCSP RR

The Authority Information Access extension, as defined in [RFC5280], provides information about the certificate in which the extension appears. In order to specify the availability of OCSP responses over DNS, Certification Authorities should use the OCSP accessMethod OID (id-ad-ocsp) and use "dns" as the transport.

Please note that, when using this accessMethod, the use of the dnsathority in the specified URI is discouraged as this might reduce the benefits coming from the caching infrastructure of DNS and, possibly, overload the referred DNS server.

### 7.1. URL definition

A DNS URL [RFC3986] begins with the protocol prefix "dns" and is defined by the following grammar, following the ABNF notation defined in [RFC5234].

```
dnsurl = scheme COLON SLASH SLASH [target]
        [QUESTION [ TYPE=rr_type ]
        ; target: is the dns entry for
        ; the lookup operation.
        ; rr_type: is the type of record
        ; to be retrieved. If not specified,
        ; the default type is OCSPRR

scheme  = "dns"

SLASH       = %x2F              ; forward slash ("/")
COLON       = %x3A              ; colon (":")
QUESTION    = %x3F              ; question mark ("?")
TYPE        = "type"            ; the keyword ("type")
```

Although this specification does not mandate for any specific format for the <target> component of the DNS URL, some examples are provided in Section 7.3 with the intent to illustrate, not define, the format.

### 7.2. DNS URL Processing

In order to process the OCSP DNS URLs in a certificate, clients have to extract the <target> and, if provided, the <type> of record from the URL. After that, client MUST query for the specified record. When the ‘‘OCSPRR’’ record type is used, the returned value MUST contain the DER encoded OCSP response related to the certificate that the client is going to validate.

### 7.3. OCSPRR URI Examples

When using the issuing CA’s DNS sub-domain in the DNS URL, the hex (or decimal) representation of the certificate’s serialNumber MAY be used as the hostname of the DNS URL. When combined with the specific sub-domain of the issuing CA this provides a unique entry that can be easily queried. For example, given that the sub-domain of the issuing CA is "ca1.example.com", the resulting URL in the issued certificate can be constructed as follows:

dns://04A3E45534A1B5.ca1.example.com?type=OCSPRR

Because the serialNumber of a certificate is guaranteed to be unique within a (single) CA, different Certification Authorities MUST use different sub-domains when using this publication algorithm to avoid collisions across different CAs.

However, in some environments, the serial number that will be used in the certificate to be issued can not be pre-fetched and embedded in the AIA’s DNS URL entry. In this case, the use of a monotonically increasing or random integer number can be used instead.

In any case, it is important to notice that since the DNS entry is to be used "AS IS" by the relying party that wants to fetch the OCSP response by using the DNS URL, other techniques (e.g., the use of prefixes for different issuing CAs combined with high-resolution clock entries and small random or monotonic integer suffixes) can be implemented independently by different Certificate Service Providers.

## 8. IANA Considerations

This document uses a new DNS RR type, OCSPRR, whose value (TBD) MUST be allocated by IANA from the Resource Record (RR) TYPEs subregistry of the Domain Name System (DNS) Parameters registry.

## 9. 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. It is important to highlight, however, that the following considerations are inherently derived from the nature of the DNS infrastructure and that deployment of the DNSSEC protocol might provide an efficient protection against them.

By lacking the ability to authenticate the originating server directly, the DNS (not DNSSEC) protocol (both in TCP and UDP mode) is vulnerable to attacks where false responses are provided. Although all the information stored in the OCSP RR is signed, the data returned to the client could potentially be altered (e.g., by providing an empty or old response). This type of attack can lead to the application's inability to retrieve the revocation information, thus this approach is vulnerable to Denial of Service (DoS), Man-in-the-middle (MITM), and Reply Attacks.

As mentioned earlier, the deployment of DNSSEC can help in mitigating the described family of attacks by providing a mean for the client (or its resolver) to verify signatures of the DNS records themselves via the DNS keys. This said, the use of DNS (instead of DNSSEC) is equivalent, from a security considerations point of view, to today's deployment best practices for OCSP where pre-computed responses are delivered by CDNs via HTTP (not HTTPS). Therefore, the provisioning of OCSP responses via DNS does not lower or alter the security considerations that apply to the use of OCSP. Last but not least, because of the availability (in most cases) of independent DNS servers that an application can query, the use of multiple requests to different DNS servers (for the same DNS record) might be implemented as a mitigating measure in case an attack is suspected or detected.

## 10. Acknowledgments

The authors would like to thank everybody who provided insightful comments and helped in the definition of the deployment considerations. In particular, the authors would like to thank Scott A. Rea for his support. We also would like to thank DigiCert and the initial discussion and support for the initial idea. Last but not least, the authors would like to thank all the people that expressed interest in implementing support for this proposal.

## 11. 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
US

Email: m.pala@cablelabs.com
URI: http://www.linkedin.com/in/mpala