dnsop
Internet-Draft
Intended status: Best Current Practice
Expires: 9 March 2026

L. Pan

5 September 2025

Certificate Transparency (CT) information of DNS resolver
draft-pan-dnsop-ct-info-of-dns-resolver-00

Abstract

This document describes the Certificate Transparency (CT) information of the DNS resolver.

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 9 March 2026.

Table of Contents

1. Background

DNS resolver can support any encrypted DNS scheme, such as DNS over HTTPS (DoH) [RFC8484], DNS over TLS (DoT) [RFC7858], or DNS over QUIC (DoQ) [RFC9250].

Certificate hijacking allows attackers to impersonate a legitimate encrypted DNS resolver, see also [MisIssuedCF].

Certificate Transparency (CT) is to combat the certificate hijacking issue [RFC9162]. This document describes the CT information of the encrypted DNS resolver.

2. Terminology

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].

Basic terms used in this specification are defined in the documents [RFC1034], [RFC1035], [RFC9499], [RFC9606], [RFC9162].

3. IANA Considerations

3.1. DNS Resolver Information Keys Registration

[RFC9606] specifies a method for DNS resolvers to publish information about themselves.

IANA has created a new registry called "DNS Resolver Information Keys" [IANA-DNS].

This document adds a new DNS Resolver Information Key: CT, to present the CT information of the encrypted DNS resolver.

Name: CT

Value: 1

Meaning: The value indicates that the certificate of the encrypted DNS resolver contains embedded SCTs.

Reference: RFC 9162

Name: CT

Value: 2

Meaning: The value indicates that the encrypted DNS resolver supports the transparency_info TLS extension.

Reference: RFC 9162

4. Security Considerations

DNS clients can get trustworthy DNS resolver information through DNSSEC query or out-of-band configuration.

Suppose the DNS clients find the CT value in the trustworthy DNS resolver information. In that case, they can mandate the CT validation in the encrypted communication channel setup process with the encrypted DNS resolver.

5. Acknowledgements

Thanks to all in the DNSOP mailing list.

6. References

6.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[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>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC9162] Laurie, B., Messeri, E., and R. Stradling, "Certificate Transparency Version 2.0", RFC 9162, DOI 10.17487/RFC9162, December 2021, <https://www.rfc-editor.org/info/rfc9162>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/info/rfc9250>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/info/rfc9499>.

[RFC9606] Reddy.K, T. and M. Boucadair, "DNS Resolver Information", RFC 9606, DOI 10.17487/RFC9606, June 2024, <https://www.rfc-editor.org/info/rfc9606>.

6.2. Informative References

[IANA-DNS] IANA, "Domain Name System (DNS) Parameters", n.d., <https://www.iana.org/assignments/dns-parameters/>.

[MisIssuedCF] Goodin, D., "Mis-issued certificates for 1.1.1.1 DNS service pose a threat to the Internet", 2025, <https://arstechnica.com/security/2025/09/mis-issued-certificates-for-1-1-1-1-dns-service-pose-a-threat-to-the-internet/>.

Author’s Address

Lanlan Pan
Guangdong
China
Email: abbypan@gmail.com