Moving DNSSEC Lookaside Validation (DLV) to Historic Status
draft-ietf-dnsop-obsolete-dlv-02

Abstract

   This document obsoletes DNSSEC lookaside validation (DLV) and
   reclassifies RFCs 4431 and 5074 as Historic. Furthermore, this
   document updates RFC 6698 by excluding the DLV resource record from
   certificates, and updates RFC 6840 by excluding the DLV registries
   from the trust anchor selection.

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 3, 2020.

Table of Contents

1. Introduction

   DNSSEC Lookaside Validation (DLV) was introduced to assist with the
   adoption of DNSSEC [RFC4033] [RFC4034] [RFC4035] in a time where the
   root zone and many top level domains (TLDs) were unsigned, to help
   entities with signed zones under an unsigned parent zone, or that
   have registrars that don't accept DS records. The root zone is
   signed since July 2010 and as of May 2019, 1389 out of 1531 TLDs have
   a secure delegation from the root; thus DLV has served its purpose
   and can now retire.

2. Terminology

   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
   [RFC2119] and [RFC8174].

3. Discussion

   One could argue that DLV is still useful because there are still some
   unsigned TLDs and entities under those zones will not benefit from
   signing their zone. However, keeping the DLV mechanism also has
   disadvantages:

   o It reduces the pressure to get the parent zone signed.

   o It reduces the pressure on registrars to accept DS records.

   o It complicates validation code.

In addition, not every validator actually implemented DLV (only BIND 9 and Unbound) so even if an entity can use DLV to set up an alternate path to its trust anchor, its effect is limited. Furthermore, there was one well-known DLV registry (dlv.isc.org) and that has been deprecated (replaced with a signed empty zone) on September 30, 2017. With the absence of a well-known DLV registry service it is unlikely that there is a real benefit for the protocol on the Internet nowadays.

One other possible reason to keep DLV is to distribute trust anchors for private enterprises. There are no known uses of DLV for this.

All things considered it is probably not worth the effort of maintaining the DLV mechanism.

4. Moving DLV to Historic Status

There are two RFCs that specify DLV:

1. RFC 4431 [RFC4431] specifies the DLV resource record.

2. RFC 5074 [RFC5074] specifies the DLV mechanism for publishing trust anchors outside the DNS delegation chain and how validators can use them to validate DNSSEC-signed data.

This document moves both RFC 4431 [RFC4431] and RFC 5074 [RFC5074] to Historic status. This is a clear signal to implementers that the DLV resource record and the DLV mechanism SHOULD NOT be implemented or deployed.

4.1. Documents that reference the DLV RFCs

The RFCs that are being moved to Historic status are referenced by a couple of other documents. The sections below describe what changes when the DLV RFCs have been reclassified as Historic.

4.1.1. Documents that reference RFC 4431

One RFC makes reference to RFC 4431 [RFC4431].

4.1.1.1. RFC 5074

RFC 5074 [RFC5074], "DNSSEC Lookaside Validation (DLV)" describes the DLV mechanism itself, and is being moved to Historic status too.

4.1.2. Documents that reference RFC 5074

Three RFCs make reference to RFC 5074 [RFC5074].

4.1.2.1. RFC 6698

RFC 6698, "The DNS-Based Authentication of Named Entities (DANE)
Transport Layer Security (TLS) Protocol: TLSA" [RFC6698] specifies:

DNSSEC forms certificates (the binding of an identity to a key) by
combining a DNSKEY, DS, or DLV resource record with an associated
RRSIG record. These records then form a signing chain extending from
the client's trust anchors to the RR of interest.

This document updates RFC 6698 to exclude the DLV resource record
from certificates.

4.1.2.2. RFC 6840

RFC 6840, "Clarifications and Implementation Notes for DNS Security
(DNSSEC)" [RFC6840] says that when trust anchors come from different
sources, a validator may choose between them based on the perceived
reliability of those sources. But in reality this does not happen in
validators (both BIND 9 and Unbound have a option for a DLV trust
anchor that can be used solely as a fallback).

This document updates RFC 6840 to exclude the DLV registries from the
trust anchor selection.

4.1.2.3. RFC 8198

RFC 8198, "Aggressive Use of DNSSEC-Validated Cache" [RFC8198] only
references RFC 5074 because aggressive negative caching was first
proposed there.

5. IANA Considerations

IANA should update the annotation of the DLV RR type (code 32769) to
"Obsolete" in the DNS Parameters registry.

6. Security considerations

When the DLV mechanism goes away, zones that rely on DLV for their
validation will be treated as insecure. The chance that this
scenario actually occurs is very low, since no well-known DLV
registry exists.

7. Acknowledgements

   Ondrej Sury for initial review.

8. 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>.

   [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "DNS Security Introduction and Requirements",
              RFC 4033, DOI 10.17487/RFC4033, March 2005,
              <https://www.rfc-editor.org/info/rfc4033>.

   [RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "Resource Records for the DNS Security Extensions",
              RFC 4034, DOI 10.17487/RFC4034, March 2005,
              <https://www.rfc-editor.org/info/rfc4034>.

   [RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "Protocol Modifications for the DNS Security
              Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005,
              <https://www.rfc-editor.org/info/rfc4035>.

   [RFC4431] Andrews, M. and S. Weiler, "The DNSSEC Lookaside
              Validation (DLV) DNS Resource Record", RFC 4431,
              DOI 10.17487/RFC4431, February 2006,
              <https://www.rfc-editor.org/info/rfc4431>.

   [RFC5074] Weiler, S., "DNSSEC Lookaside Validation (DLV)", RFC 5074,
              DOI 10.17487/RFC5074, November 2007,
              <https://www.rfc-editor.org/info/rfc5074>.

   [RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication
              of Named Entities (DANE) Transport Layer Security (TLS)
              Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August
              2012, <https://www.rfc-editor.org/info/rfc6698>.

   [RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and
              Implementation Notes for DNS Security (DNSSEC)", RFC 6840,
              DOI 10.17487/RFC6840, February 2013,
              <https://www.rfc-editor.org/info/rfc6840>.

   [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>.

   [RFC8198] Fujiwara, K., Kato, A., and W. Kumari, "Aggressive Use of
              DNSSEC-Validated Cache", RFC 8198, DOI 10.17487/RFC8198,
              July 2017, <https://www.rfc-editor.org/info/rfc8198>.

Authors' Addresses

   Matthijs Mekking
   ISC
   Netherlands

   Email: matthijs@isc.org

   Dan Mahoney
   ISC
   950 Charter St
   Redwood City, CA 94063
   USA

   Email: dmahoney@isc.org