RFC 8749
Moving DNSSEC Lookaside Validation (DLV) to Historic Status

Abstract

This document retires 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8749.

Copyright Notice

Table of Contents

1. Introduction

DNSSEC Lookaside Validation (DLV) was introduced to assist with the adoption of DNSSEC [RFC4033] [RFC4034] [RFC4035] in a time when the root zone and many top-level domains (TLDs) were unsigned. DLV allowed entities with signed zones under an unsigned parent zone or entities with registrars that did not accept DS records to publish trust anchors outside of the normal DNS delegation chain. The root zone was signed in 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. 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. Discussion

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

- • It reduces the pressure to get the parent zone signed.
- • It reduces the pressure on registrars to accept DS records.
- • 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), which was 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 being moved to Historic status are referenced by a couple of other RFCs. The sections below describe the changes to those documents due to the DLV RFCs being 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 ("DNSSEC Lookaside Validation (DLV)") [RFC5074] describes the DLV mechanism itself. This document moves RFC 5074 [RFC5074] to Historic status as well.

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 [RFC6698] 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] states 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 an option for a DLV trust anchor that can be used solely as a fallback).

This document updates RFC 6840 [RFC6840] 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 [RFC5074] because aggressive negative caching was first proposed there.

5. IANA Considerations

IANA has updated the annotation of the DLV RR type (code 32769) to "Obsolete" in the "Domain Name System (DNS) Parameters" registry.

6. Security Considerations

Once the DLV mechanism is retired, 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. 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>.

Acknowledgements

Authors' Addresses

W. (Matthijs) Mekking
ISC
Netherlands
Email: matthijs@isc.org

Dan Mahoney
ISC
United States of America
Email: dmahoney@isc.org