Internet Engineering Task Force S. Bortzmeyer

Internet-Draft Afnic

Intended status: Informational 11 September 2024

Expires: 15 March 2025

DNS Resolver Information Key for DNSSEC Validation

draft-bortzmeyer-resinfo-dnssecval-00

Abstract

This document specifies a DNS Resolver Information Key

(RFC 9606) for DNSSEC validation capability, "dnssecval".

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 15 March 2025.

Copyright Notice

Copyright (c) 2024 IETF Trust and the persons identified as the

document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal

Provisions Relating to IETF Documents (https://trustee.ietf.org/

license-info) in effect on the date of publication of this document.

Please review these documents carefully, as they describe your rights

and restrictions with respect to this document. Code Components

extracted from this document must include Revised BSD License text as

described in Section 4.e of the Trust Legal Provisions and are

provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 2

1.1. Requirements Language . . . . . . . . . . . . . . . . . . 2

2. The key . . . . . . . . . . . . . . . . . . . . . . . . . . . 2

3. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 2

4. Security Considerations . . . . . . . . . . . . . . . . . . . 3

5. References . . . . . . . . . . . . . . . . . . . . . . . . . 3

5.1. Normative References . . . . . . . . . . . . . . . . . . 3

5.2. Informative References . . . . . . . . . . . . . . . . . 3

Acknowledgements . . . . . . . . . . . . . . . . . . . . . . . . 4

Author's Address . . . . . . . . . . . . . . . . . . . . . . . . 4

1. Introduction

[RFC9606] specifies a DNS resource record (RR) type RESINFO to allow resolvers to

publish information about their capabilities and policies. Each information is unambiguously identified with a key.

. Keys are maintained in an IANA

registry called "DNS Resolver Information

Keys" under the "Domain Name System (DNS) Parameters" registry group.

This specification adds a new key to indicate that a

resolver validates with DNSSEC [RFC4033][RFC4034][RFC4035]. Such key may be used, for example, by a DNS client to prefer resolvers that enable

DNSSEC validation.

1.1. 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.

2. "dnssecval" Key

The name of the key is "dnssecval", for "DNSSEC validating

[resolver]". The presence of this key indicates that the DNS

resolver validates all answers with DNSSEC [RFC4033] [RFC4034]

[RFC4035]. Note that, per the rules for the keys defined in

Section 6.4 of [RFC6763], if there is no '=' in a key, then it is a

boolean attribute, simply identified as being present, with no value.

A resolver that announces this capability in a RESINFO record MAY

add DNSSEC-specific EDE (Extended DNS Error Codes, [RFC8914]) to the

value of the "exterr" key [RFC9606], e.g., “Unsupported DNSKEY Algorithm”, “Unsupported DS Digest Type”, and “DNSSEC Bogus”. Refer to the “Extended DNS Error Codes” registry for a definitive list of these EDEs.

"dnssecval" is an optional attribute.

3. IANA Considerations

This document requests IANA to add the following new key to the "DNS Resolver Information Keys" registry under the under the “Domain Name System (DNS) Parameters” registry group.

+==========+=====================================+==============+

| Name | Description | Reference |

+==========+=====================================+==============+

| dnssecval| The presence of the key name |This\_Document |

| | indicates that DNSSEC validation is | |

| | enabled. | |

+----------+-------------------------------------+--------------+

4. Security Considerations

DNSSEC is a very important tool for the security of the DNS and,

Therefore, it is important for users to know in advance whether the

resolver they consider supports DNSSEC. It would be better to

assume that every resolver validates (thus rendering this document

useless) but it is not the case today.

The security considerations discussed in Section 7 of [RFC9606] apply.

5. References

5.1. 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>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service

Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013,

<https://www.rfc-editor.org/info/rfc6763>.

[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>.

[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>.

5.2. Informative References

[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>.

[RFC8914] Kumari, W., Hunt, E., Arends, R., Hardaker, W., and D.

Lawrence, "Extended DNS Errors", RFC 8914,

DOI 10.17487/RFC8914, October 2020,

<https://www.rfc-editor.org/info/rfc8914>.

Acknowledgements

My cat did nothing to help.

Author's Address

Stéphane Bortzmeyer

Afnic

7 avenue du 8 mai 1945

78280 Guyancourt

France

Email: bortzmeyer+ietf@nic.fr

URI: https://www.afnic.fr/