

**DNSSEC Resource Record Should Include AAAA  
draft-byrne-v6ops-dnssecaaaa-00**

Abstract

DNS64 is a widely deployed technology allowing hundreds of millions of IPv6-only hosts to reach IPv4-only resources. DNSSEC is a technology used to validate the authenticity of information in the DNS. Currently, there are scenarios where DNS64 and DNSSEC do not work well together. This document states that any DNSSEC signed resources record should include a native IPv6 resource record as the most complete and expedient path to solve any deployment conflict with DNS64 and DNSSEC.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/1id-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

Copyright and License Notice

Copyright (c) 2018 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2</a>	The Conflict Between DNS64 and DNSSEC . . . . .	<a href="#">3</a>
<a href="#">3</a>	Resolving the DNS64 and DNSSEC Conflict by Requiring AAAA . . . . .	<a href="#">3</a>
<a href="#">3</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">4</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">5</a>	Informative References . . . . .	<a href="#">4</a>
	Authors Address . . . . .	<a href="#">4</a>



## **1 Introduction**

DNS64 [[RFC6147](#)] has documented scenarios where DNS64 may negatively interact with DNSSEC [[RFC4033](#)]. This document simply states the most complete and expedient path to avoid any negative interactions is for the DNSSEC signed resources to always include IPv6 AAAA resources records. As stated in [[RFC6540](#)], IPv6 [[RFC8200](#)] is not optional and failing to support IPv6 may result in failure to communicate on the internet, especially when DNSSEC signed IPv4-only resources are present.

## **2. The Conflict Between DNS64 and DNSSEC**

DNS64 is a key part of widely deployed IPv6-only transition mechanism such as 464XLAT [[RFC6877](#)] and Happy Eyeballs Version 2 [[RFC8305](#)]. Currently, hundreds of millions of host rely on DNS64 for access to the internet. A core function of DNS64 is generating an inauthentic AAAA DNS record when an authentic AAAA DNS record for a host is not available from the authoritative nameserver. DNSSEC's fundamental feature is detecting and denying inauthentic DNS resource records. While [[RFC6147](#)] outlines how DNS64 and DNSSEC may work in harmony, the preconditions may not always exist for harmony to be achieved

## **3. Resolving the DNS64 and DNSSEC Conflict by Requiring AAAA**

DNS64 and DNSSEC are both important components of the current and future internet. The limitation for how these protocols interact is unlikely to changes. Deploying DNSSEC and IPv6 are both commonly achievable for a typical internet system operator using their own systems or using a third party service. The resolution to the DNS64 and DNSSEC conflict is to simply deploy both IPv6 and DNSSEC in tandem. Deploying DNSSEC signed IPv4 resources records without matching IPv6 records is a risk and not recommend. Ultimately, this guidance is simply restating [[RFC6540](#)] that IPv6 is mandatory for all internet systems.



### **3 Security Considerations**

DNSSEC is a good security practice. Providing AAAA DNSSEC signed records wherever a DNSSEC signed A record is used ensures the most effective use of DNSSEC.

### **4 IANA Considerations**

None.

### **5 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>>.
- [RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", [RFC 6147](#), DOI 10.17487/RFC6147, April 2011, <<https://www.rfc-editor.org/info/rfc6147>>.
- [RFC6540] George, W., Donley, C., Liljenstolpe, C., and L. Howard, "IPv6 Support Required for All IP-Capable Nodes", [BCP 177](#), [RFC 6540](#), DOI 10.17487/RFC6540, April 2012, <<https://www.rfc-editor.org/info/rfc6540>>.
- [RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", [RFC 6877](#), DOI 10.17487/RFC6877, April 2013, <<https://www.rfc-editor.org/info/rfc6877>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, [RFC 8200](#), DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>. Authors' Addresses
- [RFC8305] Schinazi, D. and T. Pauly, "Happy Eyeballs Version 2: Better Connectivity Using Concurrency", [RFC 8305](#), DOI 10.17487/RFC8305, December 2017, <<https://www.rfc-editor.org/info/rfc8305>>.

#### Authors Address

Cameron Byrne  
T-Mobile USA  
Bellevue, WA  
United States of America  
Email: Cameron.Byrne@T-Mobile.com

