

DNSOP  
Internet-Draft  
Updates: [4035](#) (if approved)  
Intended status: Informational  
Expires: September 20, 2018

P. Wouters, Ed.  
Red Hat  
L. Xia  
Huawei  
W. Hardaker  
USC/ISI  
March 19, 2018

The Delegation\_Only DNSKEY flag  
draft-pwouters-powerbind-00

## Abstract

This document introduces a new DNSKEY flag called DELEGATION\_ONLY that indicates that the particular zone will never sign zone data across a label. That is, every dot is considered a zone cut and must have its own (signed) delegation.

## 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 <http://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 September 20, 2018.

## Copyright 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

Internet-Draft

Delegation Only DNSKEYs

March 2018

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="#">2</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	The Deep Link State problem . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Limiting the scope of a DNSKEY RRset to Delegation Only . . .	<a href="#">3</a>
<a href="#">5.</a>	Parental Transparency . . . . .	<a href="#">4</a>
<a href="#">6.</a>	Marking the root key DELEGATION_ONLY . . . . .	<a href="#">4</a>
<a href="#">7.</a>	Marking TLD keys DELEGATION_ONLY . . . . .	<a href="#">4</a>
<a href="#">8.</a>	Migrating to/from DELEGATION_ONLY . . . . .	<a href="#">5</a>
<a href="#">9.</a>	Thirdparty usage . . . . .	<a href="#">5</a>
<a href="#">10.</a>	Operational Considerations . . . . .	<a href="#">5</a>
<a href="#">11.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">12.</a>	IANA Considerations . . . . .	<a href="#">6</a>
<a href="#">13.</a>	Acknowledgements . . . . .	<a href="#">6</a>
<a href="#">14.</a>	References . . . . .	<a href="#">6</a>
<a href="#">14.1.</a>	Normative References . . . . .	<a href="#">6</a>
<a href="#">14.2.</a>	Informative References . . . . .	<a href="#">6</a>
	Authors' Addresses . . . . .	<a href="#">7</a>

## [1.](#) Introduction

The DNS Security Extensions [DNSSEC] use public key cryptography to create an hierarchical trust base with the DNSSEC root public key at the top, followed by TLD keys one level underneath. While the root and TLD zones are asumed to be almost exclusively delegation-only zones, there is currently no method to force these zones to actually behave as a delegation-only zone. This creates an attractive target for malicious use of these zones - either by their owners or through coercion. For example, the DNSSEC root key could remove a delegation for "example.com" and sign an A record and TLSA record for "example.com", overriding the authority of "com" and "example.com". If such a change is done in a targetted attack, such an attack is near impossible to detect and log in any kind of transparency audit log.

A new DNSKEY flag is introduced to signify a public commitment by the zone to state that the zone will never sign any DNS data that traverses a single label and if any such signed data is encountered by validating resolvers, that this data should be interpreted as

BOGUS. All delegations in the zone will have at most one added label. Any data found that does not comply to this commitment MUST be interpreted as BOGUS.

## [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 [RFC 2119](#) [[RFC2119](#)].

## [3.](#) The Deep Link State problem

The hierarchical model of DNSSEC ([\[RFC4033\]](#), [\[RFC4034\]](#) and [\[RFC4035\]](#)) comes with the property that a zone at one point in the hierarchy can define, and therefor override, everything in the DNS tree from their level and below. The DNSSEC root key could ignore the NS records for ".org" and "example.org" and could place a record "www.example.org" directly into its own zone, with the corresponding RRSIG signed by the root key itself. Even if resolvers would defend against this attack by not allowing RRSIG's to span across a zone cut, the root zone operator (or any level higher in the hierarchy than the target victim) could briefly remove the NS and DS records, and create a "legitimate" DNS entry for "www.example.org" that traverses a label, but has no zonecuts. The attacker could then publish DNS records such as A/AAAA records, but also records used for authentication, such as TLSA, SMIME, OPENPGPKEY, SSHP or IPSECKEY records.

Exposing such targetted attacks requires a transparency audit setup that needs to log all signed DNS data to prove that data signed by a parental DNSKEY was out of the ordinary. The very distributed nature of DNS makes such transparency logs prohibitively expensive and near impossible to operate. Additionally, it would expose all zone data to any public log operators, thereby exposing all DNS data to a public archive. This data could then be used for other malicious purposes.

## [4.](#) Limiting the scope of a DNSKEY RRset to Delegation Only

This document introduces a new DNSKEY flag called DELEGATION\_ONLY. When this flag is set on the DNSKEY with SEP bit set (KSK), the zone

commits to not sign any data that crosses a label down in the hierarchy. This forces the parent in the hierarchy to only sign NS and DS records for all (non-glue) records regarding its child zones. It will no longer be able to ignore (or briefly delete, see below) the child delegation and publish data across the label by pretending the next label is not a zone cut.

For such a parent to take over data that belongs to its child zone, it has two choices. It can (temporarily) remove its own DNSKEY DELEGATION\_ONLY flag or it can replace the NS and DS records of its child zone with its own keys for which it has the private key so it

can sign DNS data that belongs to its child zone. Both of these actions cannot be hidden, thus exposing such malicious behaviour.

## [5.](#) Parental Transparency

A parent zone, such as the root zone or a TLD, that has committed to the DELEGATION\_ONLY flag can no longer make an exception for a single delegated zone without switching its entire zone by removing the DELEGATION\_ONLY flag. This action would be highly visible, and for some domains such as the root or TLDs, require human interaction to notify the stake holders.

Removing the DELEGATION\_ONLY flag from a DNSKEY requires that the zone signals a new DS record to its parent, as changing any DNSKEY flag changes the DS record data for that corresponds to its DNSKEY.

In the case of the root key, it would require updating out-of-band root key meta information and/or perform an [\[RFC5011\]](#) style rollover to the same key with updated DNSKEY flags. Due to the timings of such a rollover, it would take at least 30 days for validating resolvers to pick this policy change. It would also be a highly visible event.

Replacing the NS and DS records of a child zone can still be done in a targeted attack mode, but these events are something that can be easily tracked by a transparency infrastructure similar to what is now in use for the WebPKI using [\[RFC6962\]](#)(bis). With client implementations of transparency, this would be logged and become visible to the owner of the child zone and would expose the parent's

malicious action.

## 6. Marking the root key DELEGATION\_ONLY

Once the root key is marked with a DELEGATION\_ONLY flag, and resolver software and [RFC 5011](#) compliant resolver setups have rolled into such a key, all TLDs are ensured that the root key can no longer be abused to create "deep link" data. Until the root key sets this bit, software MAY imply this bit is always set as this is the current mode of operation of the root zone.

## 7. Marking TLD keys DELEGATION\_ONLY

Even before the root key has been marked with DELEGATION\_ONLY, TLDs can already signal their own willingness to commit to formally being DELEGATION\_ONLY zones. Any changes of that state in a TLD DNSKEY would require those TLDs to submit a new DS record to the root, and could therefor only be done in a transparent and auditable way - preventing abuse and coercion.

Wouters, et al.

Expires September 20, 2018

[Page 4]

---

Internet-Draft

Delegation Only DNSKEYs

March 2018

## 8. Migrating to/from DELEGATION\_ONLY

There might be multiple DNSKEYs with the SEP bit set in a zone. For the purpose of declaring a zone as DELEGATION\_ONLY, only those DNSKEY's that have a corresponding DS record at the parent MUST be considered. If multiple DS records appear at the parent, some of which point to DNSKEY's with and some of which point to DNSKEY's without the DELEGATION\_ONLY flag set, the zone MUST be considered DELEGATION\_ONLY. This situation will occur when a zone is rolling its DNSKEY key at the same time as it is committing to a DELEGATION\_ONLY zone (or the reverse).

## 9. Thirdparty usage

The DELEGATION\_ONLY flag has a strong overlap in functionality with the Public Suffix List as both signal a formal split of authority between parent and child.

## 10. Operational Considerations

Setting or unsetting the DELEGATION\_ONLY flag must be handled like any other Key Signing Key rollover procedure, with the appropriate

wait times to give resolvers the chance to update their caches.

Some TLDs offer a service where small domains can be hosted in-zone at the TLD zone itself. In that case, the TLD MUST NOT set the DELEGATION\_ONLY flag. Another solution for such TLDs is to create delegations for these child zones with the same or different DNSKEY as used in the parent zone itself.

If a zone is publishing glue records for a number of zones, and the zone that contains the authoritative records for this glue is deleted, a resigning of the zone will make this orphaned glue authoritative within the zone. However, with the DELEGATION\_ONLY bit set, this (signed) DNSSEC data will be considered BOGUS as it violations the commitment to only delegate. This may impact domains that depended on this unsigned glue.

For example, if "example.com" and "example.net" use NS records pointing to "ns.example.net", then if "example.net" is deleted from the ".net" zone, and the previously unsigned glue of "ns.example.net" is now signed by the ".net" zone, the "example.com" zone will lose its NS records and fail to resolve.

The bind DNS software has an option called "delegation\_only zones" which is an option that means something completely different. It refers to ignoring wildcard records in specified zones that are deemed delegation-only zones.

## [11.](#) Security Considerations

There are no negative security impacts of using the DELEGATION\_ONLY bit?

## [12.](#) IANA Considerations

This document defines a new DNSKEY flag, the DELEGATION\_ONLY flag, whose value [TBD] has been allocated by IANA from the DNSKEY FLAGS registry.

## [13.](#) Acknowledgements

The author wishes to thank Thomas H. Ptacek for his insistence on this matter.

Thanks to the following IETF participants: Viktor Dukhovni, Shumon Huque, Geoff Huston, Rick Lamb and Sam Weiler.

## 14. References

### 14.1. 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>>.
- [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>>.
- [RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, [RFC 5011](#), DOI 10.17487/RFC5011, September 2007, <<https://www.rfc-editor.org/info/rfc5011>>.

### 14.2. 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>>.

Wouters, et al.

Expires September 20, 2018

[Page 6]

---

Internet-Draft

Delegation Only DNSKEYs

March 2018

- [RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", [RFC 6962](#), DOI 10.17487/RFC6962, June 2013, <<https://www.rfc-editor.org/info/rfc6962>>.

### Authors' Addresses

Paul Wouters (editor)  
Red Hat

Email: pwouters@redhat.com

Liang Xia  
Huawei

Email: frank.xialiang@huawei.com

Wes Hardaker  
USC/ISI  
P.O. Box 382  
Davis, CA 95617  
US

Email: ietf@hardakers.net