

DNS Extensions Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: October 10, 2013

S. Crocker  
Shinkuro Inc.  
S. Rose  
NIST  
April 08, 2013

Signaling Cryptographic Algorithm Understanding in DNSSEC  
draft-ietf-dnsext-dnssec-algo-signal-10

## Abstract

The DNS Security Extensions (DNSSEC) were developed to provide origin authentication and integrity protection for DNS data by using digital signatures. These digital signatures can be generated using different algorithms. This draft sets out to specify a way for validating end-system resolvers to signal to a server which digital signature and hash algorithms they support. The proposed extensions allow the signaling of new algorithm uptake in client code to allow zone administrators to know when it is possible to complete an algorithm rollover in a DNSSEC signed zone.

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

## 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 October 10, 2013.

## Copyright Notice

Internet-Draft

Algorithm-Signal

April 2013

Copyright (c) 2013 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="#">2</a>
2.	Signaling DNSSEC Algorithm Understood (DAU), DS Hash Understood (DHU) and NSEC3 Hash Understood (N3U) Using EDNS .	3
<a href="#">3.</a>	Client Considerations . . . . .	<a href="#">4</a>
<a href="#">3.1.</a>	Stub Resolvers . . . . .	<a href="#">5</a>
<a href="#">3.1.1.</a>	Validating Stub Resolvers . . . . .	<a href="#">5</a>
<a href="#">3.1.2.</a>	Non-Validating Stub Resolvers . . . . .	<a href="#">5</a>
<a href="#">3.2.</a>	Recursive Resolvers . . . . .	<a href="#">5</a>
<a href="#">3.2.1.</a>	Validating Recursive Resolvers . . . . .	<a href="#">5</a>
<a href="#">3.2.2.</a>	Non-validating Recursive Resolvers . . . . .	<a href="#">6</a>
<a href="#">4.</a>	Intermediate System Considerations . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Server Considerations . . . . .	<a href="#">6</a>
<a href="#">6.</a>	Traffic Analysis Considerations . . . . .	<a href="#">6</a>
<a href="#">7.</a>	IANA Considerations . . . . .	<a href="#">7</a>
<a href="#">8.</a>	Security Considerations . . . . .	<a href="#">7</a>
<a href="#">9.</a>	Normative References . . . . .	<a href="#">8</a>
	Authors' Addresses . . . . .	<a href="#">8</a>

## [1.](#) Introduction

The DNS Security Extensions (DNSSEC) [[RFC4033](#)], [[RFC4034](#)] and [[RFC4035](#)] were developed to provide origin authentication and integrity protection for DNS data by using digital signatures. Each digital signature RR (RRSIG) contains an algorithm code number. These algorithm codes tell validators which cryptographic algorithm was used to generate the digital signature.

Likewise, Delegation Signer (DS) RRs and NSEC3 RRs use a hashed value

as part of their RDATA and, like digital signature algorithms, these hash algorithms have code numbers. All three algorithm codes (RRSIG/DNSKEY, DS and NSEC3) are maintained in unique IANA registries.

This draft sets out to specify a way for validating end-system resolvers to tell a server in a DNS query which digital signature and/or hash algorithms they support. This is done using the new EDNS options specified below in [Section 2](#) for use in the OPT meta-RR [[I-D.ietf-dnsext-rfc2671bis-edns0](#)]. These three new EDNS option codes are all OPTIONAL to implement and use.

These proposed EDNS options serve to measure the acceptance and use of new digital signing algorithms. These signaling options can be used by zone administrators as a gauge to measure the successful deployment of code that implements newly deployed digital signature algorithm, DS hash and NSEC3 hash algorithm used with DNSSEC. A zone administrator is able to determine when to stop signing with a superseded algorithm when the server sees that a significant number of its clients signal that they are able to accept the new algorithm. Note that this survey may be conducted over the period of years before a tipping point is seen.

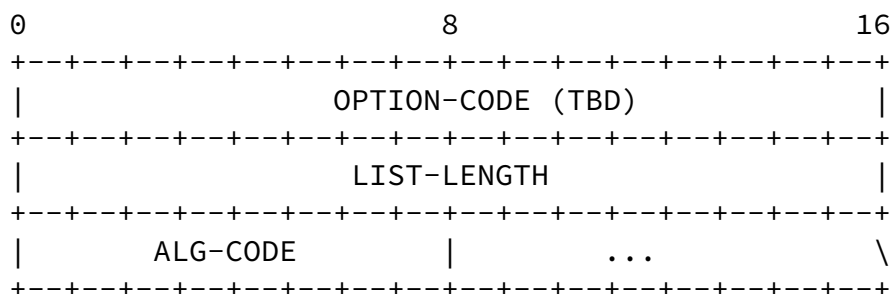
This draft does not seek to introduce another process for including new algorithms for use with DNSSEC. It also does not address the question of which algorithms are to be included in any official list of mandatory or recommended cryptographic algorithms for use with DNSSEC. Rather, this document specifies a means by which a client query can signal the set of algorithms and hashes which it implements.

## [2.](#) Signaling DNSSEC Algorithm Understood (DAU), DS Hash Understood (DHU) and NSEC3 Hash Understood (N3U) Using EDNS

The EDNS0 specification outlined in [[I-D.ietf-dnsext-rfc2671bis-edns0](#)] defines a way to include new options using a standardized mechanism. These options are contained in the RDATA of the OPT meta-RR. This document defines three new EDNS options for a client to signal which digital signature and/or hash algorithms the client supports. These options can be used independently of each other and MAY appear in any order in the OPT

RR. Each option code can appear only once in an OPT RR.

The figure below shows how each option is defined in the RDATA of the OPT RR specified in [[I-D.ietf-dnsext-rfc2671bis-edns0](#)]:



OPTION-CODE is the code for the given signaling option. They are:

- o DNSSEC Algorithm Understood (DAU) option for DNSSEC digital signing algorithms. Its value is fixed at TBD1.
- o DS Hash Understood (DHU) option for DS RR hash algorithms. Its value is fixed at TBD2.
- o NSEC3 Hash Understood (N3U) option for NSEC3 hash algorithms. Its value is fixed at TBD3.

LIST-LENGTH is the length of the list of digital signature or hash algorithm codes in octets. Each algorithm code occupies a single octet.

ALG-CODE is the list of assigned values of DNSSEC zone signing algorithms, DS hash algorithms, or NSEC3 hash algorithms (depending on the OPTION-CODE in use) that the client declares to be supported.

The order of the code values can be arbitrary and MUST NOT be used to infer preference.

If all three options are included in the OPT RR, there is a potential for the OPT RR to take up considerable size in the DNS message. However, in practical terms, including all three options is likely to take up 22-32 octets (average of 6-10 digital signature algorithms, 3-5 DS hash algorithms and 1-5 NSEC3 hash algorithms) including the EDNS option codes and option lengths in potential future examples.

### [3.](#) Client Considerations

A validating end-system resolver sets the DAU, DHU and/or N3U option, or combination thereof in the OPT meta-RR when sending a query. The validating end-system resolver MUST also set the DNSSEC-OK bit [[RFC4035](#)] to indicate that it wishes to receive DNSSEC RRs in the response.

Note that the PRIVATEDNS (253) and/or the PRIVATEOID (254) digital signature codes both cover a potentially wide range of algorithms and are likely not useful to a server. There is no compelling reason for a client to include these codes in its list of the DAU. Likewise, clients MUST NOT include RESERVED codes in any of the options. Likewise, a client is under no obligation to list every algorithm it implements and MAY choose to only list algorithms the client wishes to signal as understood.

Since the DAU, DHU and/or N3U options are only set in the query, if a client sees these options in the response, no action needs to be taken and the client MUST ignore the option values.

#### [3.1.](#) Stub Resolvers

Typically, stub resolvers rely on an upstream recursive server (or cache) to provide a response. So optimal setting of the DAU, DSU and N3U options depends on whether the stub resolver elects to perform its own validation.

##### [3.1.1.](#) Validating Stub Resolvers

A validating stub resolver already (usually) sets the DO bit [[RFC4035](#)] to indicate that it wishes to receive additional DNSSEC RRs (i.e. RRSIG RRs) in the response. Such validating resolvers SHOULD include the DAU, DHU and/or the N3U option(s) in the OPT RR when sending a query.

### [3.1.2.](#) Non-Validating Stub Resolvers

The DAU, DHU and N3U EDNS options MUST NOT be included by non-validating stub resolvers.

## [3.2.](#) Recursive Resolvers

### [3.2.1.](#) Validating Recursive Resolvers

A validating recursive resolver sets the DAU, DHU and/or N3U option(s) when performing recursion based on its list of algorithms and any DAU, DHU and/or N3U option lists in the stub client query. When the recursive server receives a query with one or more of the options set, the recursive server MUST set the algorithm list for any outgoing iterative queries for that resolution chain to a union of the stub client's list and the validating recursive resolver's list. For example, if the recursive resolver's algorithm list for the DAU option is (3, 5, 7) and the stub's algorithm list is (7, 8), the final DAU algorithm list would be (3, 5, 7, 8).

If the client did include the DO and CD bits, but did not include the DAU, DHU and/or N3U option(s) in the query, the validating recursive resolver MAY include the option(s) with its own list in full. If one or more of the options are missing, the validating recursive resolver MAY include the missing options with its own list in full.

Validating recursive resolvers MUST NOT set the DAU, DHU and/or N3U option(s) in the final response to the stub client.

### [3.2.2.](#) Non-validating Recursive Resolvers

Recursive resolvers that do not do validation MUST copy the DAU, DHU and/or N3U option(s) seen in received queries as they represent the wishes of the validating downstream resolver that issued the original query.

#### [4.](#) Intermediate System Considerations

Intermediate proxies [[RFC5625](#)] ([Section 4.4.2](#)) that understand DNS are RECOMMENDED to behave like a comparable recursive resolver when dealing with the DAU, DHU and N3U options.

#### [5.](#) Server Considerations

When an authoritative server sees the DAU, DHU and/or N3U option(s) in the OPT meta-RR in a request the normal algorithm for servicing requests is followed. The options MUST NOT trigger any special processing (e.g. RRSIG filtering in responses) on the server side.

If the options are present but the DNSSEC-OK (OK) bit is not set, the server does not do any DNSSEC processing, including any recording of the option(s).

If the server sees one (or more) of the options set with RESERVED values, the server MAY ignore recoding of those values.

Authoritative servers MUST NOT set the DAU, DHU and/or N3U option(s) on any responses. These values are only set in queries.

#### [6.](#) Traffic Analysis Considerations

Zone administrators that are planning or are in the process of a cryptographic algorithm rollover operation should monitor DNS query traffic and record the number of queries, the presence of the OPT RR in queries and the values of the DAU/DHU/N3U option(s) (if present). This monitoring can be used to measure the deployment of client code that implements (and signals) specific algorithms. Description of the techniques used to capture DNS traffic and measure new algorithm adoption is beyond the scope of this document.

Zone administrators that need to comply with changes to their organization's security policy (with regards to cryptographic algorithm use) can use this data to set milestone dates for performing an algorithm rollover. For example, zone administrators can use the data to determine when older algorithms can be phased out without disrupting a significant number of clients. In order to keep this disruption to a minimum, zone administrators should wait to complete an algorithm rollover until a large majority of clients signal that they recognize the new algorithm. This may be in the order of years rather than months.

Note that clients that do not implement these options are likely to be older implementations which would also not implement any newly deployed algorithm.

## 7. IANA Considerations

The algorithm codes used to identify DNSSEC algorithms, DS RR hash algorithms and NSEC3 hash algorithms have already been established by IANA. This document does not seek to alter that registry in any way.

This draft seeks to update the "DNS EDNS Options" registry by adding the DAU, DHU and N3U options and referencing this document. The code for these options are TBD1, TBD2 and TBD3 respectively.

## 8. Security Considerations

This document specifies a way for a client to signal its digital signature and hash algorithm knowledge to a cache or server. It is not meant to be a discussion on algorithm superiority. The signals are optional codes contained in the OPT meta-RR used with EDNS. The goal of these options are to signal new algorithm uptake in client code to allow zone administrators to know when it is possible to complete an algorithm rollover in a DNSSEC signed zone.

There is a possibility that an eavesdropper or server could infer the validator in use by a client by the presence of the AU options and/or algorithm code list. This information leakage in itself is not very useful to a potential attacker but it could be used to identify the

validator or narrow down the possible validator implementations in



use by a client, which could have a known vulnerability that could be exploited by the attacker.

## 9. Normative References

- [I-D.ietf-dnsext-rfc2671bis-edns0]  
Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", [draft-ietf-dnsext-rfc2671bis-edns0-10](#) (work in progress), December 2012.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", [RFC 4033](#), March 2005.
- [RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", [RFC 4034](#), March 2005.
- [RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", [RFC 4035](#), March 2005.
- [RFC5625] Bellis, R., "DNS Proxy Implementation Guidelines", [BCP 152](#), [RFC 5625](#), August 2009.

## Authors' Addresses

Steve Crocker  
Shinkuro Inc.  
5110 Edgemoor Lane  
Bethesda, MD 20814  
USA

EMail: [steve@shinkuro.com](mailto:steve@shinkuro.com)

Scott Rose  
NIST  
100 Bureau Dr.  
Gaithersburg, MD 20899  
USA

Phone: +1-301-975-8439  
EMail: [scottr.nist@gmail.com](mailto:scottr.nist@gmail.com)



