Signaling Cryptographic Algorithm Understanding in DNSSEC
draft-crocker-dnssec-algo-signal-06

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 cryptographic algorithms they support.

Requirements Language

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].

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 15, 2010.

Copyright Notice

Copyright (c) 2010 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
Table of Contents

1. Introduction ................................................. 3
2. Signaling Algorithm Understood (AU) Using EDNS ............ 3
3. Client Considerations ......................................... 4
   3.1. Recommendations for Stub Clients ......................... 4
   3.2. Recursive Cache Considerations ......................... 5
4. Intermediate Middlebox Considerations ...................... 5
5. Server Considerations .......................................... 5
6. Traffic Analysis Considerations ............................... 5
7. IANA Considerations ........................................... 6
8. Security Considerations ....................................... 6
9. Normative References ......................................... 6
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 help validators identify which cryptographic algorithm was used to generate the digital signature.

This draft sets out to specify a way for validating end-system resolvers to signal to a server which cryptographic algorithms they support in a DNSSEC response. This is done using the EDNS attribute values in the OPT meta-RR [RFC2671].

This proposed EDNS option serves to measure the acceptance and use of new digital signing algorithms. This algorithm signaling option can be used by zone administrators as a gauge to measure the successful deployment of code that implements a newly deployed digital signature algorithm used with DNSSEC. A zone administrator may be able to determine when to stop serving the old algorithm when the server sees that all or almost all of its clients signal that they are able to accept the new algorithm.

This draft does not seek to include a formal 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 a set of algorithms it implements.

2. Signaling Algorithm Understood (AU) Using EDNS

The ENDSO specification outlined in [RFC2671] 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 seeks to define a new EDNS0 option for a client to signal which algorithms the client supports.
The figure below shows how the signally attribute is defined in the RDATA of the OPT RR specified in [RFC2671]:

```
0                       8                      16
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                 OPTION-CODE (TBD)             |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                 OPTION-LENGTH                 |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|       ALG-CODE        |        ...            \
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

OPTION-CODE is the code for the Algorithm Understood (AU) option. Its value is fixed at TBD.

OPTION-LENGTH is the length of the data of the attribute in octets. DNSSEC algorithm codes are 1 octet long so this value is the number of octets.

ALG-CODE is the list of assigned values of DNSSEC zone signing algorithms that the client indicates as understood. The values MUST be in descending order of preference, with the most preferred algorithm first. For example, if a validating client implements RSA/SHA-1, RSA/SHA-256 and prefers the latter, the value of ALG-CODE would be: 8 (RSA/SHA-256), 5 (RSA/SHA-1).

3. Client Considerations

A validating end-system resolver sets the AU option in the OPT meta-RR when sending a query. The validating end-system resolver sets the value(s) in the order of preference, with the most preferred algorithm first as described in section 2. The 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 when including the PRIVATEDNS (253) and/or the PRIVATEOID (254) codes, the client only indicates that it understands one or more private algorithms but does not indicate which algorithms.

3.1. Recommendations for Stub Clients

Typically, stub resolvers rely on an upstream recursive server (or cache) to provide a response; any algorithm supportence on the stub resolver’s side could be overruled by the upstream recursive server. The AU EDNS option is NOT RECOMMENDED for non-validating stub clients.
The exception to the above is that validating stub resolvers which set the CD bit in queries MAY set the AU option. In the most common scenario, the validating stub indicates that it wishes to perform its own validation (via the CD bit) and may therefore wish to indicate which cryptographic algorithm(s) it supports.

3.2. Recursive Cache Considerations

DNSSEC validating recursive caches MAY set the AU option on any outgoing query from the cache when performing recursion on behalf of a non-DNSSEC aware stub client. If the stub indicates it is DNSSEC-aware, but does not set the AU option in the query, the DNSSEC validating recursive cache SHOULD NOT set the AU option to avoid conflicts.

Forwarders that do not do validation or caching SHOULD copy the AU option seen in received queries as they represent the wishes of the validating downstream resolver that issued the original query.

4. Intermediate Middlebox Considerations

Intermediate middleboxes SHOULD copy the AU option seen in queries from end system resolvers. If the system is validating, it SHOULD also check for the presence of the CD bit in the query. If present, the intermediate middlebox SHOULD copy the AU option as seen in the query. If not set or if the DNSSEC-OK bit is not set, then the validating intermediate middlebox MAY chose to ignore the AU option in the query and MAY include its own preference as the AU option.

5. Server Considerations

When an authoritative server sees the AU option in the OPT meta-RR in a request the normal algorithm for servicing requests is followed.

If the AU option is present but the DNSSEC-OK bit is not set, then the authoritative server ignores the ALG-CODE list and does not include any additional DNSSEC RRs in the response.

6. Traffic Analysis Considerations

Zone administrators that are planning or are in the process of completing a cryptographic algorithm rollover operation should monitor DNS query traffic and record the values of the AU option in queries. This monitoring can measure the deployment of client code that implements (and signals) certain algorithms. Exactly how to capture DNS traffic and measure new algorithm adoption is beyond the scope of this document.
Zone administrators can use this data to set plans for starting an algorithm rollover and when older algorithms can be phased out without disrupting the majority 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 understand the new algorithm. Note that clients that do not implement the AU option may be older implementations which would also not implement any newly deployed algorithm.

7. IANA Considerations

The algorithm codes used to identify DNSSEC algorithms has already been established by IANA. This document does not seek to alter that registry in any way.

This draft seeks to update the "DNS EDNS0 Options" registry by adding the AU option and referencing this document. The code for the option should be TBD.

8. Security Considerations

This document specifies a way for a client to signal its digital signature algorithm preference to a cache or server. It is not meant to be a discussion on algorithm superiority. The signal is an optional code contained in the OPT meta-RR used with EDNS0. The goal of this option is 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.

9. Normative References


Authors’ Addresses

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

EMail: steve@shinkuro.com

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

Phone: +1-301-975-8439
EMail: scottr.nist@gmail.com