Signaling Cryptographic Algorithm Understanding in DNSSEC
draft-crocker-dnssec-algo-signal-07

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

Copyright Notice

Table of Contents

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 tells validators which cryptographic algorithm
   was used to generate the digital signature. Authentication across
   delegation boundries is maintained by storing a hash of a subzone's
   key in the parent zone stored in a Delegation Signer (DS) RR. These
   DS RR's contain a second code number to identify the hash algorithm
   used to contruct the DS RR.

   This draft sets out to specify a way for validating end-system
   resolvers to tell a server which cryptographic and/or hash algorithms
   they support in a DNS query. 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 and hash 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 or hash 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 another process for including new
   algorithms for use with DNSSEC (see . 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 ENDS0 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 defines
   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)              |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |            DIGITAL-SIG-LIST-LENGTH            |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |      ALG-CODE         |        ...            \
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |               DS-HASH-LIST-LENGTH             |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |      HASH-CODE        |        ...            \
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```
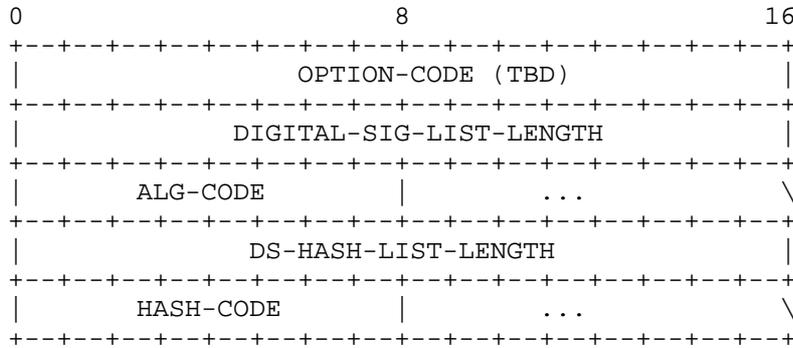
OPTION-CODE is the code for the Algorithm Understood (AU) option.
Its value is fixed at TBD.

DIGITAL-SIG-LIST-LENGTH is the length of the list of digital
signature algorithms 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
SHOULD 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).

DS-HASH-LIST-LENGTH is the length of the list of hash algorithms in
octets. DNSSEC DS hash codes are 1 octet long so this value is the
number of octets.

HASH-CODE is the list of assigned values of DNSSEC DS hash algorithms
that the client indicates as understood. Like the ALG-CODE above,
the values SHOULD be in descending order of preference, with the most
preferred algorithm first.

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(s) 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 support 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

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2671]   Vixie, P., "Extension Mechanisms for DNS (EDNS0)",
               RFC 2671, August 1999.

   [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.

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