Network Working Group
draft-ietf-dnsind-sigalgopt-00.txt

R. Austein
On Sabbatical
P. Vixie
Internet Software Consortium
October 1999

# DNS SIGALGOPT

## Status of this document

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

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/ietf/1id-abstracts.txt>

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

Distribution of this document is unlimited. Please send comments to the namedroppers@internic.net mailing list.

## Abstract

This document describes a mechanism for conserving packet space in a DNS response message in the presence of multiple DNSSEC signature algorithms.

## Motivation and Scope

DNSSEC [DNSSEC] specifies a general framework for attaching cryptographic signatures to DNS resource records. The framework includes provisions for multiple signature protocols, possibly even on a per-name basis. While this open-ended framework is good and useful, it poses a problem when multiple signature protocols are in use and DNS message sizes are limited by the underlying UDP transport packet size. EDNS0 [EDNS0] provides a way to specify a larger

payload size, but this still does not entirely solve the problem for large RRsets. Worse, in cases where multiple signature algorithms generate a response packet so large that it must be truncated, the signatures that fit into the truncated response will be useless if the resolver doesn't know how to verify signatures generated with that algorithm.

This note proposes a way for a resolver to indicate which signature algorithms it understands to a name server in the form of an ordered list. When this mechanism is in use, the name server can conserve packet space by (a) not sending signatures with algorithms that the resolver will not understand, and (b) not sending multiple signatures for the same resource records.

## Mechanism

[DNSSEC] SIG RRs include a one-octet code indicating the algorithm associated with a particular signature. The SIGALGOPT option defined below allows the resolver to specify an ordered list of signature algorithms using the same one-octet codes that DNSSEC uses.

SIGALGOPT is encoded n the variable RDATA part of the OPT pseudo-RR in the DNS request (see [EDNS0]).

The OPTION-CODE for SIGALGOPT is [TBD].

The OPTION-DATA for SIGALGOPT is an ordered list of the one-octet codes used by DNSSEC.

If the SIGALGOPT option in a query specifies multiple signature algorithms and signatures using more than one of those algorithms are available in the zone, the server must respond with the signatures corresponding to the first algorithm on the SIGALGOPT list that matches, omitting any signatures corresponding to the remaining algorithms.

We have deliberately not provided a mechanism to return all the matching signatures, because the purpose of the SIGALGOPT mechanism is to minimize packet size. If the resolver wants to see all available signatures, it should just leave off the SIGALGOPT option entirely.

## Security Considerations

Good question. What horrible things could a bad guy do by creating/altering/deleting SIGALGOPT? Are any of the possible attacks more interesting than denial of service?

## IANA Considerations

SIGALGOPT will need an option code.

The signature algorithm codes themselves are borrowed from DNSSEC and do not create any new issues for IANA.

## References

[DNSSEC] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[DNS-CONCEPTS] Mockapetris, P., "Domain names - concepts and facilities", RFC 1034, November 1987.

[DNS-IMPLEMENTATION] Mockapetris, P., "Domain names - implementation and specification", RFC 1035, November 1987.

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

## Author's addresses:

Rob Austein
On Sabbatical
sra@hactrn.net

Paul Vixie
Internet Software Consortium
950 Charter Street
Redwood City, CA 94063
+1 650 779 7001
vixie@isc.org