Workgroup: Network Working Group
Internet-Draft:
draft-hoffman-more-private-algs-01
Updates: 4034 (if approved)
Published: 24 March 2022
Intended Status: Standards Track
Expires: 25 September 2022
Authors: P. Hoffman
ICANN

More Private Algorithms for DNSSEC

Abstract

RFC 4034 allocates one value in the IANA registry for DNSSEC algorithm numbers for private algorithms. That may be too few for experimentation where multiple yet-to-be-assigned algorithms are used. This document assigns seven more values for this use case.

This document is currently maintained at https://github.com/paulehoffman/draft-hoffman-more-private-algs. Issues and pull requests are welcomed. If the document is later adopted by a working group, a new repository will likely be created.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Section A.1 of [RFC4034] assigns value 253 as "Private [PRIVATEDNS]". Section A.1.1 describes this value:

> Algorithm number 253 is reserved for private use and will never be assigned to a specific algorithm. The public key area in the DNSKEY RR and the signature area in the RRSIG RR begin with a wire encoded domain name, which MUST NOT be compressed. The domain name indicates the private algorithm to use, and the remainder of the public key area is determined by that algorithm. Entities should only use domain names they control to designate their private algorithms.

In the coming years, it is likely that there will be experimentation with new DNSSEC signing algorithms for post-quantum cryptography. At the time this document is written, it is possible that there will be many such algorithms in experimental use at the same time. If that comes to pass, it would be useful to have a handful of private use algorithms to use at the same time, such as for experimenting with zones that will have multiple simultaneous signing algorithms.

This document updates [RFC4034] to add seven more private use algorithms. Unlike private use algorithm 253, there is no restriction on the public key area in the DNSKEY RR and the signature area in the RRSIG RR. Thus, there are no domain names embdded in the public key or signature like there are with private use algorithm 253. This update brings the total number of private use algorithms that use the same format to eight.

2. IANA Considerations

This document requests that IANA allocate seven additional values, 245 through 251, in the "DNS Security Algorithm Numbers" registry (https://www.iana.org/assignments/dns-sec-alg-numbers/).

3. Security Considerations

Allocating private use values does not cause any significant security considerations.

4. Normative References

[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>.

Author's Address

Paul Hoffman
ICANN

Email: paul.hoffman@icann.org