Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 12 October 2026

P. Hoffman
ICANN

10 April 2026

Variable Length DNSKEY and RRSIG Types For Testing draft-hoffman-variable-length-nonparticipating-00

Abstract

Some DNS operators want to test what will happen when DNSSEC algorithms that have large DNSKEY records, RRSIG records, or both, are deployed. For example, they may want to see the effects on TCP retries due to large DNSSEC records. This document defines a new DNS security algorithm, named "Variable Length Nonparticipating", for such testing. To prevent possible security issues with this new algorithm, signatures with this algorithm never participate in DNSSEC validation.

This document might never become an RFC; it's purpose is just to register the new algorithm in the IANA "DNS Security Algorithm Numbers" registry.

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 https://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 12 October 2026.

Copyright Notice

Table of Contents

1. Introduction

The DNS community is considering new signing algorithms based on post-quantum cryptography for DNSSEC ([RFC9364]). Post-quantum algorithms generally have larger public key sizes, larger signatures, or both. The algorithms under consideration have different security parameters that result in different sized keys and signatures.

This document defines a new DNS security algorithm, named "Variable Length Nonparticipating", that offers no security, just the ability to create keys and signatures of desired sizes for testing. To ensure the security of the DNS, the signatures created by the Variable Length Nonparticipating algorithm do not participate in any DNSSEC validation calculations. This allows a zone operator to add DNSKEY and RRSIG records to existing RRsets to test larger sizes while still allowing zones to be validated correctly with their existing keys and signtures.

The term "TBD1" is used throughout this document to indicate the algorithm number assigned by IANA for this algorithm. See Section 4 for the registration for this algorithm.

1.1. BCP 14 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Algorithm Description for Variable Length Nonparticipating

See [RFC4034] for the description of the resource records and fields used here.

For DNSKEY records, the Algorithm field MUST be TBD1. For RRSIG records, the Algorithm field MUST be TBD1.

The contents of the Public Key field and the Signature field is opaque, and are not interpreted by validators. The fields can be any length under the 65535 limit set in [RFC1035].

A DNSSEC validator that is validating a resource record set MUST ignore any RRSIG record with the Variable Length Nonparticipating algorithm.

For DS records that cover DNSKEY records, the Algorithm field MUST be TBD1. Note that such DS records are permitted by may not be required for all use cases where the Variable Length Nonparticipating record is used.

3. Examples

The following is an example of the Variable Length Nonparticipating algorithm. The public key is 1720 (0x06b8) bytes long and the signature is 2103 (0x0837) bytes long. The data in each is the length (as a two-byte value) followed by 0x00 values.

```
example.com. 86400 IN DNSKEY 256 3 TBD1 (
  BrgAAAAAAAAAAAAAAAAAAA ... AAAAAAAAAAAAAAAAAAAAAA )

host.example.com. 86400 IN RRSIG A TBD1 3 86400 20030322173103 (
  20030220173103 2642 example.com.
  CDcAAAAAAAAAAAAAAAAAAA ... AAAAAAAAAAAAAAAAAAAA== )
```

4. IANA Considerations

IANA is requested to add the following to the DNS Security Algorithm Numbers registry (https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml) after approval by a designated expert.

Number: TBD1 (proposal: next unassigned in range 18-22)

Description: Variable Length Nonparticipating

Mnemonic: VARIABLE-LENGTH-NONPARTICIPATING

Zone Signing: Y

Trans. Sec.: *

Use for DNSSEC Signing: MAY

Use for DNSSEC Validation: MAY

Implement for DNSSEC Signing: MAY

Implement for DNSSEC Validation: MAY

Reference: This document

5. Security Considerations

Section 2 specifies that any validation of signatures that use the Variable Length Nonparticipating algorithm MUST always ignore the signature. This does not affect the validation of signatures of any other algorithm number.

6. References

6.1. 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>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

6.2. Informative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

Author’s Address

Paul Hoffman
ICANN
Email: paul.hoffman@icann.org