Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 2 December 2025

M. Andrews
ISC

31 May 2025

DS support for private DNSSEC algorithms
draft-andrews-ds-support-for-private-algorithms-01

Abstract

Extend the DS digest field of the DS record to identify the private DNSSEC algorithm of the DNSKEY matching the DS record.

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 2 December 2025.

Table of Contents

1. Introduction

When the DNSSEC algorithm is PRIVATEDNS (233) or PRIVATEOID (254) the private algorithm identifier is embedded at the start of the key data in KEY, CDNSKEY, and DNSKEY records and at the start of the signature data in the RRSIG and SIG records [RFC4034]. This allows the private algorithm to be fully identified.

DS records, however, do not embed this identifier at the start of the digest field. This results in PRIVATEDNS and PRIVATEOID keys not being able to be used in all the scenarios where non private key algorithms can be. i.e. publishing of DS records for yet to be published DNSKEYs, determining if a DS based trust anchor represents a supported algorithm.

This document adds DS digest types which embed the private algorithm identifiers to the start of the digest field to provide equivalent functionality to PRIVATE key types as described in [RFC4034], Appendix A.1.1.

This document was inspired by the work done to add private DNSSEC algorithm support to BIND 9.

1.1. Reserved Words

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 [RFC2119].

2. Updated DS digest field structure

The digest field of CDS and DS records with digest types other than SHA-1 (1), SHA-256 (2), GOST R 34.11-94 (3), SHA-384 (4), GOST R 34.11-2012 (5) and SM3 (6) MUST now embed the private algorithm identifier before the digest data if the DS algorithm field is PRIVATEDNS or PRIVATEOID in the same manner as is done for the matching DNSKEY record.

It is RECOMMENDED that only DS records with DS digest types that embed the private DNSSEC algorithm are used with private DNSSEC algorithms as allows for publishing of DS records without the corresponding DNSKEY record being published.

3. New DS Types

New DS type identifiers which support embedding the private DNSSEC algorithm identifier are needed for SHA-256, SHA-384, GOST R 34.11-2012 and SM3 are needed along with identifing names. The new names and types are SHA-256-PRIVATE (TBA), SHA-384-PRIVATE (TBA), GOST R 34.11-2012 PRIVATE (TBA) and SM3-PRIVATE (TBA) respectively.

4. IANA Considerations

IANA is requested to assign DS types for SHA-256-PRIVATE, SHA-384-PRIVATE, GOST R 34.11-2012 PRIVATE and SM3-PRIVATE.

5. Security Considerations

This adds no known security issues.

6. Normative References

[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>.

[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>.

Appendix A. Example

Below we generate a example key using a PRIVATEOID DNSSEC algorithm and generate DS records from it using the SHA-256 digest and the proposed SHA-256-PRIVATE digest types. We also generate DS records for a RSASHA256 key using the same digests for comparison. The records have been converted to multi-line form for display purposes.

```
% dnssec-keygen -a RSASHA256OID example
Kexample.+256+40597
% dnssec-dsfromkey -a SHA-256 -a SHA-256-PRIVATE Kexample.+256+40597
example. IN DS 40597 254 2 ( D34C1ED54CC310D4DDECD935626B83A21E9462A
                             41519DCE3C7B88346B88E667D )
example. IN DS 40597 254 7 ( 0B06092A864886F70D01010BD34C1ED54CC310D
                             4DDECD935626B83A21E9462A41519DCE3C7B883
                             46B88E667D )
% cat Kexample.+256+40597.key
; This is a zone-signing key, keyid 40597, for example.
; Created: 20250530054504 (Fri May 30 15:45:04 2025)
; Publish: 20250530054504 (Fri May 30 15:45:04 2025)
; Activate: 20250530054504 (Fri May 30 15:45:04 2025)
example. IN DNSKEY 256 3 254 ( CwYJKoZIhvcNAQELAwEAAd3K9HIqJL+AiOb19
                               TPx/tgDbVVigJELn+LB6PqVD7U5tNPEYqVVK8
                               aRokyCd/Id/0l9xTVXDiDOCNVnTEZc6P20nhl
                               c1+alJF4S419APxE0EL8DAiiEAU4zwzLU41/4
                               1raFqN/sRZRLElvtEswtOXxvx5IGdAqnN0Np4
                               OiXMCmm4AoJ8RwCxWP2BNNp8CjRza3QaEk61/
                               ACc0U23Ol7wYefDudUoWJLKQFK6XM7pxuG5Zn
                               T4Hc0/Mbd3X/7Vi3zcxxef55v4jQEFxgXEIin
                               VlDtDVSSOGM+unPZeviedPqpCabVuUVPHOVyY
                               q/9OdCsHNZORdpo1nJuYVdwSs0t8AM= )
% dnssec-dsfromkey -a SHA-256 -a SHA-256-PRIVATE Kexample.+008+00163
example. IN DS 163 8 2 ( CAD5B47A4EA7D8F51926202CE4F89250C367D6EF2E0
                         8D8D26367056E7F76DE9A )
example. IN DS 163 8 7 ( CAD5B47A4EA7D8F51926202CE4F89250C367D6EF2E0
                         8D8D26367056E7F76DE9A )
%
```

Author’s Address

M. Andrews
Internet Systems Consortium
PO Box 360
Newmarket, NH 03857
United States of America
Email: marka@isc.org