Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 7, 2021

K. Fujiwara
JPRS

November 03, 2020

Delegation Information (Referrals) Signer for DNSSEC
draft-fujiwara-dnsop-delegation-information-signer-00

Abstract

DNSSEC does not protect delegation information, it contains NS RRSet on the parent side and glue records. This document defines delegation information signer (DiS) resource record for protecting the delegation information, by inserting on the parent side of zone cut to hold a hash of delegation information. The DiS resource record reuses the type code and wire format of DS resource record, and distinguishes it from existing DS RRSet by using a new digest type. This document also describes the usage of DiS resource record and shows the implications on security-aware resolvers. The definition and usage are compatible with current DNSSEC.

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 May 7, 2021.

Table of Contents

1. Introduction

The current DNSSEC specifications [RFC4033], [RFC4034], [RFC4035] do not protect the parent side NS RRSet and glue contained in the delegation information.

Recently, the word "in-domain" is defined by [RFC8499]. The in-domain glue is necessary and sufficient glue information for name resolution. [I-D.ietf-dnsop-glue-is-not-optional] proposes that Glue records are expected to be returned as part of a referral and if they cannot be fitted into the UDP response, TC=1 MUST be set to inform the client that the response is incomplete and that TCP SHOULD be used to retrieve the full response.

Then, we can define complete delegation information set that contains the parent side NS RRSet and all in-domain glue. We can generate a hash of the parent side NS RRSet and in-domain glue, and put it in DNS as a parent side information.

The delegation information signer (DiS) resource record (RR) is inserted at a zone cut (i.e., a delegation point) to hold a hash of delegation information (parent side NS RRSet) and required glue. The DiS resource record reuses DS resource record and distinguishes it from DS RRSet by using a new digest type and a new algorithm number.

Recent DNSSEC validators ignore DS resource records whose algorithm and digest type are unknown. Therefore, DiS resource record does not affect current DNSSEC validation.

DNSSEC validators that support DiS resource record can verify NS RRSet and in-domain glue.

This document defines new DS RR usage, gives examples of how it is used and describes the implications on resolvers. This change is compatible with current DNSSEC.

The meaning and processing the delegation information (parent side NS RRSet and glue) are not changed. The delegation information is used for name resolution process, and not used as the result of the name resolution.

2. Terminology

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 BCP14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Many of the specialized terms used in this document are defined in DNS Terminology [RFC8499].

3. Specification of the Delegation information Signer

This section defines a new usage of the Delegation Signer (DS) RR type.

3.1. New DS RR Usage: Delegation information signer (DiS)

This document specifies that the new DNSSEC Digest Type XX (it will be assigned by IANA) to the Delegation information Signer with SHA-256 (DISSHA256) for another DS usage.

The key tag and algorithm field may require further discussion.

The digest field is calculated over the parent side NS RRSet corresponding to the owner name of the DiS resource record and whole in-domain glue for its delegation.

```
digest = SHA-256 hash( NS RRSet | in-domain glue RRSets)
```

NS RRSet and in-domain glue RRSets are ordered as [I-D.ietf-dnsop-dns-zone-digest].

Sibling glue and out-of-bailiwick glue are not the data to be signed.

Wire format and Presentation format are the same as DS Resource Record.

3.2. DiS resource record in a Zone

The DiS resource record enables delegation information (parent side NS RRSet and in-domain glue records) signature validation in a validating resolver.

A DiS RRSet is present at all delegation point even if there is no DS RRSet. Since DiS RRSet has the same type code as DS RRSet except for digest type and hash data, details of DiS resource record is the same as DS resource record defined in [RFC4035].

When DNSSEC signer signes a zone, DNSSEC signer

- Remove all DiS resource records
- for all delegation points, generate new DiS resource record
- sign all DS RRSets

3.3. Change of Authoritative servers

Authoritative servers need to support [I-D.ietf-dnsop-glue-is-not-optional]. Then, referral responses MUST contain parent side NS RRSet and whole in-domain glue.

3.4. Change of validating resolvers

When a validating resolver receives a referral response with DS RRSet and the DS RRSet contains a DS resource record that have DISSHA256 digest type, the validating resolver SHOULD validate referral NS RRSet and in-domain glue. First, calculate digest from NS RRSet and in-domain glue from the referral response. Compare the digest and the digest field from the DiS resource record. If the digests differ, the referral is compromised or modified. The validating resolver can drop the referral.

4. Compatibility with the current DNSSEC

Current DNSSEC validators do not know DS resource records with digest type DISSHA256 and these DS records should be ignored. (See Section 5.2 of [RFC4035]).

5. Signing Priming Responses

Another use case for DiS resource record is the protection of priming responses.

The priming response is not a referral. However, it is similar to the referral and the priming response is deterministic.

Then we can put DiS resource record in the root and it can be signed.

The root DiS resource record contains digest consist of the root NS RRSet and all root servers' A and AAAA resource records.

Currently, TTL value of root servers' A/AAAA differ between root servers. Before considering DiS resource record in root, the TTL value of each root server A/AAAA for the root zone and root-servers.net zone must match.

6. IANA Considerations

IANA is requested to allocate new digest type code for DS resource record.

7. Security Considerations

8. Acknowledgments

9. Normative References

[I-D.ietf-dnsop-dns-zone-digest]
Wessels, D., Barber, P., Weinberg, M., Kumari, W., and W. Hardaker, "Message Digest for DNS Zones", draft-ietf-dnsop-dns-zone-digest-14 (work in progress), October 2020.

[I-D.ietf-dnsop-glue-is-not-optional]
Andrews, M., "Glue In DNS Referral Responses Is Not Optional", draft-ietf-dnsop-glue-is-not-optional-00 (work in progress), June 2020.

[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>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[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>.

[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>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

Author's Address

Kazunori Fujiwara
Japan Registry Services Co., Ltd.
Chiyoda First Bldg. East 13F, 3-8-1 Nishi-Kanda
Chiyoda-ku, Tokyo 101-0065
Japan

Phone: +81 3 5215 8451
Email: fujiwara@jprs.co.jp