Network Working Group
Internet-Draft
Intended status: Informational
Expires: February 26, 2016

O. Gudmundsson
CloudFlare

August 25, 2015

Removing DS records from parent via CDS/CDNSKEY
draft-ogud-dnsop-ds-remove-00

Abstract

RFC7344 specifies how trust can be maintained in-band between parent and child. There are two features missing in that specification: initial trust setup and removal of trust anchor. This document addresses the second omission.

There are many reasons why a domain may want to go unsigned. Some of them are related to DNS operator changes, others are related to DNSSEC signing system changes. The inability to turn off DNSSEC via in-band signalling is seen as a liability in some circles. This document addresses the issue in a sane way.

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 http://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 February 26, 2016.

Copyright Notice

Table of Contents

1. Introduction

CDS/CDNSKEY [RFC7344] records are used to signal changes in trust anchors, this is a great way to maintain delegations when the DNS operator has no other way to notify parent that changes are needed. The original versions of the draft that became RFC7344 contained a "delete" signal, the DNSOP working group at the time did not want that feature, thus it was removed.

This document re-introduces the delete option for both CDS and CDNSKEY. The reason is simply that it is necessary to be able to turn off DNSSEC. The main reason has to do with when a domain is moved from one DNS operator to another one. Common scenarios include:

(I) moving from a DNSSEC operator to a non-DNSSEC capable one

(II) moving to one that cannot/does-not-want to do a proper DNSSEC rollover

(III) user does not want DNSSEC

Whatever the reason, the lack of a "remove my DS" option is turning into the latest excuse as why DNSSEC cannot be deployed.

1.1. Terminology

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. DNSSEC Delete Algorithm

The DNSKEY algorithm registry contains two reserved values: 0 and 255[RFC4034]. The CERT record [RFC4398] defines the value 0 to mean the algorithm in the CERT record is not defined in DNSSEC.
For this reason, using the value 0 in CDS/CDNSKEY delete operations is potentially problematic, but we propose that here anyway as the risk is minimal. The alternative is to reserve one DNSSEC algorithm number for this purpose.

Right now, no DNSSEC validator understands algorithm 0 as a valid signature algorithm, thus if the validator sees a DNSKEY or DS record with this value, it will treat it as unknown. Accordingly, the zone is treated as unsigned unless there are other algorithms present.

In the context of CDS and CDNSKEY records, DNSSEC algorithm 0 is defined and means delete the DS set. The contents of the records MUST contain only the fixed fields as show below.

(I) CDS 0 0 0

(II) CDNSKEY 0 3 0

The there is no keying information in the records, just the command to delete all DS records. This record is signed in the same way as CDS/CDNSKEY is signed.

Once the parent has verified the CDS/CDNSKEY record and it has passed other acceptance tests, the DS record MUST be removed. At this point the child can start the process of turning DNSSEC off.

3. Security considerations

This document is about avoiding validation failures when a domain moves from one DNS operator to another one. In most cases it is preferable that operators collaborate on the rollover by doing a KSK+ZSK rollover as part of the handoff, but that is not always possible. This document addresses the case where unsigned state is needed.

This document does not introduce any new problems, but like Negative Trust Anchor[I-D.ietf-dnsop-negative-trust-anchors], it addresses operational reality.

4. IANA considerations

This document updates the following IANA registries: "DNS Security Algorithm Numbers"

Algorithm 0 adds a reference to this document.

5. References

5.1. 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, <http://www.rfc-editor.org/info/rfc4034>.

[RFC7344] Kumari, W., Gudmundsson, O., and G. Barwood, "Automating DNSSEC Delegation Trust Maintenance", RFC 7344, DOI 10.17487/RFC7344, September 2014, <http://www.rfc-editor.org/info/rfc7344>.

5.2. Informative References

[I-D.ietf-dnsop-negative-trust-anchors] Ebersman, P., Kumari, W., Griffiths, C., Livingood, J., and R. Weber, "Definition and Use of DNSSEC Negative Trust Anchors", draft-ietf-dnsop-negative-trust-anchors-13 (work in progress), August 2015.

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

[RFC4398] Josefsson, S., "Storing Certificates in the Domain Name System (DNS)", RFC 4398, DOI 10.17487/RFC4398, March 2006, <http://www.rfc-editor.org/info/rfc4398>.

Appendix A. Acknowledgements

This document is generated using the mmark tool that Miek Gieben has developed.

The kick in the rear to finally write this draft came from Jacques LaTour and Paul Wouters.

Author's Address

Olafur Gudmundsson
CloudFlare

Email: olafur+ietf@cloudflare.com