Internet Engineering Task Force (IETF)
Request for Comments: 8078
Updates: 7344
Category: Standards Track
ISSN: 2070-1721

O. Gudmundsson
CloudFlare
P. Wouters
Red Hat

March 2017

Managing DS Records from the Parent via CDS/CDNSKEY

Abstract

RFC 7344 specifies how DNS trust can be maintained across key rollovers in-band between parent and child. This document elevates RFC 7344 from Informational to Standards Track. It also adds a method for initial trust setup and removal of a secure entry point.

Changing a domain’s DNSSEC status can be a complicated matter involving multiple unrelated parties. Some of these parties, such as the DNS operator, might not even be known by all the organizations involved. The inability to disable DNSSEC via in-band signaling is seen as a problem or liability that prevents some DNSSEC adoption at a large scale. This document adds a method for in-band signaling of these DNSSEC status changes.

This document describes reasonable policies to ease deployment of the initial acceptance of new secure entry points (DS records).

It is preferable that operators collaborate on the transfer or move of a domain. The best method is to perform a Key Signing Key (KSK) plus Zone Signing Key (ZSK) rollover. If that is not possible, the method using an unsigned intermediate state described in this document can be used to move the domain between two parties. This leaves the domain temporarily unsigned and vulnerable to DNS spoofing, but that is preferred over the alternative of validation failures due to a mismatched DS and DNSKEY record.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8078.

Copyright Notice

Table of Contents

1. Introduction 3
1.1. Introducing a DS Record 3
1.2. Removing a DS Record 4
1.3. Notation 4
1.4. Terminology 5
2. The Three Uses of CDS 5
2.1. The Meaning of the CDS RRset 5
3. Enabling DNSSEC via CDS/CDNSKEY 6
3.1. Accept Policy via Authenticated Channel 6
3.2. Accept with Extra Checks 6
3.3. Accept after Delay 7
3.4. Accept with Challenge 7
3.5. Accept from Inception 7
4. DNSSEC Delete Algorithm 7
5. Security Considerations 8
6. IANA Considerations 9
6.1. Promoting RFC 7344 to Standards Track 9
7. References 9
7.1. Normative References 9
7.2. Informative References 10
Acknowledgments 10
Authors' Addresses 10

1. Introduction

CDS (Child DS) and CDNSKEY (Child DNSKEY) [RFC7344] records are used to signal changes in secure entry points. This is one method to maintain delegations that can be used when the DNS operator has no other way to inform the parent that changes are needed. This document elevates [RFC7344] from Informational to Standards Track.

In addition, [RFC7344] lacks two different options for full automated operation to be possible. It does not define a method for the initial trust establishment, leaving it open to each parent to come up with an acceptance policy. Additionally, [RFC7344] does not provide a "delete" signal for the child to inform the parent that the DNSSEC security for its domain must be removed.

1.1. Introducing a DS Record

Automated insertion of DS records has been limited for many zones by the requirement that all changes pass through a "Registry" of the child zone's parent. This has significantly hindered deployment of DNSSEC at a large scale for DNS hosters, as the child zone owner is often not aware or able to update DNS records such as the DS record.

This document describes a few possible methods for the parent to accept a request by the child to add a DS record to its zone. These methods have different security properties that address different deployment scenarios, all resulting in an automated method of trust introduction.

1.2. Removing a DS Record

This document introduces the delete option for both CDS and CDNSKEY, allowing a child to signal to the parent to turn off DNSSEC. When a domain is moved from one DNS operator to another, sometimes it is necessary to turn off DNSSEC to facilitate the change of DNS operator. Common scenarios include:

1. Alternative to doing a proper DNSSEC algorithm rollover due to operational limitations such as software limitations.

2. Moving from a DNSSEC operator to a non-DNSSEC-capable operator.

3. Moving to an operator that cannot or does not want to do a proper DNSSEC rollover.

4. When moving between two DNS operators that use disjoint sets of algorithms to sign the zone, an algorithm rollover cannot be performed.

5. The domain holder no longer wants DNSSEC enabled.

The lack of a "remove my DNSSEC" option is cited as a reason why some operators cannot deploy DNSSEC, as this is seen as an operational risk.

Turning off DNSSEC reduces the security of the domain and thus should only be done carefully, and that decision should be fully under the child domain’s control.

1.3. Notation

Signaling can happen via CDS or CDNSKEY records. The only differences between the two records are how information is represented and who calculates the DS digest. For clarity, this document uses the term "CDS" to mean "either CDS or CDNSKEY".

When this document uses the word "parent", it implies an entity that is authorized to insert DS records into the parent zone on behalf of the child domain. Which entity this exactly is does not matter. It

could be the Registrar or Reseller that the child domain was purchased from. It could be the Registry that the domain is registered in when allowed. Or it could be some other entity.

1.4. 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. The Three Uses of CDS

In general, there are three operations that a domain wants to instruct its parent to perform:

1. Enable DNSSEC validation, i.e., place an initial DS Resource Record Set (RRset) in the parent.

2. Roll over the KSK. This means updating the DS records in the parent to reflect the new set of KSKs at the child. This could be an ADD operation, a DELETE operation on one or more records while keeping at least one DS RR, or a full REPLACE operation.

3. Turn off DNSSEC validation, i.e., delete all the DS records.

KSK rollover is covered in [RFC7344]. It is considered the safest use case of a CDS/CDNSKEY record as it makes no change to the trust relationship between parent and child. Introduction and removal of DS records are defined in this document. As these CDS/CDNSKEY use cases create or end the trust relationship between the parent and child, these use cases should be carefully implemented and monitored.

2.1. The Meaning of the CDS RRset

The semantic meaning of publishing a CDS RRset is interpreted to mean:

> Publishing a CDS or CDNSKEY record signals to the parent that the child desires that the corresponding DS records be synchronized. Every parent or parental agent should have an acceptance policy of these records for the three different use cases involved: Initial DS publication, Key rollover, and Returning to Insecure.

In short, the CDS RRset is an instruction to the parent to modify the DS RRset if the CDS and DS Resets differ.

The acceptance policy for CDS in the rollover case is "seeing" according to [RFC7344]. The acceptance policy in the Delete case is seeing a (validly signed) CDS RRset with the delete operation specified in this document.

3. Enabling DNSSEC via CDS/CDNSKEY

There are number of different models for managing initial trust, but in the general case, the child wants to enable global validation. As long as the child is insecure, DNS answers can be forged. The goal is to promote the child from insecure to secure as soon as reasonably possible by the parent. This means that the period from the child's publication of CDS/CDNSKEY RRset to the parent publishing the synchronized DS RRset should be as short as possible.

One important use case is how a third-party DNS operator can upload its DNSSEC information to the parent, so the parent can publish a DS record for the child. In this case, there is a possibility of setting up some kind of authentication mechanism and submission mechanism that is outside the scope of this document.

Below are some policies that parents can use. These policies assume that the notifications can be verified or authenticated.

3.1. Accept Policy via Authenticated Channel

In this case, the parent is notified via authenticated channel UI/API that a CDS/CDNSKEY RRset exists. In the case of a CDS RRset, the parent retrieves the CDS RRset and inserts the corresponding DS RRset as requested. In the case of CDNSKEY, the parent retrieves the CDNSKEY RRset and calculates the DS record(s). Parents may limit the DS record type based on local policy. Parents SHOULD NOT refuse CDS/CDNSKEY updates that do not (yet) have a matching DNSKEY in the child zone. This will allow the child to pre-publish a spare (and potentially offline) DNSKEY.

3.2. Accept with Extra Checks

In this case, the parent checks that the source of the notification is allowed to request the DS insertion. The checks could include whether this is a trusted entity, whether the nameservers correspond to the requester, whether there have been any changes in registration in the last few days, etc. The parent can also send a notification requesting a confirmation, for example, by sending email to the registrant requesting a confirmation. The end result is that the CDS RRset is accepted at the end of the checks or when the out-of-band confirmation is received. Any extra checks should have proper rate limiting in place to prevent abuse.

3.3. Accept after Delay

In this case, if the parent deems the request valid, it starts monitoring the CDS RRset at the child nameservers over a period of time to make sure nothing changes. After some time or after a number of checks, preferably from different vantage points in the network, the parent accepts the CDS RRset as a valid signal to update its DS RRset for this child.

3.4. Accept with Challenge

In this case, the parent instructs the requester to insert some record into the child domain to prove it has the ability to do so (i.e., it is the operator of the zone). This method imposes a new task on the parent to monitor the child zone to see if the challenge has been added to the zone. The parent should verify that the challenge is published by all the child's nameservers and should test for this challenge from various diverse network locations to increase the security of this method as much as possible.

3.5. Accept from Inception

If a parent is adding a new child domain that is not currently delegated at all, it could use the child CDS/CDNSKEY RRset to immediately publish a DS RRset along with the new NS RRset. This would ensure that the new child domain is never active in an insecure state.

4. DNSSEC Delete Algorithm

This document defines the previously reserved DNS Security Algorithm Number of value 0 in the context of CDS and CDNSKEY records to mean that the entire DS RRset at the parent must be removed. The value 0 remains reserved for the DS and DNSKEY records.

No DNSSEC validator can treat algorithm 0 as a valid signature algorithm. If a validator sees a DNSKEY or DS record with this algorithm value, it must treat it as unknown. Accordingly, the zone is treated as unsigned unless there are other algorithms present. In general, the value 0 should never be used in the context of DNSKEY and DS records.

The CERT record [RFC4398] defines the value 0 similarly to mean the algorithm in the CERT record is not defined in DNSSEC.

The contents of the CDS or CDNSKEY RRset MUST contain one RR and only contain the exact fields as shown below.

```
CDS 0 0 0 0

CDNSKEY 0 3 0 0
```

The keying material payload is represented by a single 0. This record is signed in the same way as regular CDS/CDNSKEY RRsets are signed.

Strictly speaking, the CDS record could be "CDS X 0 X 0" as only the DNSKEY algorithm is what signals the DELETE operation, but for clarity, the "0 0 0 0" notation is mandated -- this is not a definition of DS digest algorithm 0. The same argument applies to "CDNSKEY 0 3 0 0"; the value 3 in the second field is mandated by [RFC4034], Section 2.1.2.

Once the parent has verified the CDS/CDNSKEY RRset and it has passed other acceptance tests, the parent MUST remove the DS RRset. After waiting a sufficient amount of time -- depending on the parental TTLs -- the child can start the process of turning off DNSSEC.

5. Security Considerations

Turning off DNSSEC reduces the security of the domain and thus should only be done as a last resort in preventing DNSSEC validation errors due to mismatched DS and DNSKEY records.

Users should keep in mind that re-establishing trust in delegation can be hard and takes time. Before deciding to complete the rollover via an unsigned state, all other options should be considered first.

A parent SHOULD ensure that when it is allowing a child to become securely delegated, it has a reasonable assurance that the CDS/CDNSKEY RRset used to bootstrap the security is visible from a geographically and topologically diverse view. It SHOULD also ensure that the zone validates correctly if the parent publishes the DS record. A parent zone might also consider sending an email to its contact addresses to give the child zone a warning that security will be enabled after a certain amount of wait time -- thus allowing a child administrator to cancel the request.

This document describes a few possible acceptance criteria for the initial trust establishment. Due to a large variety of legal frameworks surrounding parent domains (Top-Level Domain (TLDs) in particular), this document cannot give a definitive list of valid acceptance criteria. Parental zones should look at the listed

methods and pick the most secure method possible within their legal and technical scenario, possibly further securing the acceptance criteria, as long as the deployed method still enables a fully automated method for non-direct parties such as third-party DNS hosters.

6. IANA Considerations

IANA has assigned entry number 0 in the "DNS Security Algorithm Numbers" registry as follows:

Number	Description	Mnemonic	Zone Signing	Trans. Sec.	Reference
0	Delete DS	DELETE	N	N	[RFC4034] [RFC4398] [RFC8078]

6.1. Promoting RFC 7344 to Standards Track

Experience has shown that CDS and CDNSKEY are useful in the deployment of DNSSEC. [RFC7344] was published as Informational; this document elevates RFC 7344 to Standards Track.

7. References

7.1. 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, <http://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, <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>.

7.2. Informative References

[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>.

Acknowledgments

We thank a number of people that have provided feedback and useful comments including Bob Harold, John Levine, Dan York, Shane Kerr, Jacques Latour, and especially Matthijs Mekking.

Authors' Addresses

Olafur Gudmundsson
CloudFlare

Email: olafur+ietf@cloudflare.com

Paul Wouters
Red Hat

Email: pwouters@redhat.com