template
Internet-Draft
Intended status: Informational
Expires: August 22, 2013

W. Kumari
Google
O. Gudmundsson
Shinkuro Inc.
G. Barwood

February 18, 2013

Easy DNSSEC Key Publish
draft-kumari-ogud-dnsop-cds-00

Abstract

This document describes a method to allow DNS operators to more easily publish updated DNSSEC Key Signing Keys. This document does not address the initial configuration of trust anchors for a domain.

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 August 22, 2013.

Table of Contents

1. Introduction

When a DNS operator first signs their zone they need to communicate their DS record(s) (or DNSKEY(s)) to their parent through some out of band method. In many cases this is a fairly annoying and manual process. Unfortunately, every time the child rolls their KSK (Key Signing Key) key they have to repeat the process, possibly multiple times. As this is a manual process DNS operators often avoid rolling their keys, as they don't want to have to do go through the annoyance of publishing the new keys.

This document describes a method to automate publication of subsequent DS records, after the initial one has been published.

Readers are expected to be familiar with DNSSEC, including [RFC4033], [RFC4034], [RFC4035] and [RFC6781].

This document is a compilation of two earlier drafts, draft-barwood-dnsop-ds-publish and draft-wkumari-dnsop-ezkeyroll

This document outlines a technique in which the parent (often registrar / registry) periodically polls its signed children and automatically publish new DS records. To a large extent the procedures this document follows are in [RFC6781] section 4.1.2

This technique is in some ways similar to RFC 5011 style rollovers, but for subdomains instead of trust anchors

1.1. Requirements notation

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. Background

For ease of explanation, we will mainly describe the "standard" case where a DNS operator registers a domain though a registrar, who then publishes the information in a registry, but this same technique can be used anywhere where a child needs to update their DS resource record. We will also assume that the registrar provides a web interface for adding DS resource record information; in a distressingly large number of cases the registrar doesn't (yet) have this functionality, and so the operator has to communicate their DS to the registrar through email or a telephone call, but the actual mechanism doesn't matter. We will further assume that the registrant is also the DNS operator - this technique is expandable to any

relationship, but the background explanation gets more tricky.

After an DNS operator first signs its zone, they login to the registrar's web interface and then paste in the zone's DS information. The registrar then communicates the DS record to the registry who publishes it. The action of logging in through the web interface authenticates that the user is authorized to publish in the zone.

Eventually the registrant may want to publish a new DS record in the parent, either because they are rolling their keys, or because they want to publish a stand-by key DS record. This involves performing the same process -- logging into a web interfaces, selecting the domain, finding the link to change DNSSEC information, pasting (or typing) their DS record (often in a non-standard format) and clicking submit (in a real world test, this took 12 steps and approximately 3 minutes). As humans (especially DNS operators :-)) dislike tedious, repetitive steps they often avoid rolling their DNSSEC keys to avoid having to perform this.

3. CDS Resource Record Format

The wire and presentation format of the CDS ("Child DS") record is identical to the DS record. IANA has allocated RR code 59 for the CDS record.

However no special processing is performed by authoritative servers or by resolvers, when serving or resolving. CDS unlike a DS resides

in the child zone.

The CDS record MUST be signed with a key that has the Secure Entry Point flag set, just like the DNSKEY record.

4. CDS Behavior

The CDS RRset MAY be used by the parent (or a parental representative) to update the DS RRset in the parent zone we call this entity "parental agent".

In many environments (for example, gTLDs) the parent will be a registry, and is expected to not have direct contact with the child (registrant). In these cases, the registrar (or a contractor for the registrar) will be the one that queries the child zone for the CDS record, and if found, will publish it in the parent (probably using [RFC5734]). It is conceivable that this could be a "value added" service.

Transfer of the contents of the CDS record can be accomplished in a number of ways. A parental agent MAY periodically check the child zone to see if the CDS RRset has changed. The child MAY request that the parent check the CDS set via registration interface, or via some other automated mechanism.

The child MUST make sure that the CDS RRset is at all times validatable using a DNSKEY that is referenced from the current DS set in the parent. This can be accomplished by making sure that at all times during a KEY rollover there are either two DS records or two DNSKEY records with SEP bit published in the DNS.

When using CDS to publish its key rollover information it is the child's responsibility to monitor the parent for changes to the DS RRset before performing the next action in the key rollover sequence. What this implies is that the child MUST NOT follow a strict timeline but rather strict sequence of steps with time checks.

4.1. Periodic check by parental agent

In this case the parental agent will query each child zone that has a DS RRset, looking for CDS RRset

If present the parental agent MUST validate [[RFC4035]] the CDS RRset. If the validation succeeds with a DNSKEY that is represented in the current DS RRset in parent. The parenteral agent should submit a request to the registry to publish the contents of the CDS RR(s) as the new a DS record(s) for that zone. The parental agent SHOULD log the date and time when of this action including the signature initiation time on the CDS record. The registry should log if possible the source of the update, user interface/CDS etc.

5. Usage

The parent zone SHOULD ensure that old versions of the CDS RRset do not overwrite newer versions, which can occur the parent performs the checks too frequently. In that case when there is a delay updating secondary name servers for the child zone. This MAY be accomplished by checking that the signature inception in the RRSIG for CDS is newer

If the CDS RRset does not exist, the parent MUST take no action. Specifically it MUST NOT delete the existing DS RRset.

If the child zone loses the secret key(s) for the zone, and needs to reset the parent DS RRset, this must be accomplished by an out-of-band mechanism not defined here.

To mitigate situations where a key signing key has been compromised, the parent zone MAY take extra security measures, for example informing (by email or other methods) the zone administrator of the change, and delaying the acceptance of the new DS RRset for some period of time. However the precise out-of-band measures that a parent zone SHOULD take are outside the scope of this document.

5.1. Going unsigned

In theory the child can use the CDS to reflect the parent to remove the DS records. This can be accomplished by publishing CDS record with the following contents:

```
@ IN CDS 0 0 0
```

This is an suggestion and its security implications have not been fully examined but an RFC5011 like process should be used before this is accepted.

If a child zone has gone unsigned, i.e. no DNSKEY and no RRsigs in the zone, the parental representative MAY treat that as intent to go unsigned. (NEEDS DISCUSSION).

6. IANA Considerations

IANA has assigned RR Type code 59 for CDS. This was done for an earlier version of this document (draft-barwood-dnsop-ds-publish).

7. Security Considerations

[This needs a more work, suggestions welcome.]

In the event of a compromise of the server generating signatures for a zone, attacker may be able to generate and publish new CDS records. These will be picked up by this technique and so may allow the attacker to extend the effective time of his attack. This can be dealt with by contacting the parent (potentially though a registrar web interface) and removing any compromised DS keys.

A compromise of the registrar, will not be mitigated by this technique

While it may be tempting, this should NOT be used for initial enrolment of keys since there is no way to ensure that the initial key is the correct one.

The CDS RRtype should allow for enhanced security by simplifying process. Since rollover is automated, updating a DS RRset by other means may be regarded as unusual and subject to extra security checks.

8. Acknowledgements

This is by no means the invention of the authors. This idea has been floating around for a long time. This simply documents it for discussion.

We would like to thank: Joe Abley, Roy Arends, Jim Galvin, Cricket Liu, Matt Larson, Olaf Kolkman, Suzanne Woolfe.

There were a large number of other folk with whom we discussed this, apologies for not remembering everyone.

9. References

9.1. Normative References

[IANA.AS_Numbers]
IANA, "Autonomous System (AS) Numbers", <http://www.iana.org/assignments/as-numbers>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

[I-D.ietf-sidr-iana-objects]
Manderson, T., Vegoda, L., and S. Kent, "RPKI Objects issued by IANA", draft-ietf-sidr-iana-objects-03 (work in progress), May 2011.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC5734] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)

Transport over TCP", STD 69, RFC 5734, August 2009.

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, December 2012.

Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication]

From -00 to -01.

- Nothing changed in the template!

Authors' Addresses

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: warren@kumari.net

Olafur Gudmundsson
Shinkuro Inc.
4922 Fairmont Av, Suite 250
Bethsda, MD 20814
USA

Email: ogud@ogud.com

George Barwood
33 Sandpiper Close
Gloucester GL2 4LZ
United Kingdom

Email: warren@kumari.net