Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 21, 2016

J. Latour
CIRA
O. Gudmundsson
Cloudflare, Inc.
P. Wouters
Red Hat
M. Pounsett
Rightside

October 19, 2015

# Third Party DNS operator to Registrars/Registries Protocol
## draft-latour-dnsoperator-to-rrr-protocol-00.txt

Abstract

There are several problems that arise in the standard Registrant/Registrar/Registry model when the operator of a zone is neither the Registrant nor the Registrar for the delegation. Historically the issues have been minor, and limited to difficulty guiding the Registrant through the initial changes to the NS records for the delegation. As this is usually a one time activity when the operator first takes charge of the zone it has not been treated as a serious issue.

When the domain on the other hand uses DNSSEC it necessary for the Registrant in this situation to make regular (sometimes annual) changes to the delegation in order to track KSK rollover, by updating the delegation's DS record(s). Under the current model this is prone to Registrant error and significant delays. Even when the Registrant has outsourced the operation of DNS to a third party the registrant still has to be in the loop to update the DS record.

There is a need for a simple protocol that allows a third party DNS operator to update DS and NS records for a delegation without involving the registrant for each operation.

The protocol described in this draft is REST based, and when used through an authenticated channel can be used to bootstrap DNSSEC. Once DNSSEC is established this channel can be used to trigger maintenance of delegation records such as DS, NS, and glue records. The protocol is kept as simple as possible.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Copyright Notice



Table of Contents

## 1. Introduction

Why is this needed ? DNS registration systems today are designed around making registrations easy and fast. After the domain has been registered the there are really three options on who maintains the DNS zone that is loaded on the "primary" DNS servers for the domain this can be the Registrant, Registrar, or a third party.

Unfortunately the ease to make changes differs for each one of these options. The Registrant needs to use the interface that the registrar provides to update NS and DS records. The Registrar on the other hand can make changes directly into the registration system. The third party operator on the hand needs to go through the Registrant to update any delegation information.

Current system does not work well, there are many examples of failures including the inability to upload DS records du to non-support by Registrar interface, the registrant forgets/does-not perform action but tools proceed with key rollover without checking that the new DS is in place. Another common failure is the DS record is not removed when the DNS operator changes from one that supports DNSSEC signing to one that does not.

The failures result either inability to use DNSSEC or in validation failures that case the domain to become invalid and all users that are behind validating resolvers will not be able to to access the domain.

## 2. Notational Conventions

### 2.1. Definitions

For the purposes of this draft, a third-party DNS operator is any DNS

operator responsible for a zone where the operator is neither the Registrant nor the Registrar of record for the delegation.

When we say Registrar that can in many cases be applied to a Reseller i.e. an entity that sells delegations but registrations are processed through the Registrar.

## 2.2. RFC2119 Keywords

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].





# 3. What is the goal ?

The primary goal is to use the DNS protocol to provide information from child zone to the parent zone, this is a way to maintain the delegation information. The precondition for this to be practical is that the domain is DNSSEC signed.

IN the general case there should be a way to find the right Registrar/Registry entity to talk to but that does not exist. Whois[] is the natural protocol to carry such information but that protocol is unreliable and hard to parse. Its proposed successor RDAP [RFC7480] has yet be deployed on any TLD.

The preferred communication mechanism is to use is to use a REST [RFC6690] call to start processing of the requested delegation information.

## 3.1. Why DNSSEC ?

DNSSEC [RFC4035] provides data authentication for DNS answers, having DNSSEC enabled makes it possible to trust the answers. The biggest stumbling block is deploying DNSSEC is the initial configuration of the DNSSEC domain trust anchor in the parent, DS record.

## 3.2. How does Domain signal to parent it wants DNSSEC Trust Anchor ?

The child needs first to sign the domain, then the child can "upload" the DS record. The "normal" way to upload is to go through registration interface, but that fails frequently. The DNS operator

may not have access to the interface thus the registrant needs to relay the information. For large operations this does not scale, as evident in lack of Trust Anchors for signed deployments that are operated by third parties.

The child can signal its desire to have DNSSEC validation enabled by publishing one of the special DNS records CDS and/or CDNSKEY[RFC7344]. Once the "parent" "sees" these records it SHOULD start acceptance processing. This document will cover below how to make the CDS records visible to the right parental agent.

We argue that the publication of CDS/CDNSKEY record is sufficient for the parent to start acceptance processing. The main point is to provide authentication thus if the child is in "good" state then the DS upload should be simple to accept and publish. If there is a problem the parent has ability to remove the DS at any time.





### 3.3. What checks are needed by parent ?

The parent upon receiving a signal that it check the child for desire for DS record publication. The basic tests include,

1. All the nameservers for the zone agree on zone contents
2. The zone is signed
3. The zone has a CDS signed by the KSK referenced i the CDS

Parents can have additional tests, defined delays, and even ask the DNS operator to prove they can add data to the zone, or provide a code that is tied to the affected zone.

## 4. OP-3-DNS-RR Protocol

### 4.1. Command

The basic call is

https://<SERVER-name>/Update/<domain>/

The following options to the commands are specified

"auth=" an authentication token

"debug=" request a debug session

The service above is defined on standard https port but it could run on any port as specified by an URI.

## 4.2. Answers

The basic answer is a jason blob the these are some possible blocks in the response:

"refer:" will contain an URI; this is an referral to an URI that is better able to do execute the command

"refused:" This command can not be executed, and the reason is inside the block

"debug:" list of debug messages normally empty unless debug flag is present, this section should be ignored in normal processing

"error:" if there was one look inside debug for more details

"domain:" what domain this is an answer for this section MUST be included in all answers





"rr:" the new list of rrs "can be empty"

"id:" An identifier for the transaction

If ``refer'' block is present in answer then the client is instructed to connect to that URI and retry the command there. Client SHOULD always honor the refer command over all other answers it gets in the answer.

## 5. Authorization

The authorization can be either based on Token (like auth code) or buy challenge i.e. inserting a blob into the zone. It is up to registrars to register the referral URI with registries, or block the access to updating DS and NS.

OAUTH??? how that would work ???

## 6. Security considerations

TBD This will hopefully get more zones to become validated thus overall the security gain out weights the possible drawbacks.

## 7. IANA Actions

URI ??? TBD

## 8. Internationalization Considerations

This protcol is designed for machine to machine communications

## 9. References

### 9.1. Normative References


[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, <http://www.rfc-editor.org/info/rfc4035>.

[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>.






### 9.2. Informative 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>.

[RFC6690] Shelby, Z., "Constrained RESTful Environments (CoRE) Link

Format", RFC 6690, DOI 10.17487/RFC6690, August 2012, <http://www.rfc-editor.org/info/rfc6690>.

[RFC7480] Newton, A., Ellacott, B., and N. Kong, "HTTP Usage in the Registration Data Access Protocol (RDAP)", RFC 7480, DOI 10.17487/RFC7480, March 2015, <http://www.rfc-editor.org/info/rfc7480>.

## Appendix A. Document History

First rough version

## Authors' Addresses

Jacques Latour
CIRA

Email: jacques.latour@cira.ca

Olafur Gudmundsson
Cloudflare, Inc.

Email: olafur+ietf@cloudflare.com

Paul Wouters
Red Hat

Email: paul@nohats.ca

Matthew Pounsett
Rightside

Email: matt@conundrum.com