
ICANN
ICANN | 52
Singapore
8-12 FEBRUARY 2015
ICANN
AT-LARGE

DNSSEC & Third-Party Operators

David C Lawrence | DNSSEC Workshop | 11 February 2015
tale@akamai.com

The Current Problem

Luna Control Center

https control.akamai.com/portal/adns/adns_detail.jsp?zone=dnssec.akamaidemo.com

Weather News Melrose Blogs Stocks Akamai Stuff Misc. Stuff Recipes Popular Civil War Reenactor Adam's List

Luna Control Center

Akamai Donald Lehman | 4 Messages | 60 Alerts | | Marketplace | Support | LUNA Control Center

Akamai Technologies - Assets MONITOR CONFIGURE PUBLISH RESOLVE PLAN

Akamai Technologies - Assets-1-3CV382 Test1 Test Manuel

Zone Transfer Status Details

Fast DNS | **Zone Transfer Status Details**

If you have a zone transfer status error, please open a ticket with Akamai Customer Care.

Zone:	dnssec.akamaidemo.com
Last Zone Status:	All name servers are up to date
Current SOA serial number:	1420822885

Current DS Record

The most recent DS record is:

```
dnssec.akamaidemo.com. 86400 IN DS 17613 10 1 ( 9a5177469e7cefcf30a719f2d50170be2bdc2400 )
```

The corresponding Key Signing Key DNSKEY record is:

```
dnssec.akamaidemo.com. 7200 IN DNSKEY 257 3 10 (
                                Av//xYLPcCkEt2BFM7C+mzIE8Dn6QoMb5KO0
                                IGAu5uZGEHx6KVVoOZJnQ9dbieC2WOHl2Uom
                                rzRGEClDgdorfgaHq7y0Impqn0uuFiMCGGRs
                                EKNKt8wpTpbHnp49HQtRzMu7pkwrhPq2c7BD
                                rSalYFn3udPXT8sXgj55SA5ZSPhSK8IQlCTx
                                StyYhWL2BIilMRxjPYEr2VAqnTjcvERElmrE
                                0f/VY8plQamvhTvbKy9GNVTmXdjqWytTWAM8
                                NL4oRqh45QIk2fxNaW5jWXaucaCk3k2lAZAH
                                aek4lPcfTpuyUFxW2UTA6Qtml7mHsJkuxEb/
                                dt3gvzrzjpiY+Ba82zgt3w==
                                )
```

These records correspond to a key pair created on Fri, 9 Jan 2015. One of these records should be provided to your parent zone to establish the DNSSEC chain of trust.

Note: According to RFC 4035, the TTL of the DS record SHOULD match the TTL of the corresponding NS record set. Please adjust the TTL in the above record (86400) as needed.

DNSSEC Sign and Serve: Active Alerts

Status: 0 Critical Alert(s), 1 Warning(s) are currently active.

PRIORITY	ALERT TYPE
Warning	No DS record in parent zone

The Current Problem

Luna Control Center

https control.akamai.com/portal/adns/adns_detail.jsp?zone=dnssec.akamaidemo.com

Weather News Melrose Blogs Stocks Akamai Stuff Misc. Stuff Recipes Popular Civil War Reenactor Adam's List

Luna Control Center

Akamai Donald Lehman | 4 Messages | 60 Alerts | | Marketplace | Support | LUNA Control Center

Akamai Technologies - Assets MONITOR CONFIGURE PUBLISH RESOLVE PLAN

Akamai Technologies - Assets-1-3CV382 Test1 Test Manuel

Zone Transfer Status Details

Fast DNS | **Zone Transfer Status Details**

If you have a zone transfer status error, please open a ticket with Akamai Customer Care.

Zone:	dnssec.akamaidemo.com
Last Zone Status:	All name servers are up to date
Current SOA serial number:	1420822885

Current DS Record

The most recent DS record is:

```
dnssec.akamaidemo.com. 86400 IN DS 17613 10 1 ( 9a5177469e7cefcf30a719f2d50170be2bdc2400 )
```

The corresponding Key Signing Key DNSKEY record is:

```
dnssec.akamaidemo.com. 7200 IN DNSKEY 257 3 10 (
                                Av//xYLPcCkEt2BFM7C+mzIE8Dn6QoMb5KO0
                                IGAu5uZGEHx6KVVoOZJnQ9dbieC2WOHl2Uom
                                rzRGEClDgdorfgaHq7y0Impqn0uuFiMCGGRs
                                EKNKt8wpTpbHnp49HQtRzMu7pkwrhPq2c7BD
                                rSalYFn3udPXT8sXgj55SA5ZSPhSK8IQlCTx
                                StyYhWL2BIilMRxjPYEr2VAqnTjcvERElmrE
                                0f/VY8plQamvhTvbKy9GNVTmXdjqWytTWAM8
                                NL4oRqh45QIk2fxNaW5jWXaucaCk3k2lAZAH
                                aek4lPcfTpuyUFxW2UTA6Qtml7mHsJkuxEb/
                                dt3gvzrzjpiY+Ba82zgt3w==
                                )
```

These records correspond to a key pair created on Fri, 9 Jan 2015. One of these records should be provided to your parent zone to establish the DNSSEC chain of trust.

Note: According to RFC 4035, the TTL of the DS record SHOULD match the TTL of the corresponding NS record set. Please adjust the TTL in the above record (86400) as needed.

DNSSEC Sign and Serve: Active Alerts

Status: 0 Critical Alert(s), 1 Warning(s) are currently active.

PRIORITY	ALERT TYPE
Warning	No DS record in parent zone

The Current Problem

Luna Control Center

https control.akamai.com/portal/adns/adns_detail.jsp?zone=dnssec.akamaidemo.com

Weather News Melrose Blogs Stocks Akamai Stuff Misc. Stuff Recipes Popular Civil War Reenactor Adam's List

Luna Control Center

Akamai Donald Lehman | 4 Messages | 60 Alerts | | Marketplace | Support | LUNA Control Center

Akamai Technologies - Assets MONITOR CONFIGURE PUBLISH RESOLVE PLAN

Akamai Technologies - Assets-1-3CV382 Test1 Test Manuel

Zone Transfer Status Details

Fast DNS | **Zone Transfer Status Details**

If you have a zone transfer status error, please open a ticket with Akamai Customer Care.

Zone:	dnssec.akamaidemo.com
Last Zone Status:	All name servers are up to date
Current SOA serial number:	1420822885

Current DS Record

The most recent DS record is:

```
dnssec.akamaidemo.com. 86400 IN DS 17613 10 1 ( 9a5177469e7cefcf30a719f2d50170be2bdc2400 )
```

The corresponding Key Signing Key DNSKEY record is:

```
dnssec.akamaidemo.com. 7200 IN DNSKEY 257 3 10 (
                                Av//xYLPcCkEt2BFM7C+mzIE8Dn6QoMb5KO0
                                IGAu5uZGEHx6KVVoOZJnQ9dbieC2WOHl2Uom
                                rzRGEClDgdorfgaHq7y0Impqn0uuFiMCGGRs
                                EKNKt8wpTpbHnp49HQtRzMu7pkwrhPq2c7BD
                                rSalYFn3udPXT8sXgj55SA5ZSPhSK8IQlCTx
                                StyYhWL2BIilMRxjPYEr2VAqnTjcvERElmrE
                                0f/VY8plQamvhTvbKy9GNVTmXdjqWytTWAM8
                                NL4oRqh45QIk2fxNaW5jWXaucaCk3k2lAZAH
                                aek4lPcfTpuyUFxW2UTA6Qtml7mHsJkuxEb/
                                dt3gvzrzjpiY+Ba82zgt3w==
                                )
```

These records correspond to a key pair created on Fri, 9 Jan 2015. One of these records should be provided to your parent zone to establish the DNSSEC chain of trust.

Note: According to RFC 4035, the TTL of the DS record SHOULD match the TTL of the corresponding NS record set. Please adjust the TTL in the above record (86400) as needed.

DNSSEC Sign and Serve: Active Alerts

Status: 0 Critical Alert(s), 1 Warning(s) are currently active.

PRIORITY	ALERT TYPE
Warning	No DS record in parent zone

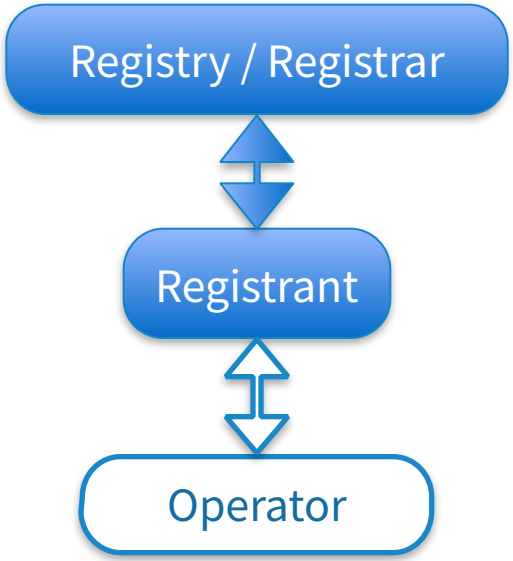
The RRR Model

The RRR Model's Missing Element

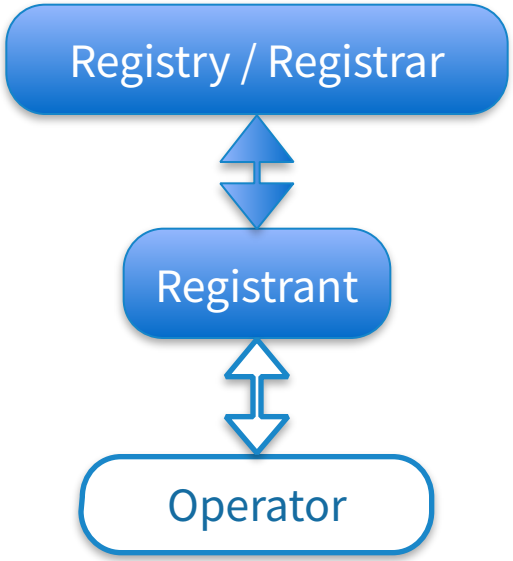
The RRR Model's Missing Element

Third-party operators are second-class citizens
Not formally acknowledged as constituents

The RRR Model's Precursor

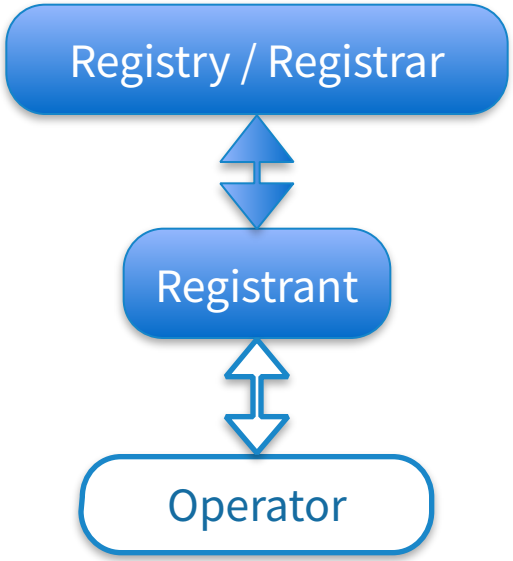


The RRR Model's Precursor



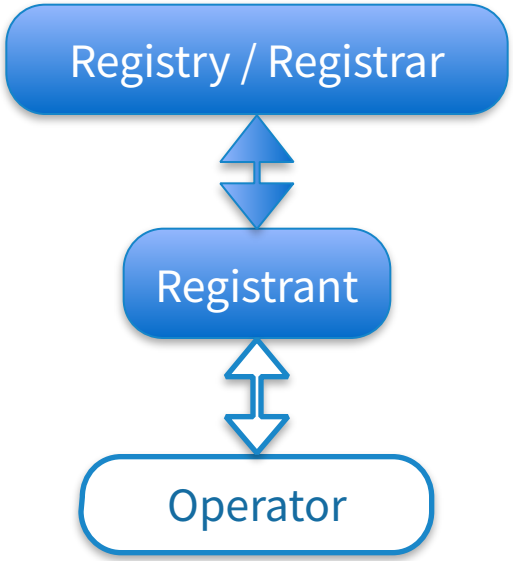
- Operator update problem has existed nearly since the DNS began

The RRR Model's Precursor



- Operator update problem has existed nearly since the DNS began
- Mattered less in the past:
  - Smaller, more technical community
  - Nameserver records rarely changed

The RRR Model's Precursor



- Operator update problem has existed nearly since the DNS began
- Mattered less in the past:
  - Smaller, more technical community
  - Nameserver records rarely changed
- Now another obstacle to DNSSEC adoption

The Original Problem

Akamai Technologies - Assets | MONITOR | CONFIGURE | PUBLISH | RESOLVE | PLAN

Akamai Technologies - Assets-1-6T5ZND > TC-INTERNATIONAL

Fast DNS

To add a new active zone or zones, click **Add Zones**. To edit an existing zone, click the **Edit** link next the zone you would like to edit or use the **Edit Multiple Zones** button to make bulk changes across multiple zones.

ACTIVE ZONES FOR AKAMAI TECHNOLOGIES - ASSETS

ADD ZONES DELETE ZONES

Filter Zone Names: dns Cancel

ZONE	ZONE TRANSFER STATUS	DATE	
dnssec.akamaidemo.com	Primary Zone Created		Status Details Edit

Edit Multiple Zones

The table below lists the Akamai authoritative name servers that serve your zones. Please perform the following actions to ensure that these servers are authoritative:

Update the zone file information on your name servers.
Ensure that zone files have correctly propagated on your name servers.
Provide your registrar with the information found in the table below.

Reassign Nameservers

Note: When you perfom a reallocation of name servers, we will not stop serving your zone information from the old name servers until you have time to switch to the new allocation.

AKAMAI AUTHORITATIVE NAME SERVERS

DOMAIN	TTL	TYPE	RDATA
	2d	NS	a1-98.akam.net.
	2d	NS	a12-65.akam.net.
	2d	NS	a13-65.akam.net.
	2d	NS	a2-64.akam.net.
	2d	NS	a3-64.akam.net.
	2d	NS	a4-65.akam.net.

Zone Transfer Agents

The Akamai Zone Transfer Agent information is now available on the Firewall Rules Notification page.Please allow zone transfers from your name servers to these IP addresses.

The Original Problem

Akamai Technologies - Assets | MONITOR | CONFIGURE | PUBLISH | RESOLVE | PLAN

Akamai Technologies - Assets-1-6T5ZND > TC-INTERNATIONAL

Fast DNS

?

To add a new active zone or zones, click **Add Zones**. To edit an existing zone, click the **Edit** link next the zone you would like to edit or use the **Edit Multiple Zones** button to make bulk changes across multiple zones.

ACTIVE ZONES FOR AKAMAI TECHNOLOGIES - ASSETS

ADD ZONES DELETE ZONES

Filter Zone Names: dns Cancel

ZONE	ZONE TRANSFER STATUS	DATE	
dnssec.akamaidemo.com	Primary Zone Created		Status Details Edit

Edit Multiple Zones

The table below lists the Akamai authoritative name servers that serve your zones. Please perform the following actions to ensure that these servers are authoritative:

Update the zone file information on your name servers.
Ensure that zone files have correctly propagated on your name servers.
Provide your registrar with the information found in the table below.

Reassign Nameservers

Note: When you perfom a reallocation of name servers, we will not stop serving your zone information from the old name servers until you have time to switch to the new allocation.

AKAMAI AUTHORITATIVE NAME SERVERS

DOMAIN	TTL	TYPE	RDATA
	2d	NS	a1-98.akam.net.
	2d	NS	a12-65.akam.net.
	2d	NS	a13-65.akam.net.
	2d	NS	a2-64.akam.net.
	2d	NS	a3-64.akam.net.
	2d	NS	a4-65.akam.net.

Zone Transfer Agents

The Akamai Zone Transfer Agent information is now available on the Firewall Rules Notification page.Please allow zone transfers from your name servers to these IP addresses.

The Consequences

1

Unnecessary Delays

Manual intervention by the registrant to make registrar updates might be as quick as minutes, but is known to be sometimes as long as days, weeks, or even more.

2

Broken Resolution

Several forms of human error — typos, cut-and-paste mistakes, unconfirmed changes, etc — can result in the domain becoming unresolvable for some or all clients.

3

Diminished Resilience

Customers have been known to either enter incomplete lists of authorities, or “re-brand” them as their own, such that they wouldn’t track address updates of their actual authorities. Operators are more constrained regarding changes they can make.

4

Increased Workload

Additional work not only for the customer, but for everyone who has to deal with problems that arise, including their users and other DNS operators.

The Options

1

Tell Operators to Become Registrars

Perhaps an acceptable solution to some operators, but others have no interest in being in the registrar business just to address this problem. Fully one fifth of the Alexa Top 500 domains are casually observed to be run by non-registrar operators.

2

Operators Interface With Registrars

Historically many registrars have shown little interest in supporting DNS changes, with it taking until the 2013 ICANN Registrar Accreditation Agreement to compel them to have some way of relaying DNSSEC data. Very hard to tell where to send updates.

3

Operators Interface With Registries

Preferential, from a simplicity standpoint. Fewer entities to deal with, and registries have typically had more interest in supporting DNS innovation. Complicated by the Registry/Registrant barrier. Likely would involve updates via EPP rather than DNS.

4

Do nothing

This is, of course, always an option. Continue the status quo with all of the downsides that entails.

Relevant Work

- **CSYNC** — https://tools.ietf.org/html/draft-hardaker-dnsop-csync
  - Intended to allow nameserver delegation records and addresses to be pulled up to the parent via DNS polling.
  - Explicitly not intended for initial delegation configuration ("bootstrapping").
  - Cumbersome in large registries.
  - Doesn't use EPP pipeline for registry updates.

- **CDS / CDNSKEY** — https://tools.ietf.org/html/rfc7344
  - Like CSYNC for DNSSEC records
  - Similar limitations with regard to bootstrapping, polling, scaling and EPP.

- **UPDATE** — https://tools.ietf.org/html/draft-andrews-dnsop-update-parent-zones
  - Uses existing, well-deployed protocol, but in a new context.
  - Expects registrars to translate updates to EPP instructions.
  - Attempts to address the problem of finding the correct registrar to contact.

- None of the above remotely attempt to address business relationships, and how to establish that a given operator is acting with appropriate consent on behalf of the registrant. This is ICANN's purview.

In Summary

1. Operators need a way to insert and maintain registry data.
2. Protocol work is needed, but only goes so far.
3. ICANN policy changes are necessary to succeed.

Thank you

David C Lawrence
tale@akamai.com

ICANN AT-LARGE

Akamai
FASTER FORWARD