

DNSSEC Workshop

**I C A N N**  
**P O L I C Y F O R U M** | 59

**JOHANNESBURG**  
26–29 June 2017

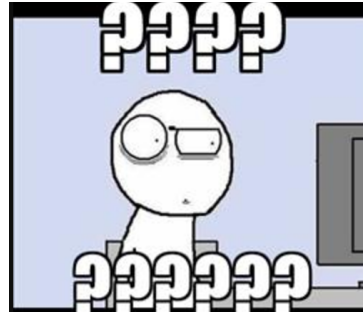
Family Matters:  
Improving the Parent/Child Relationship

David C Lawrence

Akamai Technologies  
tale@akamai.com



## Domain Holders Need to Get Delegation-Related Information into Their Parent Zone



- Many do not understand the Domain Name System
- Many do not want to be involved in regular operations
- Third-party operators to the rescue!

## The Shared Registry System (SRS) Recognizes Three Actors

### The RRR Model



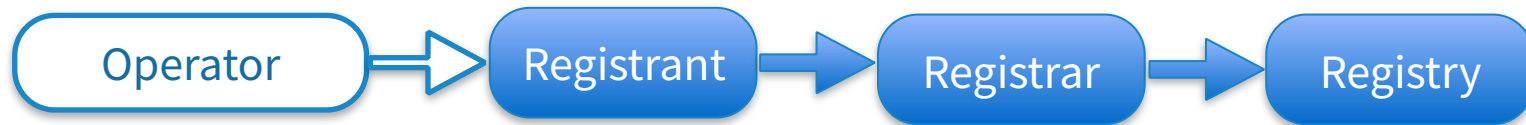
Formal data-flow relationships exist only between each level



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

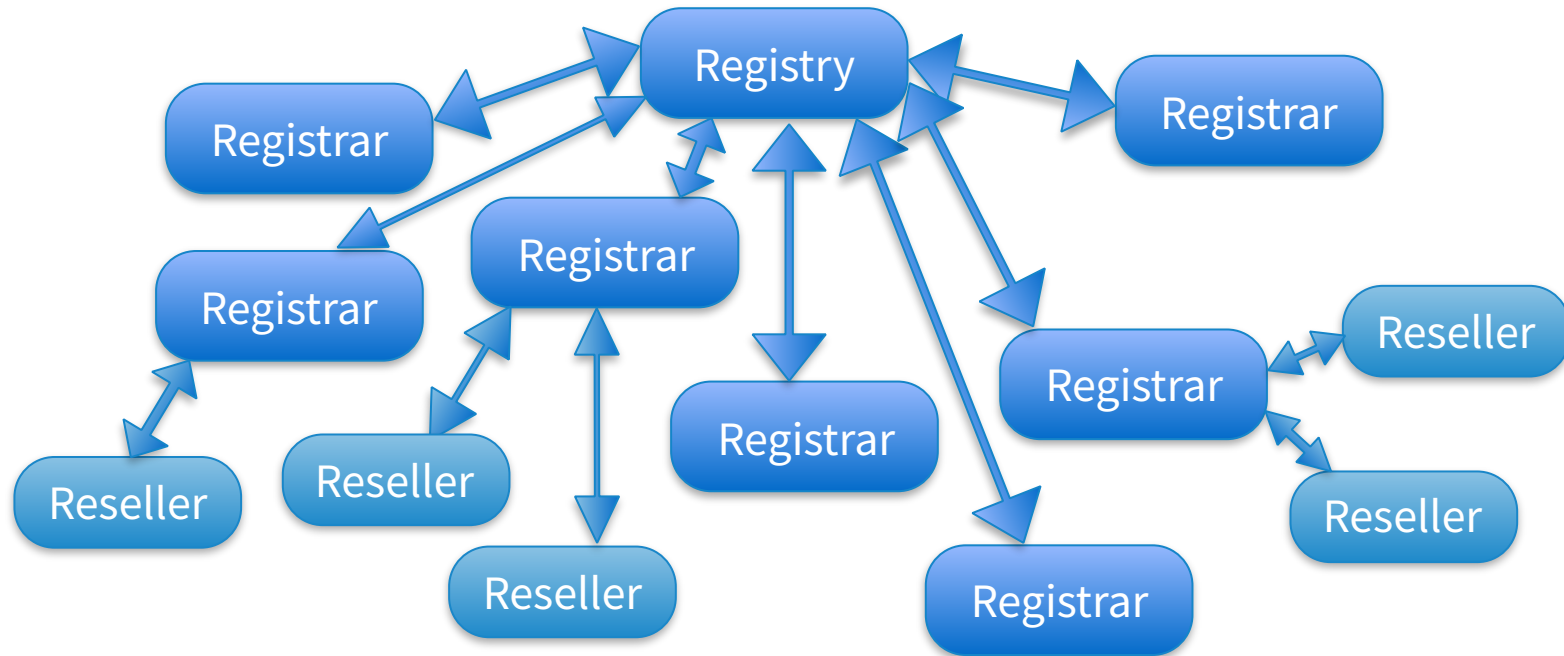
## Operators Need To Maintain Delegation Information

- Nameserver and DNSSEC records come from the operator
  - NS, DS, DNSKEY; sometimes “glue” A and AAAA
- Require registrant action to update registrar to push to registry
- Getting registrants to do this can be a huge obstacle
- Getting registrars to support some records is also problematic



- Some technical parts of a possible solution exist:
  - RFC 7477 defines CSYNC for NS, A, and AAAA (and more)
  - RFC 8078 defines CDS and CDNSKEY for DS and DNSKEY
- Each allows data published in the child to update the parent
- Neither supports bootstrapping initial delegation data
- Still need support from registrars and registries

## The RRrrRRRrrrrrrRrrRRRRrrrrrrRRrRRrRRR Model



- Getting the multitude of middlemen to support new DNS features is hard
- Many still don't even adequately support basic DNSSEC records

1

## Unnecessary Delays

Manual intervention by the registrant to make registrar updates might be as quick as minutes, but is known to be often 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.



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.



**1**

Operators need a way to insert and maintain registry data.

**2**

More technical work is needed, but only goes so far.

**3**

ICANN policy changes are necessary to succeed.

# Thank you

David C Lawrence  
tale@akamai.com