CLOUDFLARE®

DNS operator updating DS

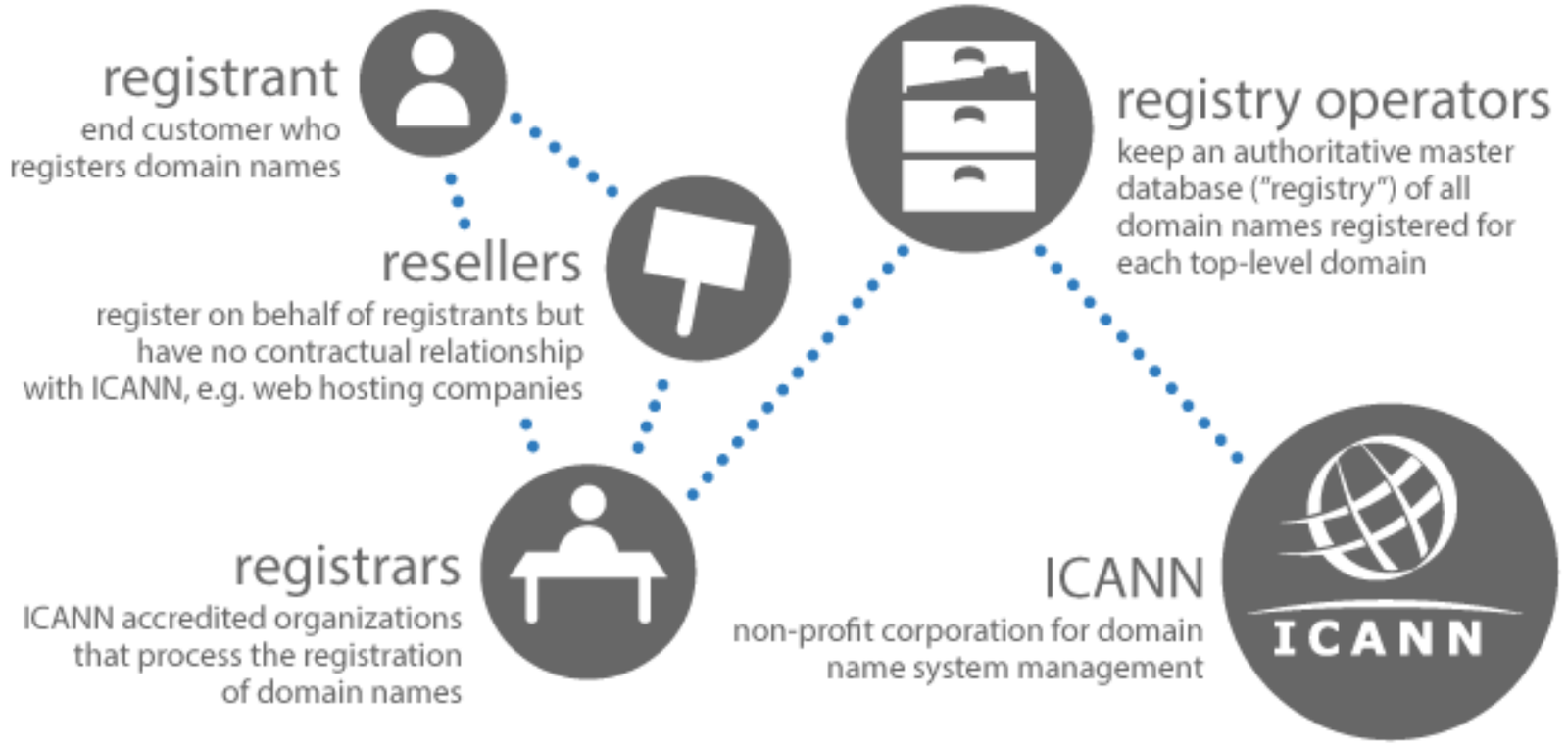
draft-latour-dnsoperator-to-RRR-protocol-03

Ólafur Guðmundsson olafur at CloudFlare.com
with Jacques Latour, Paul Wouters and Matthew Pounsett

What is the issue?

- DNS Operator wants to submit DS record to Parent for a domain it operates with DNSSEC

Where is the DNS Operator ?



domain registry process

Requirements

- Ability to publish and maintain DS record(s) for a domain hosted by a third party DNS operator
- Avoid domain hijacking
- Avoid making domain fail verification
- Security going forward
- Support all DS operations (create/update/delete)

Proposal: Simple protocol

- DNS operator
  - publishes CDS/CDNSKEY in the zone
  - visits URI for Parent requesting DS operation
- Parent
  - Checks if it is allowed to perform action ==> does checks and inserts DS reflecting CDS/CDNSKEY
  - **Parent can be Reseller, Registrar, Registry, corporate IT department or outsourced entity**

what does it look like

4.4.3. DS Maintenance (Key roll over)

4.4.3.1. Request

Syntax: PUT /domains/{domain}/cds

4.4.3.2. Response

- HTTP Status code 200 indicates a success.
- HTTP Status code 400 indicates a failure due to validation.
- HTTP Status code 404 indicates the domain does not exist.
- HTTP Status code 500 indicates a failure due to unforeseeable reasons.

Open Issues

- RFC7344 only covers updating
- DNS operator is unknown to Parent
- Finding Parent is hard
- This is a violation of contracts
- Authentication model
- draft-ietf-dnsop-maintain-ds
- Parent challenge can be added to zone
- RDAP to the rescue, we hope to include URI
- Seriously
- Separate discussion

Please adopt: urgent need

- Do we specify RDAP option here or in a different document ?
  - Can we expect RDAP deployment anytime soon?

- Running code interoperability test: Talk to Olafur