Syncing Delegation information from DNS operator

Ólafur Guðmundsson Cloudflare
Pascal Bouchareine, Gandi
Goal: Allow 3’rd party DNS operator to update DS/NS records

According to ICANN RRR model 3’rd party DNS operator does not exist

Reality is different (solvedns.com)
Lifecycle of domain at 3’rd party operator

Domain added ⇒ **Registrant** updates NS records at Registrar

Actions while domain is at 3’rd party DNS provider

  - Domain Signed ⇒ DS needs to be added/updated
  - domain moves servers ⇒ NS needs updating
  - Domain drops DNSSEC ⇒ DS needs deleting

Domain moves to another operator ⇒ **Registrant** updates NS at Registrar
Who else needs to update domain? *Outside scope*

- Email systems MX, SRV, TXT, SPF …
- Web provider: CNAME, A, AAAA, TLSA,
- Security providers: CAA, TLSA, A, AAAA
- Departments/teams ……

- In short any outsources and/or internal teams/divisions

- Domain Connect from GoDaddy attempts to solve this problem
- Gandi has a similar attempt using RDAP, DNS and URI’s
Delegation Automation goals

#0 No humans in the loop,  
      ---- possibly during setup phase

#1 DNS records are always in sync at parent and child Name servers

#2 Allow enabling and disabling DNSSEC

#3 Allow DNSSEC Key rollover

#4 Automatic detection of current Registrar
State of the world

- Most Registrars have one account for users that is all powerful
  ⇒ no good for sharing
- Finding registrar/reseller of-record is hard/impossible
  → Registry knows Registrar who may know Reseller
- Some Registrars provide API for customers but not non-customers
- ICANN world is full of rules/tradition who is NOT Allowed talk to who
Detection of current Parental Agent i.e registrar

- Whois is not adapted to service discovery:
  - Lax format makes it hard/impossible to parse
  - Rate limiting everywhere
  - Even with whois referrals, heterogeneous among registries

- RDAP has more interesting attributes:
  - Based on HTTP and could redirect for delegation
  - Using JSON and a more formal spec
  - Could take advantage of RDAP links (RFC7483 4.2) and Web linking extension relation types (RFC5988 4.2)

- Unclear how to implement delegation yet:
  - Thick registries: will probably not refer to registrar RDAP service through HTTP redirects
  - No real standard to delegate service discovery (links ?)
Outline of system

3DNS providers prefer to talk to Parental Agent in this order
[Reseller/]Registrar]/Registry/Registrant (R*)

- R* provides a Web API that can be used to trigger actions on domains:
  - Check if domain can be “automated”
    - YES/NO/Referral
    - If YES: Ask to Create/Update/Delete DS
  - If YES and DS in place check if NS can be maintained?
    - YES/NO
    - If YES then ASK sync NS
Real-life implementations (1/3)

- Existing implementations of dnsoperator-to-rrr (github):
  - DSAP, python implementation by CIRA - and real life domains for testing
  - RRR, python implementation by Gandi
- Available for key rollovers:
  - Using cdscheck.gandi.net for automatic key rollover with DNSSEC-validating DS records:
    ```bash
    pb@foo:~ curl -XPUT https://cdscheck.gandi.net/v1/domains/100k.fr/cds
    {"status": "success", "rel": 83494086}pb@foo:~
    pb@foo:~
    ```
- Also available for initial DS setup by the DNS operator, but with credentials and a DNS challenge
Real-life implementations (2/2)

Service discovery experimentations using RDAP:

```
$ curl -s rdap.gandi.net/domain/100k.fr | jq '.links[] | select(.rel == "http://rdap.io/tpda/cdscheck")'
{
  "href": "https://cdscheck.gandi.net/v1",
  "rel": "http://rdap.io/tpda/cdscheck"
}
```

Experimental federation for interested registrars and DNS operators: 
[https://rdap.io/](https://rdap.io/)

- Provides an RDAP service
- Can help locate registrar RDAP endpoint, and services endpoints
- Has a more complete spec for NS delegations, zone setup, etc.
Real-life implementations (3/3)

.DK registry provides interface for DNS operators

curl -X POST -F "userid=C999999-DK" -F "password=1234567890#Abcdefg"
-F "domain=sampleNonExistingDomain.dk" -F "keytag1=2371"
-F "algorithm1=13" -F "digest_type1=2"
-F "digest1=6ddd1edb9d586ccdf9257a71841887d3e6ee63b3b5ed74605befe97"
https://dsu.dk-hostmaster.dk/1.0
Links and Questions

- https://github.com/CIRALabs/DSAP/
- https://github.com/kalou/rrr
- https://rdap.io/
- https://github.com/Gandi/dnsknife/blob/master/docs/extending_registrar_functions.txt