DNS Operator Role
Bootstrapping DNSSEC Chain of Trust

Update since ICANN53 Buenos Aires

ICANN54 Dublin

DNSSEC Workshop

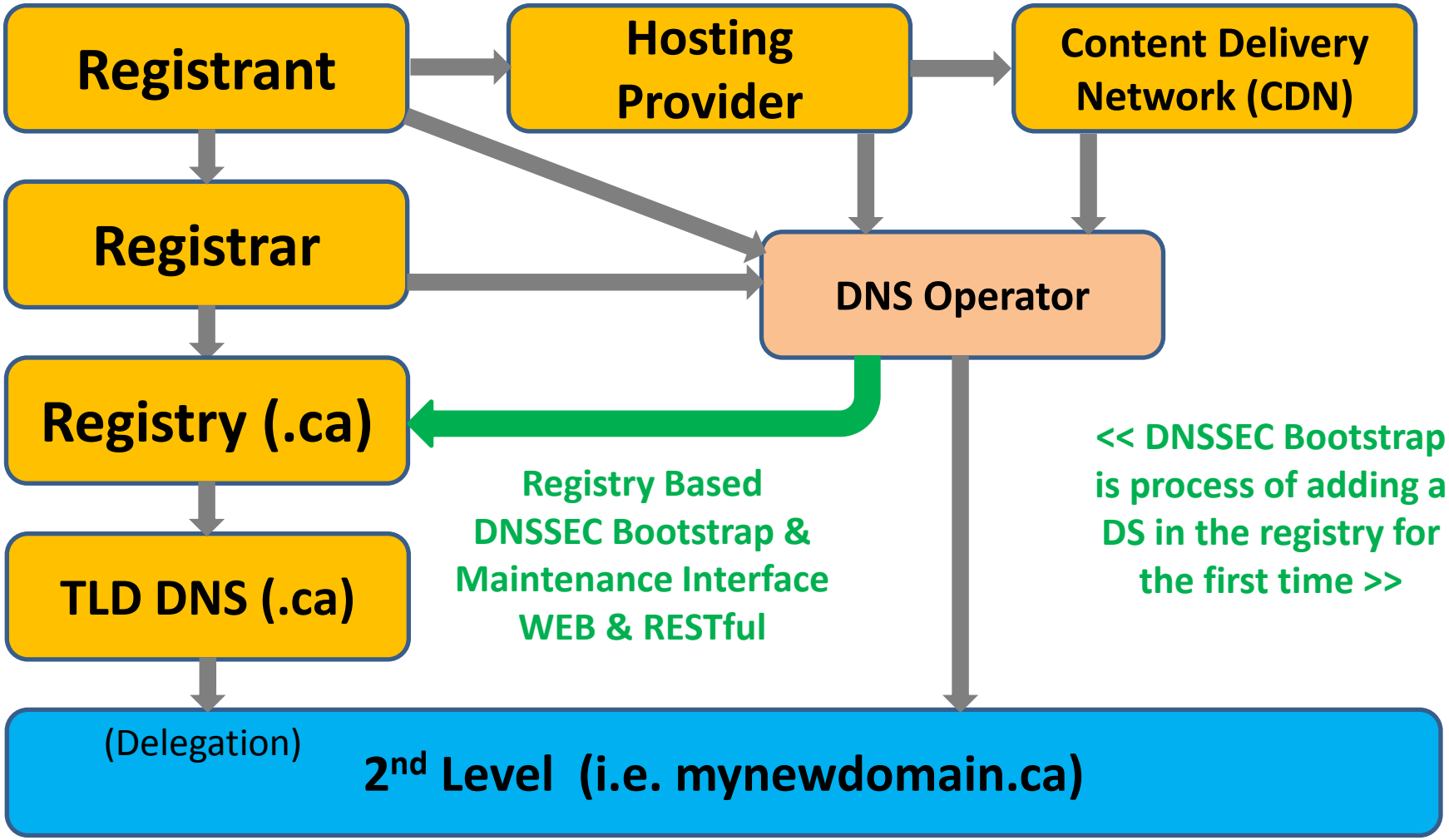
Latour - October 21, 2015

Last update – ICANN53

- DNSSEC Workshop – June 24, 2015

  https://buenosaires53.icann.org/en/schedule/wed-dnssec/presentation-dnssec-operator-role-domain-management-24jun15-en

DNSSEC Bootstrap - Revised



DNSSEC Bootstrap Validation Process

- The validation process ensures @ each name servers over TCP, that;
  - The RRsig signatures are valid (properly signed)
  - The NS RRset at parent and child are valid
  - CDS/CDNSKEY records matches DNSKEY
- The process is to make sure it's signed and delegated properly and ready
  - If already bootstrapped then ignore duplicate requests
  - If not signed properly, provide message why it failed

DNSSEC Bootstrap Validation Process

- The DNS Operator needs to prove they control and operate the properly signed and delegated 2nd level domain.
  - Control is proven by adding valid CDS/CDNSKEY record
  - Operate is proven by submitting a request at the registry (.ca) via web gui or RESTful API to trigger the bootstrap process. (so we don't poll 2.4M domains a day)

DNSSEC Unsecure Process

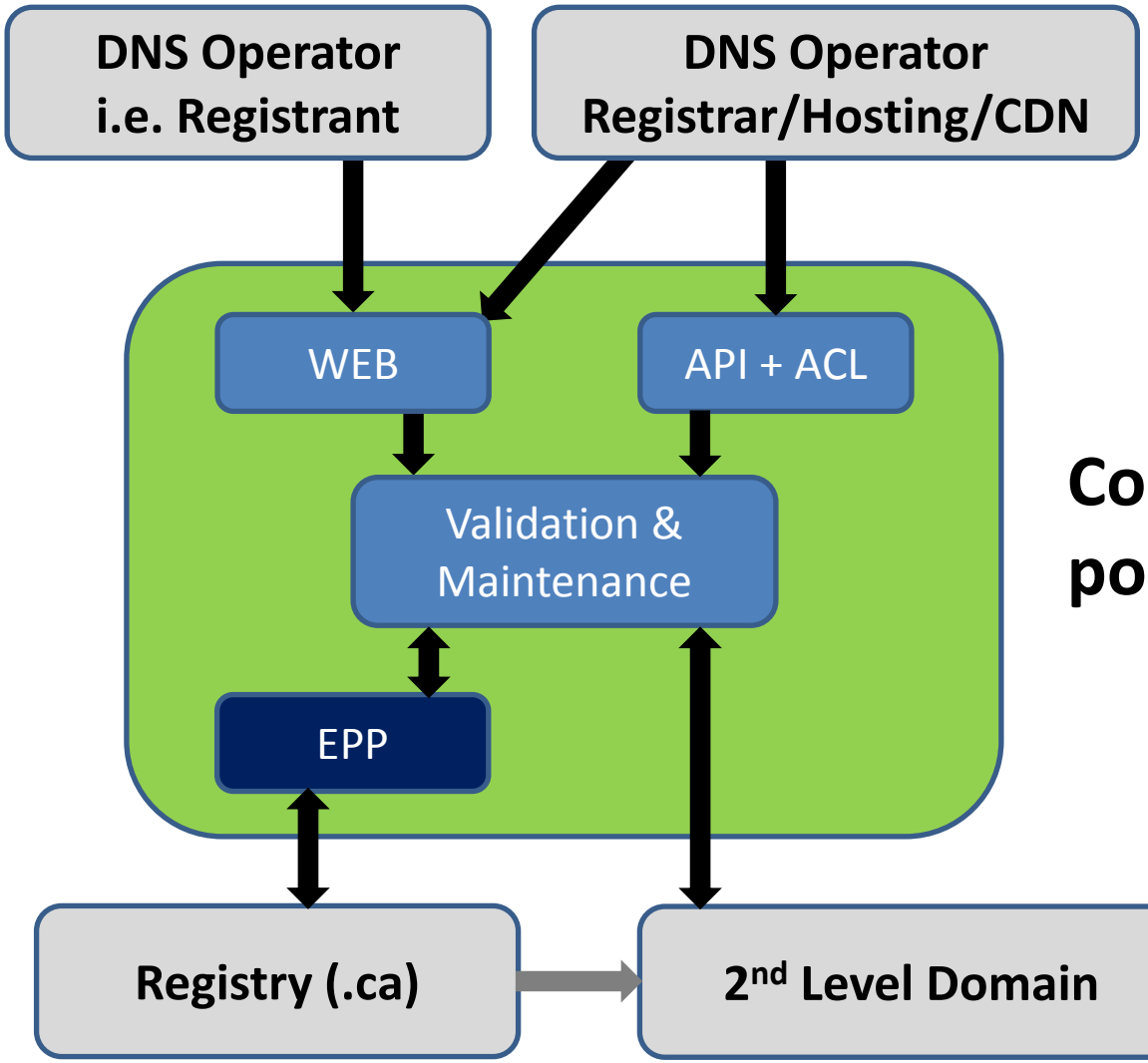
- To unsecure a delegation, when changing DNS Operator and key transfer is not possible, then the DNS Operator may want to unsecure the delegation;
  - Control is proven by adding a **null** CDS record (properly signed)
  - Operate is proven by submitting a request at the registry (.ca) via web gui or RESTful API to trigger the DS removal.

Maintenance Approach CDS/CDNSKEY Records

- The .ca Registry will take care of performing on-going DNSSEC maintenance of signed domains.
  - Daily (or specific frequency) polling for new CDS/CDNSKEY RR
  - Manage as per .ca DNSSEC policy (# keys, DS, Algo, etc…)
  - TBD: 48 hours hold + notify admin/tech contacts?
  - .ca controls the DS format… Create new DS when value in CDS/CDNSKEY are not compliant

```
[root@fedora ~]# dig cds demo.nohats.ca +short
58691 8 2 B5B99B5FBAA7565C49710DCF21137E69EF996C1FC04903BAB4B9397E 5D1BCB09
```

DNSSEC Provisioning Model



Code should be portable to Registrars

WIP - Code Development

- CIRA Registry EPP code development WIP
- Planning pilot project with Cloudflare
- The WEB & RESTful API interface prototypes
  - http://cira.nohats.ca
  - http://cira.nohats.ca/gends/

Strategy

- Continue framework development
  - Gather & include feedback
- Bind & OpenDNSSEC: asked to support CDS for bootstrap and to unsecure delegations.
- Make code Open Source for all to use
- Standardize - write draft about this process
- + draft on how to “Find "parental Agent" with RDAP (finding the registry/registar/reseller) that performs this function

Thank you!

DNSSEC-AUTO-DS

dnssec-auto-ds@elists.isoc.org

DNSSEC Coordination

dnssec-coord@elists.isoc.org