ICANN57 DNSSEC WORKSHOP DS AUTOMATED PROVISIONING (DSAP)

Presented by:

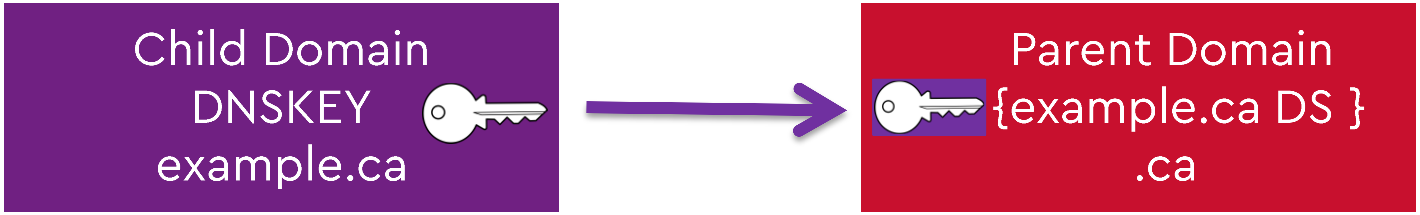
Jacques Latour

November 7, 2016

ICANN57 – Hyderabad - India

TODAY'S DNSSEC IMPLEMENTATION IS NOT USER FRIENDLY

- To create a chain of trust in DNSSEC, or to perform DNSSEC maintenance, the DNS Operator must provide the Registry one or more Delegation Signer (DS) record(s).



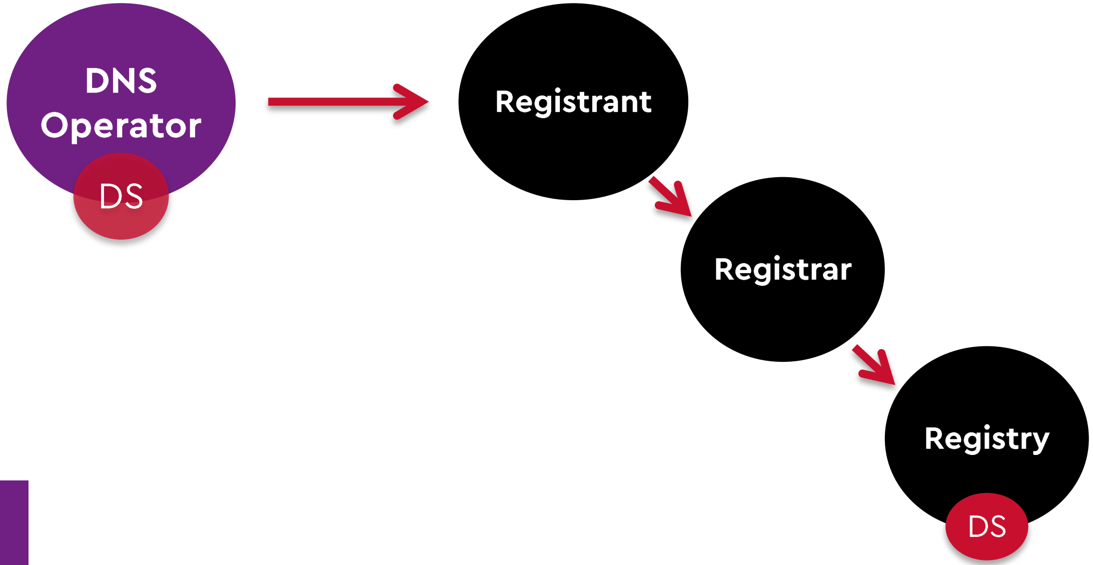
Child Domain
DNSKEY
example.ca

Parent Domain
{example.ca DS }
.ca

- Current method is for Registrar to submit DS record to the Registry via EPP

THE PREFERRED DNSSEC BOOTSTRAP METHOD

- Establishing the initial DNSSEC chain of trust through the standard Registrant, Registrar and Registry (RRR) model is preferred and recommended method, when possible.

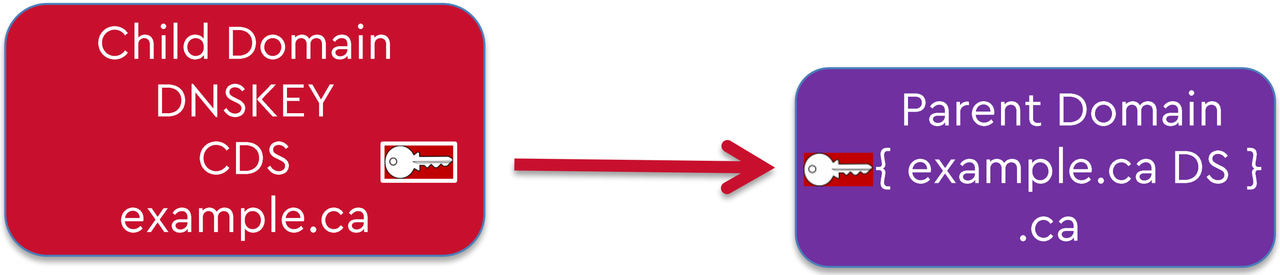


CDS (RFC7344) - THE FIRST SOLUTION FOR PARENT-CHILD SYNCHRONISATION

Third Party DNS operator to Registrars/Registries Protocol
draft-ietf-regext-dnsoperator-to-rrr-protocol

Managing DS records from parent via CDS/CDNSKEY
draft-ietf-dnsop-maintain-ds-03

The child zone uses CDS to signal and instruct the parental agent to create or delete DS record(s)



Child Domain
DNSKEY
CDS
example.ca

Parent Domain
{ example.ca DS }
.ca

WHAT IS A CDS?
A SIGNAL TO THE PARENT

```
cira-dsap-5.ca.   30   IN   CDS   12595 8 2 C6BC5DFF50A7673C904336D1..B72FC3 9BAB7DA8
cira-dsap-5.ca.   30   IN   DS    12595 8 2 C6BC5DFF50A7673C904336D1..B72FC3 9BAB7DA8
```

- Seen for the first time by the parental agent, a CDS signals the desire to establish the initial secure delegation (bootstrap)
- While the secure delegation is established, the presence of a CDS signals the addition or removal of a DS record (maintenance).
- A 'null' CDS record signals the intent to remove the secure delegation

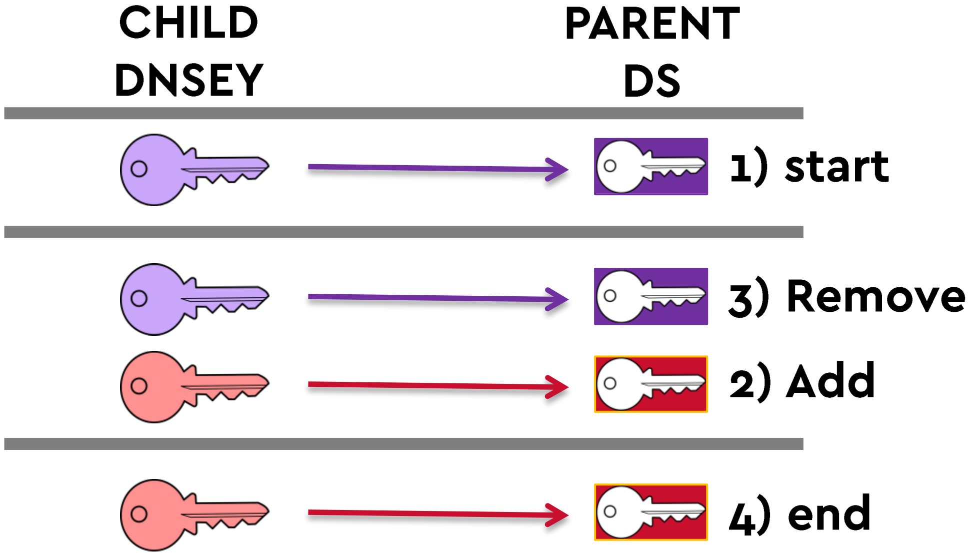
MAINTENANCE - DNSSEC KEY ROLL OVER USING (COPYING) DS

- Multiple interactions with the Registrar is required to roll a key
  1) add the DS of the new key
  2) later, remove the old DS record & key

Generally not supported by Registrars

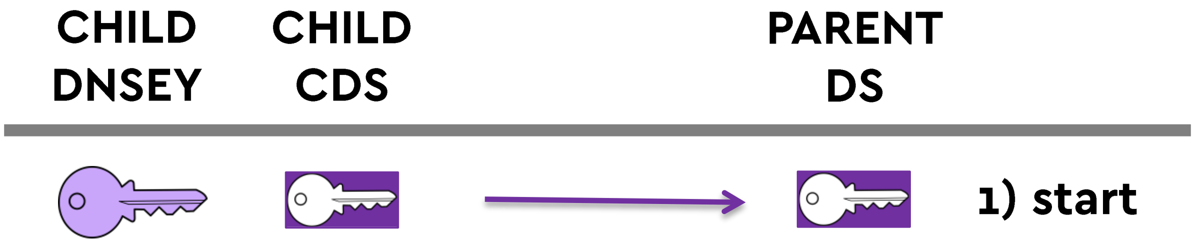
Often a manual process

Copy/paste crypto prone to error



MAINTENANCE - DNSSEC KEY ROLL OVER USING CDS

- Automated process



CHILD DNSEY

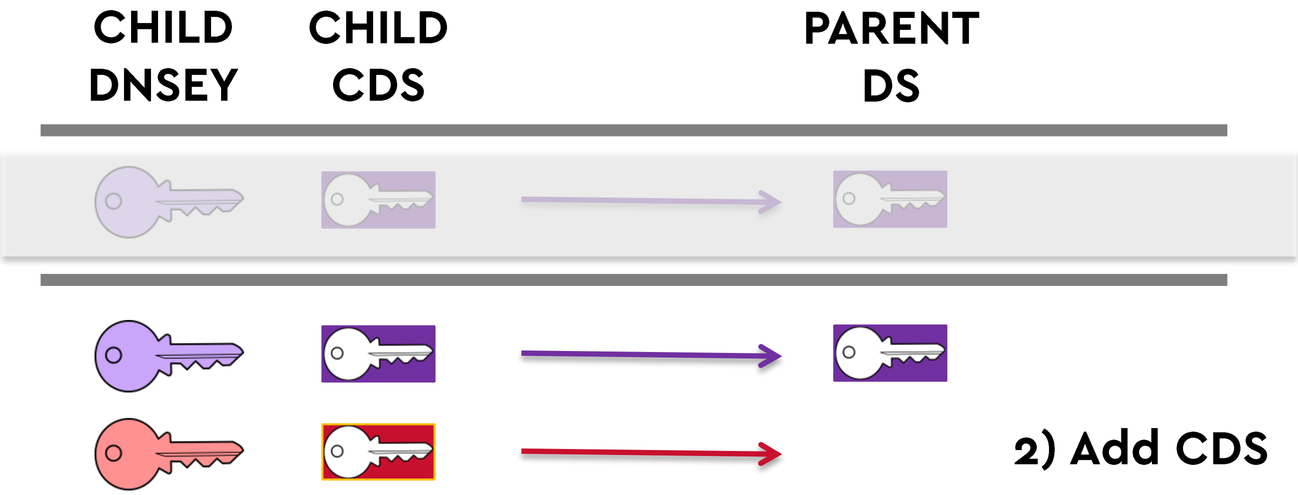
CHILD CDS

PARENT DS

1) start

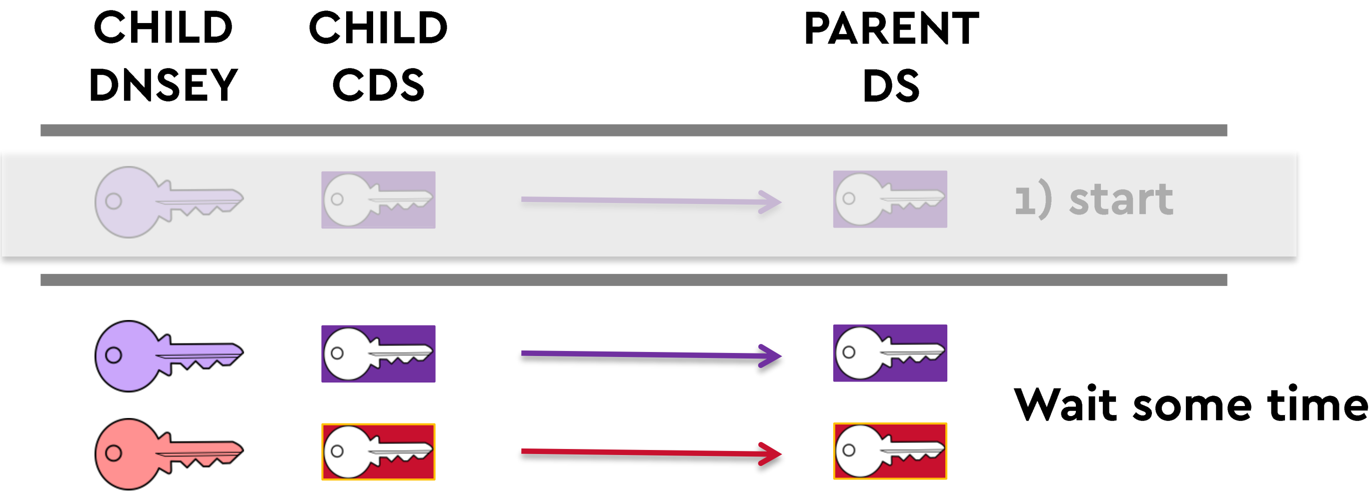
MAINTENANCE - DNSSEC KEY ROLL OVER USING CDS

- Automated process – Signal to:



MAINTENANCE - DNSSEC KEY ROLL OVER USING CDS

- Automated process – Signal to:



CHILD DNSEY

CHILD CDS

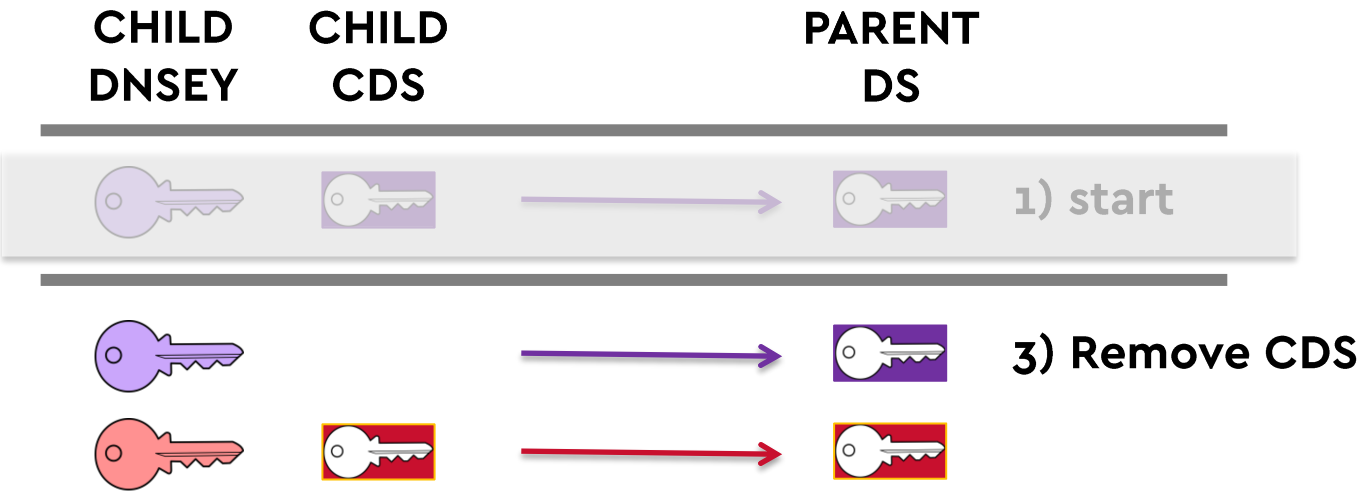
PARENT DS

1) start

Wait some time

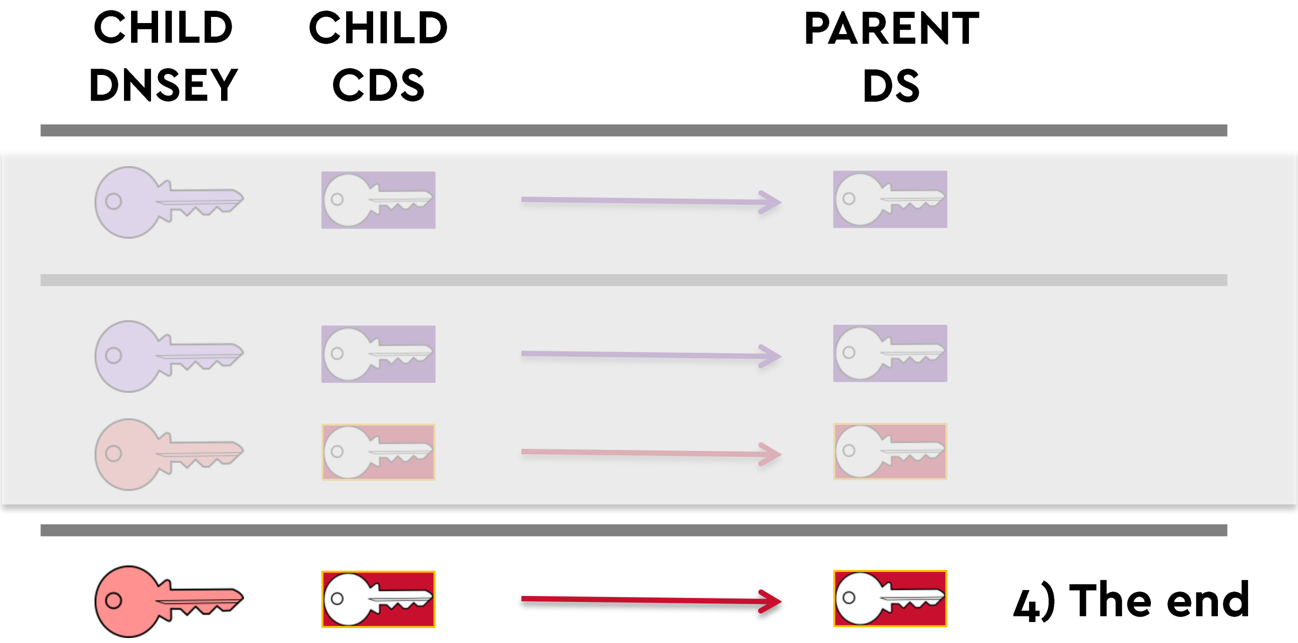
MAINTENANCE - DNSSEC KEY ROLL OVER USING CDS

- Automated process – Signal to:

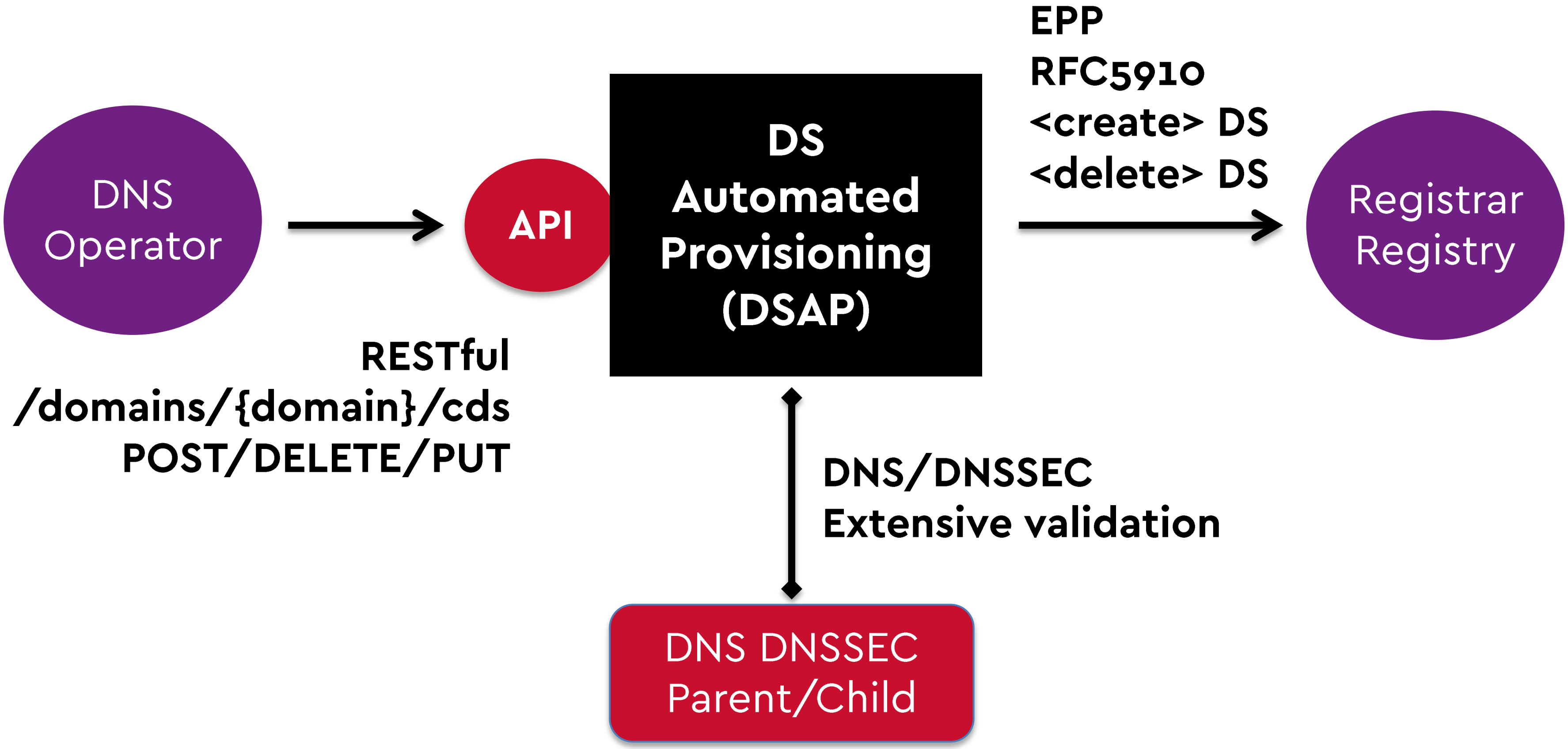


MAINTENANCE - DNSSEC KEY ROLL OVER USING CDS

- Automated process



DS AUTOMATED PROVISIONING (DSAP) COMPONENTS



DNS Operator

API

RESTful
/domains/{domain}/cds
POST/DELETE/PUT

DS Automated Provisioning (DSAP)

EPP
RFC5910
<create> DS
<delete> DS

Registrar Registry

DNS/DNSSEC
Extensive validation

DNS DNSSEC Parent/Child

EXTENSIVE VALIDATION PROCESS

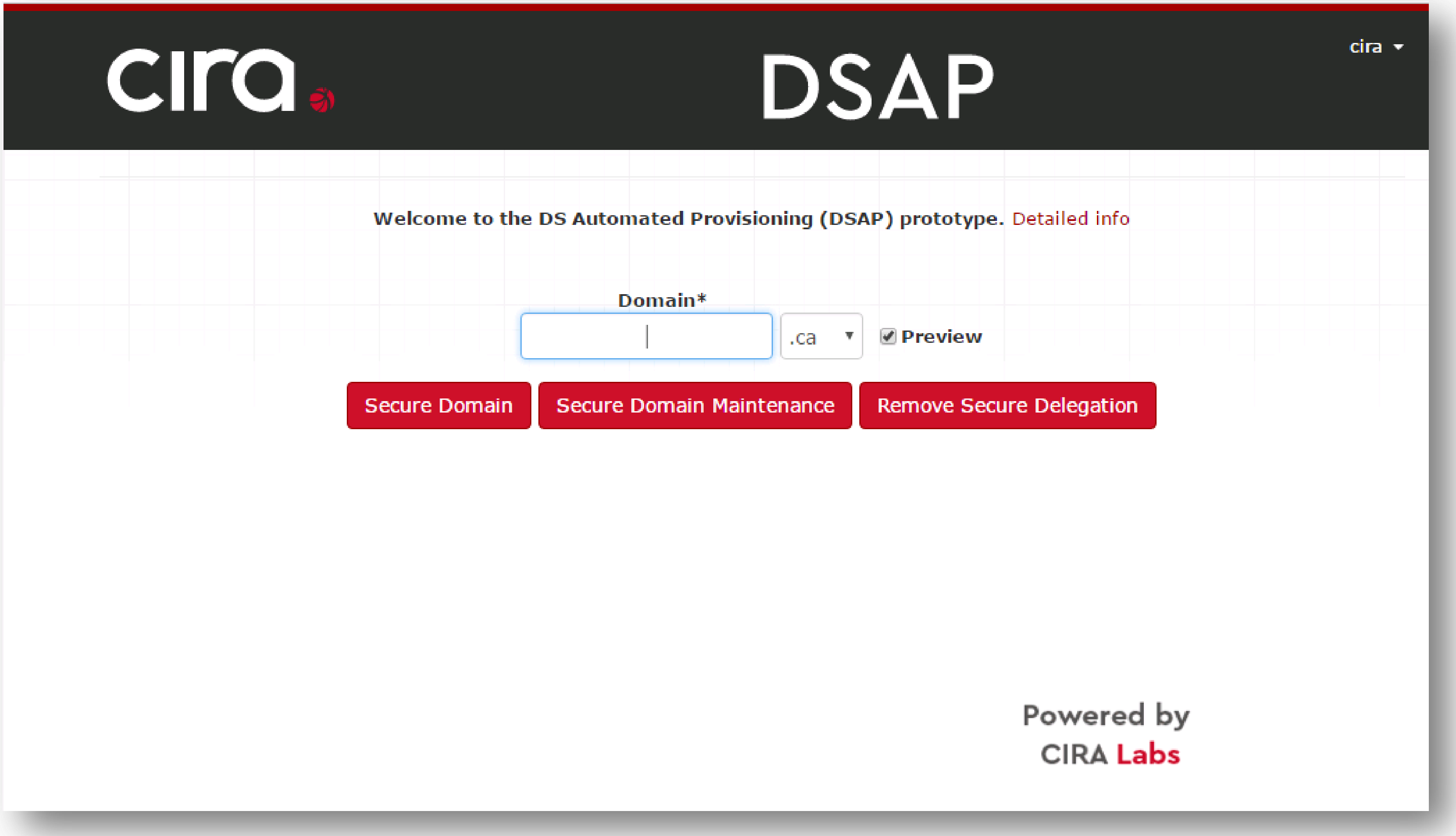
- Recursively query parent and child and ensure all name servers NS record are in sync, and that all child name servers respond to CDS and DNSKEY identically with DNSSEC validation, over TCP.
- Verify for 'excellent' domain 'hygiene'
- Think of:
  - Use zonemaster validation process?
  - Bulk validation, avoid duplication

CIRA DEVELOPED A DSAP PROTOTYPE

- DSAP Prototype: https://dsap.ciralabs.ca
- GitHub DSAP code: https://github.com/CIRALabs/DSAP
- CIRA created 5 test domains with various configuration to test the API.
  - CIRA-DSAP-1.CA, initial secure delegation – add DS
  - CIRA-DSAP-2.CA, validation failure - lame delegation
  - CIRA-DSAP-3.CA, remove secure delegation (DS)
  - CIRA-DSAP-4.CA, maintenance, remove a DS record
  - CIRA-DSAP-5.CA, maintenance, add a DS record

```
# dig cds cira-dsap-5.ca
```

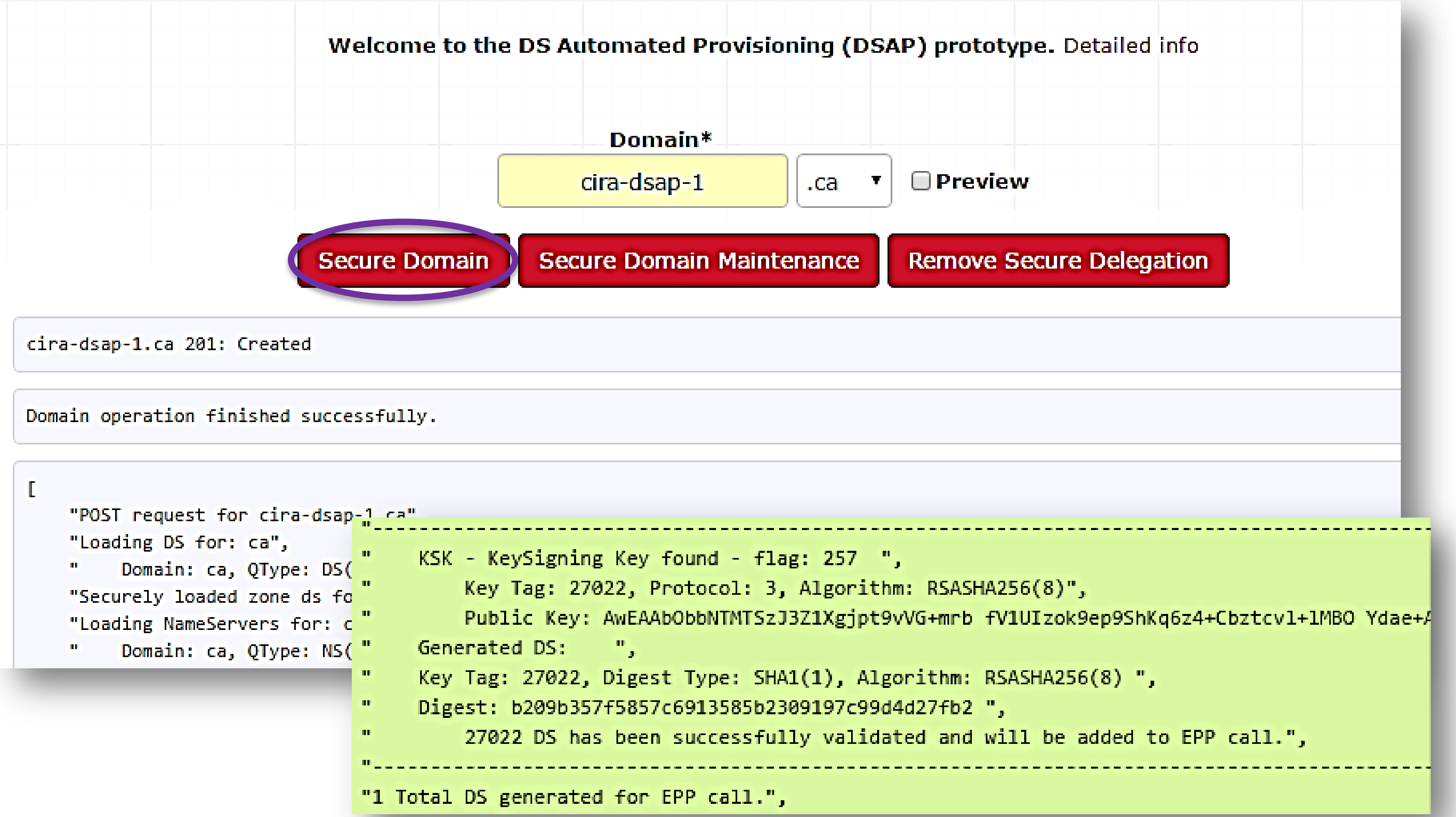
DEMO – CIRA LABS DSAP PROTOTYPE (SLIDES IN CASE YOU KNOW WHAT ☺)



Welcome to the DS Automated Provisioning (DSAP) prototype. Detailed info

Domain* .ca ☑ Preview

CREATE SECURE DELEGATION CIRA-DSAP-1.CA & POST



Welcome to the DS Automated Provisioning (DSAP) prototype. Detailed info

Domain* cira-dsap-1 .ca ☐ **Preview**

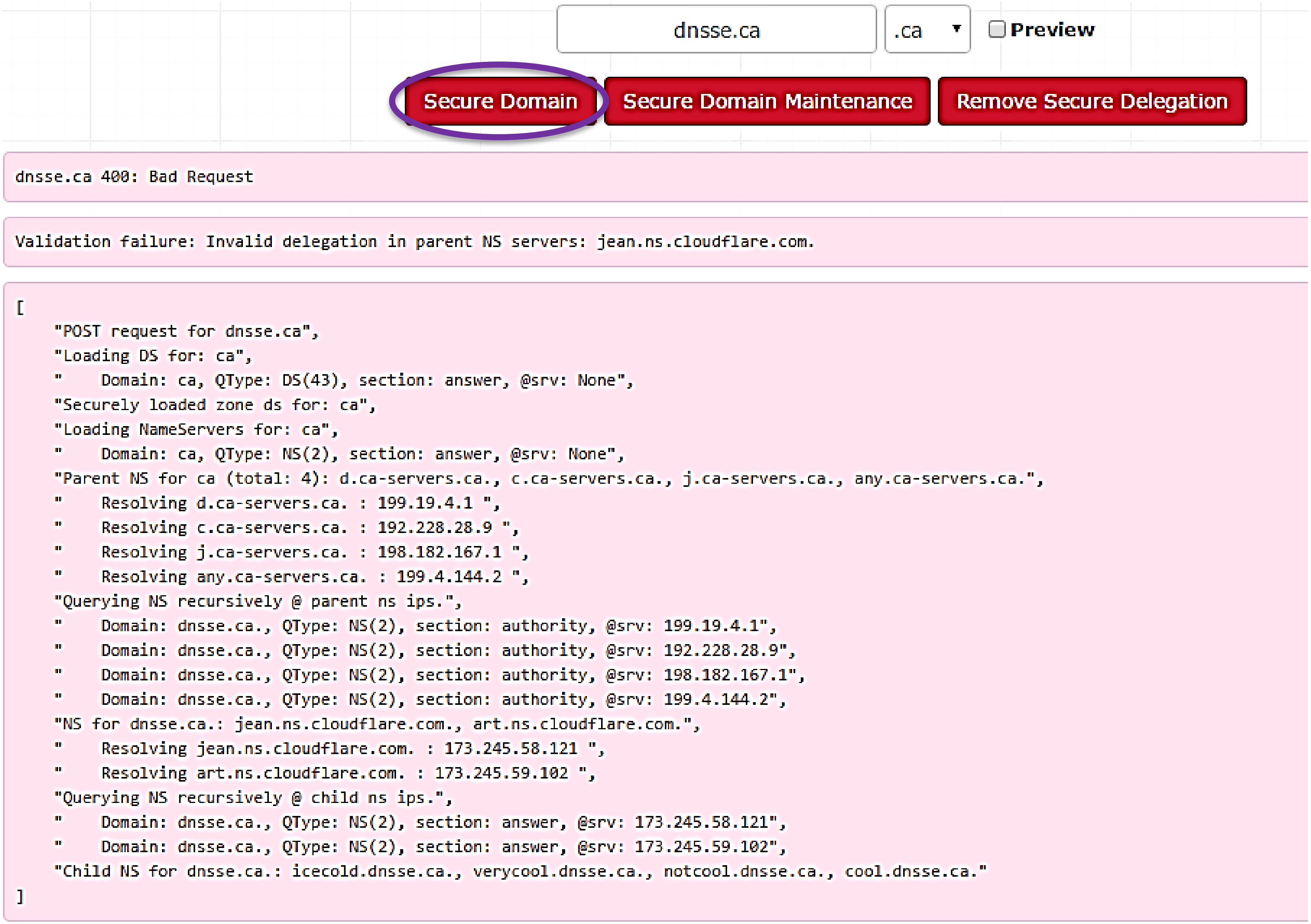
```
cira-dsap-1.ca 201: Created
```

```
Domain operation finished successfully.
```

```
[
    "POST request for cira-dsap-1.ca"
    "Loading DS for: ca",
    "     Domain: ca, QType: DS(
    "Securely loaded zone ds fo
    "Loading NameServers for: c
    "     Domain: ca, QType: NS(
```

```
"-----------------------------------------------------------------------------
"     KSK - KeySigning Key found - flag: 257  ",
"         Key Tag: 27022, Protocol: 3, Algorithm: RSASHA256(8)",
"         Public Key: AwEAAbObbNTMTSzJ3Z1Xgjpt9vVG+mrb fV1UIzok9ep9ShKq6z4+Cbztcvl+1MBO Ydae+A
"     Generated DS:     ",
"     Key Tag: 27022, Digest Type: SHA1(1), Algorithm: RSASHA256(8) ",
"     Digest: b209b357f5857c6913585b2309197c99d4d27fb2 ",
"         27022 DS has been successfully validated and will be added to EPP call.",
"-----------------------------------------------------------------------------
"1 Total DS generated for EPP call.",
```

Test domain with lame delegation



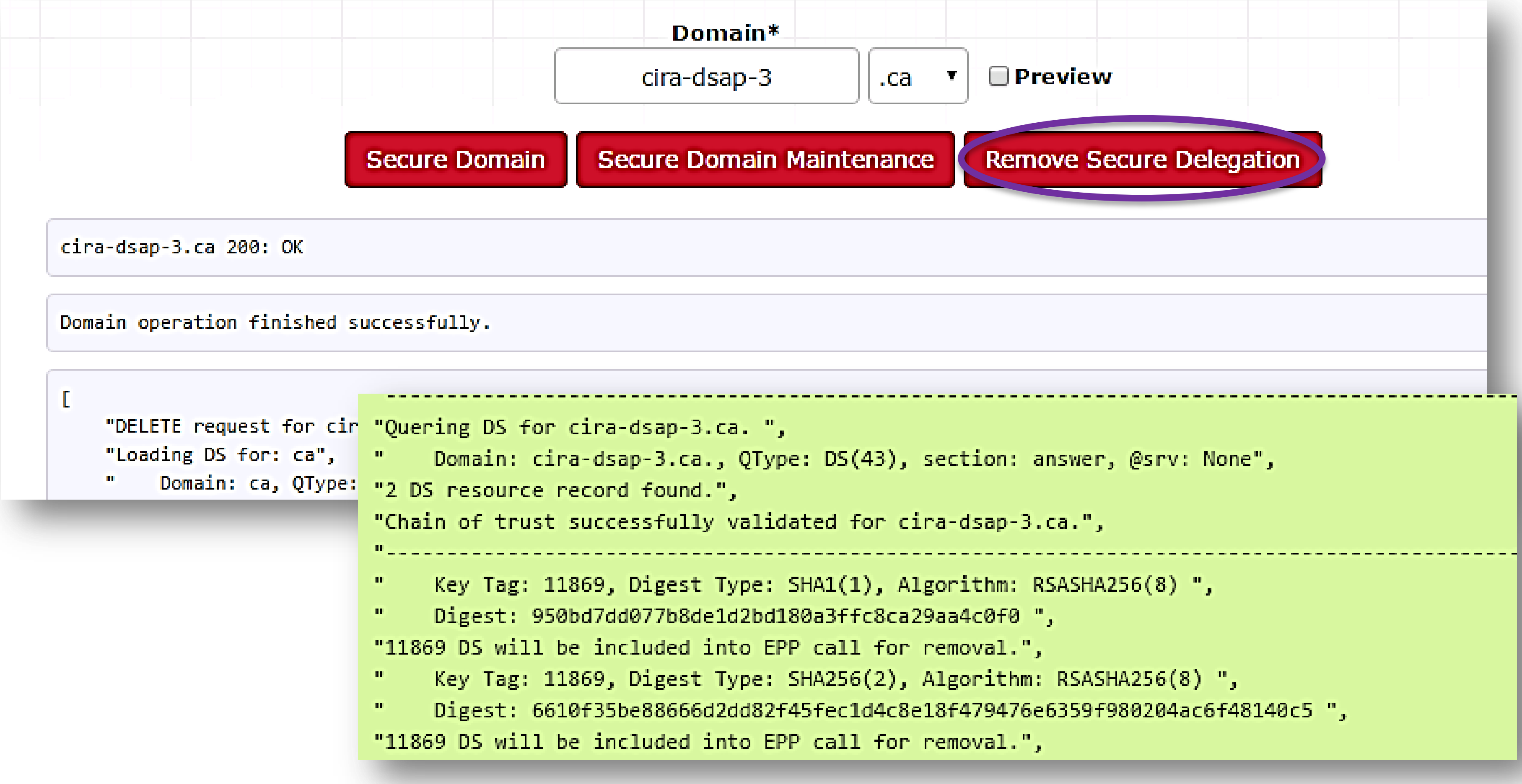
dnsse.ca | .ca ▾ | □ Preview

```
dnsse.ca 400: Bad Request
```

```
Validation failure: Invalid delegation in parent NS servers: jean.ns.cloudflare.com.
```

```
[
    "POST request for dnsse.ca",
    "Loading DS for: ca",
    "    Domain: ca, QType: DS(43), section: answer, @srv: None",
    "Securely loaded zone ds for: ca",
    "Loading NameServers for: ca",
    "    Domain: ca, QType: NS(2), section: answer, @srv: None",
    "Parent NS for ca (total: 4): d.ca-servers.ca., c.ca-servers.ca., j.ca-servers.ca., any.ca-servers.ca.",
    "    Resolving d.ca-servers.ca. : 199.19.4.1 ",
    "    Resolving c.ca-servers.ca. : 192.228.28.9 ",
    "    Resolving j.ca-servers.ca. : 198.182.167.1 ",
    "    Resolving any.ca-servers.ca. : 199.4.144.2 ",
    "Querying NS recursively @ parent ns ips.",
    "    Domain: dnsse.ca., QType: NS(2), section: authority, @srv: 199.19.4.1",
    "    Domain: dnsse.ca., QType: NS(2), section: authority, @srv: 192.228.28.9",
    "    Domain: dnsse.ca., QType: NS(2), section: authority, @srv: 198.182.167.1",
    "    Domain: dnsse.ca., QType: NS(2), section: authority, @srv: 199.4.144.2",
    "NS for dnsse.ca.: jean.ns.cloudflare.com., art.ns.cloudflare.com.",
    "    Resolving jean.ns.cloudflare.com. : 173.245.58.121 ",
    "    Resolving art.ns.cloudflare.com. : 173.245.59.102 ",
    "Querying NS recursively @ child ns ips.",
    "    Domain: dnsse.ca., QType: NS(2), section: answer, @srv: 173.245.58.121",
    "    Domain: dnsse.ca., QType: NS(2), section: answer, @srv: 173.245.59.102",
    "Child NS for dnsse.ca.: icecold.dnsse.ca., verycool.dnsse.ca., notcool.dnsse.ca., cool.dnsse.ca."
]
```

REMOVE SECURE DELEGATION CIRA-DSAP-3.CA & DELETE



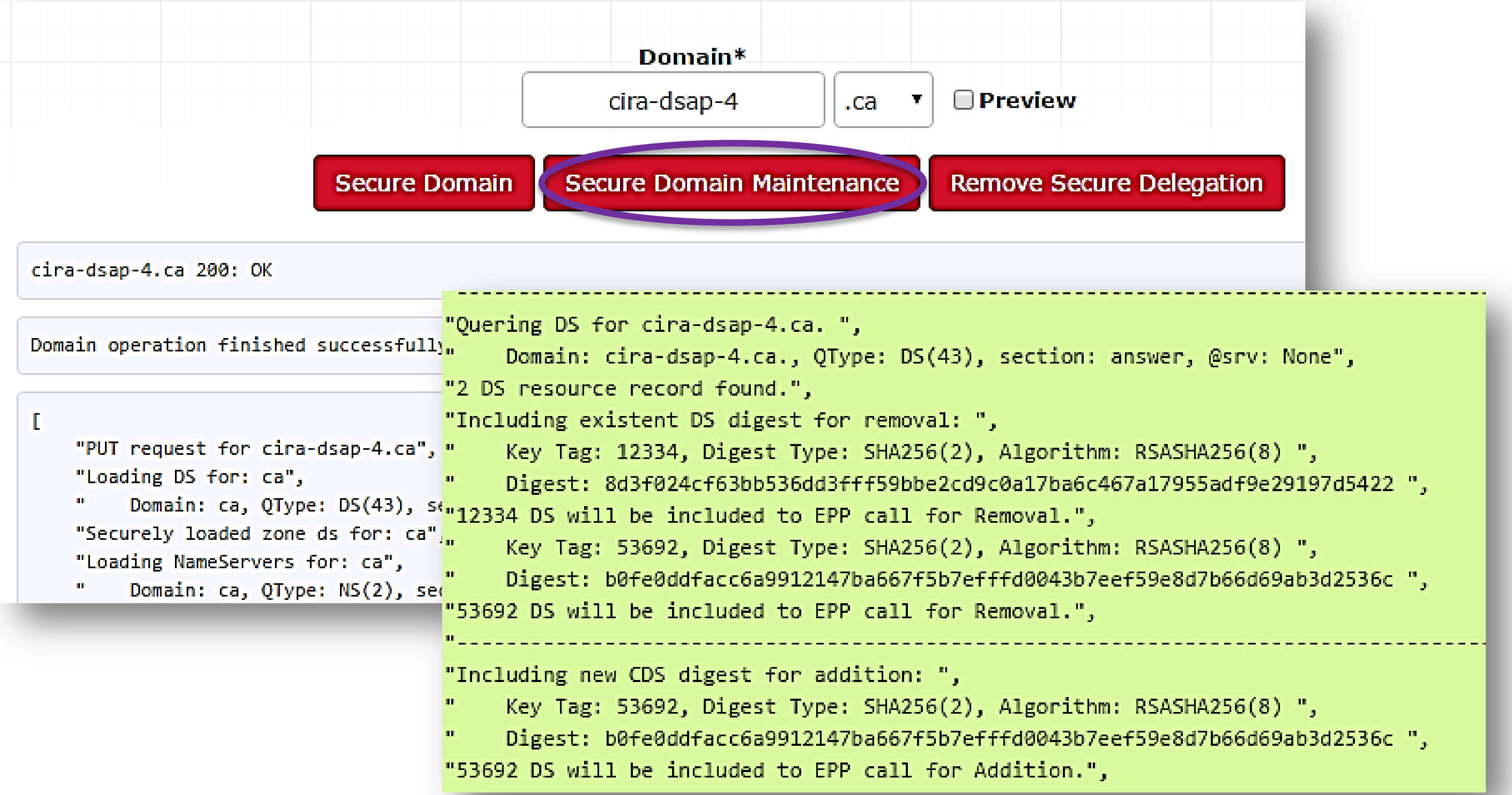
```
cira-dsap-3.ca 200: OK
```

```
Domain operation finished successfully.
```

```
[
    "DELETE request for cir
    "Loading DS for: ca",
    "    Domain: ca, QType:
```

```
  ----------------------------------------------------------------------------------------------
"Quering DS for cira-dsap-3.ca. ",
"    Domain: cira-dsap-3.ca., QType: DS(43), section: answer, @srv: None",
"2 DS resource record found.",
"Chain of trust successfully validated for cira-dsap-3.ca.",
"-----------------------------------------------------------------------------------------------
"    Key Tag: 11869, Digest Type: SHA1(1), Algorithm: RSASHA256(8) ",
"    Digest: 950bd7dd077b8de1d2bd180a3ffc8ca29aa4c0f0 ",
"11869 DS will be included into EPP call for removal.",
"    Key Tag: 11869, Digest Type: SHA256(2), Algorithm: RSASHA256(8) ",
"    Digest: 6610f35be88666d2dd82f45fec1d4c8e18f479476e6359f980204ac6f48140c5 ",
"11869 DS will be included into EPP call for removal.",
```

SECURE DOMAIN MAINTENANCE CIRA-DSAP-4.CA & PUT



```
cira-dsap-4.ca 200: OK
```

```
Domain operation finished successfully
```

```
[
    "PUT request for cira-dsap-4.ca",
    "Loading DS for: ca",
    "    Domain: ca, QType: DS(43), se
    "Securely loaded zone ds for: ca",
    "Loading NameServers for: ca",
    "    Domain: ca, QType: NS(2), se
```

```
-----------------------------------------------------------------------------------
"Quering DS for cira-dsap-4.ca. ",
"    Domain: cira-dsap-4.ca., QType: DS(43), section: answer, @srv: None",
"2 DS resource record found.",
"Including existent DS digest for removal: ",
"    Key Tag: 12334, Digest Type: SHA256(2), Algorithm: RSASHA256(8) ",
"    Digest: 8d3f024cf63bb536dd3fff59bbe2cd9c0a17ba6c467a17955adf9e29197d5422 ",
"12334 DS will be included to EPP call for Removal.",
"    Key Tag: 53692, Digest Type: SHA256(2), Algorithm: RSASHA256(8) ",
"    Digest: b0fe0ddfacc6a9912147ba667f5b7efffd0043b7eef59e8d7b66d69ab3d2536c ",
"53692 DS will be included to EPP call for Removal.",
"----------------------------------------------------------------------------------
"Including new CDS digest for addition: ",
"    Key Tag: 53692, Digest Type: SHA256(2), Algorithm: RSASHA256(8) ",
"    Digest: b0fe0ddfacc6a9912147ba667f5b7efffd0043b7eef59e8d7b66d69ab3d2536c ",
"53692 DS will be included to EPP call for Addition.",
```

SUMMARY

- CIRA is looking at DSAP implementation
- Try DSAP
- Feedback welcome

Thank you