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).

- 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)
WHAT IS A CDS?
A SIGNAL TO THE PARENT

- 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

<table>
<thead>
<tr>
<th>CHILD DNSEY</th>
<th>PARENT DS</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Key" /></td>
<td><img src="image2.png" alt="Key" /></td>
</tr>
<tr>
<td><img src="image3.png" alt="Key" /></td>
<td><img src="image4.png" alt="Key" /></td>
</tr>
<tr>
<td><img src="image5.png" alt="Key" /></td>
<td><img src="image6.png" alt="Key" /></td>
</tr>
<tr>
<td><img src="image7.png" alt="Key" /></td>
<td><img src="image8.png" alt="Key" /></td>
</tr>
</tbody>
</table>

1) start
2) Add
3) Remove
4) end
MAINTENANCE - DNSSEC KEY ROLL OVER USING CDS

- Automated process

<table>
<thead>
<tr>
<th>CHILD DNSEY</th>
<th>CHILD CDS</th>
<th>PARENT DS</th>
</tr>
</thead>
<tbody>
<tr>
<td>💋</td>
<td>🔑</td>
<td>🍼</td>
</tr>
</tbody>
</table>

1) start
MAINTENANCE - DNSSEC KEY ROLL OVER USING CDS

- Automated process – Signal to:

CHILD DNSEY  CHILD CDS  PARENT DS

1) Remove previous child keys

2) Add CDS
MAINTENANCE - DNSSEC KEY ROLL OVER USING CDS

- Automated process – Signal to:

1) start

Wait some time
• Automated process – Signal to:

1) start

3) Remove CDS
MAINTENANCE - DNSSEC KEY ROLL OVER USING CDS

- Automated process

<table>
<thead>
<tr>
<th>CHILD DNSEY</th>
<th>CHILD CDS</th>
<th>PARENT DS</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Key" /></td>
<td><img src="image2" alt="Key" /></td>
<td><img src="image3" alt="Key" /></td>
</tr>
<tr>
<td><img src="image4" alt="Key" /></td>
<td><img src="image5" alt="Key" /></td>
<td><img src="image6" alt="Key" /></td>
</tr>
<tr>
<td><img src="image7" alt="Key" /></td>
<td><img src="image8" alt="Key" /></td>
<td><img src="image9" alt="Key" /></td>
</tr>
<tr>
<td><img src="image10" alt="Key" /></td>
<td><img src="image11" alt="Key" /></td>
<td><img src="image12" alt="Key" /></td>
</tr>
</tbody>
</table>

4) The end
DS AUTOMATED PROVISIONING (DSAP) COMPONENTS

- **DNS Operator**
- **API**
  - RESTful
  - /domains/{domain}/cds
  - POST/DELETE/PUT
- **DS Automated Provisioning (DSAP)**
  - DNS/DNSSEC
  - Parent/Child
  - Extensive validation
- **Registrar Registry**
  - EPP
  - RFC5910
  - <create> DS
  - <delete> DS
• 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 😊)
CREATE SECURE DElegation
CIRA-DSAP-1.CA & POST

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

Domain*

Secure Domain  Secure Domain Maintenance  Remove Secure Delegation

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 for: ca",
  "Loading NameServers for: ca",
  "Domain: ca, QType: NS",

  KSK - KeySigning Key found - flag: 257",
  "Key Tag: 27022, Protocol: 3, Algorithm: RSASHA256(8)",
  "Public Key: AwEAAAbObbNTMTSz3Z1Xgjpt9vVG+mrb fV1UIzok9ep9ShKq6z4+Cbztcv1+1MBO Ydae+4",

  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

Secure Domain  Secure Domain Maintenance  Remove Secure Delegation

dnsse.ca 400: Bad Request


```
"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

Domain*

- cira-dsap-3 .ca

- Secure Domain
- Secure Domain Maintenance
- Remove Secure Delegation

"Quering DS for cira-dsap-3.ca. ",
"Loading DS for: 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: 950bd7dd077b8de1d2bd180a3fffc8ca29aa4c0f0 ",
"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

"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