ICANN57 – TECHDAY
DS AUTOMATED
PROVISIONING
(DSAP)

Presented by:
Jacques Latour
November 5, 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).

  ```plaintext
  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 DNS Operator is sometimes far removed from the registry.

- The DNS Operator can be the Registrant, the Registrar or a third party (DNS provider, web hosting, content provider, etc...)
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)
CONCEPT - LEVERAGE CDS TO ENABLE DS PROVISIONING FOR REGISTRARS

Child Domain
CDS
example.ca

Grab CDS

Parent Domain
{ example.ca DS } .ca

Registry

Registrar

RFC5910
EPP
<create> DS
<delete> DS

DS Automated Provisioning (DSAP)

Connects to registry with EPP

Generate EPP code

Extensive validation
Convert to DS
CONCEPT - LEVERAGE CDS TO ENABLE DS PROVISIONING FOR REGISTRIES

Child Domain
CDS
example.ca

Parent Domain
{ example.ca DS } .ca

Validate
Convert to DS

Grab CDS

DS Automated Provisioning (DSAP)

Registry

Generate EPP code & create DS

Create a registry actor that supports only DNSSEC functions + security controls (namely Registry Lock)
CONCEPT - INTERFACES TO SUPPORT SMALL AND LARGE DNS OPERATOR

- Joe User DNS Operator
- Large DNS Operator
- Registrar
- Registry

DS Automated Provisioning (DSAP)

Web

API

RESTful

DNS/DNSSEC Validation

EPP

DNS DNSSEC Parent/Child
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*

Secure Domain Secure Domain Maintenance Remove Secure Delegation

Powered by
CIRA Labs
CREATE SECURE DELEGATION
CIRA-DSAP-1.CA & POST

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

Domain*

- cira-dsap-1
- .ca

[Preview]

Secure Domain
Secure Domain Maintenance
Remove Secure Delegation

Domain operation finished successfully.

```
["POST request for cira-dsap-1.ca",
"Loading DS for: ca",
"  Domain: ca, QType: DS(43), section: answer, @srv",
"  Securely loaded zone ds for: ca",
"  Loading Nameservers for: ca",
"  Domain: ca, QType: NS(2), section: answer, @srv",
{   "add": [
      {   
        "digest_type": 1,
        "algorithm": 8,
        "key_tag": 27022,
        "digest": "b209b357f5857c6913585b2309197c99d4d27fb2"
      }
    ]
}
```
REMOVE SECURE DELEGATION
CIRA-DSAP-3.CA & DELETE

```
{
  "rem": [
    {
      "digest_type": 2,
      "algorithm": 8,
      "key_tag": 11869,
      "digest": "6610f35be88666d2dd82f45fe4d4c8e18f479476e6359f980204ac6f48140c5"
    },
    {
      "digest_type": 1,
      "algorithm": 8,
      "key_tag": 11869,
      "digest": "550bd7dd077b8de1d2bd180a3ffca29aa4c0f0"
    }
  ]
}
```
SECURE DOMAIN MAINTENANCE
CIRA-DSAP-4.CA & PUT

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

{
  "add": [],
  "rem": [
    {
      "digest_type": 2,
      "algorithm": 8,
      "key_tag": 12334,
      "digest": "8d3f024cf63b536dd3fff59bfe2cd9c0a17ba6c467a17955adf9e29197d5422"
    }
  ]
}
```
SUMMARY

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

Thank you