DS Updates and Multi-Signer Coordination – A Continuing Series ICANN 71, “The Hague” – Episode 5

Steve Crocker & Shumon Huque

steve@shinkuro.com

shuque@gmail.com

Two gaps in the DNSSEC protocol specs

- Automation of DS updates
  - Periodic key changes
  - New key in the child's zone requires new parent DS record
  - Registrar has access to parent
    - If Registrar is providing signed DNS service, conveying new DS to parent is easy
  - **But 3rd party DNS provider does not have access to the Registry**

- Multiple DNS Providers
  - Each DNS provider signs with its own keys (RFC 8901 Model 2)
  - Each must include ZSKs from the other providers
  - No defined way to share the keys
  - Needed for:
    - **Capacity and high reliability**
    - **Glitch-free transfer of a signed zone from one DNS Provider to another (Disruptions can be worse than expected)**

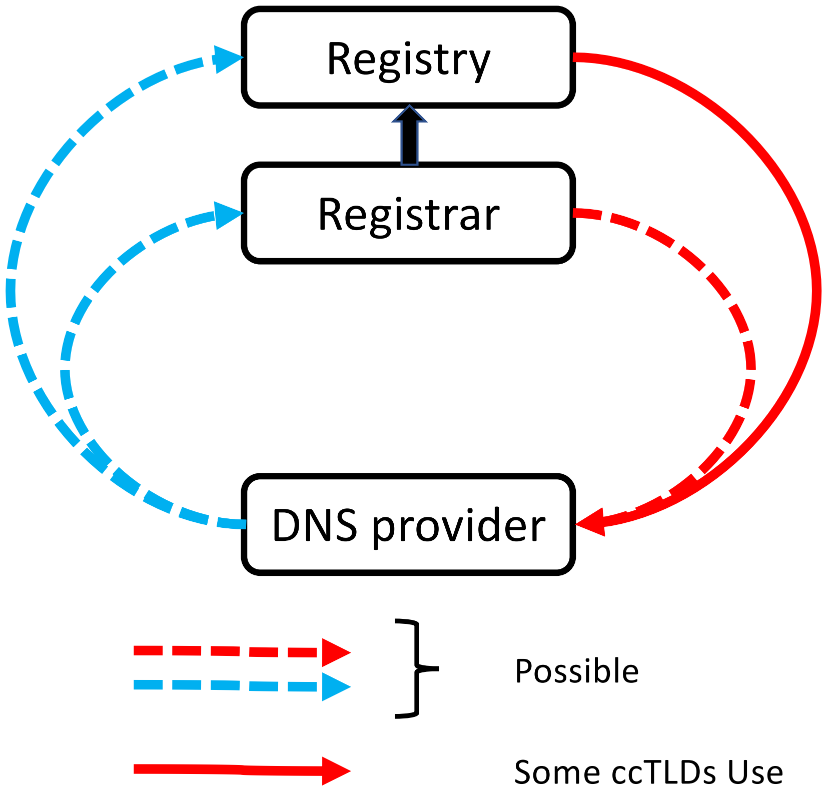
Agenda

#	Title	Speaker
3.1	DNSSEC Provisioning Automation Overview	Steve Crocker, Shinkuro, Inc
3.2	CDS scanning at RIPE NCC	Ondřej Caletka, RIPE NCC
3.3	The State of DNSSEC Automated Provisioning	Wilco van Beijnum, University of Twente
3.4	Multi-Signer Project Overview and Status	Ulrich Wisser, Swedish Internet Foundation
3.5	BIND DNSSEC Provisioning Interfaces	Matthijs Mekking, Internet Systems Consortium
3.6	PowerDNS DNSSEC Provisioning Interfaces	Peter van Dijk, PowerDNS

DS Updates

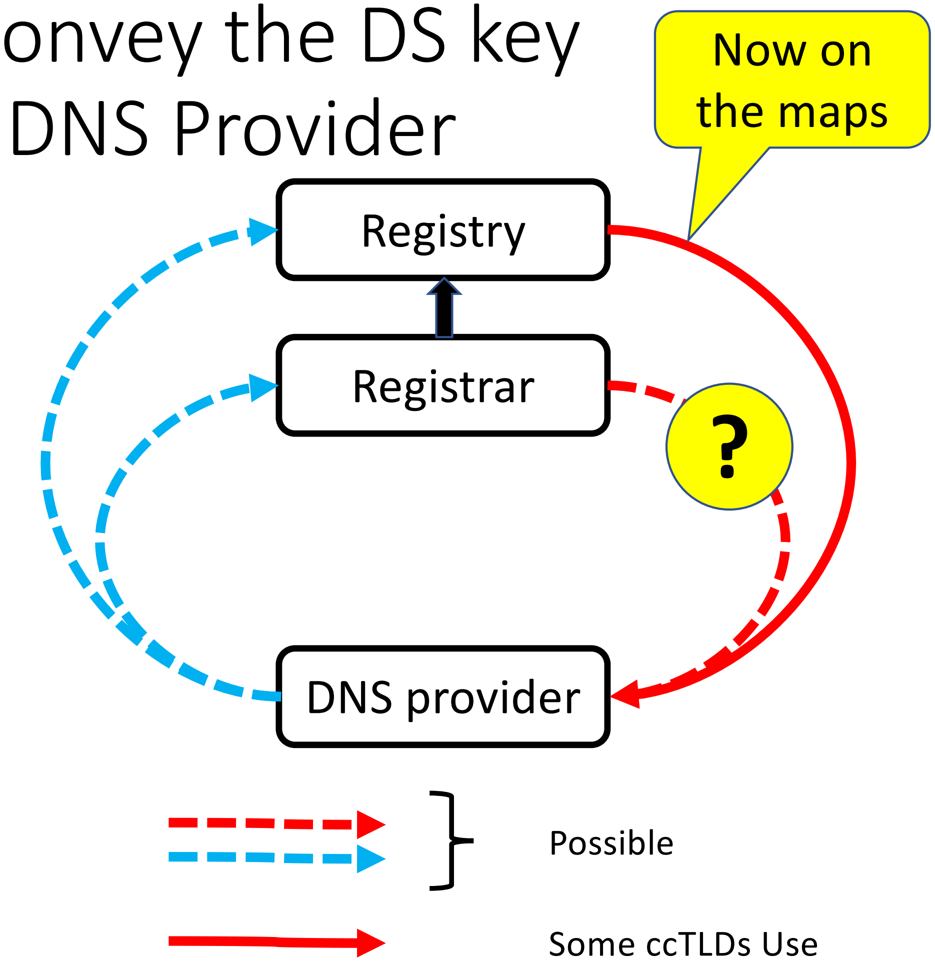
Possible Ways to Convey the DS key from 3rd party DNS Provider

	Direction	
Upper Side	Push (Calling) DNS Provider calls API at Ry, Rr	Pull (Polling) DNS Provider publishes CDS and/or CDNSKEY
Registry	1. Requires API	3. RFC 8078
Registrar	2. Requires API	4. RFC 8078



Possible Ways to Convey the DS key from 3rd party DNS Provider

	Direction	
Upper Side	Push (Calling) DNS Provider calls API at Ry, Rr	Pull (Polling) DNS Provider publishes CDS and/or CDNSKEY
Registry	1. Requires API	3. RFC 8078
Registrar	2. Requires API	4. RFC 8078

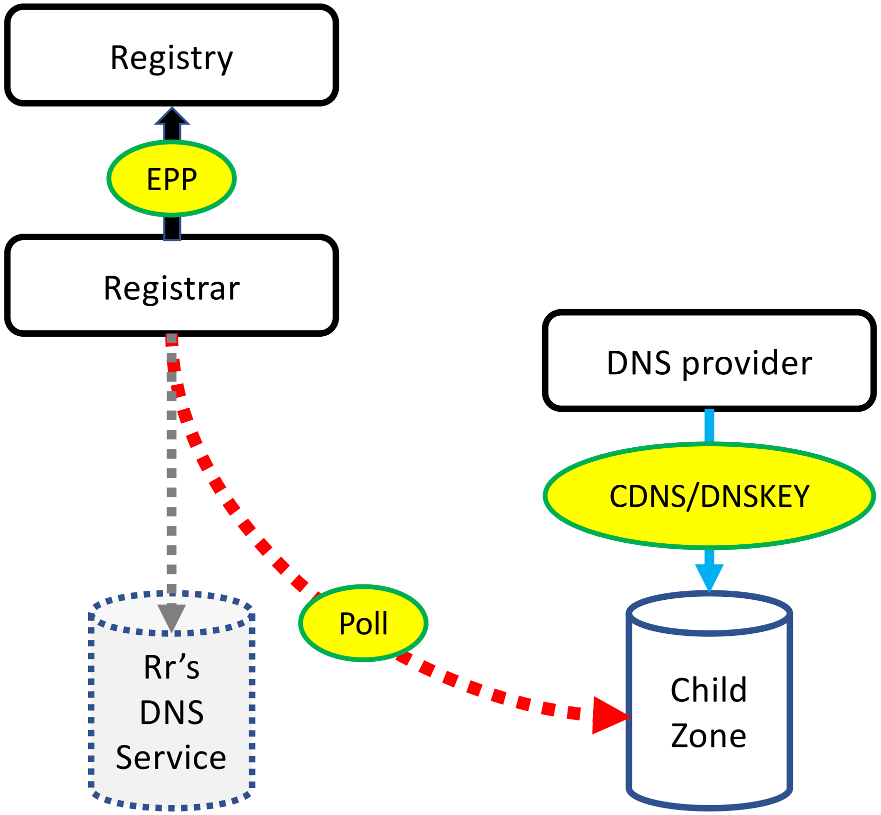

Now on the maps

Possible Ways to Convey the DS key from 3rd party DNS Provider

	Direction	
Upper Side	Push (Calling) Call Rr or Rt API	Pull (Polling) Publish CDS/ CDNSKEY
Registry		
Registrar		4. RFC 8078

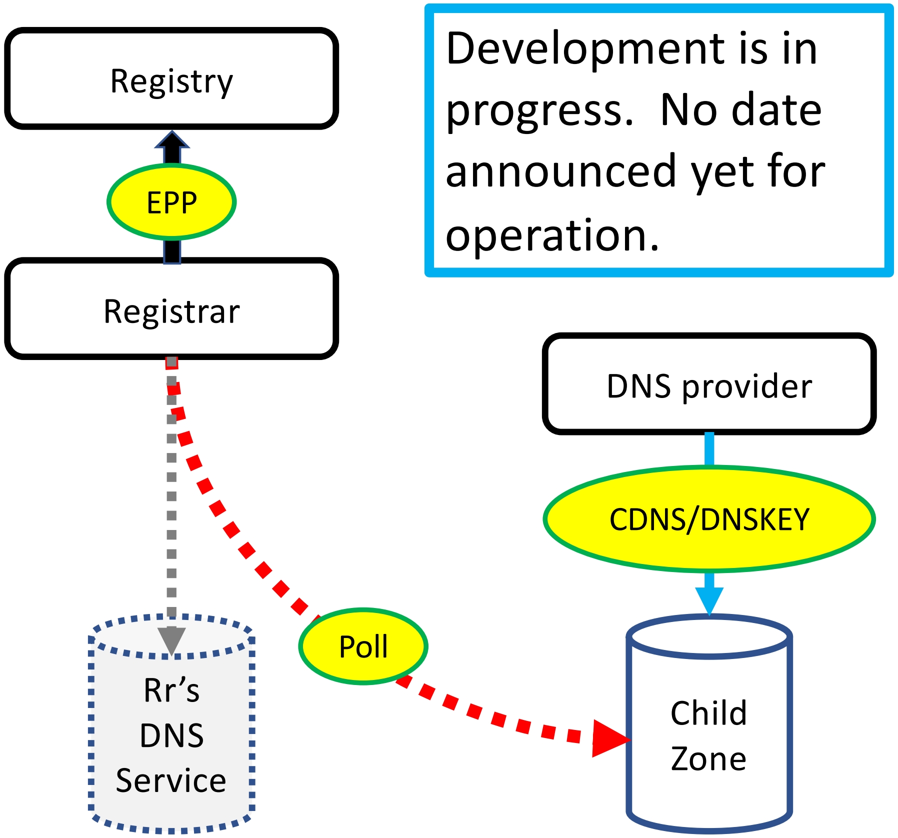
Registrar polls for CDS/CDNSKEY records.

Possible use forthcoming.



GoDaddy plans to pull the DS key from 3rd party DNS Providers

	Direction	
Upper Side	Push (Calling) Call Rr or Rt API	Pull (Polling) Publish CDS/ CDNSKEY
Registry		
Registrar		4. RFC 8078



Development is in progress. No date announced yet for operation.

GoDaddy polls for CDS/CDNSKEY records.

Possible use forthcoming.

DNSSEC:
Multi-DNS Provider Coordination & Glitch-Free Provider Change

“Glitch-Free” = No loss of resolution AND no loss of validation

Why not go insecure briefly?

- Seems easier
- Who would notice?

Why not go insecure briefly?

- Seems easier
- Who would notice?
- Secured applications depend on DNSSEC
- DNSSEC outages => Application outages
- No validation => Secured applications break
  - Web sites
  - Email
  - Other DANE-based applications

Multi-Signer Big Picture

✓ Done
□ In progress
○ Future
• Unspecified/Mixed

✓ Protocol (RFC 8901)

- Software
  - Multi-Signer Controller
    - □ Design
    - □ Implementation
  - DNS Server Interfaces
    - □ BIND, PowerDNS, …
  - Services/Operations
    - □ deSEC, NS1, Neustar …

- Analysis
  - ✓ Text
  - ○ Proof
- Observation
  - Longitudinal (Eric Osterweil)
  - Real-time
    - ○ System Design
    - ○ Deployment
    - ○ Experiments
      - ○ Positive
      - ○ Negative

Multi-Signer Software

The Swedish Internet Foundation

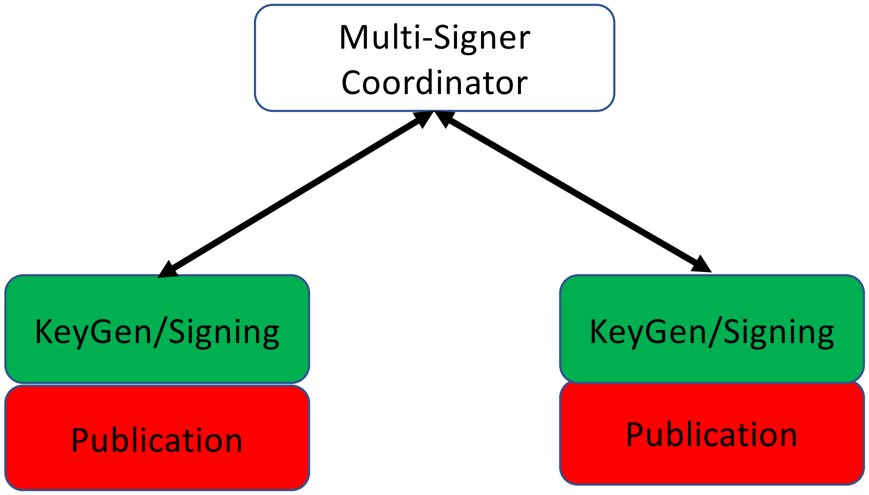
deSEC

Salesforce

George Mason University

Shinkuro, Inc.

Cross-Signing: Communicating ZSKs & KSKs



Registrant coordinates using a Multi-signer Coordinator

Multi-Signer Operational* Demonstrations

* Operational = Repeatable

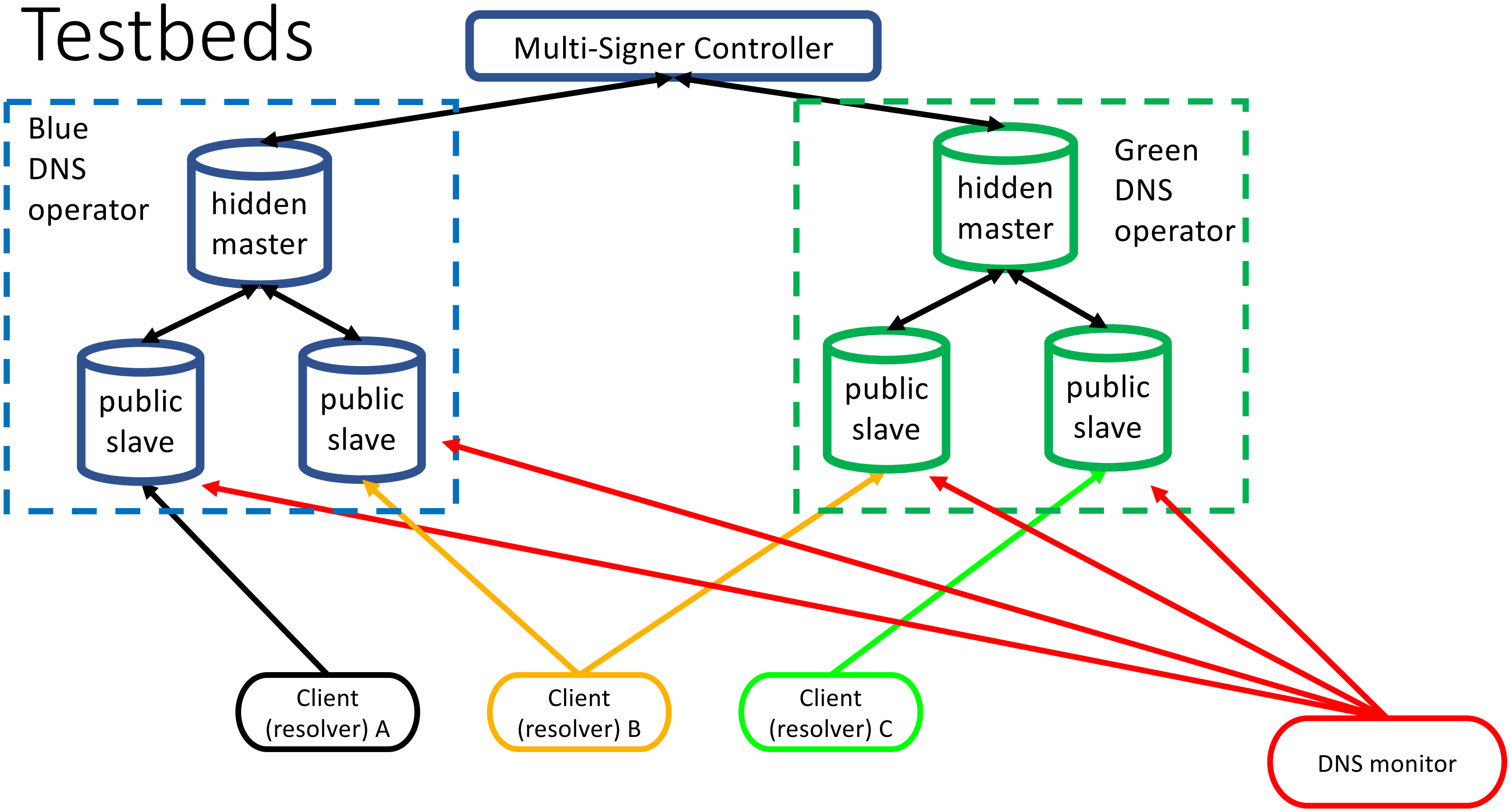
- Adding a DNS operator
- Key rollover in one of the operations
- (Concurrent key rollover – will it work?)
- Removal of an operator

▪ Observation of glitch-free operation for each of the above

- Repeat of each, violating the timing constraints

▪ Observation of glitches when timing constraints are violated

Testbeds


Multi-Signer Controller
Blue DNS operator
hidden master
public slave
public slave
Green DNS operator
hidden master
public slave
public slave
Client (resolver) A
Client (resolver) B
Client (resolver) C
DNS monitor

Multi-Signer Controller Components

- Interfaces to authoritative DNS servers
- Scenario sequencer
- User interface
  - Identities of authoritative servers
  - Credentials for access to the servers
  - Control to start, stop, undo transitions
- Module to check success of transitions
- Reporting
- Statistics

References

DNSSEC Provisioning Automation “Episodes”

Episode	Date	Meeting	DNSSEC Provisioning Automation Sessions
1	11 Mar 2020	ICANN 67 “Cancún”	https://tinyurl.com/5dwxfz2v
2	22 Jun 2020	ICANN 68 “Kuala Lumpur”	xhttps://tinyurl.com/m8eraezu
3	21 Oct 2020	ICANN 69 “Hamburg”	https://tinyurl.com/f8ma6347
4	24 Mar 2021	ICANN 70 “Cancún”	https://tinyurl.com/bj69sn87
5	14 Jun 2021	ICANN 71 “The Hague”	

Internet Society DNSSEC Maps

https://www.internetsociety.org/deploy360/dnssec/maps/

Thanks!