DS Updates and Multi-Signer Coordination – A Continuing Series ICANN 70, “Cancún” – Episode 4

Steve Crocker & Shumon Huque

steve@shinkuro.com

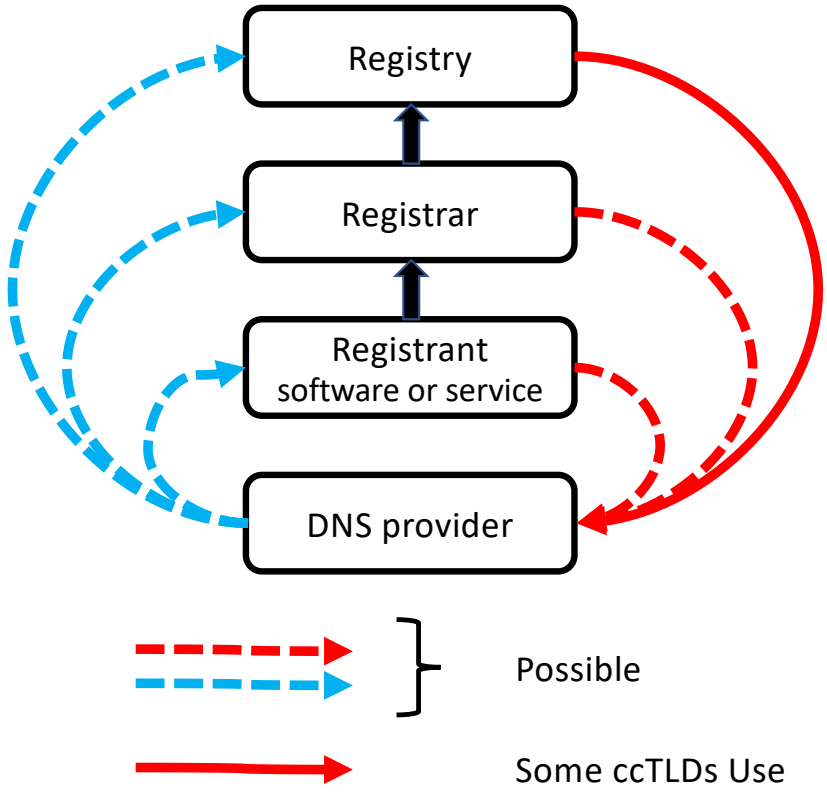
shuque@gmail.com

Two gaps in the DNSSEC protocol specs

- Automation of DS updates
  - DNSSEC calls for periodic changes of keys
  - New key in the child's zone requires new DS record in parent zone
  - Registrar has EPP access to the parent zone
    - 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**
- Cross-signing among 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:
    - **Glitch-free transfer of a signed zone from one DNS Provider to another**
    - **Capacity and high reliability**

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

	Direction	
Upper Side	Push (Calling) DNS Provider calls API at Ry, Rr or Rt	Pull (Polling) DNS Provider publishes CDS and/or CDNSKEY
Registry	1. Requires API	4. RFC 8078
Registrar	2. Requires API	5
Registrant	3. Requires APIs	6

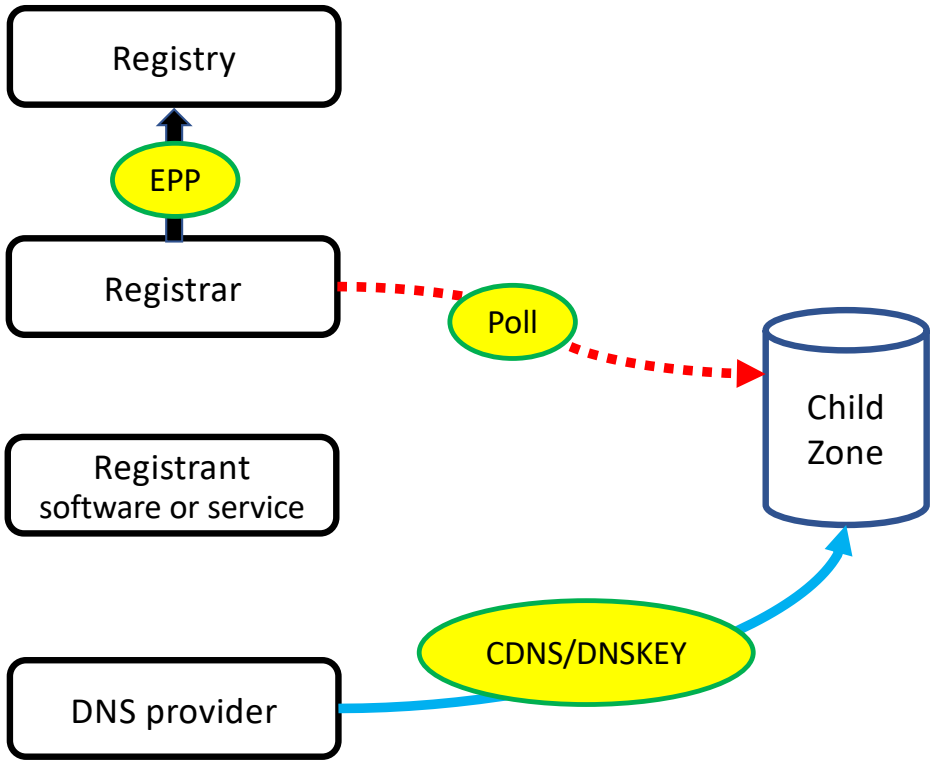


Possible Ways to Convey the DS key from 3rd party DNS Provider

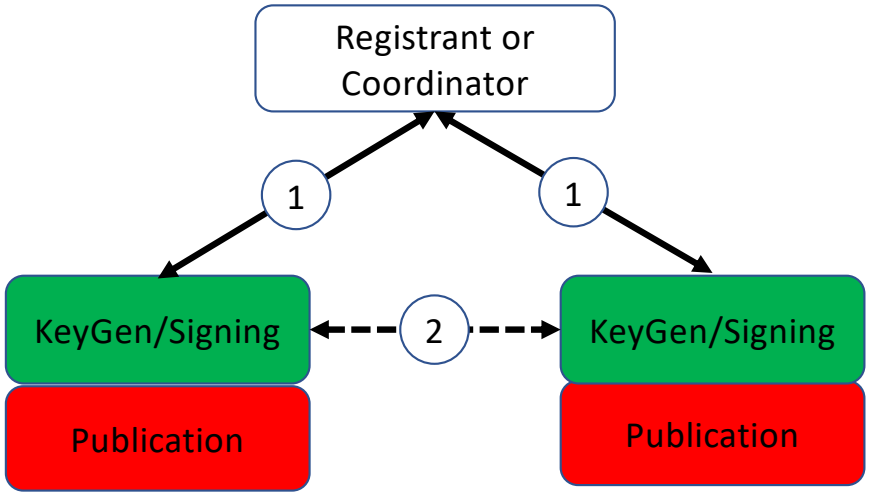
	Direction	
Upper Side	Push (Calling) Call Rr or Rt API	Pull (Polling) Publish CDS/ CDNSKEY
Registry		
Registrar		5
Registrant		

Registrar polls for CDS/CDNSKEY records.

Possible use forthcoming.



Cross-Signing: Communicating ZSKs & KSKs

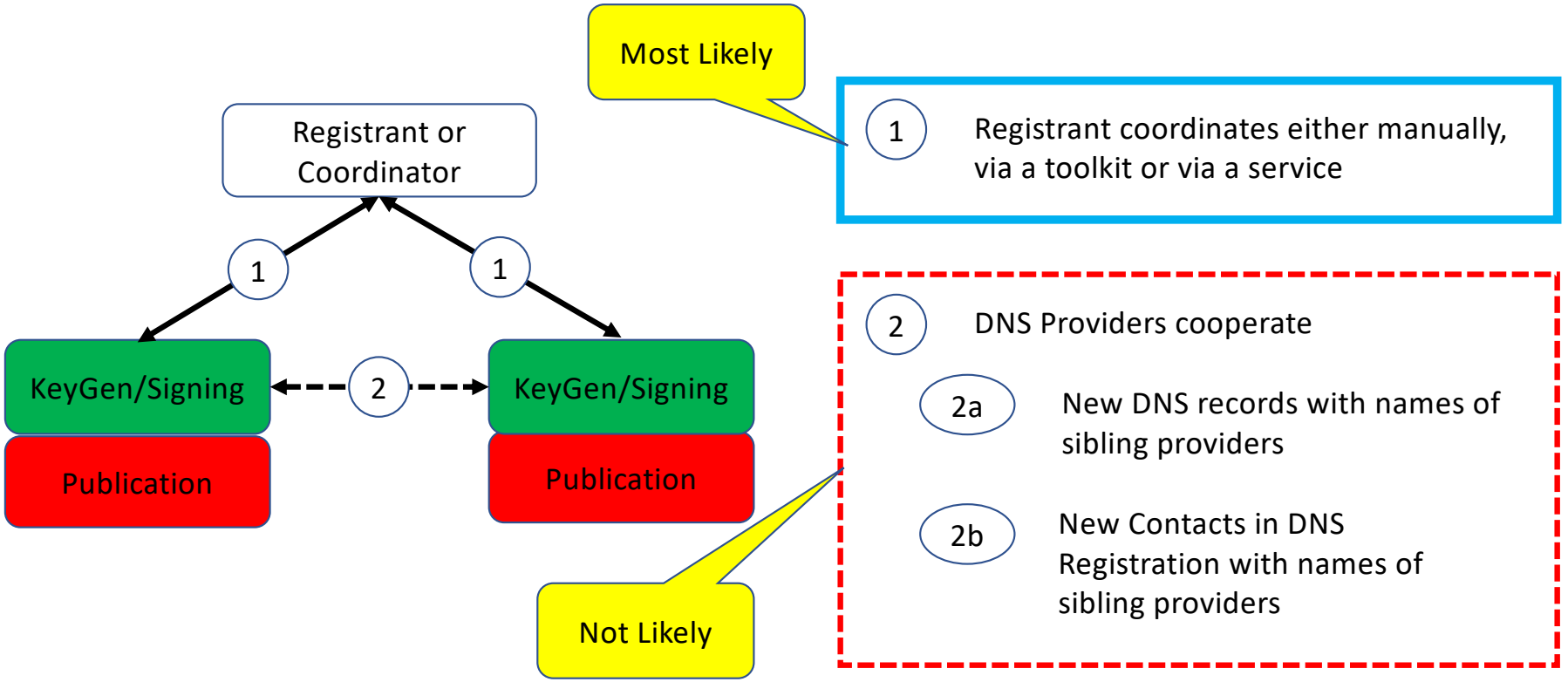


1 Registrant coordinates either manually, via a toolkit or via a service

2 DNS Providers cooperate

- 2a New DNS records with names of sibling providers
- 2b New Contacts in DNS Registration with names of sibling providers

Cross-Signing: Communicating ZSKs & KSKs



Today's Agenda

- DS Automation at GoDaddy – Brian Dickson
- The Multisigner Project Foundations
  - Shuman Huque, Salesforce – Introduction
  - Ulrich Wisser, Swedish Internet Foundation – Multi-Signer Protocols
- Multisigner Implementations
  - Multi-signer Testbed
  - Peter Thomassen, Secure Systems Engineering – Multisigner support at deSEC
- Multisigner Measurement and Observations
  - DNSKEY Transition Observatory – Pryia Ravichander, Eric Osterweil, GMU
  - Anatomy of DNSSEC Transitions – Eric Osterweil, Pouyan Fotouhi, Matthias Waehlich, Thomas C. Schmidt
- Emergent Tangents
  - Orderly process for advising on transition of algorithms
  - Update of RFCs to accommodate multiple algorithms