DS Updates and Multi-Signer Coordination – A Continuing Series

Steve Crocker & Shumon Huque

steve@shinkuro.com

shuque@gmail.com

Two gaps in the DNSSEC protocol specs

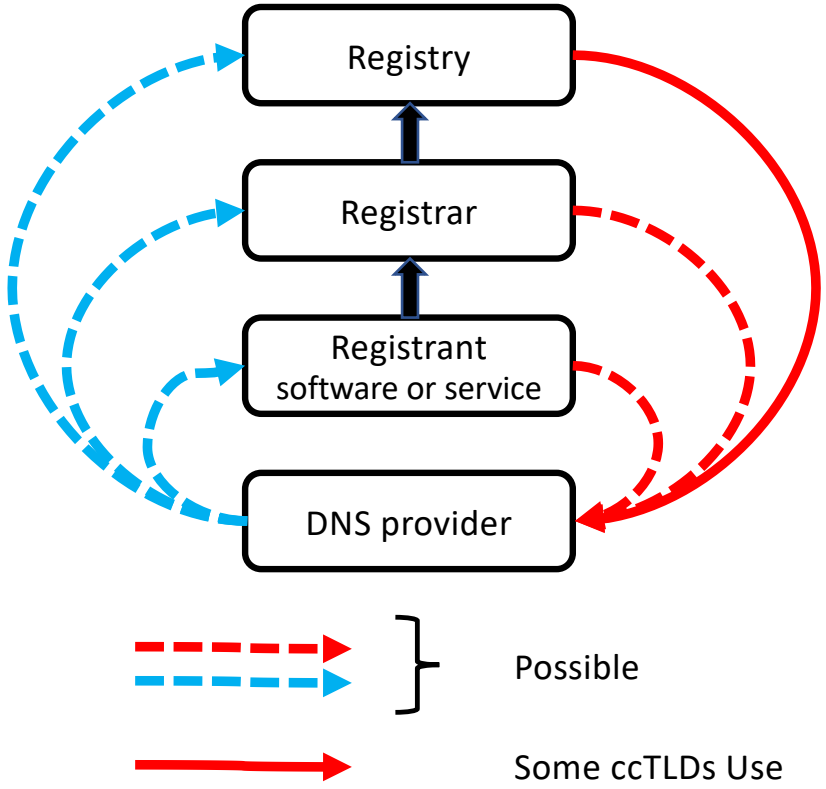
- Automation of DS updates
  - DNSSEC calls for periodic changes of keys
  - New key in the child's zone requires new DS record in parent zone
  - Registrar has EPP access to the parent zone
    - If Registrar is providing signed DNS service, conveying new DS to parent is easy
    - **But 3rd party DNS 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**

Today's Agenda

1. Overview: Framing the Issues – Shumon Huque and Steve Crocker
2. Status of DNSSEC Deployment
   - Ulrich Wisser:.SE DNSSEC History Present Future
   - Han Zhang: Deploying DNSSEC in a Large Enterprise
3. DS Automation
   - Shumon Huque: DS Automation
   - James Galvin Ph.D.: DS Automation: Non-technical Considerations
   - Brian Dickson: GoDaddy DNSSEC DS – Current and Proposed DS Update Methods
   - Mark Elkins: Gathering the Childrens DS'
   - Dan York: Evolving the DNSSEC Deployment Maps
4. Coordination of Multiple Signers and Transfers
   - Eric Osterweil: DNSSEC Census: Are DNSKEY Transitions Working?
   - Shumon Huque: Automating Multiple Signers
5. Recommended Actions: Steve Crocker

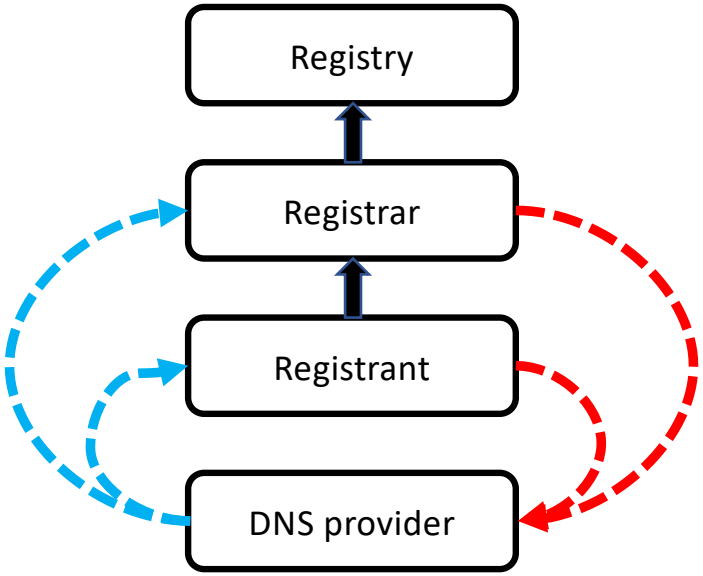
Possible Ways to Convey the DS key from 3rd party DNS Provider

	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



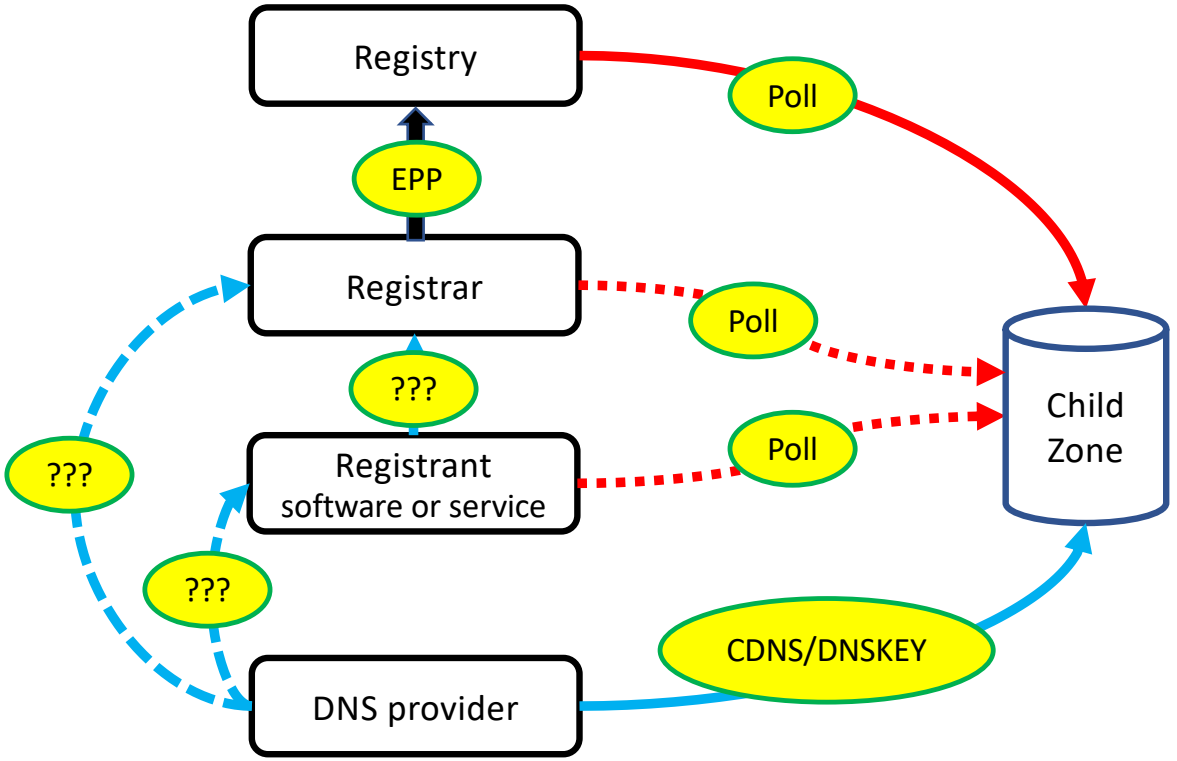
gTLD Registry Posture: Not my Problem

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

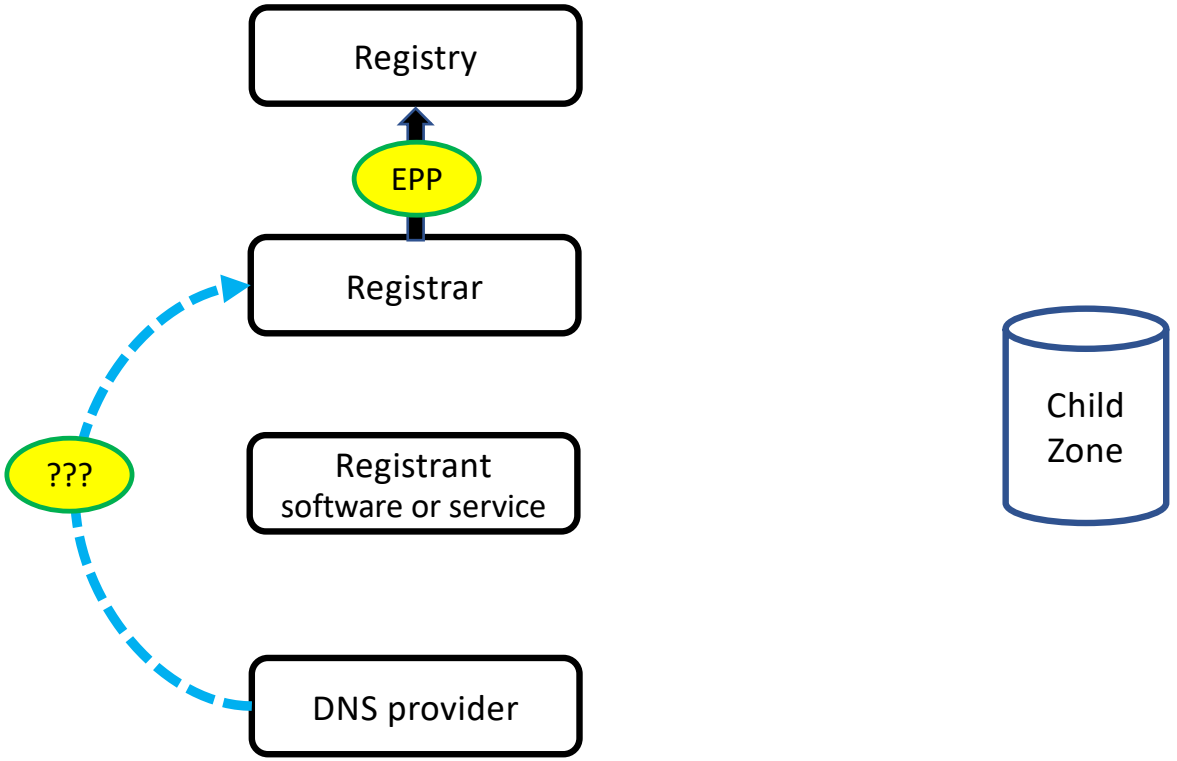


Possible Ways to Convey the DS key from 3rd party DNS Provider

	Direction	
Upper Side	Push (Calling) Call Rr or Rt API	Pull (Polling) Publish CDS/ CDNSKEY
Registry		
Registrar	2. Requires API	
Registrant		

DNS Provider pushes DS record to Registrar.

In use for DNS providers integrated with Registrar

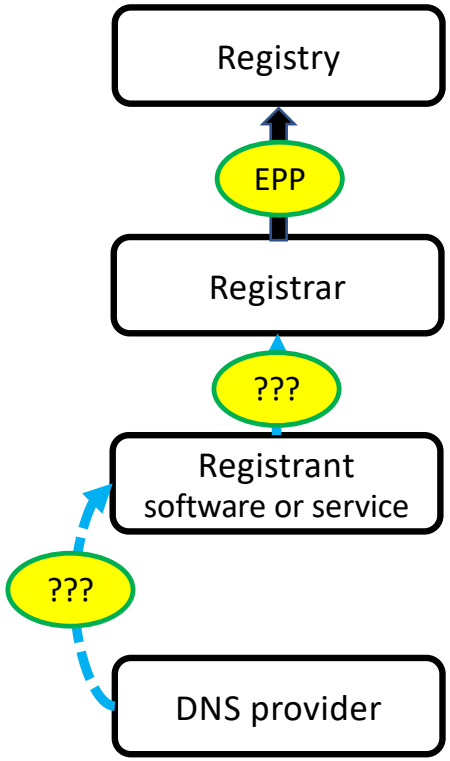


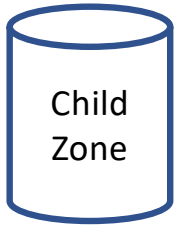
Possible Ways to Convey the DS key from 3rd party DNS Provider

	Direction	
Upper Side	Push (Calling) Call Rr or Rt API	Pull (Polling) Publish CDS/ CDNSKEY
Registry		
Registrar		
Registrant	3. Requires APIs	

DNS Provider pushes DS record to Registrant Software.

No known uses as yet.



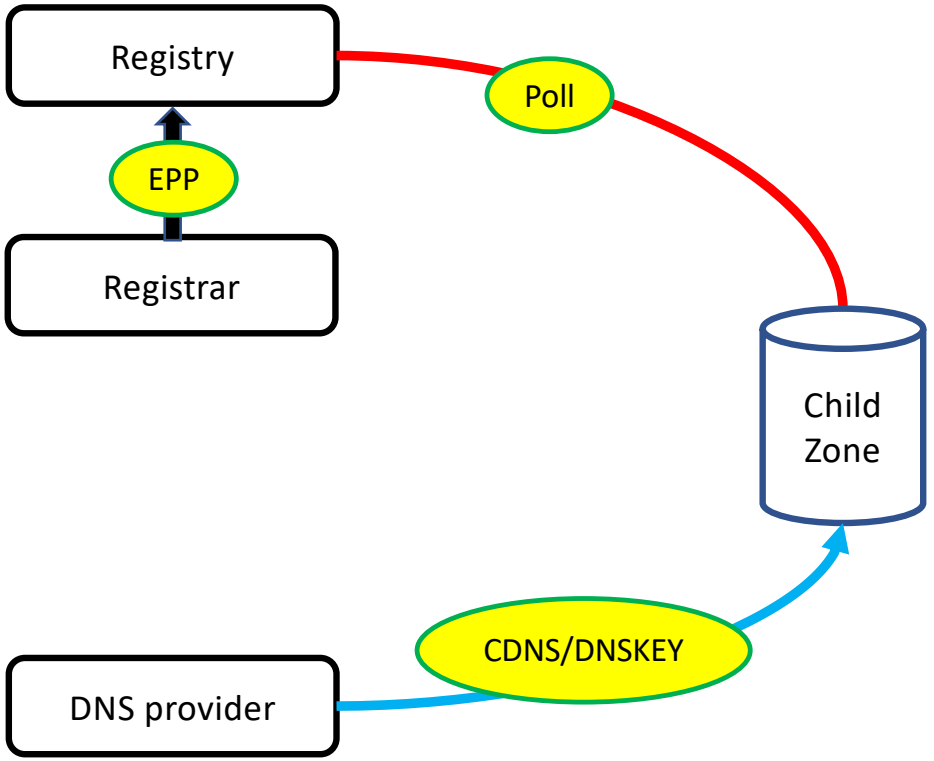


Possible Ways to Convey the DS key from 3rd party DNS Provider

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

Registry polls for CDS/CDNSKEY records.

In use among several ccTLDS.

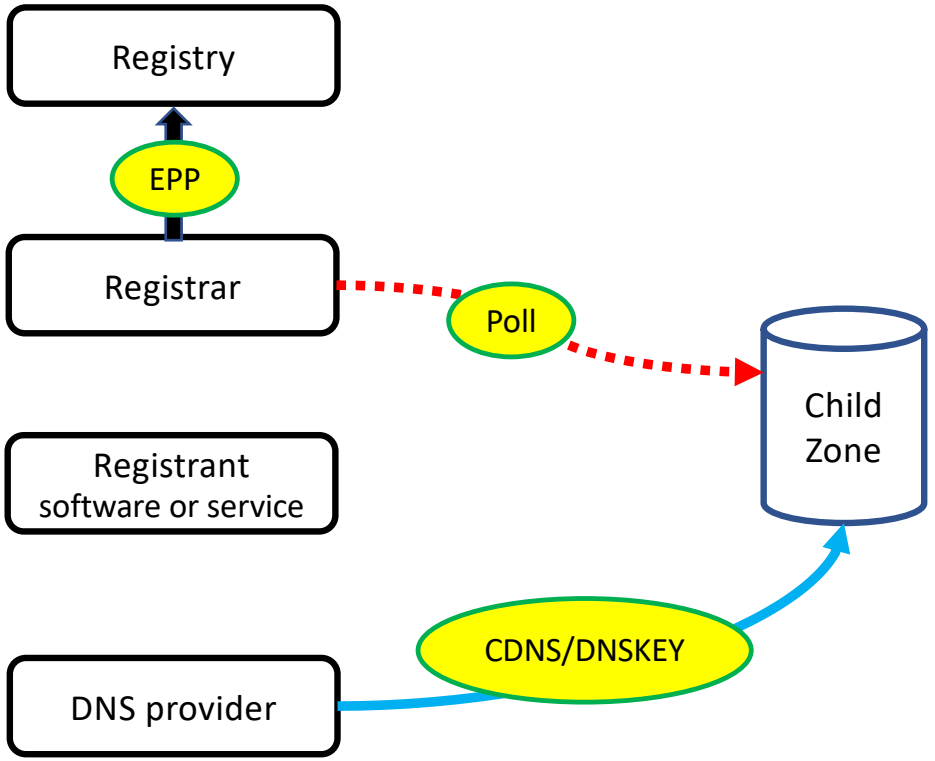


Possible Ways to Convey the DS key from 3rd party DNS Provider

	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.

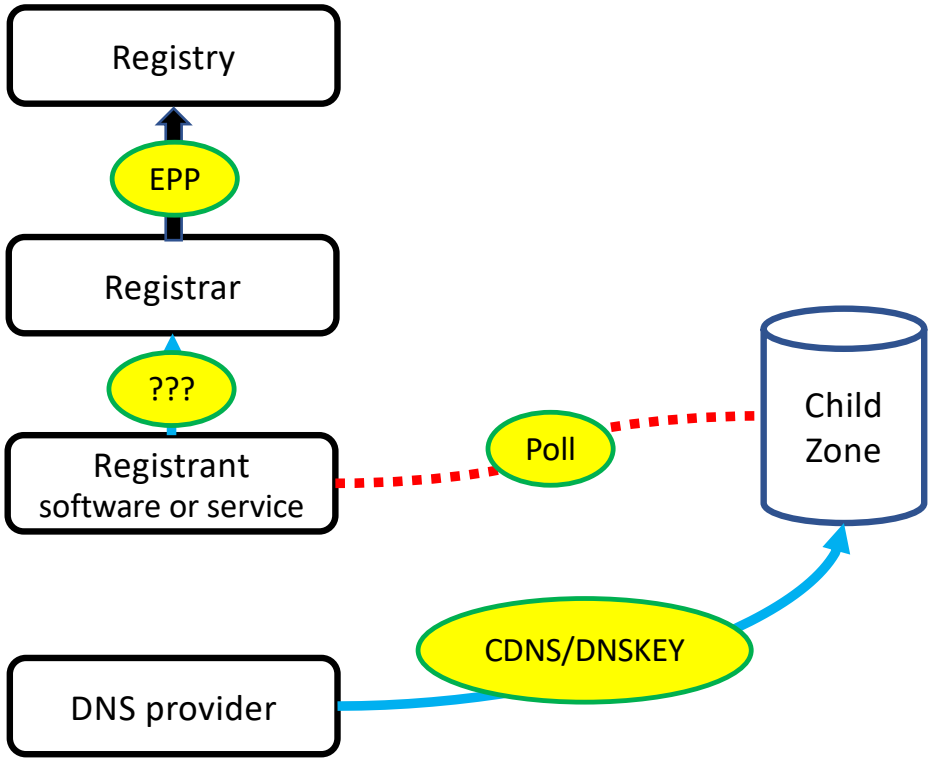


Possible Ways to Convey the DS key from 3rd party DNS Provider

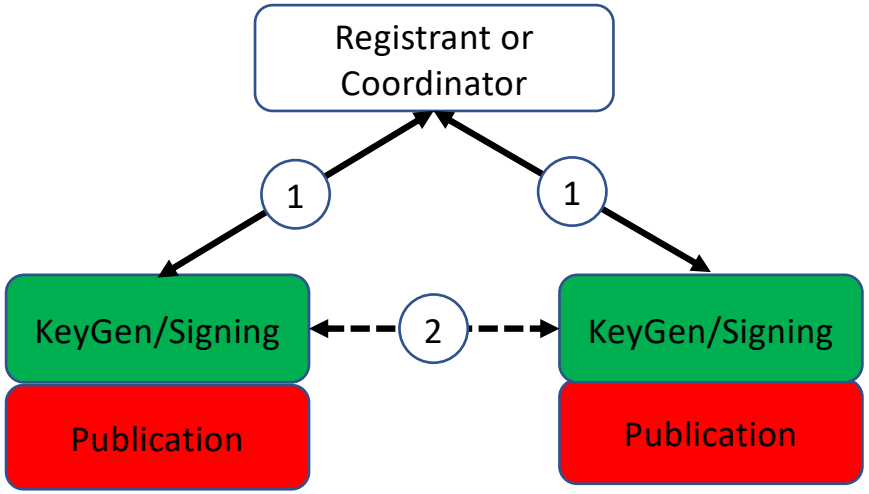
	Direction	
Upper Side	Push (Calling) Call Rr or Rt API	Pull (Polling) Publish CDS/ CDNSKEY
Registry		
Registrar		
Registrant		6

Registrant software polls for CDS/CDNSKEY records. Requires Registrant API.

No known uses as yet.



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