DNSSEC Provisioning with 3rd party DNS Providers

ICANN “Cancún” Virtual DNSSEC Workshop, March 2020

Steve Crocker

Panelists

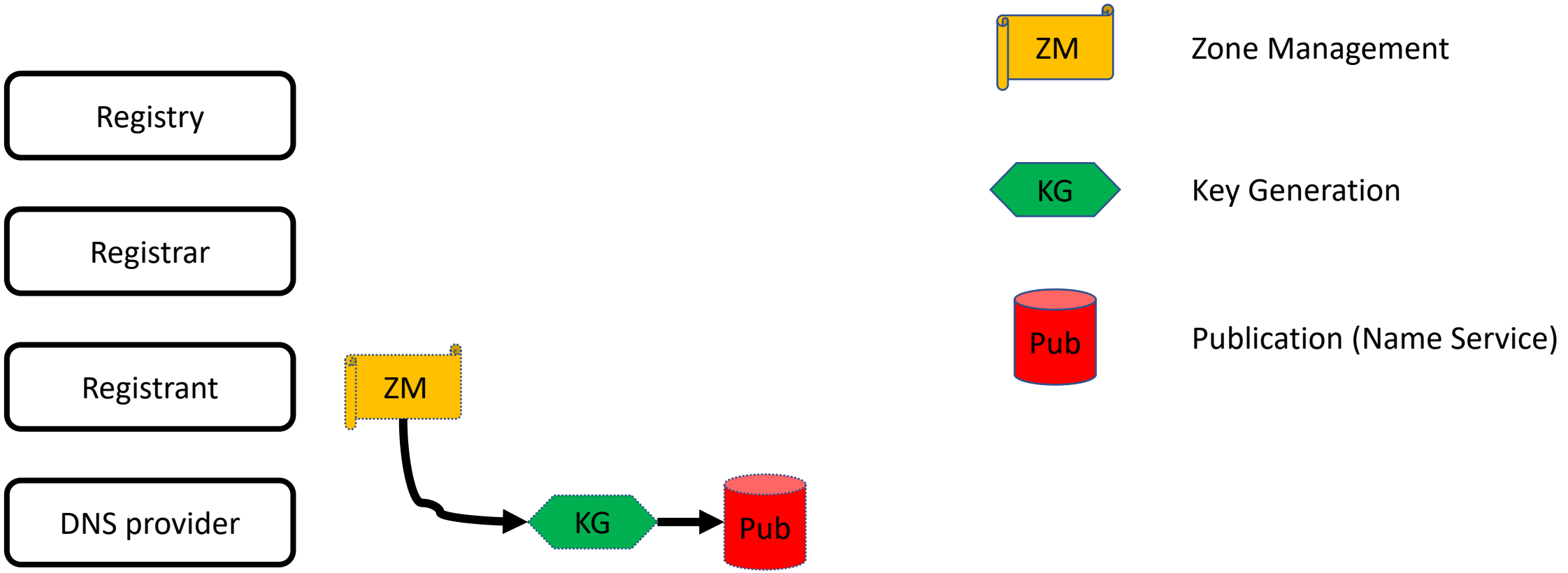
Panelists	Registry	Registrar	DNS Provider
Jim Galvin	Afilias		
Erwin Lansing	DK		
Gavin Brown, CentralNic	SK		
Brian Dickson		GoDaddy	
Jothan Frakes		PLISK	
Ólafur Guðmundsson		Cloudflare	

Today's Focus: The DS Update Problem

- DNSSEC requires the registry to have a DS record associated with the zone.
- When 3rd party DNS providers generate the key(s) and sign the zone, there is no well defined path for providing the DS record to the registry. (Some ccTLDs are implementing RFC 8078.)

- We will tackle coordination among multiple 3rd party DNS providers in other venues

3rd Party DNS Provider

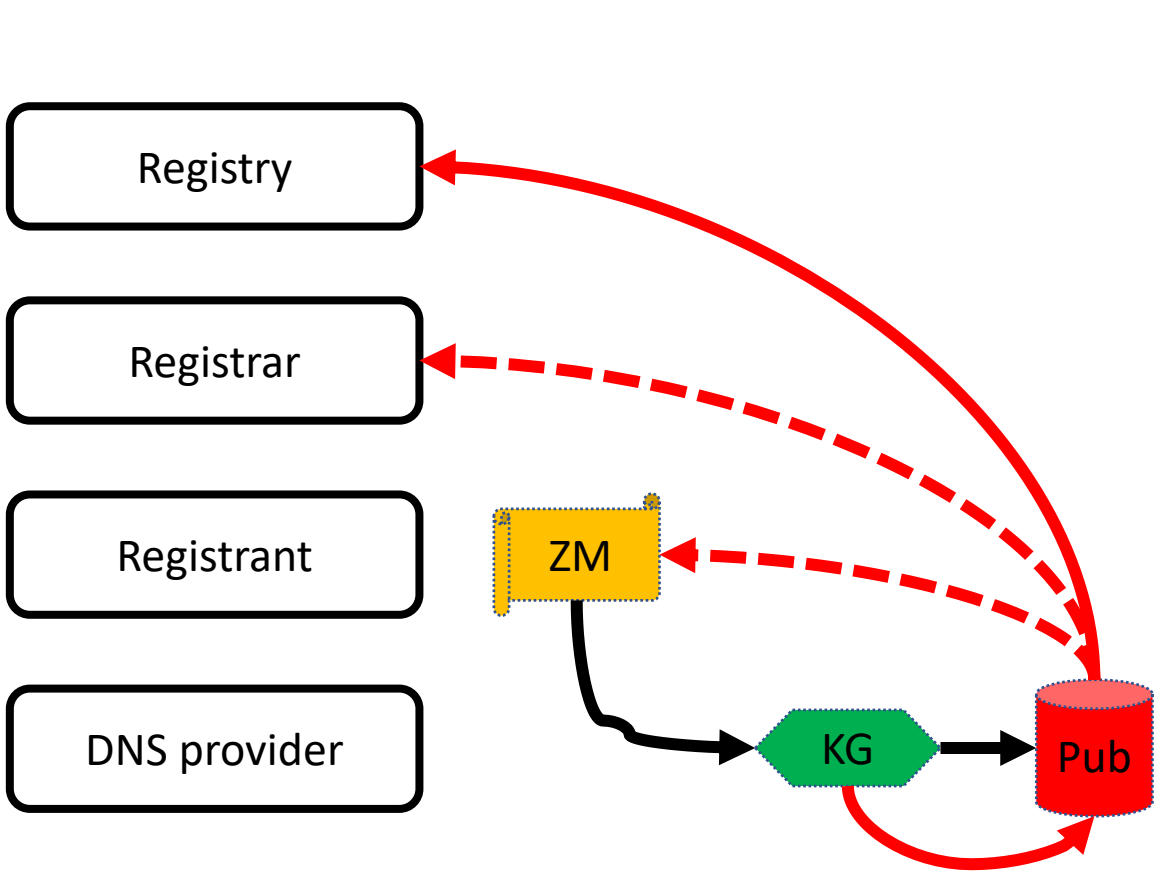


Three Dimensions of Possible Solutions

- Push vs Pull: The zone manager can push it upward or one of the higher entities can poll for it.
- The higher entity may be the Registrant, the Registrar or the Registry
- The data conveyed may be the DS record, the KSK, or both

CSK = Combined Signing Key

Publish CDS/DNSKEY and Poll



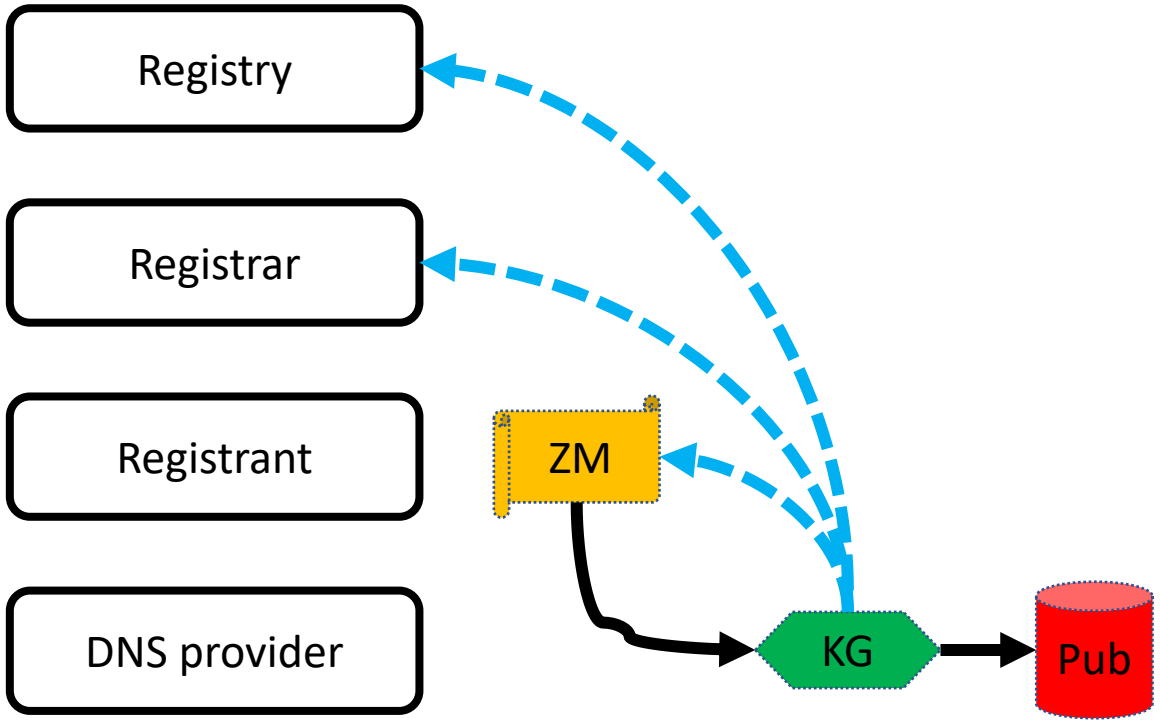
ZM — Zone Management

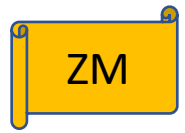
KG — Key Generation

Pub — Publication (Name Service)

CDS and/or CDNSKEY records are put into the child's zone and pulled by the registry.

Push DS record





Zone Management

Key Generation

Publication (Name Service)

DomainConnect is envisioned as a potential path for allowing a new DS record to be pushed to the registrar or registry.

Today's Panel: Registeries, Registrars and 3rd party DNS Providers

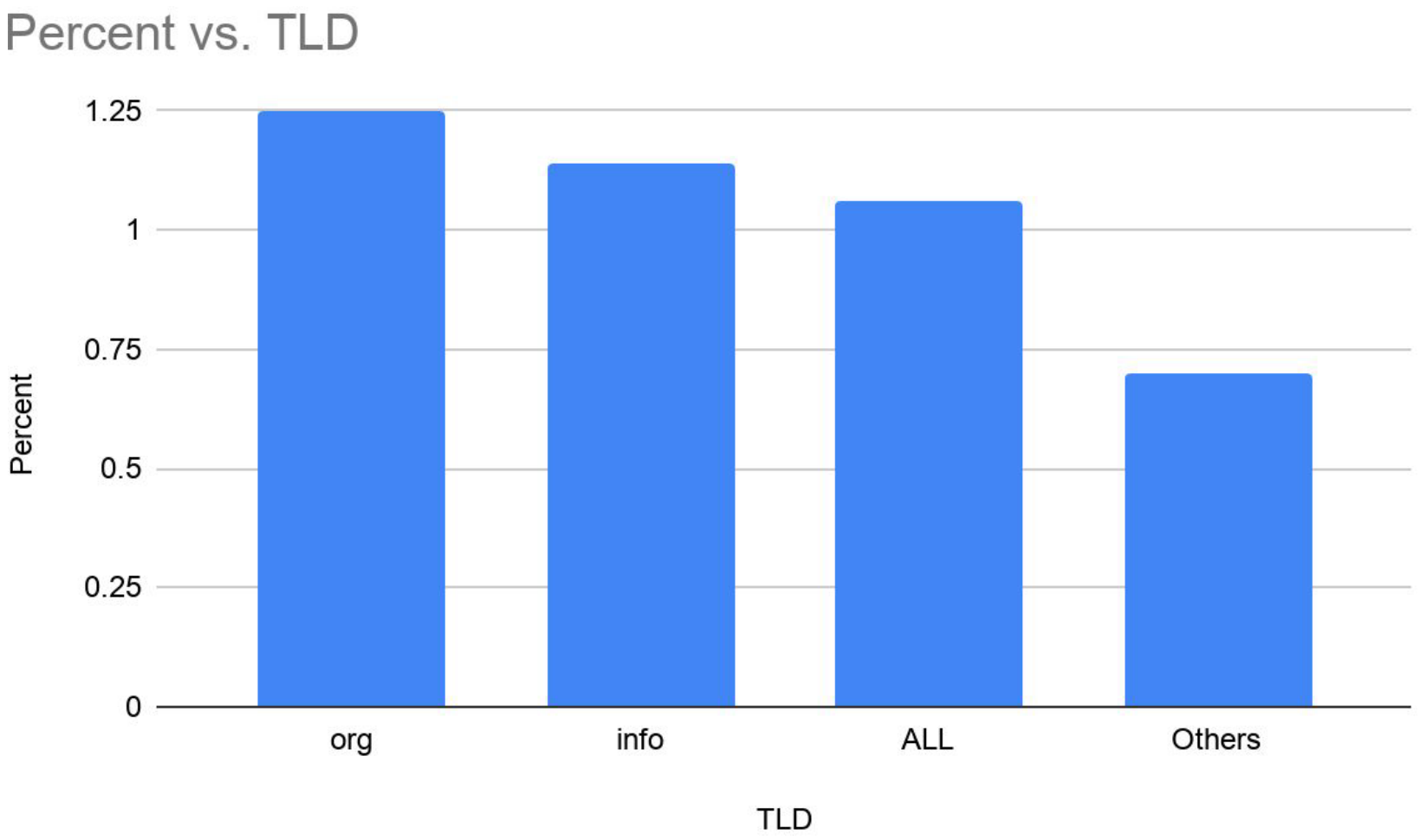
- What is the current state of automation of DS updates for 3rd party providers?
  - CDS and CDNSKEY publication ("pull") seem to be most common
  - This approach bypasses the registrar. Is this ok?
- What are the next steps for complete automation?
- What are the impediments?

Panelists

Panelists	Registry	Registrar	DNS Provider
Jim Galvin	Afilias		
Erwin Lansing	DK		
Gavin Brown, CentralNic	SK		
Brian Dickson		GoDaddy	
Jothan Frakes		PLISK	
Ólafur Guðmundsson		Cloudflare	

Jim Galvin, Afilias

Percentage of Delegated Domains



Erwin Lansing, .DK

Nameserver operator role @ .dk

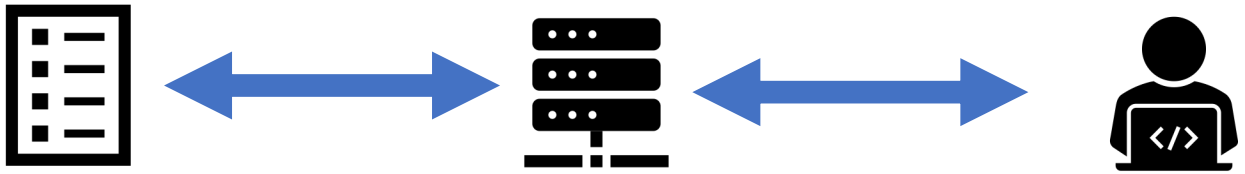
Nameserver operator

- **By policy**: All nameserver must be registered with the registry by the operator
- Registrant approval IFF within .dk domain

- Operator has a relation with the registry
- Operator can manage glue directly

- Caveats
- NS operator not involved in domain creation.
- Anyone can create a nameserver on non-.dk domains.
- No API, except EPP

Nameserver operator vs. domain



- Delegating a domain creates a relation between a domain and the NS operator
  - “Internal re-delegation” – operator can move domains between own nameservers
  - Manage DS*

  - RFC8078 on wishlist

* Conditions apply

Gavin Brown, CentralNIC

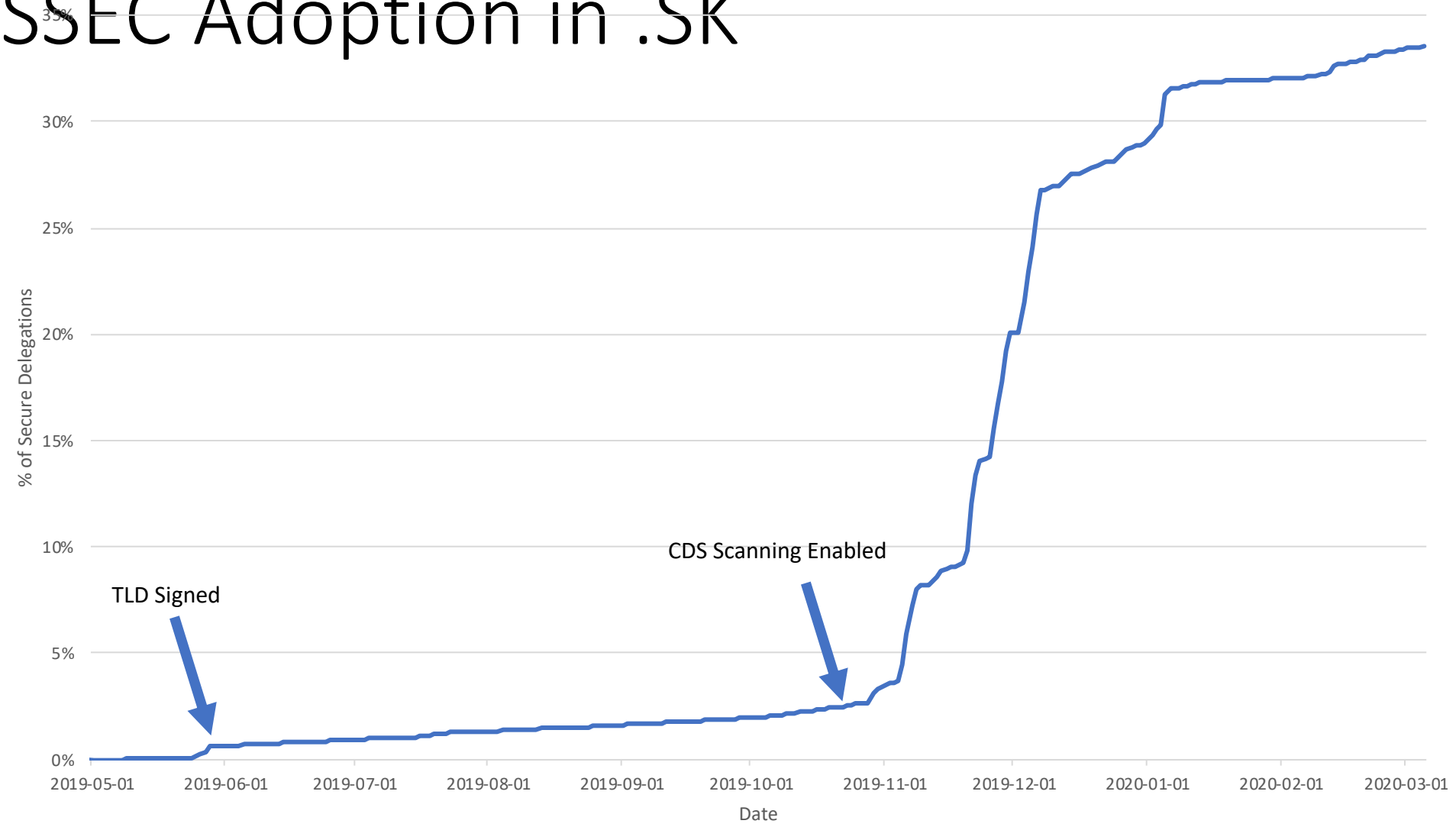
CentralNic Group PLC

Registry CDS Scanning

Gavin Brown <gavin.brown@centralnic.com>

ICANN67, March 11, 2020

DNSSEC Adoption in .SK



CDS Scanning in .SK

- .SK registrars already prepared for CDS scanning thanks to .CZ already deploying it
- Tooling inspired by FRED's CDS scanner
- Scanning policy derived partially from SWITCH's (.CH):
  - All domains (~400k) are scanned once per day (≈4.6 domains per second)
  - "Pending" domains (where CDS ≠ DS) are scanned every 3 hours
  - The CDS RRset must be stable over a period of 3 days before changes are implemented
  - Multiple independent resolvers must agree on CDS RRset over that period, otherwise, 3-day timer restarts

CDS Scanning in gTLDs - challenges

- Ambiguity (of RA): are we allowed? Would be nice to get the nod from ICANN org
- Scalability: ~20M domains, scanned once per day ≈ 230 domains per second
- As an RSP, we need approval from each of our (~60) ROs
- Need to implement Change Poll extension (RFC 8590) so registrars can stay in sync
- Potential impact: much larger DNS operator population, higher chance of operational issues

Brian Dickson, GoDaddy

GoDaddy DNSSEC DS

How We Do DS for DNS and Registry Customers

GoDaddy Registry Customers - DS

- Added via EPP
- Integrated into DNSSEC updates too
- Customer UI always available to change DS records at Registry
- Managed DNSSEC generally suppresses Manual DS updates
- Customers can disable Managed DNSSEC and submit DS
- Enabling Managed DNSSEC triggers update to DS

GoDaddy Managed DNSSEC DS

- Regardless of parent (TLD), CDS and CDNSKEY are always published
- That is all
- We encourage all Registries to poll CDS and/or CDNSKEY
- It would be nice if Registries had a way to publish which they use (CDS or CDNSKEY)
- Registrars: Please understand that DS records are “use once” in nature, and there should never be a need to obtain a DS if updated via CDS or CDNSKEY
- Registries/Registrars: Notification for non-CDS/CDNSKEY DS updates would really be a good thing. Ideally exclude CDS/CDNSKEY changes from the notification scheme.

GoDaddy DNSSEC Cross-Signing

- We don’t do anything yet
- We are interested in working on this

Jothan Frakes, PLISK

Registrars and DNSSEC

- Registrars are the interface with the Registrant, by design
- Key info used in DNSSEC furnished to Registry via Registrar, by design
- End-to-end chain requires both registration and resolution info matching, by design
- DNSSEC is complex, but it carries some benefits to Registrants
- Registrars, recognizing the benefit and value of DNSSEC created integrated solutions using their own Nameservers to simplify approach for registrant

Getting signing info to Registry (Ry)

Resolution providers want to furnish info into registration path via automation at the registrar

Path A: Records communicated Via DNS, where Registry pulls information per name from domain zone records

Pros	Cons
Pull method bypasses API / Registrar constraints	Adoption: Not widely used by registries
Self-managed	Scaling: What would this look like for a Ry w/ zone >10M or 100M entries?
Automated, less prone to human error	Pace: Frequency of update determined by Registry

Getting signing info to Registry (Ry)

Path B: Via Registrar (Rr) manually or (via some TBD API), then to Registry (Ry) via EPP

Pros	Cons – Rr Manual	Rr API (if exists)
• Rr records updated/synched with Ry • DNSSEC Works	• Complex for most users unless integrated DNS @ Rr • Prone to human error • 3P DNS provider may not offer good documentation	• N+1 integrations for 3P DNS • API provides more access to customer account than needed • Must be limited to DNSSEC info
	• Customer Support Costs @Rr even if issues from 3P Provider	
	• 3P DNS Provider using as customer lure (are they Rr)?	

Registrars also want to make certain no other paid services are disrupted in DNS, if provided directly at registrar.

Ólafur Guðmundsson, Cloudflare

DNS Delegation Automation

Ólafur Guðmundsson
Cloudflare

Automate or not to Automate ?

- DS is derived from DNSKEY via CDS or CDNSKEY
- For NS parent is authoritative for existence, child for content

Information is available in r eal time,
Changes over time
Accuracy improves the ecosystem

CLOUDFLARE

Welcome to the 21st century

- Cloudflare Registrar
  - pushes DS record to Registry
  - Removes DS when users disable DNSSEC or leave
  - Deletes DS on incoming transfers
- DNS authoritative service
  - Signs on the fly
  - Publishes CDS + CDNSKEY for all DNSSEC enables zones
    - CDS 0 when users disable DNSSEC

CLOUDFLARE

How to Get Involved

- Dnssec-provisioning@shinkuro.com is a design team mailing list

  (Send mail to steve@shinkuro.com)