

Improving DNSSEC Provisioning with 3rd party DNS Providers

Shumon Huque, Steve Crocker

8th February 2020

32nd DNS OARC Workshop, San Francisco, CA

Two Problems

1. 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.)
2. If multiple 3rd party DNS providers are serving the same zone, each is signing with its own key, they each need to include the ZSKs (or CSKs) of the other providers. “Multi-Signer DNSSEC Models” defines the general scheme, but there is no well defined protocol for coordination of the cross-signing process between the providers.

Entities and Functions

Entities

- Registry
- Registrar
- Registrant
- Authoritative DNS Provider
- (Secondary DNS Provider)

Functions

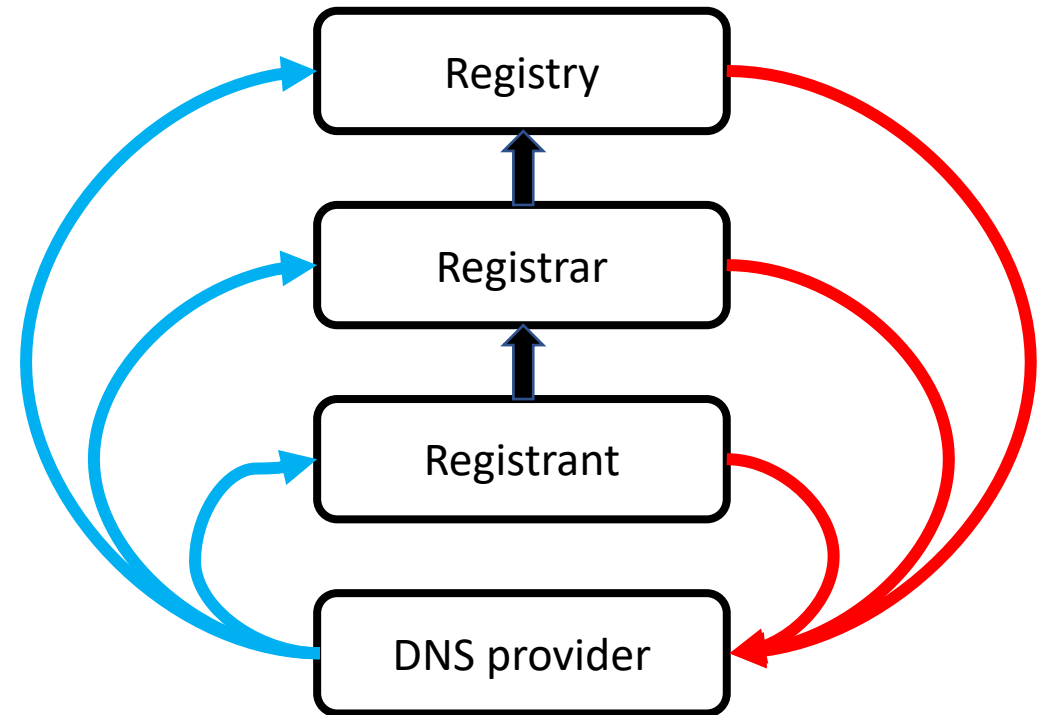
- Zone Management
- Keygen & Signing
- Zone Publishing
- Communication of DS/KSK records
- Coordination of Cross-Signing

Conveying a new DS record

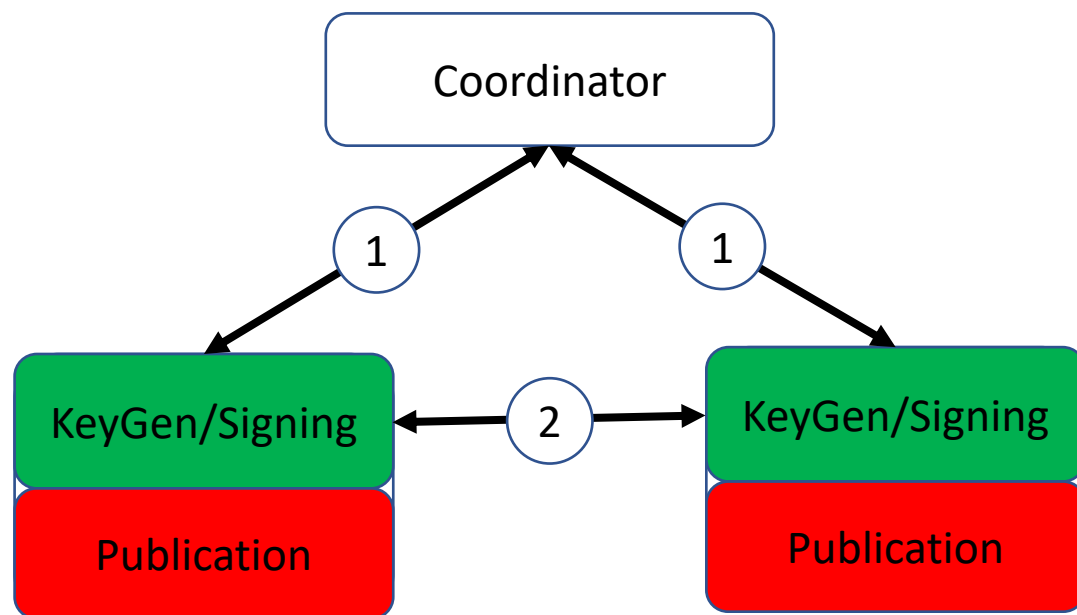
- When zone's KSK (or CSK) is rolled, the registry gets revised DS record
- Several methods are possible, based on three attributes
 - Push vs Pull: The zone manager can push it upward or one of the higher entities can poll for it.
 - The higher entity may be the Registrant, the Registrar or the Registry
 - The data conveyed may be the DS record, the KSK, or both
- Possible work: including 3rd party operators in the RRR system (formally designating them; using delegated authorization schemes ..)

Conveying the DS key from 3rd party DNS Provider

	Direction	
Upper Side	Push (Calling)	Pull (Polling)
Registry		RFC 8078
Registrar	Extension to Domain Connect	
Registrant		Manual



Coordinating Cross-Signing



Options for communicating ZSKs

- 1 Registrant coordinates either by itself or through new 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

How to Get Involved

- Dnssec-provisioning@shinkuro.com is a design team mailing list
(Send mail to steve@shinkuro.com)

Looking for a few more DNS providers and registrars

Note: there will be a DNSSEC Provisioning panel discussion at ICANN67 in Cancun next month (11 March 2020).

Appendix: Diagrammatic Toolbox

Some Signed DNS Service Configurations

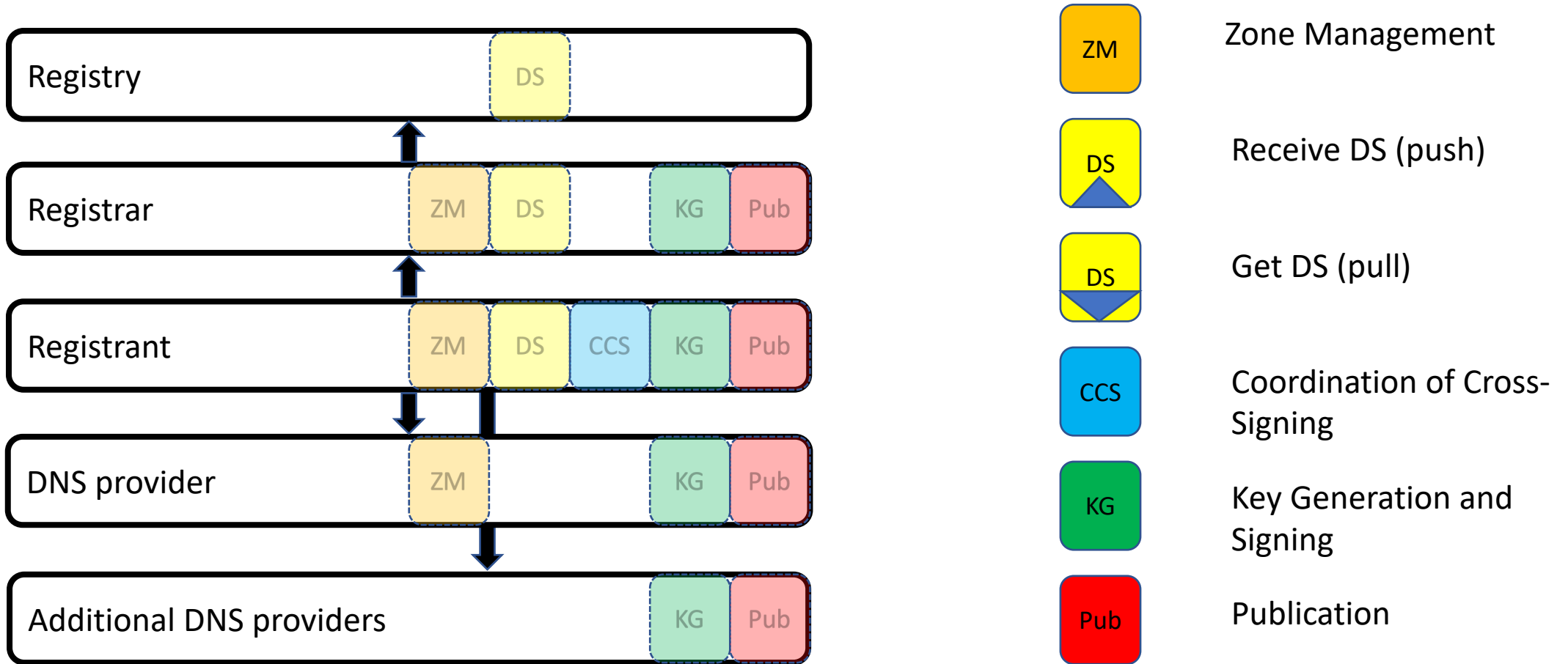
This list is not exhaustive

	Registrar Provides DNS Service	Registrant Provides DNS Service	Single Outsourced DNS	Multiple Outsourced DNS
Registry			DS pull	
Registrar	ZM, KG, Pub, DS			
Registrant		ZM, KG, Pub, DS	ZM	ZM, CCS, DS pull
DNS Provider(s)			KG, Pub	KG, Pub

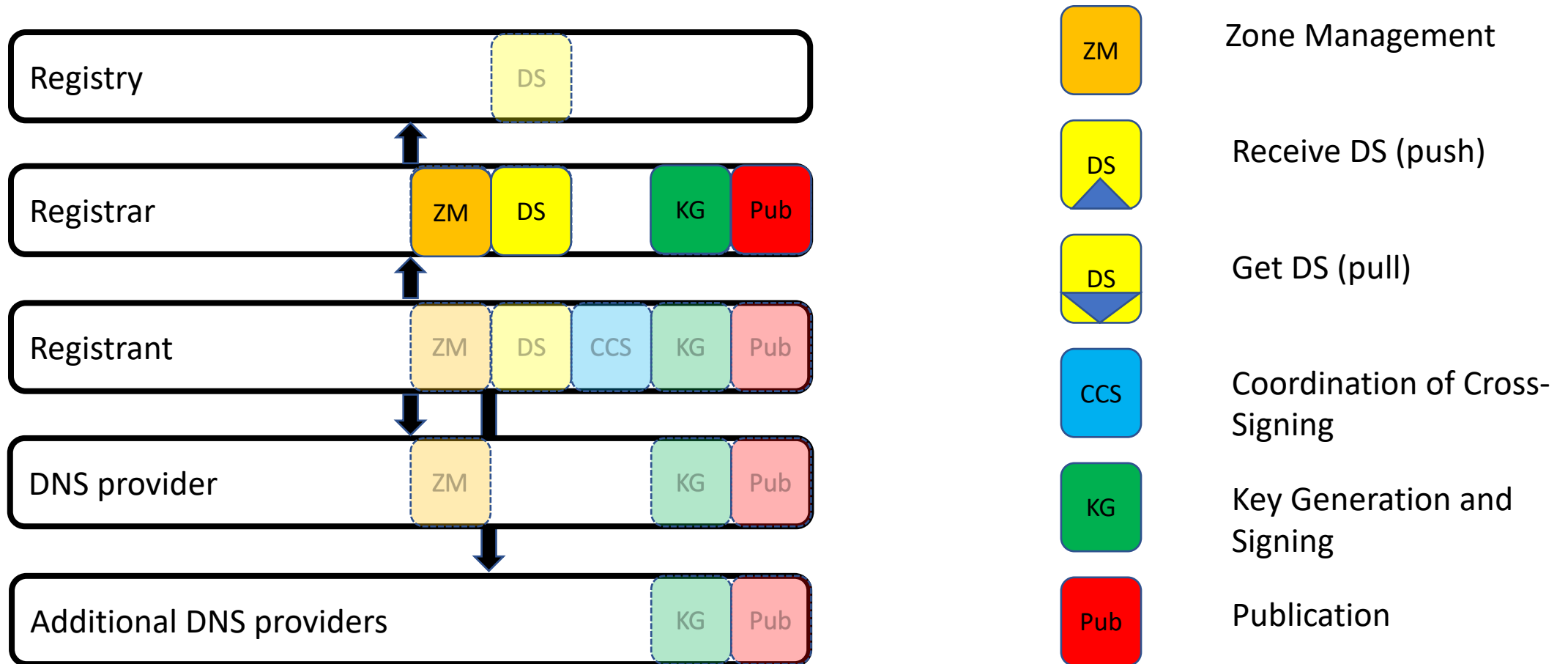
ZM = Zone Management
KG = Key Generation and Signing
CCS = Coordination of Cross-signing
Pub = Publication

- DS pull = DS record is pulled (by polling) from Publisher
- DS push = DS record is pushed upward via the Registrar
- (DS pull) indicates a possibility with no known examples
- DS pull/push? Indicates uncertainty if this is possible

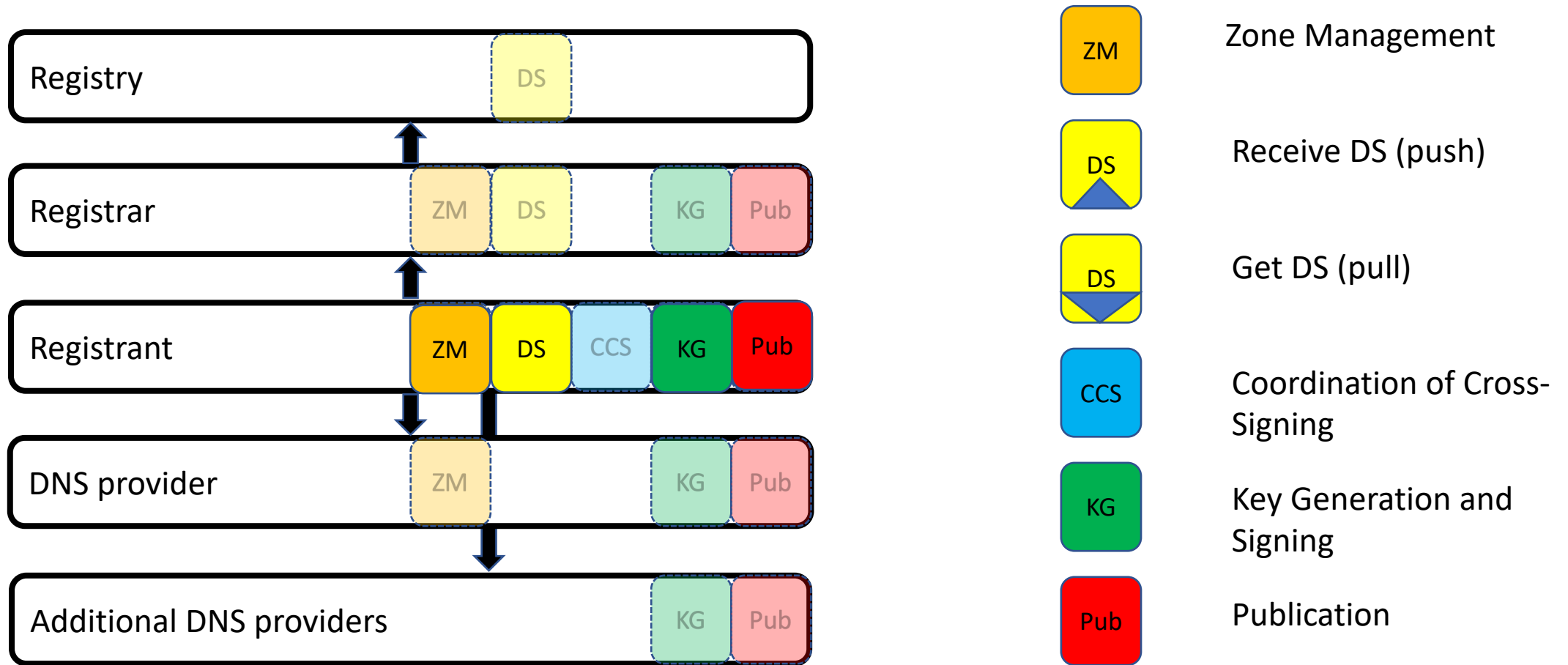
DNSSEC Provisioning Configuration Options



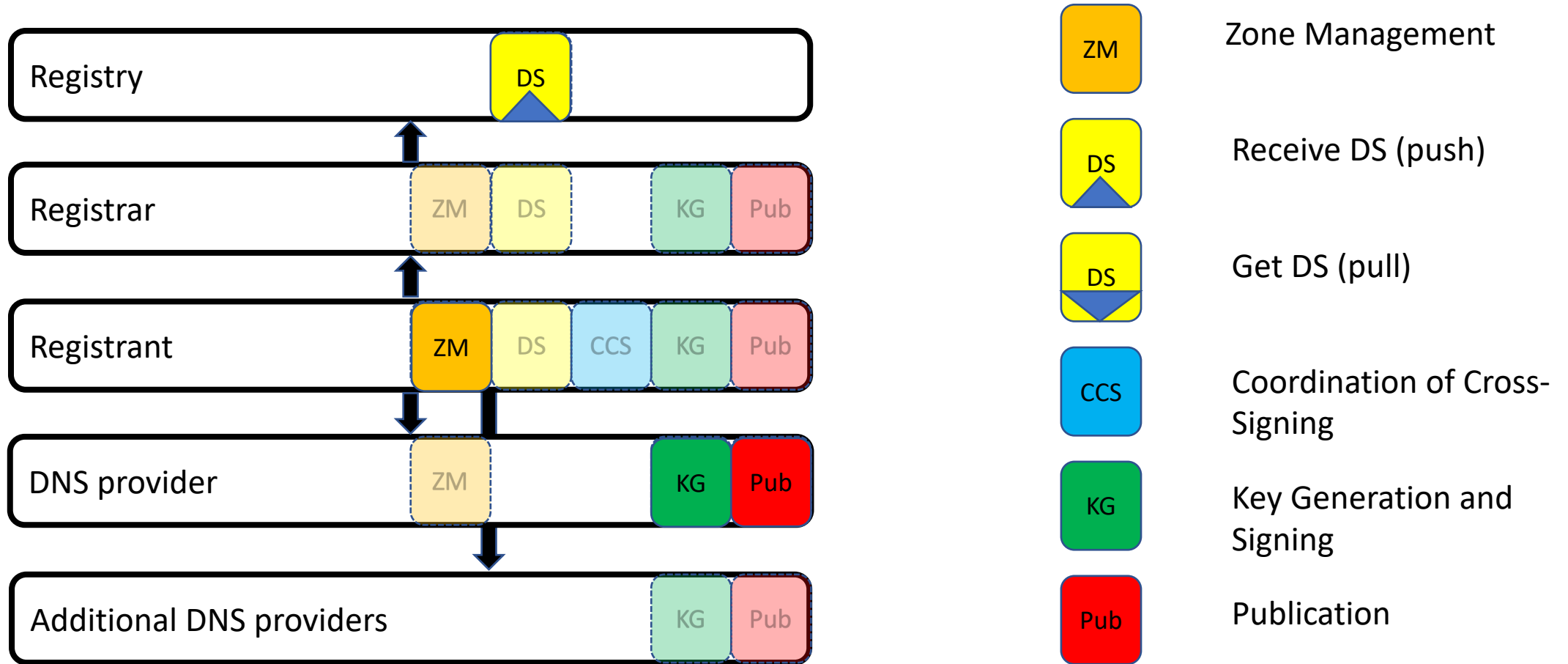
Registrar Provides DNS Service



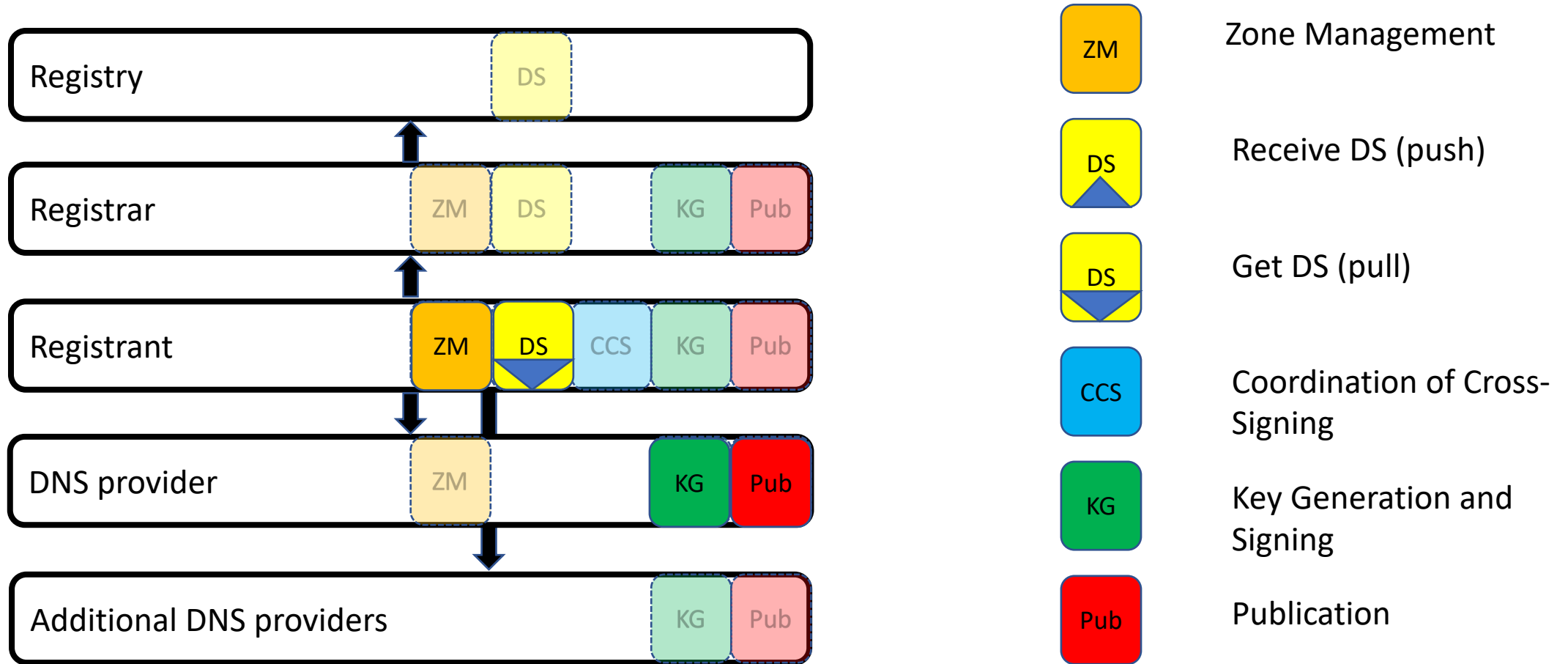
Registrant Provides DNS Service



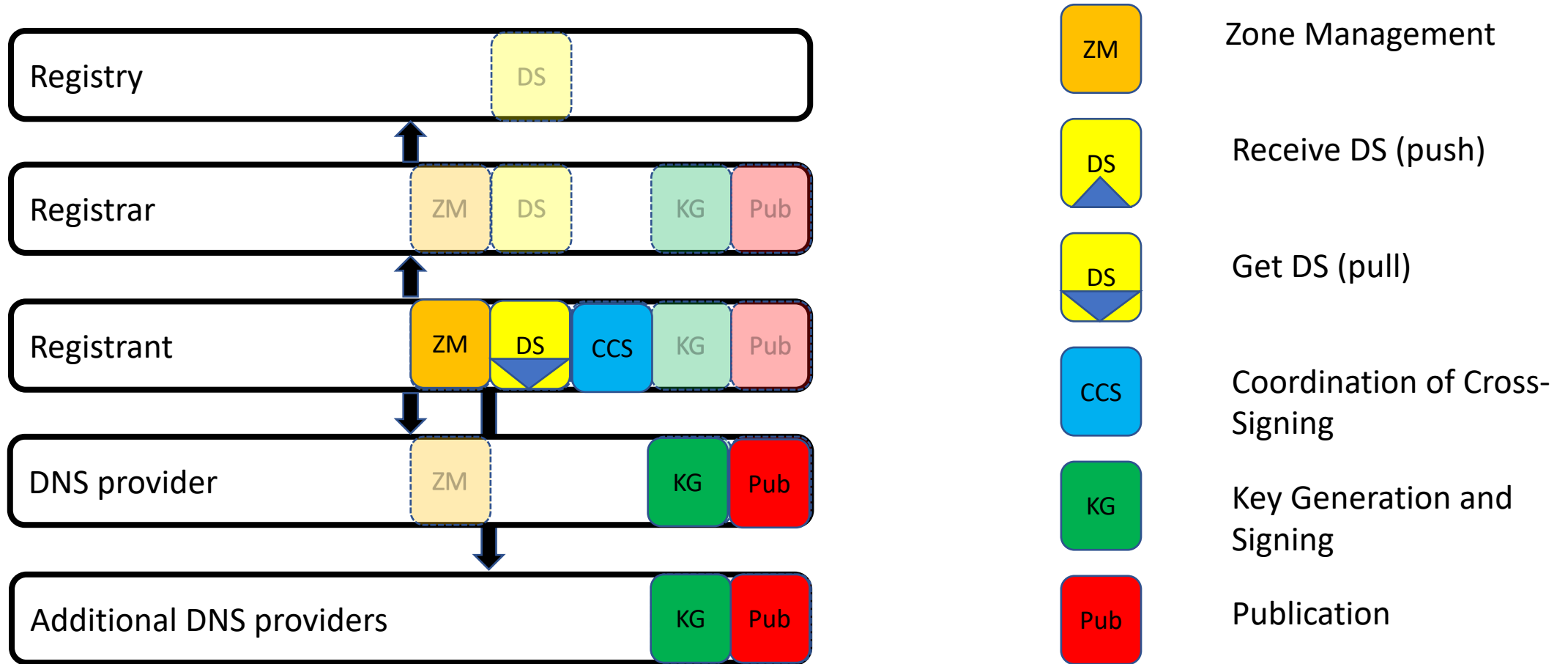
Single Outsourced DNS Provider w RFC 8078



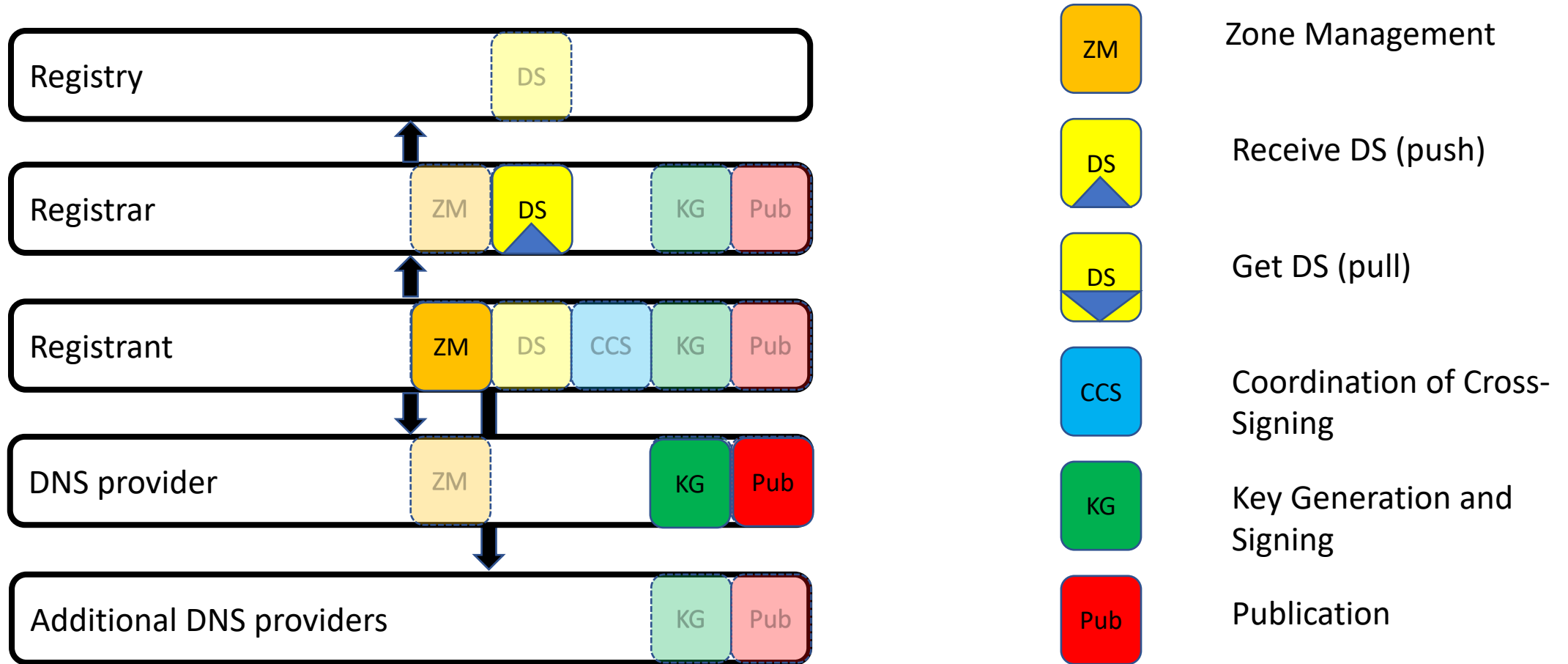
Single Outsourced DNS Provider – Registrant pulls



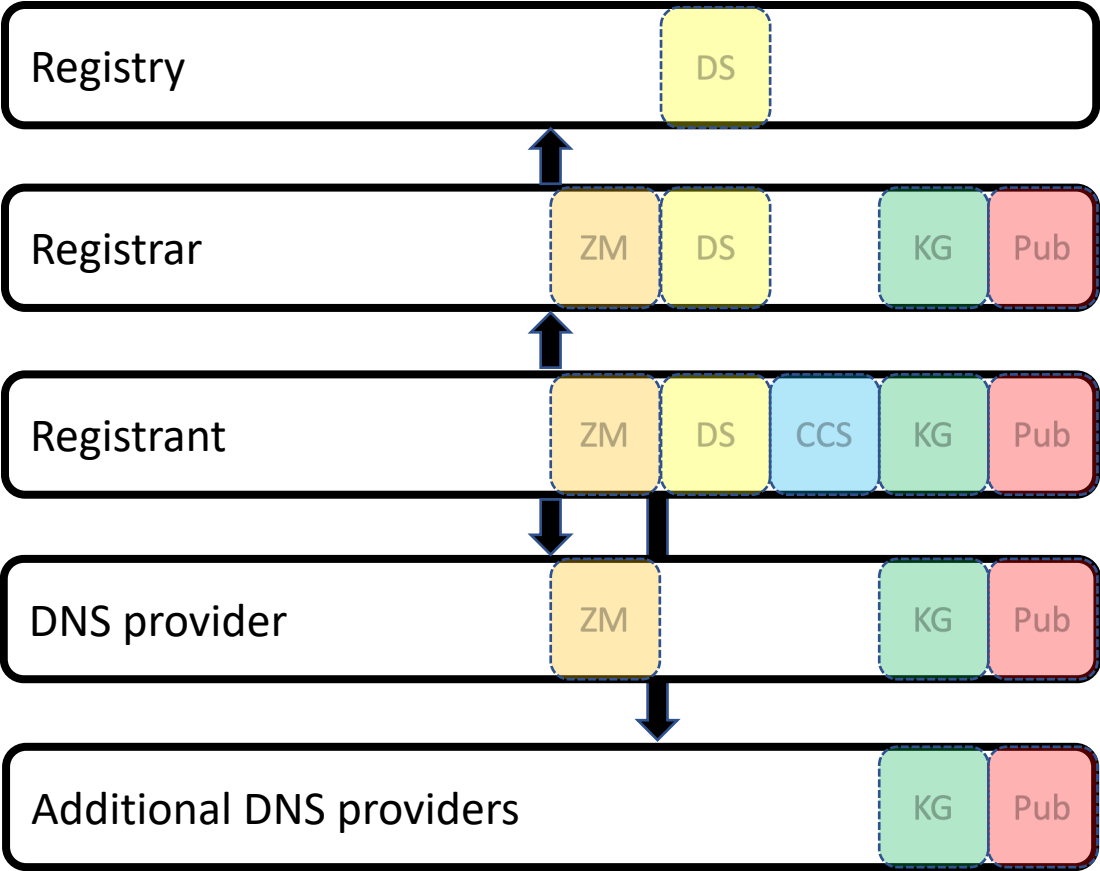
Multiple Outsourced DNS Providers









Registrar with Domain Connect



Additional Configuration



	Zone Management
	Receive DS (push)
	Get DS (pull)
	Coordination of Cross-Signing
	Key Generation and Signing
	Publication