Sunset for the DLV?

Agenda

- Background: DLV as a **transition mechanism** to aid in DNSSEC adoption
- DNSSEC adoption status
- Steps to decommission the DLV
- Proposed timeline

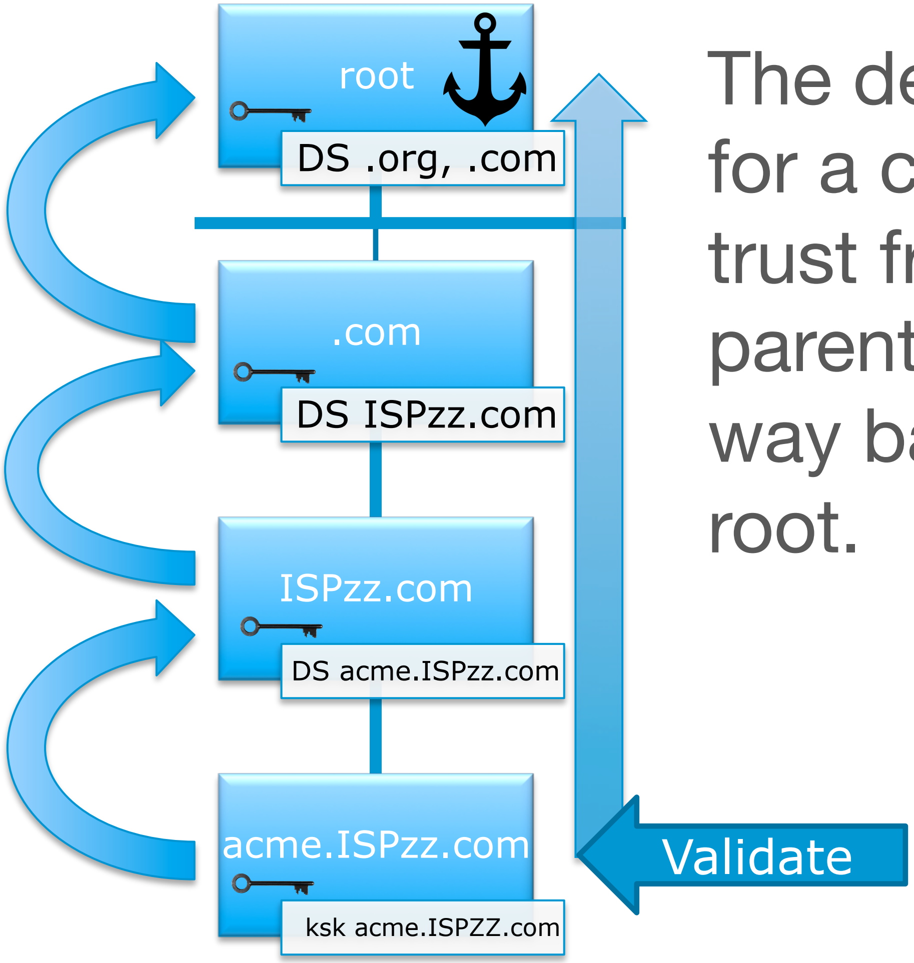
Background

(c) Interested Bystandr @flickr

Read at home

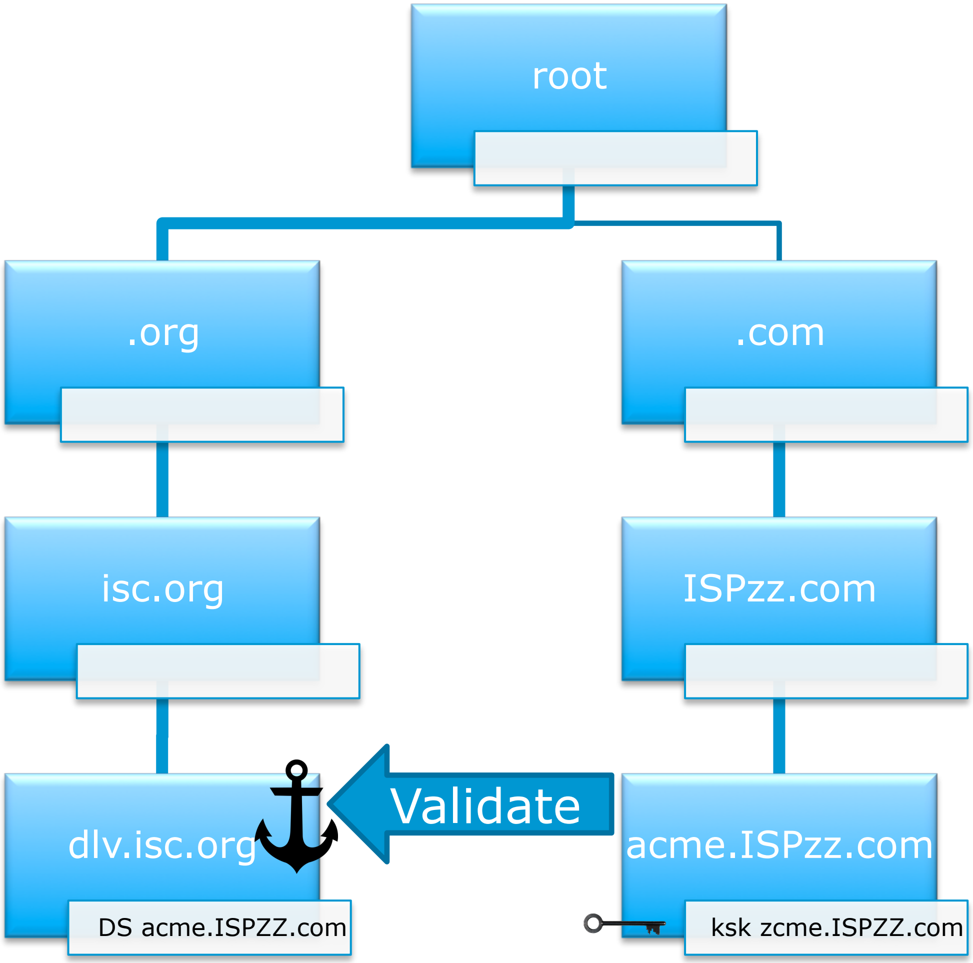
- A little context: when ISC created the DLV Registry, we were years away from the .com/.net/.org zones (let alone the root zone) from being signed, so there was a chicken and egg problem.
- Organizations wouldn't deploy DNSSEC because there was no easy way to have a validated chain of trust.
- And the TLD's themselves were reluctant to sign their zones for a multitude of reasons (bigger response sizes, etc.) and concerns as to how issues those would affect DNS resolution.
- DLV allowed organizations to sign their zones, and the caching resolver (if it has DLV validation support enabled) to validate the keys.
- Instead of looking for a chain of DS/DNSKEY records from the root DNS zone downwards the resolver walks an alternate path (via dlv.isc.org) to lookup the corresponding DLV record instead, the DLV record providing the same assurance about a key that a DS record does.
- DLV is described in RFC 4431.

DNSSEC Validation



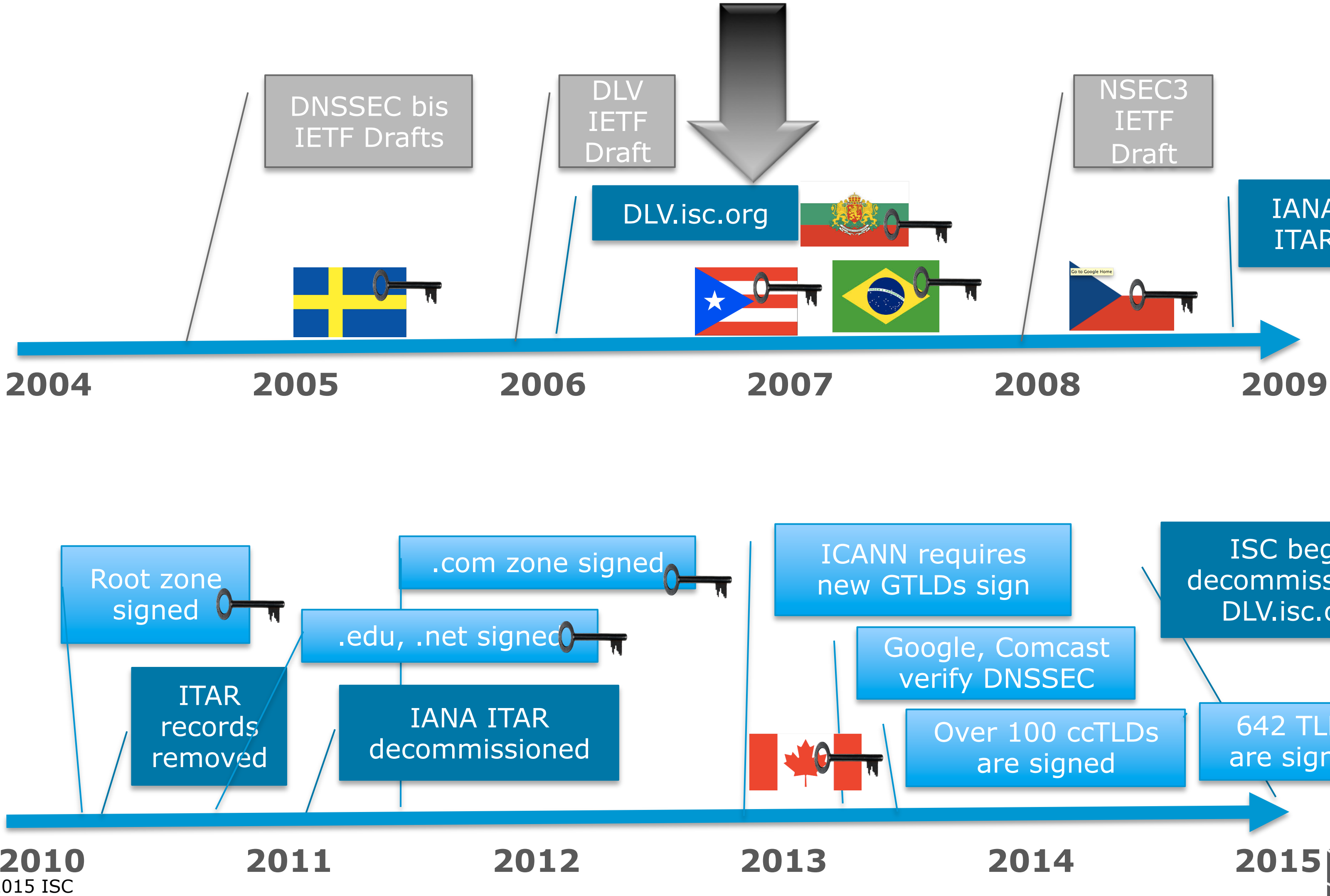
The design calls for a chain of trust from child to parent, all the way back to the root.

DLV = alternate path to trust anchor



Before the planned chain of trust was available, the DLV provided a substitute.

A lot has changed since 2006



DNSSEC bis IETF Drafts

DLV IETF Draft

DLV.isc.org

NSEC3 IETF Draft

IANA ITAR

2004

2005

2006

2007

2008

2009

Root zone signed

ITAR records removed

.com zone signed

.edu, .net signed

IANA ITAR decommissioned

ICANN requires new GTLDs sign

Google, Comcast verify DNSSEC

Over 100 ccTLDs are signed

ISC begins decommissioning DLV.isc.org?

642 TLDs are signed

2010

2011

2012

2013

2014

2015

Is DLV now DELAYING deployment?

+

Benefits

- Allows a signed zone to be validated even if the parent is not signed
- Accepts DS records from anyone
- Free service

−

Disadvantages

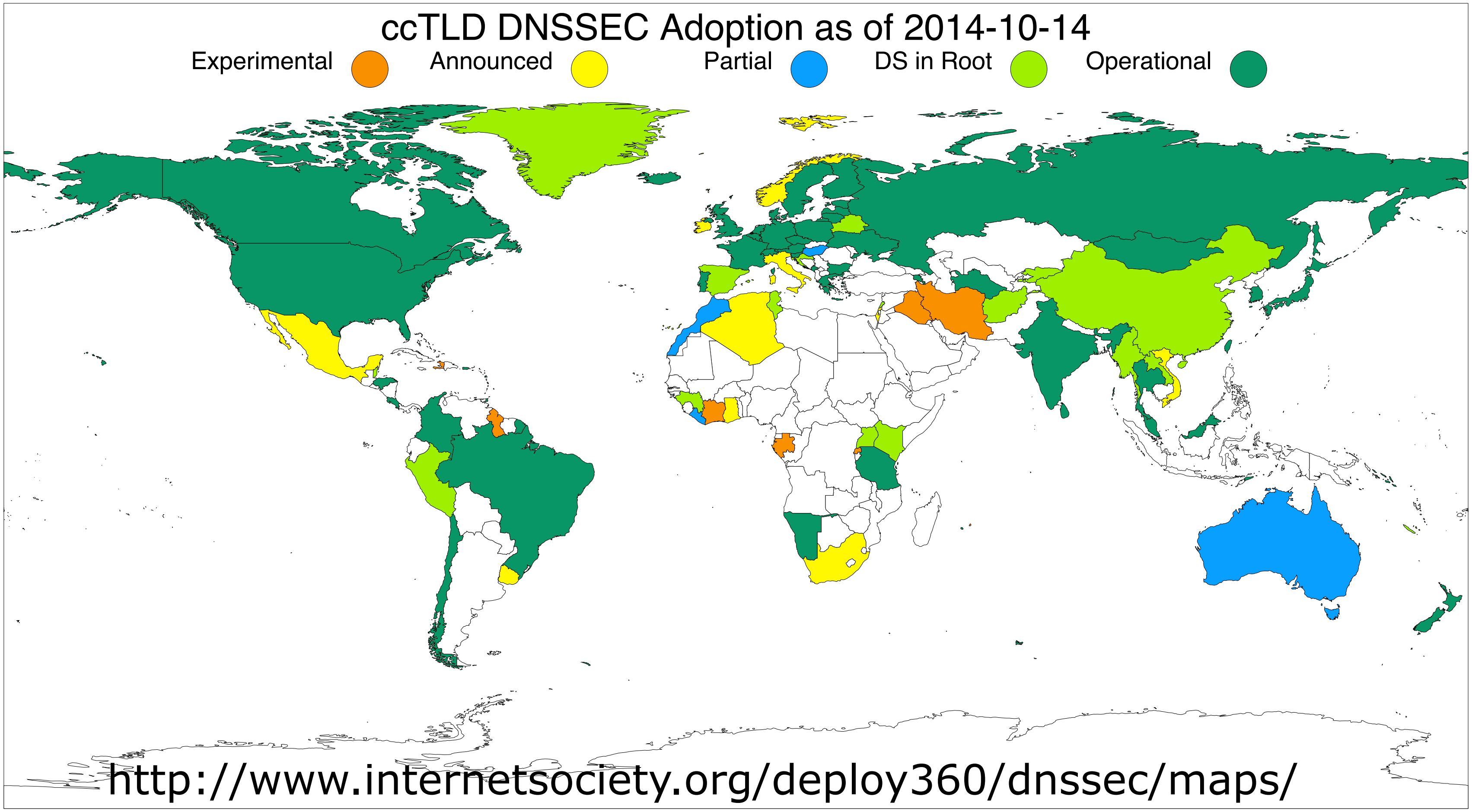
- Reduces pressure on parent to get signed
- Reduces pressure on registrars to accept DS records
- Validator has to perform an additional query to the DLV when validating

Who Needs the DLV?

- Entities with signed zones under **unsigned parent zones** (i.e., signed 2nd level domains under unsigned ccTLDs)
- Entities that use **Registrars that don't support DNSSEC** (Registrar doesn't accept DS records)

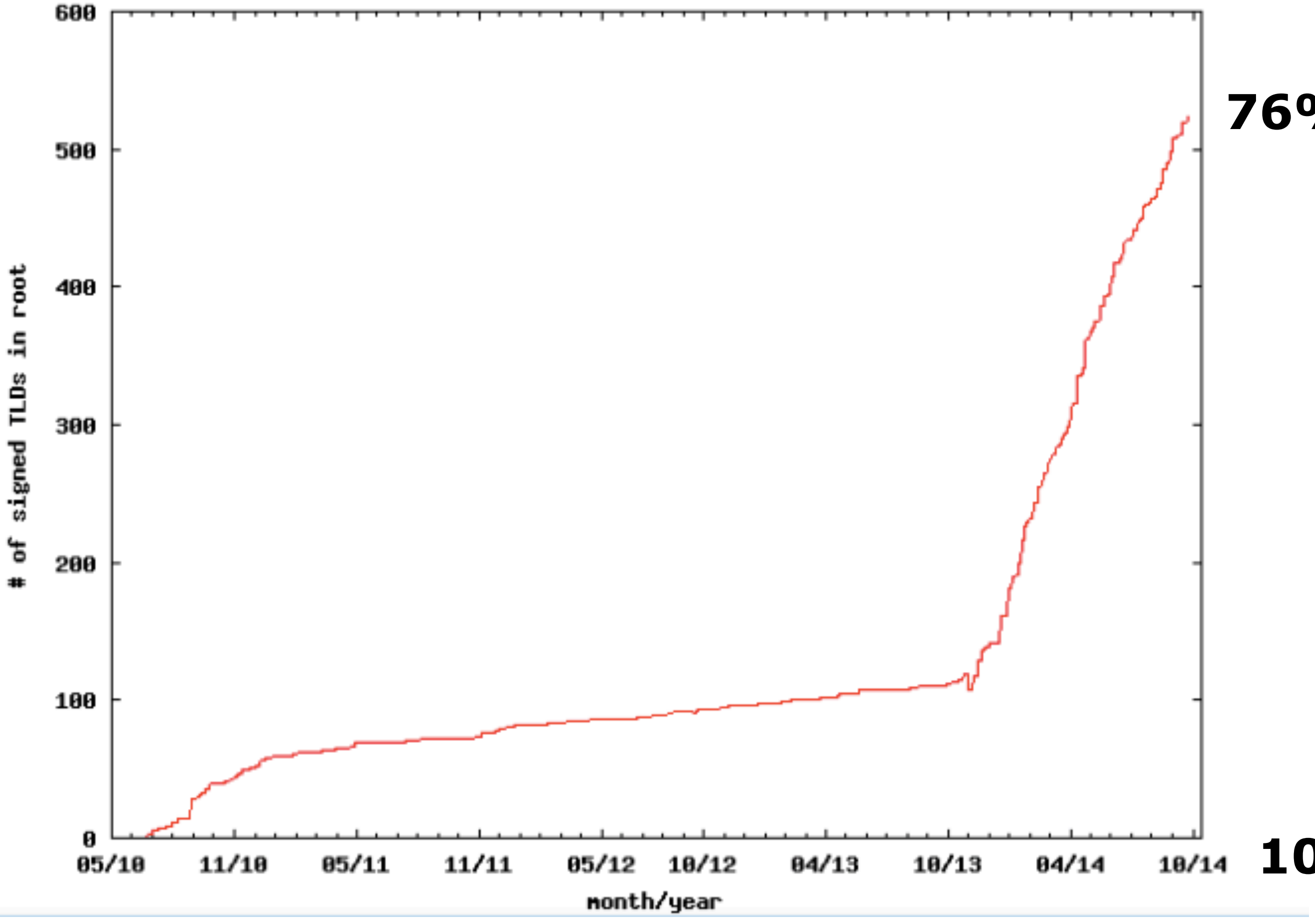
- Signed zones moving from one registrar to a new registrar may benefit from temporary coverage by DLV, esp if first registrar is uncooperative in the move

ISOC deploy360 report


ccTLD DNSSEC Adoption as of 2014-10-14
Experimental
Announced
Partial
DS in Root
Operational
http://www.internetsociety.org/deploy360/dnssec/maps/

Experimental -- Internal experimentation announced or observed (11):	CI GA GY HK HT IQ IR MS MU RW TO
Announced -- Public commitment to deploy (11):	DZ GH IE IL IT MX NO SG UY VN ZA
Partial -- Zone is signed but not in operation (no DS in root) (5):	AU HU LR MA VC
DS in Root -- Zone is signed and its DS has been published (29):	AD AF AG AW BY BZ CC CN ES FO GI GL GN HR KE KG KI LA LB LC MM NC NU PE PW SJ TN TV UG
Operational -- Accepting signed delegations and DS in root (62):	AC AM AT BE BG BR CA CH CL CO CR CX CZ DE DK EE FI FR GR GS HN IN IO IS JP KR LI LK LT LU LV ME MN MY NA NF NL NZ PL PM PR PT RE RU SB SC SE SH SI SX TF TH TL TM TT TW TZ UA UK US WF YT

DNSSEC Deployed on 586 out of 771 TLDs



76%

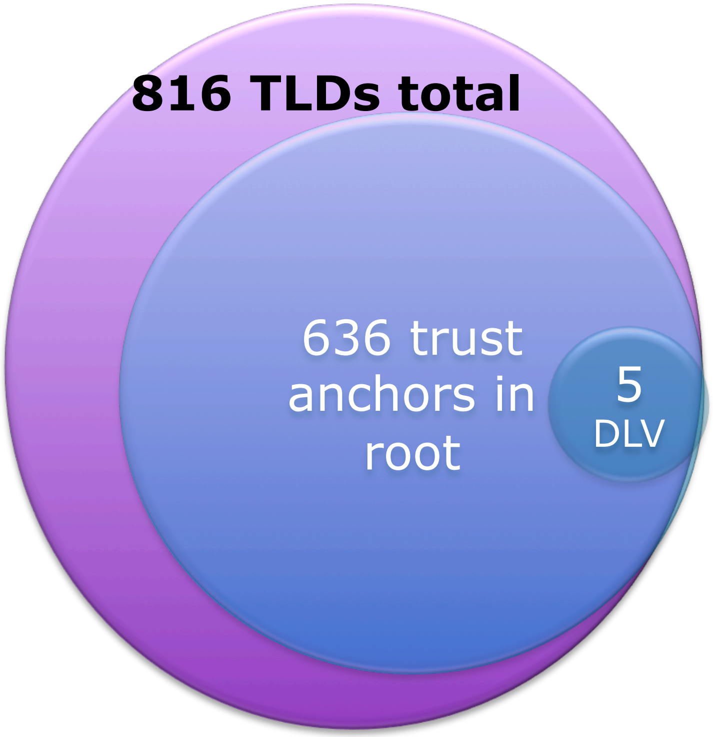
10/2014

https://www.icann.org/resources/pages/deployment-graph-2012-02-25-en

ICANN TLD DNSSEC Report

(2015-02-08)

- 816 TLDs in the root zone in total
- 642 TLDs are signed
- 636 TLDs have trust anchors published as DS records in the root
- 5 TLDs have trust anchors published in the ISC DLV
- **0 TLDs *need* DLV**



Registrar Support

- Registrar support for DS records is available but not universal
- Some DLV users will have to switch registrars, putting appropriate pressure on registrars to support DS records

Registrars that support end user DNSSEC management, including entry of DS records
https://www.icann.org/resources/pages/deployment-2012-02-25-en
Last updated: 15 December 2014
Updates to: dnssec@icann.org

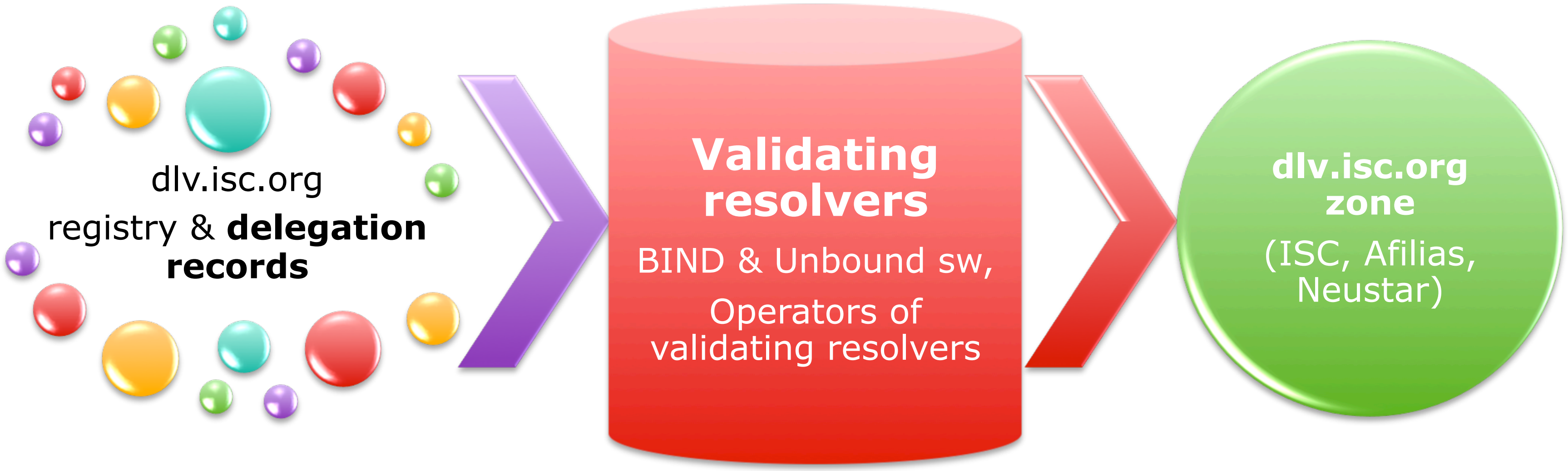
Ready to Sunset DLV?

- ✓Root signed
- ✓TLDs signed (79%)
  - ✓TLDs have trust anchors in root
- ✓Registrars supporting DNSSEC validation records for child domains
  - ✓Announcing sunset plan for DLV will encourage this
  - ○ *Possible longer-term need for registrar transition coverage*

Agenda

- Background: DLV as a transition mechanism to aid in DNSSEC adoption
- DNSSEC adoption status
- Steps in decommissioning the DLV
- Proposed timeline

DLV System Elements



dlv.isc.org registry & **delegation records**

Validating resolvers

BIND & Unbound sw,

Operators of validating resolvers

dlv.isc.org zone

(ISC, Afilias, Neustar)

1st Step = Remove Delegated Zones

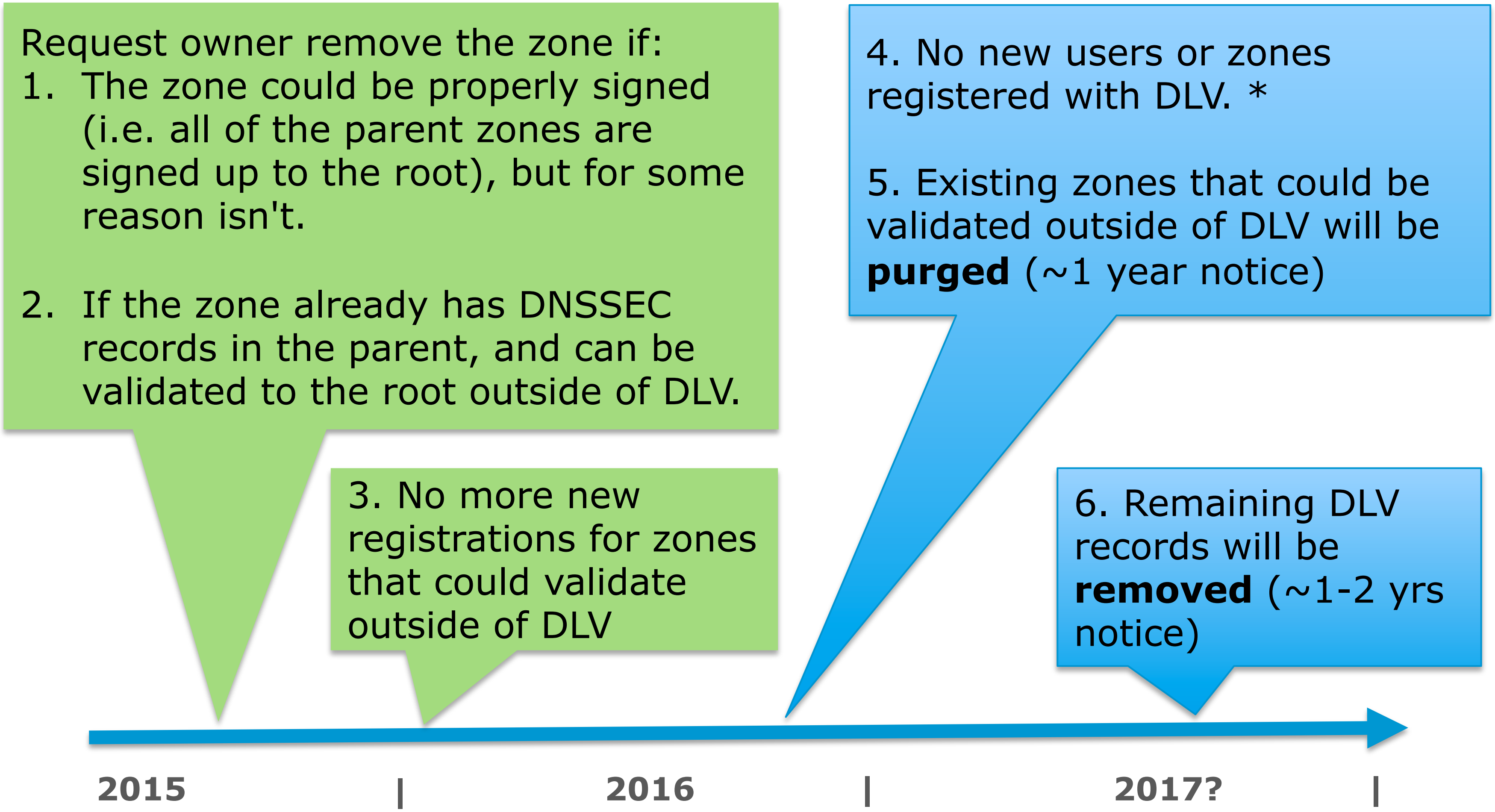
dlv.isc.org

registry & **delegation records**

4568 zones configured

- 2867 fully configured/ working zones
  - only 397 are in an unsigned parent
- Notify, and Remove unnecessarily delegated zones
- Stop adding new zones
- Eventually, remove all zones

Proposed timeline for shrinking the DLV zone list



Request owner remove the zone if:

1. The zone could be properly signed (i.e. all of the parent zones are signed up to the root), but for some reason isn't.

2. If the zone already has DNSSEC records in the parent, and can be validated to the root outside of DLV.

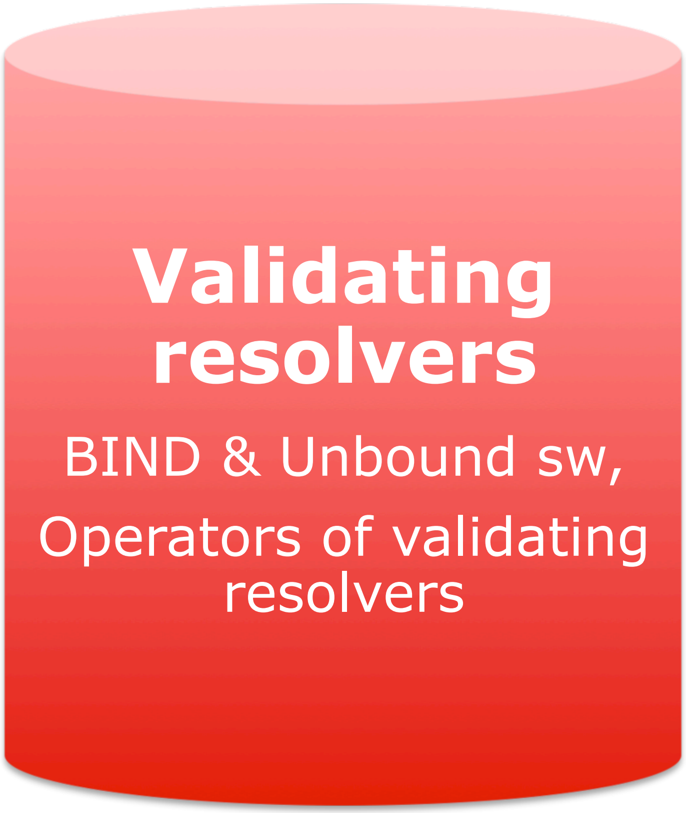
3. No more new registrations for zones that could validate outside of DLV

4. No new users or zones registered with DLV. *

5. Existing zones that could be validated outside of DLV will be **purged** (~1 year notice)

6. Remaining DLV records will be **removed** (~1-2 yrs notice)

DLV queries - burden on validating resolvers?



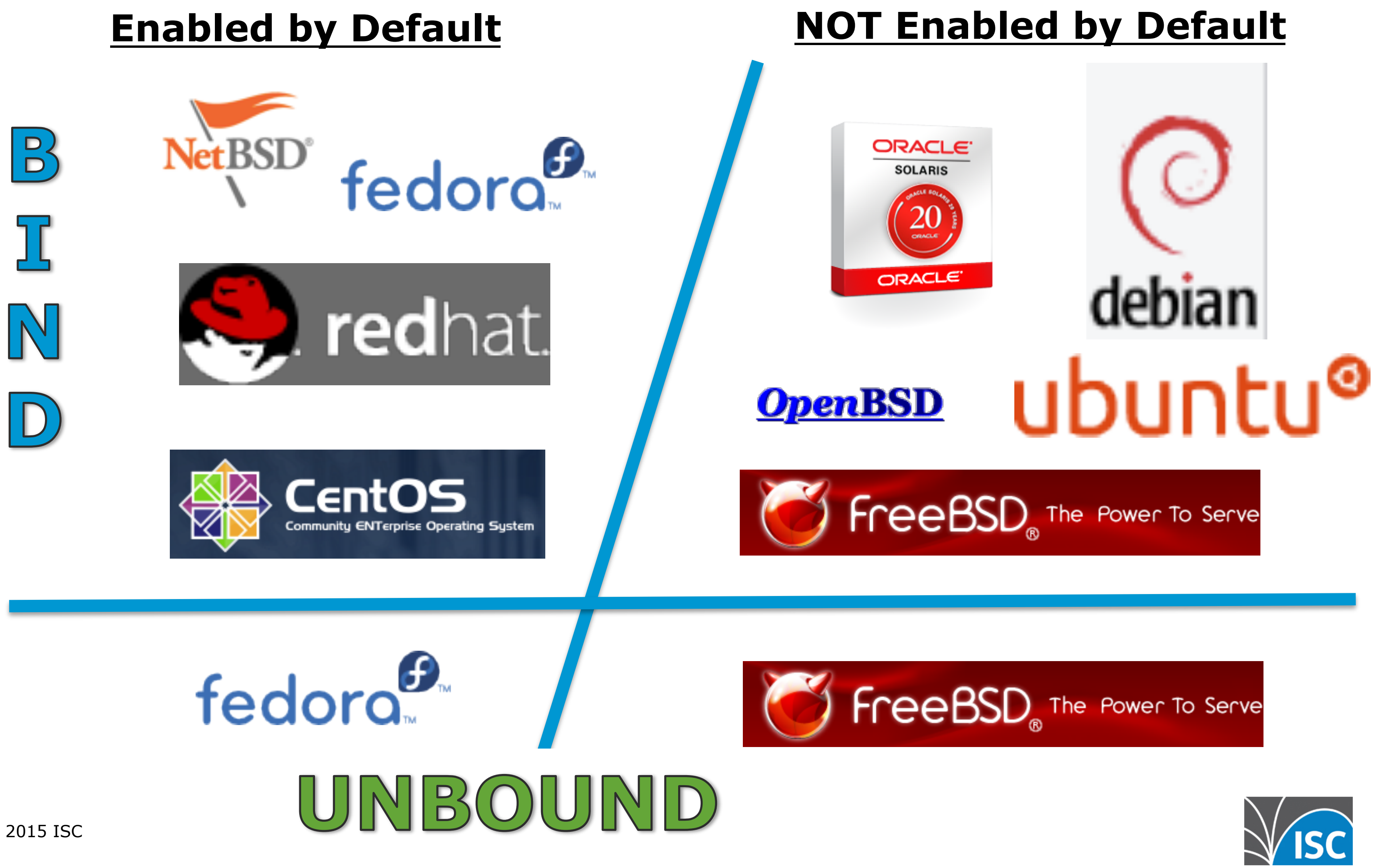
Validating resolvers

BIND & Unbound sw,

Operators of validating resolvers

- When DLV validation is enabled, validator performs an additional query to the DLV
- Turning this off means validation failures for zones in the DLV
- Long transition period
- DNSSEC ‘How-To’ docs
- SW - disable by default

DLV Enabled



Enabled by Default

NOT Enabled by Default

BIND

UNBOUND

NetBSD
fedora
redhat.
CentOS
Community ENTerprise Operating System
ORACLE
SOLARIS
20
ORACLE
debian
OpenBSD
ubuntu
FreeBSD The Power To Serve
fedora
FreeBSD The Power To Serve

DLV Zone stays up

dlv.isc.org zone

(ISC, Afilias, Neustar)

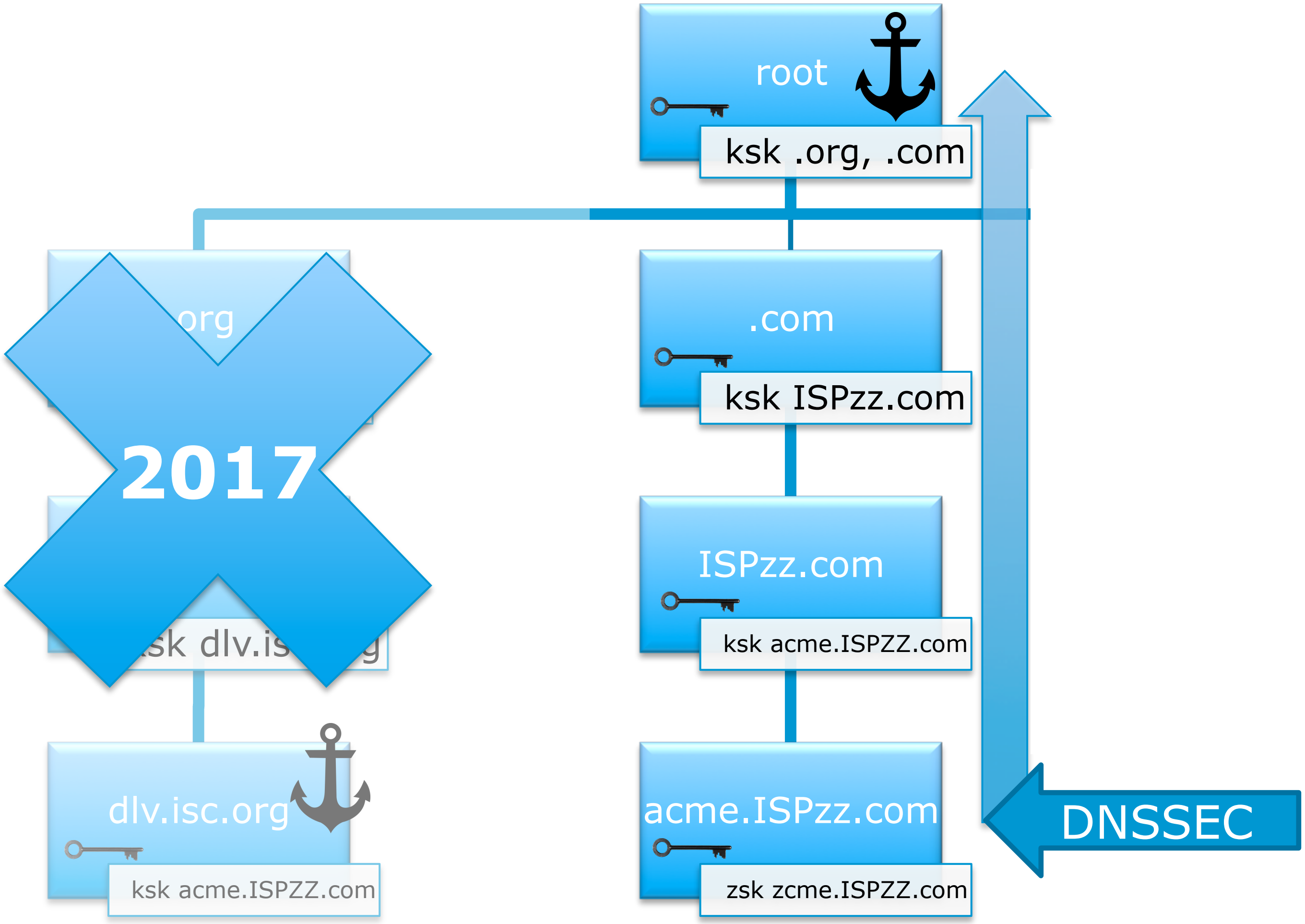
dlv.ord.sns-pb.isc.org.
ns2.isc.ultradns.net.
dlv.sfba.sns-pb.isc.org.
ns.isc.afilias-nst.info.
dlv.ams.sns-pb.isc.org.
ns1.isc.ultradns.net

- 5,000 – 10,000 queries per second (to ISC, we have no data from Afilias or Neustar)
- Failure to find this zone will adversely impact resolvers looking for it
- Leave this up as long as it is getting queries

Communications Plan

- Discuss with participants at ICANN, DNS-OARC/RIPE, operator meetings
  - Email to DNS tech discussion lists
- Notify current DLV users
- Contact DNSSEC docs publishers
- Discuss with validating resolver publishers (incl OS packagers)

Goal: DNSSEC Validation



vicky@isc.org

Balaji.D