

Sunset for the DLV?



DNSSEC Look-aside Validation = alternate path to trust anchor

root

- .org

- isc.org

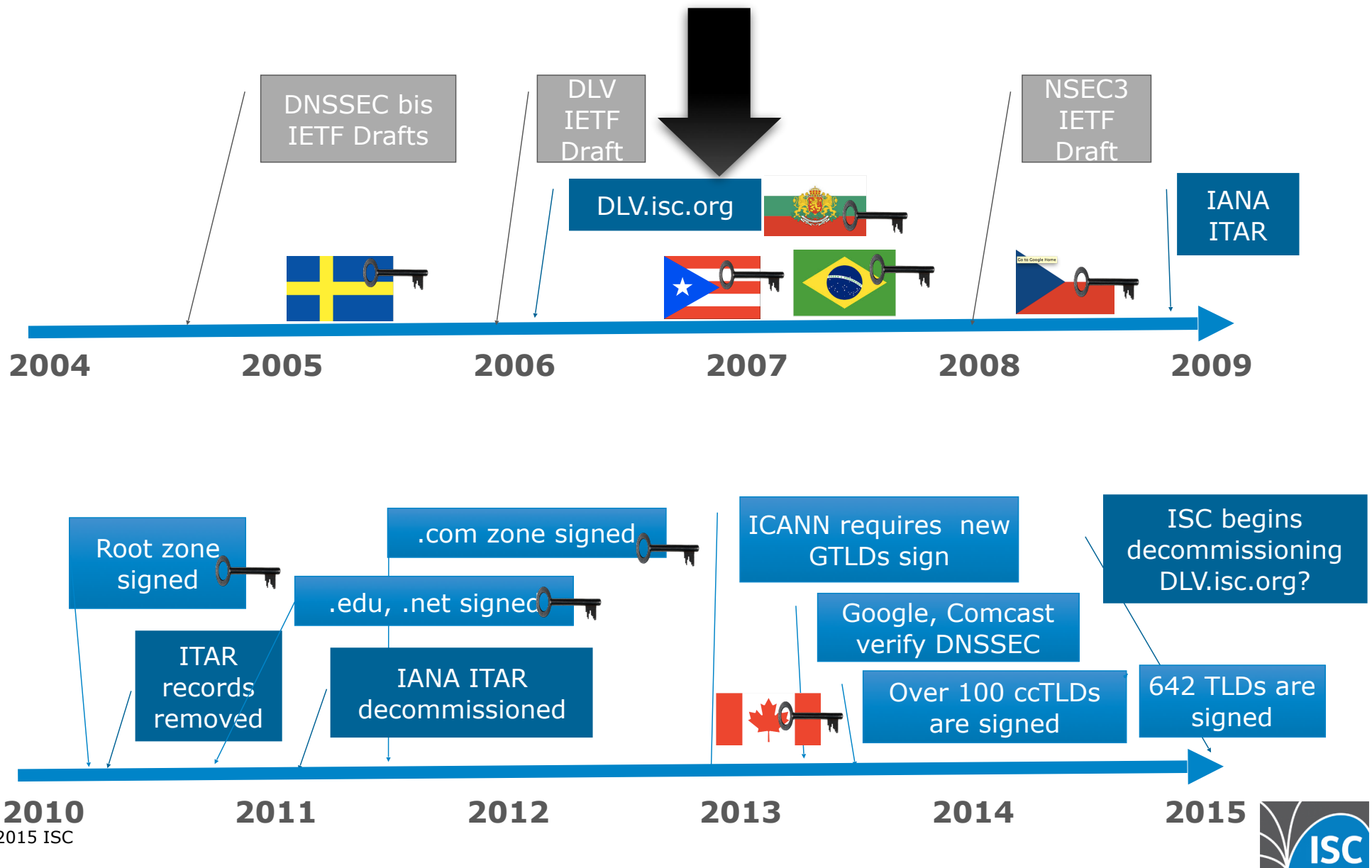


Validate

- alv.isc.

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

A lot has changed since 2006



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



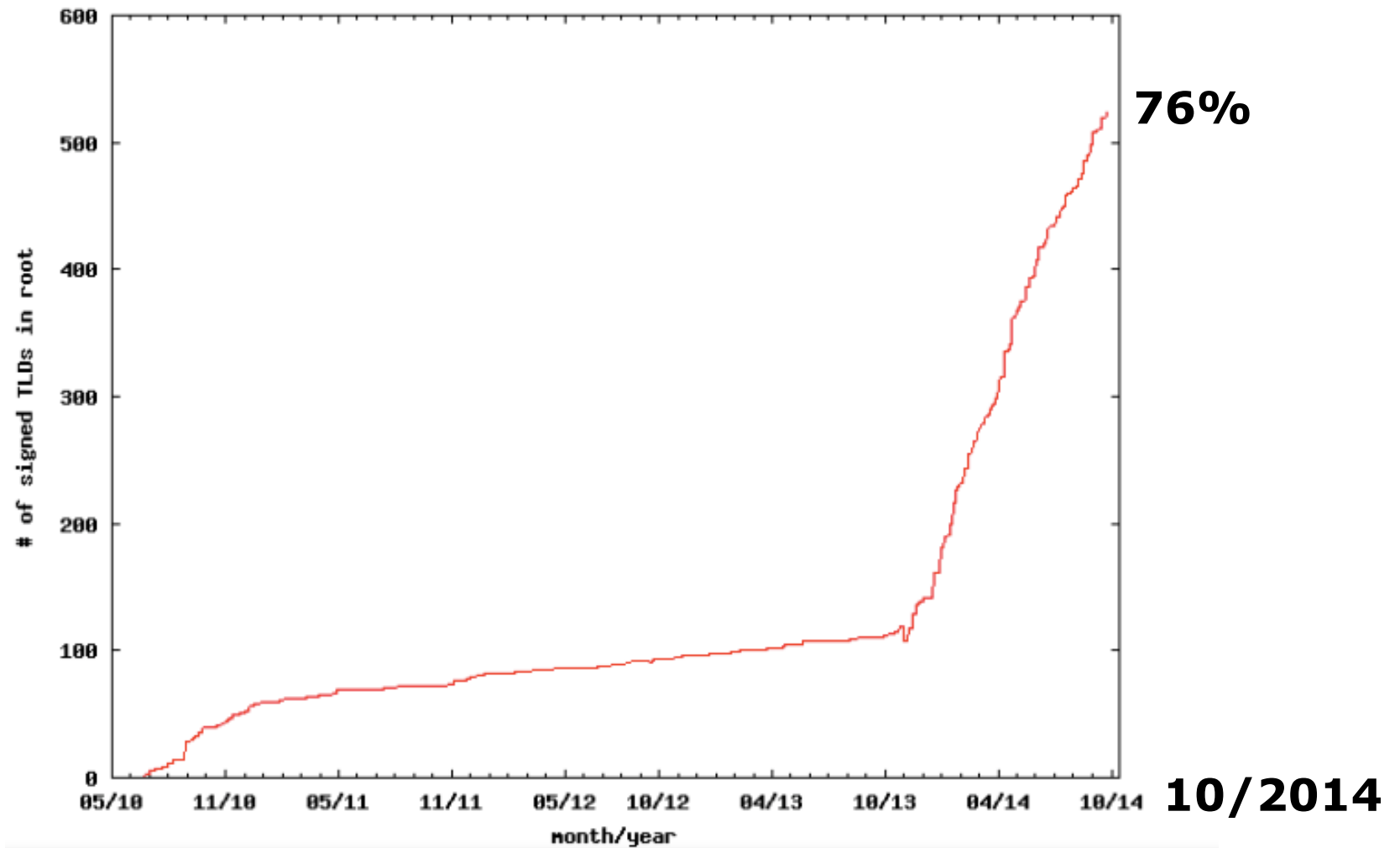
Disadvantages

- 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 parents)
- Entities that **Registrars that don't accept DS records.**

DNSSEC Deployed on 586 out of 771 TLDs



Registrar Support

- Registrar support for DS records is available but not universal
 - The 2013 ICANN Registrar Accreditation Agreement requires support
- 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
 - Remaining gap with registrar transitions

1st Step = Clean Up the Zones

4568 zones configured

- 2867 fully configured/working zones
 - only 397 are in an unsigned parent
- ~20% fully validate from the root
- 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. If the zone already has DNSSEC records in the parent, and can be validated to the root outside of DLV.
2. 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.

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)

2015

2016

2017

Goal: DNSSEC Validation





dlv@isc.org

Balaji.D