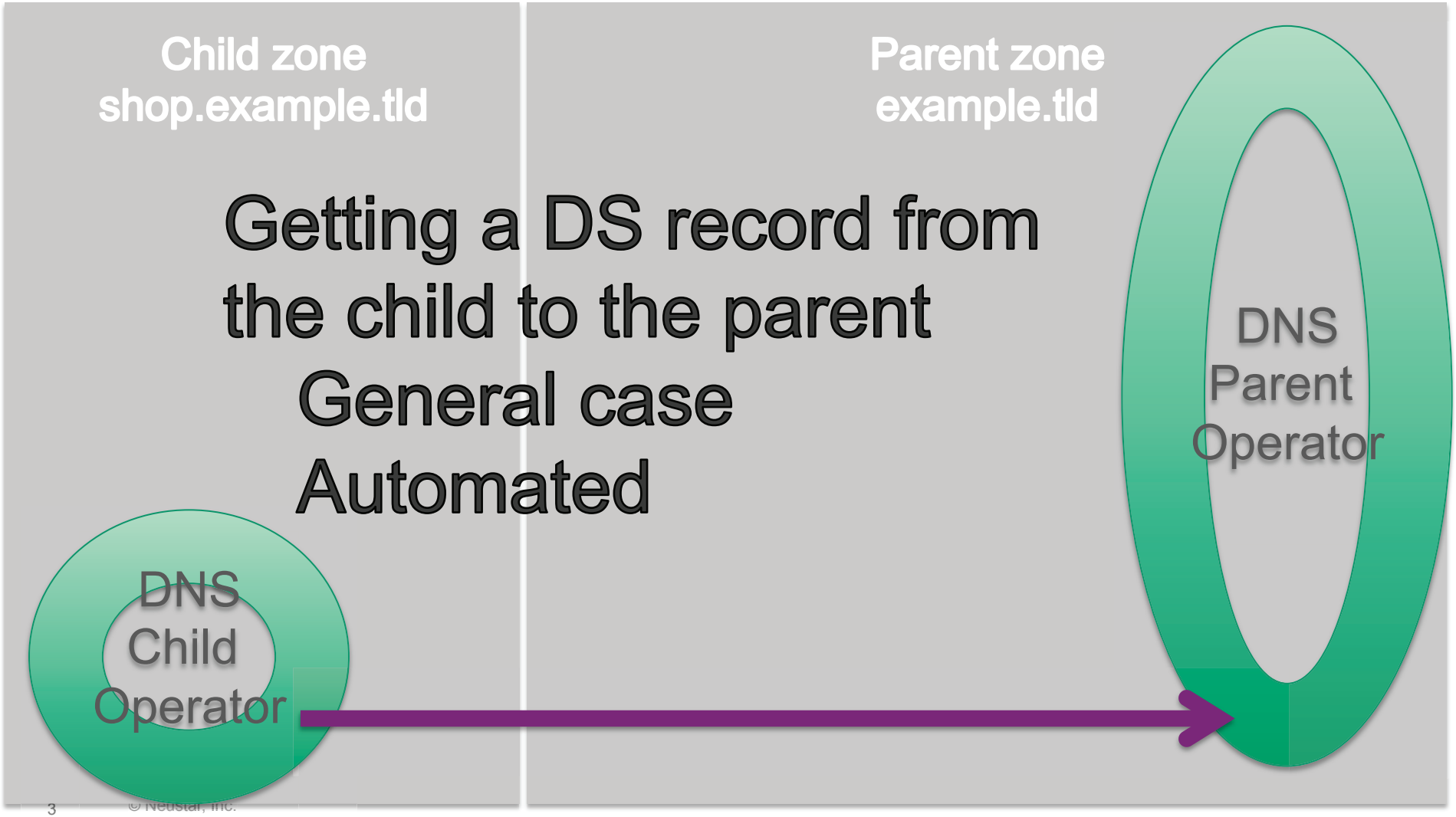
An DNSSEC Operational Gap

Edward Lewis
ed.lewis@neustar.biz
DNSSEC Workshop @ ICANN 46
April 10, 2013

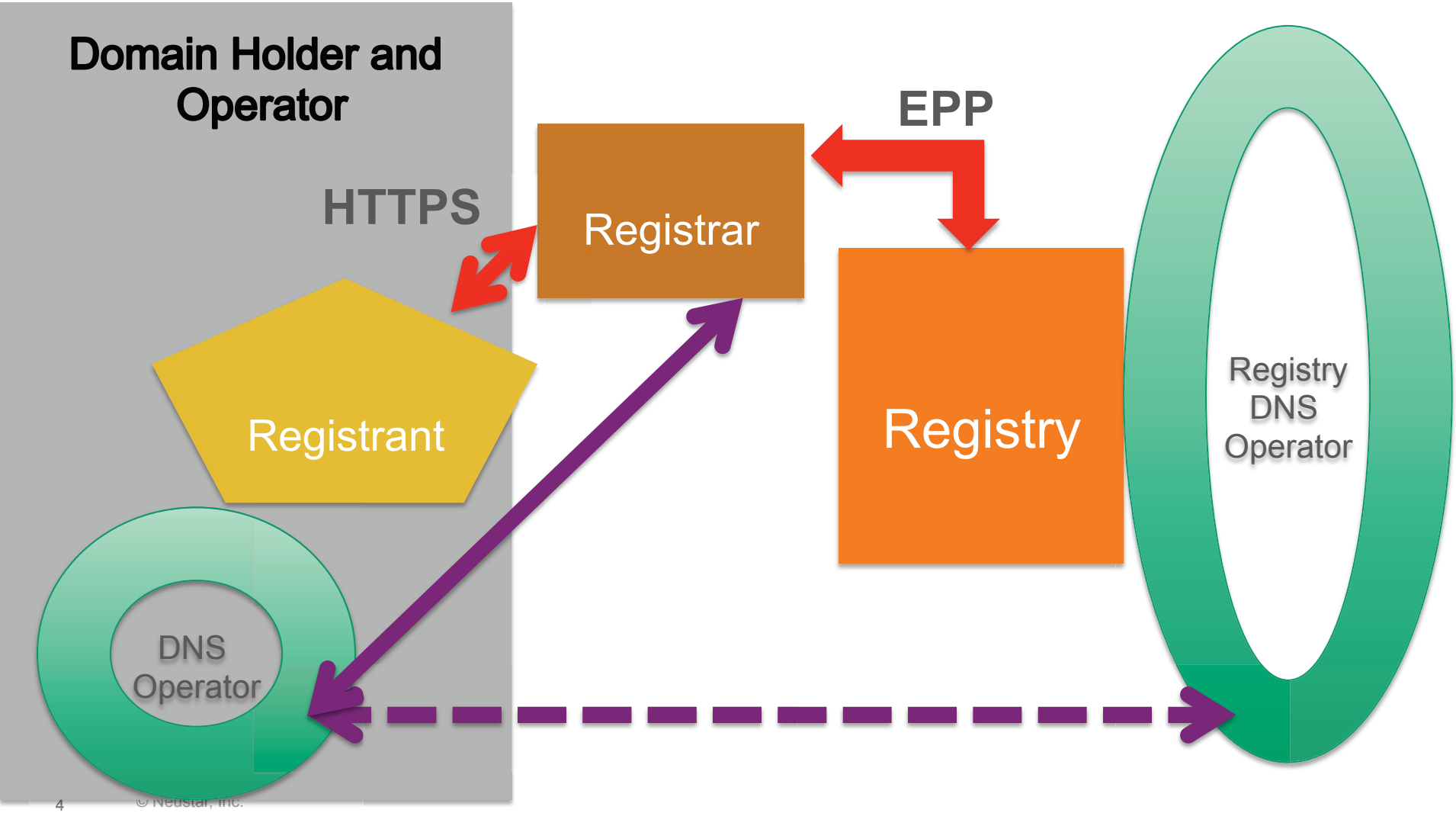
Background

- When a zone “goes DNSSEC” it is signed
- One key is a “special”
- To make DNSSEC “work” this key has to appear as a DS record in the zone above
  - Child to Parent
- Today we accomplish this manually
  - EPP helps but does not solve the whole problem
  - Web form “cut and paste” is used – yuck!
- A general solution is needed
  - The good news, this is now getting attention

A Problem Not Yet Solved

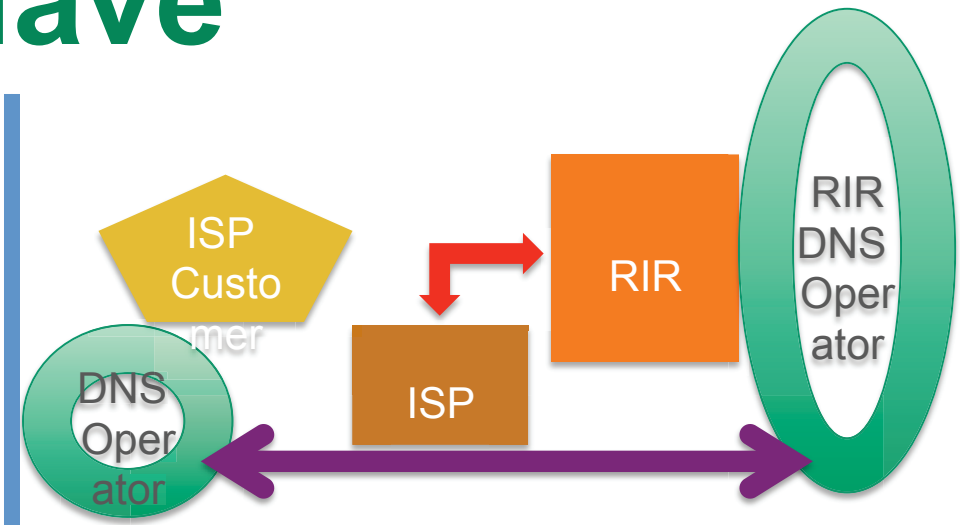


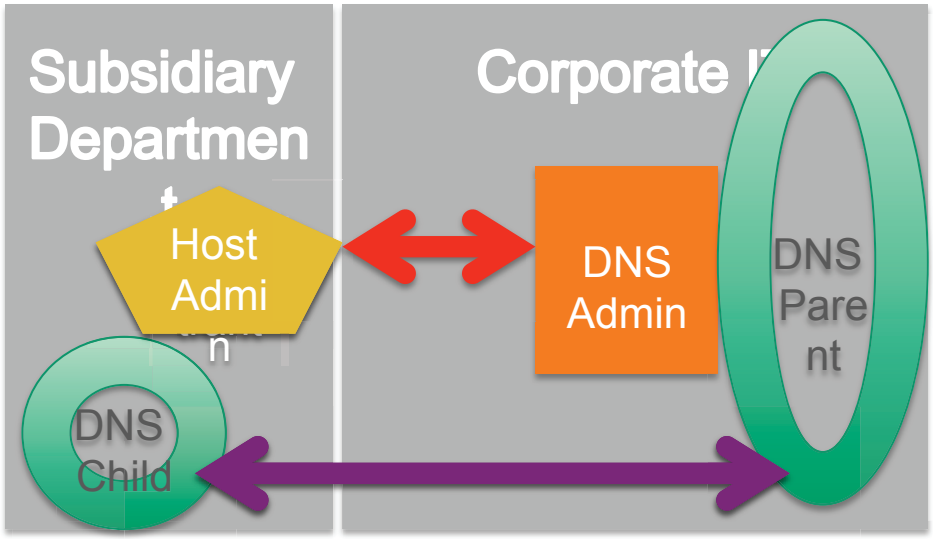
We've Created Business Rules

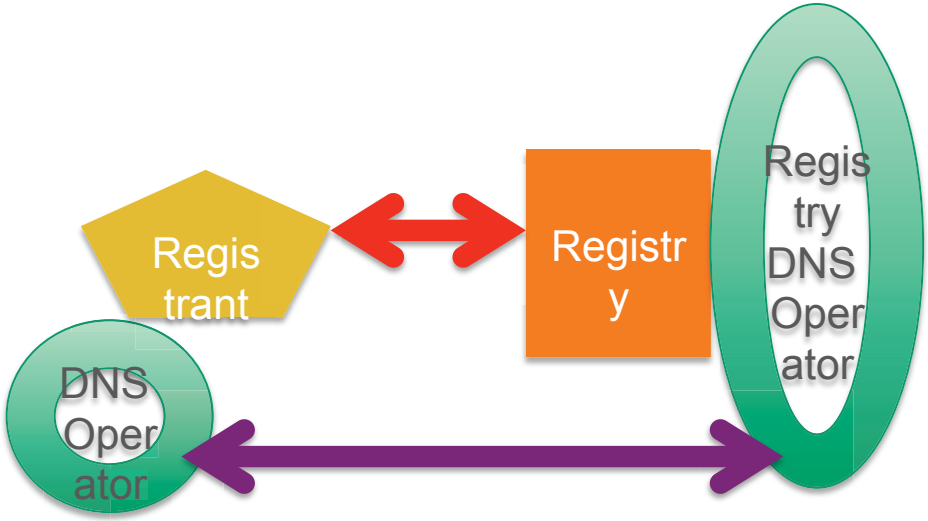


But We Also Have

- RIR, LIR Environment
- Non-Registrar Environment
- Enterprise internal
- . . . and others







And Even More Use Cases

- There are more environments
- And there are transfer considerations too
  - Transfer of operator
  - Transfer of registrar
- Too many to list in 10 minutes
  - And not all that interesting to a general audience

User's Motivation

- There's no standard, "business normal" way to move this data
  - Cut and Paste into Web Pages (Portals)
  - Or into email templates
- There are no tools that make this easy
  - Because tool makers don't have a standard, interoperable way to move this data
- The result is that DNSSEC remains "hard"
  - Even if this transfer is rare (maybe once/year or less), rarity means it'll be forgotten

DNS Operator's Goal

- Universal, interoperable standard
  - Registries of all kinds have different operational interfaces
  - Some have EPP environments, but not all
  - An operator may have zones in many TLDs and many non-TLDs
  - Common approach is needed, starting with a building block building towards the different policy environments

TLD Concerns

- Have to do this within business rules
- (Many) gTLDs cannot have direct contact with registrant operators
- Some TLDs want to work on DNSKEY and not DS material

- But TLDs are not the only DNS parent out there
  - Just the most visible, especially in an ICANN venue

Is This a Deployment Gate?

- Having a solution to this would make it much easier to make DNSSEC “work”
  - Today signing and publishing a zone is not hard
  - Today validation is not too hard
- Most DNSSEC “false positives” have come from failures in getting a DS record to the parent in a timely fashion
  - Making the problem a factor in “why not” validate
- Without the chain of trust that the DS record creates
  - DNSSEC does not have enough value to overcome the cost
- So, this is one gate (perhaps not the *only* one)

Recent Activity

- IETF 86, last month in Orlando, Florida, US
  - The DNSOP WG saw a draft resuming work on this topic
  - The “CDS” proposal
  - Very early stage at this point

  - https://datatracker.ietf.org/doc/draft-kumari-ogud-dnsop-cds/

- Still in the discussion phase, needs more work