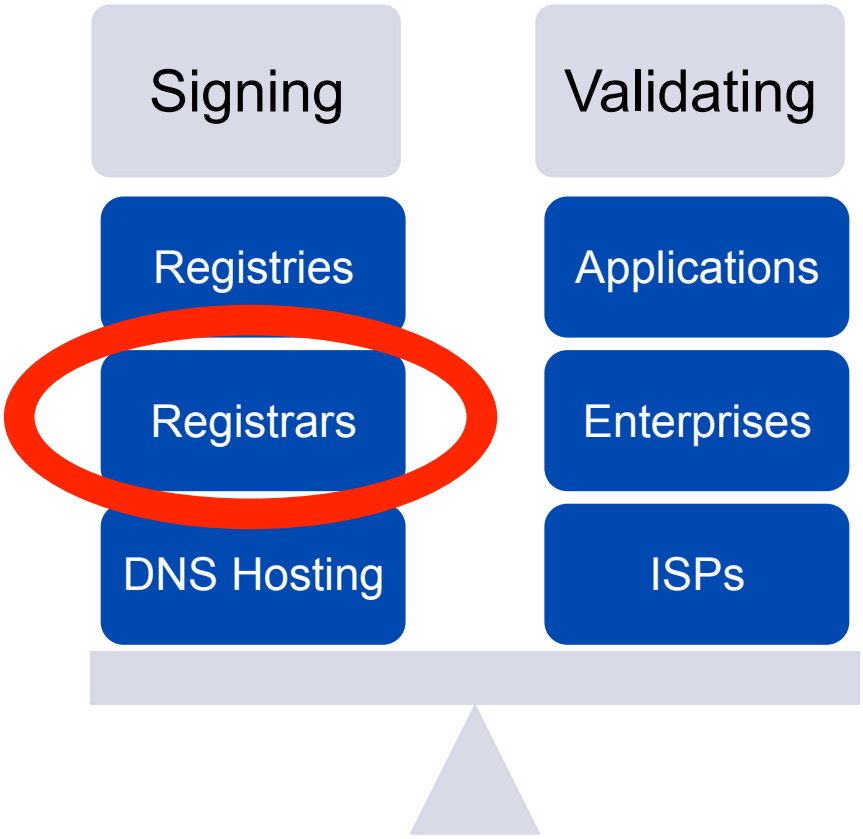
DNSSEC Obligations in the 2013 Registrar Accreditation Agreement (RAA)

Dan York, Internet Society

ICANN 49 DNSSEC Workshop
26 March 2014

The Two Parts of DNSSEC



Internet Society™

Registrars and DNSSEC - RAA

- **2013 ICANN Registrar Accreditation Agreement (RAA) has section on DNSSEC**
  - Specifically the "Additional Registrar Operations Specification"
  - http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm#operation
  - Covers:
    - DNSSEC
    - IPv6
    - IDNs
- **2013 RAA required for registrars to work with newgTLDs**

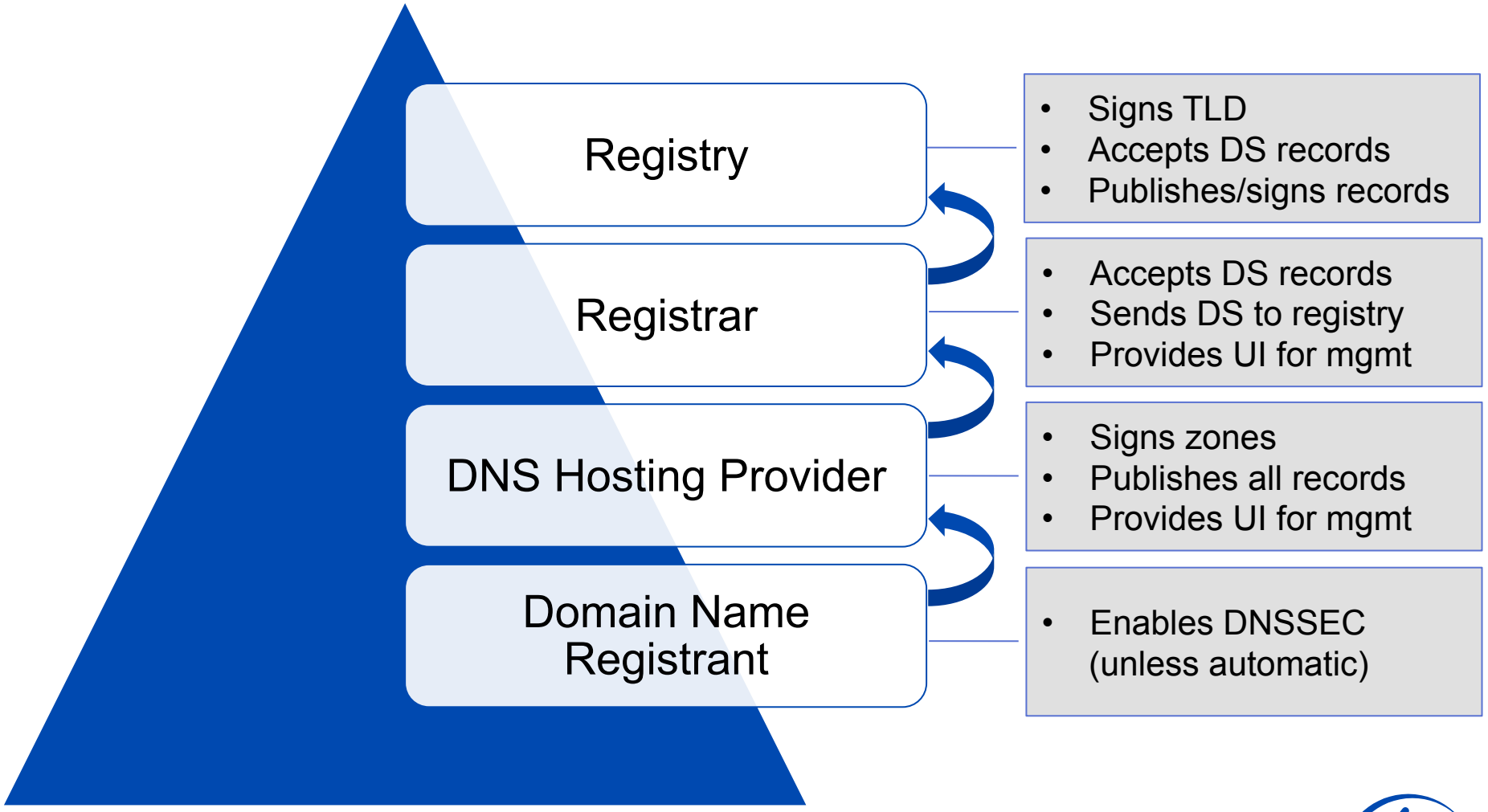
Registrars and DNSSEC - RAA

New specification states:

1. DNSSEC

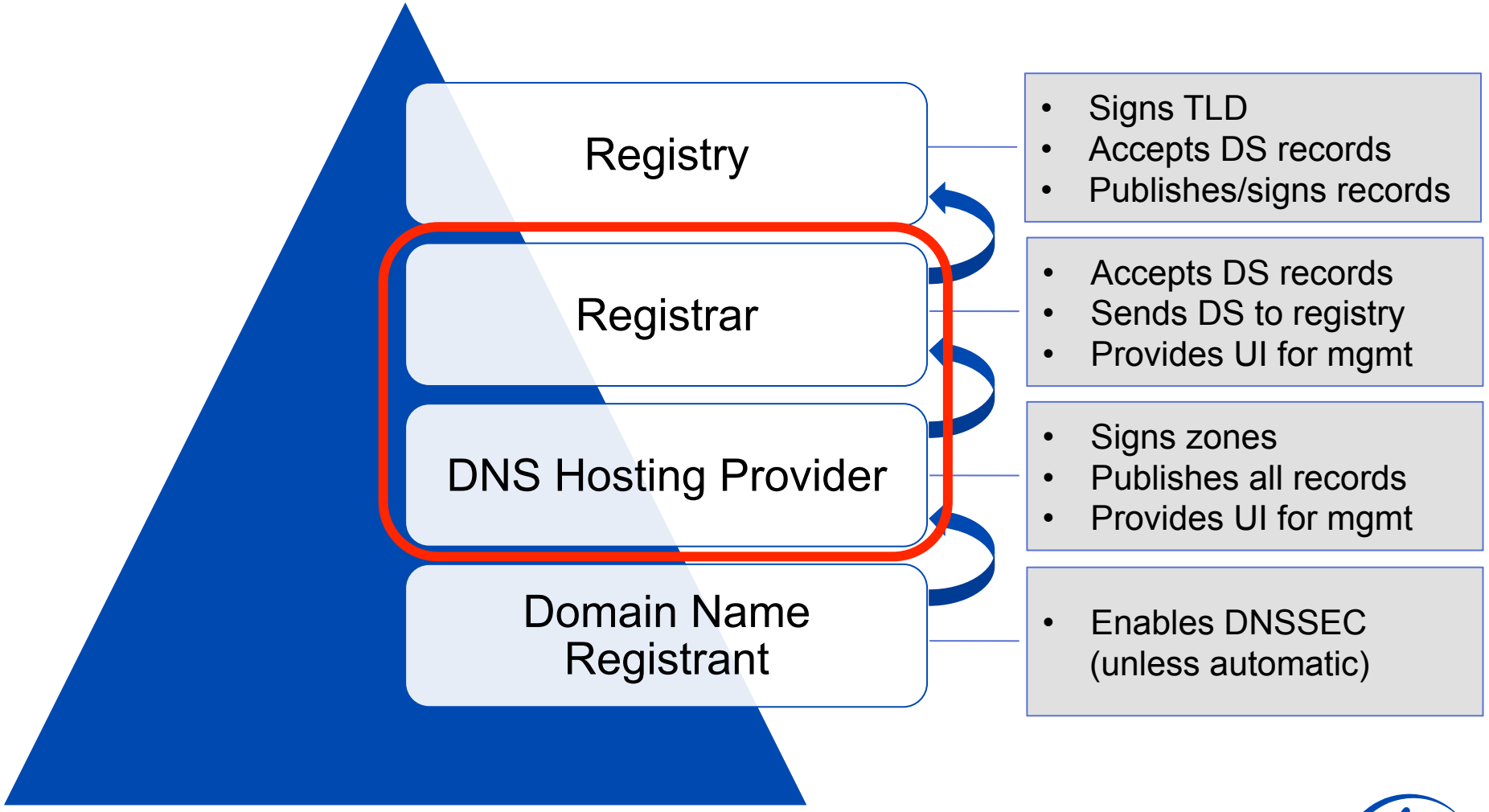
Registrar must allow its customers to use DNSSEC upon request by relaying orders to add, remove or change public key material (e.g., DNSKEY or DS resource records) on behalf of customers to the Registries that support DNSSEC. Such requests shall be accepted and processed in a secure manner and according to industry best practices. Registrars shall accept any public key algorithm and digest type that is supported by the TLD of interest and appears in the registries posted at: <http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml> and <http://www.iana.org/assignments/ds-rr-types/ds-rr-types.xml>. All such requests shall be transmitted to registries using the EPP extensions specified in RFC 5910 or its successors.

DNSSEC Signing - The Individual Steps



Internet Society™

DNSSEC Signing - Registrar Providing Hosting

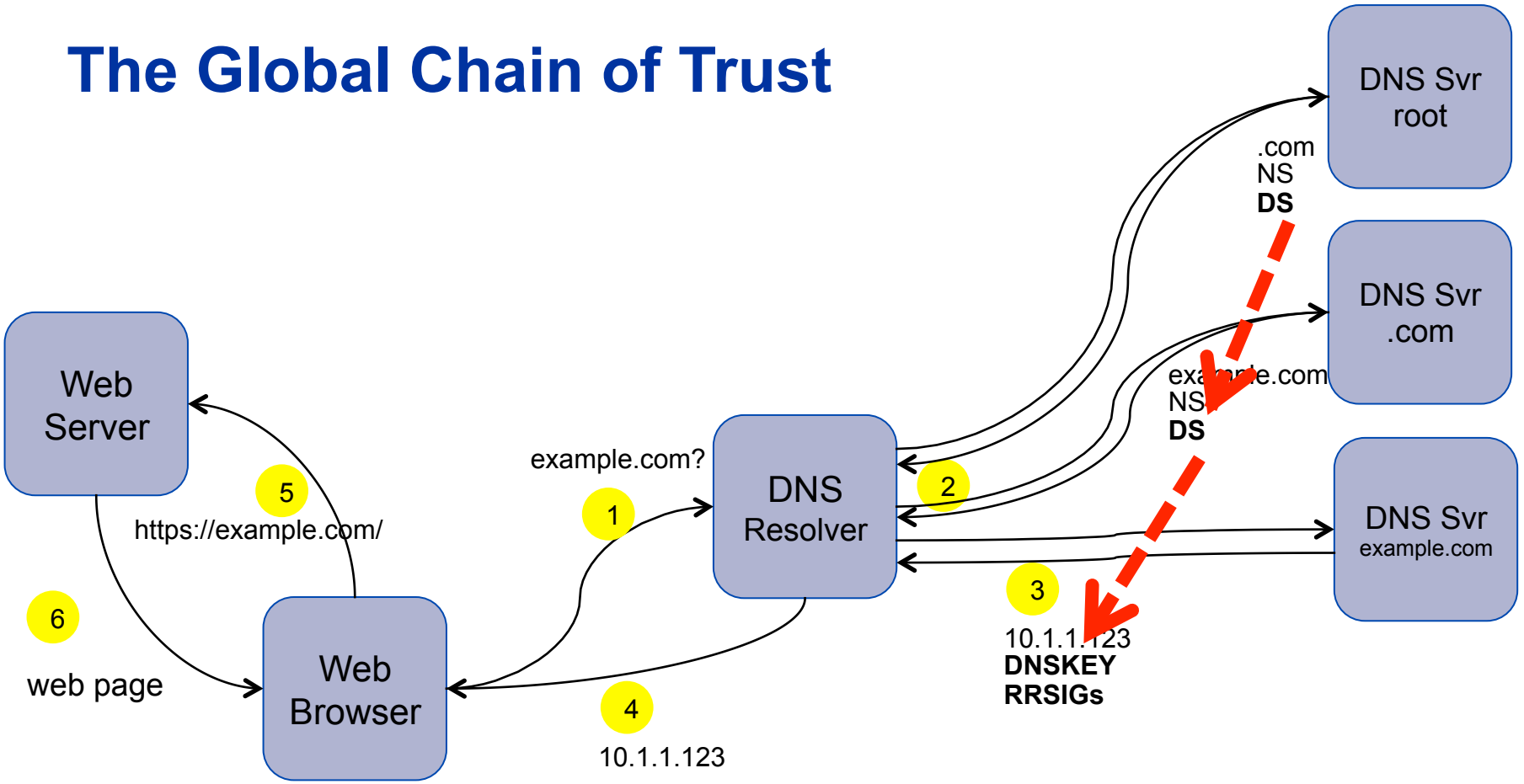


Internet Society™

Registrar's Critical Role

- **By passing the DS or DNSKEY record up to the TLD registry, registrars ensure the "global chain of trust" is intact.**

The Global Chain of Trust



Internet Society™

What the 2013 RAA Requires

- **Registrar must allow its customers to use DNSSEC**
  - Add
  - Change
  - Remove
- **Registrar needs some mechanism to accept DNSSEC records (DNSKEY or DS records) from customer**
- **Registrar must communicate those DNSKEY/DS records to TLD registry using EPP extensions defined in RFC 5910**

What the 2013 RAA Does NOT Require

- **If registrar also provides DNS hosting, it is *not* required to perform DNSSEC-signing of hosted domains (although your customers will benefit if you do)**

- **Registrar is not required to sign own domains (although you can show leadership by doing so)**

Steps To Get Started

1. Learn more about DNSSEC and what it offers

2. Identify how you can provide a user interface for registrants to communicate DNSSEC records (either DS or DNSKEY)

3. Identify how you can communicate to TLD registries using appropriate RFC 5910 EPP extensions

4. Implement steps 2 and 3

5. Consider signing your own domain(s) and offering DNSSEC signing if you provide DNS hosting

Additional Points

- **Secure transfer of a DNSSEC-signed domain still not fully defined. One proposed EPP extension:**
  - http://tools.ietf.org/html/draft-ietf-eppext-keyrelay

- **TLD registries have different requirements for EPP extensions.**

- **Some TLD registries ask for DS record while others ask for DNSKEY record.**

Resources

- **Internet Society Deploy360 Programme:**
  - http://www.internetsociety.org/deploy360/home/registrars/
  - http://www.internetsociety.org/deploy360/dnssec/

- **ICANN Registrar Stakeholder Group**
  - http://icannregistrars.org/

- **Universal Registry/Registrar Toolkit**
  - http://sourceforge.net/projects/epp-rtk/

Dan York

Senior Content Strategist
Internet Society

york@isoc.org

Thank You!