DNS / DNSSEC / DANE / DPRIVE @ IETF 95 Hackathon

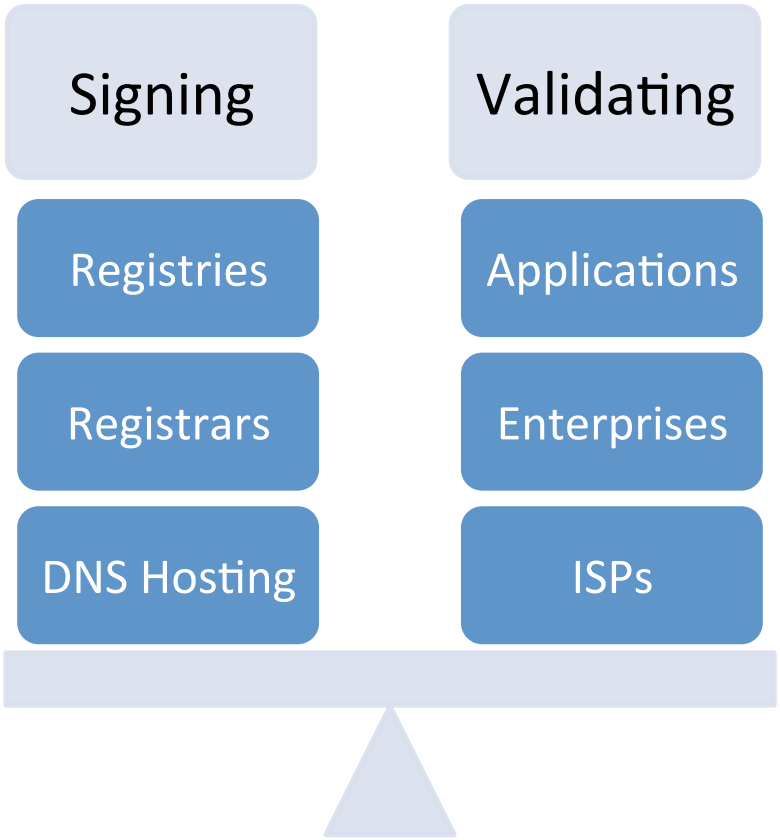
April 2-3
Buenos Aires,
Argentina

https://www.flickr.com/photos/chrissam42/3989126075/

Answering 4 Questions

- **How can you be sure the information you get *out* of DNS is the same info the domain operator put *in* to DNS?** (DNSSEC)
- **How do you know you are using the correct TLS certificate?** (DANE/DNSSEC)
- **How can you protect the *confidentiality* of your DNS queries from surveillance?** (DPRIVE)
- **How can make the overall DNS infrastructure more agile in order to be more secure?**

The Two Parts of DNSSEC



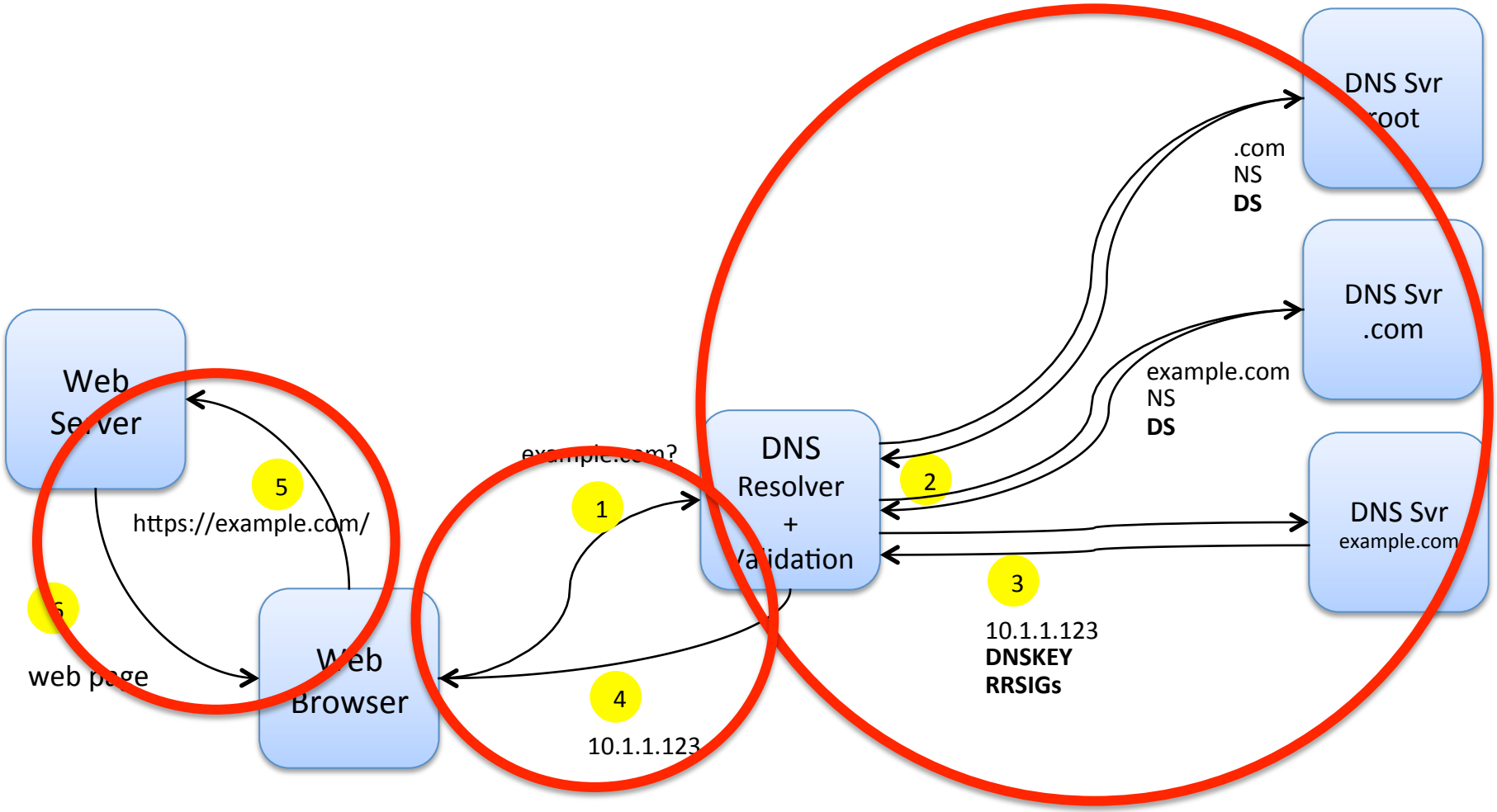
DANE

- RFC 6698
- Adds TLS certificate (fingerprint or entire cert) as a DNS record – and signs that with DNSSEC
- Apps can then verify via DNSSEC that this is correct cert (or CA) to use
- Being used now between email servers, XMPP servers, plugins for browsers
- Concept expanded to S/MIME certs, OpenPGP

DNS PRIVate Exchange (DPRIVE)

- Protecting the **confidentiality** of DNS queries
- https://datatracker.ietf.org/wg/dprive/charter/
- Focused on communication between DNS clients (i.e. stub resolvers) and DNS iterative resolvers
- Solutions include sending DNS queries over TLS or DTLS

Summary – What We Are Working On



TRUST IN TLS - DANE **CONFIDENTIALITY - DPRIVE** **INTEGRITY – DNSSEC**

IETF 95Hackathon Ideas

- Library-independent interfacing with TLS
- NSSWITCH getdns
- EDNS0 chain query
- DNSSEC cyber-ledger (TRANS WG)
- getdns version for mbed/Raspbian
- security testing of getDNS library
- automated DNSSEC key maintenance/rollover scheduling tool for BIND
- auto-update for DNS software
- documentation and text updates
- And more...

Join Us!

- **Help us make DNS (and the Internet) more secure and private!**

- Champions:
  - Dan York, Internet Society york@isoc.org
  - Allison Mankin, Verisign Labs amankin@verisign.com
  - Benno Overeinder, NLnet Labs benno@nlnetlabs.nl
  - Sara Dickinson, Sinodun sara@sinodun.com
  - John Dickinson
  - Willem Toorop
  - Linus Nordberg
  - Jan Včelák
  - Evan Hunt