Deploying DNSSEC in the .CA Registry

Buenos Aires, Argentina

Canadian Internet Registration Authority (CIRA)

Stuart Olmstead-Wilcox

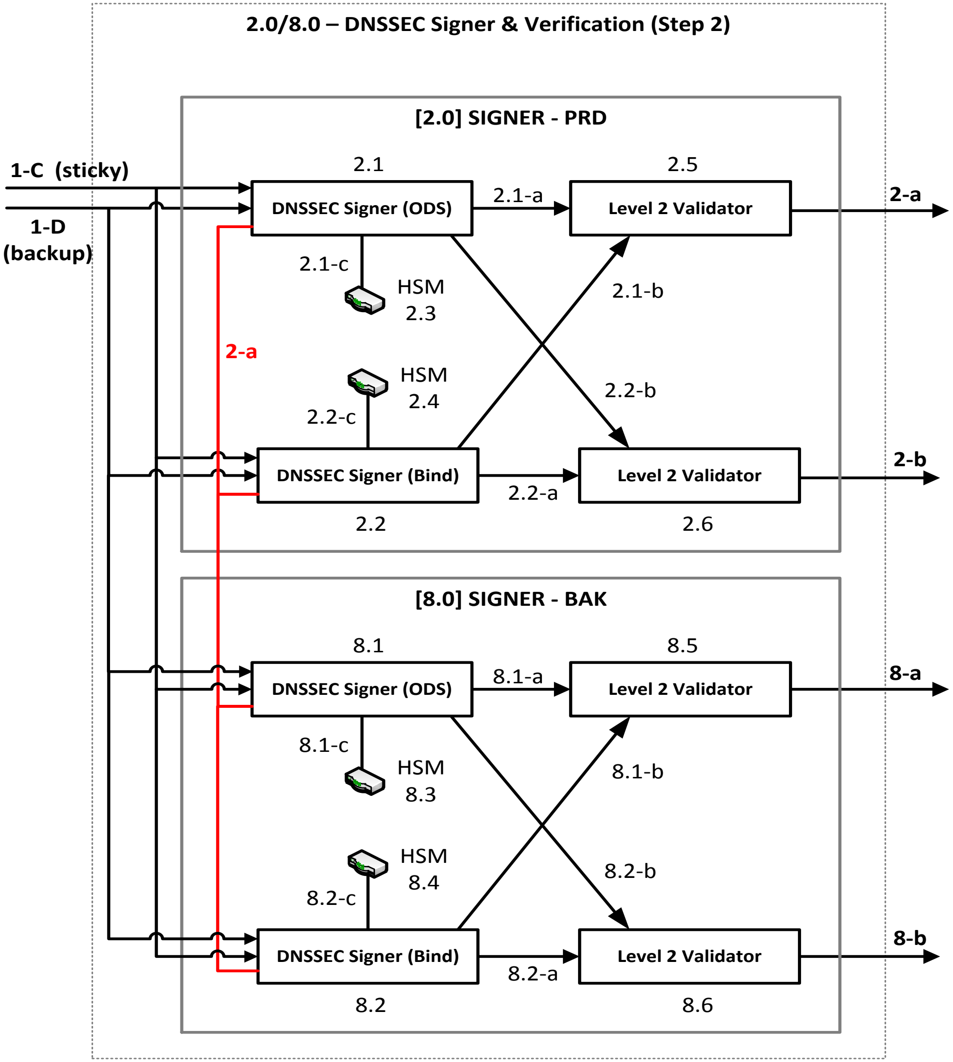
DNSSEC @ .CA

DNSSEC is a multi phase project

- Phase 1 – Sign .CA (completed January 2013)
  - Dual in-line signer – works great!
- Phase 2 – Implement DNSSEC support in the .CA registry
  - Current work in progress, planned for March 2014
- Phase 3 – Promote adoption of DNSSEC in Canada
  - .CA registrars, Internet service providers, enterprise
  - April 2014 and on-going

DNSSEC Signer & Validation

- Dual online signer sets located in different locations
  - Sign with Bind & OpenDNSSEC
  - Signed zone file validation
  - DR site always up to date
- Resilient solution
  - 9 months in production
  - 8 ZSK rollover
- 80 signed domains 🔑



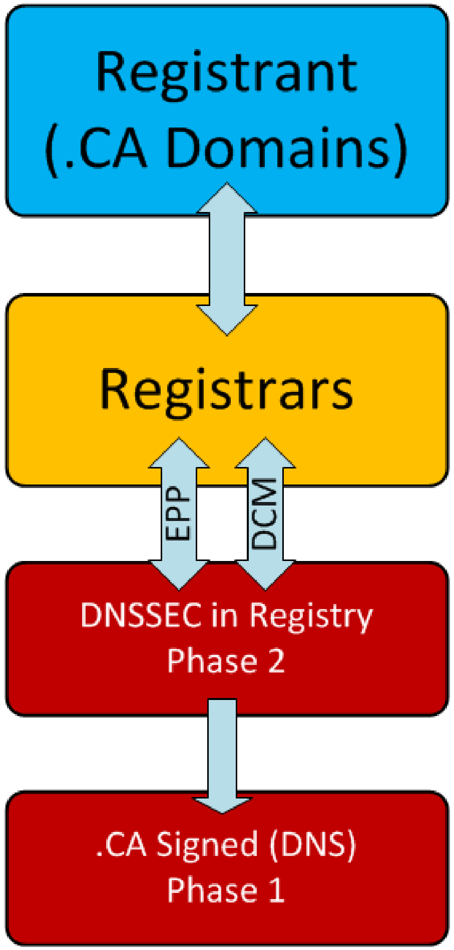
DNSSEC in the .CA Registry

- Primary objectives:

Keep it simple for Registrars to work with .CA

DNSSEC in the .CA Registry

- Accepting DNSSEC material from Registrants via the Registrars into the registry for inclusion in .CA zone file
- EPP extensions for DNSSEC are defined in RFC5910.
- **Not re-inventing the wheel. Implementing predefined EPP standards**



CIRA’s Implementation of DNSSEC

RFC5910 Support DNSKEY and DS Interface

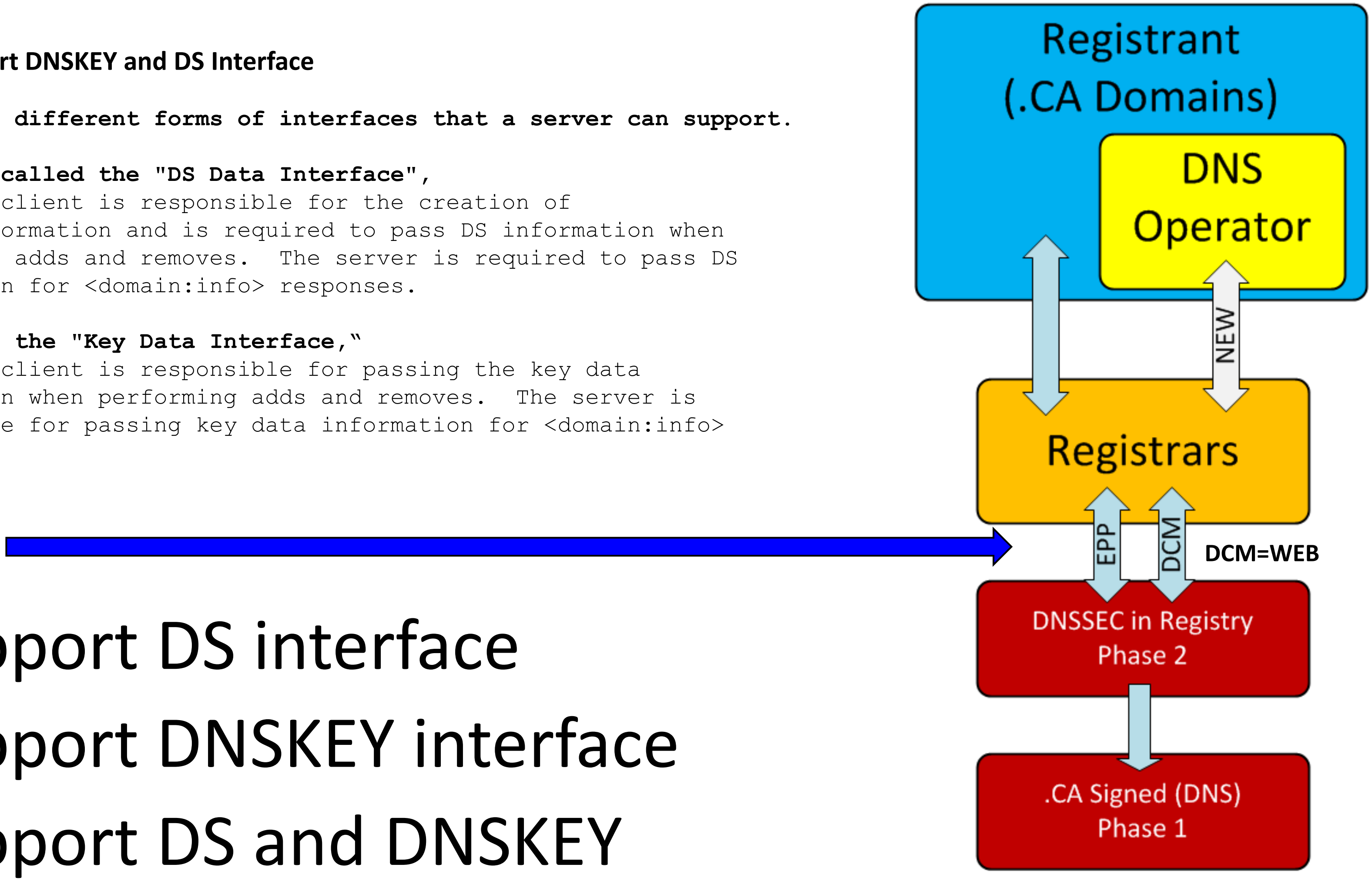
There are two different forms of interfaces that a server can support.

The first is called the "DS Data Interface", where the client is responsible for the creation of the DS information and is required to pass DS information when performing adds and removes. The server is required to pass DS information for <domain:info> responses.

The second is the "Key Data Interface,“ where the client is responsible for passing the key data information when performing adds and removes. The server is responsible for passing key data information for <domain:info> responses.

CIRA

- Support DS interface
- Support DNSKEY interface
- Support DS and DNSKEY



Some DNSSEC Parameters

- secDNS-1.1.xsd – RFC-5910
- Store a maximum of 6 DS and/or DNSKEY
- Support of all 11 algorithms identified as valid Zone Signing algorithms (DSA, RSA, GOST, ECDSA, etc…)
- Support of 4 algorithms when accepting DS data records (SHA-1/256/384, GOST R 34.11-94)
- When CIRA is given a DNSKEY record and generates the DS record, digest algorithm SHA-1 will be used.
- When given a DNSKEY and DS record, CIRA generates second DS from DNSKEY using indicated digest type and validates that it matches provided DS.
- Optional <secDNS:maxSigLife> element NOT supported
- Optional attribute urgent NOT supported.
- Whois will show the DNSSEC status (signed/unsigned)

Some DNSSEC points

- Adhering to only accepting DS (or DS and DNSKEY) OR DNSKEY on add, but not both. If DS AND DNSKEY are given on add, will fail.

- On update, will accept the addition of DS (or DS and DNSKEY) OR DNSKEY records even if previously added data was the opposite.

- If a DNSKEY is removed, all DS records linked to that key are removed as well.

- If a DS record which has an associated DNSKEY is removed – and it was the last DS record linked to the key, then the DNSKEY record is removed as well.

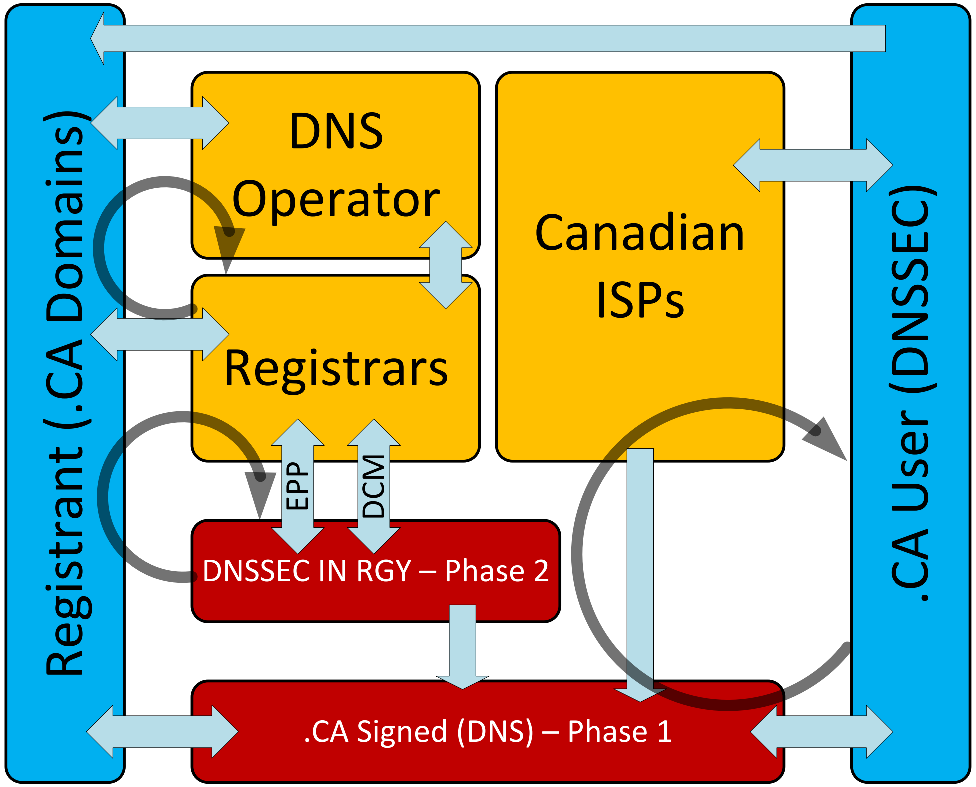
DNSSEC – Canadian Adoption

DNSSEC Strategy:

- Develop value proposition
- Document end user benefits
- Identify operational impacts
- Provide DNSSEC technology awareness and education

To Canadian:

- Registrars
- Registrants
- ISPs / DNS Operator
- .CA Internet Users
- Enterprise/Governments



Questions

- If you want our DNSSEC Registrar specifications document, let me know, 40 pages of good stuff.
- Please contact us @ CIRA if you have any questions

cira-dnssec@cira.ca