2013 RAA & DNSSEC

Rob Villeneuve

CEO, Registrar Group, Momentous.com

CIRA (.CA) Board Member

rob.villeneuve@momentous.com

ca.linkedin.com/robvilleneuve

2013 RAA

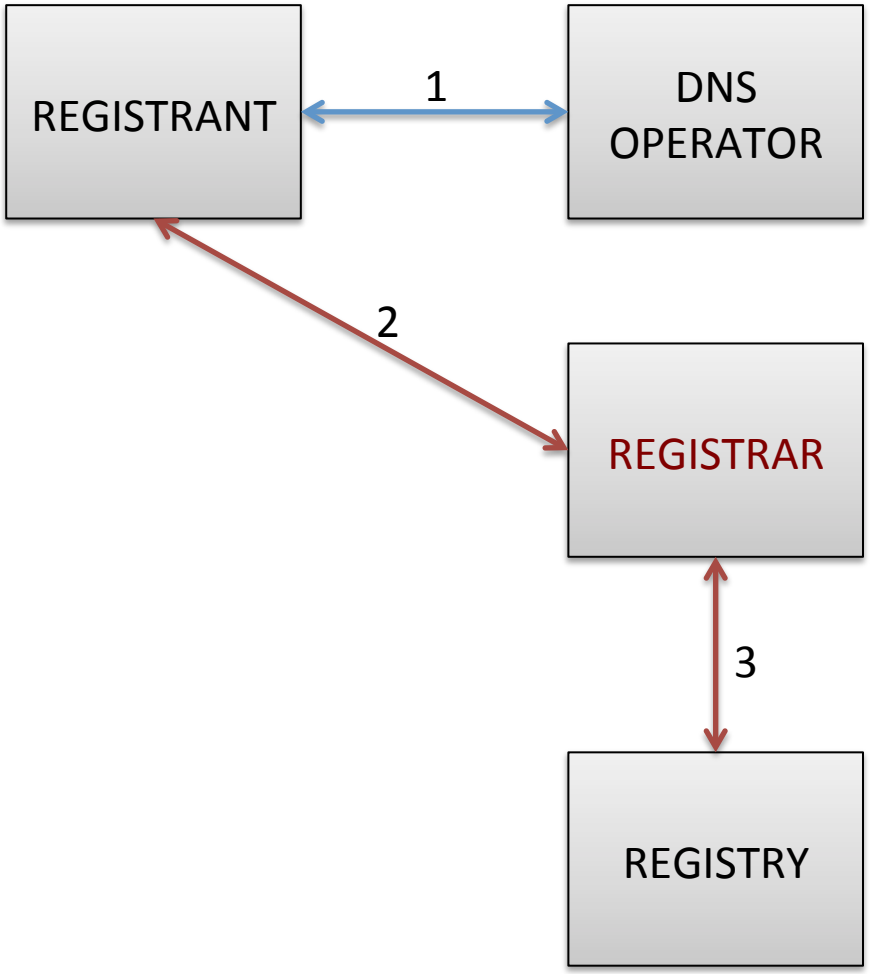
- Registrar Accreditation Agreement
- Contract between ICANN and each Registrar
- Optional for registrars to update to 2013 RAA
- 2013 RAA is required for new gTLDs.
- January 1st, 2014 implementation deadline

DNSSEC in the 2013 RAA

Section 3.19 - 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.

http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm#operation

DNSSEC Setup - Roles



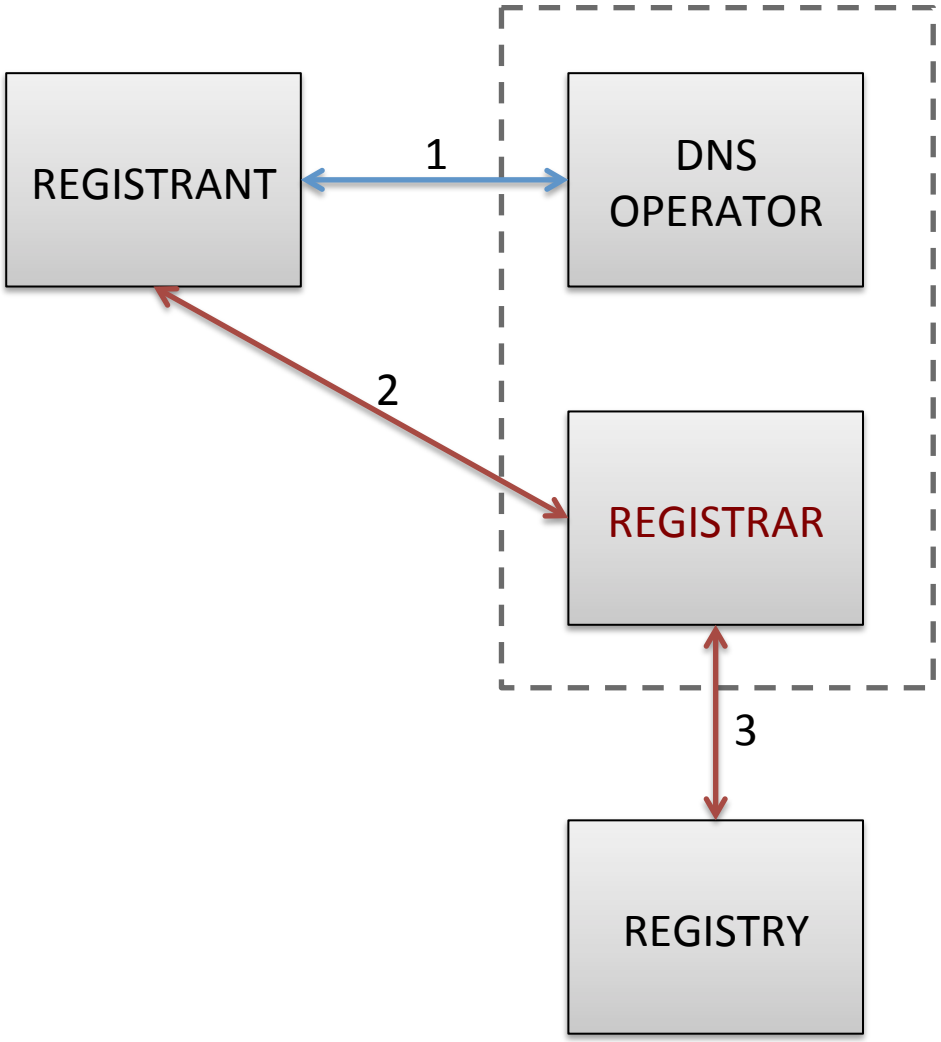
1: Registrant works with DNS Operator to configure DNSSEC. DNS Operator provides Registrant with public key details. (DS/ DSKEY).

2: Registrant provides Registrar with DSKEY/DS modifications.

3: Registrar updates DS/DSKEY information at registry via EPP.

RAA Applies to steps 2 & 3.

DNSSEC Setup - Roles



1: Registrant works with DNS Operator to configure DNSSEC. DNS Operator provides Registrant with public key details. (DS/ DSKEY).

2: Registrant provides Registrar with DSKEY/DS modifications.

3: Registrar updates DS/DSKEY information at registry via EPP.

RAA Applies to steps 2 & 3.

Registrar Obligations

- Allow customer to create & modify a domain's DS and/or DNSKEY records at registry via EPP.
- Security, Authentication, Authorization.
- Why EPP? RARs can handle infrequent or complex requests manually.

Other considerations

- WHOIS DNSSEC field: Signed vs. Unsigned
- Domain Transfers (Inbound)
- Registry On-boarding
  - Custom DNSSEC EPP Implementation
  - Custom DNSSEC policies.
- Customer support & education.

Other Considerations

- DNSSEC for ccTLDs
- Implement DNSSEC for own domains.
- DNSSEC as DNS Operator

DNSSEC – EPP Tools

EPP – Registries are providing DNSSEC Extensions to their own toolkits and/or the RTK.

The Universal Registry/Registrar Toolkit (RTK)

http://sourceforge.net/projects/epp-rtk/

EPP Schema Definition version 1.1

http://www.iana.org/assignments/xml-registry/schema/secDNS-1.1.xsd

Resources

Registrar Stakeholder Group
http://icannregistrars.org/

RFC 5910
http://www.ietf.org/rfc/rfc5910.txt

https://www.iana.org/dnssec
https://www.arin.net/resources/dnssec/
http://www.dnssec-deployment.org/
http://www.dnssec.net/