DNSSEC Workshop

ICANN 45

Toronto, Canada

Canadian Internet Registration Authority (CIRA)

Jacques Latour

DNSSEC Status @ .ca

- We expect to have our zone signed

November 12, 2012

- Key signing ceremony: September 4, 2012
  - Went well !!!
  - CIRA DPS online
  - KSK, RSA, size: 2048 bits, length: 365 days
  - ZSK: RSA, site: 1024 bits, length: 30 days

http://www.cira.ca/assets/Documents/DNSSEC/CIRA-DPS-EN-0-Public-Final-v1-4.pdf

Why it took so long?

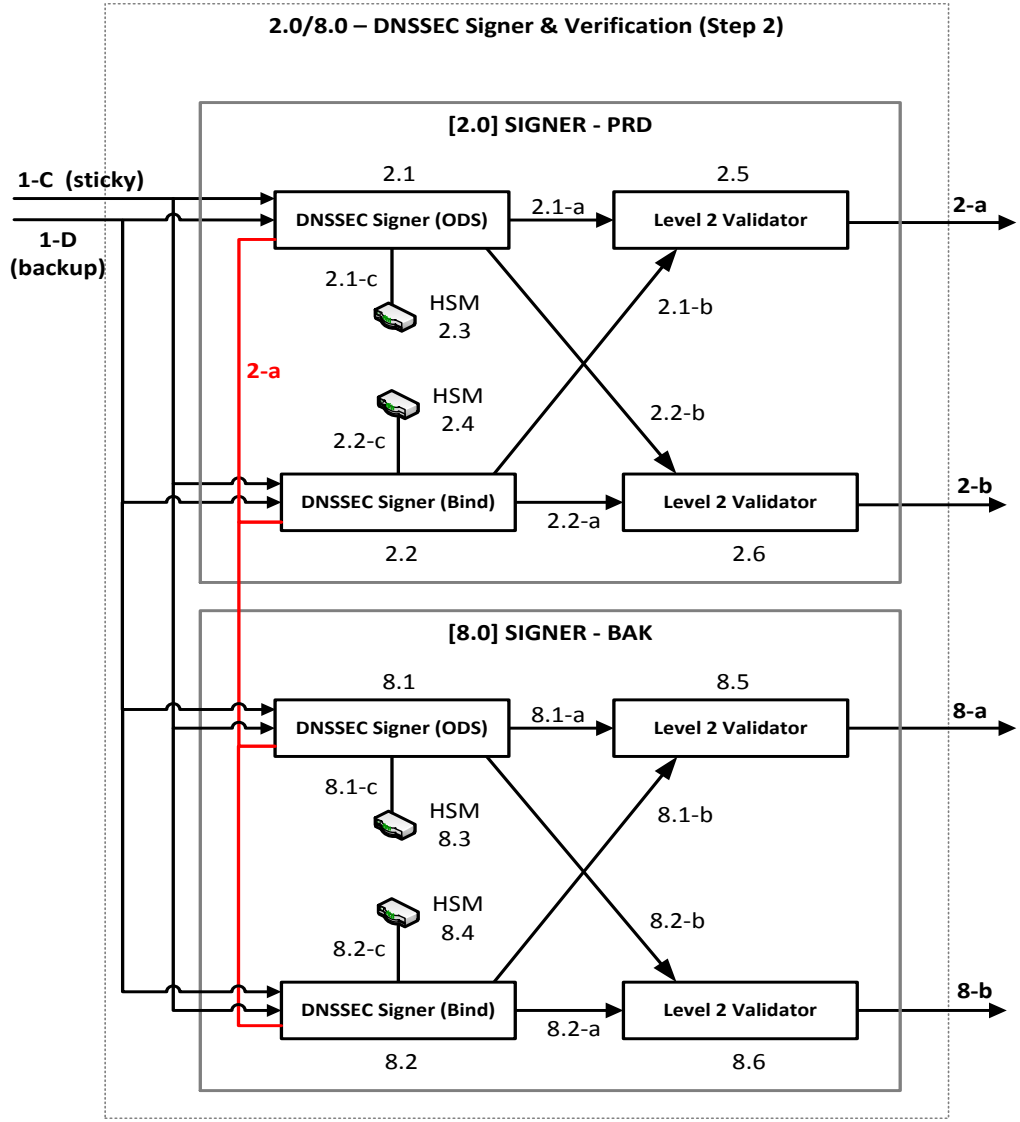
- We used a different approach to sign .ca
  - Risk adverse, high availability & resilient solution
- Dual Independent signing engines
  - We create two independent signed zones using Bind and OpenDNSSEC
- Comprehensive DNSSEC validation process
  - We perform multiple levels of zone file validation
  - If there's an issue with either signer or HSM, we stop
  - Hardest task, important because it is the only way to detect a signer engine implementation problem

Risk Adverse

- CIRA's solution took in account known DNSSEC related service impacting outages;
  - DNSSEC software issues
  - Key management issues
  - Implementation issues (infrastructure)
  - Operational issues

DNSSEC Signer & Validation

- Online signer sets located in different facilities/cities
- Worked closely with OpenDNSSEC team to make v1.4.0 functional for our production, although they recommend it's not for production use yet ☺
- Total of 4 AEP Keyper HSM on-line with key synchronizations



Our Validation Process

- **Level 1 Validation: (pre-signing)**
  - Check md5 sum – Verifies that .md5 checksum matches .zone contents
  - Check percent change – has the file size changed by more than $x percent (currently 1%)
  - Check file diff – has the contents of the file changed by more than $x lines (currently 15K lines)
  - named-checkzone – Verify 'named-checkzone' succeeds on the unsigned zone

- **Level 2 Validation: (post-signing, validation code independent from signers)**
  - Check md5 sum – Verifies that .md5 checksum matches .zone contents
  - ldns – Verify that the zone can be read into ldns-readzone with no errors (ldns-verify-zone in future)
  - Required files met – Requires the two independently signed zones to compare. If one is missing, signing set is marked bad.
  - Check dnskey – Verify that the KSK has not changed
  - validns – Validate all RRSIGs and the NSEC3 chain and on the two zones
  - Check rrsigs – validate signer engines - Zero out signature and timestamp data, signed zones should be identical
  - named-checkzone – Verify 'named-checkzone' succeeds on the signed zone

- **A corrupted or suspected zone will not be published**

Next Steps

- Support DNSSEC in the registry (2013)
- ISPs in Canada to resolve DNSSEC
- CIRA Registrar's to support DNSSEC
- Promotion campaigns to .ca registrants

Conclusion

- CIRA is committed to implementing DNSSEC in a timely and controlled fashion ☺

- Coming **November 12, 2012**