DNSSEC Workshop

ICANN Silicon Valley
Francisco, California

Canadian Internet Registry Authority (CIRA)

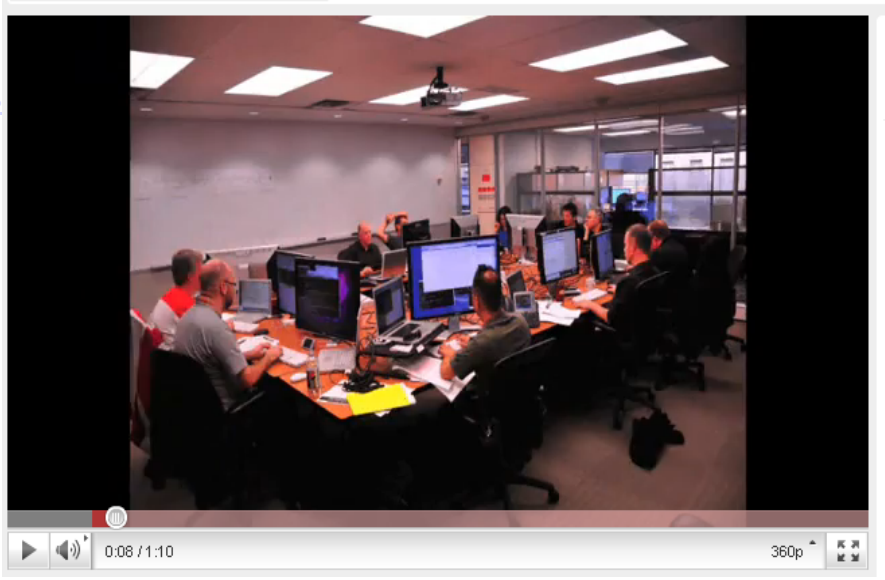
Jacques Latour

DNSSEC Workshop 16 March 2011

Canadians Connected

Current State

- We just migrated our Registry to support EPP and new business processes
  - 18 Month project
  - Migration: 24 hours on October 12, 2011
  - New hardware, OS, applications & DB
  - http://www.

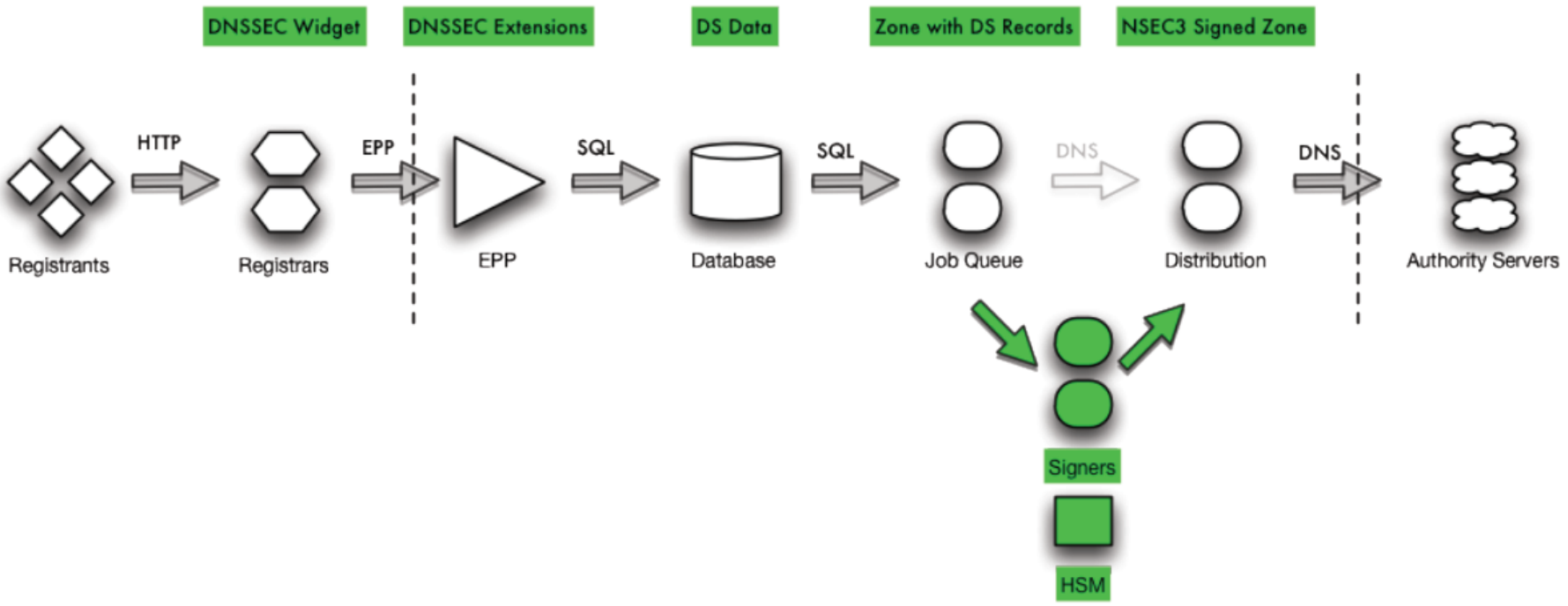


DNSSEC Project

- Started detailed DNSSEC planning
  - Lot's of research and training
- Preliminary solution architecture & design
- Developing a detailed project plan
- Project execution
- Process development
- Risk management

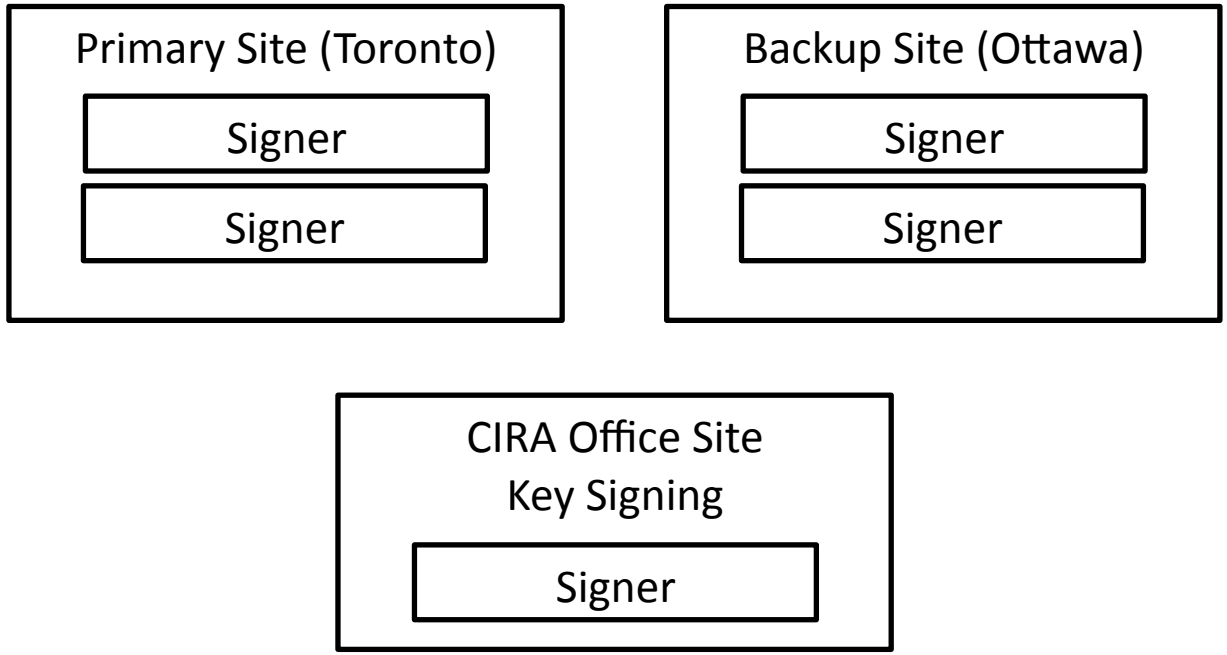
DNSSEC Project Impact

- Impacts all aspect of the Registry & DNS system
- Not just a “Bump in the Wire”



Solution Architecture

- Multiple signers in multiple locations
- Multiple roles control crypto elements



Preliminary Schedule

Milestone	Target Completion Date
Draft Summary of Approach completed (Completed)	2011-01-31 (X)
Draft DNSSEC Policy and Practice Statement (DPS) (Completed)	2011-02-28 (X)
Recommendations for Hardware Purchases delivered (Completed)	2011-02-28 (X)
Draft Signer Design completed	2011-03-31
Draft Monitoring and Measurement Design completed	2011-03-31
Initial Technical Training Session completed	2011-03-31
DPS published for external review	2011-06
Measurement and Monitoring infrastructure deployed	2011-06
Lab signer environment deployed	2011-06
Impact Assessment for Nameservers completed	2011-07
Technical Training completed	2011-10
Production signer environments deployed	2011-10
DPS finalised following external review	2011-10
First production key ceremony completed	2011-12
Key materials successfully replicated to on-line signers	2011-12
Initial DS RRSet for CA in root zone submitted to IANA	2012-02
Production signed CA zone deployed	2012-02

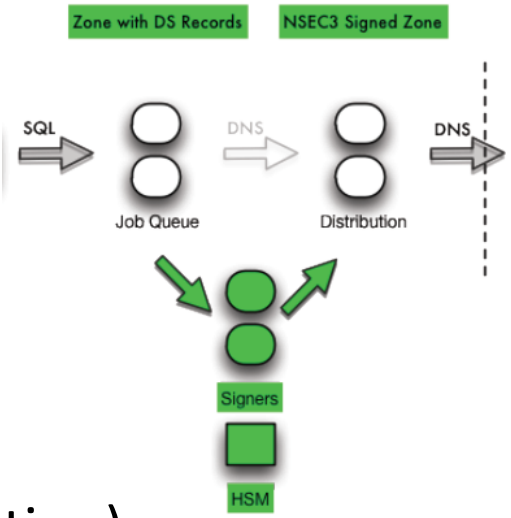
Tentative DNSSEC Parameters

- Reasonable compromise between operational practicality and security

Parameter	Value
Key Signing Key (KSK)	2048-bit RSA
KSK Rollover Schedule	every 12 months
KSK Signature Algorithm	RSASHA256
Zone Signing Key (ZSK)	1024-bit RSA
ZSK Rollover Schedule	every 28 days
ZSK Signature Algorithm	RSASHA256
Authenticated Proof of Non-Existence	NSEC3 with opt-out

Development Process

- Add zone signing process as part of CIRA's software development life cycle
  - CIRA follows the Agile process
  - Quality Assurance Process;
    - Requirements specifications
    - Architecture design specifications
    - Implementation of design (code/integration)
    - Robustness, performance & functional testing
    - Release management



Risk Management

- DNSSEC & zone signing technology is still in its infancy.
- Not a lot of DNSSEC experience available out there
- TLD have seen various type of DNSSEC related service impacting outages;
  - DNSSEC Software bugs
  - Key management issues
  - Implementation issues
  - Operational issues

Conclusion

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