DNSSEC WORKSHOP
ICANN61 SAN JUAN

DNSSEC @ CIRA GENERATION 2

Prepared by: Jake Zack (apologies)

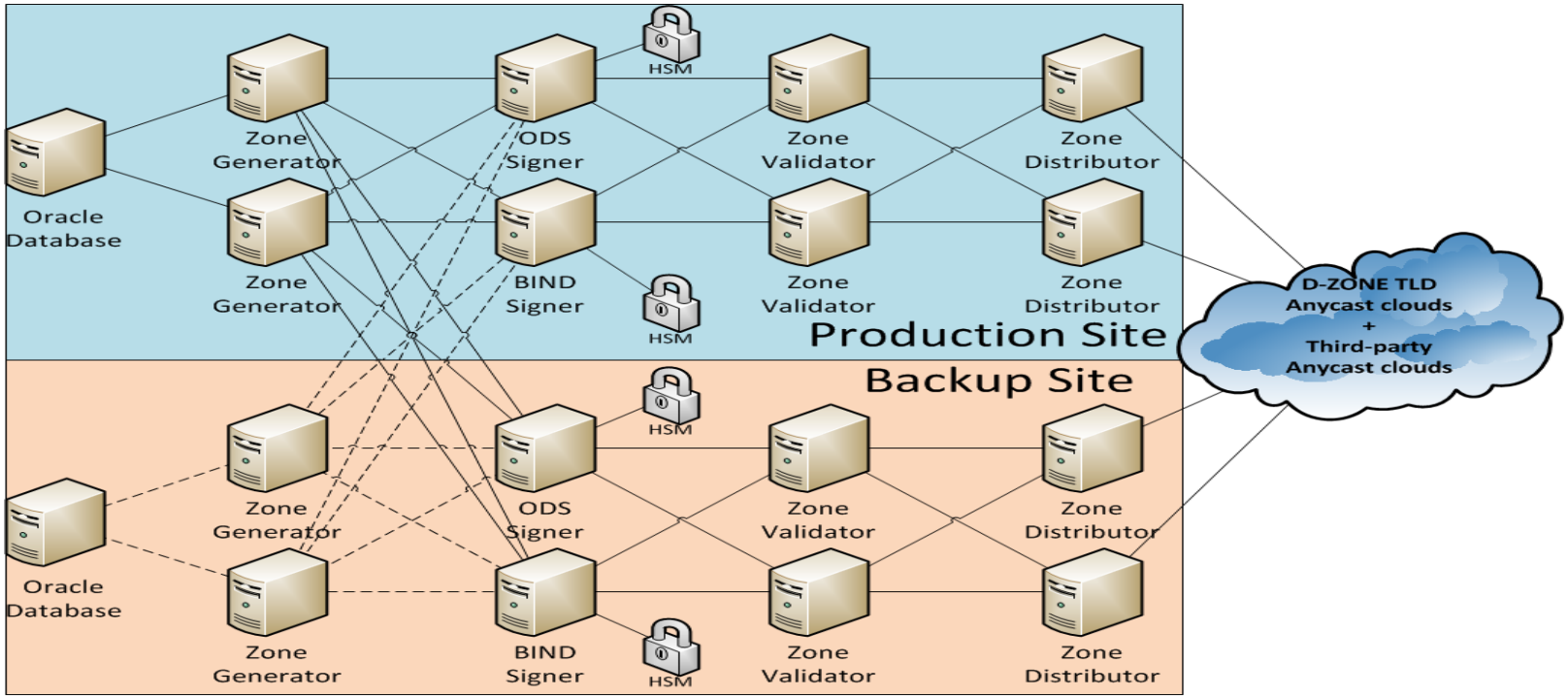
Presented by: Jacques Latour

March14, 2018

.CA DNSSEC OVERVIEW

- ~2.7 Million signed domains
- ~2400 signed delegations
- NSEC3 + Opt Out
- KSK: 2048 bit SHA256
- ZSK: 1024 bit SHA256
- OLD: BIND/OpenDNSSEC + AEP Keyper’s (2013->)
- NEW: OpenDNSSEC + Gemalto Safenet Luna’s

LEGACY .CA DNSSEC SETUP



LEGACY .CA DNSSEC SETUP (CONT.)

- Utilized BIND and ODS Signing
  - One active Oracle instance at a time [PRD | BAK]
  - BIND uses OpenDNSSEC keys/enforcer
    - Keys/KaspDB replicated to all 4 signers
  - Validation compares zones at the end
    - Zero-ize signatures/times
    - Compare zones, publish only when agree

LEGACY .CA DNSSEC SETUP (CONT.)

- Each step launched via cron
  - :00 Zone generation (~11 minutes)
  - :15 Zone signing (~2 minutes)
  - :25 Zone validation (~6 minutes)
  - :35 Zone distribution (~1 minute)

  …with built-in tolerances for high load events.

LEGACY .CA DNSSEC ISSUES

- Single Oracle DB instance
  - No automagic failover from site to site
- Linux Systems
  - 16 physical servers/blades
  - 16 OS licenses + support
  - Way too much SCP’ing
- CRON orchestration
  - Slow and limiting (hourly publish times)

LEGACY .CA DNSSEC ISSUES (CONT.)

- AEP Keyper HSM's
  - Limited remote management
    - Requires people/smart cards on-site
  - Limited load-balancing
    - We chose direct-connect over networked
  - Requires old AEP-hacked BIND libraries
  - Not rack-mountable – we used rack-mounted safe
  - Very little documentation / support

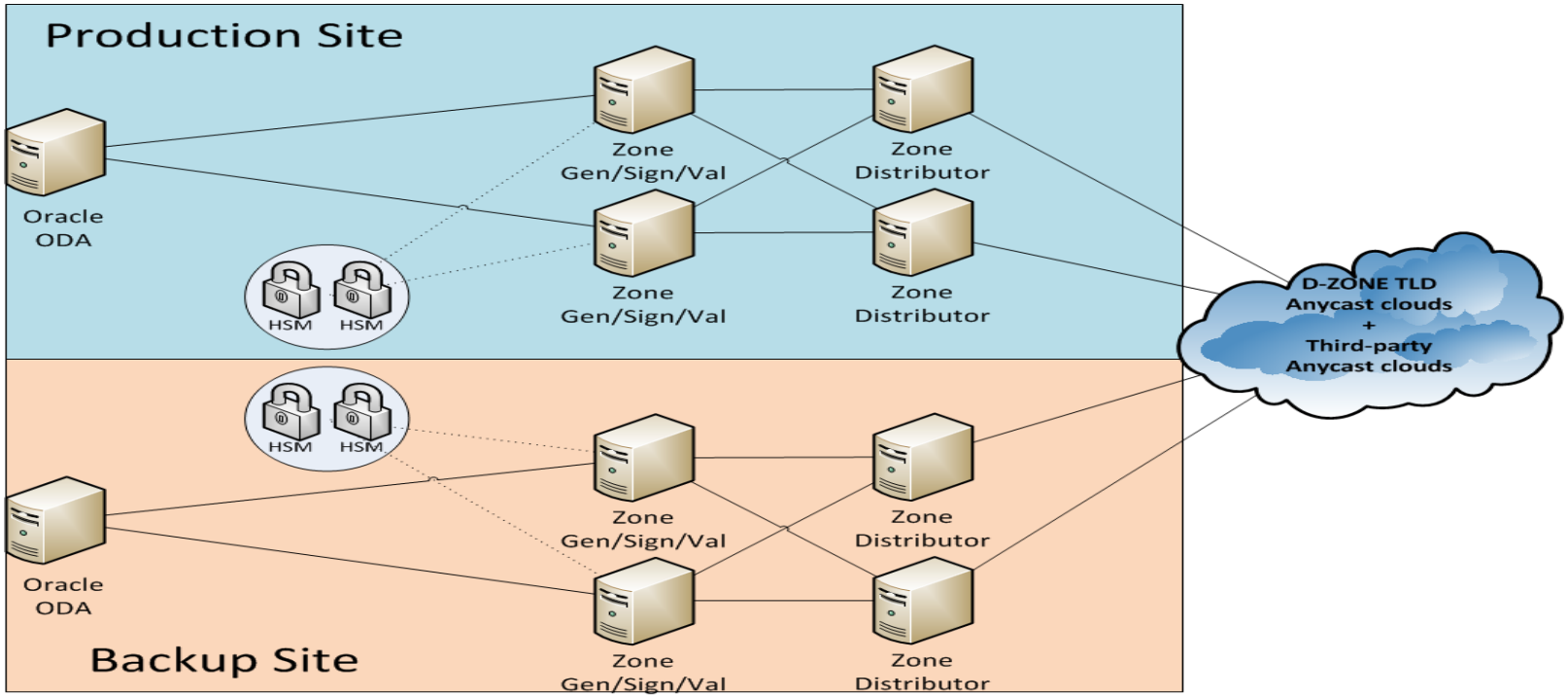
LEGACY .CA DNSSEC ISSUES (CONT.)

- Zone Validation
  - Comparing BIND+ODS zones great for research!

    …found lots of bugs in things…

    …but problematic in production operations.
  - BIND and ODS re-use signatures differently
    - Every rollover meant forcing a full re-sign
    - Often some manual intervention
    - Ruins 3-day weekends and Super Bowls

NEW .CA DNSSEC SETUP



SELECTION OF GEMALTO LUNA HSM

- Allows partitions [PRD|DEV] or [CUST1|CUST2|…]
- Faster signing speeds
- Greater key capacity
- Better role-based access + accounting
- Manage HSM’s as a cluster
- Fully load-balanced
- Allows for remote management (physical token)
- Rack-mountable! No more rack safes!

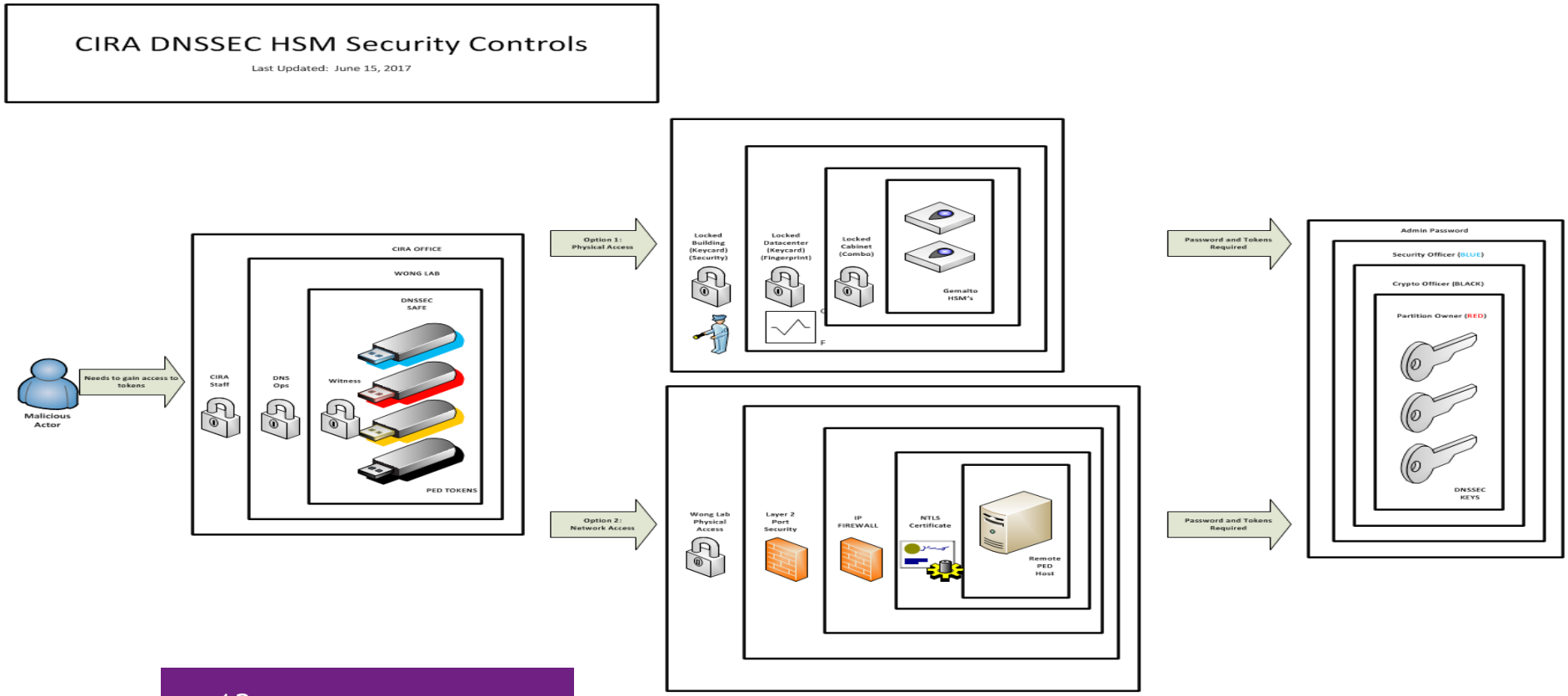
CHANGES TO INFRASTRUCTURE

- Switch to Oracle ODA+Dataguard – active/active
  - Oracle DB replicated in near-real-time
- Switch to VM's – reduces power/space usage
  - Reduced complexity, freed up Redhat licenses
  - Easier to manage, configs in Puppet
- Backup keys to external device after ceremonies
  - Gemalto Backup Unit – same security level
  - (AEP we kept an offline full HSM + smart cards)

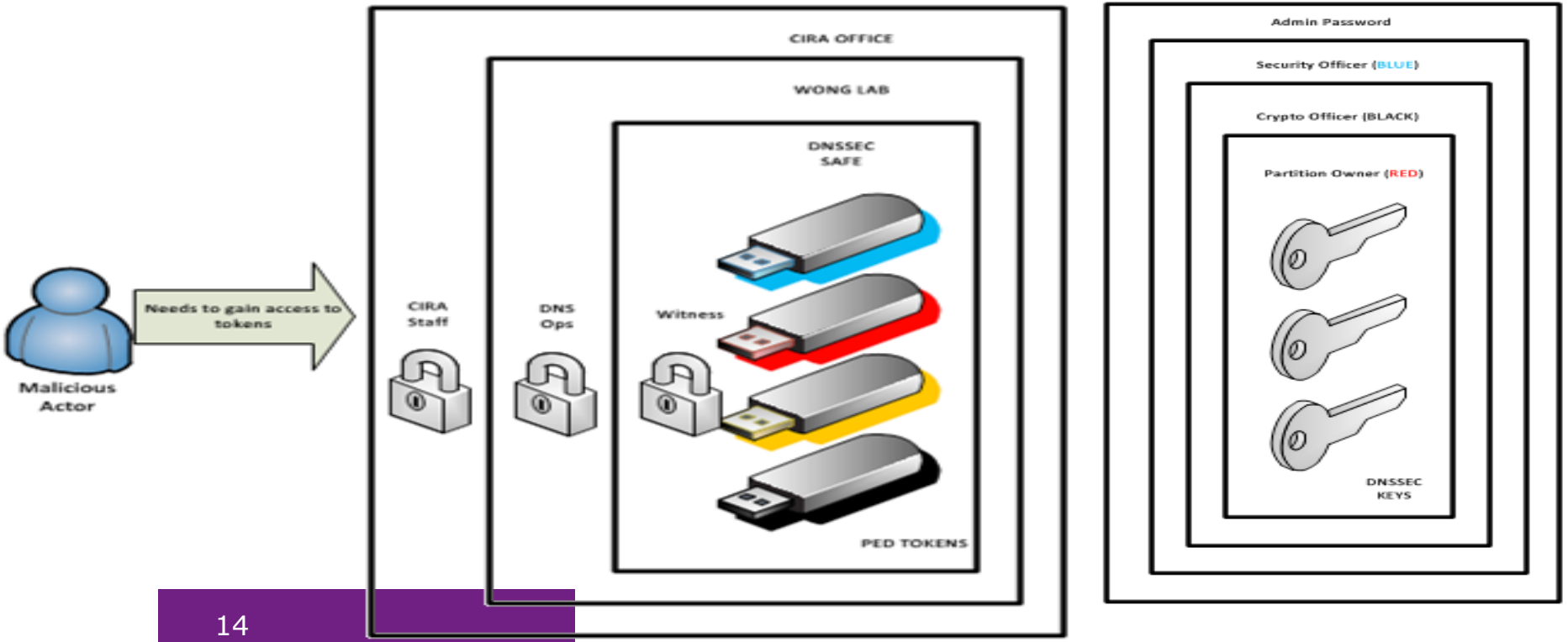
CHANGES TO DNSSEC

- No more dual-signing ODS / BIND zones. ODS wins!
- Fixed ENT's! (Empty non-terminals)
- No more CRON execution – Springbatch orchestration
- HSM's now load-balanced, no single point of failure
- No more zone comparing in validation
- Better monitoring & alerting
  - Active and passive checks now
  - CTIME based serial freshness checks

CHANGES TO SECURITY AROUND HSM'S



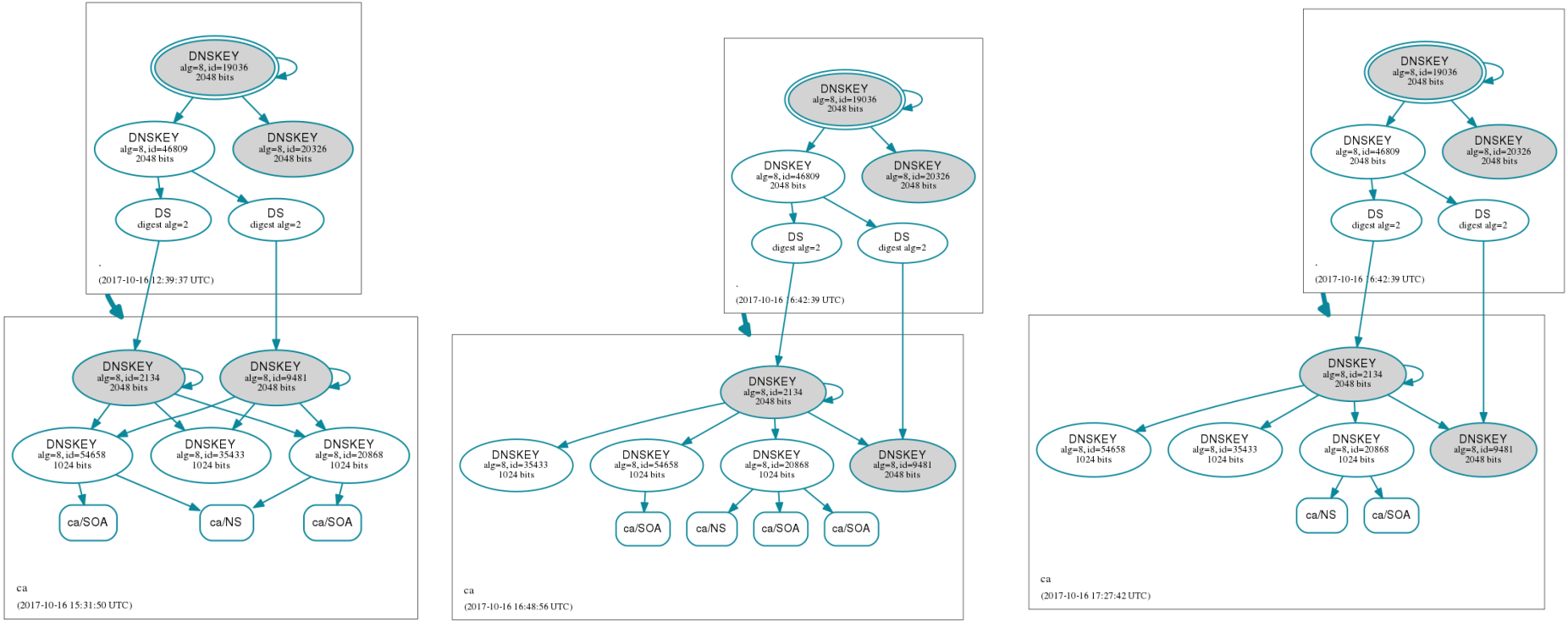
CHANGES TO SECURITY AROUND HSM'S



DNSOP / KSK ROLLOVER

- Old keys on old signers using AEP Keyper HSM’s
- New keys on new signers using Gemalto HSM’s
- Each side signs each other’s DNSKEY sets
- Update IANA RZM to contain both DS sets
- Cut-over once TTL’s are happy on all the things
- Wait for TTL’s (old records clear from caches)
- Remove old DNSKEY sets from new signers
- Update IANA RZM to remove the outgoing keyset

DNSOP / KSK ROLLOVER - IMAGES



DNSSEC RESULTS

- Cut-over to new platform was successful
- Removed need for ZSK roll manual intervention
- Now publishing every 30 minutes (was hourly)
- KSK Ceremonies now take minutes instead of hours
- HSM changes no longer require trips to other cities
- Full process now done in 11 minutes
  - Most of this time is with PERL + Oracle

    …refactoring this piece now.

GRACIAS POR ESCUCHAR

Preguntas?