

PCH DNSSEC Signing Service

Robert Martin-Legène

ICANN 53

Buenos Aires

June 2015

What does it do?

Keys created in key ceremonies 3-4 times / year.

Keys stored in the HSMs can never be exported.

Security on-par with root zone security.

FIPS 140-4 Level 4 - same as for the root.

Signs with NSEC3, opt-out.

Automated ZSK rolls.

Can be used as a “pluggable” service.

Conservatively signing with old version of BIND.

How does it do it?

TSIG preferred.

Pre-publication verification using several tools.

From us to you (and the world).

Tests can even be done on signed zone (without DS in root).

What does the ccTLD need to do?

Put DS from children in their TLD zone.

PCH signs DS with RRSIGs - chain of trust established to child.

Not so steep learning curve.

Slowly get familiarity with DNSSEC.

PCH helpful to help transition of signing back to registry.

Diverse Locations

Americas

- San Jose, USA
- Equinix Datacenter
- Commercial

Europe

- Zurich, Switzerland
- SWITCH Facility
- Research & Education

Asia-Pacific

- Singapore

PCH Anycast DNS

Add (more) anycast to your zone(s).

Anycast via 100 locations.

Also happy to come to “your” IXP.

Don't have one? Let's make one!

Questions



Robert Martin-Legène

robert@pch.net