Support for and adoption of CDS in .CH and .LI

SWITCH

Oli Schacher
oli.Schacher@switch.ch

22.6.2020

.CH/.LI RFC 7344/8078 implementation

Heavily inspired by .cz

- Daily scan of all CDS records (2.3 M domains in ~6 hours)
- Registry application compares and processes scan results and activates DS updates

…with a few differences

- Changes are activated after 3 days
- We scan for CDS instead of CDNSKEY RRSETS
- Status website instead of email communication
- Registrar notification through RFC 8590 EPP change poll extension

Adoption

- .ch / .li domains with published CDS records
  - **2018**: 650
  - **2020**: 13’000
- 12’000 domains bootstrapped
  - Most of these from a small amount of hosting companies publishing CDS for all their domains
- 75 domains performed key rollovers
- 27 domains removed active DS using **CDS 0 0 00**

Work in progress

- SHAmbles mitigation [1]
  - «Software implementing CDNSKEY and CDS checks must ensure that the records are properly signed by a KSK, not just a ZSK.»
  - Requires coordination with hosting providers running old signers
- Algorithm 15/16 support
  - Supported over EPP, but not by all components in our CDS processing chain

[1] https://blog.apnic.net/2020/01/17/sha-1-chosen-prefix-collisions-and-dnssec/