DNSSEC.CZ

DNSSEC Workshop

Ondrej Filip • ondrej.filip@nic.cz • 21 Oct 2015 • Dublin

CZ DOMAIN REGISTRY

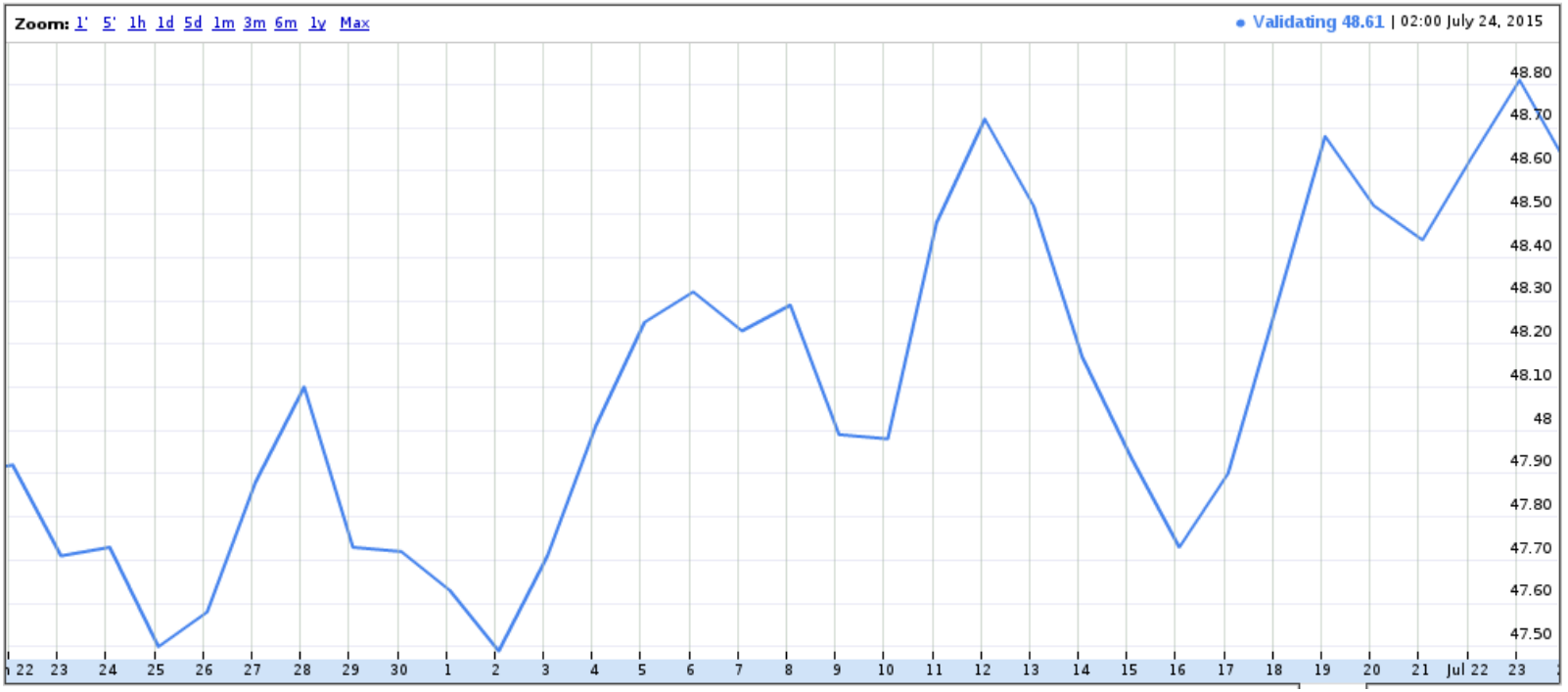
Signed domains

- 38% of all Czech domains (465k of 1.2M) – growing very slowly now
- All major registrars (with 90% of market share) support DNSSEC – many sign by default
- Many important sites signed – news, banks, ...
- DNSSEC in gov. strategy – Digital Czech 2.0 and also Cyber security strategy

Validation

- Almost 50% of resolvers validate (according to Geoff Huston's measurement) – major ISPs

Use of DNSSEC Validation for Czech Republic (CZ)



Knot DNS 2.0

- GnuTLS library instead of OpenSSL
- KASP (Key and Signature Policy) – define policies for zones, engine just enforces the policy
- Automatic management
  - Generating initial signing keys
  - ZSK rotation (key pre-publish method)

Knot DNS 2.1 - soon

- DNSSEC on-line signing
  - Experimental
- Stacks well with modules (e.g., PTR records synthesis)
- Uses Single-Type Signing Scheme
- Uses Minimally Covering NSEC Records
- rewrites NXDOMAIN to NODATA for performance reasons and smaller size of the answers

Knot DNS Resolver

- Open-source DNS Resolver
  - https://gitlab.labs.nic.cz/knot/resolver
- Comes with extensive documentation
  - http://knot-resolver.rtfd.org
- Platform for building recursive DNS service.
- DNSSEC Validation with Automated Trust Anchor Management (RFC5011) and Negative Trust Anchors (RFC7646)
- Fast, written in C (+LUA), extensible
- Internally tested, testing on Turris

Thank You!

Ondrej Filip • ondrej.filip@nic.cz • http://www.nic.cz