# Signing .si
# Before and After

benjamin.zwittnig@register.si

- Before
  - DNSSEC validation
  - Preparing for signing
- Signing .si
- After
  - Adapting registry system
  - Raising DNSSEC awareness

# Before

- Low interest for DNSSEC

- Dnssec validation on recursive nameservers

  - We have learned that

    - Some domains were not resolved any more
    - No reported problem regarding CPEs
    - Traffic increase was not significant
    - Load increase was not significant
    - Around 40% queries with DO bit
    - Reply lengths are (still) mainly under 512 bytes

# Before

- Preparation for signing

  - DNSSEC testbed

  - A lot of documentation

  - Testing (hardware, software, rollovers…)

  - Backup location

  - Monitoring

    - Sanity checks before publishing a signed zone

    - Nagios for nameservers and DNSSEC (RRSIG validity, chain of trust..), RIPE's DNSMON

    - DSC, cacti

# Signing .si

- OpenDNSSEC

  - HSM Sun/Oracle sca6000 for KSKs

  - SoftHSM for ZSKs

  - Keys

    - Algorithm 8 (RSASHA256)

    - NSEC3 with OptOut

  - KSK

    - Size 2048b

    - lifetime 1year

  - ZSK

    - Size 1024b

    - lifetime 30days

  - RRSIG

    - lifetime 14 days

# Signing .si

- 30th of Nov 2011

  - 13:00 Key Generation Ceremony

  - 17:00 First signed version of .si zone was published

- 23th of Dec 2011

  - DS record for .si was added to root zone

# After



- No problems detected

- Increase of traffic on a nameserver we are running for .si

- Increase of DS lookups (expected)

# After

- Almost no interest for DNSSEC

  - Governmental institutions

  - Banks

  - Two registrars

- At the moment only few delegations signed (~ 20)

# After

- We need to adapt our registry system for DNSSEC

- Signing zones we are operating as a registrar

    - in-addr.arpa, ip6.arpa

    - Zones we are hosting

- We need to raise DNSSEC awareness

    - Resolver operators to turn on DNSSEC validation

    - Hosting providers to start signing their domains

    - Registrars to publish DS records

- Trainings

- Signing service?

# Questions?