Registry role in ccTLD

Jaromir Talir • **jaromir.talir@nic.cz** • **30.05.2016**

Three levels structure

- Propagating changes to upper level (root)

- Technically maintaining delegated level (TLD)

- Joining lower level domains (SLD)

Propagating changes to upper level

- ICANN / IANA administration

- Mainly changes in NS and DS records - https://www.iana.org/help/nameserver-requirements

- Web interface for changes - https://rzm.iana.org/

- Authorization by admin contact

Maintaining delegated level

- Zone file generation

- DNS servers administration

- DNSSEC

Zone file generation

- Most crucial piece

  - Bug can disable internet in the country

- Do as much checking as possible

  - Zone file correctness
  - Number of changes between versions

Zone file generation

- Delegation resource records only

- NS records

- A records - glue

- DS or DNSKEY records

Zone file generation

- Dynamic updates
  - Provides online changes
- Periodical generation of full zone from database
  - Needs some time

DNS servers administration

- Bind, NSD, Knot DNS

- One (hidden) DNS master server

  - Feeds dynamic updates or generated zone file

- Network of slave servers

- Hosted or under own control

  - Control of software

  - Access to statistics

DNS servers administration

- Transfers from primary to secondary

- IXFR or AXFR

- ACL and TSIG

- SOA parameters

DNS servers administration

- Anycast technology

- Announcing the same address from different places

  - Nearest server is selected – speed up of DNS response time

  - Redundancy creates reliability

- Check RIR policy for anycast addresses

DNSSEC

- DNS is vulnerable

  - Spoofed responses

  - Cache poisoning

- DNSSEC brings proof of authenticity and integrity

  - Asymmetric cryptography

  - Chain of trust

DNSSEC

- DNS is vulnerable

  - Spoofed responses

  - Cache poisoning

- DNSSEC brings proof of authenticity and integrity

  - Asymmetric cryptography

  - Chain of trust

DNSSEC

- Introducing DNSSEC means:

  - Signing own zone

  - Propagation of own keys to root zone

  - Accepting SLD keys in own zone

- Signing may be automated:

  - OpenDNSSEC, Bind, Knot DNS

- Accepting of SLD DNSKEY of DS material

DNSSEC

- New tool for attackers

  - Big responses for small queries

  - Amplification attacks

- Response Rate Limiting as protection

  - Configuration option in DNS server

  - After reaching limit server switch to TCP

Joining lower level domains

- Policy and rules

- Registry model

- Registrar communication – EPP

- Registrant communication – WHOIS

- Billing and marketing

- Delegation technical checks

Policy and rules

- Who will be able to register domains?

- Will some names be forbidden?

- Will there be IDN and in what form?

- What are prices, grace periods and other parameters?

- What UDRP to follow?

Policy and rules

- Legal form of registry

- Multistakeholder approach

- ISPs, Registrars, domain owners

- Regulator, Government

Registry model

- Registry-Registrar-Registrant model
    - Registry concentrates on important topics
    - Registrars can provide added value to Registrants
    - Registrars connect to multiple Registries
- Sometimes Registry serves as the only existing Registrar

Registry model

- Registry
    - Ensure uniqueness of registered domains
    - Ensure fair distribution – first come first serve
- Registrar
    - Provide correct user data

Registrar communication

- EPP – Extensible Provisioning Protocol

- IETF standard

- XML messages for registry object provisioning (create, update, delete, transfer, info)

- Security (ACL, SSL, Authentication)

- Tools and libraries

Registrar communication

- Domains, Contacts, Hosts

- Extensions and incompatibility

  - NSSets

Registrant communication

- Notifications of changes

- Notifications of expiration

- Validation of contact information

- Solving of registrants problems

- Domains locks

Registrant communication

- WHOIS – public information about registry

  - Port 43

  - Web WHOIS

- Only disclosed information about contacts

- New initiative called RDAP

  - Structured data, Authentication, Localization

cz.nic | CZ DOMAIN REGISTRY

Billing and marketing

- Payment models

  - Prepaid model
  - Postpaid model

- What to bill

  - Registration + renewal
  - Annual fee
  - Minimal registrations
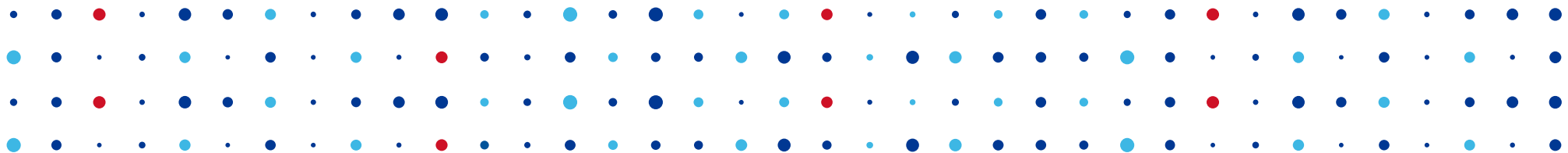 - EPP transactions

Billing and marketing

- Marketing to registrars
  - Co-marketing campains
- Marketing to registrants
  - Advantages of having own domains

Delegation technical checks

- Are delegations correct?

  - Reachability, Configuration,...

- Pre-delegation or post-delegation checks

- Tools

  - https://dnsviz.net

  - https://zonemaster.net

Thank You

Jaromir Talir • jaromir.talir@nic.cz