FRED – open source registry solution

Jaromir Talir • jaromir.talir@nic.cz

CZ DOMAIN REGISTRY

Agenda

- CZ.NIC story
- FRED overview
- Deployments
- Data model
- Interfaces
- Features

CZ.NIC story - year 2005

- CZ.NIC had 4 employees
- Number of domains was 250 000
- Price for domain was 16 USD/year
- Registry system was completely outsources to other company
  - Roughly 90% of income went to outsourcing company

CZ.NIC story - year 2005

- Decision was made to cancel outsourced model
  - Registry administration is **core business**
- Technical staff was hired (sysadmins + developers) and development of new registry called FRED started
- In September 2006, .0.2.4.e164.arpa ENUM zone management was started using new registry system
- In September 2007, .CZ zone management was migrated to FRED

CZ.NIC story - year 2016

- CZ.NIC has 100 employees
- Number of domains is 1 250 000
- Price for domain is 5 USD/year
- Big portfolio of activities
  - CZ.NIC Edition – Translation of books
  - CZ.NIC Academy – Technical courses for public
  - CZ.NIC Labs - R&D department

In-house system advantages

- Complete control over the system
  - Adjustment possibilities (if open source software is used)
- Gaining expertise and keeping knowledge at home
- Becoming a leader/teacher in Internet technologies in your country

Open source registry systems

- FRED
  - https://fred.nic.cz
- CoCCA
  - https://wiki.cocca.org.nz
- Estonian registry
  - https://github.com/internetee/registry

FRED

- FRED – **F**ree **R**egistry for **E**NUM and **D**omains
- Set of open source tools for managing domain registry
- Platform: C/C++/Python + Linux + PostgreSQL
- Available at https://fred.nic.cz
  - Download page with installation instructions

FRED

- FRED scope
  - Management of domain registrations in multiple zones via set of interfaces
  - Generation of DNS zonefiles for all zones
- Registry-Registrar-Registrant model (3R)
  - Registry has no direct connection to registrants (with a few exceptions)
  - Registrars are responsible for the data in registry

Deployments

- 2006 – 0.2.4.164.arpa
- 2007 – CZ, CO.CZ
- 2008 – IT.AO, CO.AO
- 2009 – TZ
- 2010 – FO, CR, ~~EE~~
- 2013 – AL
- 2014 – MK
- 2016 – MW, AR

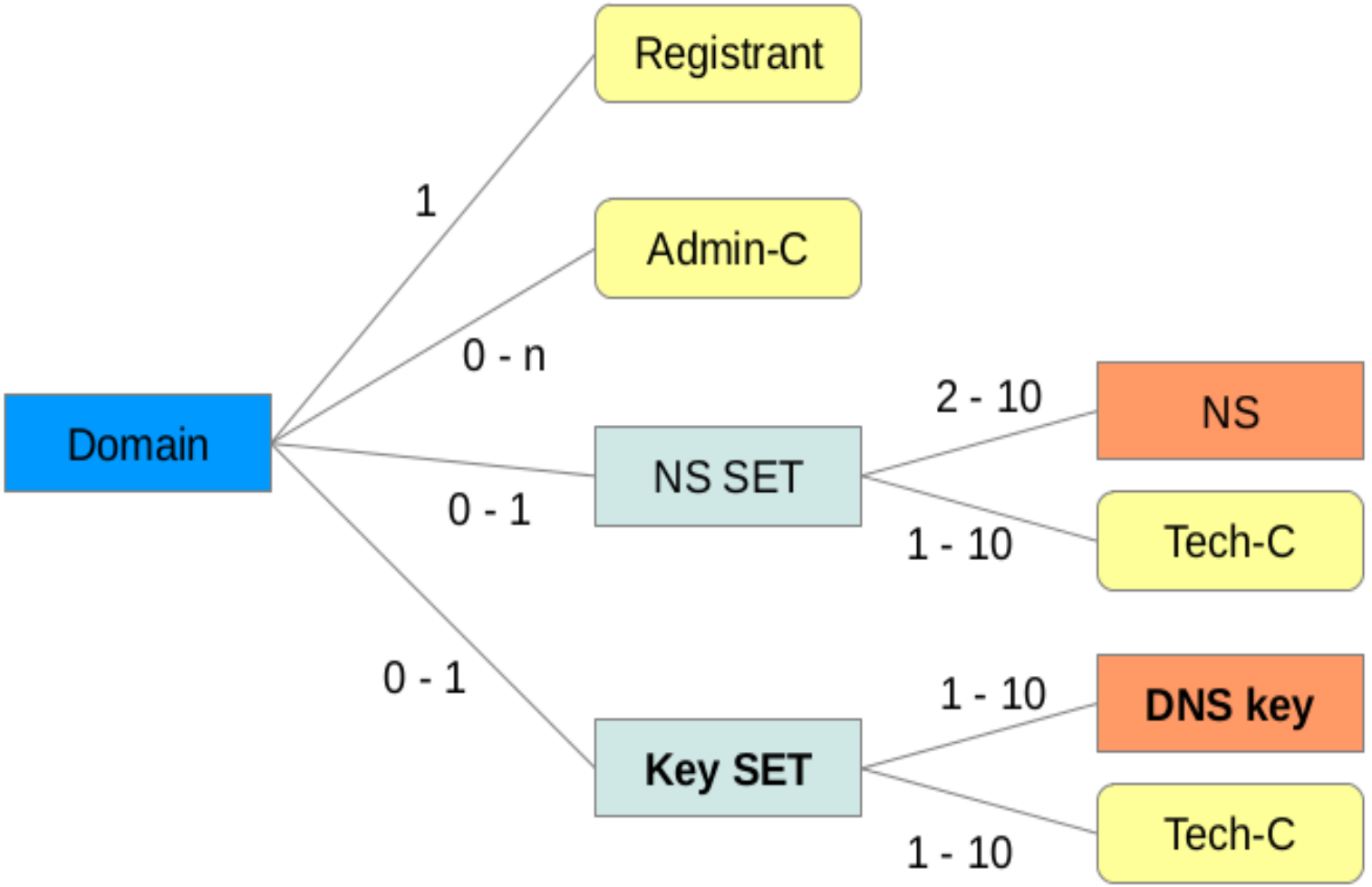
Deployments

- 2R registries
  - CR, FO, AR
  - Web frontend build on top of FRED
- 3R registries
  - All others
  - Many modifications (EE – identity document in EPP, AL – billing contacts, TZ – credit management)

Data model

- Primary objects
  - **Contact** - contact information, registrants, admin contacts, tech contacts
  - **NSSet** - collection of DNS hosts
  - **KeySet** - collection DNSKEY data for DNSSEC
  - **Domain**
- Objects can be shared

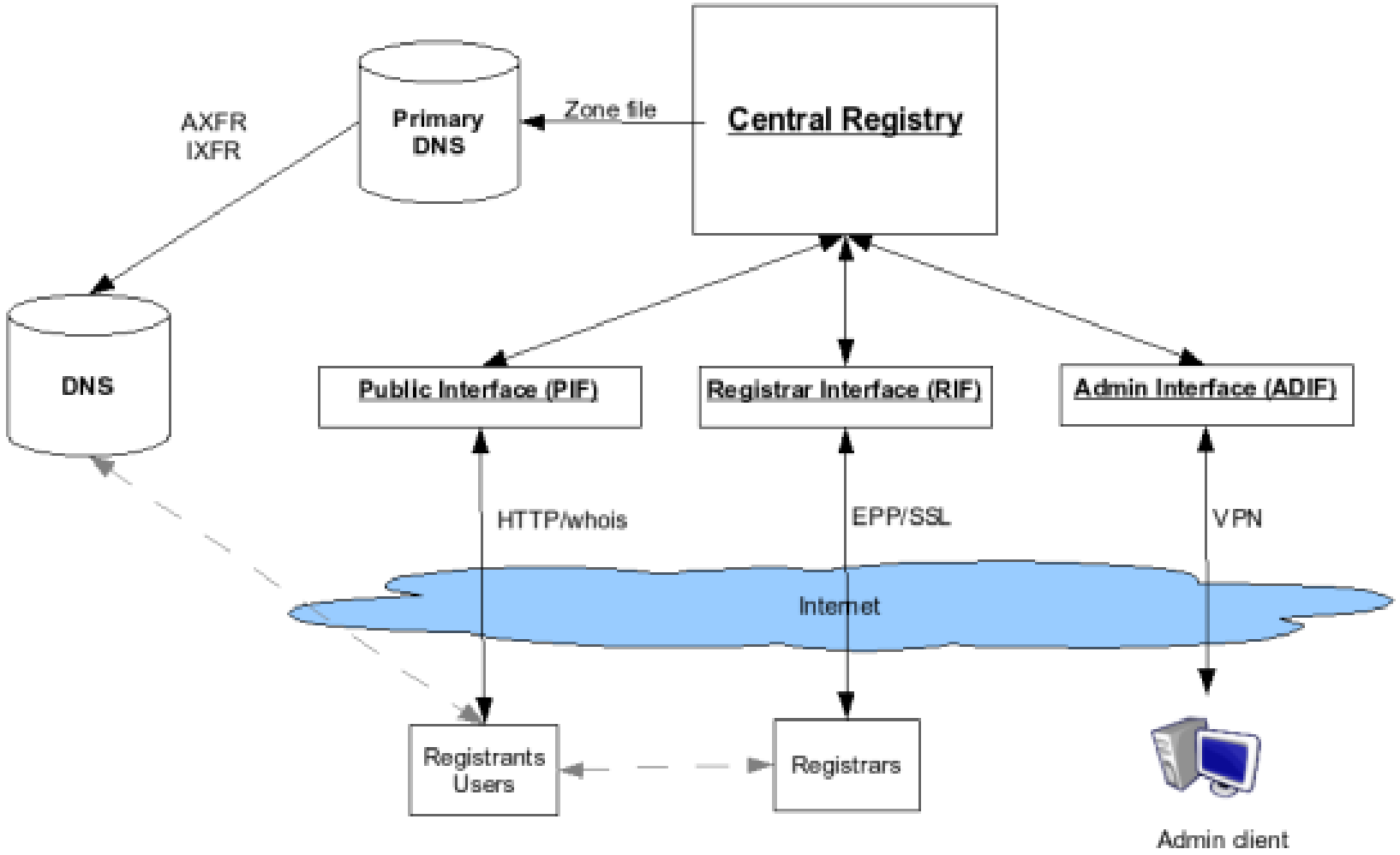
Data model


Registrant
Admin-C
NS SET
NS
Tech-C
Key SET
DNS key
Tech-C
Domain
1
0 - n
0 - 1
0 - 1
2 - 10
1 - 10
1 - 10
1 - 10

Data model

- All objects have “sponsoring” registrar and only this registrar can do changes
- All registrars can see the data of all objects except of secret transfer code called “authinfo”
- Users may decide to change registrar by providing authinfo to new registrar

Interfaces


AXFR
IXFR
Primary DNS
Zone file
Central Registry
DNS
Public Interface (PIF)
Registrar Interface (RIF)
Admin Interface (ADIF)
HTTP/whois
EPP/SSL
VPN
Internet
Registrants Users
Registrars
Admin client

Interfaces - EPP

- Few extensions
  - New objects NSSets and KeySets
  - Contact has new fields for identification purposes
  - Bulk info operations, credit discovery, authinfo requests, invocation of technical checks
- Python library and cmdline client (fred-client)

Interfaces - WHOIS

- Lookup in all objects
- Privacy concerns – disclose flags interpretation
- Three forms:
  - Port 43 - reverse search
  - Web WHOIS – web form and result page with hyperlinks to linked objects
  - RDAP – only lookup queries

Interfaces – Web administration

- Lookups
  - history of all objects
  - all interface transactions
  - client communication
- Registrar administration
- Domain activation/deactivation
- Contact validation

Interfaces – CLI administration

- CLI scripts
- All regular operations
  - Notifications about expired domains
  - Deleting of expired domains
  - Processing bank transactions
- Periodical invocation is handled by Cron tool

Interfaces – Zonefile generation

- CLI script – genzone
- Produce zonefiles for all configured domains
- Output is plain unsigned zonefile
- Post processing scripts not included
  - Zonefile correctness checking
  - Checking of number of changes
  - DNSSEC signing

Features - DNSSEC

- KeySet object with DNSKEY records
- KeySets can be shared among many domains
- Generation of DS records during zone file generation
- Signing is out of scope, you can use anything you want (Bind, OpenDNSSEC, Knot DNS)

Features - ENUM

- Storing phone numbers as domains in DNS
- Arbitrary number of labels in domain
- Validation date as a mean of verification of number ownership
- Not actively promoted project in .CZ

Features - IDN

- Strong opposition against IDN in .CZ
- Configuration option that may be turned on
- Limitations
  - No character sets checking
  - No bindings with non-IDN domains

Features - Billing

- Charging is aimed to registrars
- Both prepaid and postpaid models supported
- Flat price lists – one price per zone per operation
- EPP registrations and renewals are charged
- EPP transactions over limit are charged

Features – Contact notification

- Via email
  - When there are changes in data
  - Important events (expiration, deactivation)
  - Once a year sending reminder email with all contact data
- Sending a snail mail letter after domain deactivation

Features – Registry locks

- Direct channel between Registrar and Registry
- Website with form with request for locking domain
- Request must be followed by electronically signed email or officially signed letter
- Request must be processed manually by staff after checking authentication
- Unlocking is the same process

Features – Delegation checks

- Only informational – no influence on delegations
- Reachability, proper delegation, DNSSEC functionality,...
- Technical contacts are informed via email
- Automated periodical invocation
- Registrars can invoice checks via EPP

Features – Contact validation

- Contacts are randomly selected for validation
- Automated controls checks syntactical correctness, address check with street registry, etc..
- In case of problems manual checks by staff follows and communication with contact starts
- When there is no response, domain is deleted

Requirements

- Depends on expected traffic
  - Because of modular design, it can be one server or six servers
  - Disk storage based on how long you want to store audit records

Adoption

- Installation – easy on Ubuntu or Fedora
- Configuration – parameters in config files
- Customization – email and web templates
- Migration of data – via EPP + SQL
- Distribution of EPP access to registrars
  - Or implementation of registrar interface

Thank You

Jaromir Talir • jaromir.talir@nic.cz

CZ DOMAIN REGISTRY