

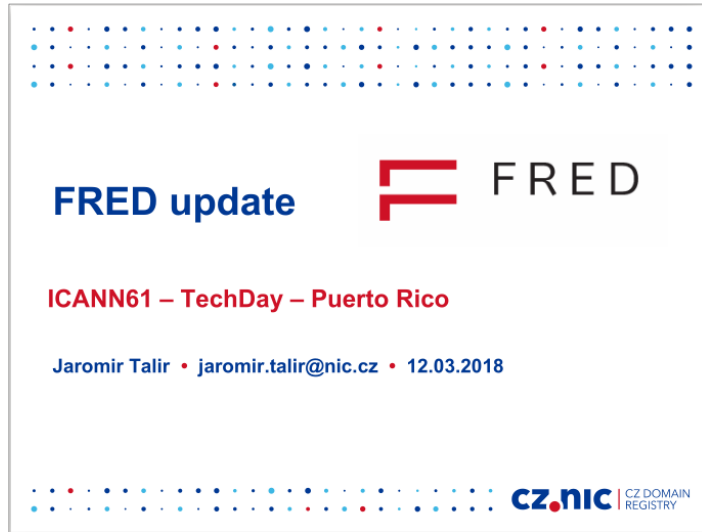


FRED update

ICANN78 – TechDay – Hamburg

ICANN TechDay updates

- Link to last FRED update



FRED

- Open source registry solution
- EPP, WHOIS, RDAP, DNSSEC with automation via CDNSKEY scanning, ...
- Developed (and used) by CZ.NIC since 2006
- Website: <https://fred.nic.cz>
- Comprehensive documentation: <https://fred.nic.cz/documentation/html/>
- Source code: <https://gitlab.nic.cz/fred>
- It is possible to order support (consultations, help with migration, NBD responses...)

Who uses FRED



Main development drivers

- Catching up with industry progress
- Main languages are Python and C/C++
 - 2020 was end of live of Python 2 → everything had to be rewritten in Python 3
 - Sometimes it was easier to rewrite from scratch
- CORBA RPC technology is aging
 - Some required libraries (i.e ORBit) not maintained anymore
 - Decision was made to move to gRPC
- Modern Python systems requires a lot of dependencies that are not distributed via system packaging
 - Moving to deployment via Docker

Payment processing

- Ongoing effort to separate billing and invoicing into independent module (or ideally integrate with external billing/accounting software)
 - There is a lot of country specific features in this area
- New API for processing incoming payments
- New web application for administration of incoming payments based on Czech specific rules

Web administration interface

- Completely rewritten from scratch
- Python3, gRPC, Docker deployment
- Modular architecture with plugins
- New features
 - MFA with FIDO keys
 - Full-text searches
 - Reports generation
- Missing “in-progress” features
 - Administrative blocking

Domain

Current data

Current data

Last month

Last year

Last 5 years

Full history

CZ.NIC

HISTORY VERIFIED STATEMENT LOGGER REQUESTS

Sponsoring registrar:

Handle: REG-CZNIC

Technical contact:

Handle: JTALIR

Name: Jaromir Talir

Technical details:

Technical check level: 3

DNS hosts:

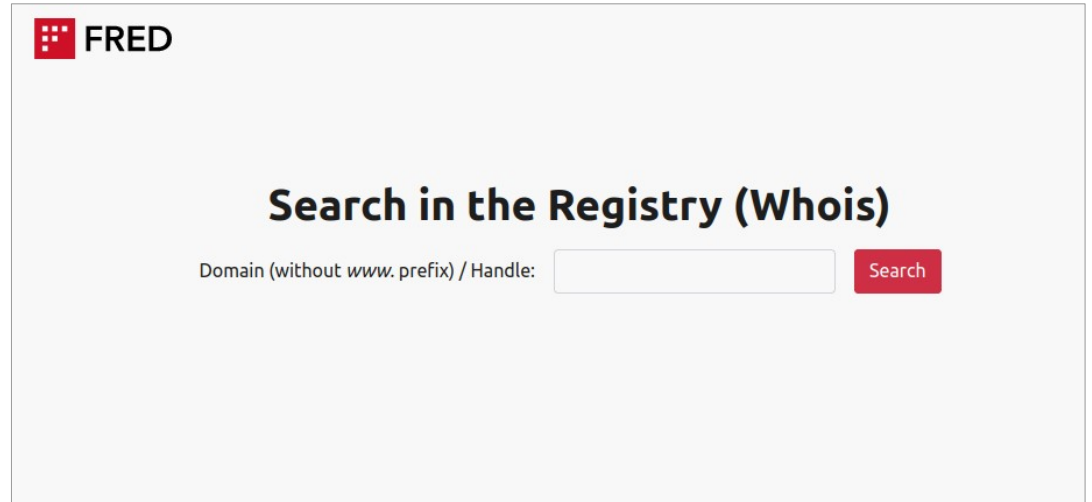
a.ns.nic.cz: 194.0.12.1, 2001:678:f::1

b.ns.nic.cz: 194.0.13.1, 2001:678:10::1

d.ns.nic.cz: 193.29.206.1, 2001:678:1::1

WebWHOIS & RDAP

- Migration to Python3, gRPC and Docker
- Drop support for old Python/Django versions
- RDAP
 - Object states based on RFC8056
- WebWHOIS
 - Remove .CZ specific template
 - Show CDNSKEY scan results



The screenshot shows the FRED WebWHOIS search interface. At the top left is the FRED logo, consisting of a red square with a white grid pattern followed by the text "FRED". In the center, the heading "Search in the Registry (Whois)" is displayed in bold. Below this heading is a search form with the label "Domain (without www. prefix) / Handle:" followed by a text input field and a red "Search" button.

EPP client

- Starting from scratch with Python3

- EPP library moved to separate project
 - <https://gitlab.nic.cz/fred/utils/epplib>
- FRED EPP interactive client (fred-eppic)
 - <https://gitlab.nic.cz/fred/eppic/>

```
REG-FRED_A@epp.regtest.nic.cz > info-domain nic.cz
info-domain
send-auth-info-domain
```

- Due to slow progress we had to do Python2→Python3 migration of original fred-client tool
 - As a result now we have two epp clients
 - Old one will be supported only for limited time

Messenger

- New component responsible for sending messages (emails, sms, letters)
 - Database with archive is separated from FRED
 - Unified approach to all types
 - Administration interface for templates (secretary)
 - Better performance
 - Plugins for senders
- Migration can be complicated
 - Templates
 - Archive

The screenshot displays the Django administration interface. The top navigation bar includes the 'Django administration' logo and user links: 'WELCOME, ADMIN', 'VIEW SITE / CHANGE PASSWORD / LOG OUT'. The breadcrumb trail shows the path: 'Home > Secretary > Templates > notification-renew-body.txt (7fdb742f-2a81-450b-a335-1201bba7b171)'. On the left sidebar, a search bar is present above a list of menu items: 'AUTH TOKEN' (Tokens), 'AUTHENTICATION AND AUTHORIZATION' (Groups, Users), and 'SECRETARY' (Assets, Tags, Template collections, Templates). The 'Templates' item is highlighted. The main content area is titled 'Change template' and shows the details for 'notification-renew-body.txt (7fdb742f-2a81-450b-a335-1201bba7b171)'. It includes a 'Name' field with the template name, a checked 'Is active' checkbox, and a 'Content' text area containing a template string with placeholders for domain, ticket, and registrar information, followed by a renewal notification message.

Current state of refactoring

- Still a few missing tasks
 - EPP, processing part and Port 43 Whois
 - Zonefile generation is rewritten as well, but still not deployed
 - Technical checks are abandoned in favor of Zonemaster integration
- For new architecture we prepared a new installation script
 - Since several components are using Docker, it is not possible to deploy into LXC environment
 - Installation via script should be considered as “demo” and not used in production
- New development not related to refactoring follows...

New authinfo usage and handling

- Securing access to contact data
 - Registrars could always access all contacts data in the registry
 - Now the access (contact_info) is secured with authinfo for not owned contact
- Authinfo is stored as hash and expires
 - Implementation of RFC9154 (Extensible Provisioning Protocol (EPP) Secure Authorization Information for Transfer)
 - For each authinfo “usage” (transfer, contact_info) there must be a new authinfo generated either via registrar or via registry
 - It is not possible to query authinfo from the registry
 - Expiration is configurable (14 days for .CZ)

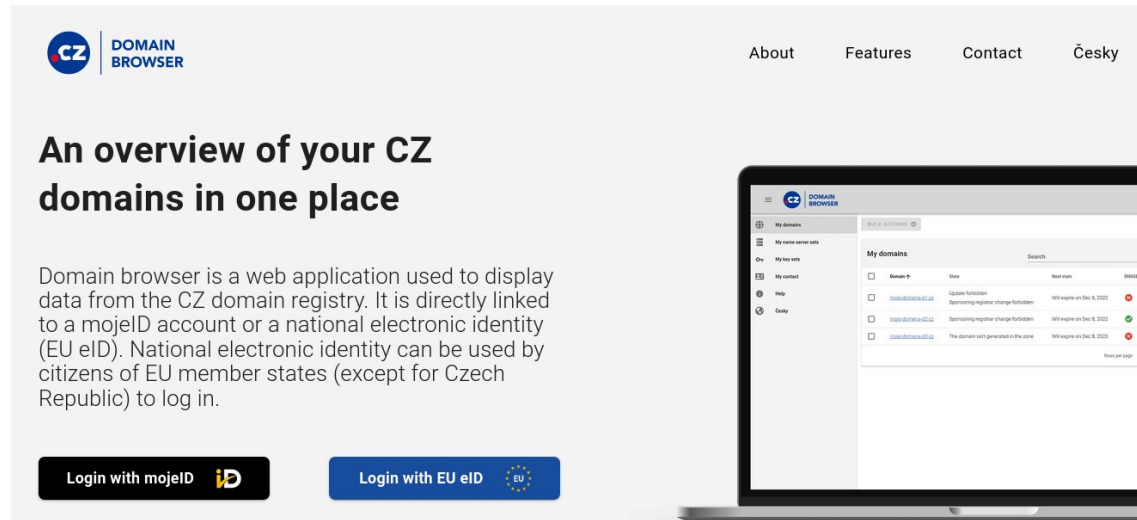
Statistical dashboard

- Independent application that collects all the data from our systems
- Visual graphs and REST API to the data



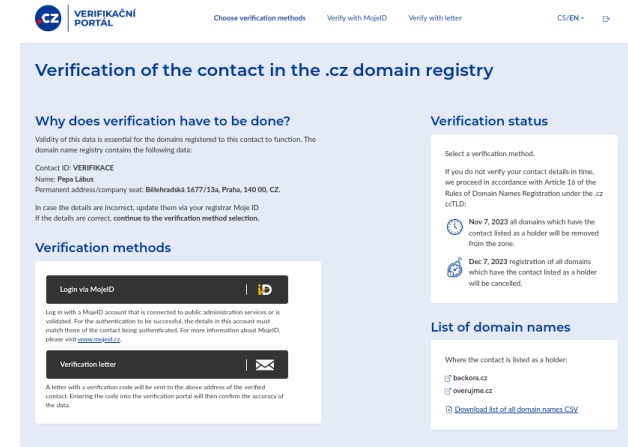
DomainBrowser and eID

- Registrant portal
 - Not part of distribution due strong dependency on our identity service
 - Refactored with eIDAS authentication included
 - Full generalization of access possibilities still in progress

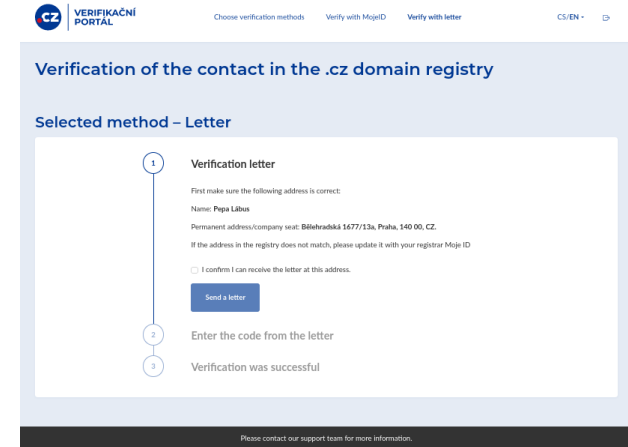


Verification portal

- As reaction to NIS2 we need more flexible approach for registrant data verification
- New web portal where registrant can select method for verification
- First version is out to collect feedback
 - with methods send letter or use MojID
- More work is needed to make it general for other registries



The screenshot shows the 'VERIFIKAČNÍ PORTÁL' (Verification Portal) interface. At the top, there are links for 'Choose verification methods', 'Verify with MojID', and 'Verify with letter'. The main heading is 'Verification of the contact in the .cz domain registry'. Below this, there are three main sections: 'Why does verification have to be done?', 'Verification methods', and 'Verification status'. The 'Why does verification have to be done?' section explains the importance of accurate contact data for domain functionality. The 'Verification methods' section offers two options: 'Login via MojID' and 'Verification letter'. The 'Verification status' section provides information on domain removal deadlines (Nov 7, 2023 and Dec 7, 2023) and a 'List of domain names' where users can check the status of their domains.



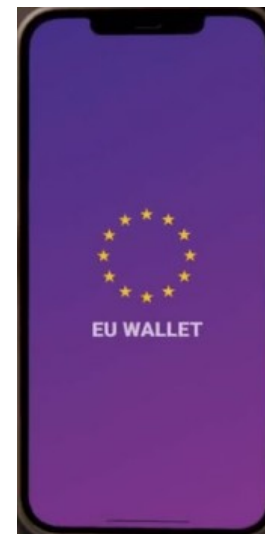
The screenshot shows the 'Selected method - Letter' page. It features a vertical progress indicator on the left with three steps: 1. Verification letter, 2. Enter the code from the letter, and 3. Verification was successful. The first step is active. The main content area for step 1 includes a heading 'Verification letter', instructions to verify the address, and a 'Send a letter' button. Below the button, there is a checkbox for 'I confirm I can receive the letter at this address.' The bottom of the page has a footer with contact information for support.

Auctions

- Reaction to complains about unfair access to expired domain
- Inspired by successful implementation of auctions in Estonia
 - However with some differences (open auctions)
- Auction portal implemented in DomainBrowser
 - It will again require verified digital identity to participate
- Expected launch in 2024

Future

- Finishing refactoring
 - Thanks to modular architecture we can rebuild “as we go”
- Be fully “cloud ready” using Docker
- Embracing digital credentials and wallets
 - Potentially universal technology that we can use in DomainBrowser and Verification portal
 - Crazy idea: “Registries as the issuers of domain ownership credentials that are accepted by issuers of TLS certificate as the alternative to domain validation”
 - To explore these possibility we participate in Large Scale Pilots for European Digital Identity Wallet as part of EWC consortium



Thank you for watching!