Registry Object Locking In FRED

Jaromir Talir • **jaromir.talir@nic.cz** • **23.06.2014**

Why to speak about registry locks again?

- Domain hijacking is still an issue

- Only 1/3 of European ccTLD registries has this feature according survey in Oct 2013

- Registry object locking is/should be a **feature of registry software** – in FRED since 2008

- **New registrant interface** in .CZ - Sep 2013

- **Administrative locking GUI** in FRED – Jan 2014

cz.nic | CZ DOMAIN REGISTRY

What is registry lock

- Protection against EPP changes of objects in registry issued by **Registrar**

- **Registrant** (as the requester) must use different channel then EPP

- Protection is set by the **Registry** after proper authorization of request

What is FRED

- Open source domain registry software – http://fred.nic.cz

- Developed and used by CZ.NIC since 2007

- Used by other countries: Angola, Tanzania, Costa Rica, Faroe Islands, Estonia, Albania, **Macedonia (since Jan 2014)**

- Version 2.18 – July – Better contact validation

- Version 2.19 – August – RDAP protocol

Registry object locking in FRED

- Entry point is the web form

  - Can be integrated into registry website
  - Template can be customized

- Requester must fill:

  - What changes should be blocked
  - Object handle and type
  - Means of requester authentication

Registry object locking in FRED
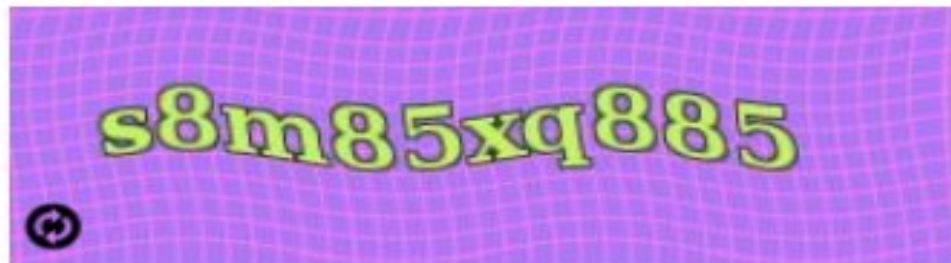
Request: Blocking of all changes

Object type: Domain

Handle:

Confirmation method: E-mail signed by a qualified certificate

s8m85xq885

Security code (retype from image):

Send

CZ.NIC | CZ DOMAIN REGISTRY

Registry object locking in FRED

- Two levels of protection:
  - Only transfer to other registrar
  - All changes of object data
- Locking is possible for all registry objects
  - Domain
  - Contact – registrant, admin-c, tech-c
  - NSSet – collection of NS information
  - KeySet – collection of DNSKEY information

Registry object locking in FRED

- Object "owner" can authorize request

  - Domain -> registrant, admin-c

  - Contact -> contact itself

  - NSSet, KeySet -> tech-c

- Authentication means

  - Letter with notarized signature

 - Email with digital signature based on official CA certificate

Registry object locking in FRED

- After submitting request, requester provides authentication to our client center operator

- Client center operator verifies authentication and confirms lock setting through web administration interface

  - Despite manual procedure, service is free of charge

- Registrar will receive "Object status prohibits operation" EPP response

  - Anyone can see ServerTransferProhibited and ServerUpdateProhibited status in WHOIS

Registry object locking in FRED
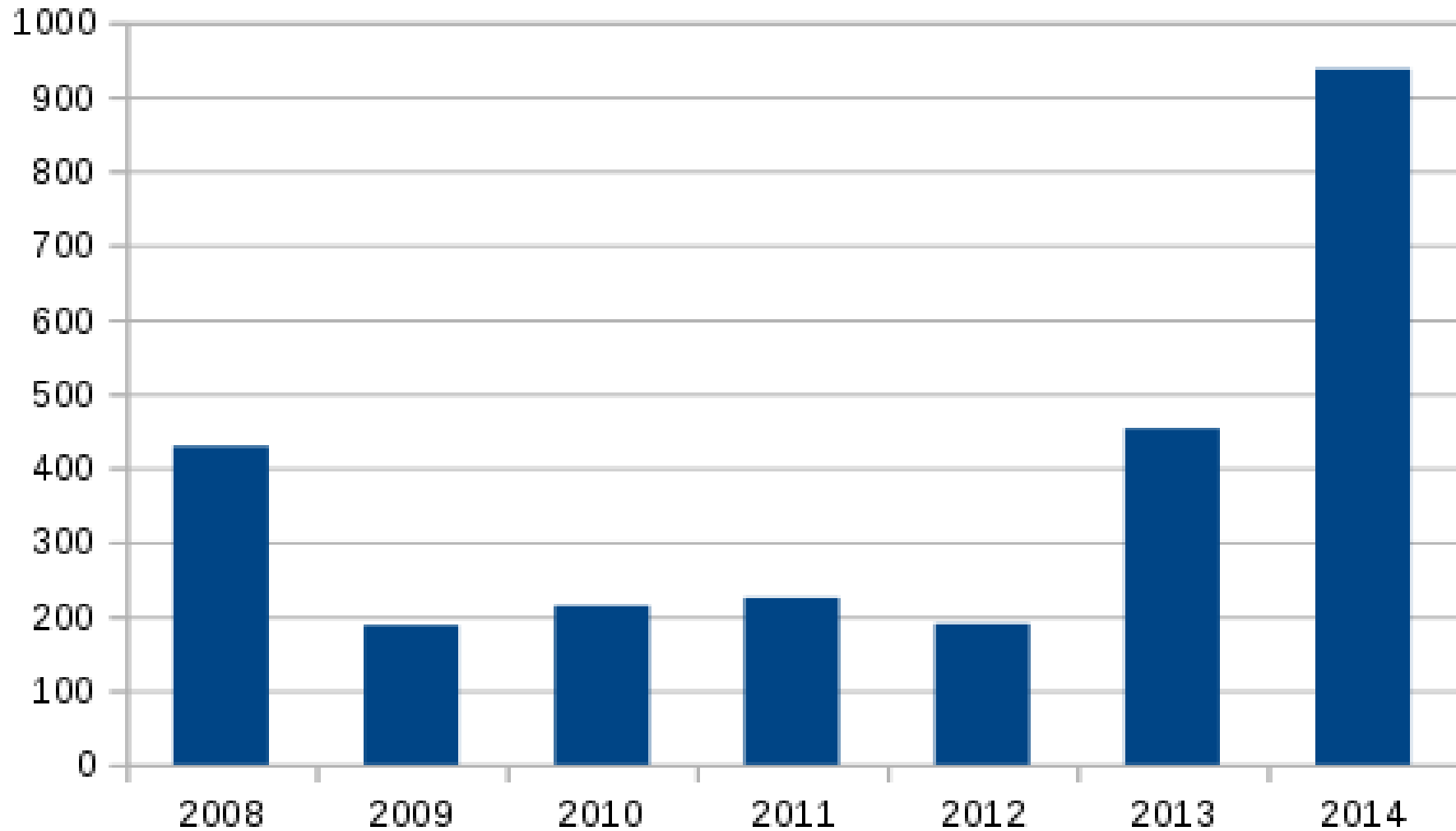
Domain browser

- New **registrant interface** into registry - https://domenovyprohlizec.cz

- Integration of **registry** and our identity service **mojeID** - https://mojeid.cz

  - MojeID is the internal registrar only for contacts

  - Data of those contacts are validated

  - Providing those contacts web authentication (password, ssl certificates, two factor authentication)

Domain browser

- Provided that we have validated registrant through mojeID service, we can offer him direct services of registry

  - Cross-registar view of owned objects (domains, nsset, keysets)

  - Direct access to auth info code necessary for transfer objects to other registrars

  - Possibility to merge the same contacts into one

  - **Registry object locking and unlocking**

Domain browser

Administrative locking

- Important part of the registry operations is **cooperation with Law Enforcement Agencies**

- New option in our registration rules is that **anybody can ask for temporary lock** with proper papers about ongoing dispute issued by appropriate court

- Used to be seldom activity done manually by CLI tools

- Increased occurrence demanded integration into web administration interface

- Implemented in FRED-2.16 (Jan 2013)

Administrative locking

- Almost any EPP request can be blocked

    - Transfer, Update, Delete, Renew

    - Appropriate status Server*Prohibited is shown in WHOIS together with new status ServerBlocked

    - Registrar will again receive "Object status prohibits operation" EPP response

- Domain can be deactivated as part of locking

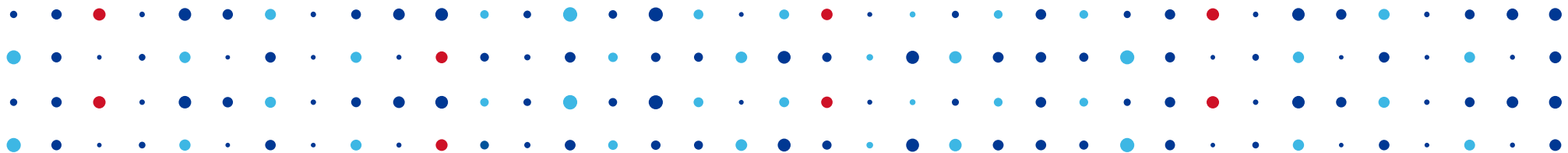- Locking can be bounded by time period

Administrative locking
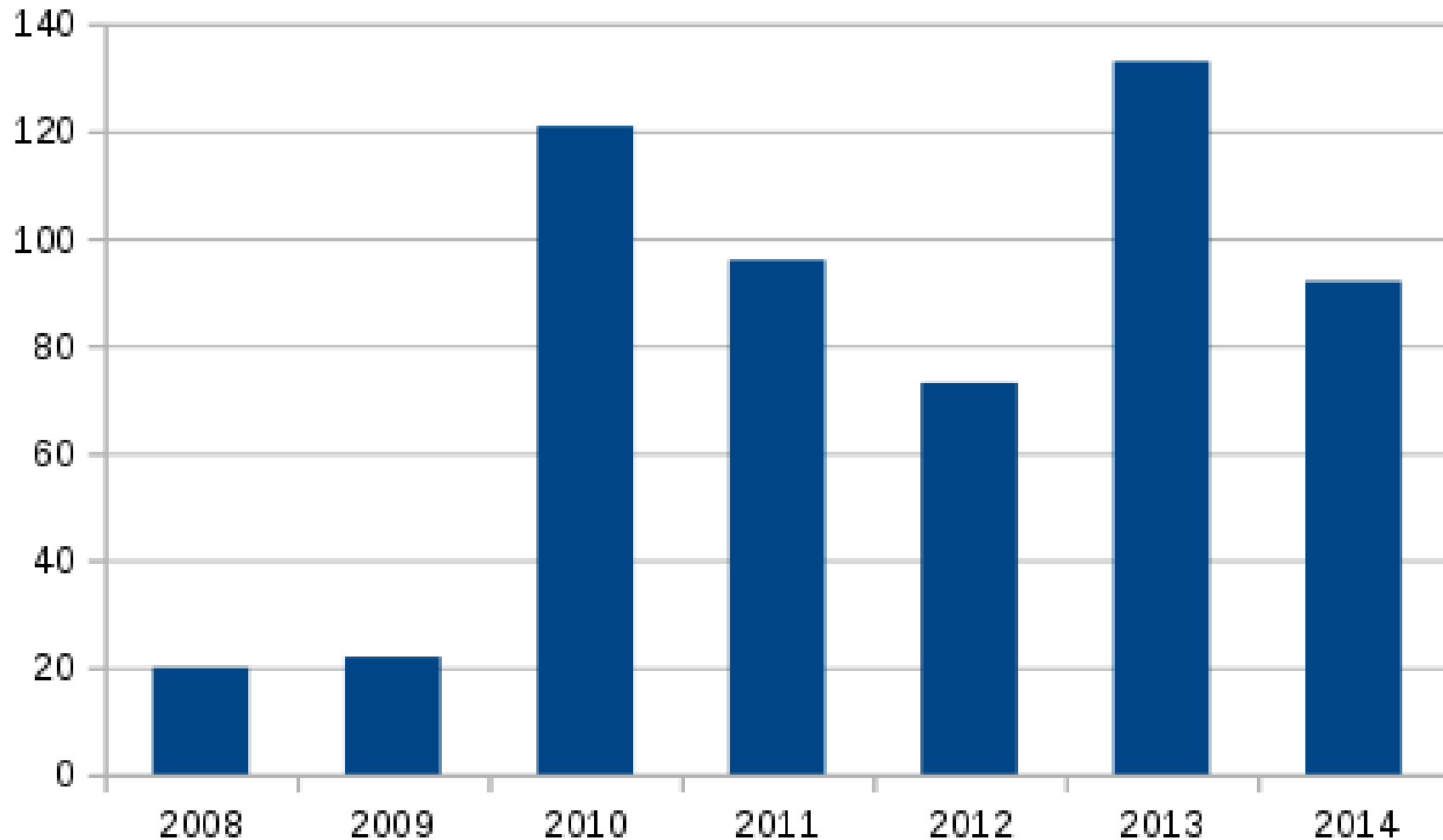
Conclusion

- Even in Registry-Registrar-Registrant model there are use cases for enhanced Registry-Registrant communication like **registry objects locking**

- There is not only **voluntary locking** requested by registrant but also **administrative locking** requested by LEA – both are supported in FRED

Thank You

Jaromir Talir • jaromir.talir@nic.cz