

9 years of integration of Domain Registry and Identity Provider

Jaromír Talíř • jaromir.talir@nic.cz • 18.10.2019

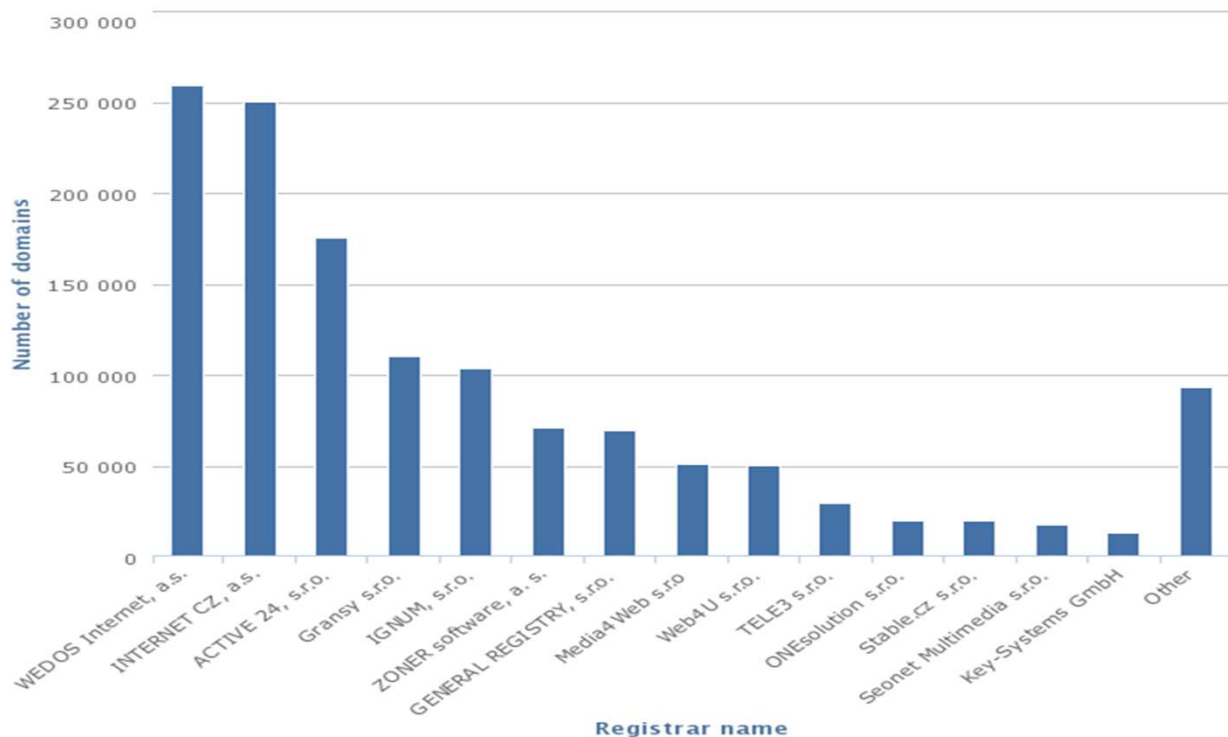
Who are we



- Domain registry for .CZ
- Association of legal entities (ISP's, some registrars, some registrants)
- Non for profit
- 1 328 708 domains
- **803 510** contacts (registrants, admin-c, tech-c)
- 45 registrars (28 CZ / 17 non CZ)

Registrars

2019-10-15



CZ.NIC – <https://stats.nic.cz/>

Problem of accuracy of contact data

```
domain:      myfakedomain.cz
registrant:  XYZ1
registrar:   REG-FRED_A
registered:  16.10.2019 11:41:09
expire:      16.10.2020
```

```
contact:     XYZ1
name:        Mickey Mouse
address:     Disneyland
address:     Paris
address:     12345
address:     FR
registrar:   REG-FRED_A
created:     16.10.2019 11:40:51
```

- Issue for trustworthiness of the registry
- Registrars should be responsible to verify contact data but it's registry who has to deal with problems

Problem of accuracy of contact data

- Proper verification is expensive
- Registration rules orders to remove domain registered to fake contact → registry must do verification
- One approach is random selection semi-automated verification
- Name and Address is published in WHOIS to support public control

Problem of accuracy of contact data

- Inaccuracy may be a result of duplication
- Shared registry allows to have single (well maintained contact) linked to many domains
- Simple de-duplication can be managed by registry

Idea

- Why not to give registrant an option to manage contact data directly with us? → *No more duplication*
- Why not to take care of proper verification of contact data by ourselves? → *We have much broader possibilities*
- Why not to provide some additional services to those who will subscribe? → *Single Sign On features*

mojeiD is born

- Production launch was in October 2010
- Can be viewed as „internal“ registrar only for Contact objects
- New user may immediately associate his account/contact with his domains
- It is possible to transfer existing contact to mojeiD
- Free for to both local and foreign users
- <https://mojeid.cz/registration>

Registration

CREATE NEW ACCOUNT

Prefill form with:

Google

facebook

Username:*

*Your mojeiD will have the format username.mojeid.cz
Use only lower case letters, numbers and a dash inside the username.*

First name:*

Last name:*

Email:*

The code PIN1 will be send to this email. You need it to activate your account.

Mobile phone:*

+420

The code PIN2 will be send to this phone. You need it to activate your account.

Mailing address

Street and number:*

City:*

Postal code:*

Country:*

Czech Republic

The code PIN3 will be send to this address. You need it to fully activate your account.

Transfer

CREATE ACCOUNT FROM DOMAIN REGISTRY

Handle:*

[Show data from registry](#)

Username:

Your mojeiD will have the format username.mojeid.cz

Use only lower case letters, numbers and a dash inside the username.

Control code:*



Retype the code from the image

☐ I agree with [the terms of service](#)*

NOTE: Once your account is activated, your sponsoring registrar in the domain registry will be updated.

Create an account

Verification of user provided data

- Mandatory check of e-mail and phone



- Optional check of postal address



- Optional full identity check by showing ID card



Identity check / Validation

- Personal visit in the office or contracted validation place
- Document stamped by notary and sent us via post
- Online via eGov project called Data Boxes
- Visit at governmental offices called Czech Point

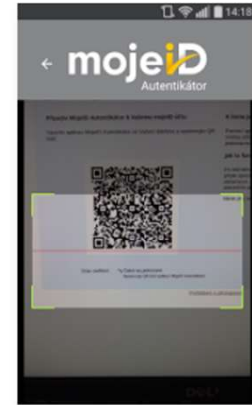


Authentication possibilities

- User always needs to set password
- Basic strength verification (zxcvbn library)
- Optional two factor authentication
- X509 certificate + key
- Password + One Time Password
- TOTP - RFC6238
- Google Authenticator, Authy, etc...

Authentication possibilities

- Password + confirmation by a click in mobile app
- mojeiD Authenticator
- Shared key exchanged via QR
- Challenge is sent via GCM/FCM
- Signed response is sent back
- Introduced in March 2016
- Google launched similar service in June 2016

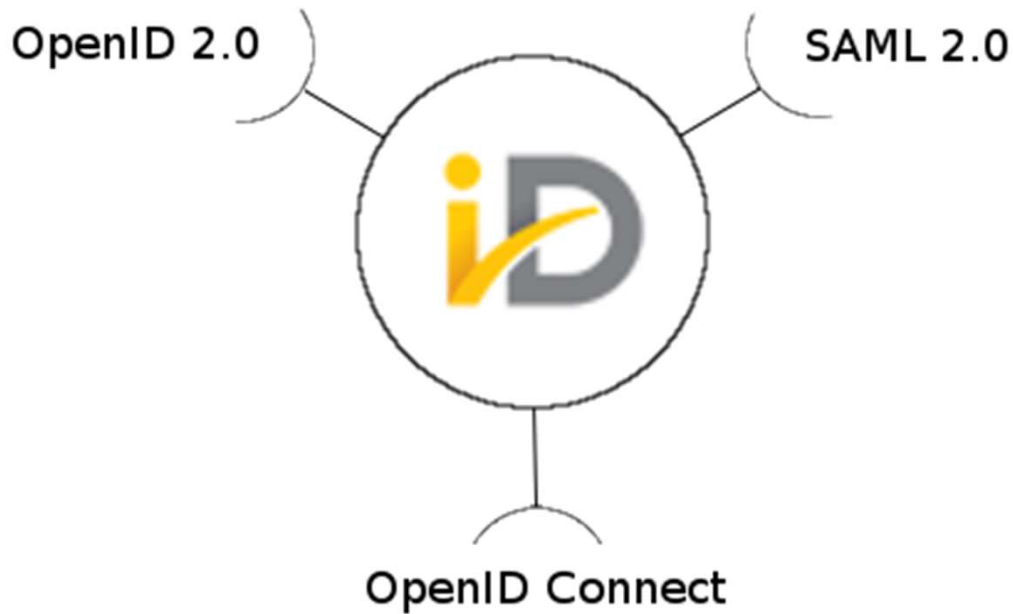


Authentication possibilities

- Password + FIDO 2 device
- Recent standard with a big uptake over the last year
- Still in testing phase



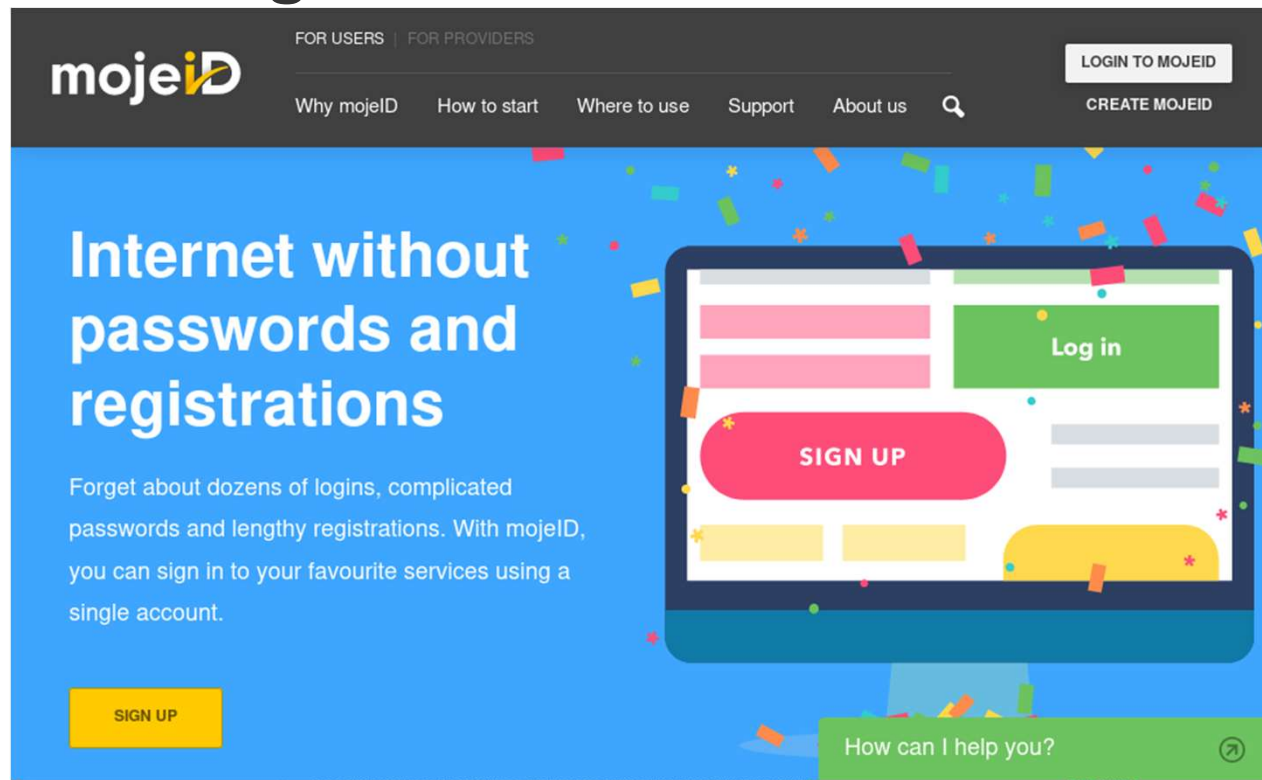
Single Sign On




Authentication protocols

- **OpenID 2.0** – 2010
 - Still used by majority of service providers
- **SAML 2.0** – 2014
 - Mainly academical and gov service providers
 - eduID, STORK, eIDAS
- **OpenID Connect** – 2015
 - Support migration from OpenID 2.0

How to get users

The image is a screenshot of the mojeiD website's homepage. The background is a vibrant blue, decorated with falling confetti in various colors like pink, orange, green, and yellow. On the left side, the text 'Internet without passwords and registrations' is written in a large, white, sans-serif font. Below this, a smaller white paragraph explains the service: 'Forget about dozens of logins, complicated passwords and lengthy registrations. With mojeiD, you can sign in to your favourite services using a single account.' At the bottom left of this section is a yellow rectangular button with the text 'SIGN UP' in black. On the right side, there is a stylized illustration of a laptop screen. The screen displays a simplified login and registration interface with pink input fields, a green 'Log in' button, and a large pink 'SIGN UP' button. Above the laptop, there are more confetti elements. At the bottom right of the page, there is a green chat bubble containing the text 'How can I help you?' and a circular icon with a question mark. The top of the page features a dark grey navigation bar. On the left of this bar is the mojeiD logo. To its right are links for 'FOR USERS' and 'FOR PROVIDERS'. Further right are links for 'Why mojeiD', 'How to start', 'Where to use', 'Support', and 'About us', followed by a magnifying glass icon. On the far right of the navigation bar are two buttons: 'LOGIN TO MOJEID' and 'CREATE MOJEID'.

How to get service providers



FOR USERS | FOR PROVIDERS

Why MojeiDOptions and pricesGetting startedAbout us


LOGIN TO MOJEID

CREATE MOJEID

Verified users for your site

Say goodbye to fake accounts, wrong telephone numbers and non-existent addresses. MojeiD users are verified by us, so you always know who's on the other side.

SET UP MOJEID



How can I help you?

Two options for service providers

- Any service provider can join for free with limited access – 1000 service providers
- No access to information about verification status of a user
- Service provider can sign contract to get full access – 400 service providers
- ~40 EUR/year, exceptions for academia, registrars, etc...
- Pre-selected checkboxes in consent dialog

Motivation program

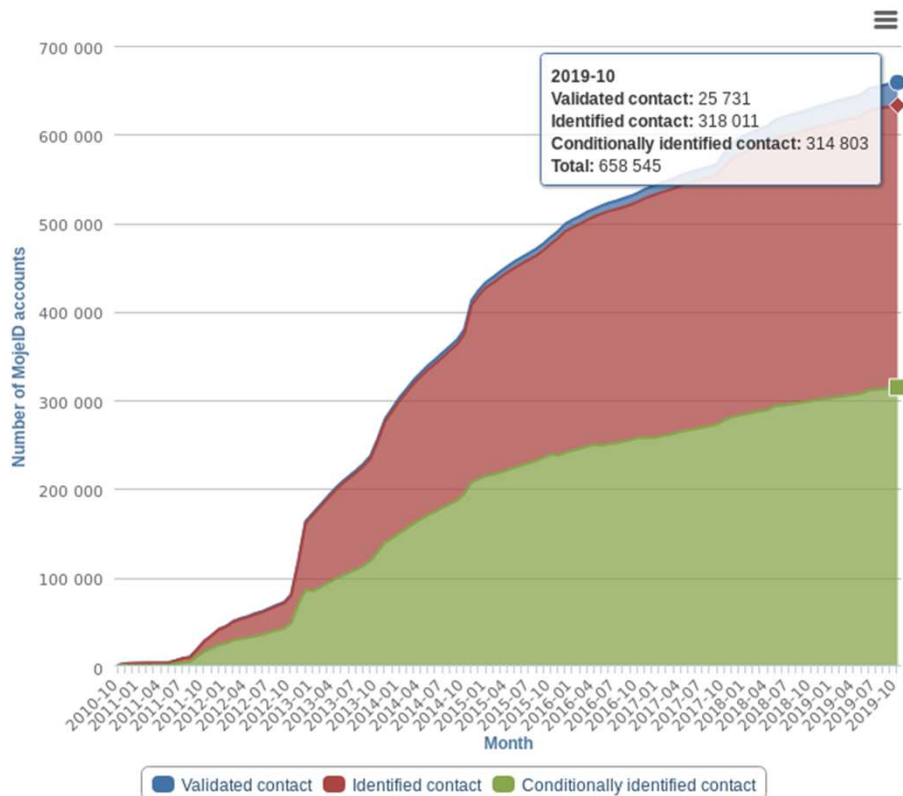
- Motivation for service providers to outsource user account management to mojeiD and implement Single Sign On with mojeiD
- We provided API to transfer user data from service provider to mojeiD
- Monthly payment for new accounts created
- Program stopped several years ago

Catalogue <https://www.mojeid.cz/en/where-to-use/>

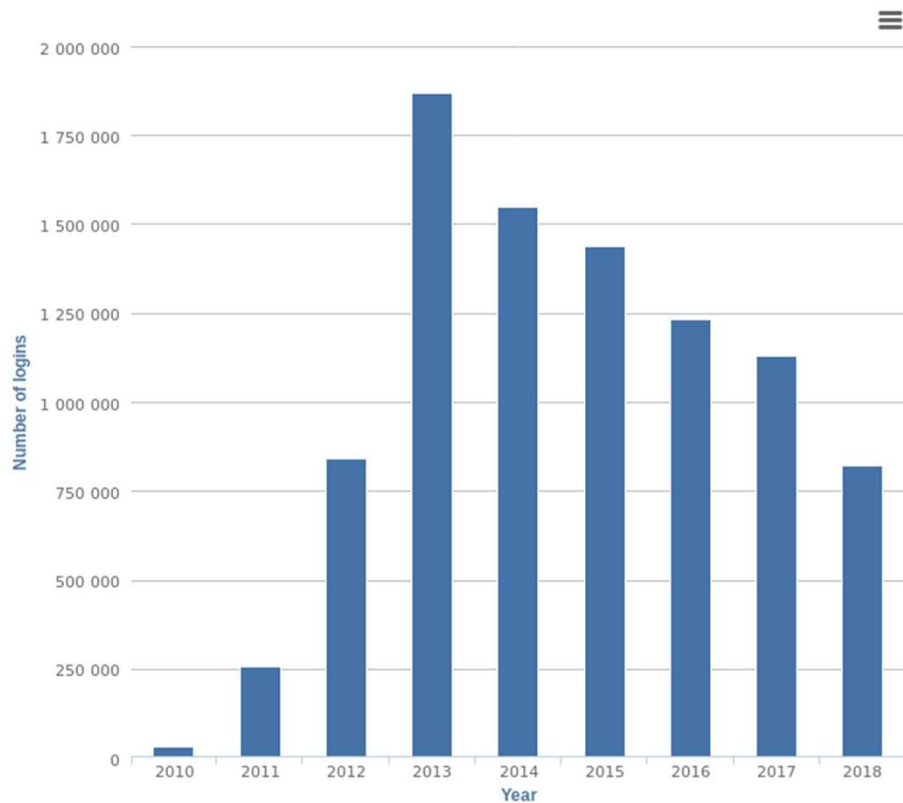
Accounts <https://stats.nic.cz/stats/>

FROM 2010-10 TO 2019-10



Logins <https://stats.nic.cz/stats>

FROM 2010 TO 2018




Participation of registrars

- There is 13 out of 45 registrars who implemented „Login with mojeID“
- Many of them participated on motivation program
- If they know who is the user they don't need additional authorization for domain changes






























Registrars list <https://www.nic.cz/whois/registrars/>

 Registrar supports secured domains DNSSEC

 Registrar supports mojeID

 Registrar supports IPv6


 Registrar Certified for Retail

Registrar	Website	Technologies	Certification
ACTIVE 24, s.r.o.	www.active24.cz	  	★★★★★
INTERNET CZ, a.s.	domeny.fornpsi.cz		★★★★★
IGNUM, s.r.o.	www.domena.cz	  	★★★★★
GENERAL REGISTRY, s.r.o.	www.domainmaster.cz	 	★★★★★
Web4U s.r.o.	www.spravadomen.cz	  	★★★★★
Stable.cz s.r.o.	kvapem.cz	  	★★★★★
WEDOS Internet, a.s.	www.wedos.cz/		★★★★★
ZONER software, a. s.	www.regZone.cz	  	★★★★★
KRAXNET s.r.o.	www.xnet.cz	  	★★★★★
ONesolution s.r.o.	www.onebit.cz/domeny/	 	★★★★★
TELE3 s.r.o.	www.tele3.cz	  	★★★★★
e-BAAN Net s.r.o.	www.banan.cz	 	★★★★★
TERMS a.s.	www.thosting.cz/		
MarkMonitor Inc.	www.markmonitor.com/		
OVH, Sas	www.ovh.cz		
O2 Czech Republic a.s.	www.o2.cz/domena		

Participation of registrants

- There is only ~ 40 000 users linked to a domain
- After address verification, they can **hide address** in WHOIS/RDAP
- They can take advantage of **registrant portal**
- Cross registrar overview of domains
- Registry lock
- Authinfo discovery
- Merge duplicates

Registrant portal <https://www.domenovyprohlizec.cz>



AboutFeaturesContactČesky

An overview of your CZ domains in one place

Login with mojeiD

Sign up to mojeiD
Why mojeiD?

Můj kontakt

<https://www.domenovyprohlizec.cz/mycontact/detail/>

Moje domény Moje sady jiných serverů Moje sady klíčů Můj kontakt nápověda

Můj kontakt HANDLE-ERX033

Osobní údaje

Celé jméno	Hana Procházková	✓ Všechno
Organizace		✓ Všechno
Typ identifikace	id	✓ Všechno
Identifikační údaj	4372272054	✓ Všechno
DiC		✓ Všechno
Telefon	+420 649127300	✓ Všechno
Fax		✓ Všechno

Moje domény

Pro provedení změn musí být kontakt identifikován nebo validován [přijez p validaci /aktu mojeiD/](#)

Zobrazeno od 21 do 40 ze 165 záznamů

Přidat na vybrané položky

Doména	Stav	Následující stav	DNSSEC	Role	Registrátor
domaintroveset.cz.ne	Je navrženo na další záznam v registru. Není povolená změna údajů. Není povolená změna určeného registrátora. Doména je blokována.		✗	Držitel	ignum
domena.netyla.state	Je navrženo na další záznam v registru. Není povolená změna údajů. Není povolená změna určeného registrátora. Doména je blokována.		✓	Držitel	Tester f. 2

Cross-border EU cooperation
















- EU pilot project STORK
- 2009-2011 & 2012-2015
- mojED was the only nationwide IdP
- EU Login uses mojED
- Connectis (NL) is service provider connected to mojED

ec.europa.eu requires you to authenticate

Log in with your eID

Please select your country of origin

This is a demonstration Pilot. Authentication is performed by the individual countries on a voluntary basis, therefore service availability is not guaranteed. The Live service will be rolled out in 2017 within the scope of the [eIDAS regulation](#).

<input type="radio"/>  Austria	<input type="radio"/>  Belgium	<input type="radio"/>  Czechia
<input type="radio"/>  Estonia	<input type="radio"/>  Iceland	<input type="radio"/>  Italy
<input type="radio"/>  Latvia	<input type="radio"/>  Lithuania	<input type="radio"/>  Luxembourg
<input type="radio"/>  Portugal	<input type="radio"/>  Slovakia	<input type="radio"/>  Slovenia
<input type="radio"/>  Spain	<input type="radio"/>  Sweden	<input type="radio"/>  Switzerland

Cross-border EU cooperation

- eIDAS network launched on 29. 9. 2018
- Network of interconnected SAML gateways
- CZ.NIC operates production instance of Czech gateway for (2018-2020)
- Participation on eIDAS Technical SubGroup that defines eIDAS protocol
- New version has just been published that allows participation of **non-notified eID schemes**

• <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile>

Cross-border EU cooperation

Choose your country to proceed with authentication



Germany

Service provided by CZ.NIC, CZ domain registry.

cz.nic

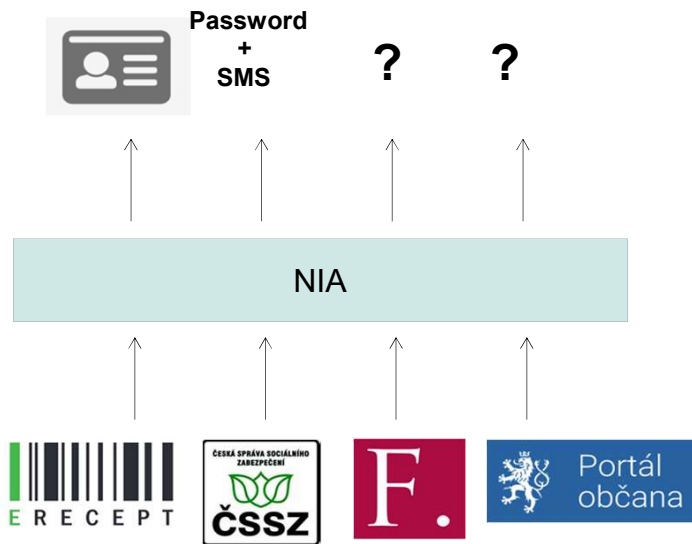
mojeiD

Cross-border EU cooperation

- EU commission is regularly funding projects that extends eIDAS network
- Joint project of CZ, EE, DK, NL, Connectis and CENTR to fund integration of registry interfaces into eIDAS network
- Submitted in May
- Decision will be published at the end of October

eID in Czech Republic

- New eID governmental project launched in July 2018



eID in Czech Republic

- We are working to fulfill all requirements to become accredited Identity Provider
- Strong authentication tied with strong identity verification is a MUST
- Discussion with government about Level Of Assurance of our identity service

mojeID and ID4me

- ID4me is a protocol, mojeID is a service – more similar to DENIC-ID
- 2 in 1 (Identity Authority & Identity Agent)
- We published ID4me DNS record for all mojeID users
- Wherever you see **Login with ID4me**, just fill **mojeid.cz**
- Could we server other Identity Agents? Not sure

Future?

- Integration with eGovernment
- More integration into registry
- RDAP service with mojeID authentication?
- Better marketing towards registrars?

Thank You

Jaromír Talíř • jaromir.talir@nic.cz • www.mojeid.cz

