



RegelD

Using eIDAS to verify identity of registrants

RIPE 84 – Berlin – 20. 5. 2022

Jaromír Talíř – CZ.NIC



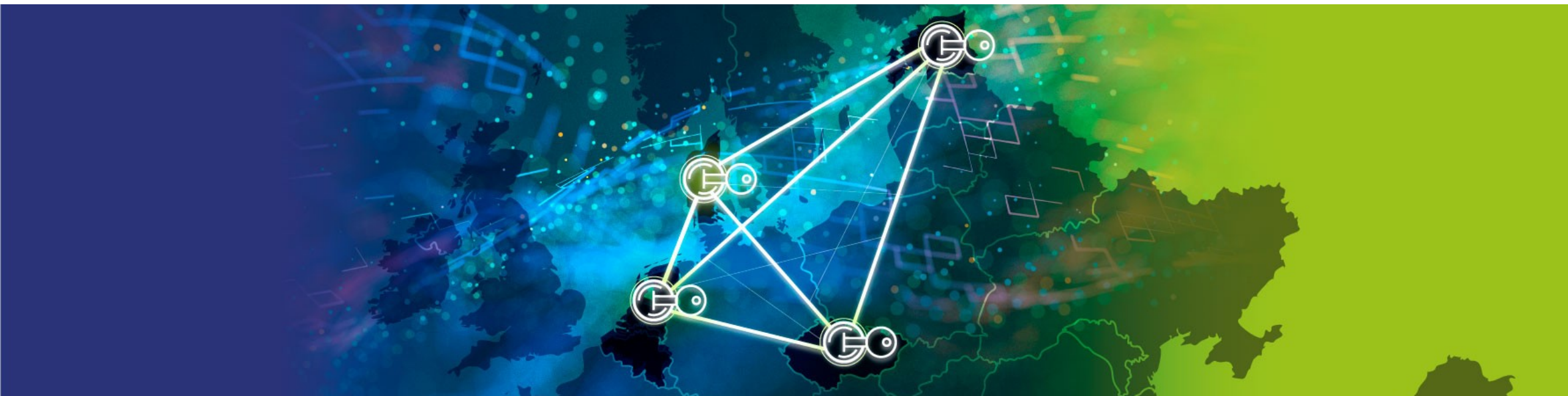
Co-financed by the Connecting Europe
Facility of the European Union

Digital identity (eID) is on the rise. It provides possibility of remote trustworthy identification to other party. But is it already usable? The demand to properly verify owners of the registry resources is growing (TLDs, RIRs,...). The group of ccTLDs took a chance to explore the possibility of using digital identities available via the eIDAS network as part of RegeID project co-funded by EU grant.

Agenda

- What is the eIDAS
- Description of RegeID project
- Research output
- Implementation showcase from CZ registry
- Summary of challenges
- Conclusion

What is the eIDAS network



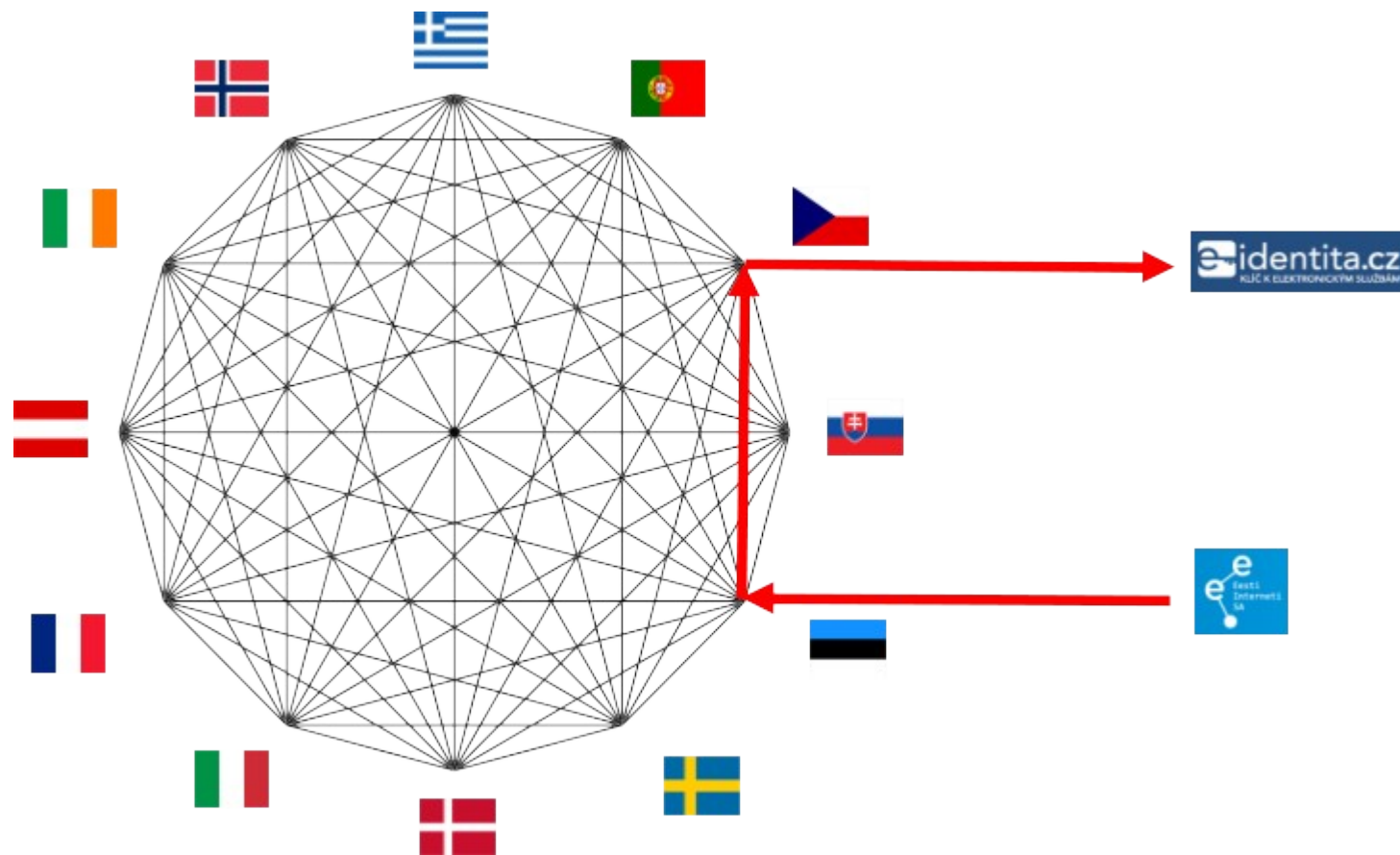
eIDAS regulation (eID part) - 910/2014

- The cross-border recognition of governmental eIDs in EU (EEA)
- Mandatory for all public online services that require strong authentication since September 2018
 - Access of private services is left on decision of national legislation
- Introduces concept of “Levels of assurance” that encapsulates strength of the eID mean and strength of verification during issuance
 - Low, Substantial and High
- Defines mandatory and optional attributes of natural and legal persons
- Describes process of notification of eID that includes peer review of all technical and procedural aspects of notified eID

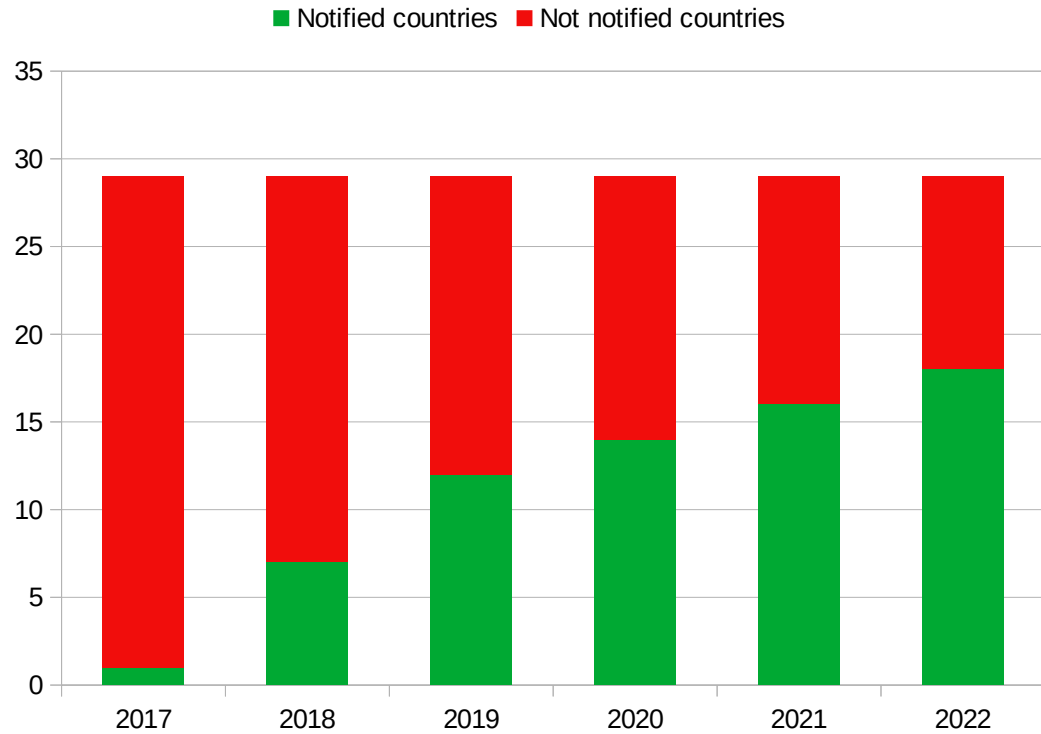
The eIDAS network

- The network of eIDAS nodes deployed in EU countries
 - Notified eID means are connected to the nodes to provide authentication
 - Online services are connected to the nodes to request authentication
- Interoperability is achieved by defining SAML2 profile as the protocol between nodes
- The policy requirements and technical requirements for connecting services is different in each country

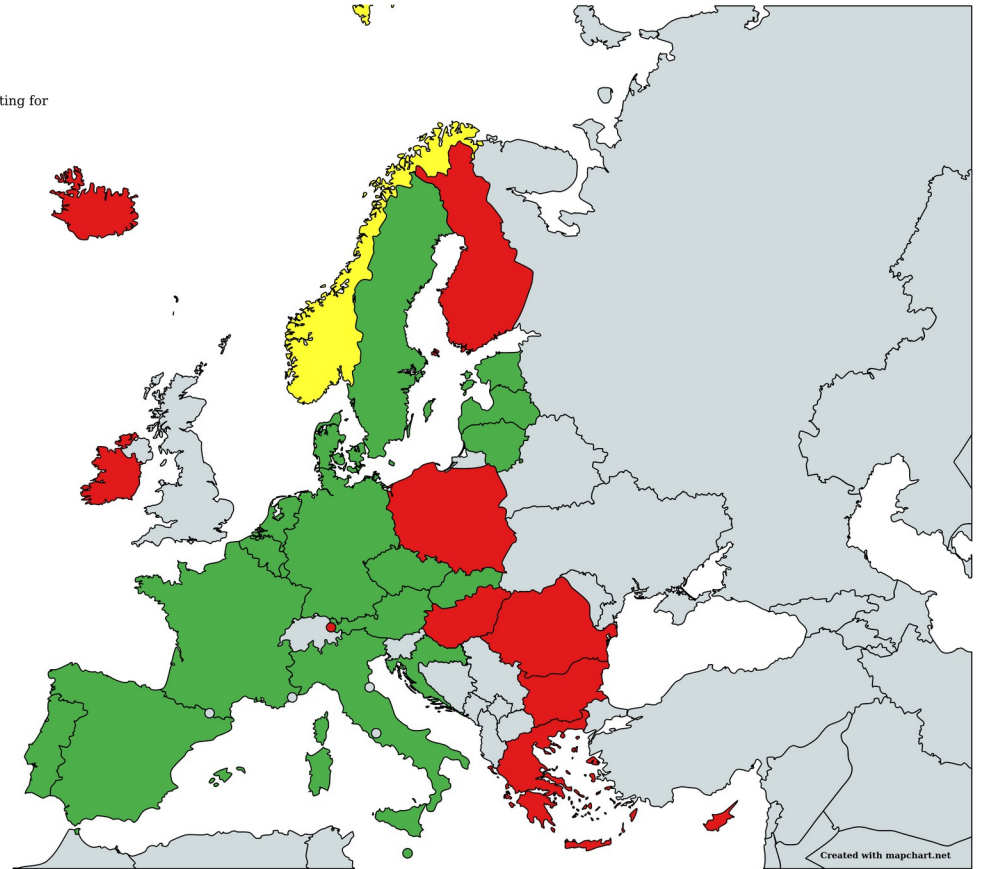
The eIDAS network



Notified countries



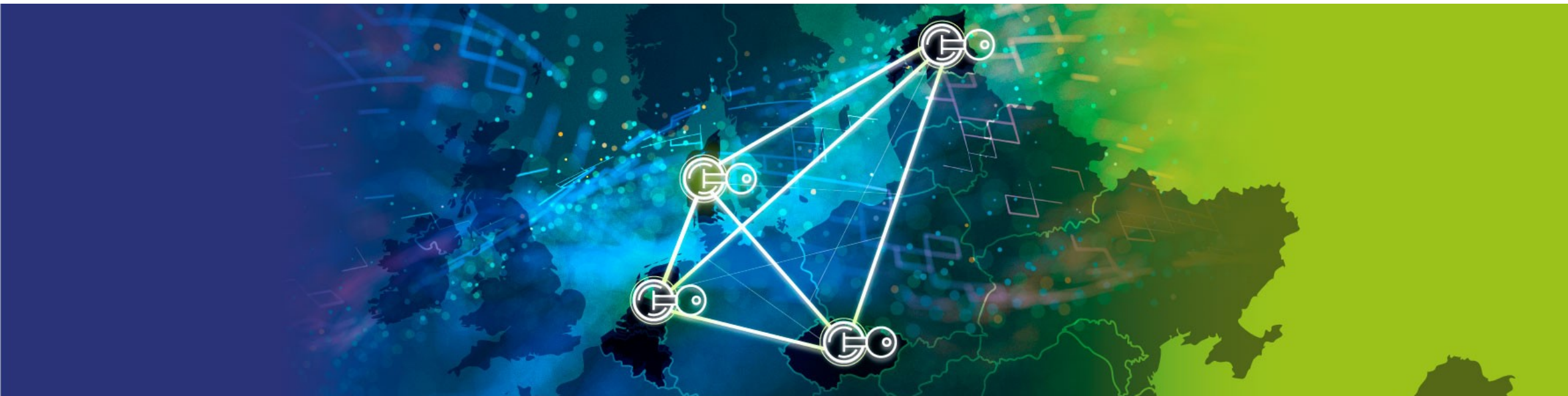
■ 18 Notified
 ■ 1 Peer reviewed, waiting for notification
 ■ 10 Not notified



Revision of eIDAS regulation

- First draft announced in June 2021
- Introduces concept of European Digital Identity Wallet to store identity, attributes and credentials for online and offline use
- Decentralized rather than current centralized approach
- Should be mandatory not just for public sector but also for big platforms and private services that require strong authentication (i.e. banks)
- Legislative process and technical solution is being developed in parallel and some outputs should be available by the end of 2022
- Not related to our project

Description of RegelID project



Grants of European Commission

- CEF Telecom funding in programming period 2014 – 2020
- Almost every year there was a call for projects
 - Main objective: *“Integrating the eID DSI (Digital Service Infrastructures) in existing e-services/systems/online platforms in various public or private sectors”*
 - 75% funding
- Consortium of several companies submitted response to the call under the name “RegelD”
- First submission in 2018 failed
- Second submission in 2019 succeeded

Project partners



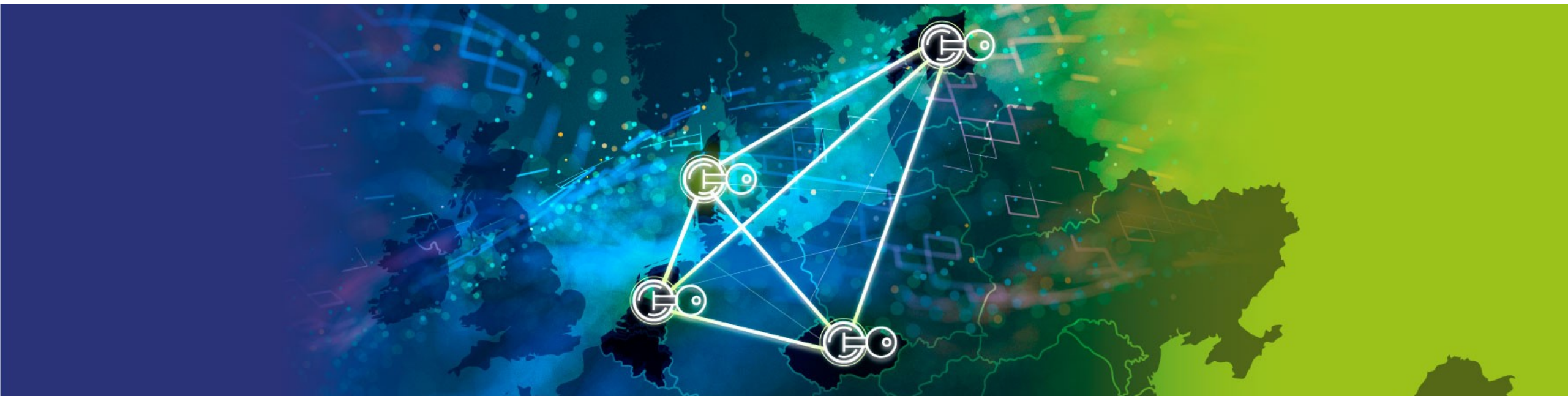
Scope

- Connect registrant facing portals to the eIDAS network and implement linking of eIDAS identity with the contacts in the registry
 - CZ.NIC, EIS, DK Hostmaster, SIDN
- Research and analysis of potential usage by other registries and registrars
 - Signicat
- Dissemination of project goals and achievements in domain industry
 - CENTR

Results

- Visual identity and the website <https://regeid.eu>
- Video explaining eIDAS and it's potential for DNS industry
- Research done and comprehensive report submitted to grant agency
- Registrant portals connected to eIDAS network
 - <https://registrant.internet.ee/>
 - <https://www.domenovyprohlizec.cz/>
 - <https://self-service.dk-hostmaster.dk/>
- SIDN's solution is in pre-production at the moment

Research output



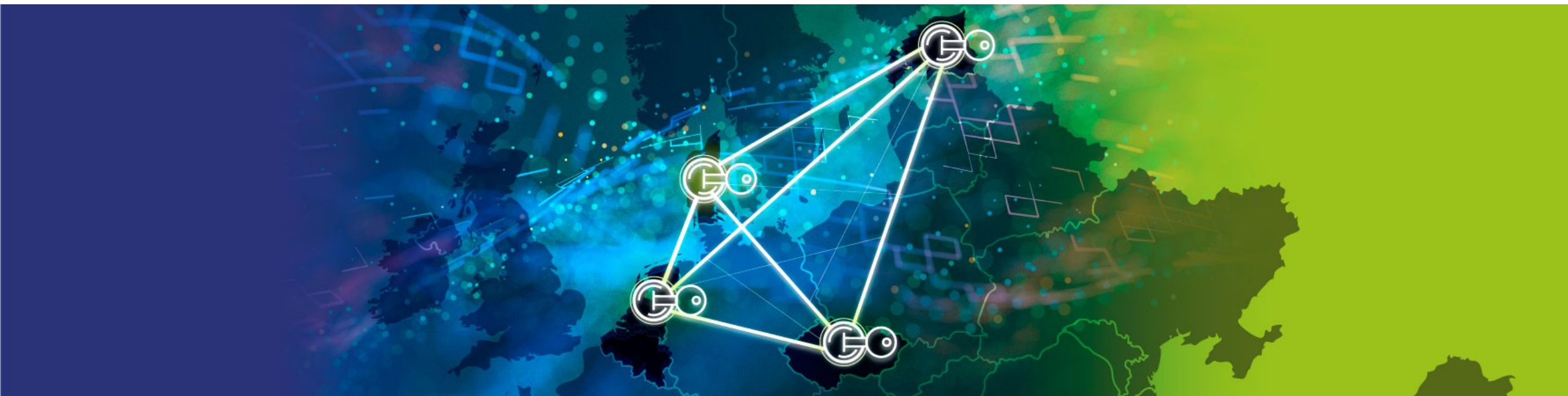
Findings on survey for registries

- Registries find it important to verify registrant data
 - but they have limited opportunities to do so
 - relying heavily on paper-based procedures
- Registries able to use national eIDs for registrant verification have better options to do so in less cumbersome way
- Vast majority of registries would welcome the opportunity to accept verified, trustworthy eIDs
- Some concerns that still need to be addressed:
 - Limited availability of identities for legal entities
 - Registrants residing outside of Europe

Findings on survey for registrars

- Registrars are very mixed bunch
 - Often embedded in variety of broader services
- Most of them operate on international (global) scale so they want solutions that are standardized and easily usable
 - for all of their customers
 - with all of their services (and TLDs they represent)
- Registrars don't regard themselves as (primarily) responsible for validation of domain registration data, but acknowledge their part in ecosystem for securing against fraud and abuse
- Cost and complexity is major issue for registrars

Showcase from .CZ registry




Implemented changes

- CZ.NIC maintains open source registry <https://fred.nic.cz> used by ~10 other TLDs
 - New database tables and APIs to maintain link between contact and eID
- The DomainBrowser is primary registrant portal
 - Long standing features:
 - Overview of all domains registered to authenticated user
 - Setting Registry Lock on domains
 - Merge duplicate contacts
 - See the DNS traffic on user's domains
 - Authentication part was updated to include connection to eIDAS network



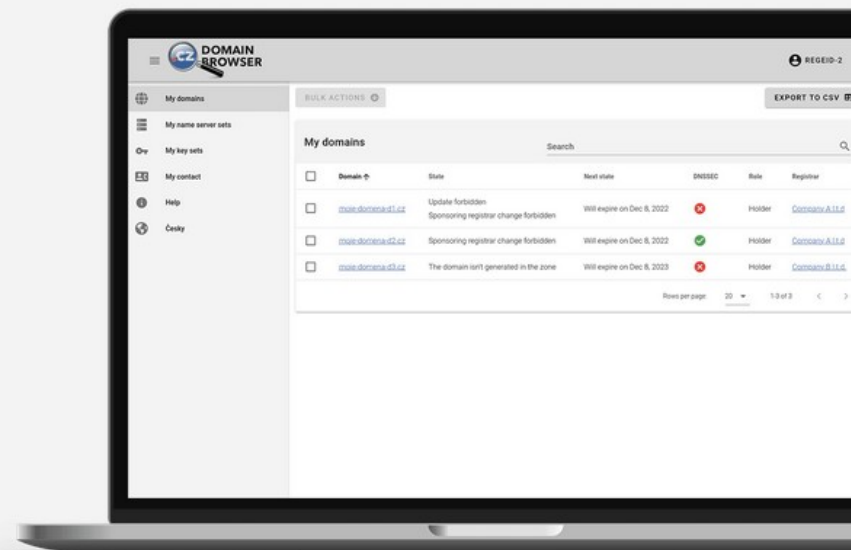
An overview of your CZ domains in one place

Domain browser is a web application used to display data from the CZ domain registry. It is directly linked to a mojID account or a national electronic identity (EU eID). National electronic identity can be used by citizens of EU member states (except for Czech Republic) to log in.

Login with mojID 


Login with EU eID 

[Register mojID account](#)



If your mojID account or national electronic identity is attached to a domain as a holder or an administrative contact, you can use the Domain browser to:


Choose your country to proceed with authentication


 Germany

 Sweden

 Greece

 Italy


 Austria


 Belgium

 Cyprus


 Denmark

 Estonia

 France

 Ireland


 Croatia

 Hungary

 Iceland


 Latvia

 Lithuania

 Luxembourg

 Malta

 Netherlands

 Norway

 Poland

 Portugal

 Slovenia

 Slovakia


 Spain

[Svenska](#)

Choose from available eID services

The following eID providers can be used for secure identification.

 Freja eID Plus

 Sweden Connect Reference IdP

Why is my eID not supported? ▼

[Cancel](#)

[Svenska](#)

Sweden Connect Reference IdP

Swedish Citizen Adapter requests your authentication. Select the person to authenticate as from the list below.

Magdalena Karlgren (194606109108) ▼

[Advanced >>](#)

Select assurance level for the authentication:

<http://id.elegnamnden.se/loa/1.0/eidas-nf-sub> ▼

Authenticate

What is the Sweden Connect reference IdP? ▼

I'm debugging my SP and need to look at the IdP logs ... ▼

[Svenska](#)

Verify your identity data

I approve that the following information is sent for secure identification.

Magdalena Karlgren
1946-06-10
International ID:
SE/CZ/194606109108

Approve

[Cancel](#)



Please give consent to provide the following details for Service provider -
CZ.NIC, z. s. p. o. (<https://domainbrowser.regtest.nic.cz/saml2/metadata>)

Claims for which a consent may be refused

Name	Magdalena	<input checked="" type="checkbox"/> Provide details
Date of birth	1946-06-10	<input checked="" type="checkbox"/> Provide details
Surname	Karlgren	<input checked="" type="checkbox"/> Provide details


Show values of the optional claims.


I give PERMANENT consent

I give ONE-TIME consent


I do NOT give consent

You log in with an electronic identity that is not attached to any contact in the domain registry. To attach it, enter the contact's identifier and transfer password (authinfo). This information should be available on the contact's registrar portal. The details of the contact in the registry must match the electronic identity details. The name must be **"Magdalena Karlgren"** and the date of birth **"1946-06-10"**, otherwise attaching the identity to the contact cannot be completed.






Domain Browser and the mojID service are operated by CZ.NIC, CZ domain registry. If you have any questions concerning the Domain Browser or mojID, do not hesitate to contact us +420 222 745 111 and podpora@nic.cz.

×  **DOMAIN BROWSER** DEMO-CONTACT

My domains My name server sets My key sets My contact Help Česky

BULK ACTIONS EXPORT THE ENTIRE LIST TO CSV

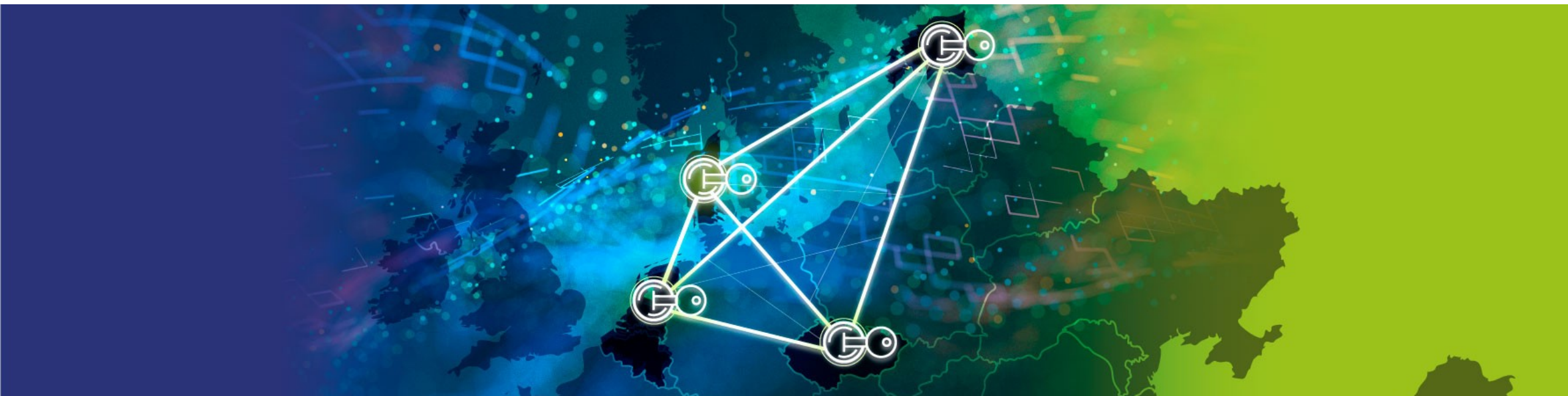
My domains

<input type="checkbox"/>	Domain	State	Next state	DNSSEC	Role	Registrar
<input type="checkbox"/>	demo-contact-domain.cz	The domain isn't generated in the zone	Will expire on May 19, 2023		Holder	Company A Ltd

Rows per page: 20 1-1 of 1

[cz.nic](#) [MojeID](#) [How to use the Internet](#) [Publications](#) [Don't be afraid of the Internet](#) [Academy](#) [Good Domain](#) [CSIRT.CZ](#) [Turris](#) [IDN](#) [How DNS works](#) [Domain Browser](#) [Web Scanner](#) [Tablexia](#) [Datovka](#) [more](#)

Project challenges



Access to eIDAS node

- Every country has different rules and requirements to get access and mostly it is opened only for governmental organizations (liability reasons), but there can be exceptions
 - DK Hostmaster operates under the “domain act” that requires them to verify identities.
- Most of TLDs are non-governmental organizations, so the access is rather an exception
 - Before the grant was submitted, appropriate national agencies had to approve the access to the node
- With this respect, NIS2 legislation and its verification requirements may be the opportunity to get access to fulfill these requirements

Selection of proper Level of Assurance

- This is up to each service provider to decide
- It would be great to agree on the same level
- Balance between required authentication strength and availability of means should be considered
 - In DK, almost everybody has NemID, but it is only on Substantial level
- Participants agreed to require Substantial level

Natural and legal persons

- Even though regulation defines attributes of legal person, it is almost not used
- Only two eID schemes notified offer these attributes
 - Netherlands (eHerkenning)
 - Austria
- Participants concentrated only on natural persons

Insufficient identity data for matching

- Mandatory data are CurrentFirstName, CurrentGivenName and DateOfBirth and unique PersonIdentifier
 - This is not enough for automated matching
- CurrentAddress is optional
 - Only about half of countries declare they provide this attribute
 - It is structured attribute based on Core ISA Vocabulary CvAddressType
 - Thoroughfare, PostName, PostCode, LocatorDesignator, AdminUnitFirstline, AdminUnitSecondLine, CvAddressArea, POBox
 - Different countries provide different subsets
- Participants decided not to rely on CurrentAddress and keep it for the potential future update

Identity matching procedure

- Participants explored and implemented different approaches how to match identity data with contact in the registry
 - Using PersonIdentifier provided via registrar as part of registration data
 - The issue is that users usually doesn't know it's identifiers
 - Using registry authorization code (authinfo)
 - Potentially together with check for other data (name, surname, date of birth)
 - Using some pre-existing authentication
 - Using verification links and manual checks

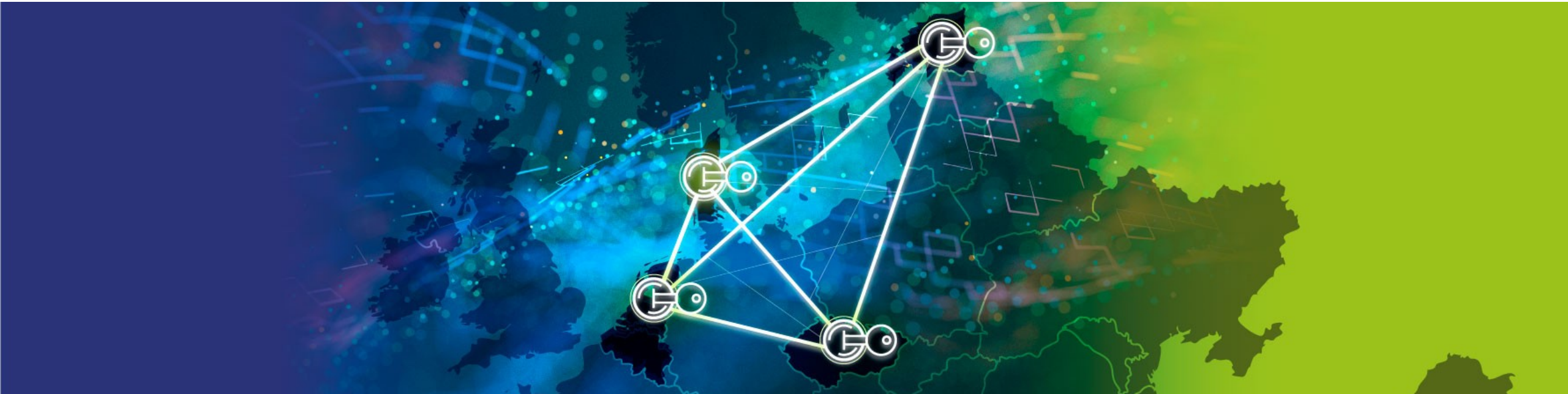
Updating linked contacts

- When identity is linked to contact in registry it is preferred that verified contact data are not changed via registrar
- Contact could be “taken” from registrar and maintained by registry but this would break registry-registrar responsibilities in many ways
- Rather dedicated status as “ServerUpdateProhibited” is used to indicate to registrars that this data cannot be changed.
- Contact data can be updated from eID with every authentication and registrars can be informed by registry about such update

UX/UI aspects

- It is clear, that working with cross border authentication is not easy from user experience perspective
 - Multiple parties are involved in the single authentication transaction
 - Lot's of redirects on the way
 - Different UI experience in every country
 - Hard to trace failures
- There are some efforts on EU side to help, but it's not mandatory to take it
 - New logo for eIDAS authentication
 - UX guidelines

Conclusion



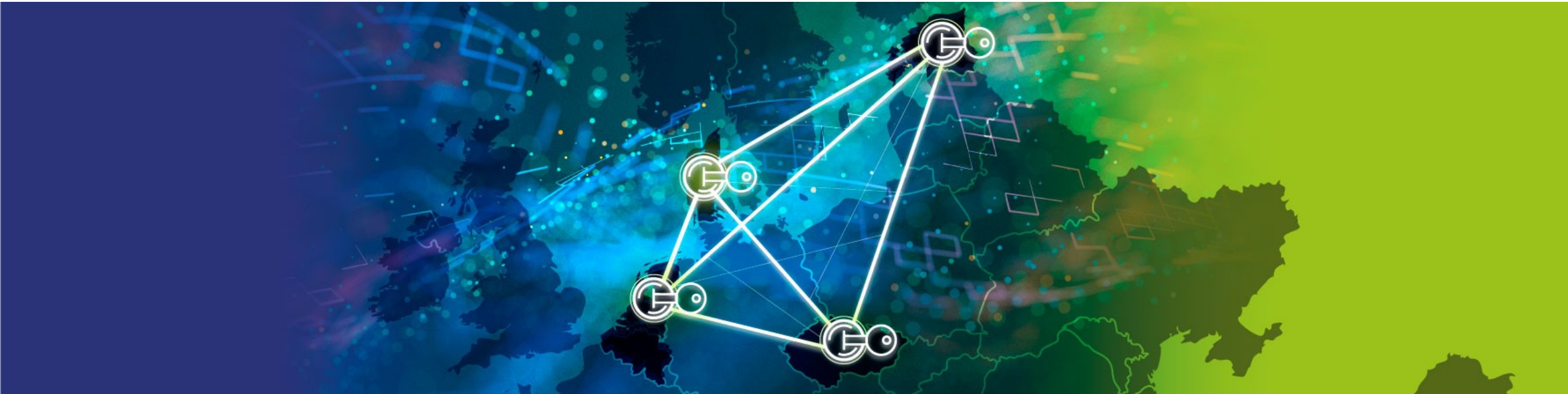
Conclusion

- Does eIDAS provides generally usable solution without any caveats? Not yet
- Do not hold your breath while waiting for EUDI Wallet, it can take some time
- Still current eIDAS can be useful tool if you accept all limitations
- We have created infrastructure that we can build on
 - For example we can offer this possibility when asking some suspicious contacts to verify

Thank you

Jaromir.talir@nic.cz

Backup slides



Testing instance

- It is possible to connect to testing instance of FRED as the registrar. More information about the testing instance here, documentation for the client communication is here

```
$ wget -q https://www.nic.cz/files/fred/fred-client-openinstance.zip
$ unzip -q fred-client-openinstance.zip
$ cd fred-client-openinstance/
$ ./fred-client
FredClient 2.13.0
Type "help", "license" or "credits" for more information.
```

```
Using configuration from data_files/conf/fred/fred-client.conf
Connecting to demo.regtest.nic.cz, port 700 ...
Connected!
```

```
REG-FRED_A@demo.regtest.nic.cz>
```


Registration of sample contact and domain

```
REG-FRED_A@demo.regtest.nic.cz> create_contact DEMO-CONTACT 'Magdalena
Karlgrén' mail@example.com Street City 12345 SE NULL '' myauthinfo --
ident.number="1946-06-10" --ident.type="birthday"
Do you really want to send this command to the server? (y/N): y
Contact ID: DEMO-CONTACT
Created on: 2022-05-19T00:01:33+02:00
```

```
REG-FRED_A@demo.regtest.nic.cz> create_domain demo-contact-domain.cz
DEMO-CONTACT
Do you really want to send this command to the server? (y/N): y
Domain name: demo-contact-domain.cz
Created on: 2022-05-19T00:01:54+02:00
Expiration date: 2023-05-19
```

Linking contact and identity in DomainBrowser

- Go to <https://domainbrowser.regtest.nic.cz/>
- Select Login with EU eID
- Select Sweden
- Select Sweden Connect Reference IdP
- Select Magdalena Karlgren
- Approve all consents
- In the DomainBrowser fill handle "DEMO-CONTACT" and authinfo "myauthinfo" or whatever you have registered on previous slide