tnc23
DIGITAL GENERATIONS
TIRANA, ALBANIA | 5-9 JUNE 2023

Standing on the shoulders of giants

Christos Kanellopoulos (GÉANT)

Licia Florio (NORDUnet)

GÉANT

Co-funded by
the European Union

Aim of this session

AAIs have become important infrastructure: thanks to the AARC BPA and its implementation via eduTEAMs we could offer identity services to address international use-cases:

- Erasmus+, via **MyAcademicID** service;
- EuroHPC: via Fenix AAI; Lumi via Puhuri AAI and **MyAccessID**
- EOSC via the EOSC AAI Federation and the science clusters AAIs

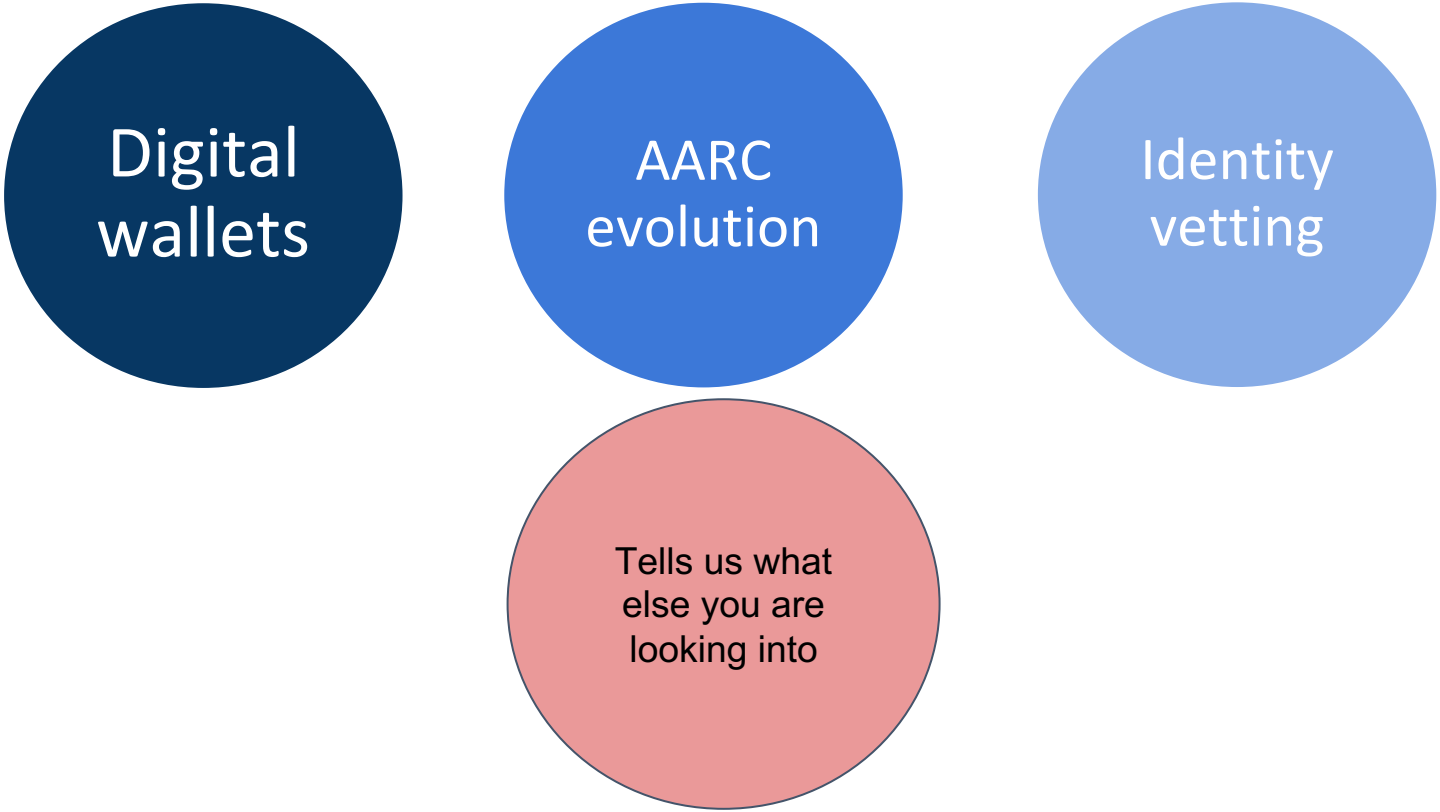
In depth look at

Overview on the work done

Why do we need different AAIs?

Interoperability aspects

Coming up


Digital wallets
AARC evolution
Identity vetting
Tells us what else you are looking into

Agenda

Overview of the work done (2 h)

- Welcome (5m)
- T&I building blocks and Core AAI, Christos (20m)
- Overview of the AAI deployments:
  - MyAID, Licia (10 m)
  - MyAccessID and Fenix, Christos (20m)
  - Puhuri AAI, Anders (15-20m)

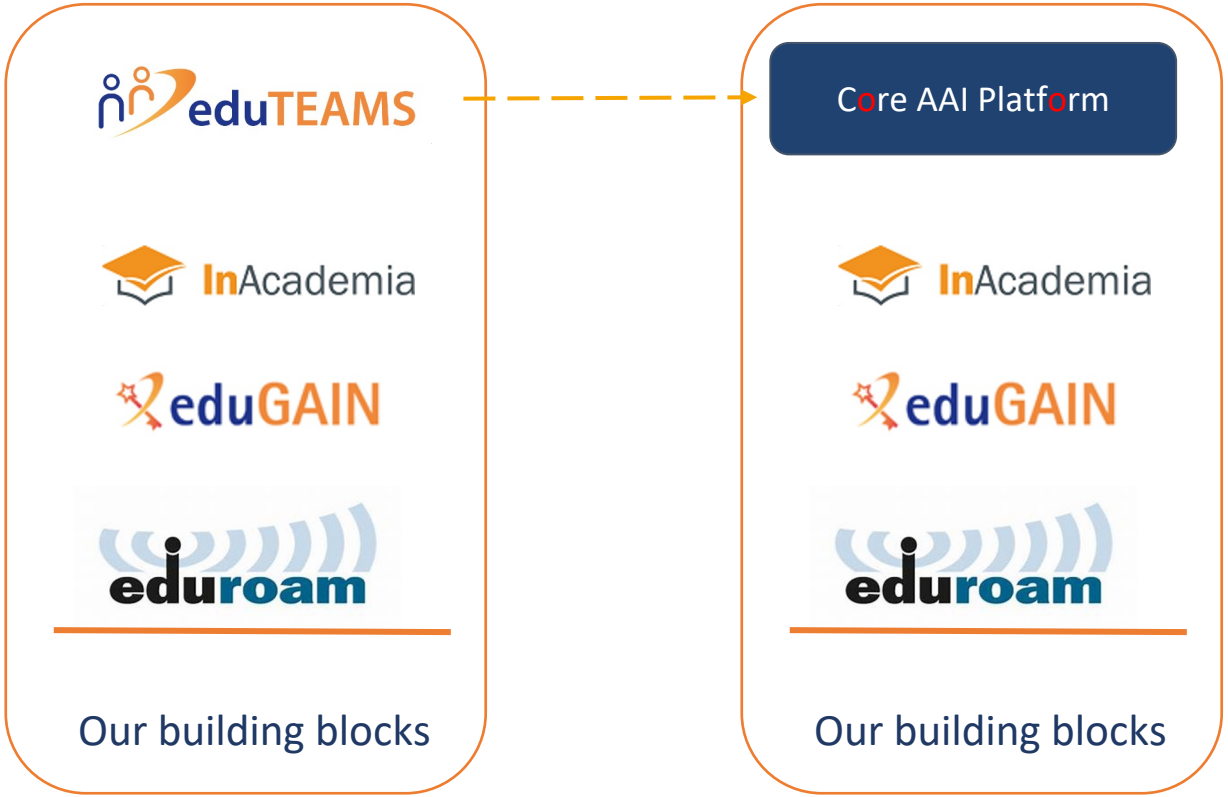
Break (20 min)

Coming up (1h)

- Identity vetting, Leif (15m)
- Wallets, Lluis (15m)
- AARC evolution, David Groep (15m)
- Open discussion

T&I Building blocks: from eduTEAMS to a Core AAI Platform

T&I Building blocks: from eduTEAMS to a Core AAI Platform



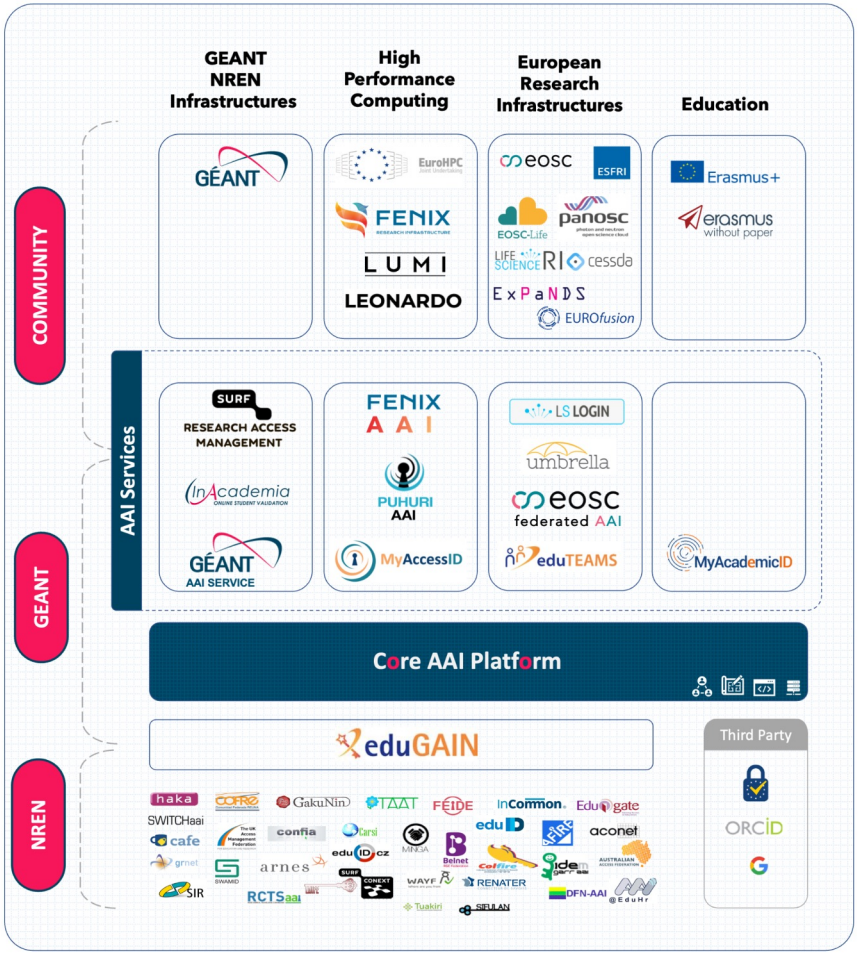
Core AAI Platform

WHY
The great demand for eduTEAMS resulted in a growth of the infrastructure and each eduTEAMS deployment requires significant effort from the team. In addition to **expanding the team** to meet the demand, we need to **evolve the technical stack** to a Core AAI platform that will ensure **sustainable scalability**.
This measure will reduce of the overhead for the delivery of existing and new added value identity services.

Core AAI Platform

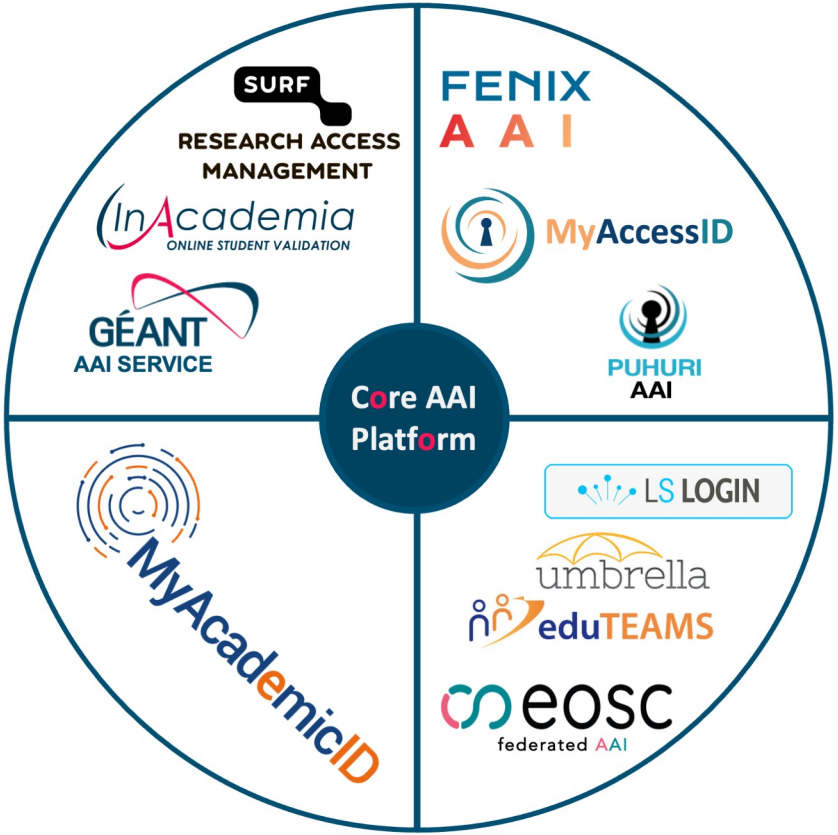
Our building blocks

Core AAI Platform



Core AAI Platform

Core AAI Platform



MyAcademicID: the Identity and Access Management Platform for Erasmus+

Enable NRENs to support a very important and large education use-case

MyAID IAM launched in Nov 2020

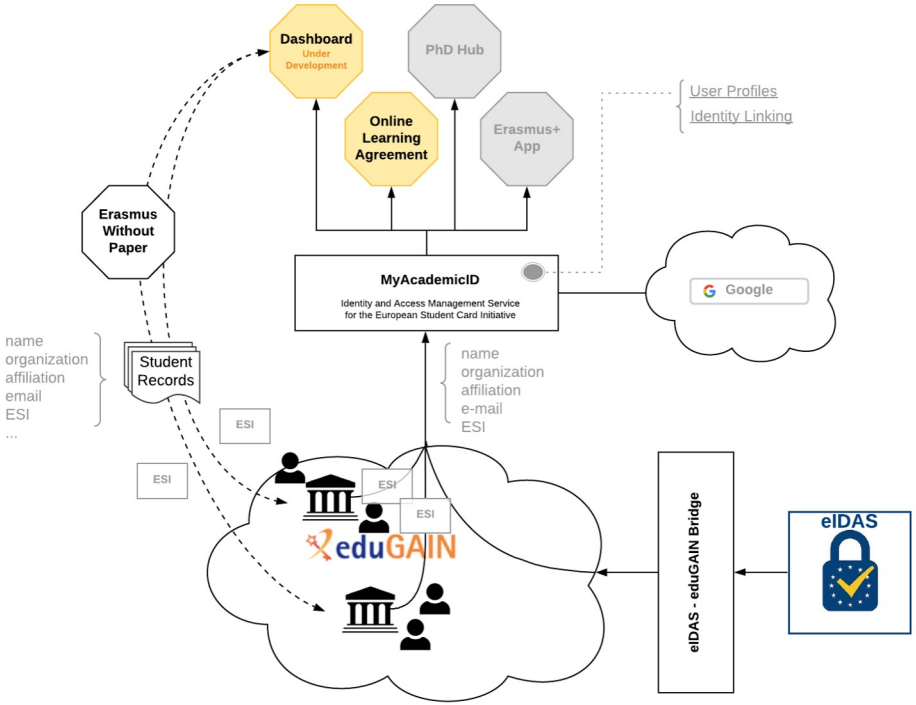
MyAID IAM operated by GÉANT

MyAID IAM based on eduTEAMS

Leverages eduGAIN and eIDAS

MyAID Architecture

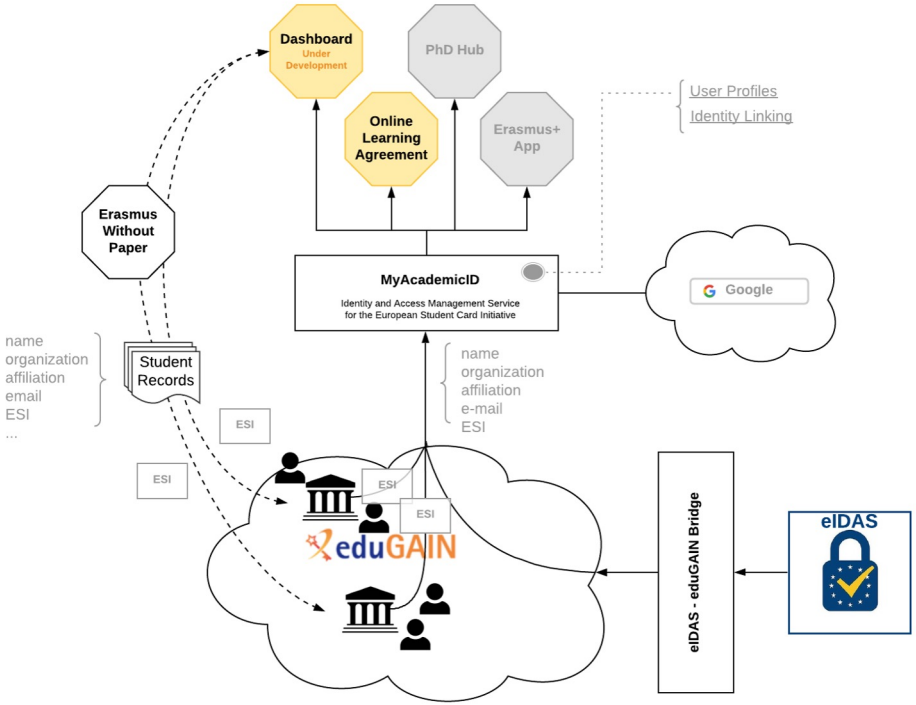
- Provides an Authentication Proxy for the core Erasmus+ services (Online Learning Agreement, Dashboard, PhD Hub and the Erasmus+ App).
- Supports authentication via eduGAIN, eIDAS and Google



MyAID Architecture

An IdP of last resort, built on MyAID, is provided for HEIs in Erasmus+ that cannot use eduGAIN

- Provides an Authentication Proxy for the core Erasmus+ services (Online Learning Agreement, Dashboard, PhD Hub and the Erasmus+ App).
- Supports authentication via eduGAIN, eIDAS and Google



European Student Identifier (ESI)

Exchange of student records between the sending and the receiving institutions and the services.

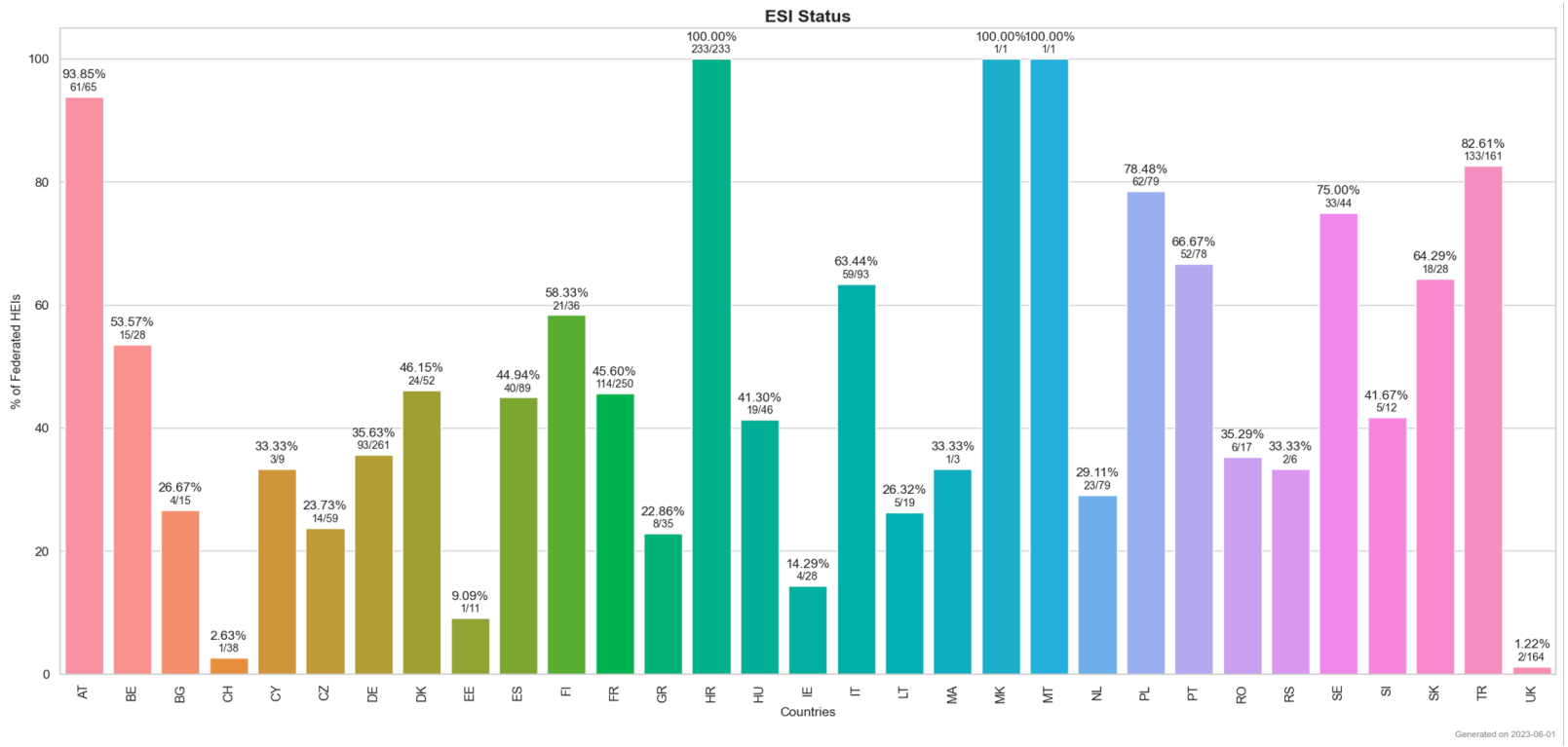
The exchange of records and authentication of students are separate, thus the need for an identifier that will follow the student

The identifier is protocol neutral

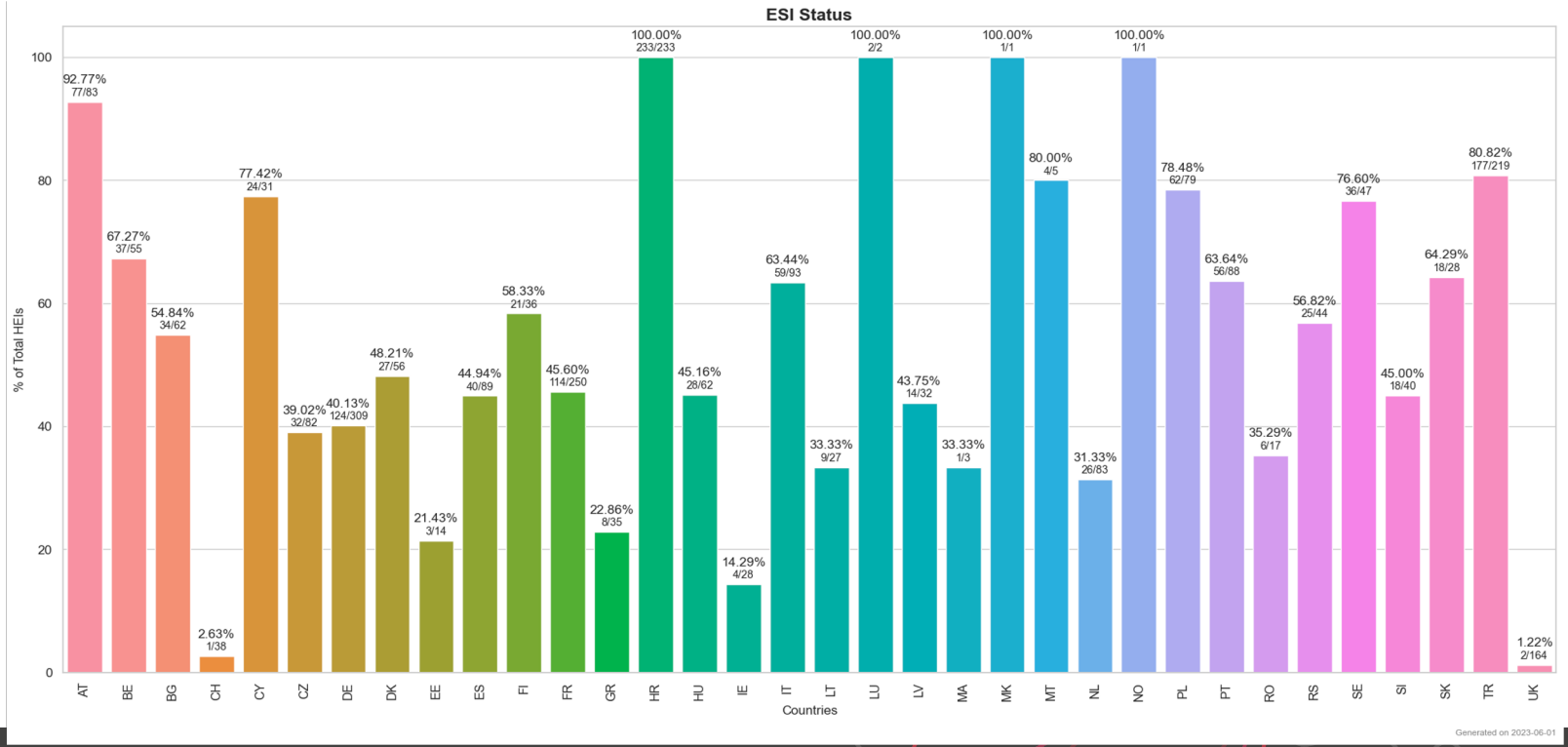
Bi-weekly ESI Calls with the NRENs

https://wiki.geant.org/display/SM/European+Student+Identifier

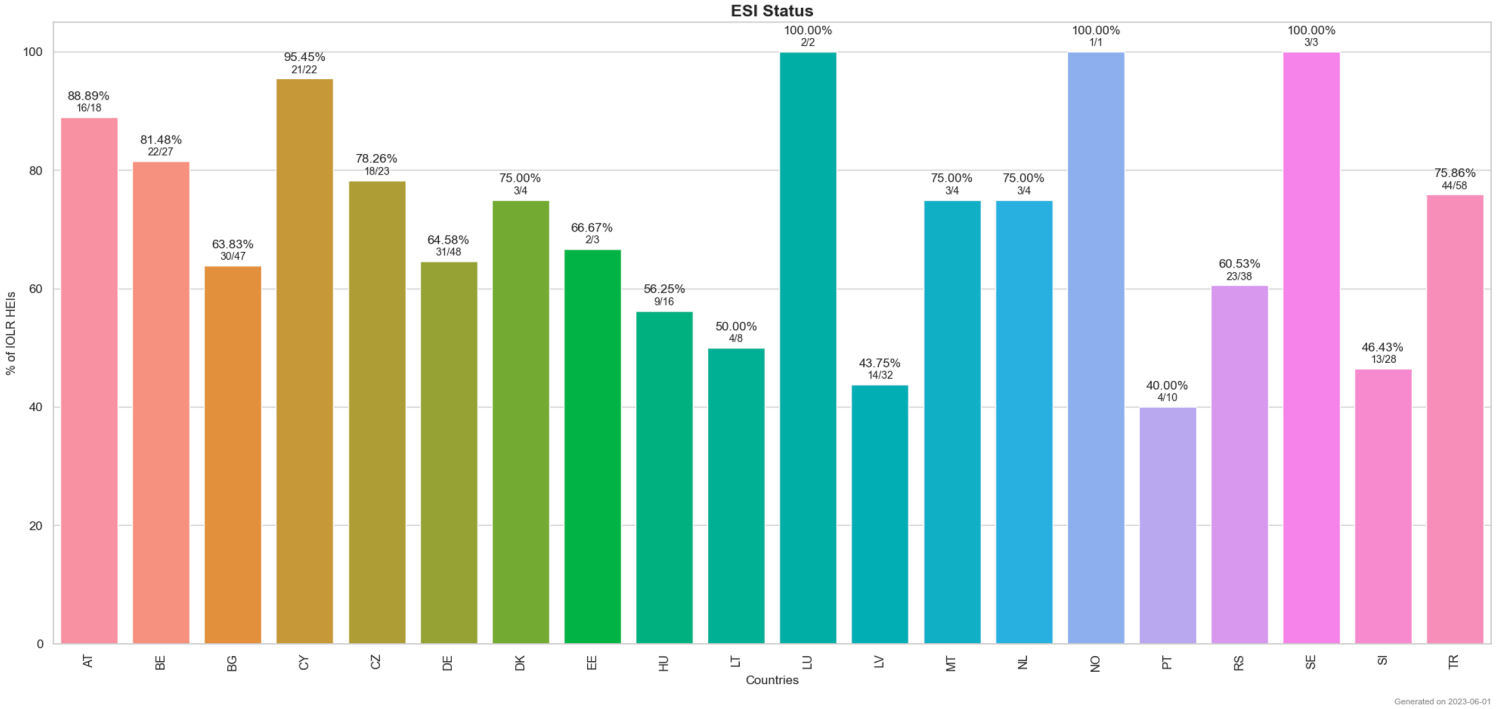
MyAID: % of federated HEIs



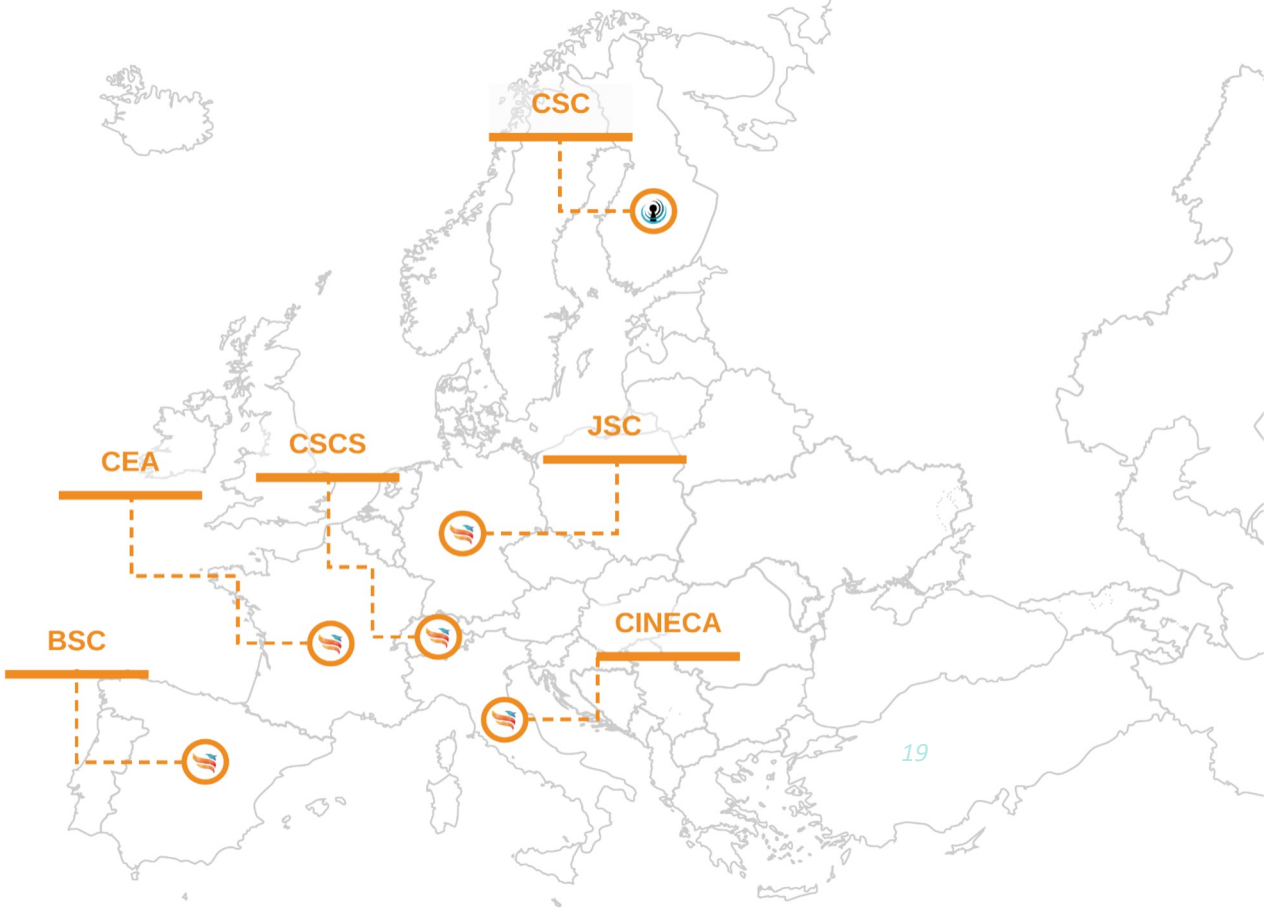
MyAID Stats: % of total HEIs



MyAID Stats: % IdPOLR HEIs

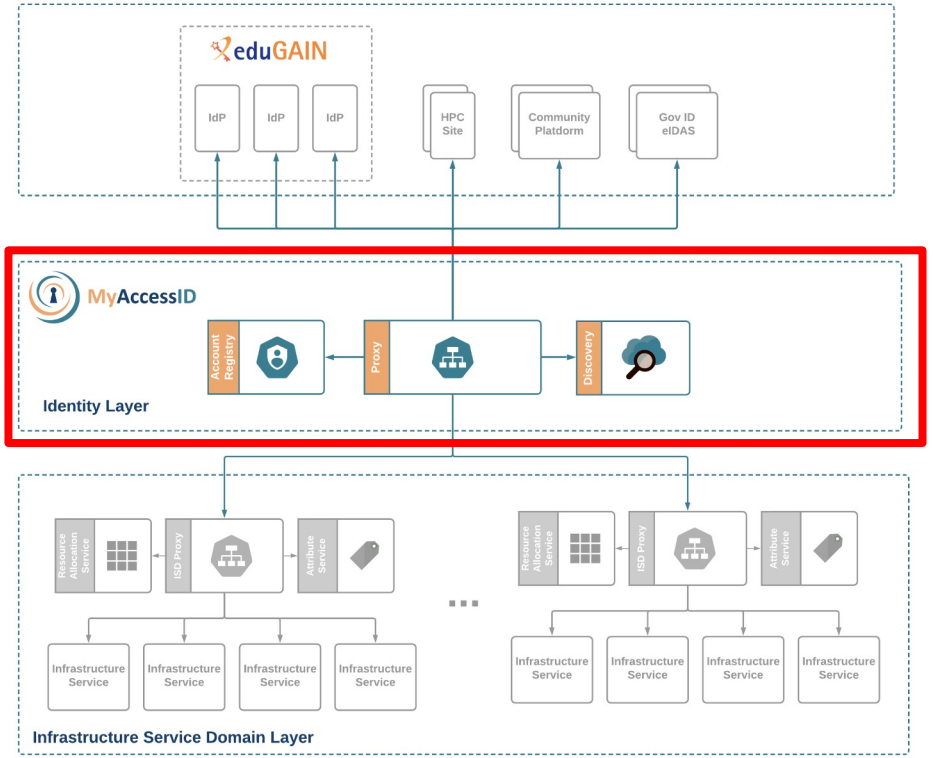


FENIX
RESEARCH INFRASTRUCTURE

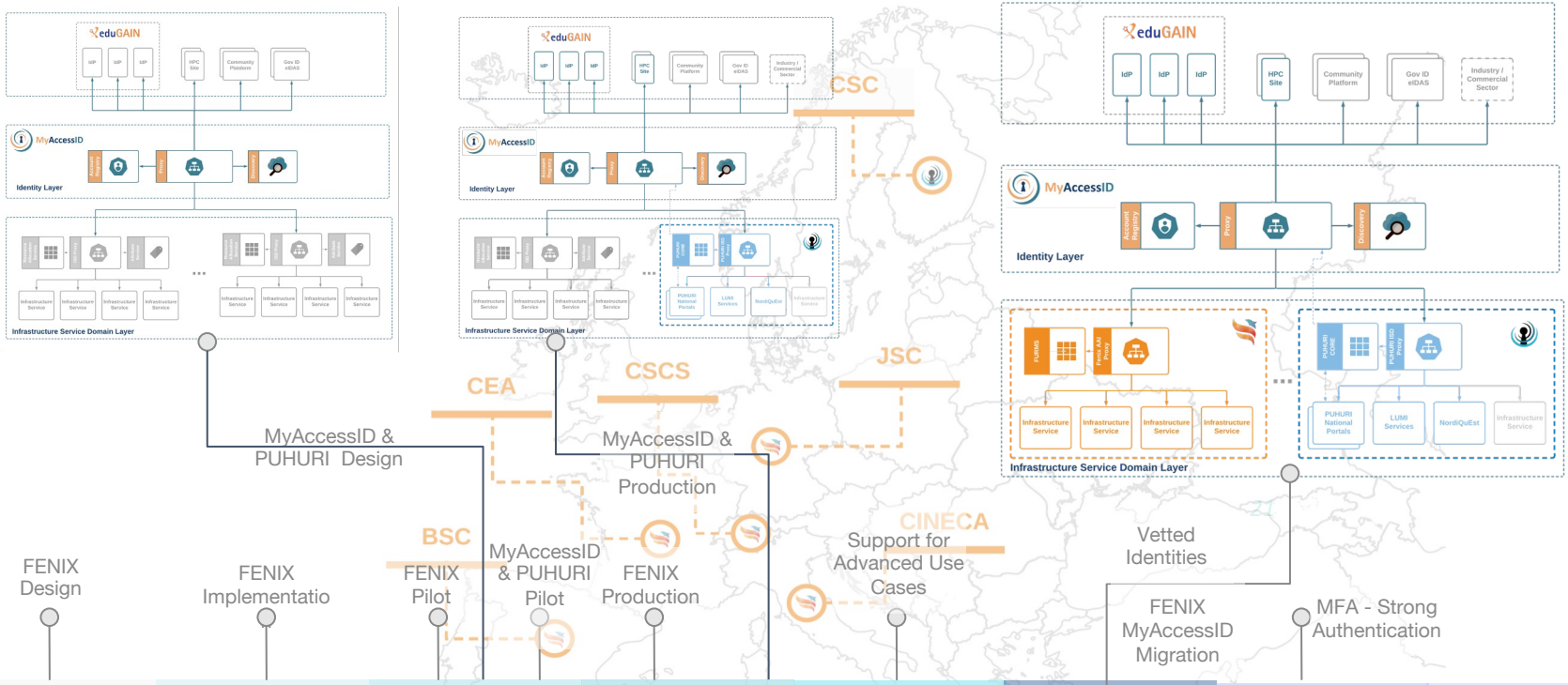


MyAccessID

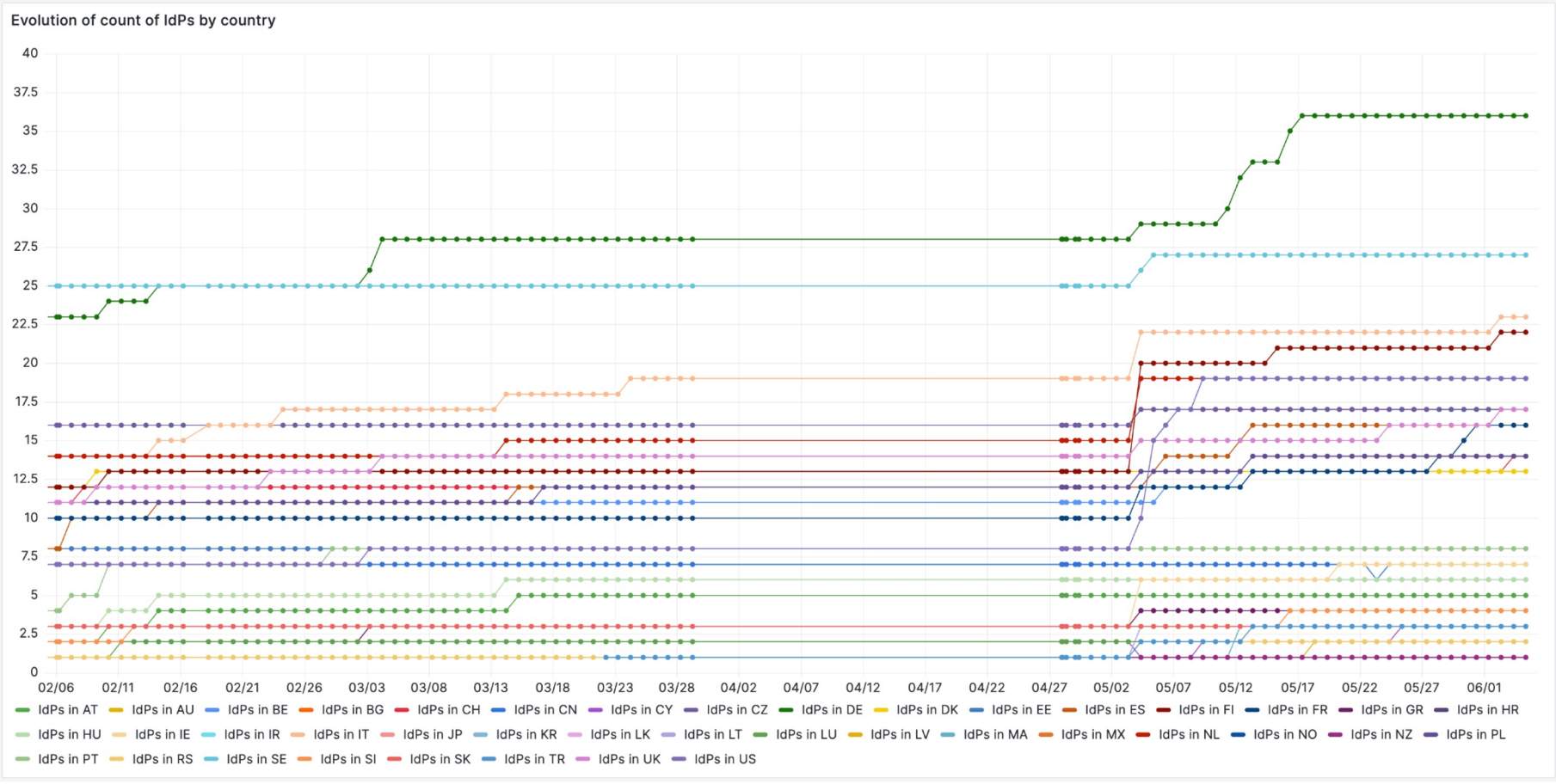
- HPC Datacenters are in the process of transforming to Infrastructure Service Providers with a diverse Service Portfolio
- These infrastructure services become available in different administrative and policy domains, which we call Infrastructure Service Domains
- A common Authentication and Authorization Infrastructure enables uniform accessibility to scientists and engineers at European scale



MyAccessID



tnc23 DIGITAL GENERATIONS


Evolution of count of IdPs by country
40
37.5
35
32.5
30
27.5
25
22.5
20
17.5
15
12.5
10
7.5
5
2.5
0
02/06
02/11
02/16
02/21
02/26
03/03
03/08
03/13
03/18
03/23
03/28
04/02
04/07
04/12
04/17
04/22
04/27
05/02
05/07
05/12
05/17
05/22
05/27
06/01
IdPs in AT
IdPs in AU
IdPs in BE
IdPs in BG
IdPs in CH
IdPs in CN
IdPs in CY
IdPs in CZ
IdPs in DE
IdPs in DK
IdPs in EE
IdPs in ES
IdPs in FI
IdPs in FR
IdPs in GR
IdPs in HR
IdPs in HU
IdPs in IE
IdPs in IR
IdPs in IT
IdPs in JP
IdPs in KR
IdPs in LK
IdPs in LT
IdPs in LU
IdPs in LV
IdPs in MA
IdPs in MX
IdPs in NL
IdPs in NO
IdPs in NZ
IdPs in PL
IdPs in PT
IdPs in RS
IdPs in SE
IdPs in SI
IdPs in SK
IdPs in TR
IdPs in UK
IdPs in US


Evolution of assurance level
380
360
340
320
300
280
260
240
220
200
180
160
140
120
100
80
60
40
20
0
02/06
02/11
02/16
02/21
02/26
03/03
03/08
03/13
03/18
03/23
03/28
04/02
04/07
04/12
04/17
04/22
04/27
05/02
05/07
05/12
05/17
05/22
05/27
06/01
low
medium
high
missing
all

tnc23
DIGITAL GENERATIONS
TIRANA, ALBANIA | 5-9 JUNE 2023

Standing on the shoulders of giants

Puhuri AAI and Level of Assurance

Anders Sjöström NeIC Puhuri

GÉANT
Co-funded by the European Union

Puhuri

A system to facilitate easy and efficient access to high-performance computing (HPC) and related services throughout Europe

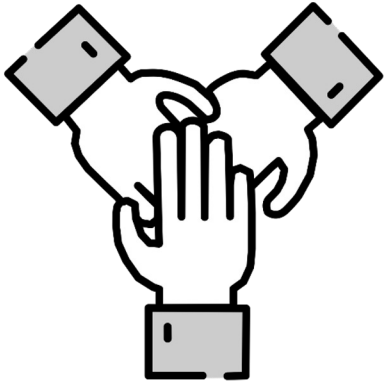
- Reduced administration costs
- Improved usability
- federated services for AAI and resource allocation

- long-term availability
- sustainable operations
- well-defined processes
- trusted AAI solution
- level of assurance information available

Origin of Puhuri

NeIC Dellingr 2017-2020

A lightweight framework for sharing High Performance Computing (HPC) resources implemented between Nordic countries

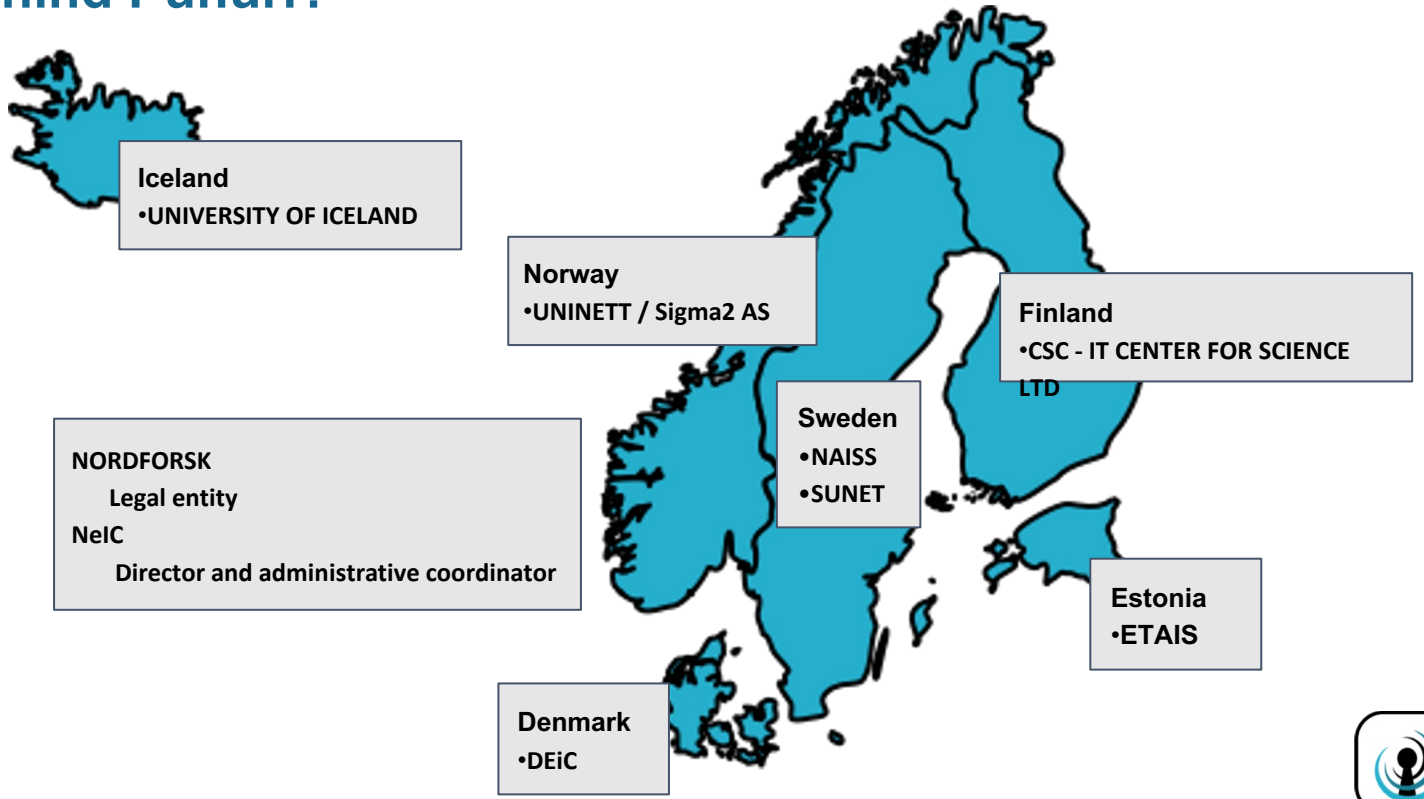


Conclusion:

The technical solutions are available

Legal, economic, and policy issues remain

Who are behind Puhuri?



Scope of Puhuri

Single system multiple service owners
Unified allocation, project, and user management system

- Authentication
- Authorisation
- Identification
- Resource allocation
- Project management
- Etc.

Why Puhuri?

- Need to service LUMI
- Multi-stakeholder system (10 countries + JU)
- Each stakeholder allocates on the system
- Automatic population of the allocation table (e.g. grantfile in SLURM)
- Reporting to each stakeholder separately
- Dual-use designation

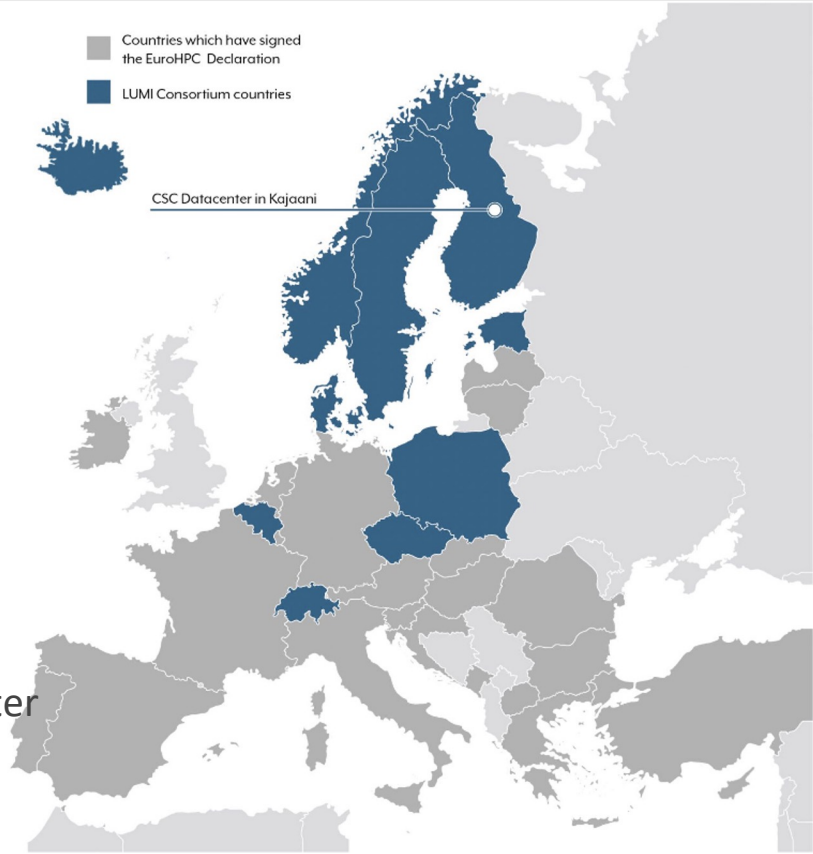
What is LUMI?

LUMI, **EuroHPC pre-exascale** supercomputer,
Located at the CSC data centre in Kajaani, Finland

Hosted by **ten European countries** forming the LUMI consortium:

> **Finland**, **Belgium**, the **Czech Republic**, **Denmark**, **Estonia**, **Iceland**, **Norway**, **Poland**, **Sweden**, and **Switzerland**

Puhuri provides seamless access to the LUMI supercomputer and to other Resources used by NeIC projects and other projects



Can anyone use a HPC system?

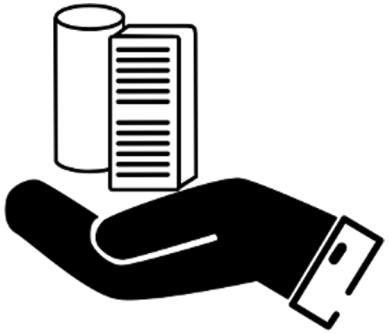
EuroHPC systems are open to European users:

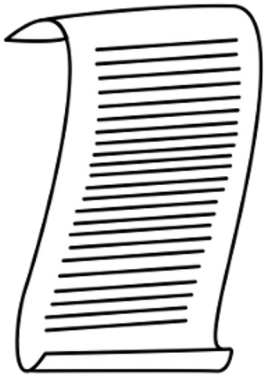
- Scientific
- Industrial
- Public sector

Project owners (PI:s) can invite collaborators

Users from embargoed countries are not allowed

https://www.sanctionsmap.eu

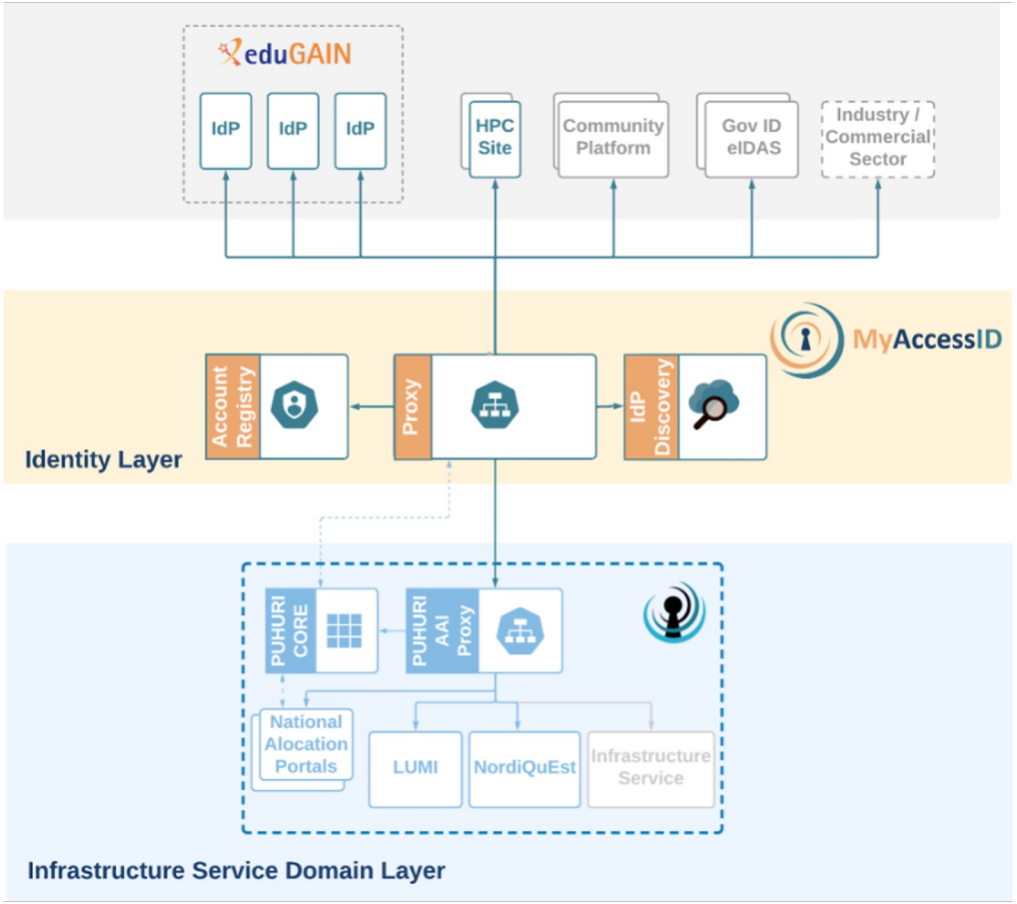




How do we know who's who?

Through MyAccessID

- Receiving Identity information from IdP:s
- Connecting identities at service providers with identity from IdP
- Maintain records of who can use what
- Need LoA information



Is this enough?

- **For the Industry**

  Industry can provide a list of eligible users
- **For the public sector**

  Public sector knows who is to be using the resource
- **For the academia**

  PI is inviting co-investigators

Coffee Break

Identity vetting, Leif

- eduID.se
- ID-proofing using passports (SvipeID)
- Next: wallets and ID-proofing as verifiable credential

tnc23
DIGITAL GENERATIONS
TIRANA, ALBANIA | 5-9 JUNE 2023

The EUDI Wallet in a nutshell

Standing on the shoulders of giants

Lluís Ariño

Tirana

2023/06/05

GÉANT

Co-funded by
the European Union

eIDAS review (eIDAS2)

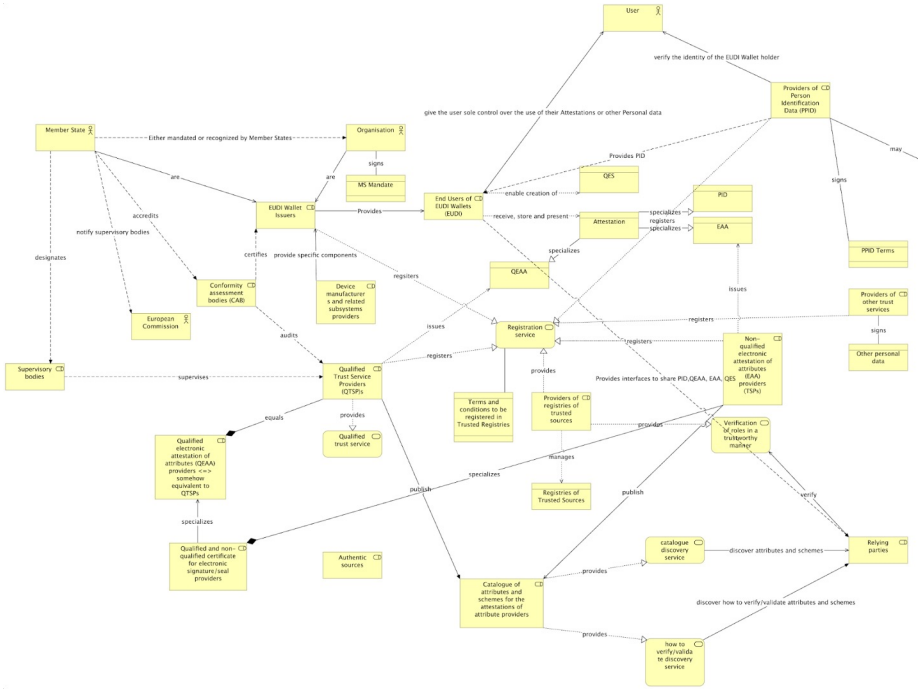
- eIDAS 1: **inherent limitations** to the public sector; limited possibilities and complexity for online private providers to connect to the system; insufficient availability of notified eID solutions in all Member States; citizens identity non-mandatory in all Member States; lack of flexibility to support a variety of use cases.
- **Identity solutions falling outside the scope of eIDAS** (social media providers and financial institutions), raise privacy and data protection concerns, and do not have cross-border recognition.

- A new environment where the **focus** has shifted from the provision and use of rigid digital identities to the provision and reliance on **specific attributes related to those identities**.
- An increased demand for electronic identity solutions that can deliver these capabilities providing efficiency gains and a **high level of trust** across the EU, both in the private and the public sector, relying on the need to identify and authenticate users with a high level of assurance.
- A new approach to ensure that both, citizens and companies, can **trust on digital services** of the digital decade.
- A new approach to **citizen's** privacy and **sovereignty** on their identity and data.

eIDAS2 key highlights

- **Natural** and **legal persons**.
- **All MS** are mandated to issue EUDIW (including PID)
- That these solutions are linked to a variety of attributes and allow for the targeted **sharing** of identity data **limited to the needs** of the specific service requested.
- The user shall be **in full control** of their identity(es) and data.
- The issuer of the EUDIW shall **not collect information about the use** of the wallet
- Obligation of admission
  - by **public sector entities** and by **private providers**.
  - by **very large online platforms that require authentication**.
- **Cross border recognition principle**:
  - A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in any other Member State.
  - An attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be recognised as an attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in all Member States.

eDAS2: Architecture Reference Framework (ARF)

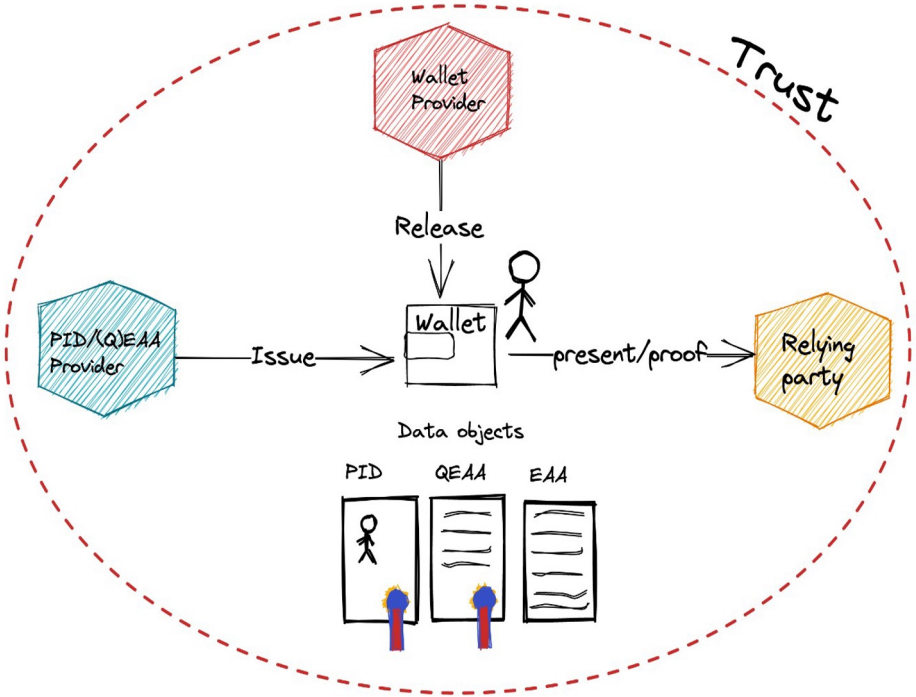


Qualified Trust Service Providers (QTSP)s
Other trust service providers
Trust Service Providers (TSPs)
Authentic sources
Catalogue of attributes and schemes for the attestations of attribute providers
Conformity assessment bodies (CAB)
End Users of EUDI Wallets (EUDI)
Providers of other trust services
Device manufacturers and related subsystems providers
EUDI Wallet Issuers
Relying parties
Supervisory bodies
Providers of Person Identification Data (PPID)
Providers of registries of trusted sources
Organisations that today issue official identity documents or electronic identity means
Non-qualified electronic attestation of attributes (EAA) providers (TSPs)
Qualified and non-qualified certificate for electronic signature/seal providers
Qualified electronic attestation of attributes (QEAA) providers <=> somehow equivalent to QTSPs

European Digital Identity Wallet: EUDIW

- Electronic identification as public good approach. The EUDIW shall be issued by a Member State; under a mandate from a Member State; independently but recognised by a Member State.
- The EUDIW shall be issued under a notified electronic identification scheme of level of assurance ‘high’, albeit the EU Council text authorises a ‘substantial’++ remote mechanism.
- Member States shall notify […] at least one electronic identification scheme including at least one identification means.
- The use of the EUDIW shall be free of charge to natural persons. This opens the door to interesting business models for legal persons. The EU Council text clarifies that services different from authentication may not be free (e.g. issuing electronic attestations of attributes).
- Unique and persistent identification over time, when used for user authentication, limited to specific domains

EUDI Wallet: Architecture (I)



Personal Identification Data

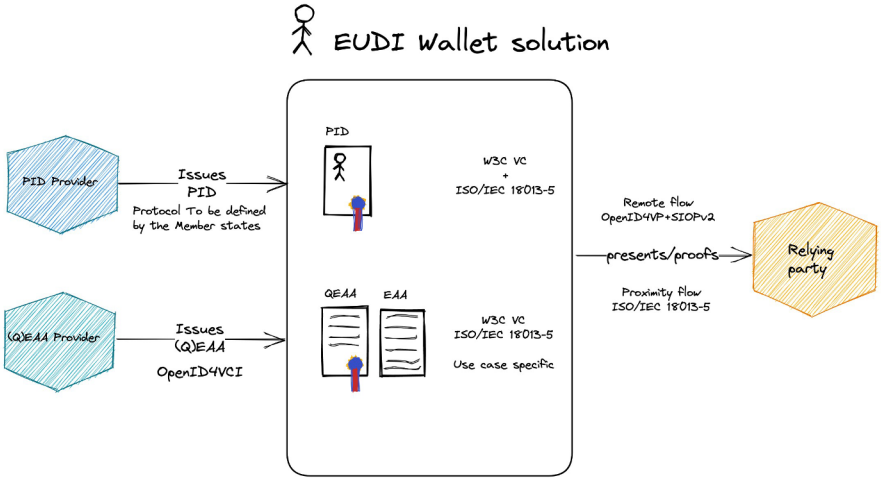
Attributes used for identification:

- First & Family name
- Date of birth
- And others

(Qualified) Electronic Attestation of Attributes

- Digital travel credentials
- Education credentials (Diplomas, certifications, etc)
- Mobile Driving License
- Membership Card
- Event Tickets

EUDI Wallet: Architecture (II)



Type 1 configuration

- **Overall focus on interop, ease of deployment, existing support etc**
- PID / EUDIW Instance binding serves as root of trust
- Re-issuance instead of backup
- Single device only

Type 2 configuration

- **Overall focus on flexibility and allows for more “advanced” solutions.**
- Use case dependent root of trust
- Backup and recovery allowed
- Multi device flows possible

Large Scale Pilots

20 countries

56 public and 80+ private entities

Use cases:

Electronic Government services, Bank Account opening, SIM registration, mobile driving licence, Remote Qualified Electronic Signature and ePrescription.

22 countries

36 public and 40+ private entities

Use cases:

Educational credentials and professional qualifications, Portable Document A1 (PDA1), European Health Insurance Card (EHIC).

POTENTIAL
European Consortium for Digital Identity

EWC

DC4EU

NOBID CONSORTIUM

19 countries

18 public and 40+ private entities

Use cases:

Digital Travel Credentials, Payments, Legal persons

8 countries

6 private and 15 private entities

Use cases:

payments use-cases at both a cross-country and cross-sector level with partners coming from both private and public sector

Total budget: >90 Million (50% EU contribution), >250 Participants,

EUDI wallet: Opportunities for NRENs or NRENs to the rescue?

1. Universities as authentic sources and issuers of (Qualified) Electronic Attestations of Attributes ⇔ The autonomous university

1. Universities as authentic sources ⇔ Must give access to certified issuers of (Qualified) Electronic Attestations of Attributes

1. NRENs on behalf of universities ⇔ The perfect alliance?
   a) NREN as an authentic source on behalf of the universities
   b) NREN as a trusted issuer of electronic attestations of attributes on behalf of the universities
   c) NREN as a qualified trusted issuer of electronic attestations of attributes on behalf of the universities
   d) …

tnc23
DIGITAL GENERATIONS
TIRANA, ALBANIA | 5-9 JUNE 2023

Thank you

Any questions?

GÉANT

Co-funded by
the European Union

tnc23
DIGITAL GENERATIONS
TIRANA, ALBANIA | 5-9 JUNE 2023

EBSI and DC4EU

Standing on the shoulders of giants

Lluís Ariño

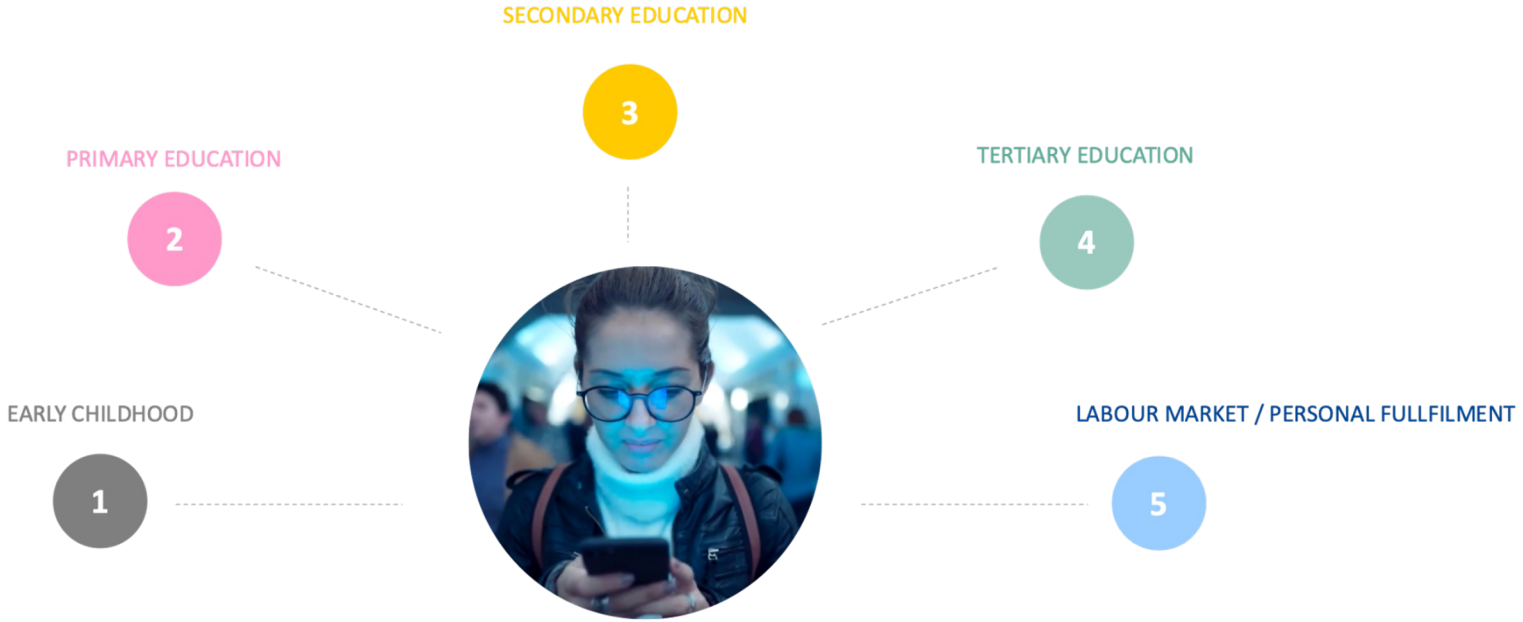
Tirana

2023/06/05

GÉANT

Co-funded by
the European Union

We learn throughout the course of our life



The need for a more flexible education ecosystem

USER-CENTRIC

Learners at the centre of the credentials exchange.

The ecosystem must place learners/citizens as the focus of any action/interaction through a credentials exchange. Learners need to be empowered to easily request and share credentials with anyone at anytime

MOBILE

Cross-border and mobile credentials exchange.

The ecosystem must facilitate interoperability and cross-border common data models and ontologies (such as the European Learning Model, MyAcademicID data model and others)

ADAPTIVE

Lifelong learning and micro-credentials.

The ecosystem must facilitate Lifelong Learning (LLL) – that is, formal, non-formal, informal education. It must facilitate Personal Learning pathways (PLP) and the stacking of verifiable credentials, including micro-credentials.

CONTINUOUS

Support the entire educational credential lifecycle.

The ecosystem must support the entire educational credentials lifecycle. That means the capability to issue, share, verify, revoke, suspend and expire credentials.

PERSONAL

Learners can control their own credentials / information

The ecosystem must respect data privacy. It should provide the option for selective disclosure information from their Personal Learning Record (owned and controlled by learners / citizens).

CONNECTED

Connected to the demands of society

The labour market is increasingly volatile (demand/supply) and citizens and companies face great challenges in the so-called digital decade. There is a real opportunity to align the demands of the labour market with the training offer, and the demands of society.

VERIFIABLE & TRUSTWORTHY

European Blockchain Services Infrastructure (EBSI)

Provide decentralised services that Citizens can trust.

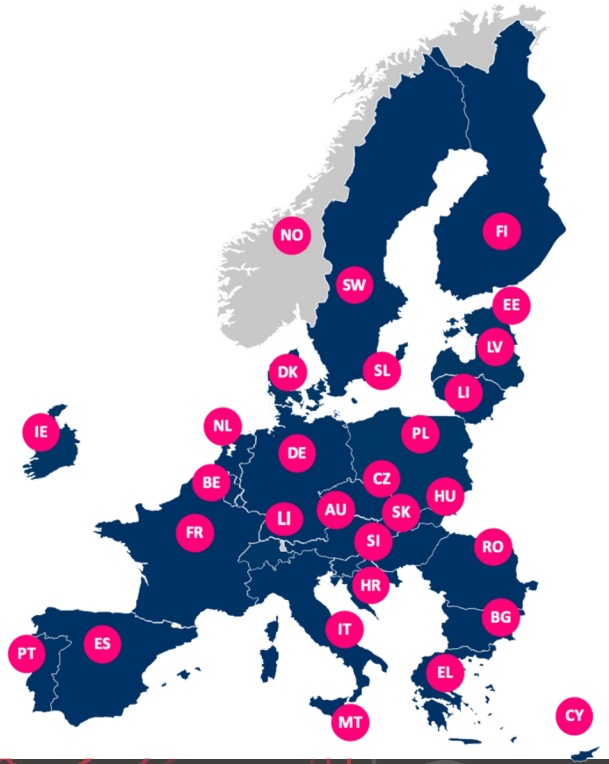
Privacy Preserving (self-sovereignty) - No personal data stored on chain

Contribute to data spaces (discourage data monopolies) and support the green agenda.

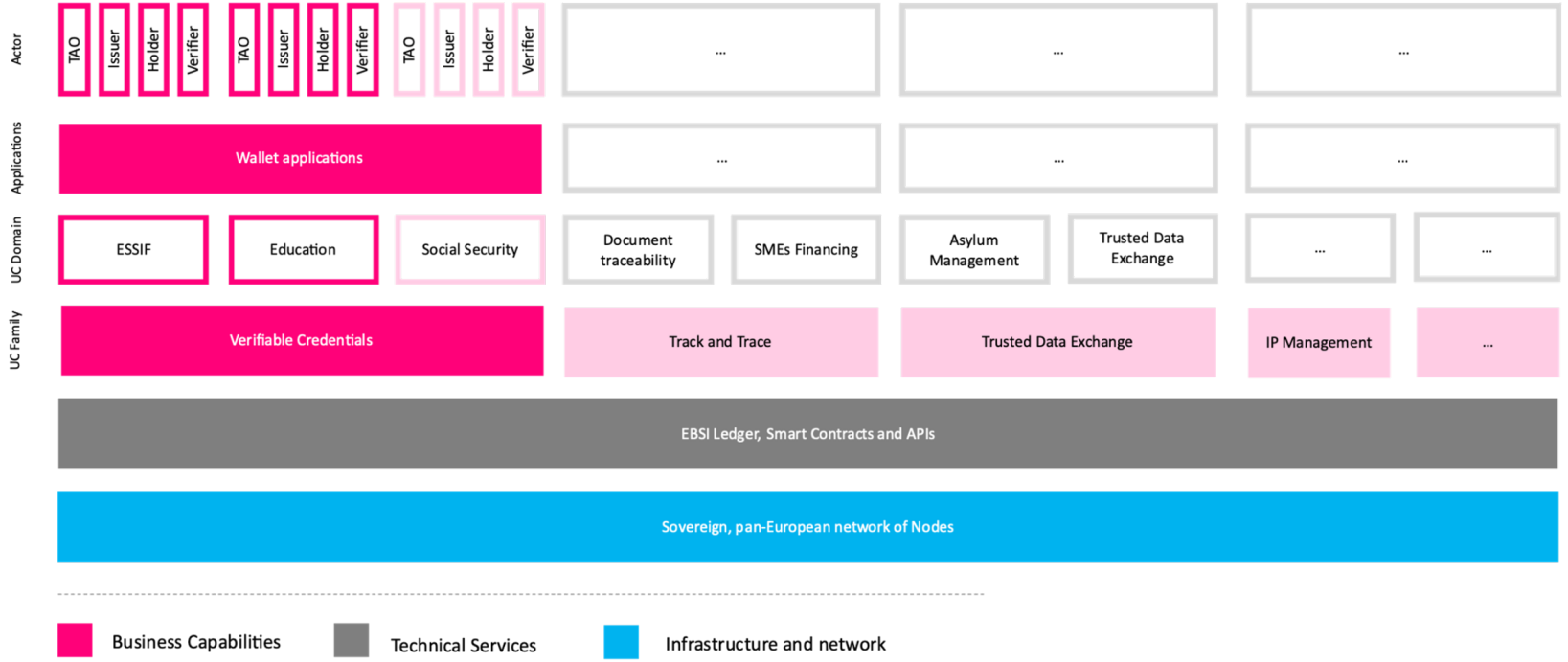
Eco-friendly - Proof of Authority requires almost no computing power, and therefore almost no electricity for its operation.

Run European nodes in line with EU values and regulations.

EU governed, sovereign infrastructure - A permissioned blockchain -information can be *read* by all – however, only selected actors are allowed to *write*

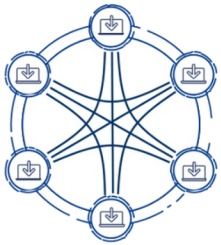


EBSI as a cross sector initiative focused on harnessing the power of electronic ledgers for public service and trust



3 key elements for sovereignty

Information is easy to verify, almost impossible to fake and controlled by citizens



Blockchain / Ledger

Don't Trust, Verify

Digital Wallet

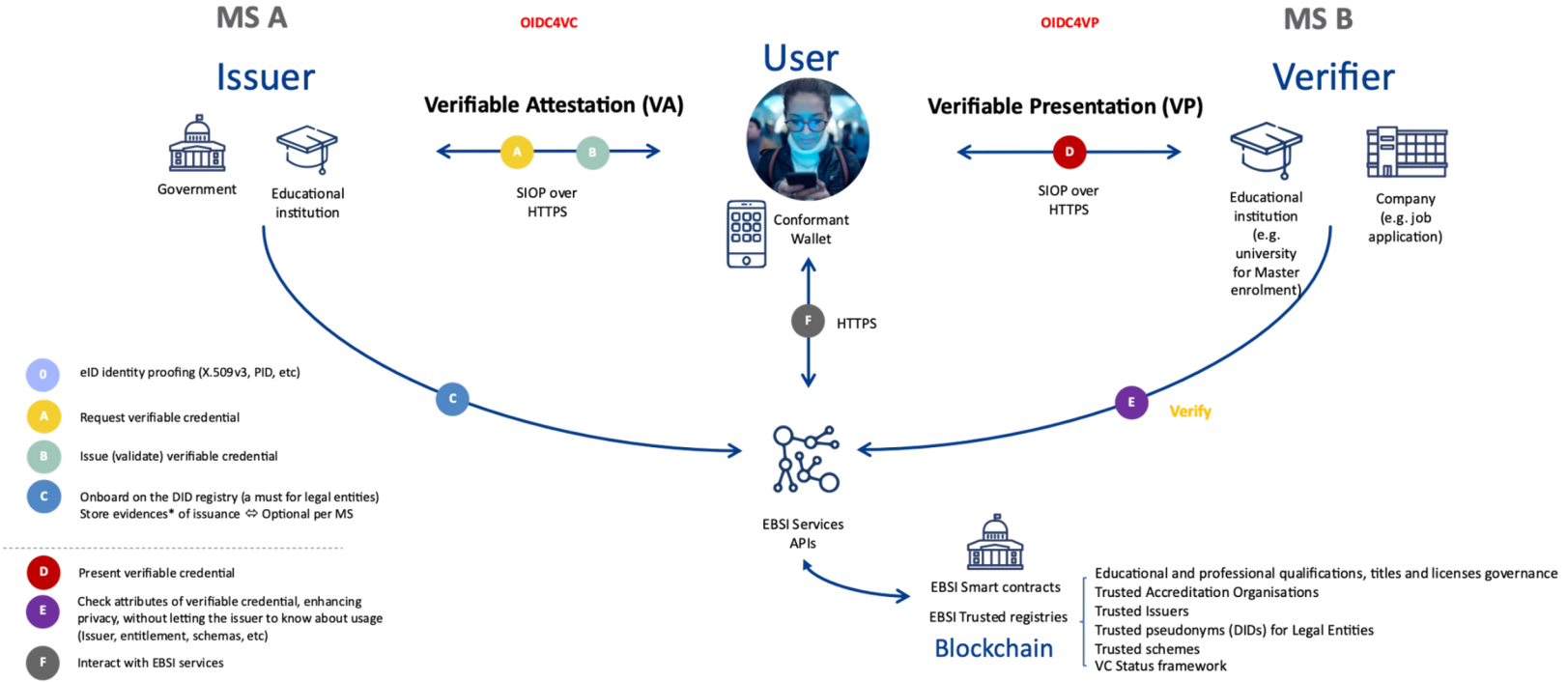
Not your keys, not your digital asset

Verifiable Credentials

A new way of expressing and automating information

Metadata | Claims | Proofs (signatures)

EBSI enables a new paradigm to exchange data between parties



Advantages that highlight the transformative potential of verifiable credentials based on electronic ledgers

Trust and Authenticity:

Verifiable credentials leverage cryptographic techniques to ensure authenticity and integrity.

They provide a higher level of trust compared to non-verifiable digital credentials, as they are tamper-resistant and can be easily verified.

Security and Immutability:

Verifiable credentials are stored in decentralized systems, such as blockchain or distributed ledgers.

This distributed nature enhances security and makes the credentials immutable, preventing unauthorized changes or fraud.

Privacy and Data Control:

Verifiable credentials enable individuals to have more control over their personal data.

They allow selective disclosure, meaning individuals can share only the necessary information without revealing their entire credential or identity.

Efficient Verification:

Verifiable credentials streamline the verification process, reducing reliance on manual checks.

Relying parties can quickly verify the authenticity of a credential by validating it against the distributed ledger, saving time and effort.

Interoperability and Portability:

Verifiable credentials adhere to standardized formats and protocols, ensuring interoperability across different systems and platforms.

They can be easily shared and transferred between individuals, organizations, or services, making them highly portable.

Reduction of Fraud and Counterfeiting:

Verifiable credentials, with their built-in trust mechanisms, significantly reduce the risk of fraud and counterfeiting.

The cryptographic techniques used in verifiable credentials make it extremely difficult for malicious actors to forge or tamper with the information.

Future-proof and Scalable:

Verifiable credentials offer a forward-looking solution that can adapt to evolving technological advancements.

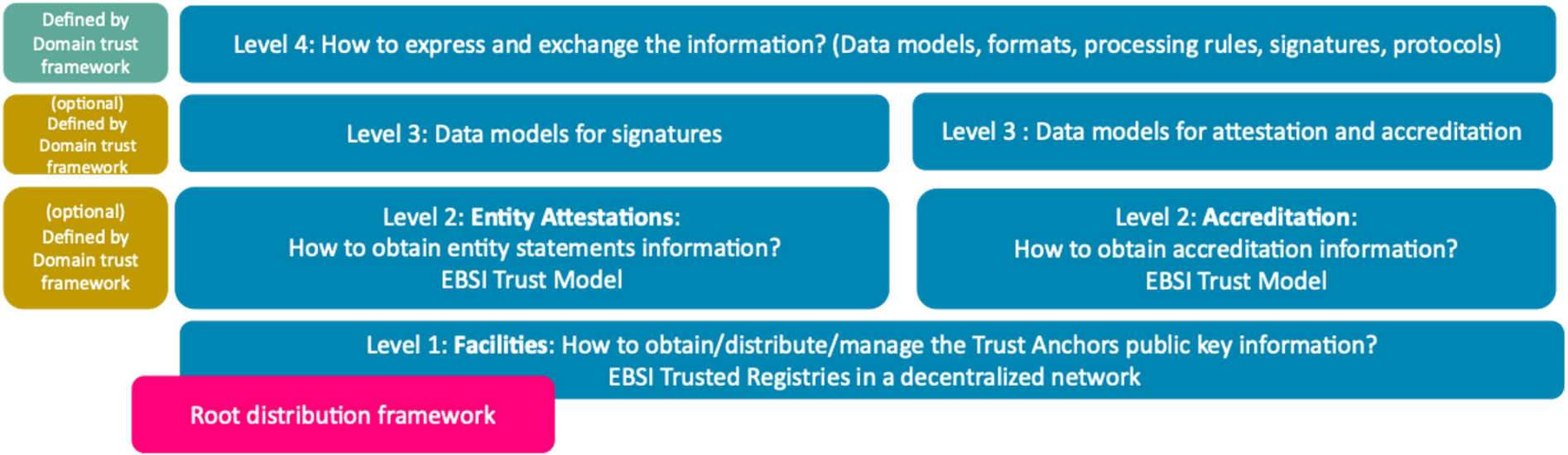
The decentralized nature of electronic ledgers provides scalability, allowing for a large number of credentials to be managed efficiently.

Enhanced Transparency and Auditability:

Verifiable credentials recorded on electronic ledgers enable greater transparency and auditability.

The transaction history and verification records can be traced back, providing a verifiable and immutable audit trail.

EBSI is use-case agnostic, hence use-case specific elements should be defined



EBSI Wave 2 (15 MS, 20 HEIs, 2 EUA)

Study

01 A student gets a diploma with a list of course units validated from Erasmus (Transcript of Records Credential) (ES/BE/IT)

02 ~~A student applies for a~~ PhD with a Bachelor / Master degree from a foreign country (Bachelor/Master Diploma Credential) (RO/GR/FR)

03 ~~A student gets~~ access to local discounts using student credential (European Student IDentity) (BE/ES)

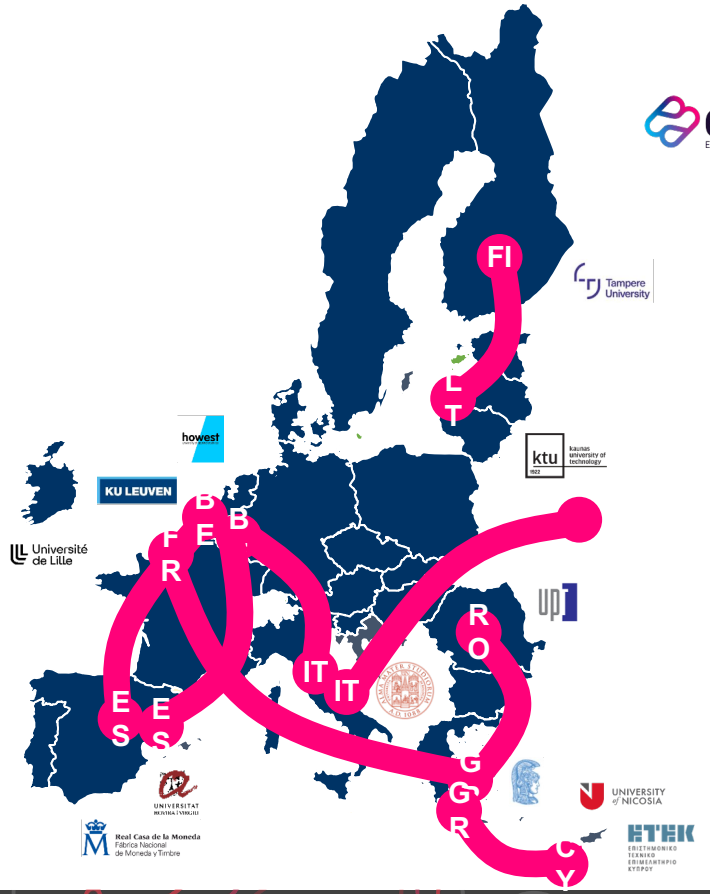
04 A refugee presents an EQPR to a European Italian University to apply for a Master (EQPR - CoE Refugee Passport) (IT/DE)

Work

05 A graduated citizen applies for a job with a Degree from a foreign country (License to Practice Credential) (GR/CY)

Grow

06 A PhD student applies for specific courses in a foreign country (Cross-border Micro-credentials) (FI/LT)



EBSI Wave 3 (29 countries, +30HEIs, 5 UA)

Identity

A **<citizen>** from a **<Country A>** gets access to public services in a **<Country B>** using national ID

- National ID

12 applications

MyAcademicID for authentication purposes

A **<student>** from an **<educational institution>** in a **<Country A>** wants to access resources and facilities from **<educational institution>** in a **<Country B>**.

- (Student ID)

12 applications

Formal Accreditation and Recognition

A **<student>** who has completed a **<formal education degree>** in a **<University>** from **<Country A>** wants to enroll for another formal **<formal education degree>** at **<University>** from **<Country B>** .

- *(Secondary Education diploma)*
- Bachelor diploma
- Master diploma
- PhD diploma

13 applications

Micro-credentials as verifiable credentials in Higher Education

A **<student>** from a **<University>** in a **<Country A>** takes a short course from a **<University>** in a **<Country B>**. Upon successful completion and verification, **<University>** in a **<Country A>** issues transcript of record.

- Transcript of records (short-courses | micro-credentials)

21 applications

University Alliances

A student from from a **<University>** in a **<Country A>** takes a short course from a **<University>** in a **<Country B>. Both Universities are part of** an the alliance.

- (Student ID)
- Transcript of Record

7 applications

Formal accredited Vocational Education and training

A **<professional>** from a **<Company>** in a **<Country A>** wants to take a **<course>** in a specific domain to improve her competences and skills and make sure that it is accredited by a **<VET>** from a **<Country B>.**

- Transcript of records (short-courses | vocational training certificate)

8 applications

Employment

A **<professional>** from a **<Company>** in a **<Country A>** wants to apply for a job at a **<Company>** in a **<Country B>.**

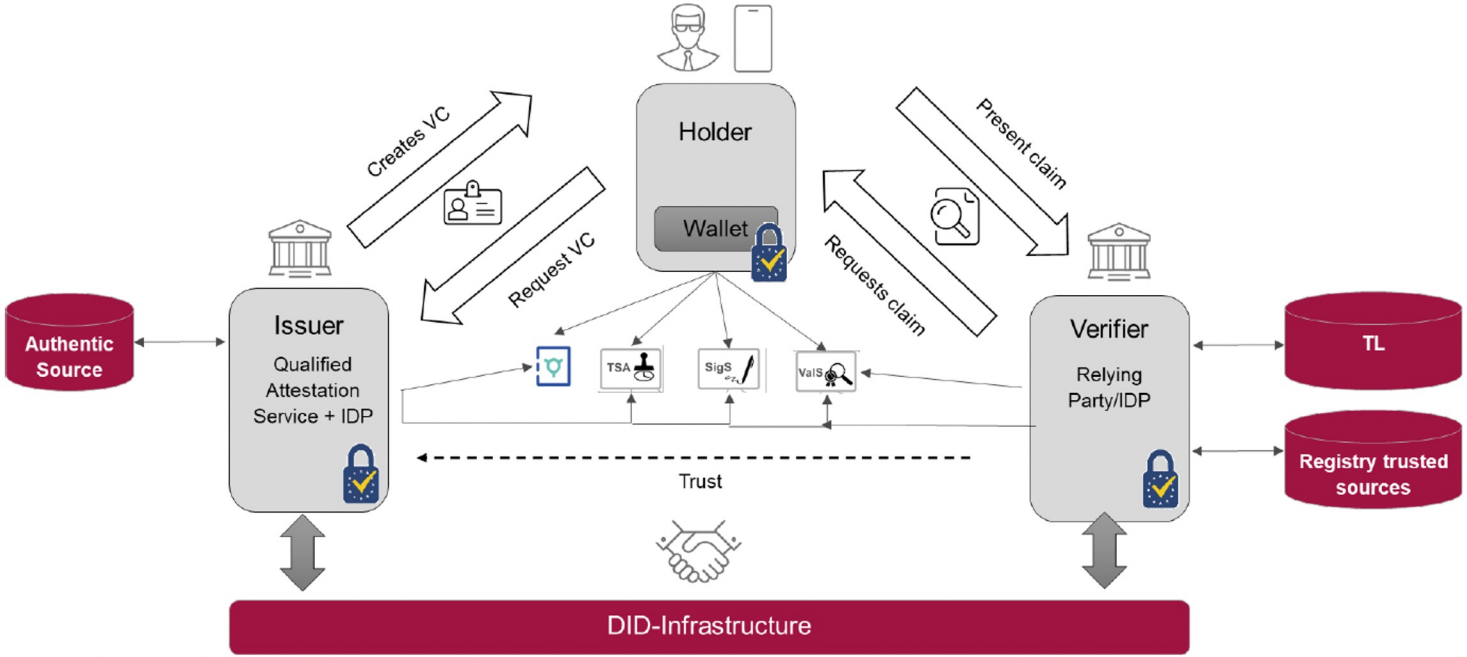
- Verifiable CV
  - Certificate of Employment
  - Identity
  - Diploma
- License to practice

7 applications

eIDAS review: a game changer

- **Natural** and **legal persons**.
- **All MS** are mandated to issue EUDIW (including PID)
- That these solutions are linked to a variety of attributes and allow for the targeted **sharing** of identity data **limited to the needs** of the specific service requested.
- The user shall be **in full control** of their identity(es) and data.
- The issuer of the EUDIW shall **not collect information about the use** of the wallet
- Obligation of admission
  - by **public sector entities** and by **private providers**.
  - by **very large online platforms that require authentication**.
- **Cross border recognition principle**:
  - A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in any other Member State.
  - An attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be recognised as an attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in all Member States.

eIDAS and EBSI … not so far



Large Scale Pilots: impact is key (so adoption is key)!

20 countries

56 public and 80+ private entities

Use cases:

Electronic Government services, Bank Account opening, SIM registration, mobile driving licence, Remote Qualified Electronic Signature and ePrescription.

22 countries

36 public and 40+ private entities

Use cases:

Educational credentials and professional qualifications, Portable Document A1 (PDA1), European Health Insurance Card (EHIC).

POTENTIAL
European Consortium for Digital Identity

EWC

DC4EU

NOBID CONSORTIUM

19 countries

18 public and 40+ private entities

Use cases:

Digital Travel Credentials, Payments, Legal persons

8 countries

6 private and 15 private entities

Use cases:

payments use-cases at both a cross-country and cross-sector level with partners coming from both private and public sector

Total budget: >90 Million (50% EU contribution), >250 Participants,

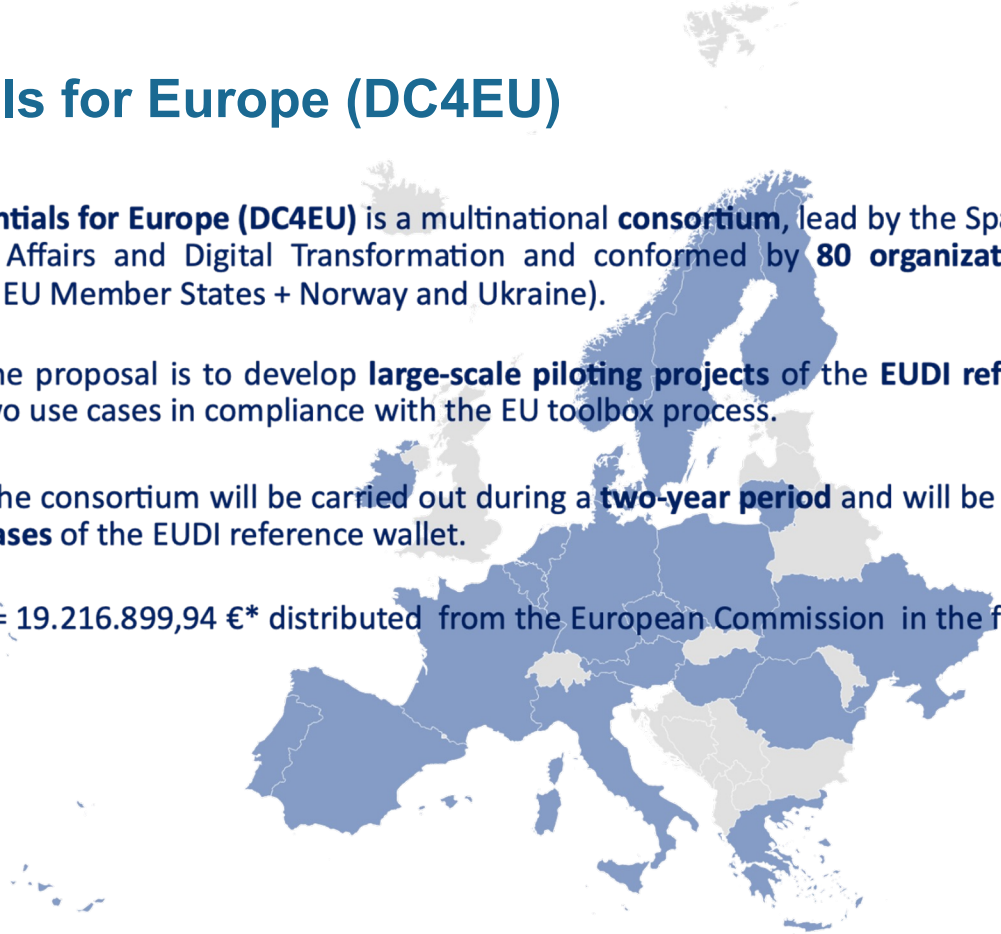
Digital Credentials for Europe (DC4EU)

Digital Credentials for Europe (DC4EU) is a multinational **consortium**, lead by the Spanish Ministry of Economic Affairs and Digital Transformation and conformed by **80 organizations** from **22 countries** (20 EU Member States + Norway and Ukraine).

The **aim** of the proposal is to develop **large-scale piloting projects** of the **EUDI reference wallet** addressing two use cases in compliance with the EU toolbox process.

The work of the consortium will be carried out during a **two-year period** and will be guided by the **iterative releases** of the EUDI reference wallet.

Total budget = 19.216.899,94 €* distributed from the European Commission in the form of 2 payments



DC4EU

The **EUID wallet is a hybrid solution** to bridge both worlds (**centralized** / federated / distributed **& decentralized**).

Enhanced data lifecycle due to **verifiable credentials usage.**

Using EBSI as trusted registry (trusted source) to support governance, actors, roles, etc.

- **Enhanced privacy**
- **Trust service providers cannot receive Information about the use of atributes**
- **Easy way to store ID atributes**
- **Easy mechanism to create trust in relying parties**
- **More resistant to correlation and data exploitation**
- **Trusting Information outside the own business domain**
- **Allows management of multiple citizens identities**
- **Enhance security**
- **Sustainability**

DC4EU

Educational credentials formal qualifications issuance: Primary, secondary, tertiary education

- Request secondary degree to apply to tertiary education
- Request PID and Bachelor to be issued with professional qualification accreditation
- Request bachelor degree to apply to Master education
- TVET
- Request transcript to move from secondary school to secondary school
- Request micro credentials issuance

Non-foundational identity/authentication

- European Student IDentifier
- MyAcademicID
- InAcademia

DC4EU

- ELMO to ELM converter
- eduGAIN gateway
- EMREX gateway
- EDSSI gateway

- EWP – OLA
- Open Badges to ELM converter
- eIDAS gateway
- Europass & EDC alignment

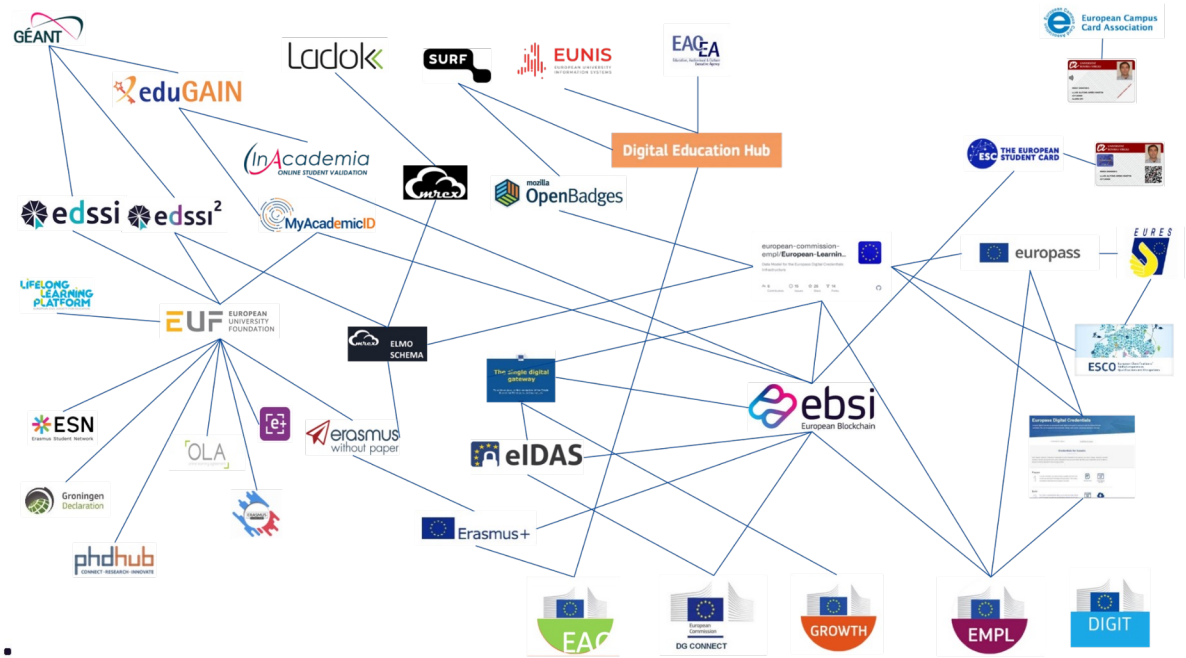
Provided by MSs

DC4EU: building bridges

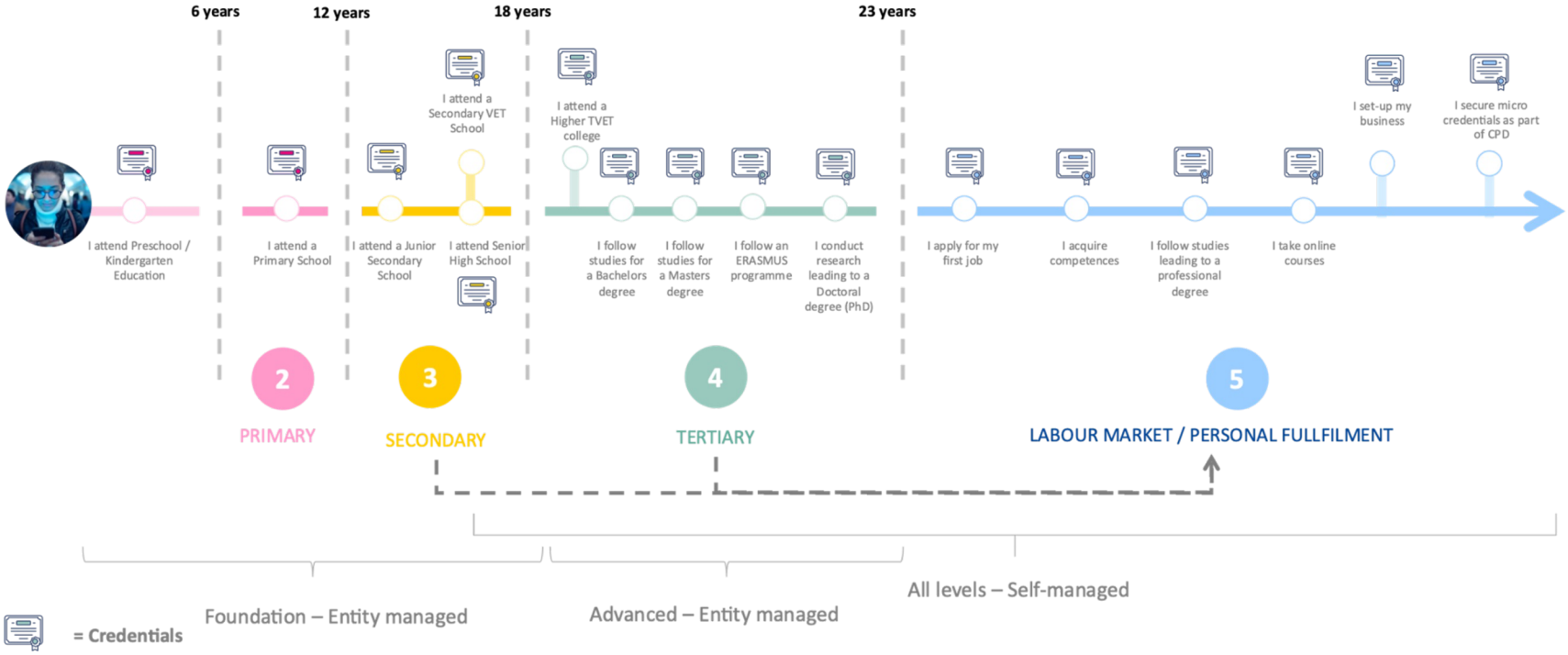
The EUDI wallet is the real container for the Individual Learning Record (ILR)

eIDAS

ebsi
European Blockchain



Different models, different paradigms: it's not one or the other



Cross-border mobility programs are accelerators of the change from a managed to a self-managed/sovereign model (Erasmus+, etc.)

EUDI wallet: Opportunities for NRENs or NRENs to the rescue?

1. Universities as authentic sources and issuers of (Qualified) Electronic Attestations of Attributes ⇔ The autonomous university

1. Universities as authentic sources ⇔ Must give access to certified issuers of (Qualified) Electronic Attestations of Attributes

1. NRENs on behalf of universities ⇔ The perfect alliance?
   a) NREN as an authentic source on behalf of the universities
   b) NREN as a trusted issuer of electronic attestations of attributes on behalf of the universities
   c) NREN as a qualified trusted issuer of electronic attestations of attributes on behalf of the universities
   d) …

tnc23
DIGITAL GENERATIONS
TIRANA, ALBANIA | 5-9 JUNE 2023

Thank you

Any questions?

lluisalfons.arino@urv.cat

GÉANT
Co-funded by the European Union

Authentication and Authorisation for Research and Collaboration

and all that I can see is just another … AARC TREE!

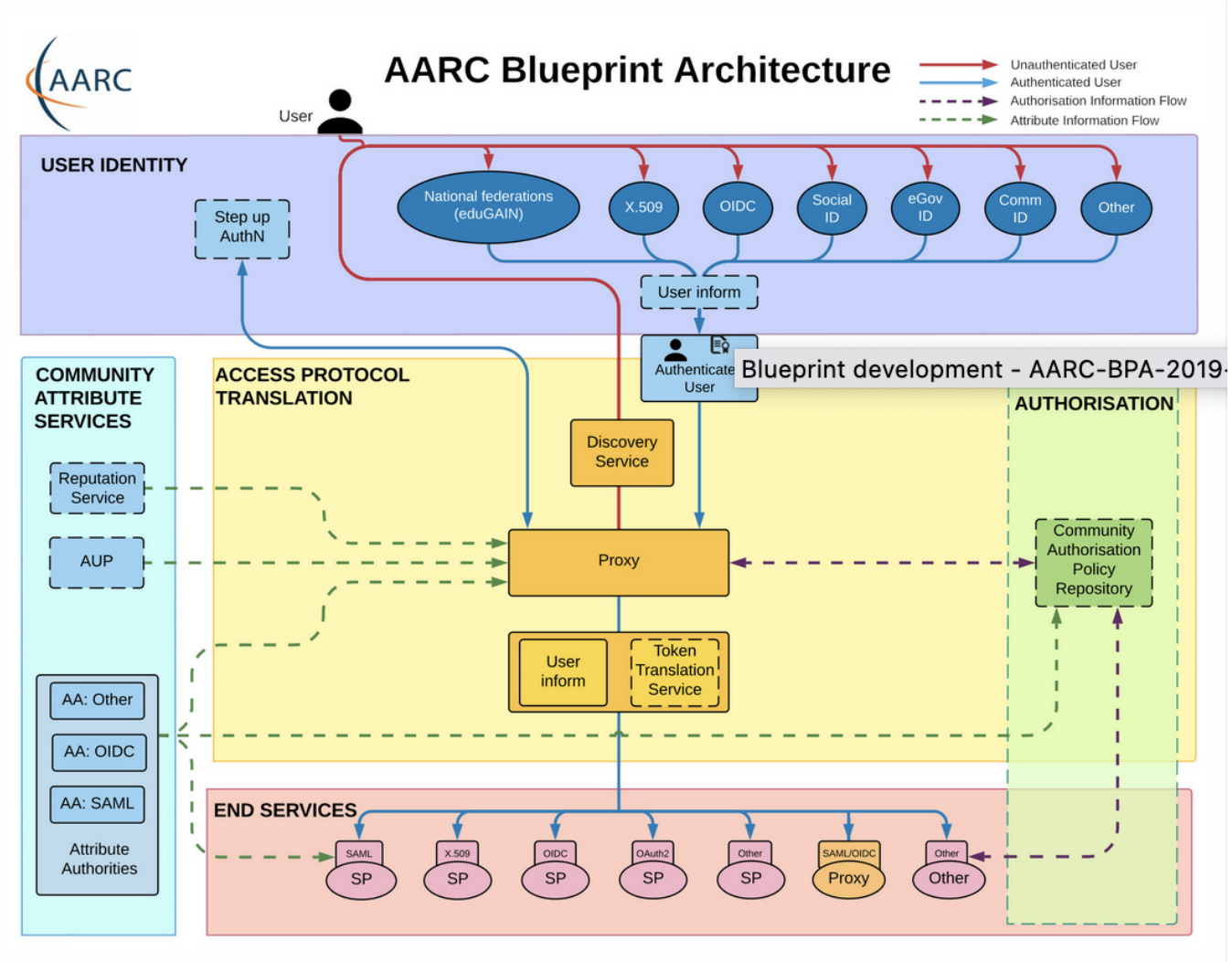
a preliminary insight in potential developments in the AARC Community

David Groep
AARC Policy Area Coordinator
Nikhef Physics Data Processing programme and UM Dept. Advanced Computing Sciences

Nikhef Maastricht University

TNC23 Workshop *Standing on the shoulders of giants*
June 2023

Arguably the best remembered picture from our AARC community



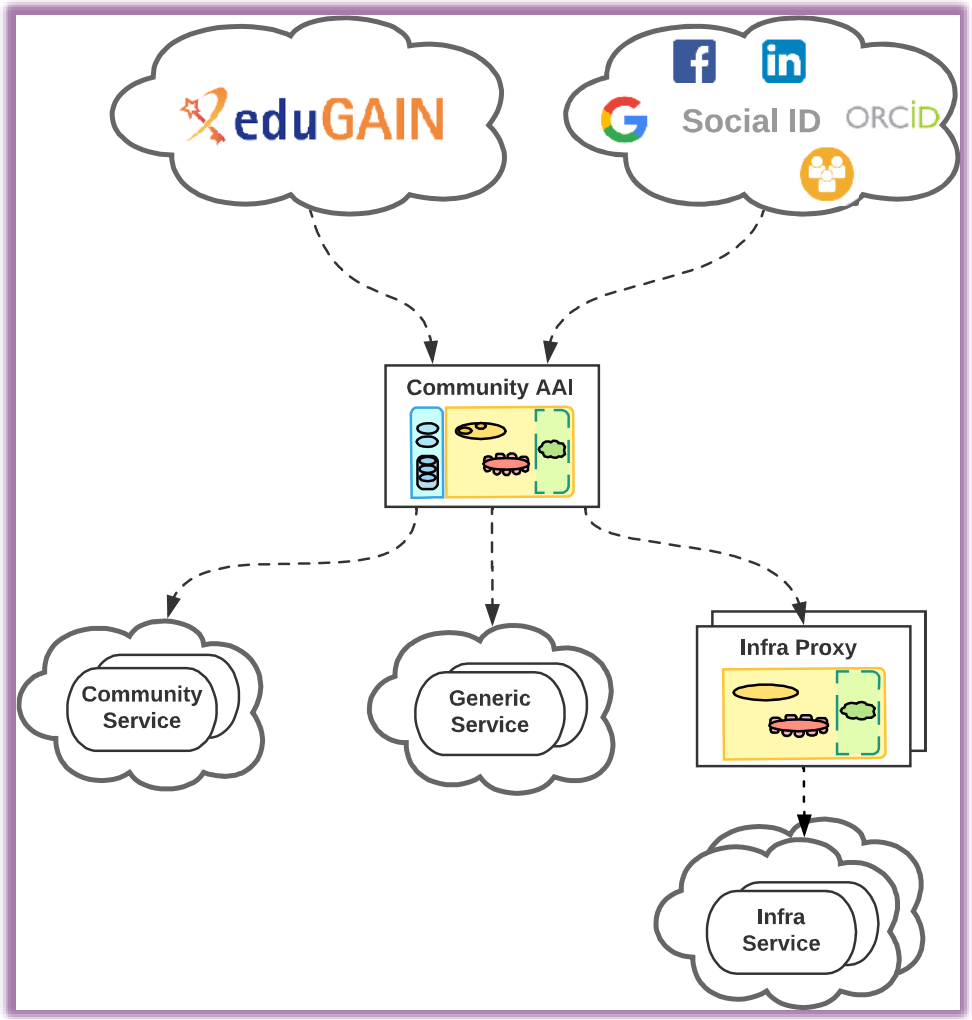
Beyond a single BPA proxy – complexities in composite infrastructure

EOSC AAI was one of the triggers to extend the BPA but is and will not be the only one!

- 2019 “BPA Reloaded” (AARC-G045) lead us to composite proxy architectures

- and as we see the need grow for multiple instances of community and e-Infra proxies to work together, we end up with …

… a federation of proxies ?! ☺



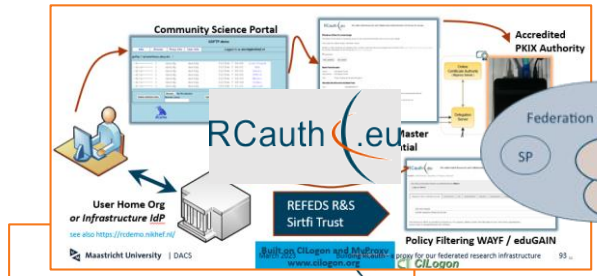
AARC G045 https://aarc-community.org/guidelines/aarc-g045/
and EOSC AAI Task Force report – ISBN 978-92-76-28113-9, DOI:10.2777/8702

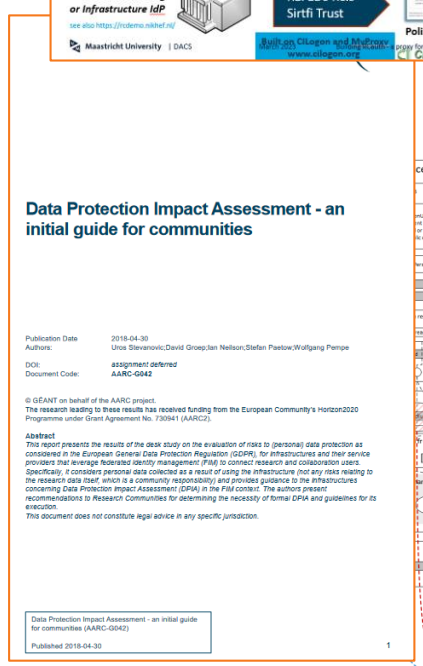
And an AARC beyond Sirtfi, RCauth, and the Policy Development Kit?

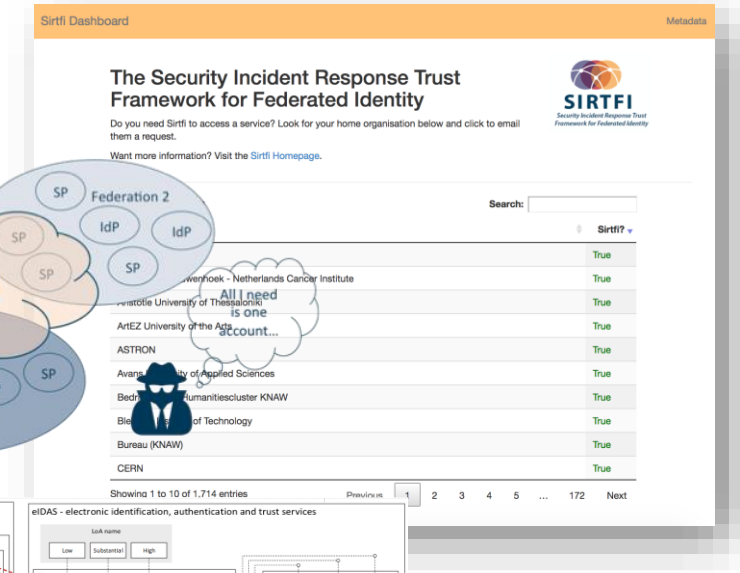
Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	Google Doc
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Google Doc
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.	Google Doc
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.	Google Doc
Policy on the Processing of Personal	Infrastructure Management & Data Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.	Google Doc
Privacy	Infrastructure	Users (view)	This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.	Google Doc
		(abide	This policy defines requirements for running a service within the Infrastructure.	Google Doc
		(abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.	Google Doc
	restrictions)			

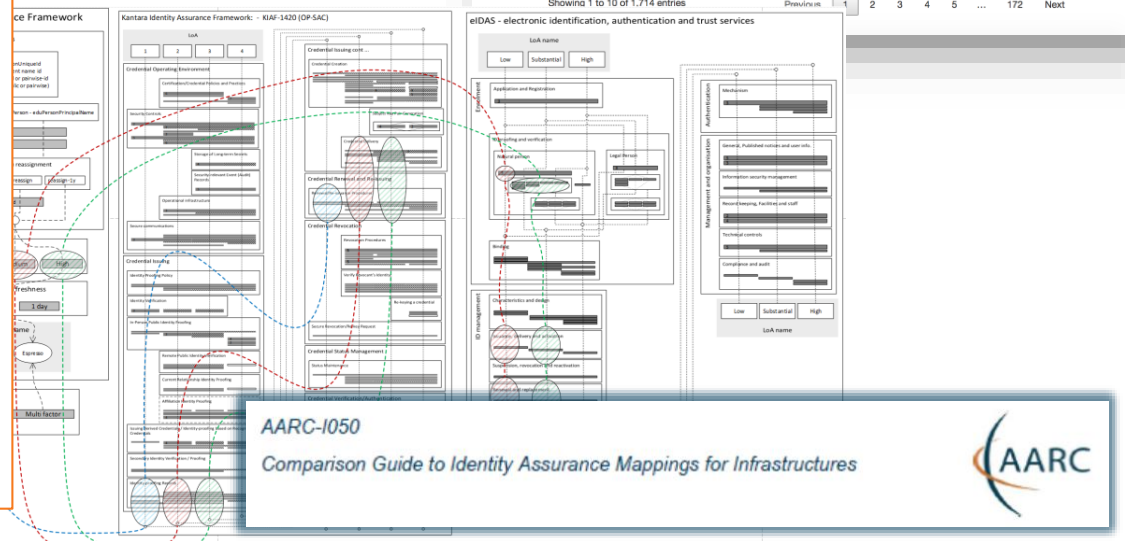
Showing 1 to 9 of 9 entries Previous Next

PDK









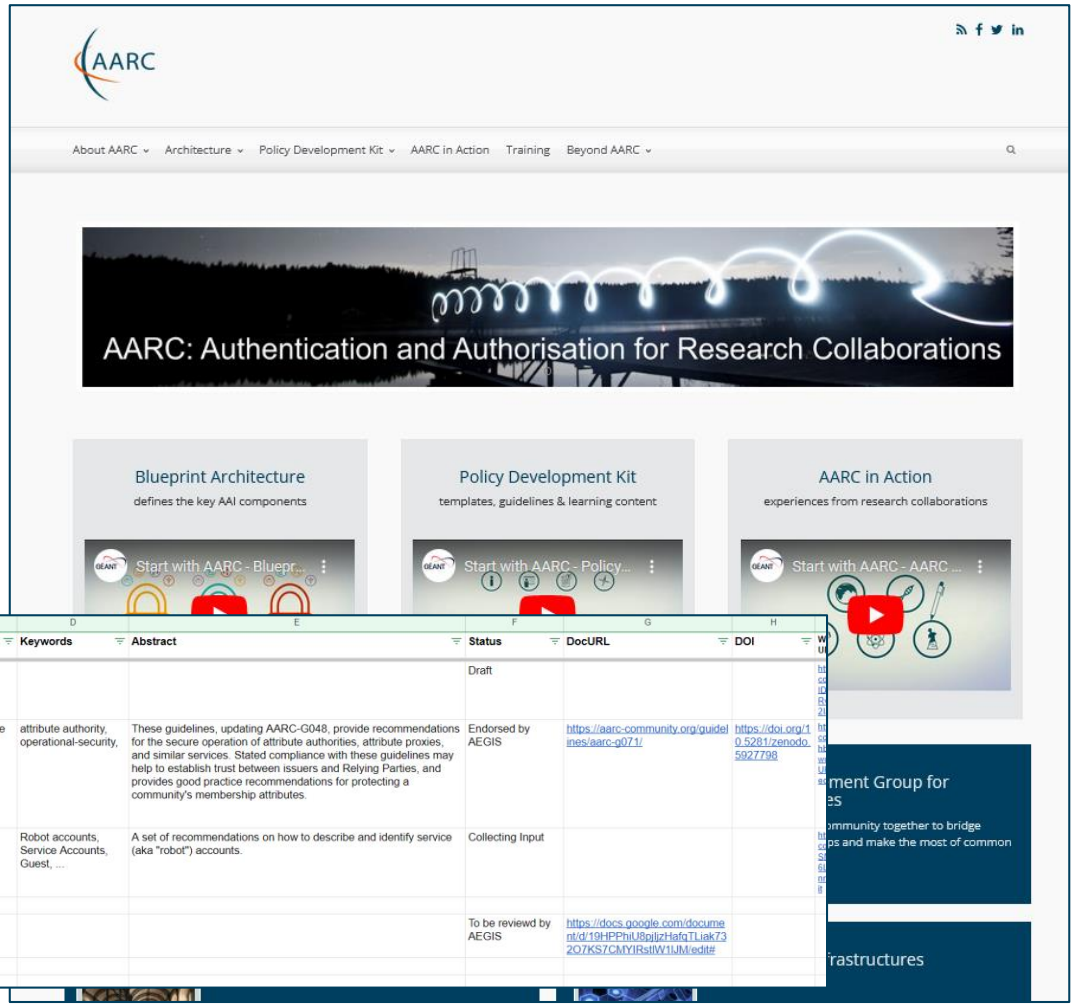
Our AARC Community

Work on structuring AAI is far from over – and the **AARC community & AEGIS** provide the framework:

- **architecture** guidelines: primary group membership, service account information, entity categories, composite BPA proxy models
- **policy** developments: 'AAOPS', trust federation 'across proxies', assurance, and community formation in the Policy Development Kit

Today supported by a range of (inter)national infrastructures and projects (like 'GN51 EnCo' & 'EOSC')

Using WISE, IGTF, REFEDS,
as open venues to convene and work



DocNum	Other Ic	Title	Keywords	Abstract	Status	DocURL	DOI
AARC-G070		Expression of primary group Membership			Draft		
AARC-G071		Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements	attribute authority, operational-security,	These guidelines, updating AARC-G048, provide recommendations for the secure operation of attribute authorities, attribute proxies, and similar services. Stated compliance with these guidelines may help to establish trust between issuers and Relying Parties, and provides good practice recommendations for protecting a community's membership attributes.	Endorsed by AEGIS	https://aarc-community.org/guidelines/aarc-g071/	https://doi.org/10.5281/zenodo.5927798
AARC-G072		Guidelines for expressing service account information	Robot accounts, Service Accounts, Guest, ...	A set of recommendations on how to describe and identify service (aka "robot") accounts.	Collecting Input		
AARC-G079		Specification of AARC Entity Categories			To be reviewd by AEGIS	https://docs.google.com/document/d/19HPPhiU8pIjzHafqTLiak732O7KS7CMYIRsIlW1IJM/edit#	
AARC-G080		AARC Blueprint Architecture 2022+					

So what are we facing now?!

- meta-federations of research infrastructures and horizontal providers
- interoperability with broader provider base, and not limited to *just* EU Wallets or SSI
- need better uptake and integration of the BPA, and in more Research Infrastructures
- a need for assurance (in FIM4R and beyond),
  without a ubiquitous source in R&E … but with govt. eID capabilities for some
- plus all the things we just heard about before!

It's time to enhance the effectiveness of the AARC BPA and PDK

leverage AARC's structuring effect to ease interoperation across thematic areas, and increase impact of the BPA in new communities (within and outside of EOSC)

Who should sit under the AARC TREE … and who do we need on board

Research Infrastructures and e-Infrastructures, both national and international facilities

- providers of resources and services for research communities, ERICs, ESFRIs, and other (data) sources

Research Communities

- scientific communities, collaborations and individual researchers, (so including our mid-sized groups)

EU and global initiatives

- International Data Spaces Association (IDSA), GAIA-X, EU ID Wallets, FIM for Research (FIM4R), &c

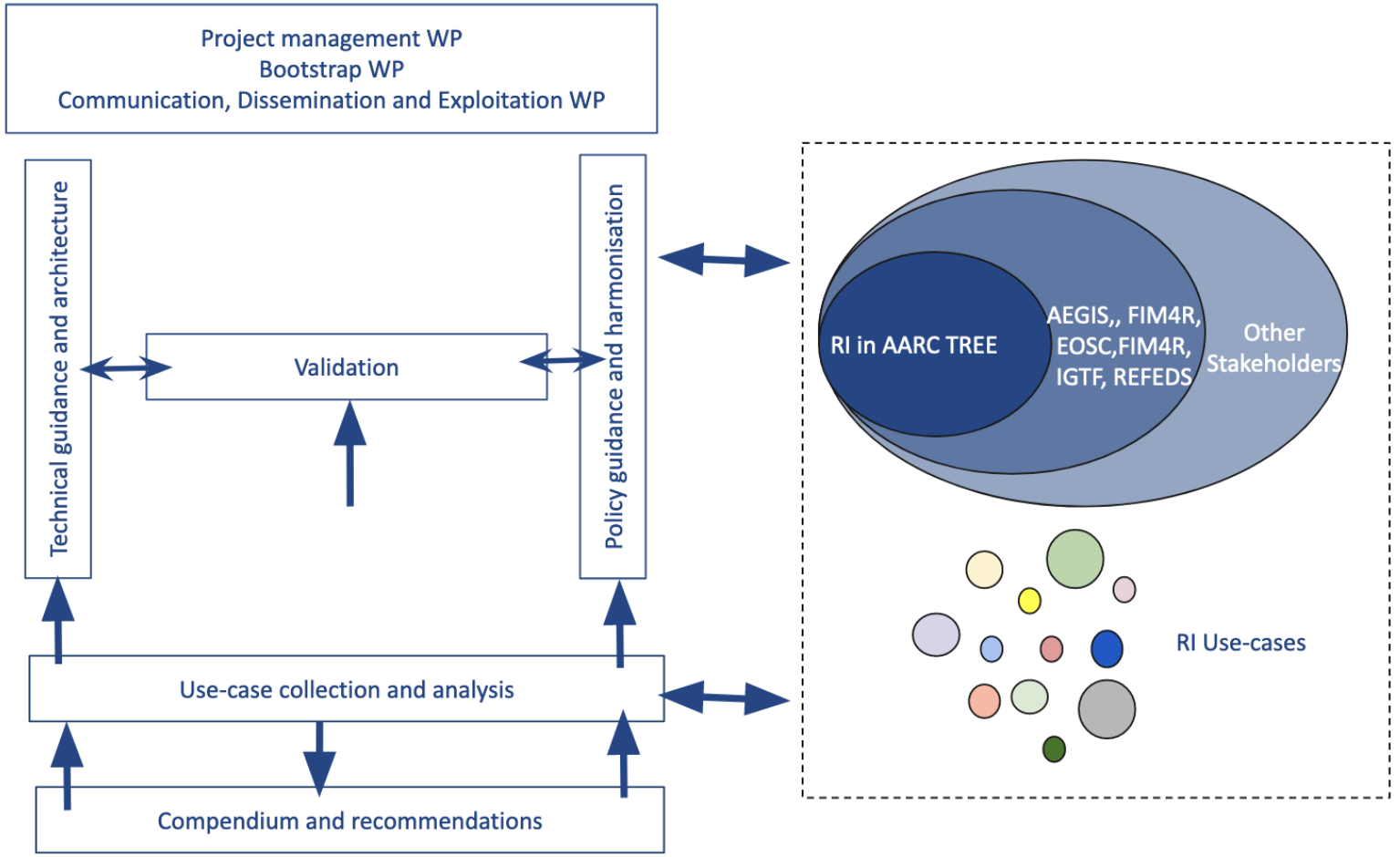
Service and resource providers:

- AAI and other providers interested in offering their services and resources to researchers

EOSC Ecosystem

- EOSC related initiatives like EOSC Association Task Forces and other EOSC projects

Growing an AARC TREE



sprouting an evolved architecture

Evolution of the AARC Blueprint Architecture

- including a more prominent role for OpenID Connect federation
- federated authorization mechanisms

Harmonisation of community user attributes

- application integration across different protocols

OpenID Connect Federations

- deployment profile of the specification
- addressing the challenges we face now in the heterogeneous EOSC AAI ecosystem

Authorisation for Federated Resources

- authorization policy interoperability

Decentralised Identities

- EU Digital Identity Wallet, distributed Identifiers, verifiable creds & presentations, decentralised storage

and evolved AARC policy development

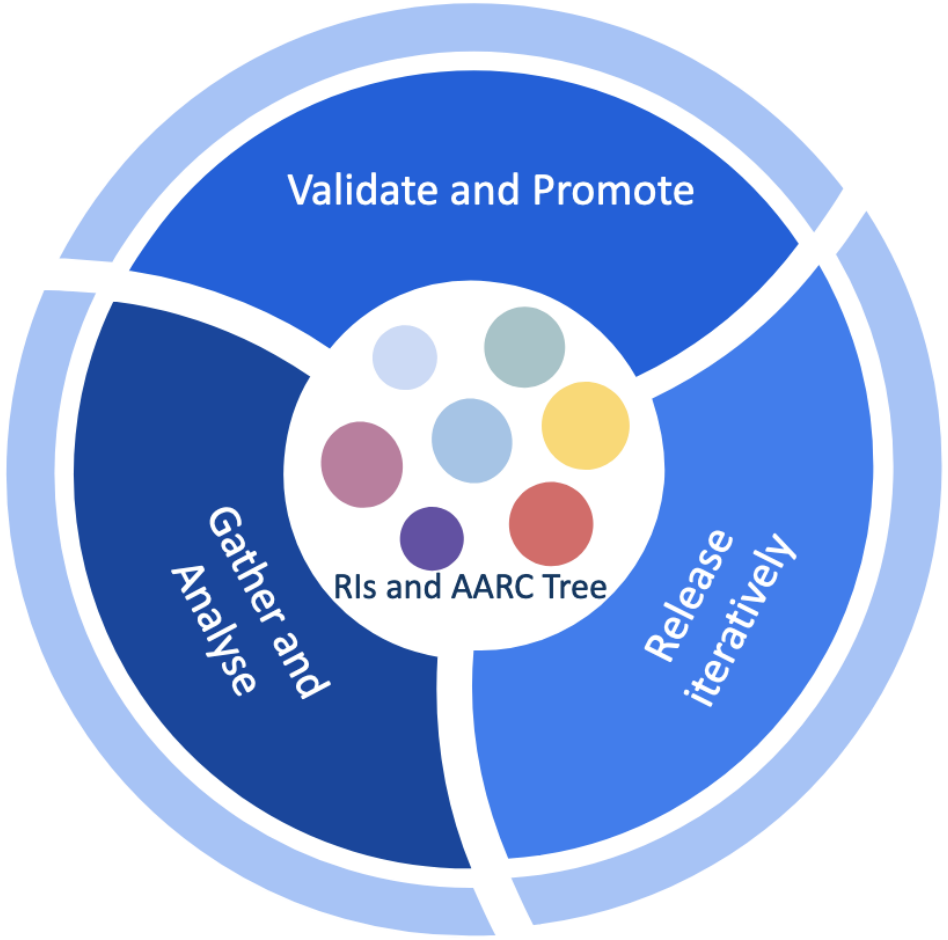
Research-infrastructure alignment and policy harmonisation

- Operational Trust for Community and Infrastructure BPA Proxies
- Snctfi - increasing acceptance of research infrastructure proxies with R&E identity providers and sources of authentication
- Review infrastructure models for **coordinated AUP, T&C, and privacy notices**, improving cross-infrastructure user experience

User-centric trust alignment and policy harmonisation

- Lightweight community management policy template
- Guideline on cross-sectoral trust in novel federated access models
- Assurance in research services through (eIDAS) public identity assertion
- FIM4R policy workshop series on validation of the restructured policy framework (together with the new 'BPA')

A proven methodology



- Provide guidance based on a broad and open community process: FIM4R, EOSC, AEGIS, WISE, REFEDS, IGTF, AppInt, …
- Experts gather in open, dedicated teams
- Iterative stakeholder engagement
- practical validation in use cases of the research and e-infras, e.g. through AEGIS

We need our collaborators and stakeholders … and thus: you!

Use Cases Collection and Analysis

- with the large ESFRI RIs, clusters, and national nodes to validate BPA effectiveness and
  act as a flywheel to increase its application

followed by adoption and validation

Compendium & Recommendations

- have the validators and use cases have a broader impact by promoting them as ‘community good practice’ examples – and telling the world about it.

The ‘Compendium’ model helped us before ☺

just some of the RIs that are looking for a BPA with enhanced effectiveness

What would be the presents under a (funded) AARC Tree?

- **Updated AARC Blueprint architecture** for emerging technologies and services in pan-European research infrastructures
  - Up-to-date guidance on implementing the architecture of their Authentication and Authorisation Infrastructure service components, incorporating new requirements, use cases and new technologies.
- Recommendations for a **common long-term strategy for AAI services and best practices**
  - AARC TREE best practices and recommendations with new technical approaches and collaboration in its implementation across scientific domains
- Updated **interoperability framework**
  - Framework to harmonise AAI policies to empower identity providers, service providers and user communities to identify interoperable policies for the open science vision.

Thank you

Any Questions?

davidg@nikhef.nl

AARC

https://aarc-community.org

Any and all information in this document SHOULD NOT be construed as an endorsement of any particular organisation or plan. All information subject to change without notice. Information presented here MUST NOT be quoted out of context. (RFC 2119)

Lemon tree image: Tomwsulcer, https://commons.wikimedia.org/wiki/File:Lemon_Tree_in_Santa_Clara_California.jpg