The journey to knowing your users

Experiences on federated access and reaching reasonable LoA in the Puhuri-project

Anders Sjöström, Lund University

GARR 2023

Who are we?

Anders Sjöström
Puhuri Project Manager

Marina Adomeit (sunet)
Puhuri Project AAI Manager

Eivind Lysø (Sikt)
Puhuri Project AAI activity lead

Ilja Livenson (University of Tartu)
Puhuri Project Activity 3 lead

Jarno Laitinen (CSC)
Puhuri Project Activity 2 Lead

Pål Axelsson (sunet)
Puhuri Project AAI Manager

About Puhuri and LUMI

PUHURI

Food for thought

World's 20 Happiest Countries in 2022

1. Finland
2. Denmark
3. Iceland
4. Israel
5. Netherlands
6. Sweden
7. Norway
8. Switzerland
9. Luxembourg
10. New Zealand
11. Austria
12. Australia
13. Canada
14. Ireland
15. United States
16. Germany
17. Belgium
18. Czech Republic
19. United Kingdom
20. Lithuania

Food for thought

World's 20 Happiest Countries in 2022

1. Finland
2. Denmark
3. Iceland
4. Israel
5. Netherlands
6. Sweden
7. Norway
8. Switzerland
9. Luxembourg
10. New Zealand
11. Austria
12. Australia
13. Canada
14. Ireland
15. United States
16. Germany
17. Belgium
18. Czech Republic
19. United Kingdom
20. Lithuania

Food for thought

World's 20 Happiest Countries in 2022

1. Finland
2. Denmark
3. Iceland
4. Israel
5. Netherlands
6. Sweden
7. Norway
8. Switzerland
9. Luxembourg
10. New Ze...
11.
...
1...many
17. Belgium
18. Czech Republic
19. United Kingdom
20. Lithuania

8 of 20 are serviced by Puhuri

What is Puhuri

- A system to facilitate easy and efficient access to high-performance computing (HPC) and related services throughout Europe
- The key objective is to minimize the administrative costs of service providers while simultaneously improving the useability of these services
- To be achieved by establishing federated services for Authentication and Authorization Infrastructure (AAI) as well as resource allocation services
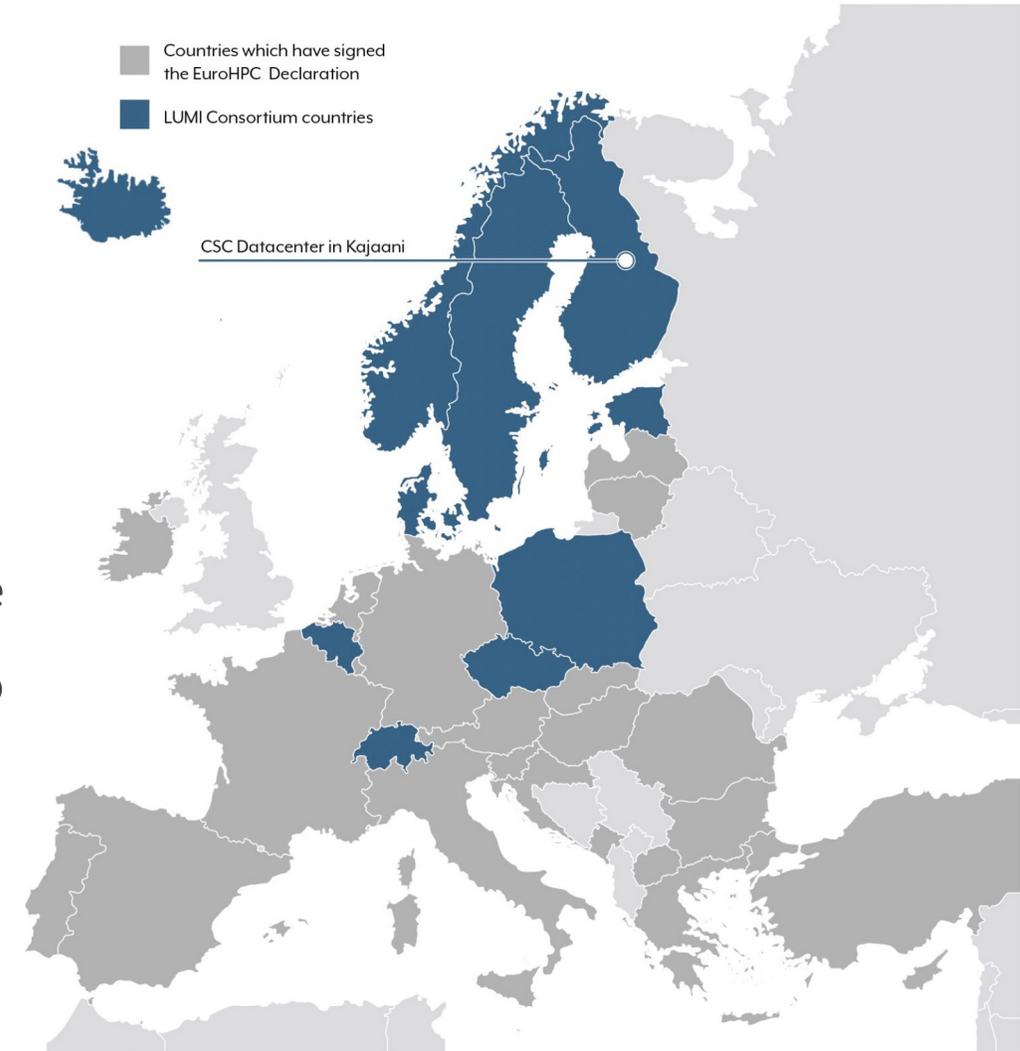
Why Puhuri?

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

PUHURI

What is LUMI

- LUMI, one of the **EuroHPC pre-exascale** supercomputers, located at CSC's data centre in Kajaani, Finland

- The supercomputer is hosted by the **ten European countries** of the LUMI consortium:

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

- Bringing together their unique expertise and experience, these countries together provide added value for the whole of Europe

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

Countries which have signed the EuroHPC Declaration

LUMI Consortium countries

CSC Datacenter in Kajaani

neic
PUHURI

LUMI

So we need to know our users…

- Identity
- Access
- Utilization
- Cost
- Traceability

MyAccessID and Puhuri Access Management

MyAccessID serving the HPC community

Strive towards seamless user experience and ease of access

HPC community should focus on resource allocation and "outsource" user identification part

Support federation of euroHPC resources

Streamline user access

Unifi access policies as much as possible

Funnel requirements towards R&E federated identities

Implement solutions where R&E federated identities are not available or of sufficient quality

Initial requirements

Users: Researchers, industry, public sector

Rely on the R&E federated identities in eduGAIN

Enable existing community IdPs to connect

Enable use of eIDAS

Solution for industry and public sector

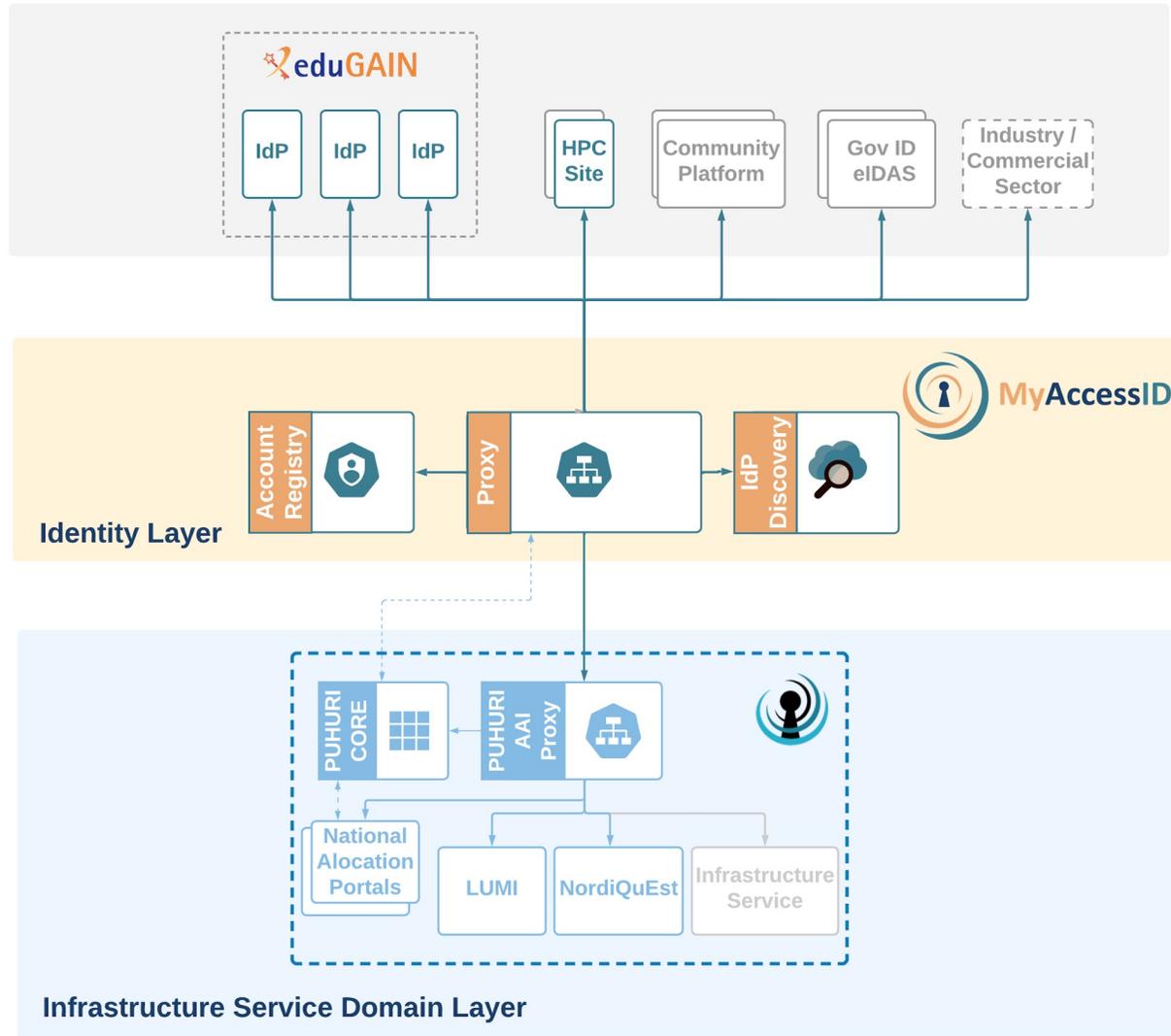Solution for users without federated identity

Authentication characteristics

Enable Multi-factor authentication

Enable SSH access to compute resources

Identity characteristics

Minimum set of attributes

Minimum identity proofing

PUHURI

PUHURI access management and MyAccessID

PUHURI 1 project start

MyAccessID & PUHURI Design

MyAccessID & PUHURI Pilot

LUMI Pilots

2020

Policy for Quality of Identities/LoA

MyAccessID & PUHURI Production

2021

LUMI General Availability

Community coordination on LoA

2022

Implement policy on LoA

External Identity Vetting

2023

MFA - Strong Authentication

2024

PUHURI access management and MyAccessID

PUHURI project start ● 2020

MyAccessID & PUHURI Design ●

Collaboration with Fenix ●

MyAccessID & PUHURI Pilot ●

LUMI Pilots ○

Policy for Quality of Identities/LoA ● 2021

MyAccessID & PUHURI Production ●

MyAccessID & Fenix decision ●

LUMI General Availability ○ 2022

Community coordination on LoA ●

Implement policy on LoA ●

External Identity Vetting ● 2023

MyAccessID & Fenix migration ●

MFA - Strong Authentication ● 2024
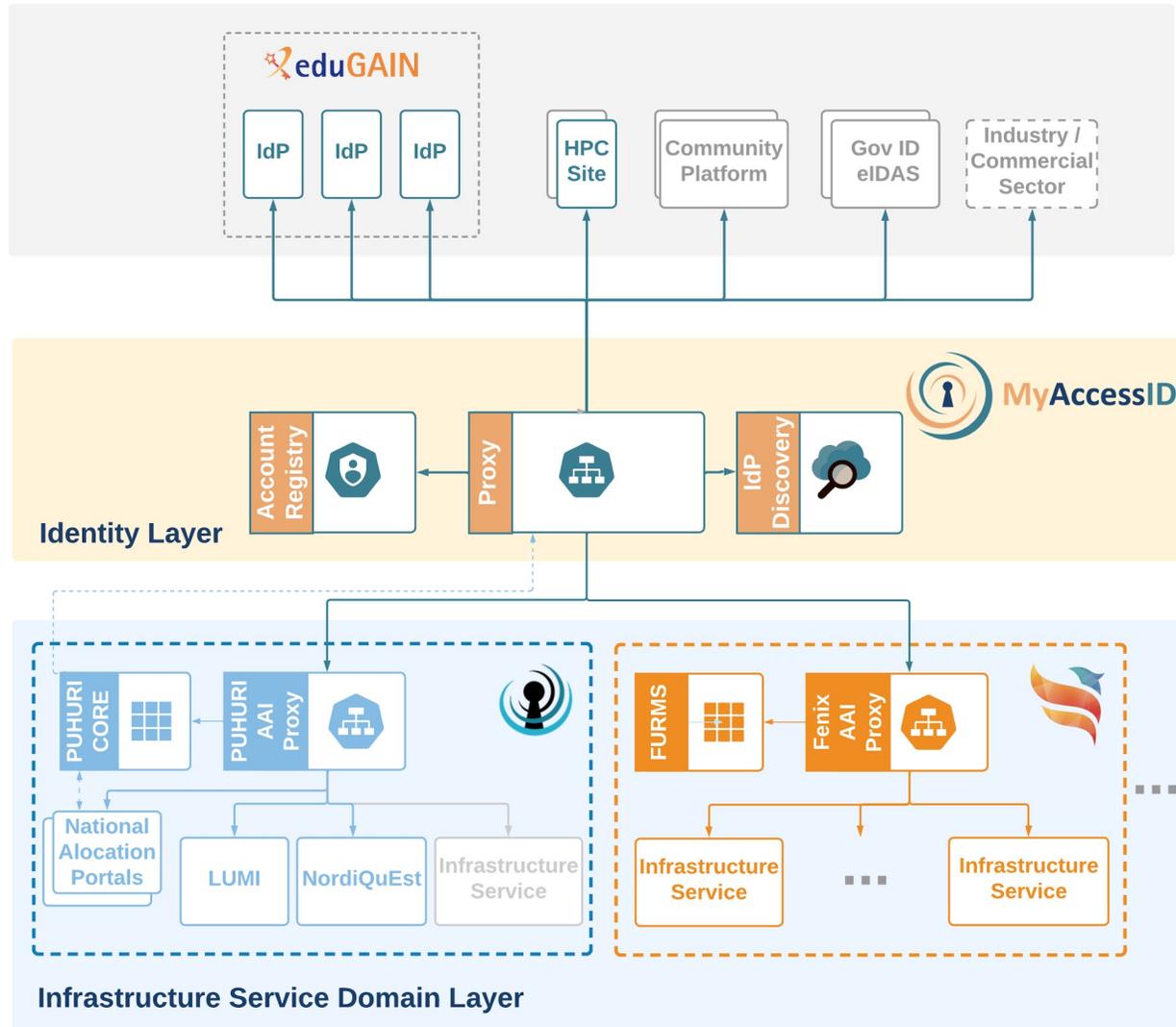
Journey of the LoA Implementation

Level of Assurance implementation plan and... reality

Plan

LoA requirements socialised within LUMI consortium and wider

LUMI requirements translated into LoA

| 2021 | 2022 | 2023 |

Reality

Well accepted, half of the partners declared support by their federation already

neic
PUHURI

Level of Assurance and Attribute Requirements

Attribute requirements

https://puhuri.neic.no/idp_integration/attributes/

Identifier

Name

email

Affiliation

Assurance

Organisation

Level of assurance requirements

REFEDS Assurance Framework https://wiki.refeds.org/display/ASS

To insure sufficient **identity proofing and credential issuance, renewal, and replacement**

https://refeds.org/assurance/IAP/medium; or

https://refeds.org/assurance/IAP/high

To insure **identifier uniqueness**

https://refeds.org/assurance/ID/UNIQUE; or

https://refeds.org/assurance/ID/eppn-unique-no-reassign

PUHURI

Level of Assurance implementation plan and... reality

Plan

LoA requirements socialised within LUMI consortium and wider

MyAccessID warning message 1. March deadline

LUMI requirements translated into LoA

Regular coordination with federation operators

2021	2022	2023

Reality

Well accepted, half of the partners declared support by their federation already

Well received, triggered internal discussion to adopt LoA in several federations

LoA tracking shows about 15% adoption

neic
PUHURI

Level of Assurance implementation plan and... reality
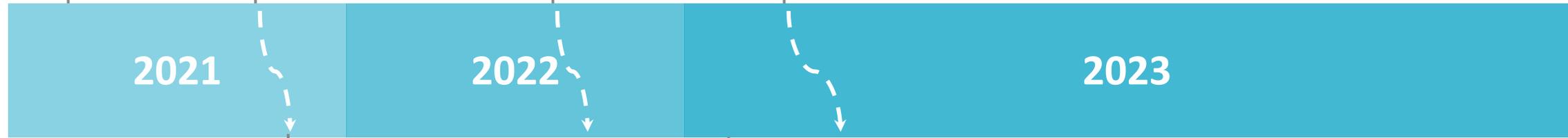
Plan

2021 **2022** **2023**

Reality

LUMI requirements translated into LoA

LoA requirements socialised within LUMI consortium and wider

Regular coordination with federation operators

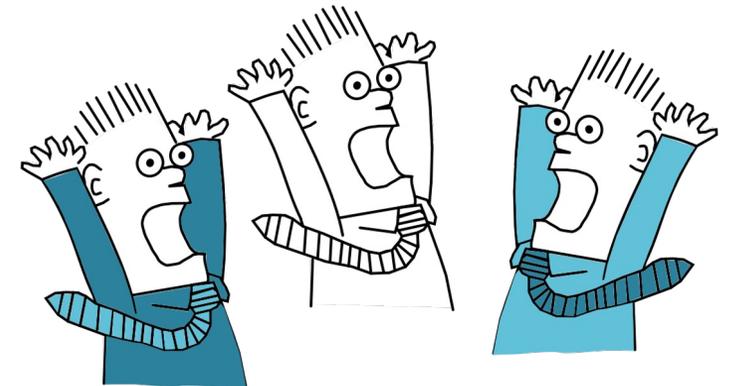MyAccessID warning message 1. March deadline

Well accepted, half of the partners declared support by their federation already

Well received, triggered internal discussion to adopt LoA in several federations

LoA tracking shows about 15% adoption

Users react

neic
PUHURI

Tickets from users and identity providers

User of Alfa university reports that they "login as another user" => IdP was releasing duplicate user identifiers

A Boo University confirms that they can not release identifier uniqueness assurance as it is not supported by University's policy

University of Foo had misconfigured assurance values that they were releasing and this was fixed

Schoo University confirms that they can not release assurance information as they don't maintain this information in the user identity

Moo University has a process of elevating assurance of individual user accounts, based on a request

neic
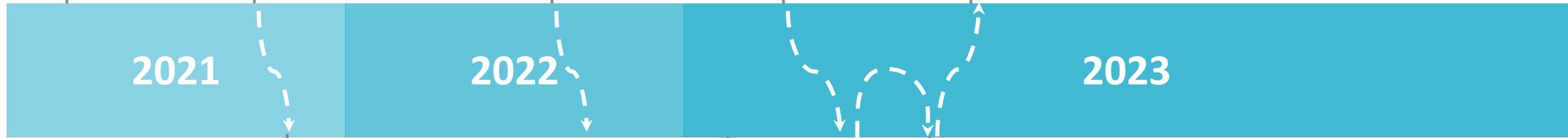PUHURI

Level of Assurance Implementation plan and... reality

Plan

LoA requirements socialised within LUMI consortium and wider

MyAccessID warning message 1. March deadline

LUMI requirements translated into LoA

Regular coordination with federation operators

Deadline changed for later in 2023
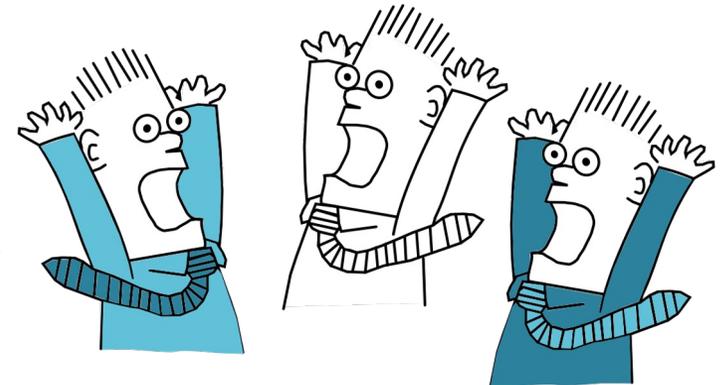
2021

2022

2023

Reality

Well accepted, half of the partners declared support by their federation already

Well received, triggered internal discussion to adopt LoA in several federations

LoA tracking shows about 15% adoption

Users react

LUMI reacts

MyAccessID (New) Warning Message

Dear Boo Wooo,

The digital identity provided by your organization when you log in to this service does not meet the required levels for assuring your identity.

During 2023 this will become a mandatory requirement for you to continue to access LUMI HPC resources. We are working on solutions for the level of assurance of your identity, and to speed up this process it would be helpful if you could send the information below to the indicated IT support for your organization.

If your organization cannot meet the requirements, you will be provided with an alternative to assure your identity and continued access. If so, this will be communicated to you in good time before the requirement is in effect.

To: support@example.idp.org

Subject: Request to support the required level of assurance for MyAccessID/LUMI EuroHPC
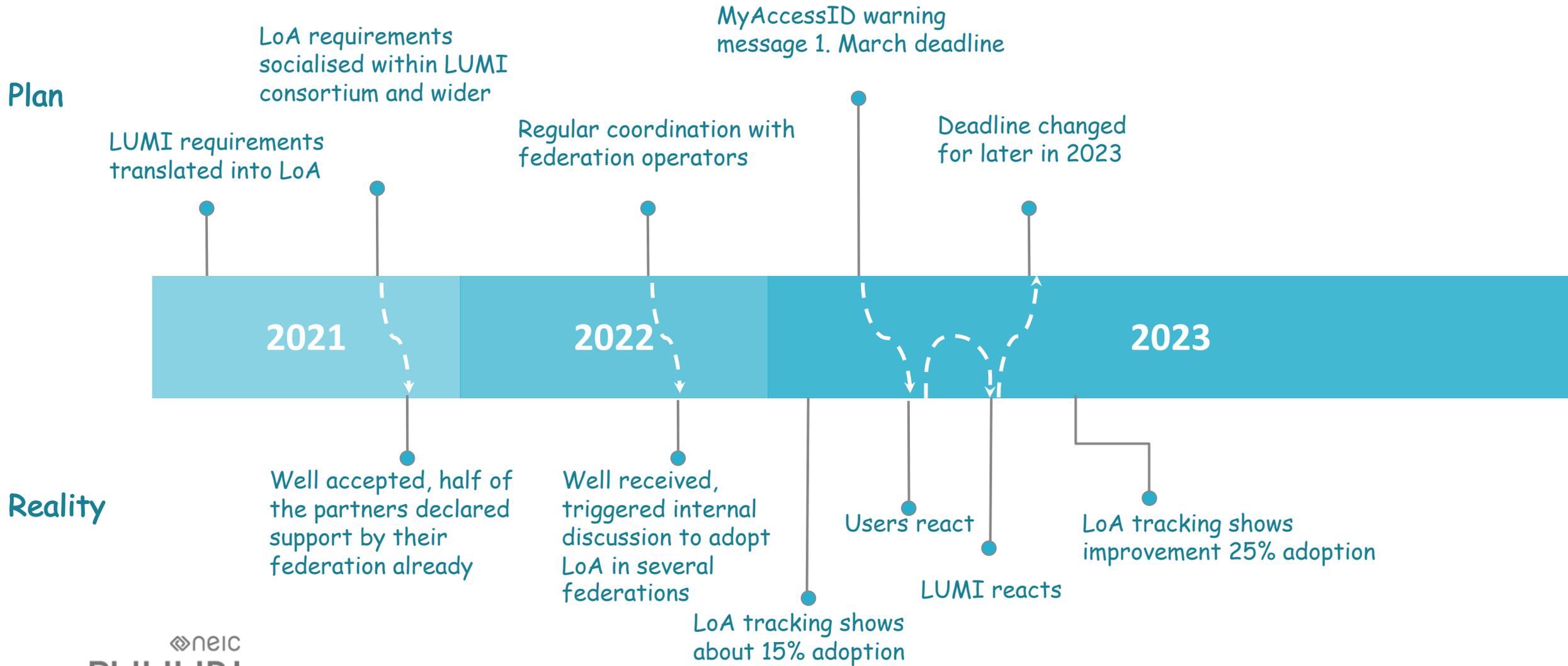
Dear Example IdP support,

For the users of our institution to access MyAccessID (entityID: https://proxy.myaccessid.org/metadata/backend.xml), our institution needs to release the required levels of assurance as it is described here: https://puhuri.neic.no/idp_integration/requirements-edugain/

It is important for the users of our institution to support this requirement as soon as possible, as services such as EuroHPC LUMI supercomputer are requesting that in order to trust the identity provider's information for legal reasons.

Thank you in advance,
Boo Wooo

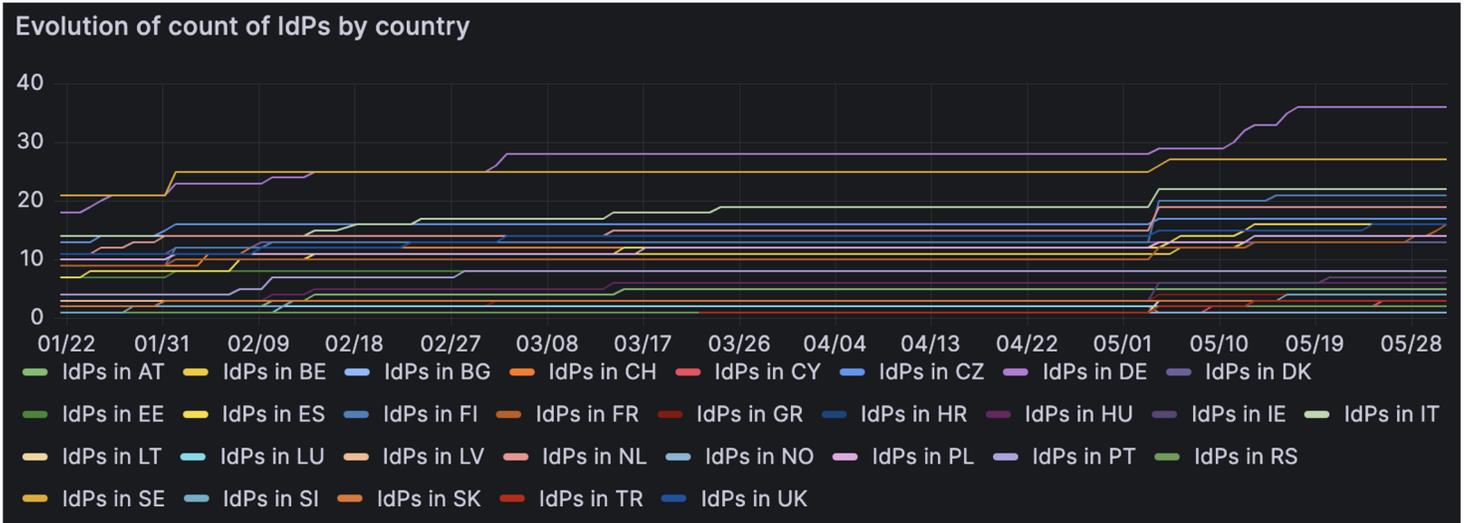# Level of Assurance implementation plan and... reality

Plan

LoA requirements socialised within LUMI consortium and wider

MyAccessID warning message 1. March deadline

LUMI requirements translated into LoA

Regular coordination with federation operators

Deadline changed for later in 2023

2021

2022

2023

Well accepted, half of the partners declared support by their federation already

Well received, triggered internal discussion to adopt LoA in several federations

Users react

LoA tracking shows improvement 25% adoption

Reality

LUMI reacts

LoA tracking shows about 15% adoption

neic
PUHURI

European Identity Provider Attribute Release Statistics

30 Countries

187 IdPs

308 IdPs

1650 Users
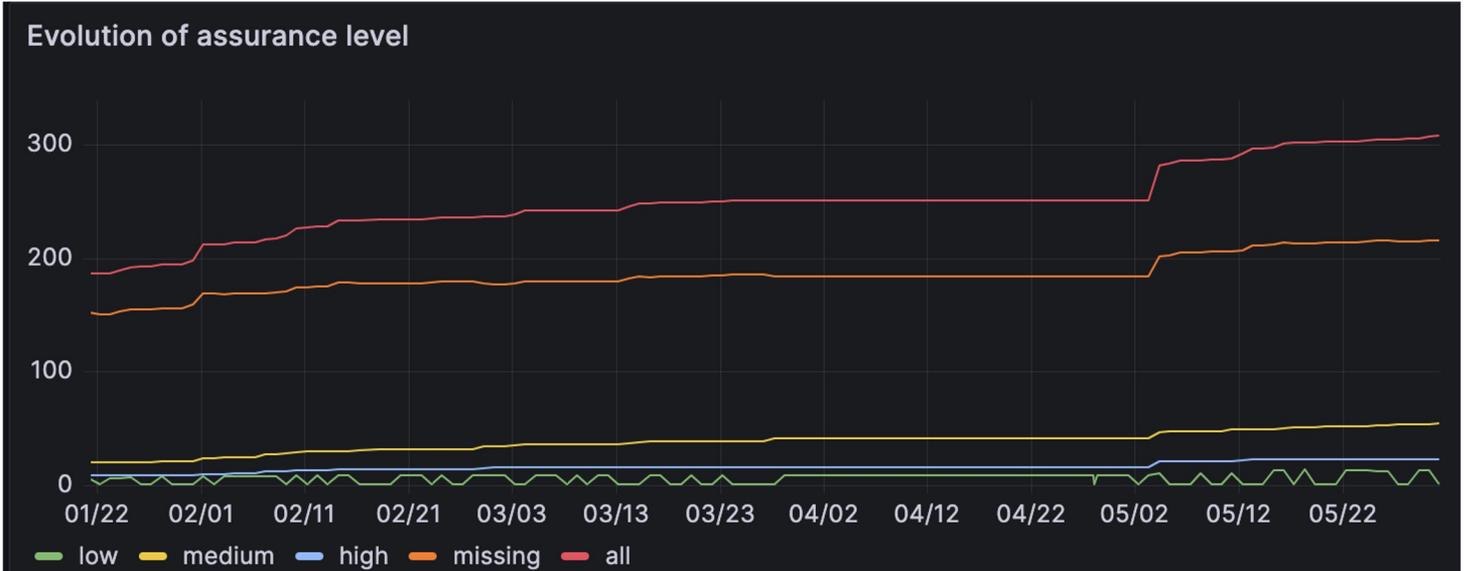
27 LoA Med./High

78 LoA Med./High

Level of Assurance implementation plan and... reality

Plan

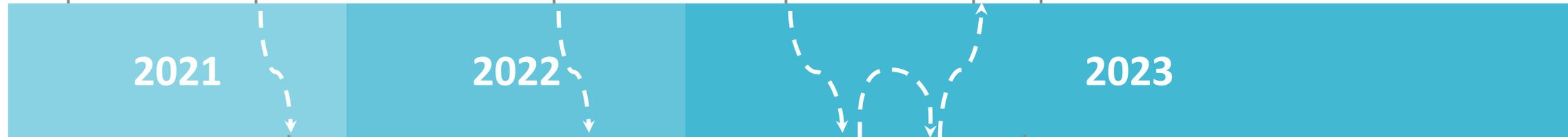LoA requirements socialised within LUMI consortium and wider

LUMI requirements translated into LoA

Regular coordination with federation operators

MyAccessID warning message 1. March deadline

Deadline changed for later in 2023

Start to work on alternative solution: Identity vetting

2021   **2022**   **2023**

Reality

Well accepted, half of the partners declared support by their federation already

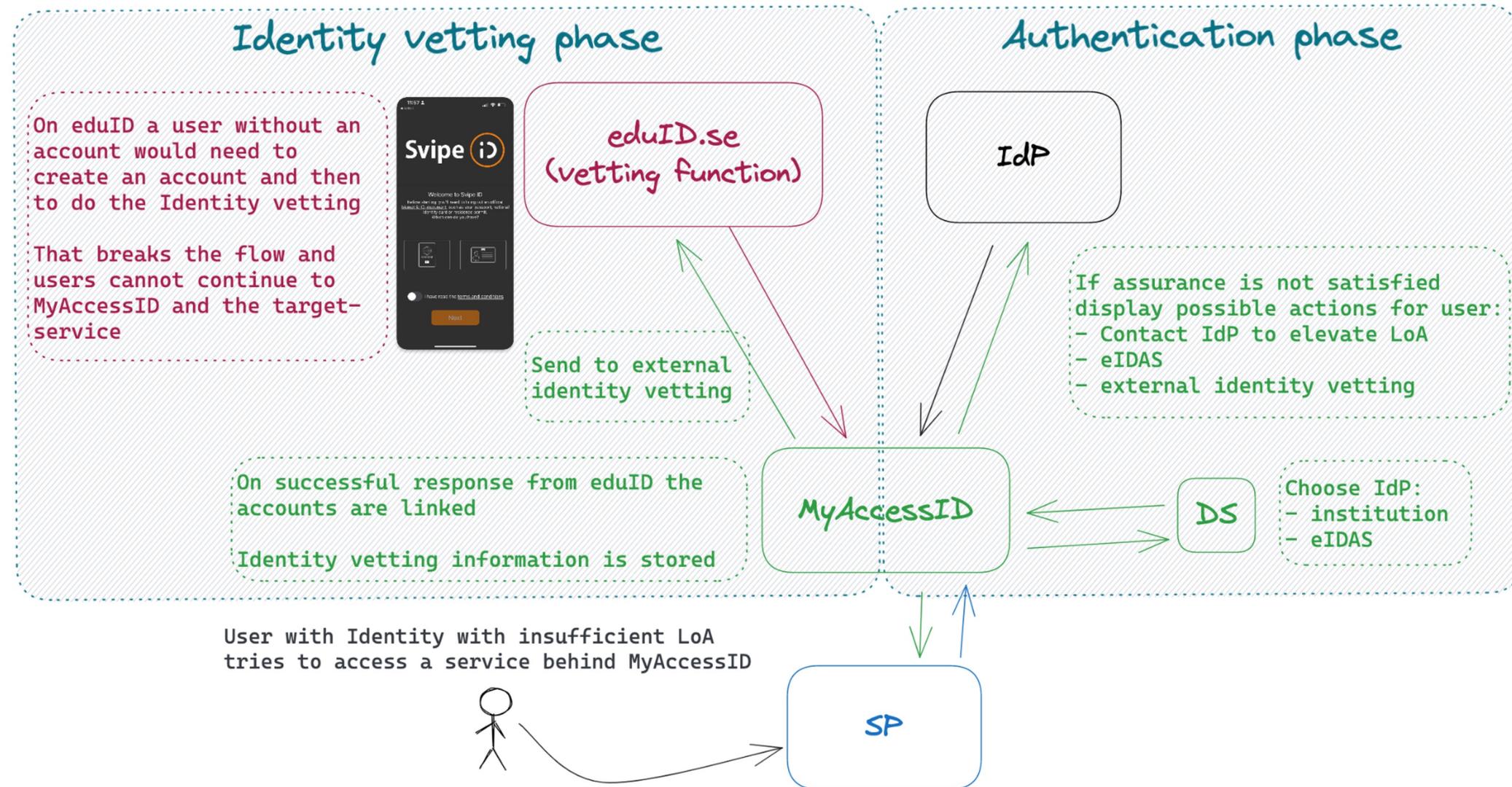Well received, triggered internal discussion to adopt LoA in several federations

Users react

LUMI reacts

LoA tracking shows improvement 25% adoption

LoA tracking shows about 15% adoption

neic
PUHURI

Flow with external Identity Vetting

Identity vetting phase

On eduID a user without an account would need to create an account and then to do the Identity vetting

That breaks the flow and users cannot continue to MyAccessID and the target-service

eduID.se (vetting function)

Send to external identity vetting

On successful response from eduID the accounts are linked

Identity vetting information is stored

Authentication phase

IdP

If assurance is not satisfied display possible actions for user:
- Contact IdP to elevate LoA
- eIDAS
- external identity vetting

MyAccessID

DS

Choose IdP:
- institution
- eIDAS

User with Identity with insufficient LoA tries to access a service behind MyAccessID

SP

Level of Assurance implementation plan and... reality

Plan

LoA requirements socialised within LUMI consortium and wider

LUMI requirements translated into LoA

Regular coordination with federation operators

MyAccessID warning message 1. March deadline

Deadline changed for later in 2023

Start to work on alternative solution: Identity vetting

Identity vetting through eduid.se implemented

LoA policy enforced

2021   2022   2023

Reality

Well accepted, half of the partners declared support by their federation already

Well received, triggered internal discussion to adopt LoA in several federations

LoA tracking shows about 15% adoption

Users react

LUMI reacts

LoA tracking shows improvement 25% adoption

neic

PUHURI

Federation Operators Feedback

Likelihood of implementation
- From 100%,
- to We are getting there,
- to We need more incentives for IdPs to drive the adoption

Incentives for IdPs
- Need high profile SPs to request the LoA
- Make the LoA mandatory

How to help
- Quality documentation in one place
- Provide more information to nag the users
- Clear deadlines

# Key takeaways

Conclusion

THE GOOD
- Federated access to resources is possible and desired
- Interesting possibilities with access to reasonable LoA
- Elevation of LoA is possible via identity vetting on top of the federated identity
- Federating resources makes for a scalable solution

THE BAD
- Low uptake on exposure of LoA
- The threat of losing access is too large a cannon

THE UGLY
- Hard to exert pressure to motivate IdPs to improve the release of LoA information

neic
PUHURI
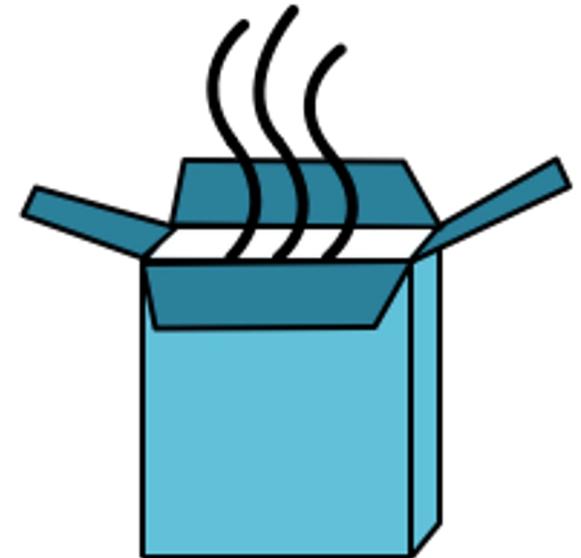
Thank you for attention!

Questions?

support@puhuri.io

PUHURI