The journey to knowing your users

Experiences of implementing RAF for access to LUMI EuroHPC

Marina Adomeit, SUNET
T&I Townhall, Stockholm, October 2023
About Puhuri and LUMI
What is LUMI and Puhuri

- **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 is a system to facilitate easy and efficient access to high-performance computing (HPC) and related services throughout Europe
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 (name, email, identifier, affiliation, organisation, assurance)
- Minimum identity proofing
  https://puhuri.neic.no/idp_integration/attributes/
Access control to supercomputer resources

Identification of the users

Resource allocation and management

Out of scope for PUHURI

In scope for PUHURI
PUHURI access management and MyAccessID

PUHURI project start
MyAccessID & PUHURI Design
Collaboration with Fenix
MyAccessID & PUHURI Pilot
LUMI Pilots
Policy for Quality of Identities/LoA
MyAccessID & PUHURI Production
MyAccessID & Fenix decision
LUMI General Availability
Community coordination on LoA
Implement policy on LoA
External Identity Vetting
MyAccessID & Fenix migration
MFA - Strong Authentication
Journey of the LoA Implementation
Level of Assurance and Attribute Requirements

**Attribute requirements**

- Identifier
- Name
- Email
- Affiliation
- Assurance
- Organisation

**Level of assurance requirements**

**REFEDS Assurance Framework** [https://wiki.refeds.org/display/ASS](https://wiki.refeds.org/display/ASS)

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

- [https://refeds.org/assurance/IAP/medium](https://refeds.org/assurance/IAP/medium); or
- [https://refeds.org/assurance/IAP/high](https://refeds.org/assurance/IAP/high)

To insure *identifier uniqueness*:

- [https://refeds.org/assurance/ID/UNIQUE](https://refeds.org/assurance/ID/UNIQUE); or
- [https://refeds.org/assurance/ID/eppn-unique-no-reassign](https://refeds.org/assurance/ID/eppn-unique-no-reassign)

[https://puhuri.neic.no/idp_integration/attributes/](https://puhuri.neic.no/idp_integration/attributes/)
Identity Provider Attribute Release Statistics

https://wiki.geant.org/display/MyAccessID/IdP+Status+Report
European Identity Provider Attribute Release Statistics

- 187 IdPs
- 393 IdPs
- 33 Countries
- >2k Users
- 27 LoA Med./High
- 88 LoA Med./High
Level of Assurance implementation plan and... reality

Plan

- 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

Reality

- 2021: LUMI requirements socialised within LUMI consortium and wider
- 2022: LoA policy enforced
- 2023: LoA requirements well accepted, half of the partners declared support by their federation already
- Identity vetting through eduid.se implemented

- Users react
- LUMI reacts
- LoA tracking shows about 15% adoption
- LoA tracking shows improvement 23% adoption
- Well received, triggered internal discussion to adopt LoA in several federations
- Well accepted, half of the partners declared support by their federation already
Challenges with implementing RAF 1.0

• There is no signaling of IdP capabilities
  ○ Difficult to make decision about enforcement of LoA early on
  ○ Difficult to re-inforce LoA later on
• It is very difficult for IdP admins to interpret RAF 1.0 LoA medium and high requirements into operational decisions, and even for federation operators to support them
• Access to EuroHPC is high profile but low volume use case, not enough traction
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.

On successful response from eduID the accounts are linked
Identity vetting information is stored

Send to external identity vetting

MyAccessID

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

Authentication phase

eduID.se (vetting function)

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

Choose IdP:
- institution
- eIDAS

DS

IdP

SP
Thank you for attention!

Questions?

support@puhuri.io