

Federated Identity Management Protecting Access to your Research Data

David Kelsey (STFC), Hannah Short (CERN), Carlo Maria Zwölf

Welcome

Session organised by the RDA Federated Identity Management Interest Group* - thank you for joining!

Aims of today

- Begin to dissect how our research communities can use assurance
- Learn about best practices for protecting research collaborations
- Learn about the EOSC strategy for protecting multiple research collabs.

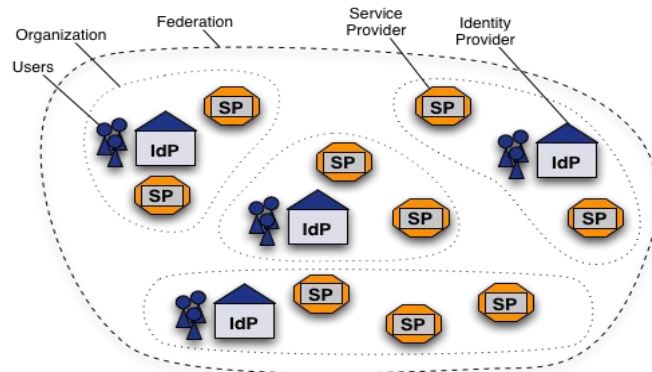
* <https://www.rd-alliance.org/groups/federated-identity-management-ig>

Agenda

Time (UTC)	Item	Speaker
15:00	Welcome - What is FIM - What the FIM4R Group Does	David Kelsey (STFC, UK Research & Innovation)
15:10	The current big FIM Question: Assurance. Presentation, quiz and discussion	Hannah Short (CERN)
15:40	Protecting Research Communities (AARC Guidelines)	Nicolas Liampotis (GRNET)
16:00	Protecting Shared Infrastructure (EOSC)	Christos Kanellopoulos (GÉANT)
16:25	Closing questions	

Federated Identity Management

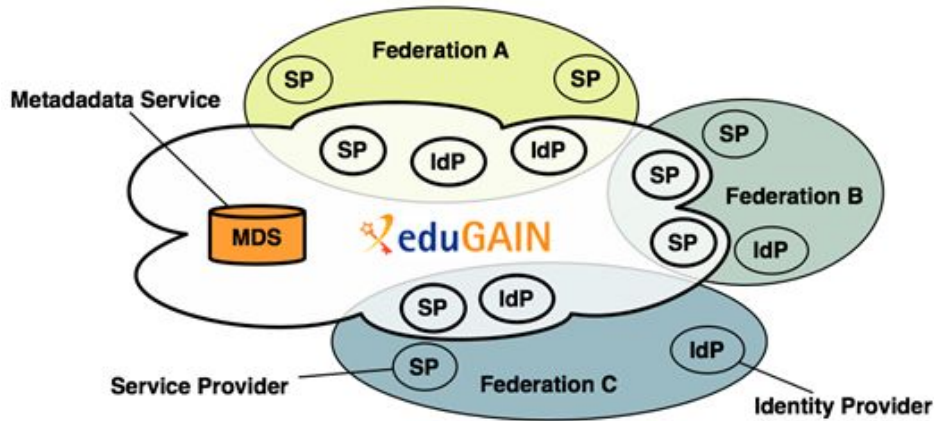
- Federated Identity Management (**FIM**) is the concept of groups of Service Providers (**SPs**) and Identity Providers (**IdPs**) agreeing to interoperate under a set of policies.
- Federations are typically established nationally and use the SAML2 protocol for information exchange
- Each entity within the federation is described by metadata



<https://www.switch.ch/aai/about/federation/>

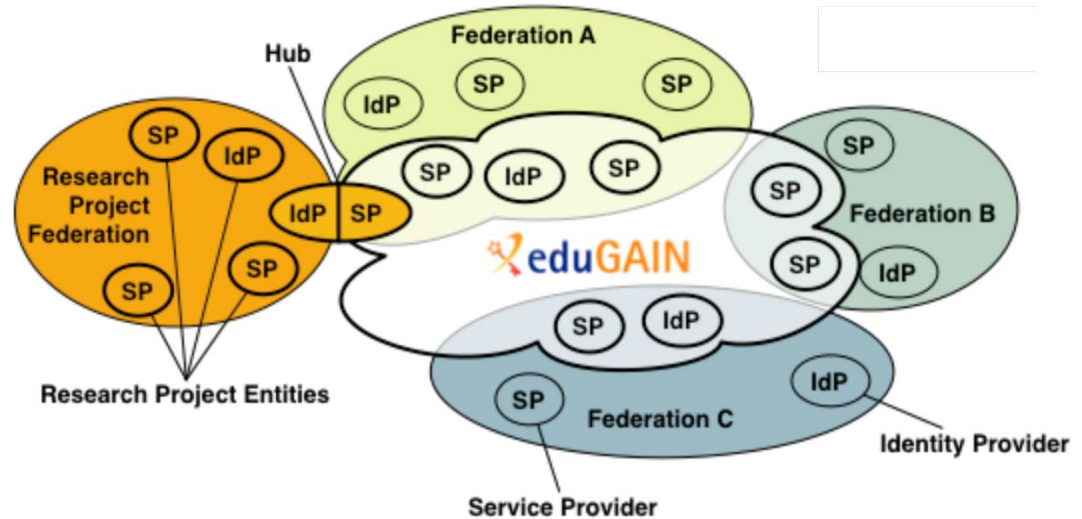
Federated Identity Management Worldwide

- eduGAIN is a form of interfederation
- Participating federations share information (metadata) about entities from their own federation with eduGAIN
- eduGAIN bundles this metadata and publishes it in a central location.



Our Interaction with Identity Federations

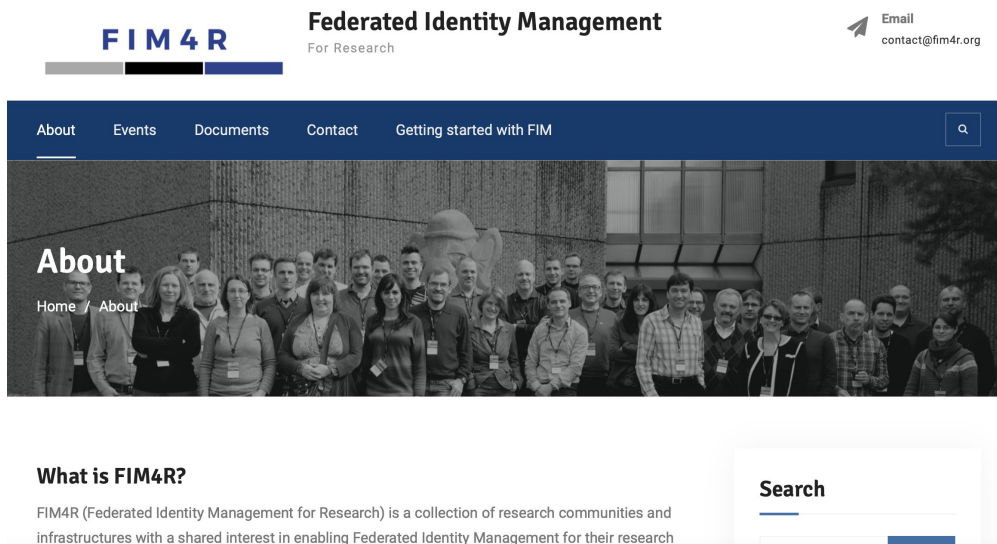
- Research Communities typically join through an SP-IdP proxy
 - From the outside (eduGAIN) it looks like an SP
 - From the inside it looks like an IdP
- We depend on the stability of eduGAIN as an authentication infrastructure



Source: GEANT, GN3PLUS13-642-23

Active Groups in FIM

- REFEDS: R&E Federations Group
- GN4-3 Project: EC funded project to advance Trust and Identity
 - Maintains outputs at <https://aarc-community.org>
- FIM4R Group: Research Community FIM representatives
 - Represents the common needs of Research Communities to FIM stakeholders
 - Existed prior to RDA FIM IG
 - New contributors always welcome!



FIM4R Federated Identity Management
For Research

Email
contact@fim4r.org

About Events Documents Contact Getting started with FIM

About
Home / About

What is FIM4R?
FIM4R (Federated Identity Management for Research) is a collection of research communities and infrastructures with a shared interest in enabling Federated Identity Management for their research

Search

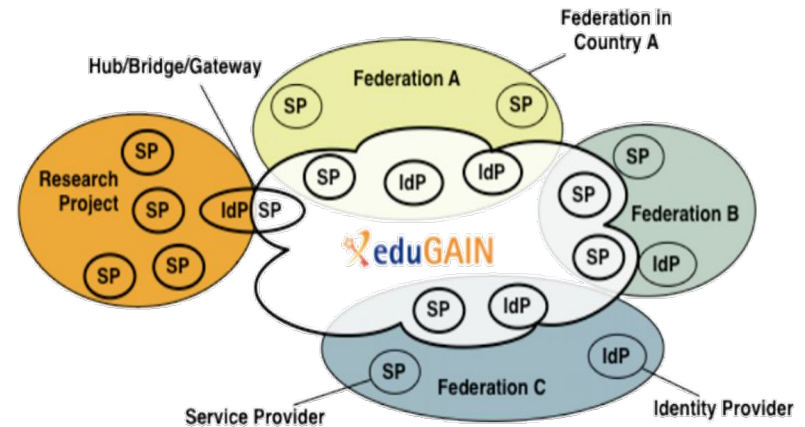
<https://fim4r.org/about/>

Assurance for Federated Identity Management

RDA 2021, 21 April 2021
Hannah Short, Dave Kelsey, slides by Jule Ziegler
(Leibniz-Rechenzentrum München)

How sure can we be about a federated user's identity?

- How was the registration/Identity Proofing done?
Is that a shared account (libraryuser1@university.org)?
- Can this user ID be later reassigned to some other person?
- Is their information, e.g. name or status, accurate or could it have changed?
- How was the user authentication done?



What is Assurance?

- The degree of confidence that a digital credential really belongs to the expected entity/user
- Multiple important aspects
 - Reliable identifiers (do they change, are they unique)
 - ID Proofing (was an ID check done? how?)
 - Attributes (are they accurate? expected freshness?)
 - Authentication (was 2FA used?)
- Service providers may choose to trust users based on the assurance information issued by their Identity provider
- Alternatively, they may boost assurance by e.g. performing ID proofing

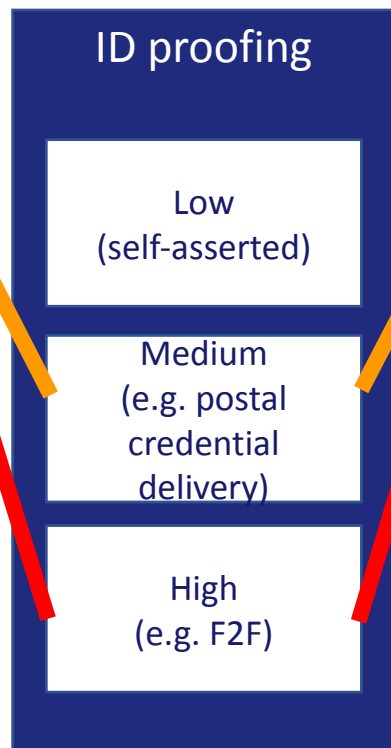
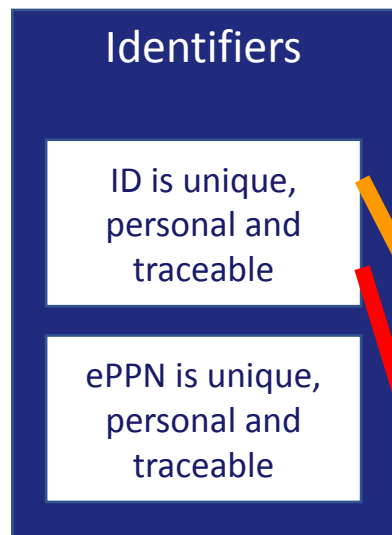
Current Work around Assurance

- Likely that some research communities may start **requiring** a certain level of assurance for their authenticating users
- Several assurance **profiles** (that define levels of trustworthiness) exist e.g. REFEDS, IGTF, InCommon, Kantara
 - So far very few Identity Providers support these profiles, they are missing driving use cases
- Research Communities may be able to influence the **uptake** of such profiles by combining our voices (concretely a short whitepaper authored by the [FIM4R community](#))

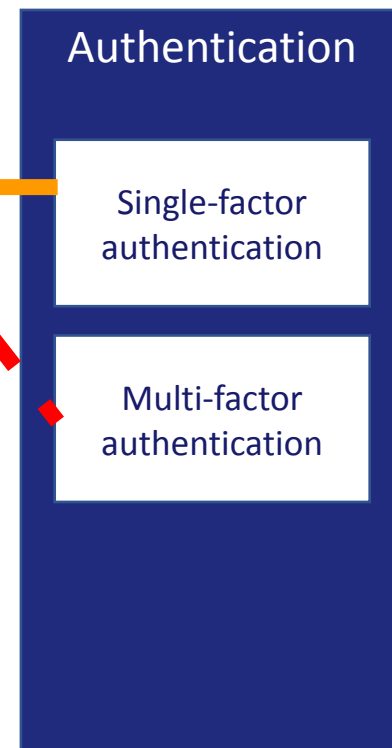
Example Assurance Profile: REFEDS

- Consisting of three individual specifications:
 - REFEDS Assurance Framework (RAF), ver 1.0, published 2018
 - REFEDS Single Factor Authentication Profile (SFA), ver 1.0, 2018
 - REFEDS Multi Factor Authentication Profile (MFA), ver 1.0, 2017
- Component-based approach
- Two identity assurance profiles: Espresso (high assurance) and Cappuccino (moderate assurance)

REFEDS Assurance Framework (RAF)



Authentication Profiles



— Cappuccino
— Espresso

Over to you!

slido

Would you consider trusting external assurance for your researchers?

 Start presenting to display the poll results on this slide.

slido

How do you handle identity proofing for your researchers

 Start presenting to display the poll results on this slide.

slido

Who would you be willing to trust to perform
identity vetting?

 Start presenting to display the poll results on this slide.

slido

Do your researchers use 2FA to access your services?

 Start presenting to display the poll results on this slide.

slido

What would help you to trust an assertion of
2FA from an identity provider?

 Start presenting to display the poll results on this slide.

Thank you!

Discussion time, please raise your hand or use the Question
box