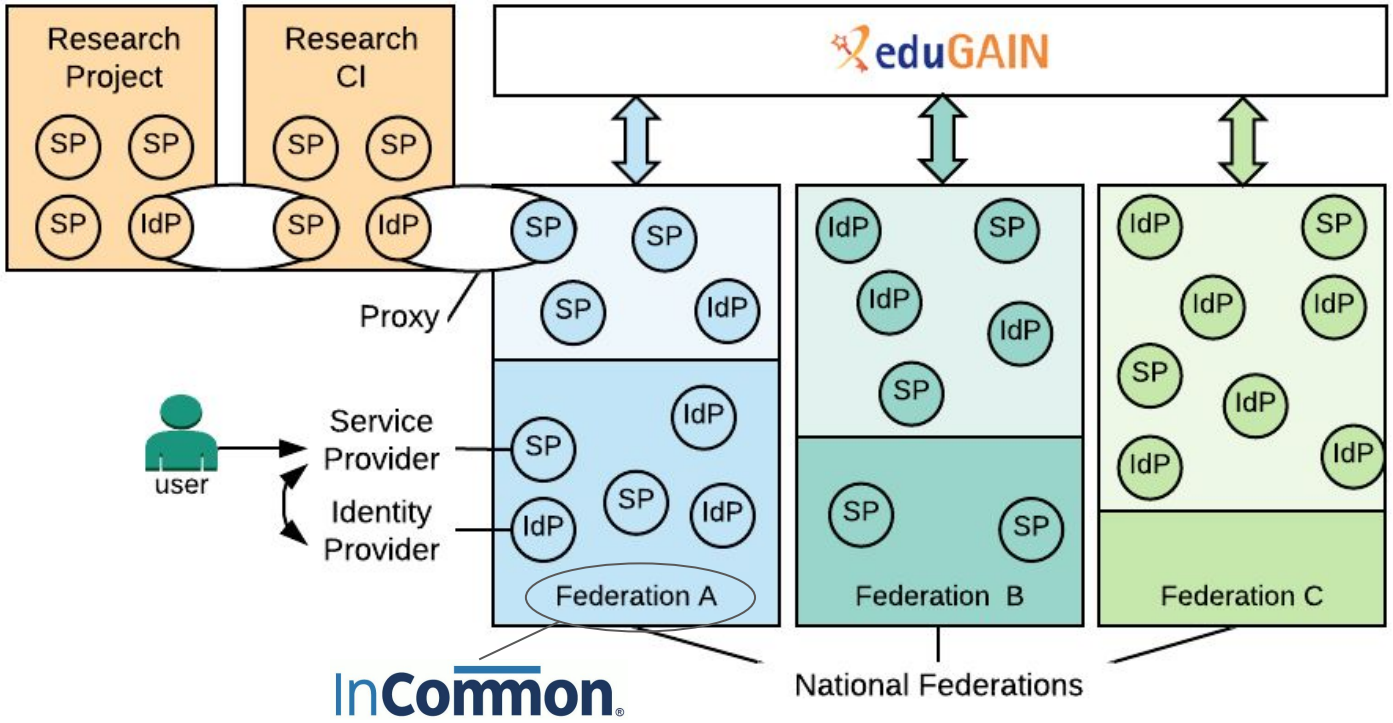
NSF CI PoC IdM WG

Chris Whalen, RDCT
Tom Barton, UChicago & Internet2

Recall how federated access happens



68 countries + 7

> 6700 eduGAIN entities
> 25% InCommon

> 19000 total entities
> 25% InCommon

10M - 100M users

(July 2020)

How to join international federation, superficially

0. Do you need to join a federation?
1. Put your Service Provider into InCommon
2. While at InCommon's Federation Manager doing so, check the box that says to export it to eduGAIN
3. Let the collaborators access your Service Provider

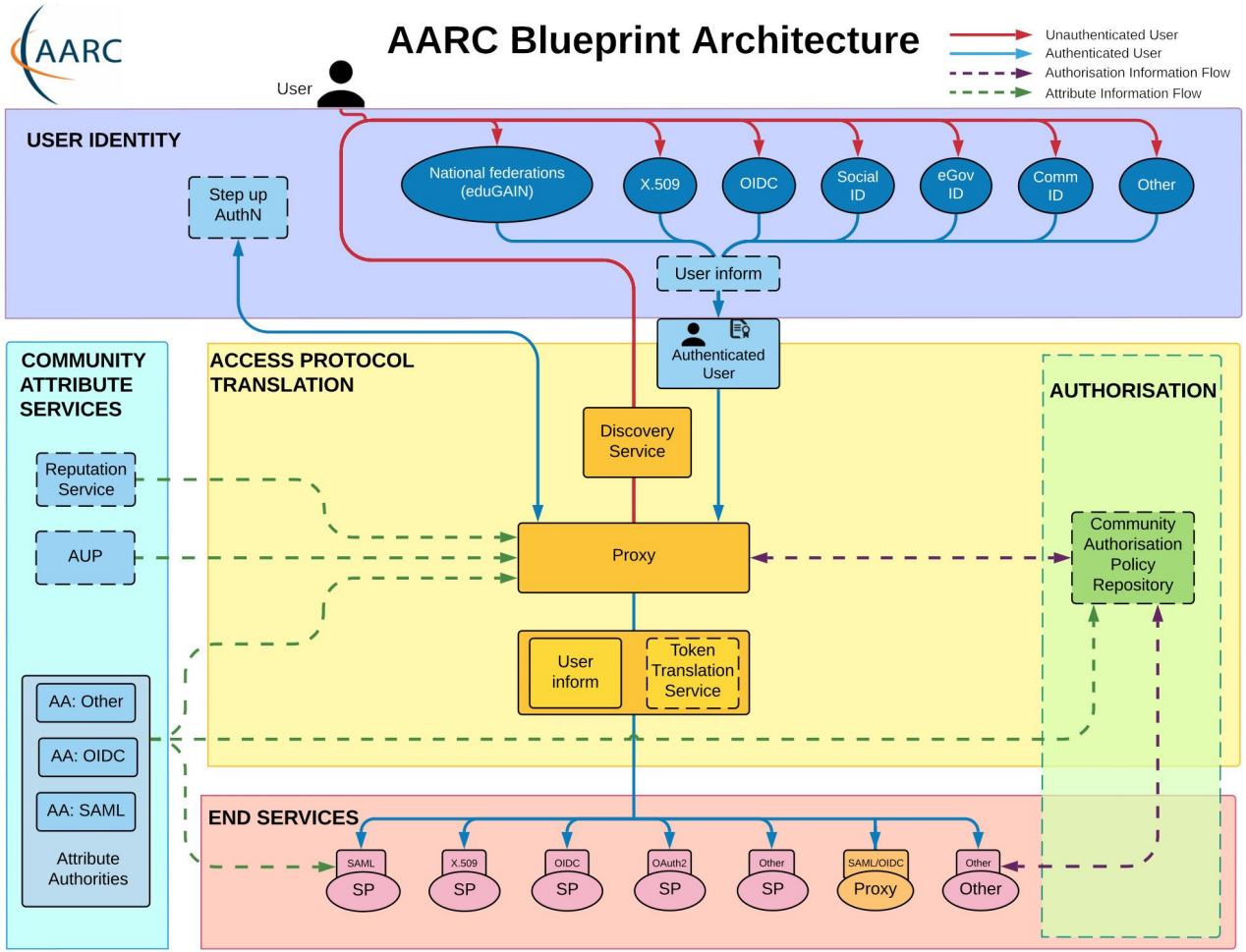
Although, this might take quite a lot of planning and effort!

- Prepare architecture for adding federated access to existing services
- Under whose auspices will your SP/proxy be added to InCommon?
- Do all collaborators' home org Identity Providers work well in federation?
- What about collaborators whose home orgs don't belong to a federation?

Read this! FIM4R v2*

These research and scholarly communities spent 18 months to distill what they most need from Federation

* “Federated Identity Management for Research, version 2”, July 2018



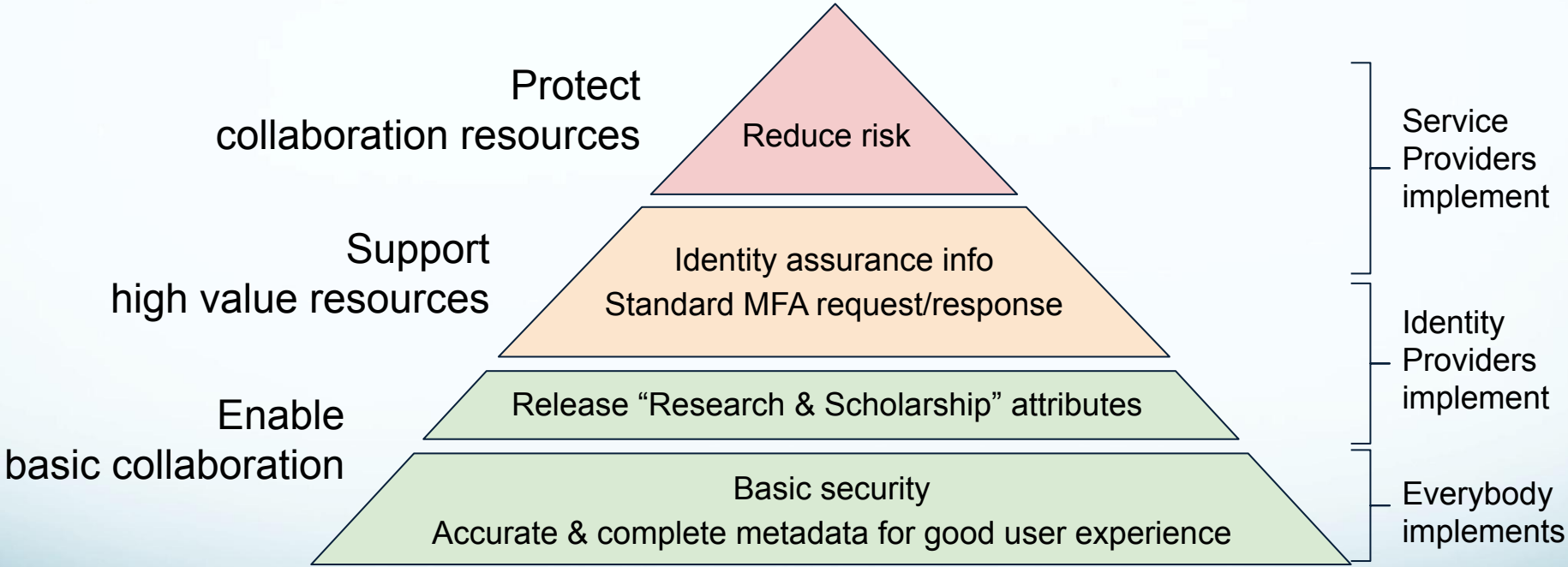
https://aarc-project.eu/wp-content/uploads/2019/05/AARC2-DJRA1.4_v2-FINAL.pdf

Further preparation to federate

- CILogon or Globus Auth can fulfill some of the architectural needs
- Are all LFs legal orgs? For those not, which legal org will sponsor their InCommon membership (if that's the route to take)?
- What else do you need of collaborators' home orgs?
  - Identity proofing, affiliation freshness/info, credential strength?
  - Incident response?

REFEDS establishes standards and best practices to address such things across R&E federations

InCommon's Baseline Expectations program gradually ensures ubiquitous adoption of selected standards and practices



What FIM4R wants and what Baseline Expectations intends to deliver over time

What’s good

- InCommon, REFEDS, and FIM4R communities
  - Great people, smart, capable, helpful
  - Understand that research is a major reason for trust federations in R&E to exist
- Collaboration at scale - onboarding and provisioning
- Federated credentials are better than self-asserted, even with their attendant issues
  - Federated users’ credential issues are addressed by their home orgs, not you
  - Those credentials are also used within their home orgs for important things
  - Deprovisioning simplified and centralized
- International Baseline Expectations looks like it will happen
  - But change management for 1000’s of orgs across dozens of countries can be glacial
- Alignment of audit trails for traceability

Speed bumps

- IdPs use various federated identifiers; SPs must deal with that
  - ePTID, ePPN, ePUID, new SAML identifiers
- Under GDPR, some EU IdPs have become conservative about user attributes
  - LF SPs might need to assert “CoCo” compliance* when that’s available outside the EU
- Users whose home orgs don’t federate
  - Must use an IdP “of Last Resort” (which likely means infrequent use, forgotten passwords)
  - Some IdPs of Last Resort have difficult registration practices, others are too easy, eg, give out accounts to anyone with an email, few or no controls in place
  - ORCID might be a good choice, or google etc if you are not very concerned about who’s actually using the credential
- For many orgs, research use cases are a small fraction of their IdP usage
  - Operators don’t always take those into account, eg, change user identifiers during an upgrade

*https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

More speed bumps

- Uneven practices by national federations -
  - Not all SPs are reachable by all IdPs
- Software developers at your LF or collaborating institutions might need to learn OIDC or SAML or SciTokens
- When things go wrong, it can be hard to debug
  - Engineering can help but knowing the environment can help

Science Persona Ecosystem Research Community

The laboratory – one or multiple orgs

- Principal Investigators
- Trainees
- Technicians
- Administrative

Sponsors – one or multiple orgs/gov

- Grants, Contracts, Cooperative agreements
- Administrators
- Program officers
- Regulatory and Oversight

Outside contractor support

- Procurement
- Vendor
- Equipment Maintenance

Core Facility/Host organization

- Administrators
- Security Staff
- Facilities
- Motor Pool
- Infrastructure

Resource slides

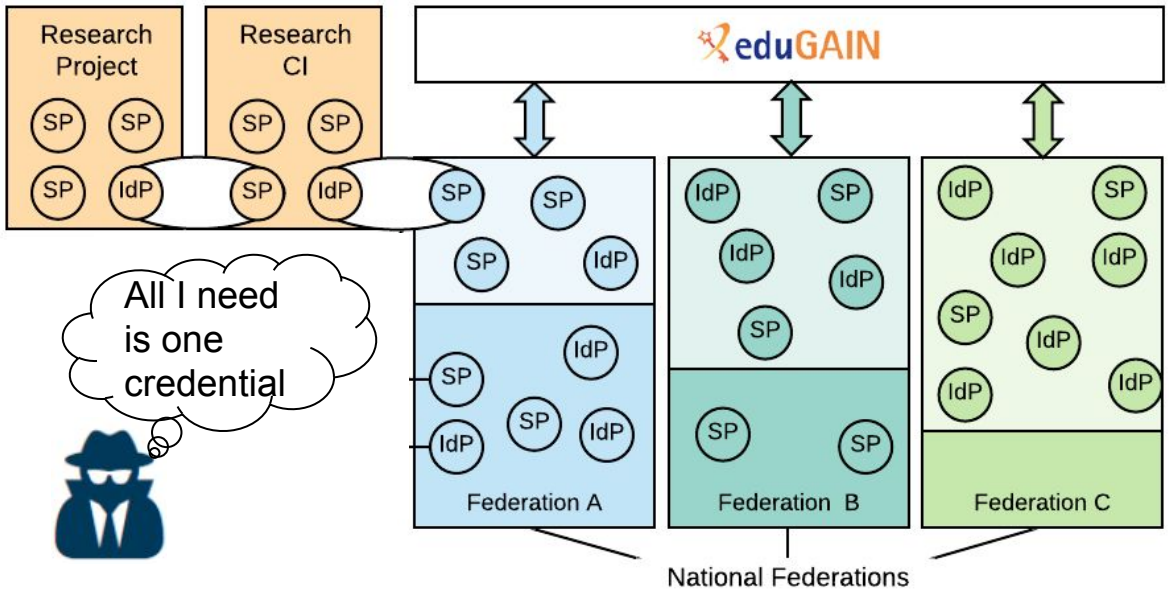
SIRTFI - federated security incident response

Be willing to collaborate in responding to a federated security incident.

Apply basic operational security protections to your federated entities

in line with your organization’s priorities.

Self-assert SIRTFI “tag” so that others will know to trust this about you.



Research & Scholarship attribute release

- Many services for research and scholarship need a few user attributes
  - Name, email, affiliation, persistent identifier
- Those service providers are “tagged” by their national federation operators as “R&S”
- Academic Identity Providers automatically release the R&S attributes to R&S tagged services
- Such Identity Providers are also tagged as “R&S” so that services can elect to require R&S attributes in order to provide service
- The R&S program contributes to good privacy practice under the European General Data Protection Regulation (GDPR)*

*https://wiki.refeds.org/pages/viewpage.action?pageId=4194359

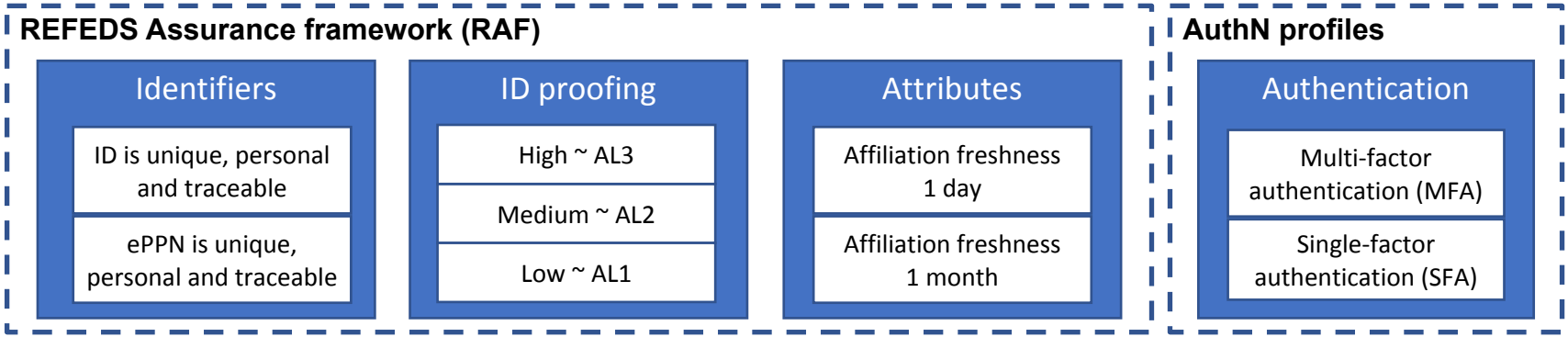
What do research services and funders need from institutions to make informed authorization decisions?

It depends from case to case, but some things are common…

- Access is mostly given on project basis and researchers are given basic access based on their organizational affiliation
  - Terminate access when the affiliation of the person is terminated
  - ➢ Institutional affiliation of a person ⇒ ***attribute assurance & freshness***
  - ➢ Binding of a person to their institution ⇒ ***attribute assurance***
- Minimize risks of unauthorized access
  - Due diligence on service provider side
  - ➢ Known real identity of a researcher ⇒ ***identity assurance & unique identifiers***
  - ➢ Strong enough authentication ⇒ ***authentication assurance*** ⇒ *MFA/SFA*

An international research assurance framework

- A common “language” for communicating identity assurance between Identity Providers and Service Providers
- Basic identity, authentication, and attribute assurance information
- Conformance is self-determined and self-asserted



https://refeds.org/assurance