Federated Identity Management for ARCHIVER

Hannah Short
CERN IT
GÉANT Project Participant

ARCHIVER Meeting, Stanstead Airport
23/05/2019

Agenda

- Introduction to Federated Identity Management
- Federated Identity Management for ARCHIVER
- Technology
- Policy
- Getting started

Agenda

- Introduction to Federated Identity Management
- Federated Identity Management for ARCHIVER
- Technology
- Policy
- Getting started

Federated Identity Management

Federated identity management (FIM) *is the set of policies and technologies that enables one party to rely on the authentication performed by another trusted party, and the secure transfer of identity information for authorisation purposes.*

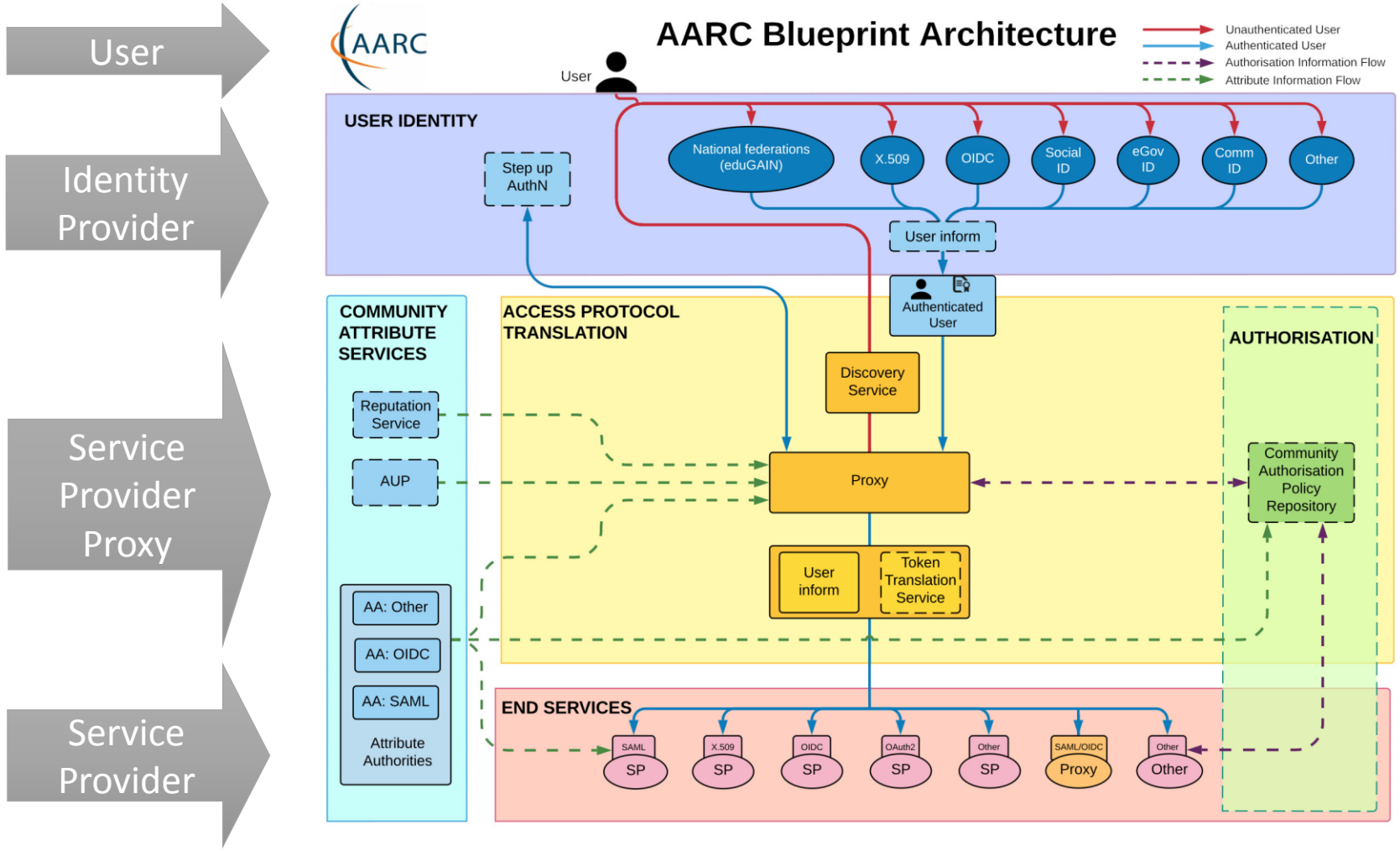
Credit to Licia Florio, GÉANT

FIM Components

User:	Identity Provider (IdP):	Service Provider Proxy	Service Provider (SP):
• A user is characterized by an identity, a collection of attributes that represent properties about that specific person.	• Asserts authentication and identity information about the user.	• Controls access to a set of service providers • Adds authorization information	• Receives and checks authentication and authorization information to grant access to the service.

Credit to Alessandra Scicchitano, GEANT, for this slide

Blueprint Architecture

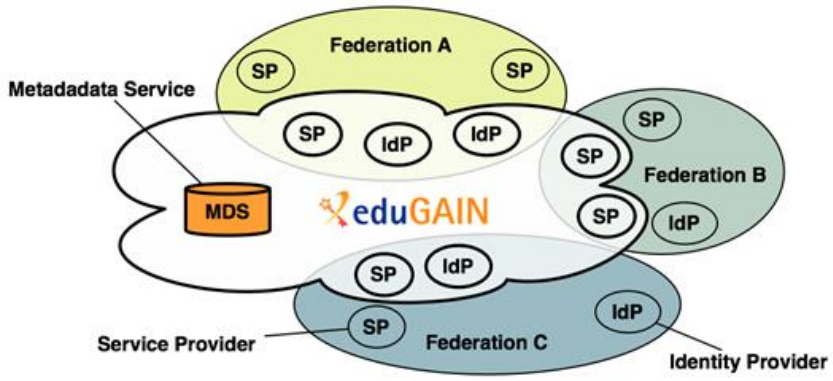


https://aarc-project.eu/architecture/

FIM Protocols

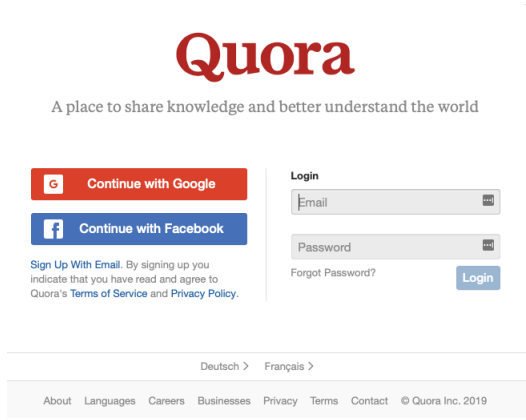
SAML

- Security Assertion Markup Language
- Exchange of metadata (including keys) to establish trust, facilitates by Identity Federations
- Authentication Assertions sent as XML packets



OIDC

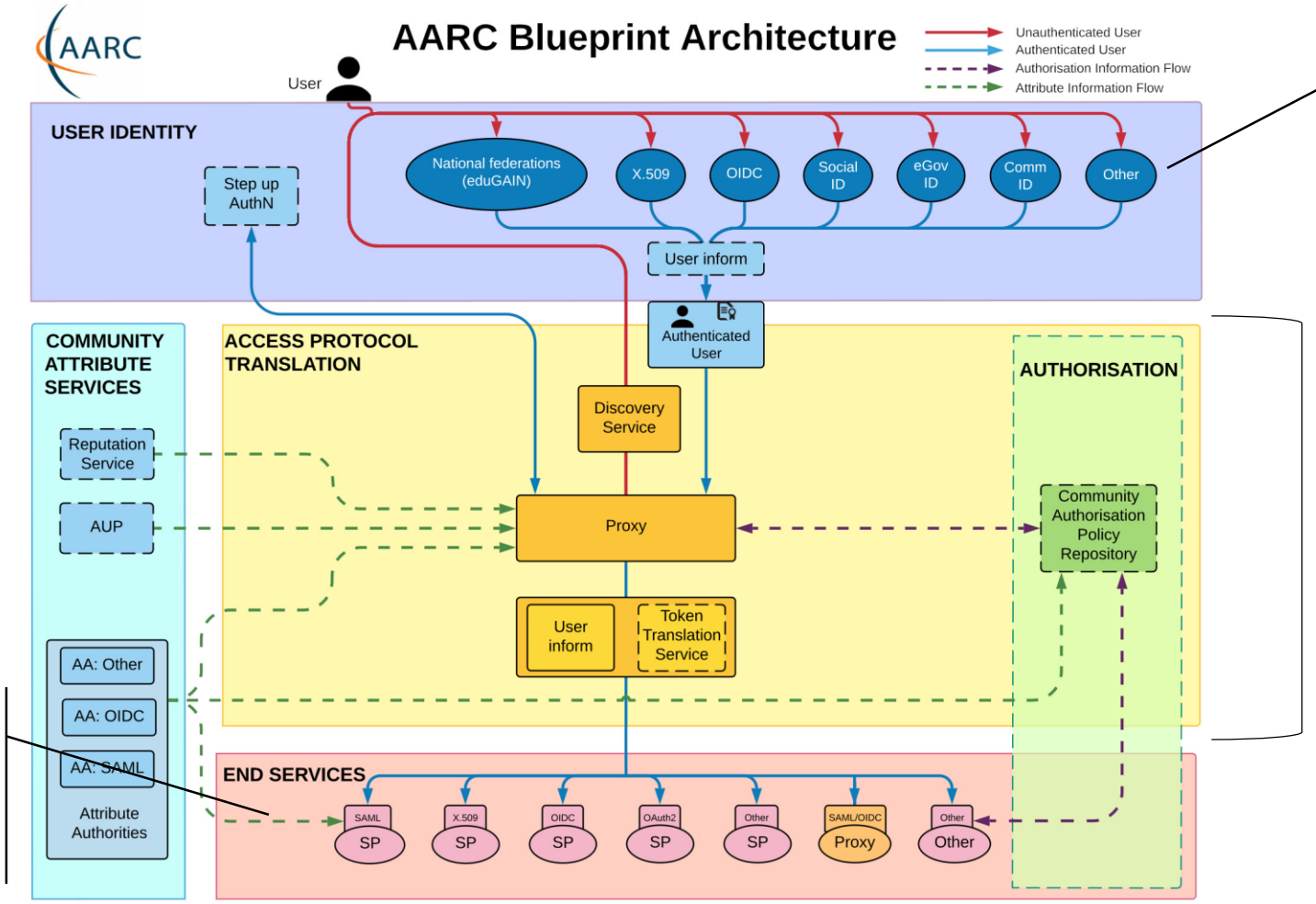
- OpenID Connect
- Clients register to OIDC Providers
- Authentication and Authorisation typically sent as Jason Web Tokens



Agenda

- Introduction to Federated Identity Management
- Federated Identity Management for ARCHIVER
- Technology
- Policy
- Getting started

Who does what?



Research Institute IdPs, through eduGAIN

?

ARCHIVER Services

https://aarc-project.eu/architecture/

Which protocols should you use?

Identity Providers (Research Institutes)

- Research Institutes typically already have an IdP in eduGAIN that talks SAML
- If your Research Institute doesn't yet have an IdP, contact your National Federation for guidance https://technical.edugain.org/status

Service Providers (ARCHIVER Services)

- Many commercial services already support SAML or OIDC
- Most Service Provider proxies (where you will connect your service) also support both
- If your Service Provider supports neither you will need to implement it. See training:
  - OIDC examples for multiple platforms https://aarc-project.eu/training/integrating-your-service-with-openid-connect/
  - SAML example with Shibboleth https://aarc-project.eu/training/saml-and-shibboleth-introduction/

Service Provider Proxy Options, Software (all participate in EOSC Projects)

Service	Supporting organisation	SP protocols supported	Deployment models advertised	Link
eduTEAMS	GÉANT	SAML, OIDC	Hosted or standalone	https://www.geant.org/Innovation/eduteams/Pages/Getting-Started.aspx
EGI Check-in	EGI/GRNET	SAML, OIDC	Hosted or standalone	https://www.egi.eu/wp-content/uploads/2017/09/Check-in.pdf
B2ACCESS	EUDAT	SAML, OAuth2 (similar to OIDC)	Standalone	https://marketplace.eosc-portal.eu/services/b2access
INDIGO IAM	INDIGO/INFN	OIDC	Standalone	https://www.indigo-datacloud.eu/identity-and-access-management

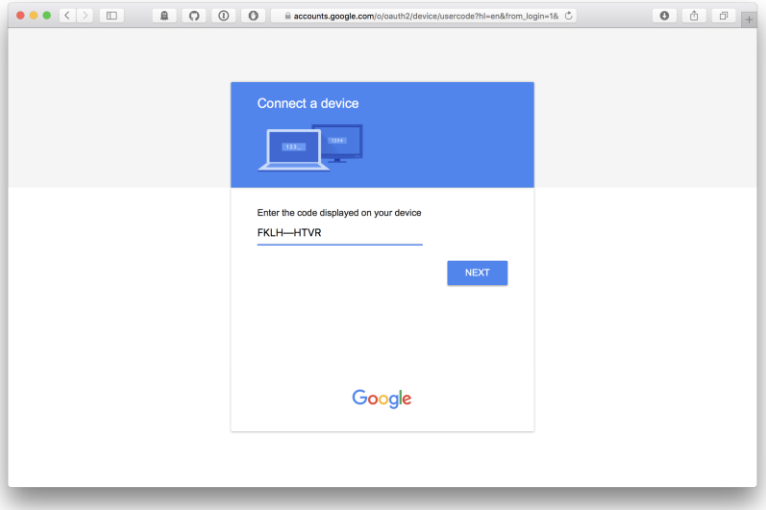
Service Provider Proxy Options, Governance

The ARCHIVER project should carefully consider the following questions

- How many Service Provider Proxies should be set up? (Would recommend one for simplicity)
- Who will set up authorisation groups?
- Who will maintain group membership?

Command line access

- Multiple ways have been explored to provide command line access
  - Device Code Flow with OAuth (enter a code on a browser to validate a command line authentication request)
  - SSH Key upload (collect users' SSH keys at the Service Provider Proxy and provision them at the resource)
  - OIDC Agent (https://indigo-dc.gitbooks.io/oidc-agent/) that dynamically provisions OIDC tokens in a similar way to SSH keys)
- Discuss with the Service Provider Proxy what they recommend or can support



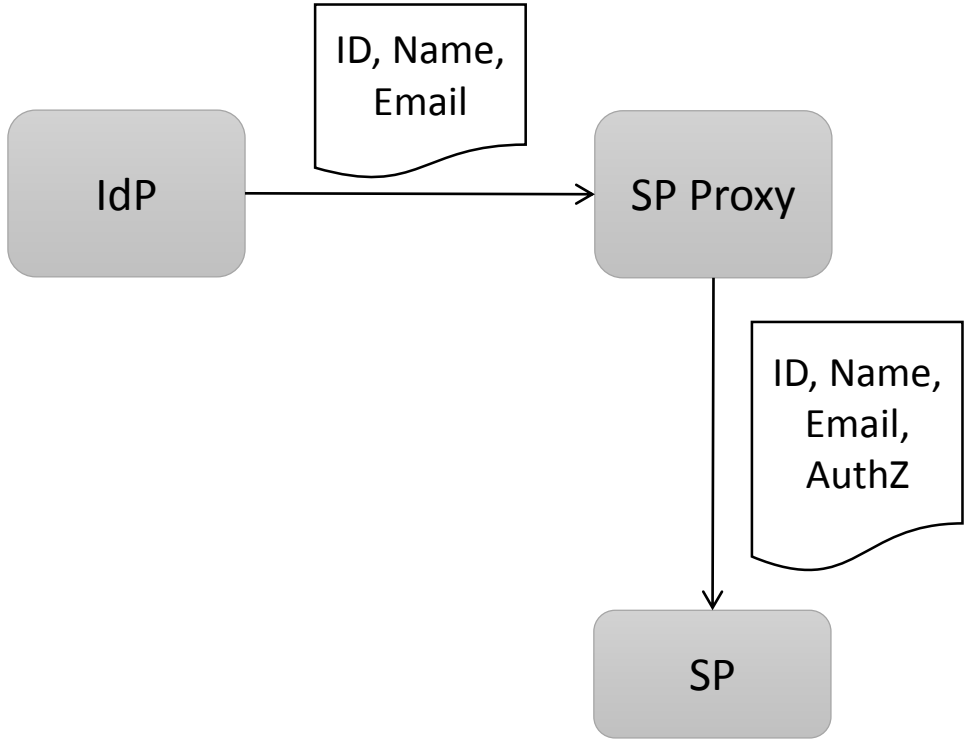
Agenda

- Introduction to Federated Identity Management
- Federated Identity Management for ARCHIVER
- Technology
- **Policy**
- Getting started

Policies: FIM Frameworks

Attribute Release

- Research IdPs should release the Research and Scholarship attribute bundle (persistent id, name, email)
- To encourage attribute release from IdPs, Service Providers (or the Proxy) should*
  - Support Research and Scholarship (**R&S**) https://refeds.org/category/research-and-scholarship
  - Adopt the GÉANT Data Protection Code of Conduct (**CoCo**) https://wiki.geant.org/display/eduGAIN/Recipe+for+a+Service+Provider
  - Comply with the Security Incident Response Trust Framework (**Sirtfi**) https://refeds.org/sirtfi



**Note, a Service Provider Proxy would assert compliance with R&S, CoCo and Sirtfi for the group of Services behind it*

Policies: FIM Frameworks

Operational Security

- To support Security Incident Response, ARCHIVER Services should require that IdPs
  - Comply with the Security Incident Response Trust Framework (**Sirtfi**)
  - Publish a Security Contact

Policies: FIM Frameworks

Attribute Release

- Research IdPs should release the Research and Scholarship attribute bundle (persistent id, name, email)
- To encourage attribute release from IdPs, Service Providers (or the Proxy) should*
  - Support Research and Scholarship (**R&S**) https://refeds.org/category/research-and-scholarship
  - Adopt the GÉANT Data Protection Code of Conduct (**CoCo**) https://wiki.geant.org/display/eduGAIN/Recipe+for+a+Service+Provider
  - Comply with the Security Incident Response Trust Framework (**Sirtfi**) https://refeds.org/sirtfi

Operational Security

- To support Security Incident Response, ARCHIVER Services should require that IdPs
  - Comply with the Security Incident Response Trust Framework (**Sirtfi**)
  - Publish a Security Contact

**Note, a Service Provider Proxy would assert compliance with R&S, CoCo and Sirtfi for the group of Services behind it*

Additional Policies

- ARCHIVER users will be presented with multiple policy points for consent and/or accepting terms and conditions (at IdPs, SP Proxy, SPs). To aid user experience you may wish to consider interoperable policies that can be accepted once, in particular:
  - Acceptable Use Policy to be accepted at the SP Proxy when registering https://wiki.geant.org/display/WISE/Baseline+Acceptable+Use+Policy+and+Conditions+of+Use
- There may be requirements for each ARCHIVER Service to comply with additional policies, such as
  - Service Operations Security Policy
  - Policy on the Processing of Personal Data

Further guidance is available at https://aarc-project.eu/policies/policy-development-kit/

Agenda

- Introduction to Federated Identity Management
- Federated Identity Management for ARCHIVER
- Technology
- Policy
- **Getting started**

Next Steps

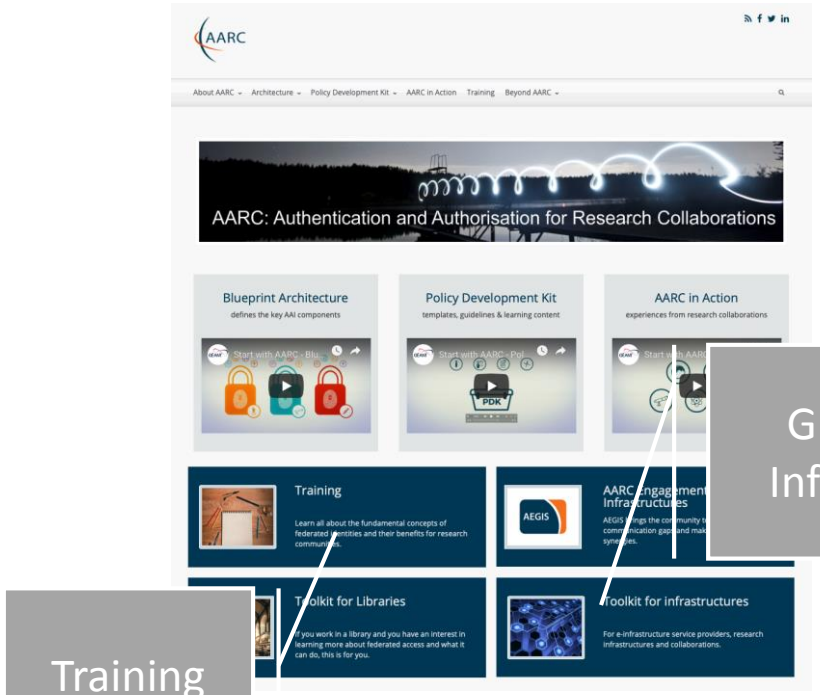
1. The ARCHIVER project should decide on a Service Provider Proxy implementation and operator
2. Research Institutes should ensure that they have a SAML IdP registered in eduGAIN that releases the Research & Scholarship Attribute Bundle
3. ARCHIVER Services should ensure that their Services can be authenticated via SAML or OIDC (depending on the chosen Service Provider Proxy implementation)

Looking for help?

Testing tools

- Test your SAML IdP (Research Institutes) or SP (ARCHIVER Services) https://samltest.id
- Test your OIDC Service https://openidconnect.net

https://aarc-project.eu



Thank you

Any questions?

hannah.short@cern.ch

GÉANT

Networks · Services · People

www.geant.org