SAML and eduGAIN - Introduction

Sasa Cavara	sasa.cavara@CARNet.hr
Robert Hackett	robert.hackett@heanet.ie
Ioannis Kakavas	ikakavas@noc.grnet.gr
Lukas Hämmerle	lukas.haemmerle@switch.ch

December 16th 2016

Agenda

- Objectives
- Overview of the SAML/eduGAIN for the GÉANT Framework
- Overview of SAML and how it works
- Identity Federations and eduGAIN
- Sources of technical information and support on SAML and eduGAIN
- Q&A

SAML/eduGAIn and the GÉANT Framework

- SAML as a mandatory requirement
- Implementation – with assistance from GÉANT team or NREN
- eduGAIN – preferred option
- Reseller Portals
- Acceptance Form
- Next steps planning & implementation

SAML

SAML

- **SAML - Security Assertion Markup Language**
  - OASIS standard describing the XML messages exchanged between Identity Provider (IdP) and Service Provider (SP)
  - Its purpose is to enable the authentication and secure exchange trusted identity information (attributes) between IdP and SP
- **SAML 2.0** is the de facto standard for academic identity federations
- **SAML 2.0** Web Browser Single Sign On Profile
  - Profile that describes how to use SAML in order to achieve SSO
  - Main use of SAML within Identity Federations

SAML

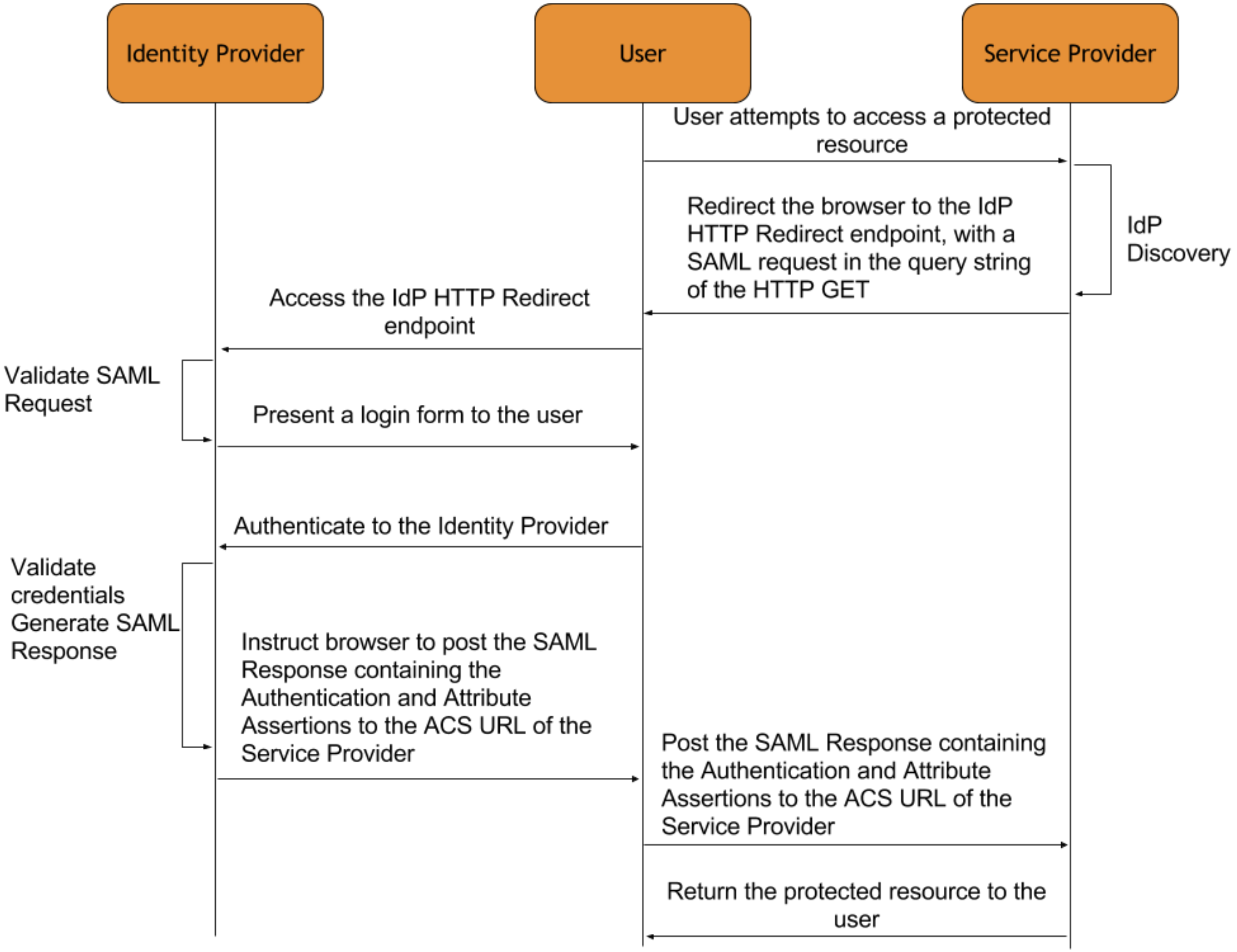
- **SAML2int Interoperable SAML 2.0 Profile**
  - A deployment profile for SAML2.0 Web Browser Single Sign On profile
  - Aims to influence how a SAML entity should be implemented
  - Aims to influence how a SAML entity implementation should be configured

SAML Entities

- **SAML Identity Provider (IdP)**
  - A SAML authority that authenticates users against a user repository
  - Retrieves information for the users in the form of attributes
  - Transfers the authentication event along with the attributes to a SAML Service Provider

- **SAML Service Provider (SP)**
  - A SAML consumer that acts as a middleware in order to protect Web Applications
  - Consumes SAML messages from the Identity Provider and deduces authentication events and attributes

SAML Authentication Flow



Identity Provider
User
Service Provider
User attempts to access a protected resource
Redirect the browser to the IdP HTTP Redirect endpoint, with a SAML request in the query string of the HTTP GET
IdP Discovery
Access the IdP HTTP Redirect endpoint
Validate SAML Request
Present a login form to the user
Authenticate to the Identity Provider
Validate credentials Generate SAML Response
Instruct browser to post the SAML Response containing the Authentication and Attribute Assertions to the ACS URL of the Service Provider
Post the SAML Response containing the Authentication and Attribute Assertions to the ACS URL of the Service Provider
Return the protected resource to the user

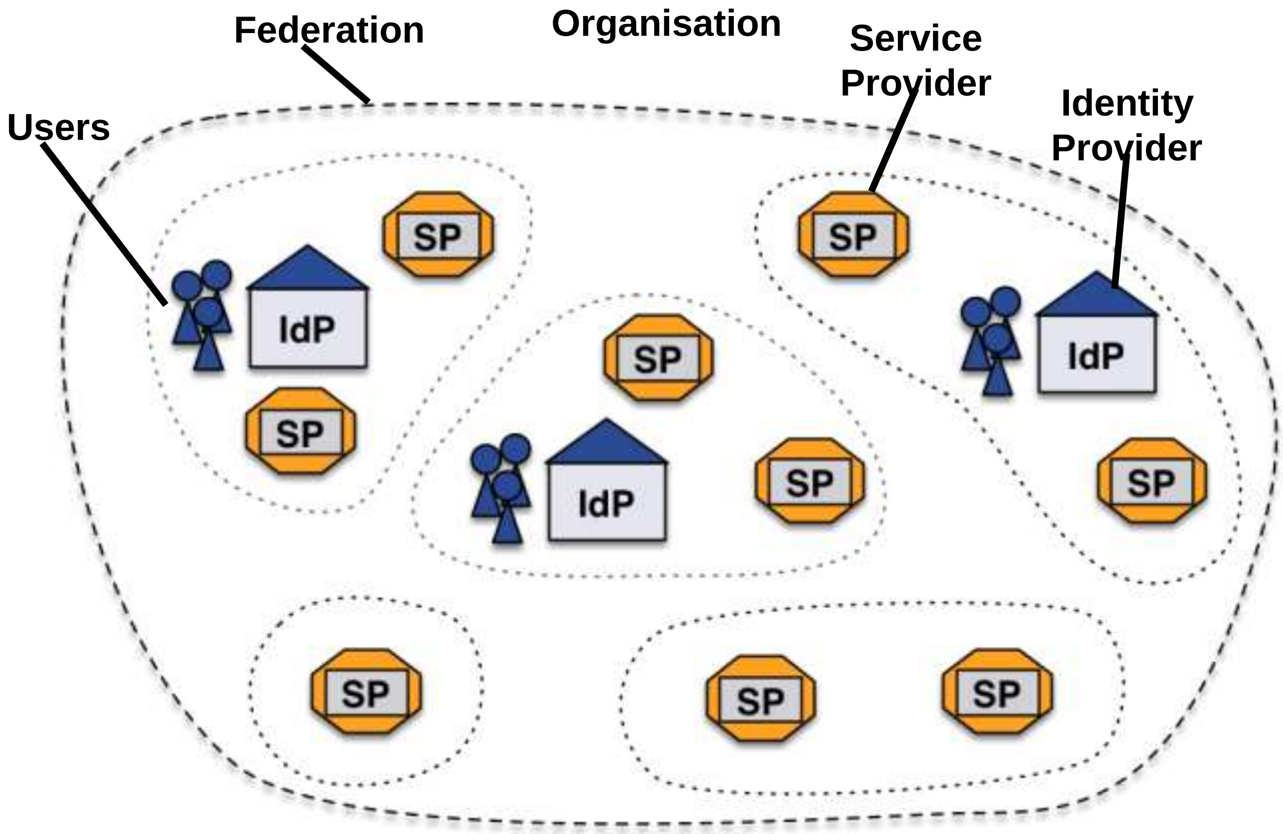
FIM

Federated Identity Management

"common set of policies, practices and protocols in place to manage the identity and trust into IT users and devices across organizations"

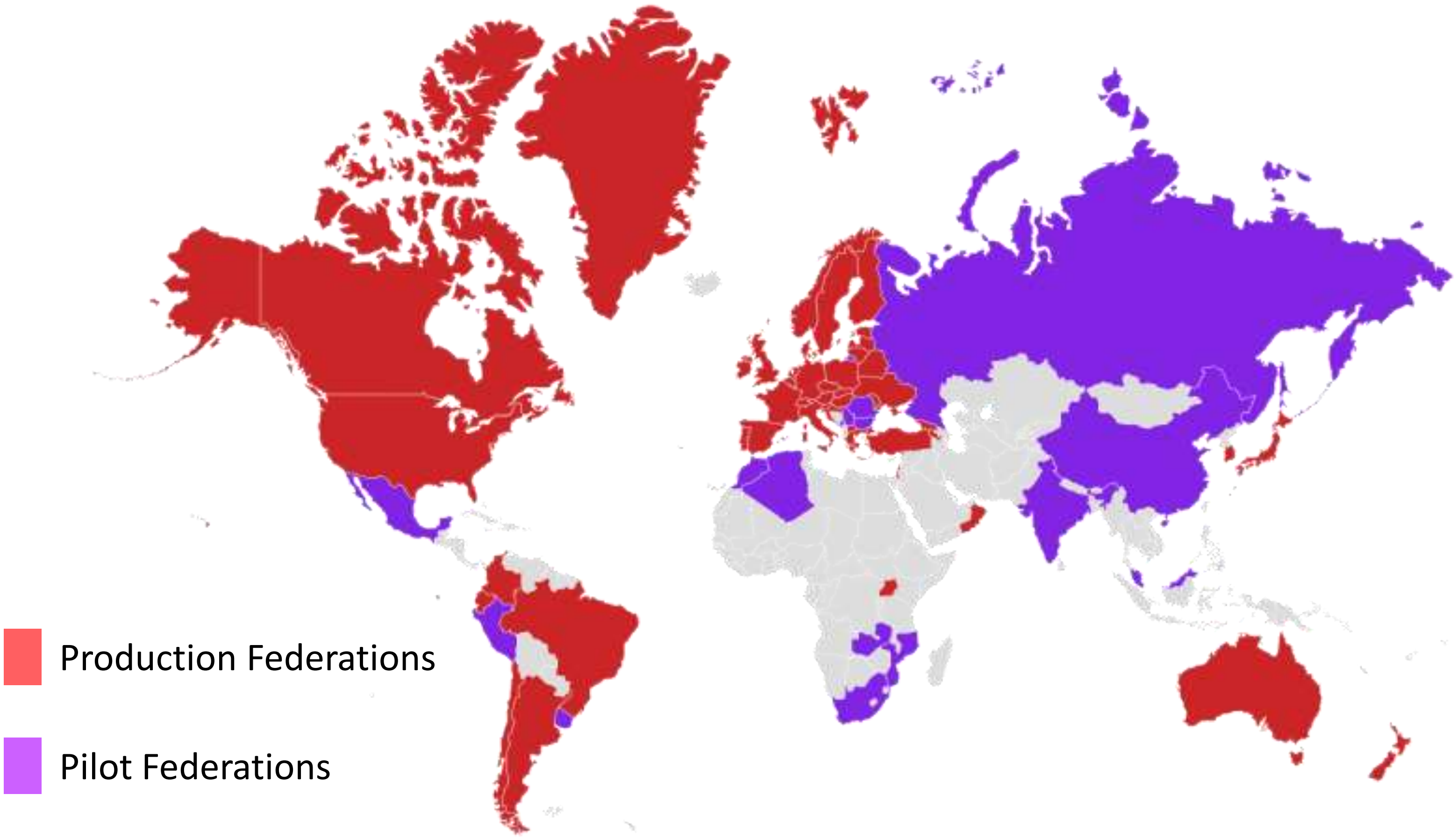
“As a SAML Entity, how do I know which Entities I can trust in order to exchange SAML messages with ?”

Federations



Federation ~= Organizations that exchange trusted identity information (attributes) using common protocols and policies

Academic Identity Federations



🟥 Production Federations

🟪 Pilot Federations

https://refeds.org/federations/federations-map (14.12.2016)

How to Support SAML2 in 3 steps

1. **Choose SAML2 implementation**
   Don't reinvent the wheel by developing your own. Follow federation's deployment instructions
2. **Choose IdP Discovery Service**
   Important with users from so many organizations! Recommendations https://discovery.refeds.org/ E.g. Shibboleth Embedded Discovery Service
3. **Adapt and Test your Web Application**
   Use user attributes/info provided by SP to identify/authorize/auto-enroll user. Test against www.testshib.org or eduGAIN Access Check

SAML2 Service Provider Implementations

- **Shibboleth Service Provider 2** (most common in academic environment, most comprehensive set of features, requires apache2 httpd or IIS)
- **SimpleSAMLPHP** (second most common, mostly suitable for PHP applications)
- **Microsoft ADFS** (limited SAML2 support, much handwork to get it running in a federation)
- **pySAML2** (python implementation)
- **mod_mellon** (Apache module, small user base)
- **SAML passport** (node.js, hard to work within a federation)

SAML2 Service Provider Selection criteria

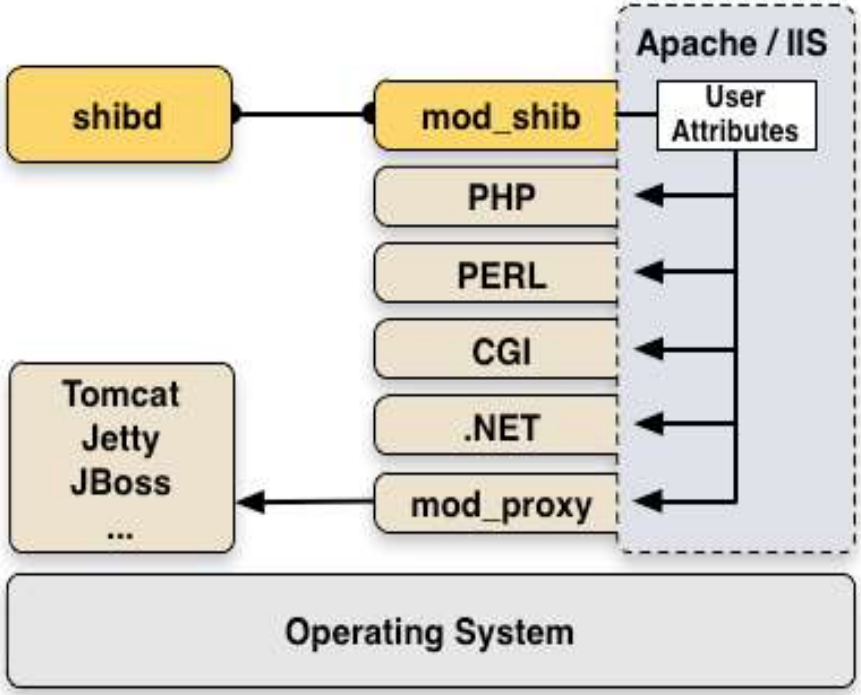
- Can it consume SAML2 metadata?
  - Containing > 3k entities
  - More than 22MB in size
  - Can metadata be refreshed automatically
- Does it support the Web SSO profile (saml2int.org)?
  - E.g. can it process signed and encrypted SAML assertions from IdPs with self-signed X.509 certificates?
- Is it a secure, well adopted implementation backed by a strong community or vendor ?

Introduction to Shibboleth

- **The Origin**
  - Internet2 in the US launched the open source project in 2000
- **The name**
  - Word Shibboleth was used to identify members of a group
- **The standard**
  - Based on Security Assertion Markup Language (SAML)
- **The Consortium**
  - The new home for Shibboleth development
  - Collect financial contributions from deployers worldwide
- The Shibboleth software is the most widely used in the research and education environment
- Website: https://shibboleth.net/

Shibboleth Service Provider

- Runs on: Linux, Solaris, Windows, Mac OS X, FreeBSD, …
- Protects web applications
- shibd processes attributes
- Can authorize users with
  - Apache directives
  - Shibboleth XML Access rule
- Provides attributes to applications via web server environment variables or headers



How to join eduGAIN

What is eduGAIN

eduGAIN is an interfederation service that connects 39 identity federations around the world

and many more

Interconnecting national federations → Interfederation

- Distributed infrastructure (in some ways works like DNS)
- Components are Identity Providers and Service Providers
- Most components are operated by universities, research institutes, schools
- Subset of national federations is in eduGAIN, with subset of their entities

eduGAIN – Service Introduction

- In production since 2011
- Built by EC-funded GÉANT Project
  - National research networks (NRENs) together with their customers (universities, research institutions, schools)
- NRENs all operate their own federations
  - Self-interest of national federations to operate eduGAIN
- Governed by eduGAIN member federations
- 66% of all known IdPs are in eduGAIN (+21% in last 18 months, https://met.refeds.org/, 14.12.2016)

eduGAIN – Why join ?

- Get access to **education and research users** around the world
  - Alone in Europe around 50 million users (not all in eduGAIN yet though)
- User identity and affiliation **data is asserted and maintained** by users home organization (e.g. university, research organization, school), where it's best known
- **Easier onboarding process** because user's don't have to register (you get their attributes)

eduGAIN vs 1-1 SAML “peerings”

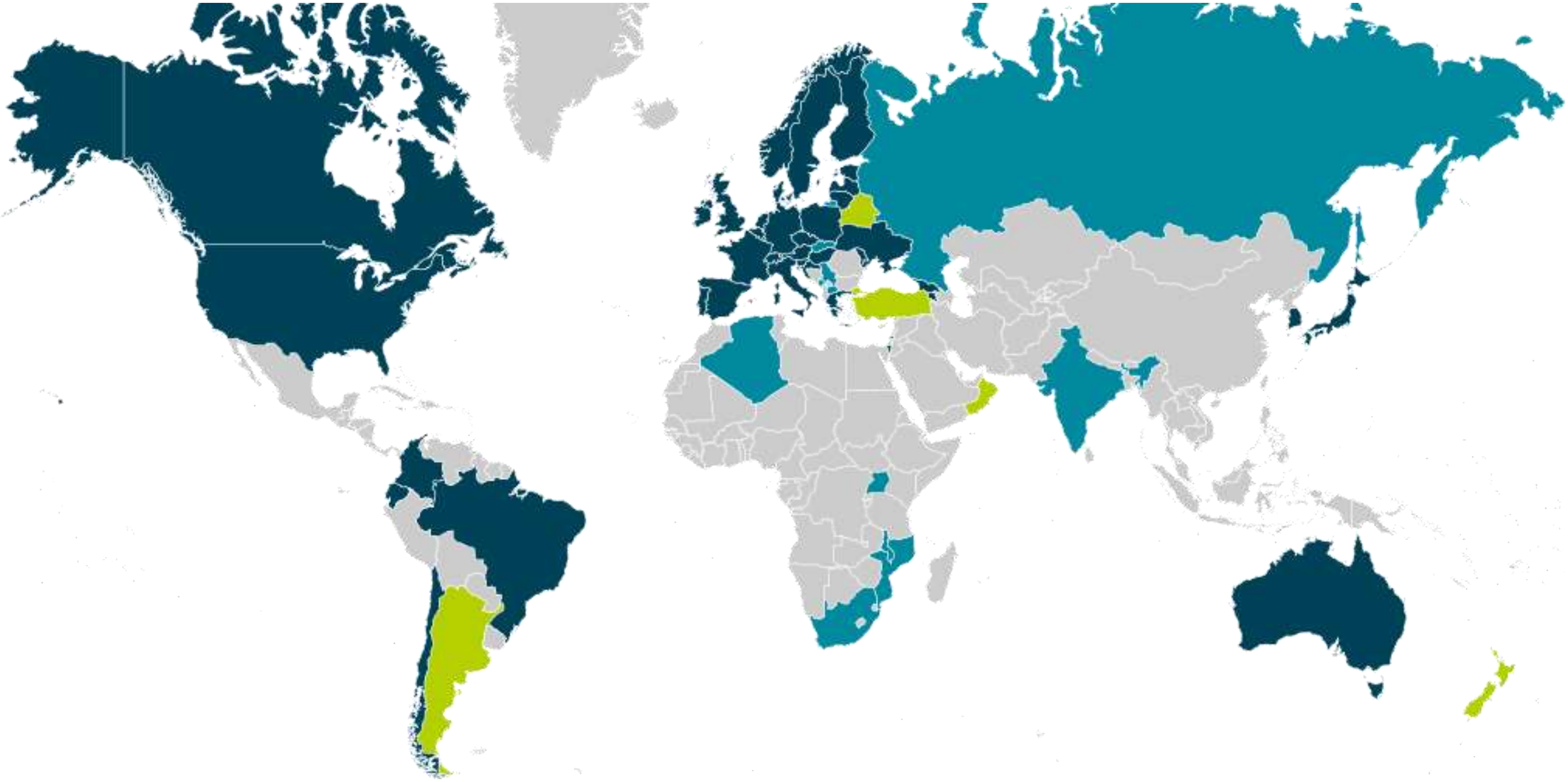
- There is a common language for you and the Identity Providers
  - SAML2int
  - Federations policy
- You can leverage REFEDS R&S (if applicable) to facilitate attribute release
- You will not require manual configuration for each IdP, while maintaining the option to whitelist if necessary
- You only need to trust one source of information (metadata aggregates) instead of each IdP

eduGAIN – Which attributes should I expect?

- User's organization name, logo, tech. contact, ... (available via metadata)
- Personal Identifiers
  - email address
  - person name (givenName + sn, displayName, cn)
  - eduPersonPrincipalName
- Pseudonymous Identifier
  - eduPersonTargetedID
- Affiliation
  - eduPersonScopedAffiliation (e.g. "staff", "student", ...)

eduGAIN – How to join ?

Add Service via one of the 39 member federations



https://technical.edugain.org/status

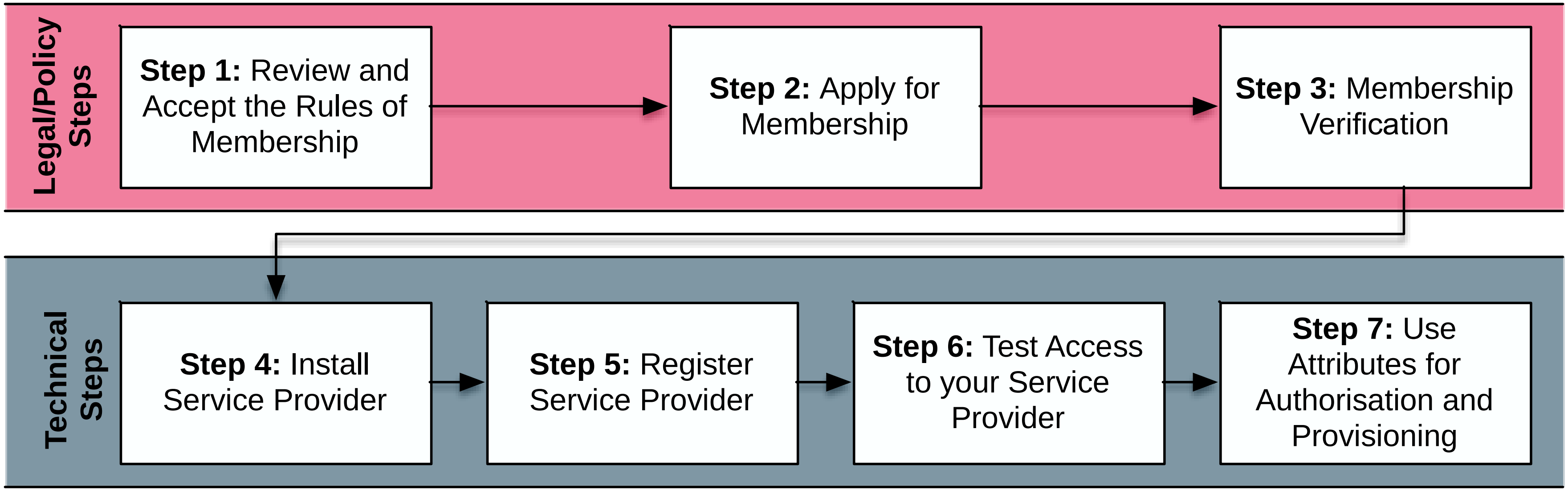
eduGAIN – Via which federation?

- If you have geographical or logical connections with one of the national federations, select that.
  - List of federations with contact points :

    http://technical.edugain.org/status

- Otherwise use the UK Access Management Federation

eduGAIN – Join in 7 steps


Legal/Policy Steps
Step 1: Review and Accept the Rules of Membership
Step 2: Apply for Membership
Step 3: Membership Verification
Technical Steps
Step 4: Install Service Provider
Step 5: Register Service Provider
Step 6: Test Access to your Service Provider
Step 7: Use Attributes for Authorisation and Provisioning

Detailed instructions in

https://wiki.edugain.org/How_to_join_eduGAIN_as_Service_Provider

Technical Recommendations for Joining

- Use well-known SAML implementation
    - Most SPs use Shibboleth or SimpleSAMLPHP
    - Microsoft ADFS also works but is very limited

- Support GÉANT Data Protection Code of Conduct
    - More information on https://wiki.edugain.org/Recipe_for_a_Service_Provider

- Service should not expect too fancy attributes for users (birthday, study course etc.)
- Service should not require unnecessary attributes

Example Services in eduGAIN

- Wiki: wiki.edugain.org
- Cloud: accounts.okeanos-global.grnet.gr
- Conference Registration: tnc16.geant.org
- Video Conference System: connect.sunet.se
- Event Management System: indico.cern.ch
- Large File Sender: filesender.internet2.edu

... and more than 1100 other services

How to start your journey

Generic instructions:
https://wiki.edugain.org/How_to_Join_eduGAIN_as_Service_Provider

Contact us:
edugain-integration@geant.net

Thank you

ikakavas@noc.grnet.gr

GÉANT

Networks · Services · People
www.geant.org