NI4OS-Europe pre-production environment

Authentication & Authorisation Infrastructure (AAI)

Online NI4OS-Europe training:
Developing FAIR and EOSC skills,
28 Jan 2021

Nicolas Liampotis, GRNET

Nick Evangelou, GRNET

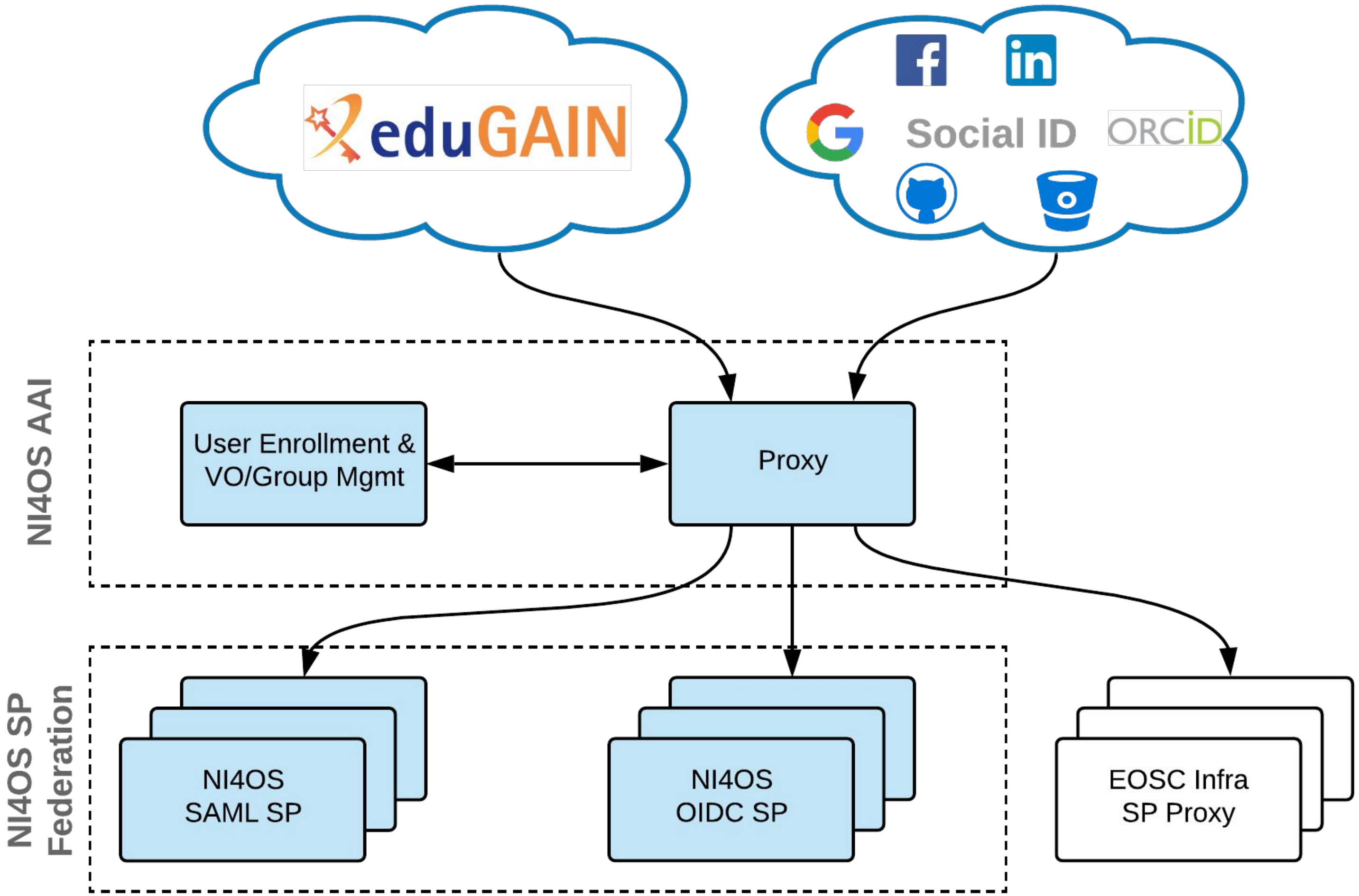
AAI

Introduction

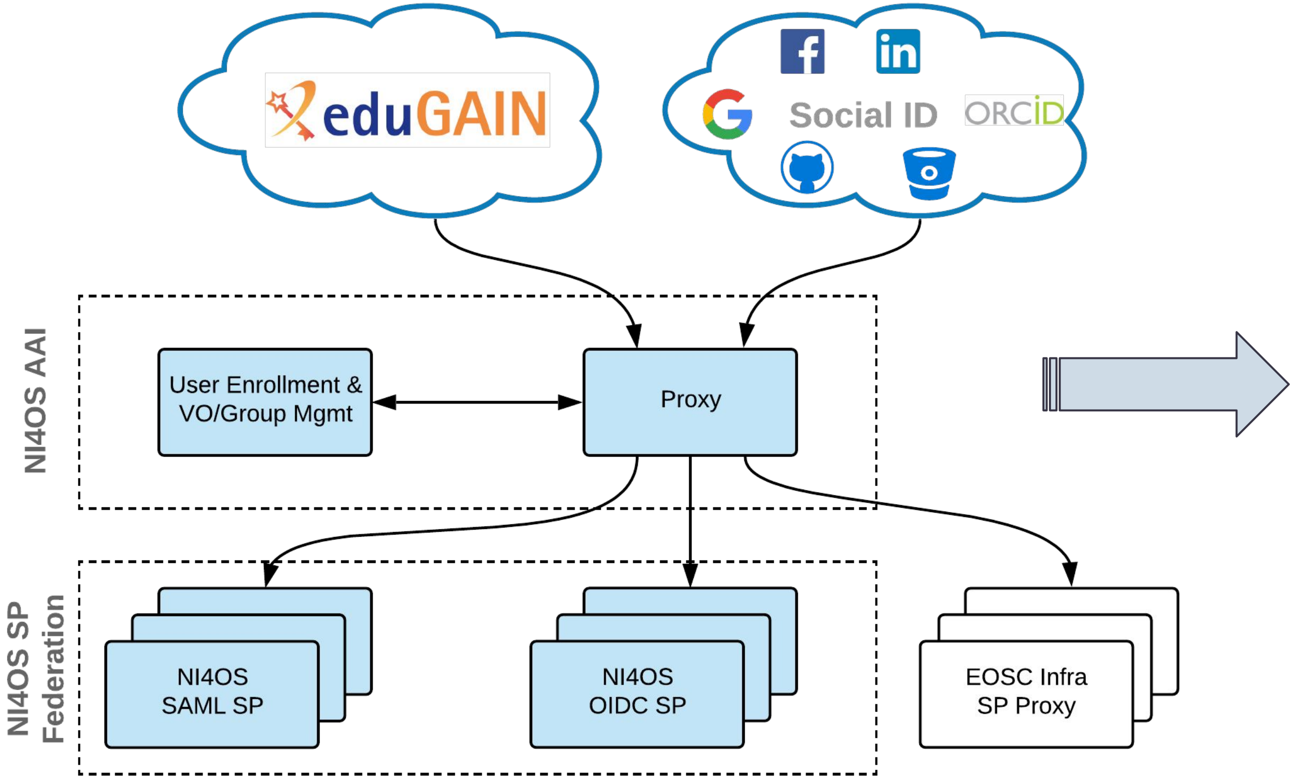
Motivation behind AAI

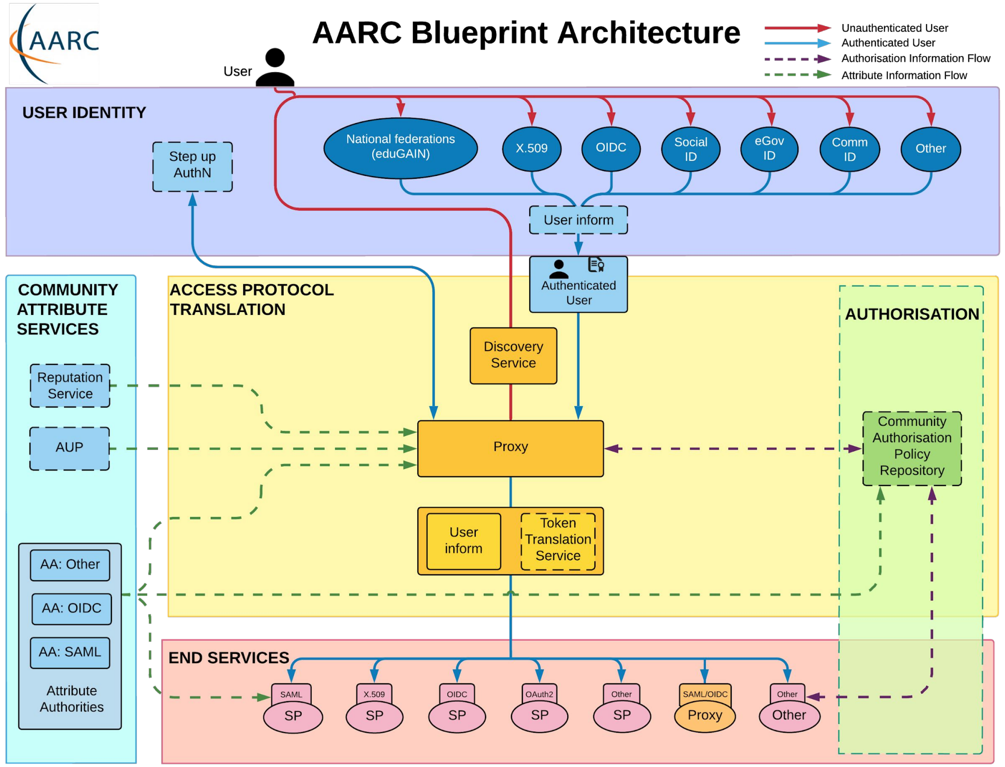
- ❑ Allow researchers from different institutions to access resources in order to **collaborate**
- ❑ Support **different authentications providers**, incl. eduGAIN & social media
  - ❑ Minimises the number of accounts users have to manage
  - ❑ Reduces complexity and security risks
- ❑ Support access to multiple **heterogeneous web and non-web services** and resources offered by different infrastructures
- ❑ Enable **authorised access based on attributes** (e.g. user groups, roles, affiliation) and **capabilities** managed by the user's Home IdP and/or the Research Community
- ❑ **Interoperability and integration** with the existing AAIs of e-Infrastructures and research communities

NI4OS AAI Architecture



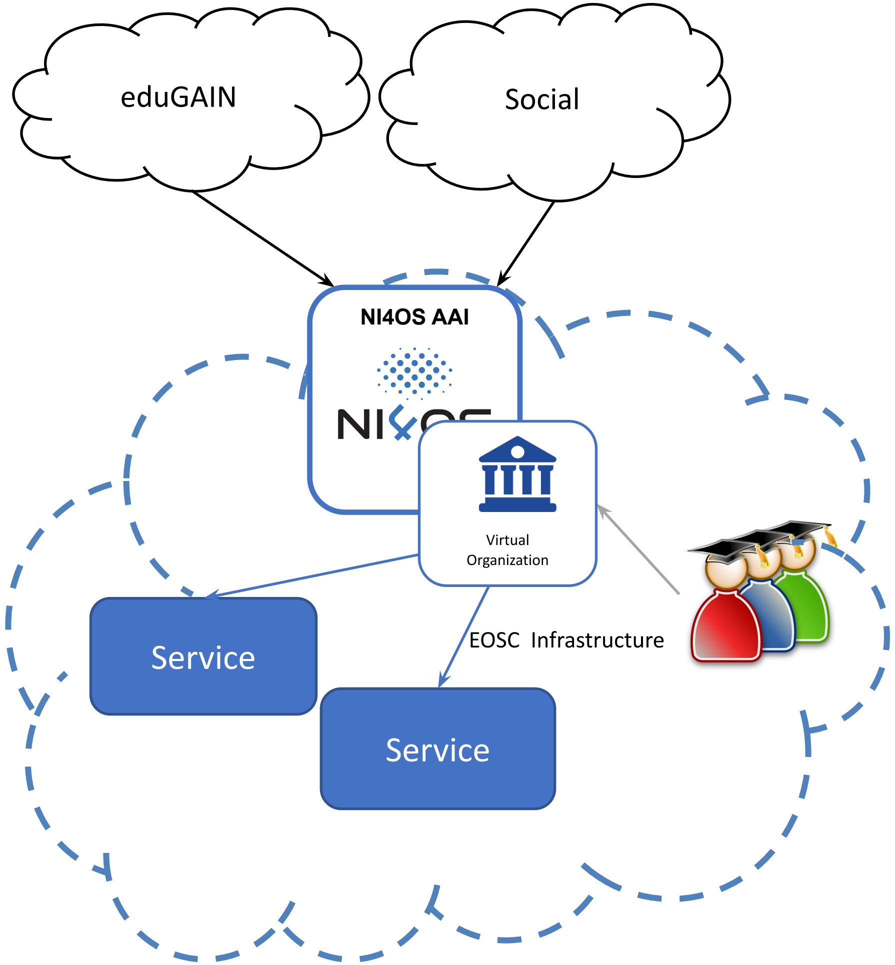
NI4OS AAI Architecture: AARC BPA Implementation





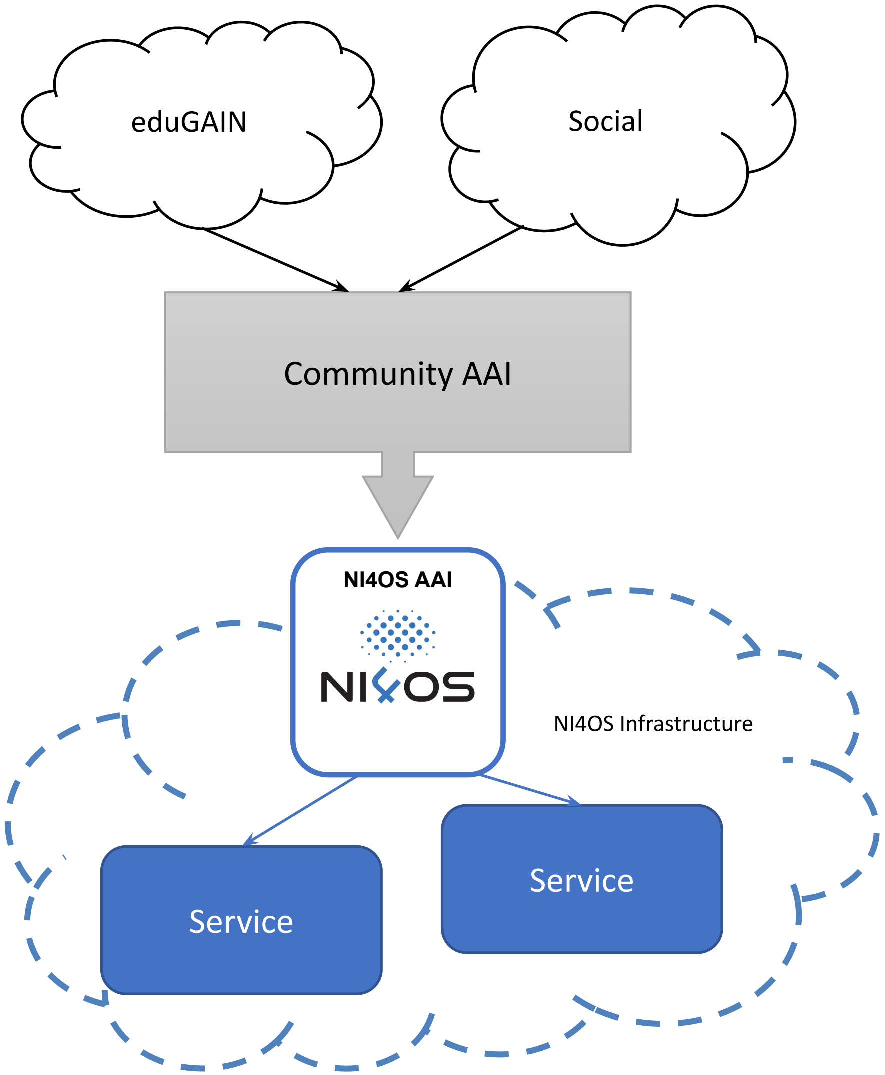
Use case: For communities in need of a group management solution to manage access to resources

- Communities that do not operate their own group management service can leverage the group management capabilities of the NI4OS AAI to:
  - Avoid overhead of deploying a dedicated group management service
  - Allow authorised group admins to manage the information about their users independently
  - Enable easy and secure access to resources offered by NI4OS and other infrastructures participating in EOSC



Use case: For communities operating their own AAI

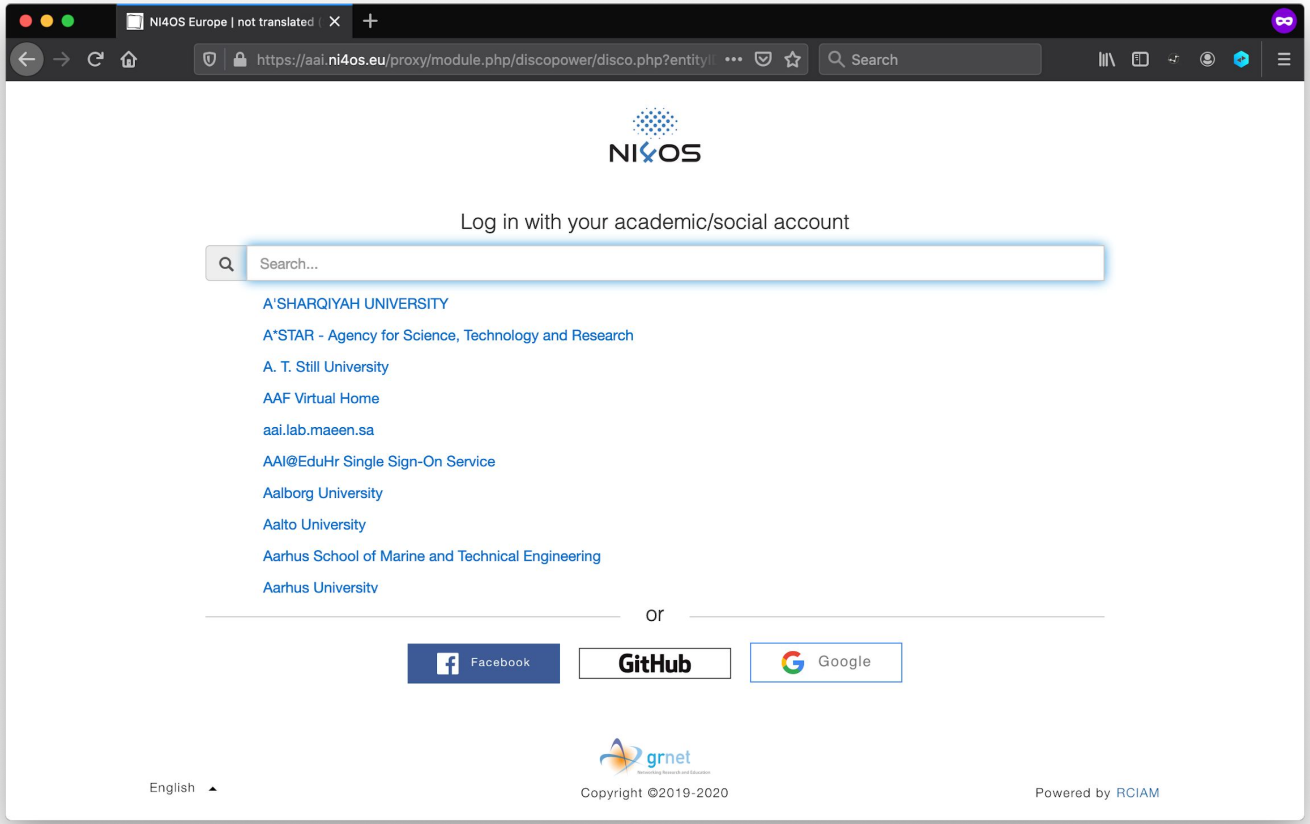
- Community can connect its Community AAI to NI4OS as an IdP to allow its users to access NI4OS services & resources



AAI

Pre-production environment

Authentication Options


NI4OS Europe | not translated
https://aai.ni4os.eu/proxy/module.php/discopower/disco.php?entityI
Search
NI4OS

Log in with your academic/social account

Search...

- A'SHARQIYAH UNIVERSITY
- A*STAR - Agency for Science, Technology and Research
- A. T. Still University
- AAF Virtual Home
- aai.lab.maeen.sa
- AAI@EduHr Single Sign-On Service
- Aalborg University
- Aalto University
- Aarhus School of Marine and Technical Engineering
- Aarhus University

or

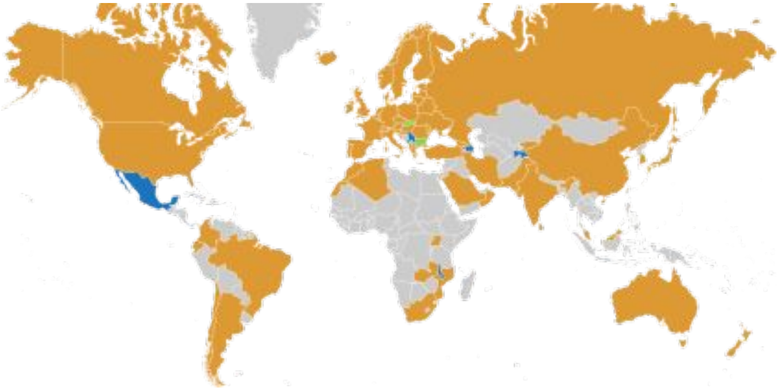
Facebook GitHub Google

English

Copyright ©2019-2020

Powered by RCIAM

- ❑ Academic login from 4100+ Identity Providers eduGAIN

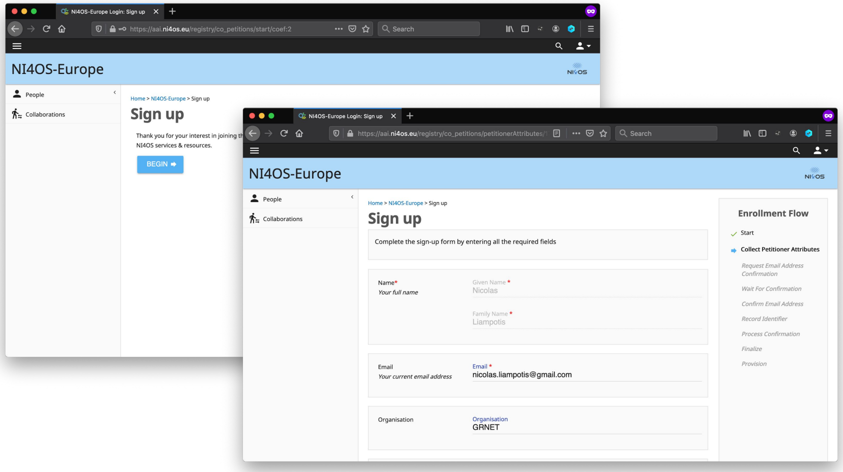


- ❑ Social login

User Enrollment

1. User registration form

Users need to supply only the information not provided by their authentication provider


NI4OS-Europe Login: Sign up
https://aai.ni4os.eu/registry/co_petitions/start/coef:2
Search
NI4OS-Europe
People
Collaborations
Home > NI4OS-Europe > Sign up
BEGIN
NI4OS-Europe Login: Sign up
https://aai.ni4os.eu/registry/co_petitions/petitionerAttributes/
Search
NI4OS-Europe
People
Collaborations
Home > NI4OS-Europe > Sign up

Sign up

Thank you for your interest in joining th
NI4OS services & resources.

Sign up

Complete the sign-up form by entering all the required fields

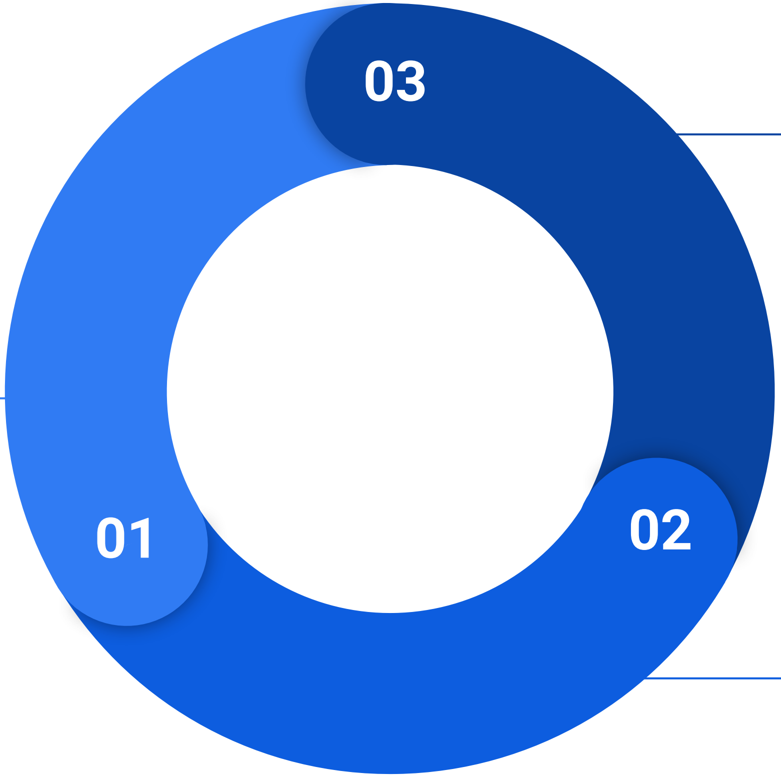
Name*
Your full name
Given Name * Nicolas
Family Name * Liampotis

Email
Your current email address
Email * nicolas.liampotis@gmail.com

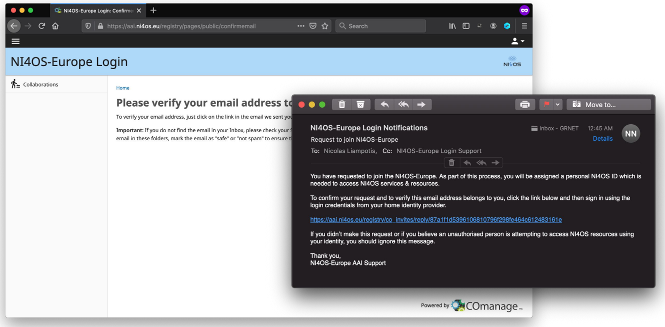
Organisation
Organisation GRNET

Enrollment Flow

- ✓ Start
- Collect Petitioner Attributes
- *Request Email Address Confirmation*
- *Wait For Confirmation*
- *Confirm Email Address*
- *Record Identifier*
- *Process Confirmation*
- *Finalize*
- *Provision*



3. Email verification (not required when a verified email address is already available)



Please verify your email address to

To verify your email address, just click on the link in the email we sent yo

Important: If you do not find the email in your Inbox, please check your S
email in these folders, mark the email as "safe" or "not spam" to ensure t

NI4OS-Europe Login Notifications
Request to join NI4OS-Europe
To: Nicolas Liampotis, Cc: NI4OS-Europe Login Support

You have requested to join the NI4OS-Europe. As part of this process, you will be assigned a personal NI4OS ID which is needed to access NI4OS services & resources.

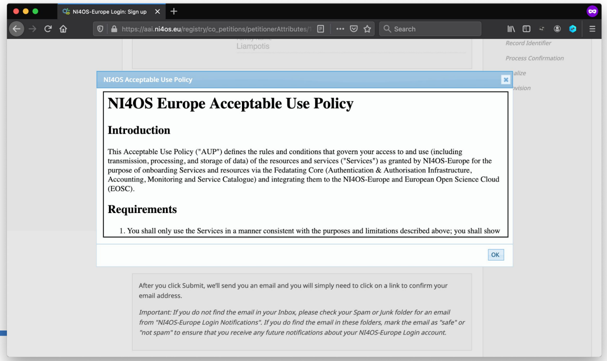
To confirm your request and to verify this email address belongs to you, click the link below and then sign in using the login credentials from your home identity provider.

https://aai.ni4os.eu/registry/co_invites/reply/87a1f1d5396106810796f298fe464c612483161e

If you didn't make this request or if you believe an unauthorised person is attempting to access NI4OS resources using your identity, you should ignore this message.

Thank you,
NI4OS-Europe AAI Support

2. Acceptance Use Policy


NI4OS-Europe Login: Sign up
https://aai.ni4os.eu/registry/co_petitions/petitionerAttributes/
Search
Liampotis
Record Identifier
Process Confirmation
alize
ovision
NI4OS Acceptable Use Policy
OK

NI4OS Europe Acceptable Use Policy

Introduction

This Acceptable Use Policy ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by NI4OS-Europe for the purpose of onboarding Services and resources via the Fedatating Core (Authentication & Authorisation Infrastructure, Accounting, Monitoring and Service Catalogue) and integrating them to the NI4OS-Europe and European Open Science Cloud (EOSC).

Requirements

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show

After you click Submit, we'll send you an email and you will simply need to click on a link to confirm your email address.

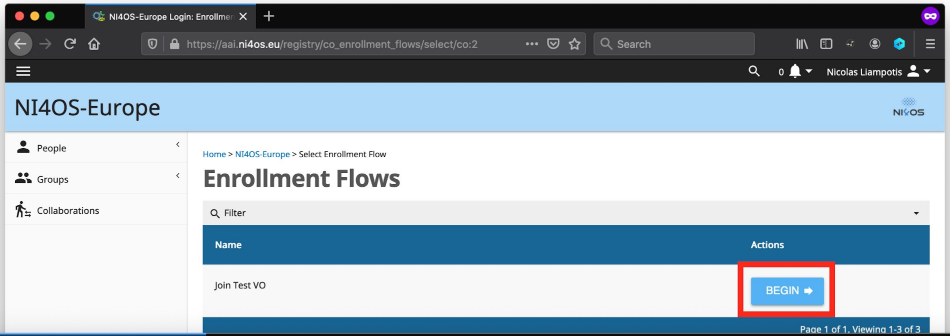
Important: If you do not find the email in your Inbox, please check your Spam or Junk folder for an email from "NI4OS-Europe Login Notifications". If you do find the email in these folders, mark the email as "safe" or "not spam" to ensure that you receive any future notifications about your NI4OS-Europe Login account.

https://aai.ni4os.eu/signup

VO/Group Membership Management

- Researchers from different institutions can collaborate in the context of Virtual Organisations (VOs)
- What is a VO?
  - groups together users with a common purpose
  - represents a single integration point for resource providers
  - provides centralised management of users enrolment and user lifecycle
  - defines their authorization space by organizing users in groups, assign them roles & other attributes

VO/Group Membership Management


NI4OS-Europe Login: Enrollme
https://aai.ni4os.eu/registry/co_enrollment_flows/select/co:2
Search
Nicolas Liampotis
NI4OS-Europe
People
Groups
Collaborations

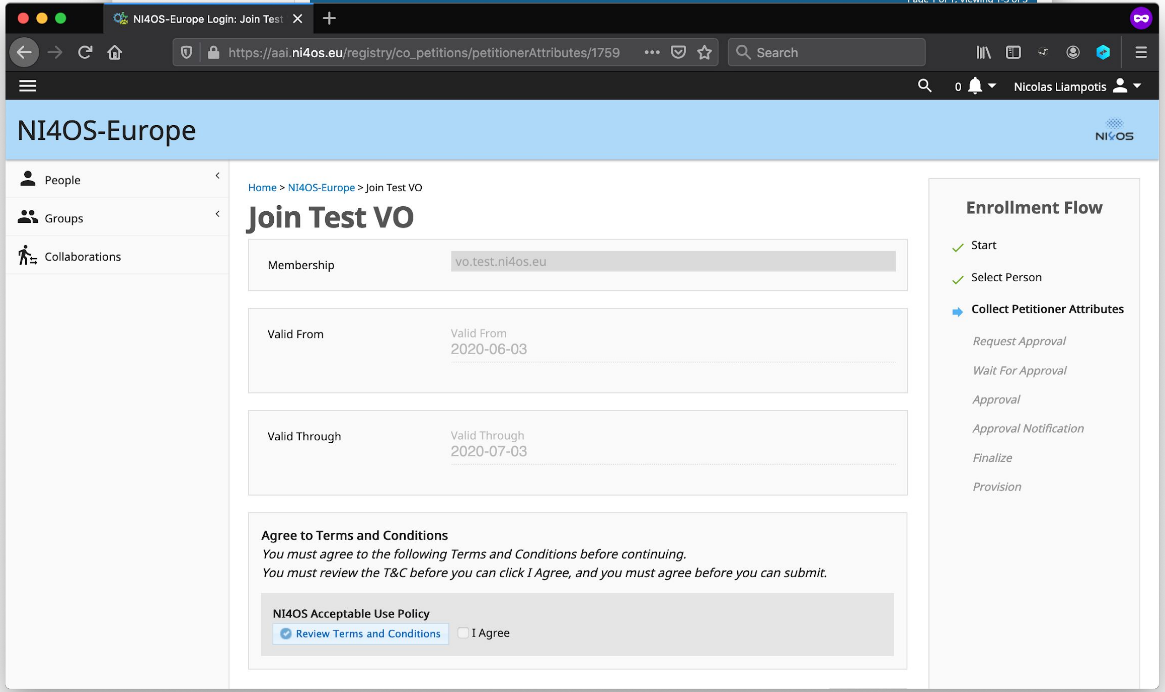
Home > NI4OS-Europe > Select Enrollment Flow

Enrollment Flows

Filter

Name	Actions
Join Test VO	BEGIN ➡

Page 1 of 1, Viewing 1-3 of 3


NI4OS-Europe Login: Join Test
https://aai.ni4os.eu/registry/co_petitions/petitionerAttributes/1759
Search
Nicolas Liampotis
NI4OS-Europe
People
Groups
Collaborations

Home > NI4OS-Europe > Join Test VO

Join Test VO

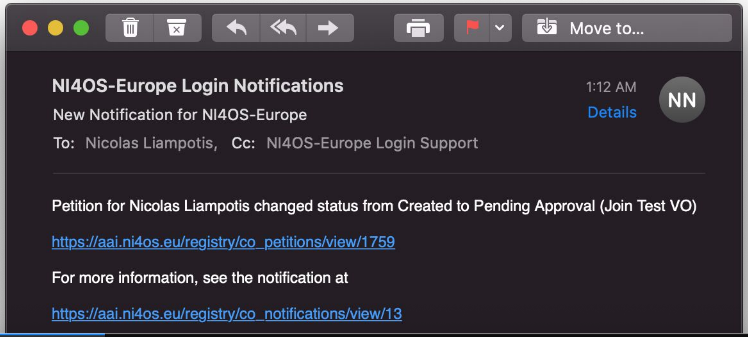
Membership	vo.test.ni4os.eu
Valid From	Valid From 2020-06-03
Valid Through	Valid Through 2020-07-03

Agree to Terms and Conditions
You must agree to the following Terms and Conditions before continuing.
You must review the T&C before you can click I Agree, and you must agree before you can submit.

NI4OS Acceptable Use Policy
Review Terms and Conditions □ I Agree

Enrollment Flow
- ✓ Start
- ✓ Select Person
- ➡ Collect Petitioner Attributes
- *Request Approval*
- *Wait For Approval*
- *Approval*
- *Approval Notification*
- *Finalize*
- *Provision*

User



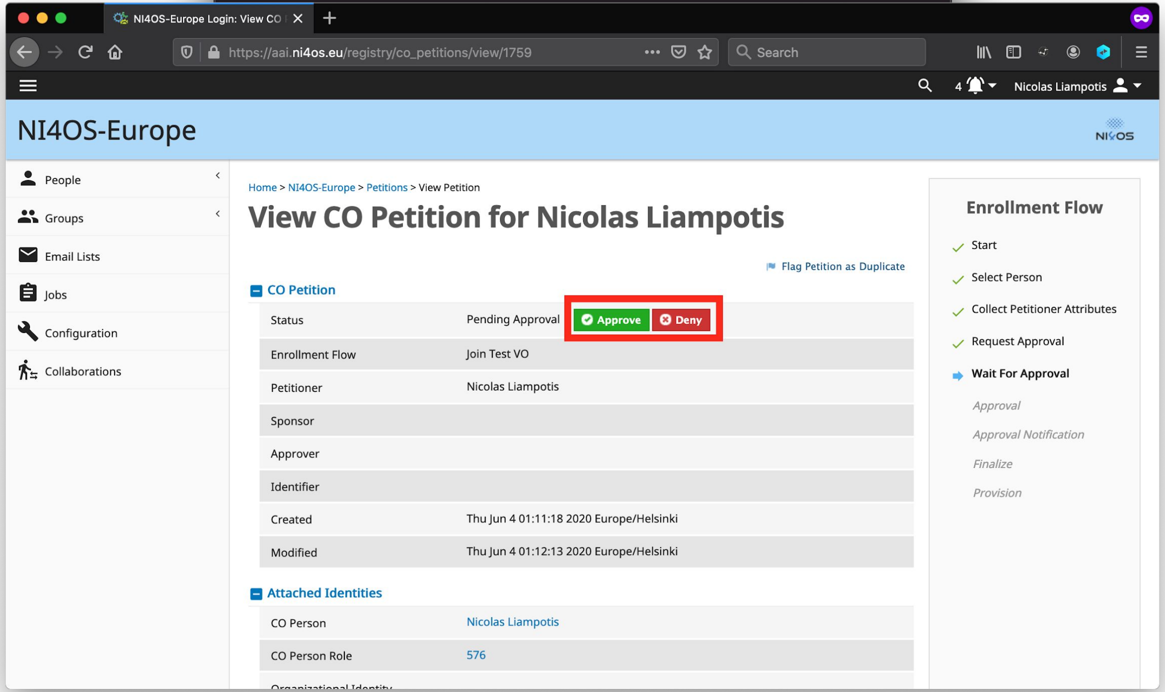
NI4OS-Europe Login Notifications
New Notification for NI4OS-Europe
To: Nicolas Liampotis, Cc: NI4OS-Europe Login Support
1:12 AM
Details
NN

Petition for Nicolas Liampotis changed status from Created to Pending Approval (Join Test VO)

https://aai.ni4os.eu/registry/co_petitions/view/1759

For more information, see the notification at

https://aai.ni4os.eu/registry/co_notifications/view/13



Home > NI4OS-Europe > Petitions > View Petition

View CO Petition for Nicolas Liampotis

Flag Petition as Duplicate

CO Petition

Status	Pending Approval ✓ Approve ✕ Deny
Enrollment Flow	Join Test VO
Petitioner	Nicolas Liampotis
Sponsor	
Approver	
Identifier	
Created	Thu Jun 4 01:11:18 2020 Europe/Helsinki
Modified	Thu Jun 4 01:12:13 2020 Europe/Helsinki

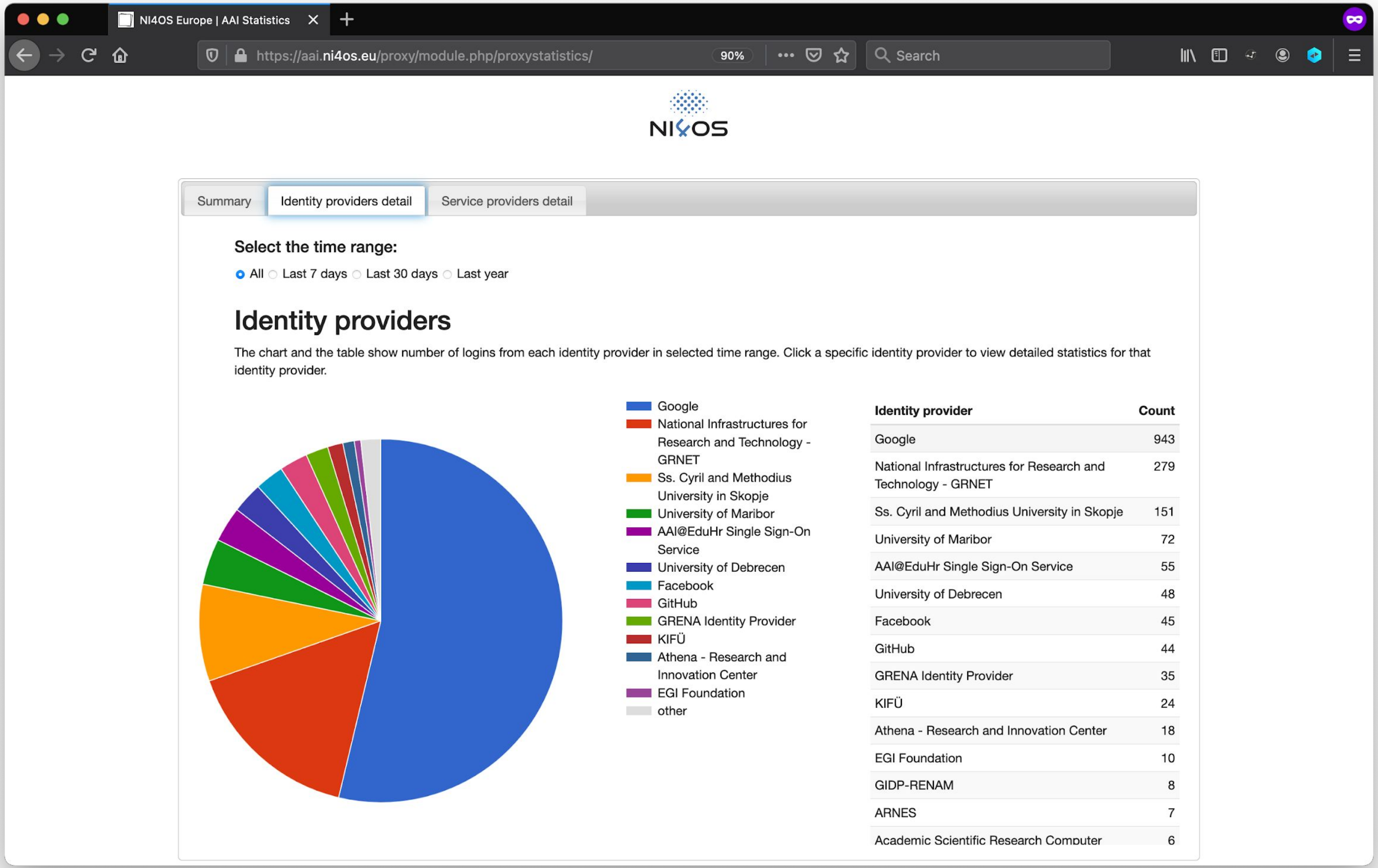
Attached Identities

CO Person	Nicolas Liampotis
CO Person Role	576
Organizational Identity	

Enrollment Flow
- ✓ Start
- ✓ Select Person
- ✓ Collect Petitioner Attributes
- ✓ Request Approval
- ➡ Wait For Approval
- *Approval*
- *Approval Notification*
- *Finalize*
- *Provision*

VO Manager

Statistics


NI4OS Europe | AAI Statistics
https://aai.ni4os.eu/proxy/module.php/proxystatistics/
90%
Search
NI4OS
Summary
Identity providers detail
Service providers detail
Google
National Infrastructures for Research and Technology - GRNET
Ss. Cyril and Methodius University in Skopje
University of Maribor
AAI@EduHr Single Sign-On Service
University of Debrecen
Facebook
GitHub
GRENA Identity Provider
KIFÜ
Athena - Research and Innovation Center
EGI Foundation
other

Select the time range:

● All ○ Last 7 days ○ Last 30 days ○ Last year

Identity providers

The chart and the table show number of logins from each identity provider in selected time range. Click a specific identity provider to view detailed statistics for that identity provider.

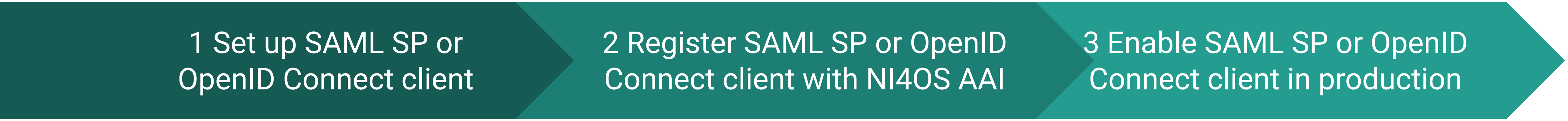
Identity provider	Count
Google	943
National Infrastructures for Research and Technology - GRNET	279
Ss. Cyril and Methodius University in Skopje	151
University of Maribor	72
AAI@EduHr Single Sign-On Service	55
University of Debrecen	48
Facebook	45
GitHub	44
GRENA Identity Provider	35
KIFÜ	24
Athena - Research and Innovation Center	18
EGI Foundation	10
GIDP-RENAM	8
ARNES	7
Academic Scientific Research Computer	6

https://aai.ni4os.eu/proxy/statistics

AAI

Service onboarding

Connecting Services to NI4OS AAI: Integration Process



1 Set up SAML SP or OpenID Connect client

2 Register SAML SP or OpenID Connect client with NI4OS AAI

3 Enable SAML SP or OpenID Connect client in production

NI4OS AAI supports two authN & authZ protocols that you can choose from:

- **SAML:** Install a SAML 2.0 Service Provider software (e.g. Shibboleth-SP) and integrate it into your application
- **OpenID Connect:** Install an OpenID Connect client software (e.g. mod_auth_openidc) and integrate it into your application

- Identify user attributes needed by your service
- Provide SAML SP/OIDC client registration information to NI4OS AAI team
- The NI4OS AAI team checks the information and informs you that your service is registered and ready for testing
- During the testing phase, the service is only accessible by members of the Test VO

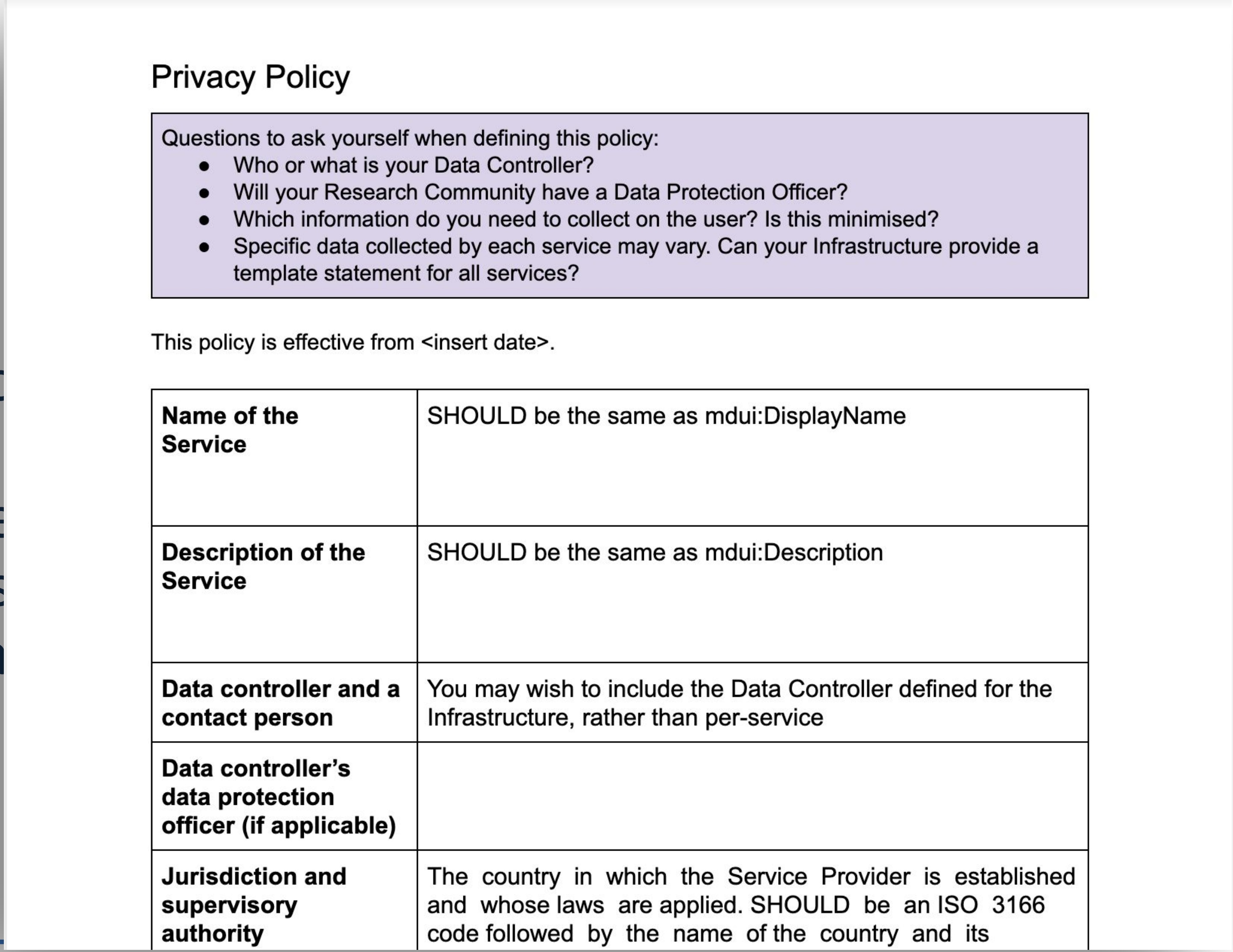
After successfully testing AAI functionality you can request to enable your service for production use

Connecting Services to NI4OS AAI: Registration information

- ❑ Name of the service
- ❑ Short description
- ❑ Privacy statement URL: The privacy policy is used to document the data collected and processed by the service. See the Privacy Policy template.
- ❑ Technical contact address(es)
- ❑ Security contact address(es): Who to contact in case of a security incident (e.g. compromised/misbehaving user account)
- ❑ Logo URL (if available)

Connecting Services to NI4OS AAI: Registration information

- ❑ Name of the service
- ❑ Short description
- ❑ Privacy statement URL: data collected and proc template.
- ❑ Technical contact addre
- ❑ Security contact addres incident (e.g. comprom
- ❑ Logo URL (if available)



Privacy Policy

Questions to ask yourself when defining this policy:

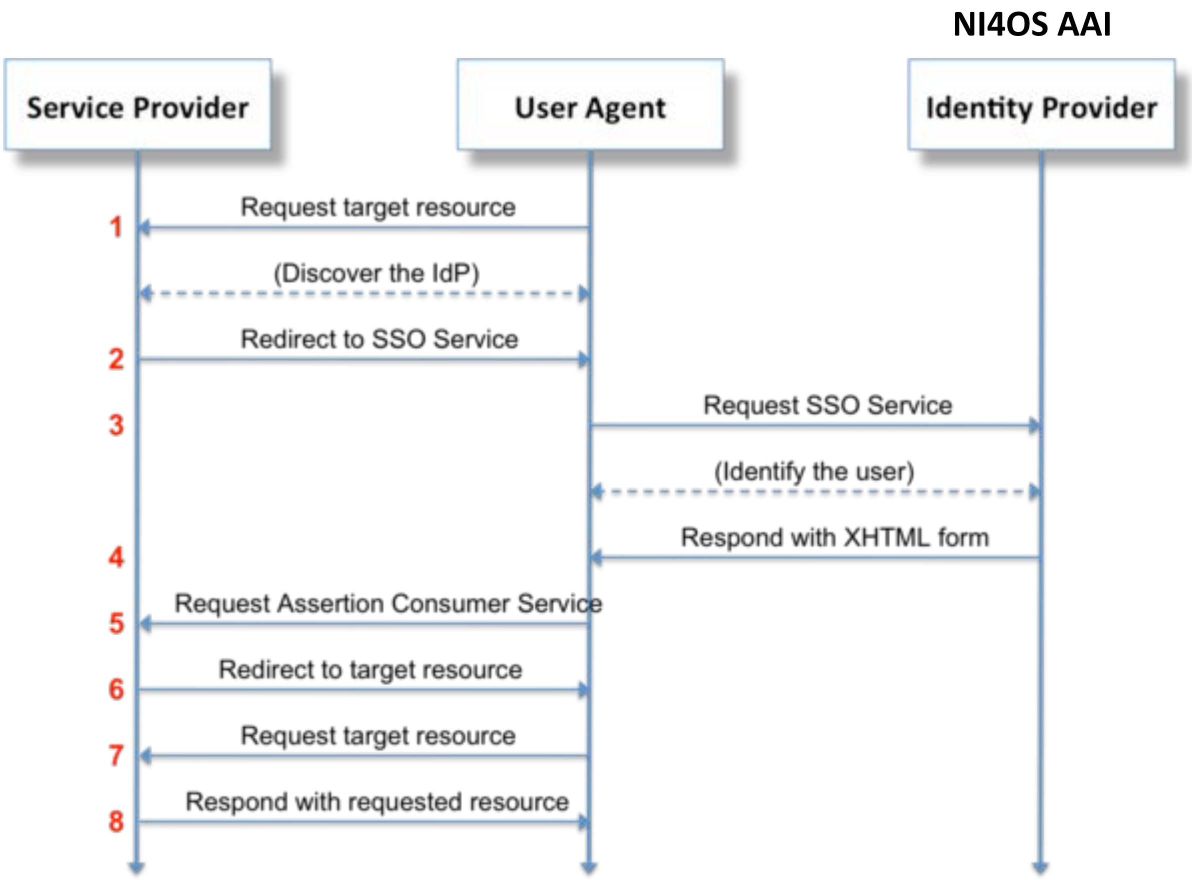
- Who or what is your Data Controller?
- Will your Research Community have a Data Protection Officer?
- Which information do you need to collect on the user? Is this minimised?
- Specific data collected by each service may vary. Can your Infrastructure provide a template statement for all services?

This policy is effective from <insert date>.

Name of the Service	SHOULD be the same as mdui:DisplayName
Description of the Service	SHOULD be the same as mdui:Description
Data controller and a contact person	You may wish to include the Data Controller defined for the Infrastructure, rather than per-service
Data controller's data protection officer (if applicable)	
Jurisdiction and supervisory authority	The country in which the Service Provider is established and whose laws are applied. SHOULD be an ISO 3166 code followed by the name of the country and its

Connecting Services to NI4OS AAI: SAML

- ❑ To enable federated access to a web-based application, you can connect to the NI4OS AAI IdP as a SAML Service Provider (SP).
- ❑ Once the user is authenticated, the NI4OS AAI IdP will return a SAML assertion to the SP containing information about the authenticated user



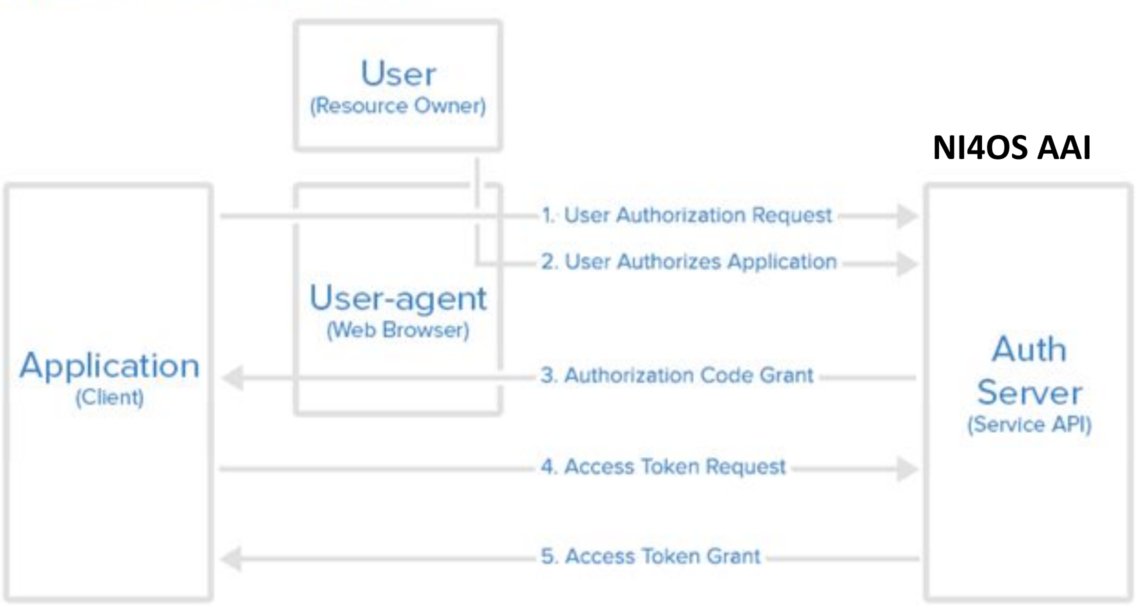
Connecting Services to NI4OS AAI: SAML (contd.)

- SAML authentication relies on the use of metadata. Both parties (you as a SP and the NI4OS AAI IdP) need to exchange metadata in order to know and trust each other.
- The metadata include information such as the location of the service endpoints that need to be invoked, as well as the certificates that will be used to sign SAML messages.
- It is important that you serve your metadata over HTTPS using a browser-friendly SSL certificate, i.e. issued by a trusted certificate authority.
- Add the NI4OS AAI IdP metadata to your SP from:

  https://aai.ni4os.eu/proxy/saml2/idp/metadata.php

Connecting Services to NI4OS AAI: OpenID Connect

- ❑ OpenID Connect is an identity layer on top of OAuth 2.0, which allows clients to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user.
- ❑ You need OAuth 2.0 credentials (client ID and secret) to authenticate users through the NI4OS OIDC Provider.



Connecting Services to NI4OS AAI: OpenID Connect

- Identify scopes:
  - `openid` (mandatory) → user identifier
  - `profile` → name
  - `email` → email
  - `eduperson_entitlement` → VO/group information and/or capabilities
  - `offline_access` → Refresh Token:
    - Used to obtain a renewed Access Token without the user being present
    - You can request new Access Tokens until the Refresh Token is blacklisted
    - Applications must store Refresh Tokens securely
- Specify one or more redirect URIs → Web authentication
- Indicate whether your client should be granted token introspection access → Resource providers/API access

Connecting Services to NI4OS AAI: SAML vs OpenID Connect

SAML v2.0
Security Assertion Markup Language

- Based on XML
- Supports Web-browser SSO

OpenID

- Based on JSON
- Supports Web-browser SSO
- Supports Non-web-browser access use cases:
  - API authorisation
  - Offline access
  - Input-constrained devices (e.g. terminals)

AAI

Managing access to resources

Authorisation

1. Attribute-based authorisation
   - ❑ VO/Group membership and role information
   - ❑ Assurance information
   - ❑ Affiliation with home organisation

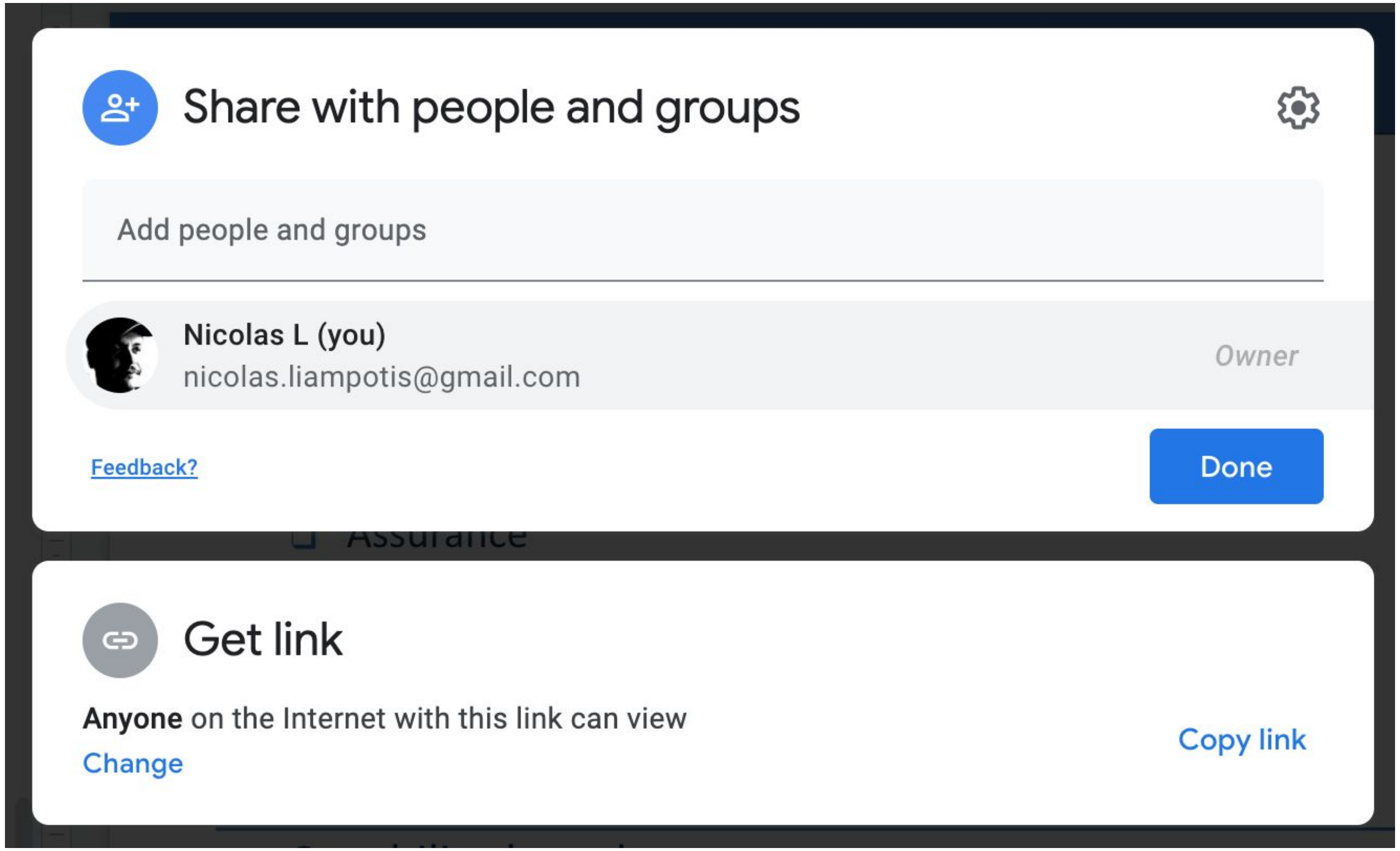
2. Capability-based authorisation
   - ❑ Resources a user is allowed to access
   - ❑ Optional list of specific actions the user is entitled to perform

Attribute-based vs. Capability-based authorisation

The two models *can* co-exist even within the same service

Attribute-based authorisation

Capability-based authorisation



Share with people and groups

Add people and groups

Nicolas L (you)
nicolas.liampotis@gmail.com — *Owner*

Get link

Anyone on the Internet with this link can view

Slide courtesy of B. Bockelman

Attribute-based Authorisation: VO/Group Membership & Roles

- Allows services to control access to resources based on information about the VO/groups a user is a member of

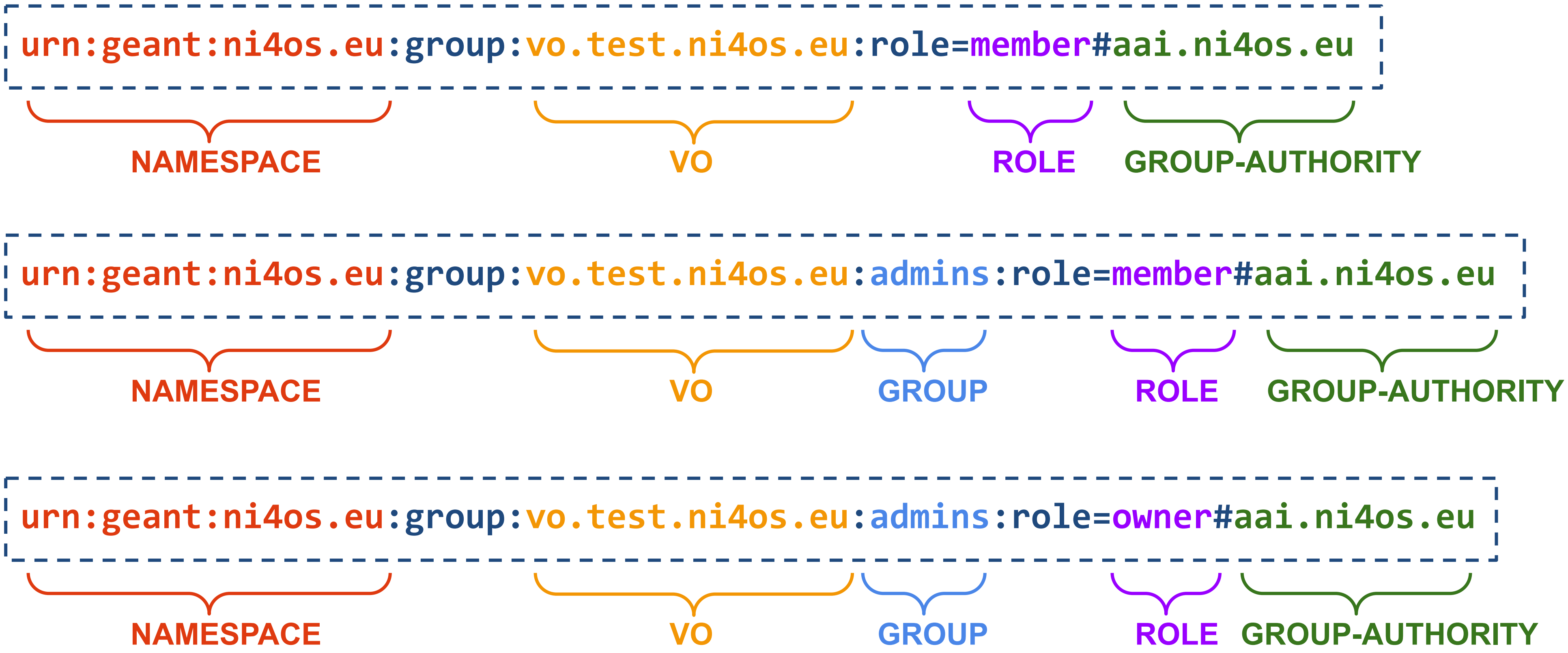
- One or more values encapsulated in:
  - `eduPersonEntitlement` attribute (SAML)
  - `eduperson_entitlement` claim (OIDC)

- Each value formatted as a URN ⟶ AARC-G002

```
<NAMESPACE>:group:<VO>[:<GROUP>*][:role=<ROLE>]#<GROUP-AUTHORITY>
```

Attribute-based Authorisation: VO/Group Membership & Roles

- Examples



urn:geant:ni4os.eu:group:vo.test.ni4os.eu:role=member#aai.ni4os.eu

urn:geant:ni4os.eu:group:vo.test.ni4os.eu:admins:role=member#aai.ni4os.eu

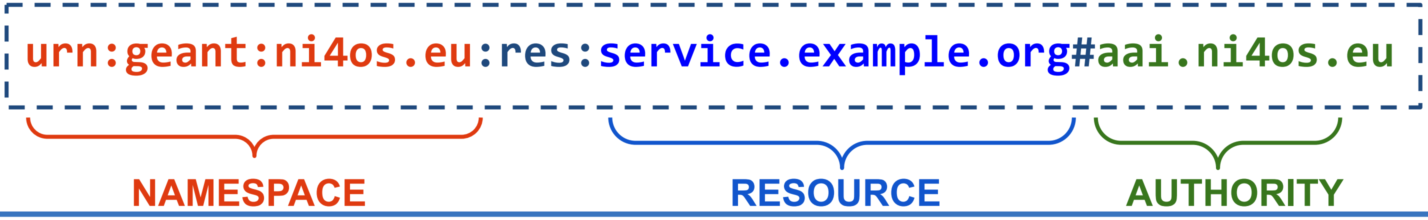
urn:geant:ni4os.eu:group:vo.test.ni4os.eu:admins:role=owner#aai.ni4os.eu

Capability-based Authorisation

- Capabilities can be used to convey authorisation information to services in a compact form
- One or more values encapsulated in:
  - `eduPersonEntitlement` attribute (SAML)
  - `eduperson_entitlement` claim (OIDC)
- Each value formatted as a URN → [AARC-G027]()

```
<NAMESPACE>:res:<RESOURCE>[:<CHILD-RESOURCE>]...
[:act:<ACTION>[,<ACTION>]...]#<AUTHORITY>
```

- Example value:



```
urn:geant:ni4os.eu:res:service.example.org#aai.ni4os.eu
```

AAI

Standards & interoperability guidelines for service onboarding

AAI Standards & APIs

Standard	Short description	References
Security Assertion Markup Language (SAML) 2.0	OASIS standard for exchanging authentication and authorisation data between parties.	https://www.oasis-open.org/standards#samlv2.0
OAuth 2.0	Standard for authorisation that enables delegated access to server resources on behalf of a resource owner	"The OAuth 2.0 Authorization Framework", RFC 6749, https://www.rfc-editor.org/info/rfc6749
OpenID Connect 1.0	Identity layer on top OAuth 2.0. Enables Clients to (i) verify the identity of the End-User based on the authentication performed by an AS; (ii) obtain basic profile information about the End-User in an interoperable and REST-like manner	“OpenID Connect Core 1.0”, https://openid.net/specs/openid-connect-core-1_0.html

AAI Standards & APIs (contd.)

Standard	Short description	References
X.509	ITU-T standard for a public key infrastructure (PKI), also known as PKIX (PKI X509)	"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, https://www.rfc-editor.org/info/rfc5280 "Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile", RFC 3820, https://www.rfc-editor.org/info/rfc3820
Lightweight Directory Access Protocol (LDAP)	Provides access to distributed directory services that act in accordance with X.500 data and service models	https://tools.ietf.org/html/rfc4511

AAI Standards & APIs (contd.)

API	Short description	References
OAuth 2.0 Token Introspection	Protocol that allows authorised protected resources to query the authorisation server for determining the set of metadata for a given OAuth2 token, including its current validity.	https://tools.ietf.org/html/rfc7662
OAuth 2.0 Token Exchange	Protocol for requesting and obtaining security tokens from OAuth 2.0 authorization servers, including security tokens employing impersonation and delegation	https://tools.ietf.org/id/draft-ietf-oauth-token-exchange-14.html

AAI Standards & APIs (contd.)

API	Short description	References
OAuth 2.0 Device Authorization Grant	Enables OAuth 2.0 clients on input-constrained devices to obtain user authorisation for accessing protected resources without using an on-device user-agent	https://tools.ietf.org/html/draft-ietf-oauth-device-flow-15
System for Cross-domain Identity Management (SCIM) 2.0	Open API for managing identities	SCIM: Core Schema , RFC7643, https://tools.ietf.org/html/rfc7643 SCIM: Protocol, RFC7644, https://tools.ietf.org/html/rfc7644 SCIM: Definitions, Overview, Concepts, and Requirements, RFC7642, https://tools.ietf.org/html/rfc7642

Any Questions?