InAcademia

Simple Validation Service

Niels van Dijk

InAcademia lead, GN4-1 SA5

Technical Product Manager, SURFnet

TF-MSP, Espoo, Finland

10-09-2015

Academic Affiliation and Federations

- Many Services (want to) provide benefits or discounts for members of Academia (Student/Employee)
- And a federated (SAML) login with the (eduPerson)Affiliation attribute can be used to validate membership of the academic community.

- However:
  - Joining a federation has several obstacles (policies and contracts)
  - Implementing SAML and doing federation is not easy
  - Interfederation is even harder
  - Upfront cost, but no customers

- A lot of work, while the service *only* needs the Affiliation, which is pretty low risk in the data protection spectrum

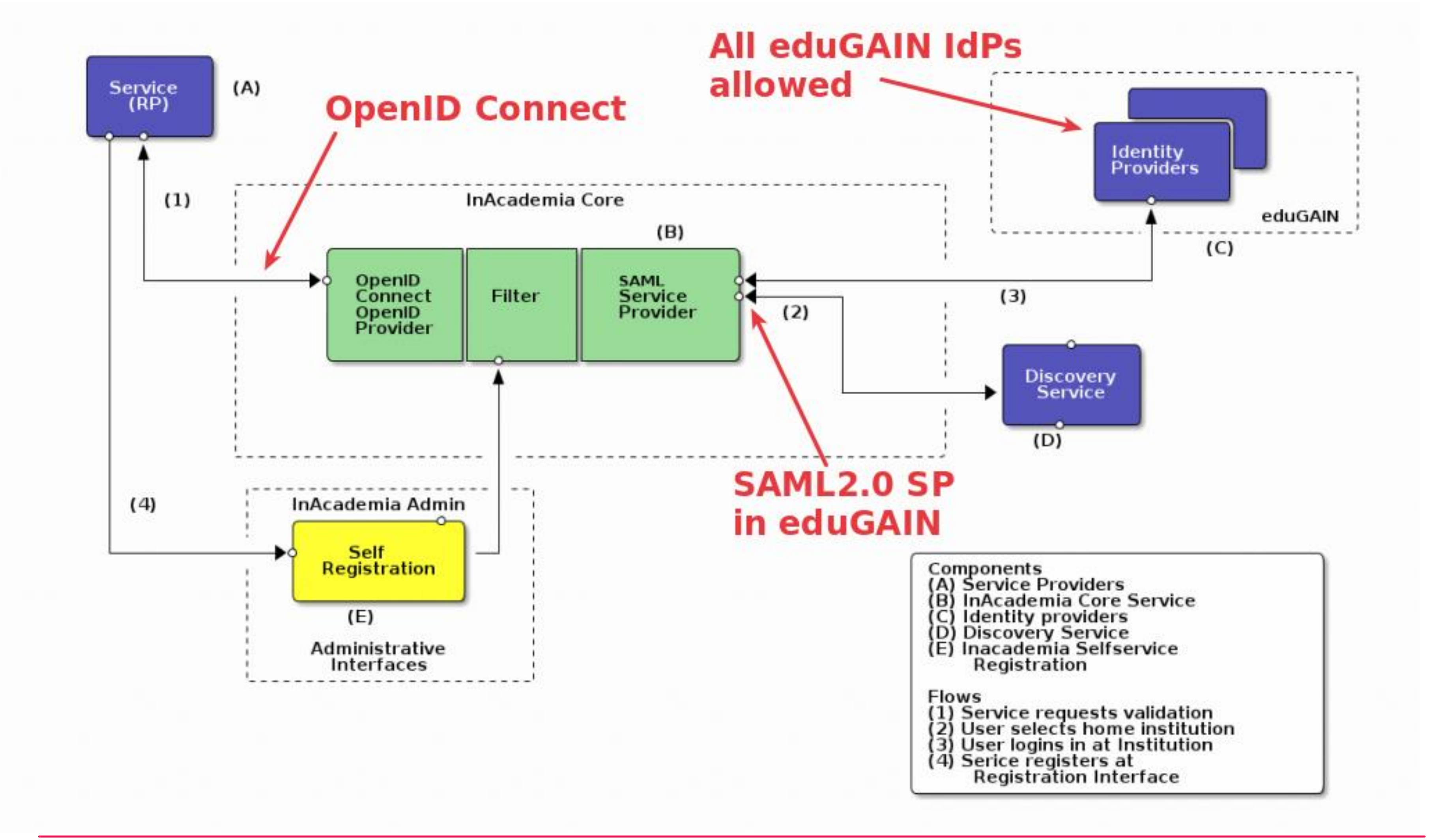
Example use cases for Affiliation validation

- Discount at web shops
- One-time discount, e.g., at Telco (GN3plus SA7 mobile procurement)
- ‘Free’ access to generic cloud service: Microsoft, Apple, Adobe
- Online reservations for Theatres and Sports accommodations on Student Campuses
- Validate affiliation on relevant ‘Social’ platforms such as Mendeley, ResearchGate, LinkedIn, etc.
- Lightweight validation for research services such as ORCID

InAcademia - *a Simple validation Service*

- What would make affiliation validation easier?
  - Services get **most attributes from user** (self asserted)
  - Only affiliation *must* come from the Home Organisation
  - Query a **single, centralised service** to **confirm** affiliation
  - A user ‘proves’ affiliation by authentication with home IdP
  - A **simple protocol** can be used by the Services
  - Validation service accessible for all eduGAIN IdPs
  - The **policy barrier** for using should be **low**
  - Service pays a **small transaction fee**

InAcademia - *Simplified overview*



Components
(A) Service Providers
(B) InAcademia Core Service
(C) Identity providers
(D) Discovery Service
(E) Inacademia Selfservice Registration

Flows
(1) Service requests validation
(2) User selects home institution
(3) User logins in at Institution
(4) Serice registers at Registration Interface

InAcademia - *Supported scopes*

	Description
Affiliation Scopes	Based on [1], [2]
affiliated	This person is affiliated to the institution (Student, Employee). Affiliation value is **not** revealed.
employee	Institutional workers whose primary role is teaching or research and workers other than teachers or researchers
student	A student at the institution
alum	An alumnus at the institution
Identifier Scopes	(not the SAML persistent ID)
persistent	A persistent identifier, unique for this person, on a per RP, per IdP basis
transient	A transient identifier, which is unique for each transaction

[1] http://www.geant.net/service/eduGAIN/resources/Documents/GN3-11-012%20eduGAIN_attribute_profile-05%2012%202013.pdf
[2] http://www.terena.org/activities/refeds/docs/ePSAcomparison_0_13.pdf

InAcademia - *Supported claims*

	Description
Claims	(Optional)
country	What is the country of the users home institution? -> Deducted from Country of IdP
domain	What is the domain name of the institution of the user? -> SchacHomeOrganisation attribute

Examples:
scope=affiliated
scope=affiliated transient
scope=affiliated persistent
scope=affiliated persistent & claim = country
scope=student persistent & claim = country domain

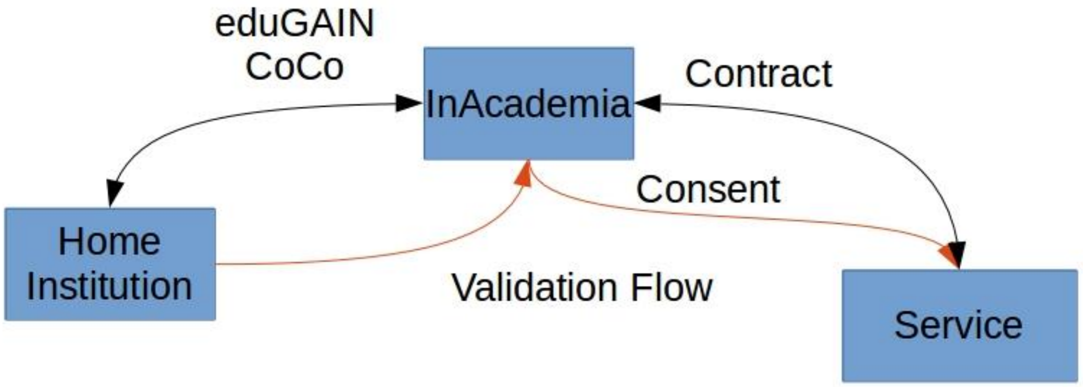
Legal considerations

- Technical measures for dealing with personal data:
  - InAcademia supports eduGAIN Code of Conduct
  - InAcademia requests pseudonymous id and affiliation from IdP
  - InAcademia sends (different) pseudonymous identifier and affiliation confirmation to Service
  - All transactions are atomic: No user data stored, consent always asked, no SSO
  - All consent logging will be stored pseudonymously (SHA512)
  - Transaction data is aggregated immediately

- Two legal models for InAcademia, in relation to how the contracts are arranged
  - Direct legal responsibility: Broker
  - Just passing data: Gateway

Scenario 1: InAcademia 'Broker'

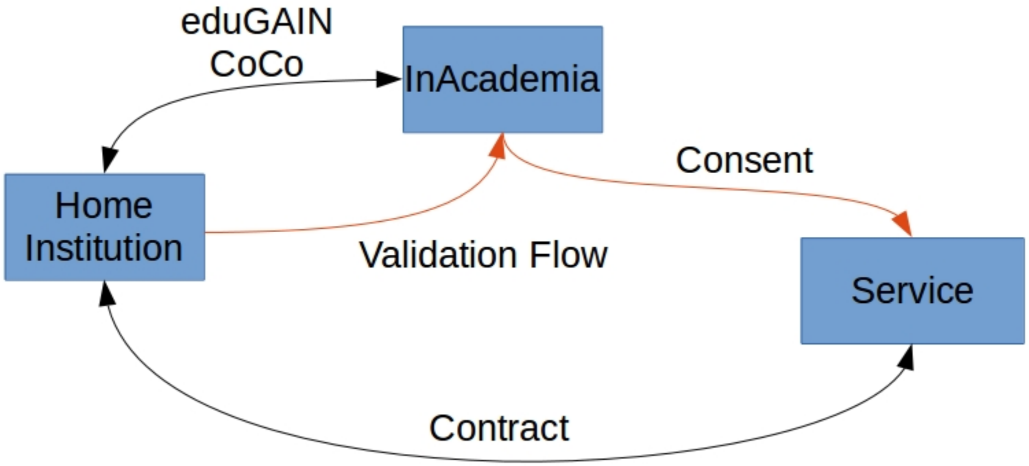
- InAcademia 'Broker': InAcademia engages in contracts with services



- InAcademia is a Service Provider in the local Federation (via eduGAIN)
- Even if InAcademia supports eduGAIN, there is no legal ground to process data coming from an Institution
- Consent from an end user suffices here, **but must be given freely.** That cannot be guaranteed for all services
- Solution is a (two party) contract between Home Institution and InAcademia. Scales poorly….

Scenario 2: InAcademia ‘Gateway’

- InAcademia ‘Gateway’: InAcademia facilitates data transfer



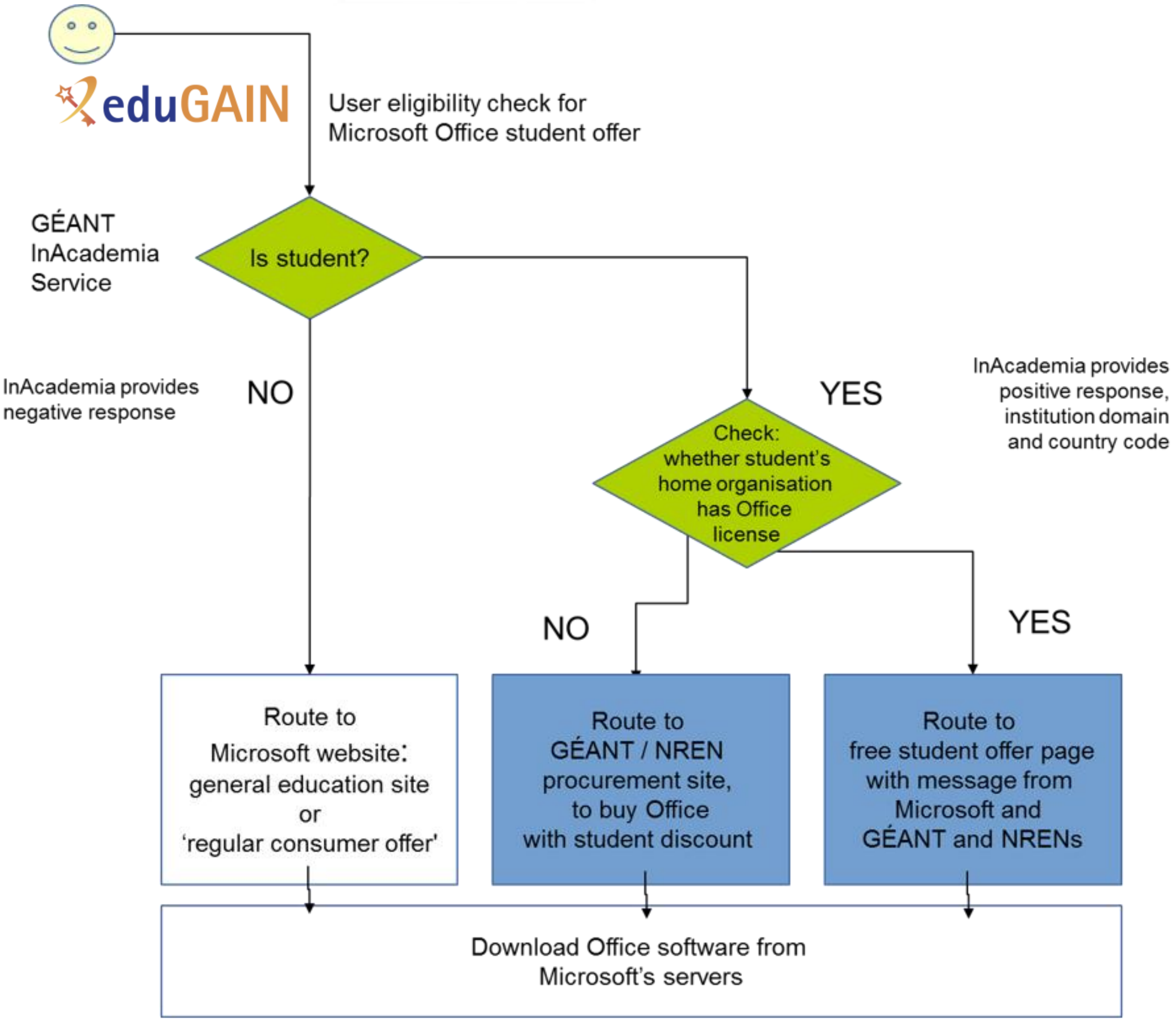
- Contract between Service and Home Institution – or its representatives: NRENs, Federations, Procurement Org., GÉANT, etc
- Contract should at minimum contain clauses from eduGAIN CoCo
- InAcademia is now (only) the technical transfer mechanism, handling personal data on behalf of Home Institution
- Requires good support for connecting services
- Investigate opt-in vs opt-out for Home Organisations

Cost and Benefit: “The numbers game”

- *Cost*
  - InAcademia platform is nimble and has all characteristics to scale well
  - If support is routed through NRENs / Federations operational cost is expected to be low

- *Benefit*
  - As this service does not directly benefit Institutions, it should be self sustaining
  - A ‘pay per use’ model is proposed where an initially low transaction fee gradually increases, in relation to transaction frequency
  - No or low fees for research services within community
  - Support from NRENs/GÉANT is required for a few years to allow InAcademia reach a point where it can sustain itself

Showcase: Microsoft Office365 for Students



User eligibility check for Microsoft Office student offer

GÉANT InAcademia Service

Is student?

InAcademia provides negative response

NO

YES

InAcademia provides positive response, institution domain and country code

Check: whether student's home organisation has Office license

NO

YES

Route to Microsoft website: general education site or 'regular consumer offer'

Route to GÉANT / NREN procurement site, to buy Office with student discount

Route to free student offer page with message from Microsoft and GÉANT and NRENs

Download Office software from Microsoft's servers

Proposal: Two operational models for InAcademia

- *“End-user” version*
  - InAcademia is a independent SP in the federation and directly deals with connecting services for end-users.
  - NOT for services that are in primary process
  - There is one contract for all services (no per-service exceptions)
  - Transaction fee billed towards Service
  - Centrally operated (GEANT org?)

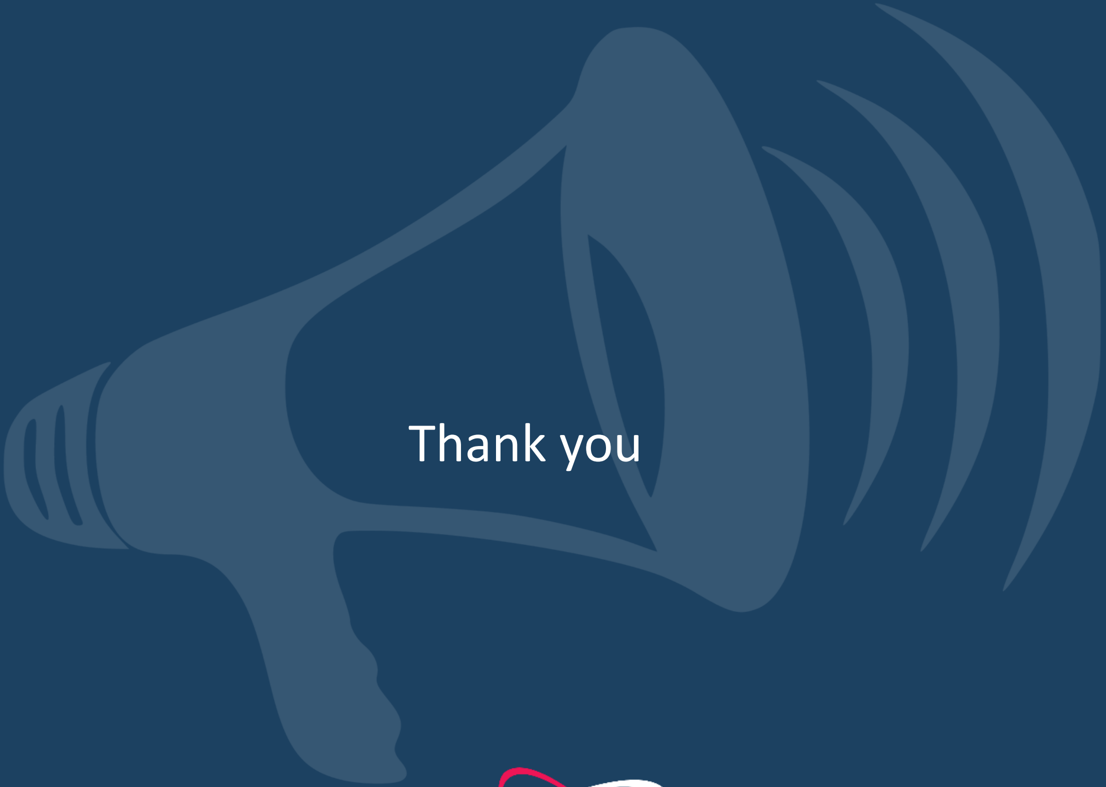
- *“Business” version*
  - InAcademia is technical gateway, NREN/Federation deals with services.
  - All services may be included
  - Procurement done nationally, Pan EU (GEANT.org and/or SA7), coalition of willing (TCS)
  - Transaction fee billed towards NREN/Federation/Procurement Org
  - Centrally operated, but self-service for NREN/Federation/Procurement Org

InAcademia - Recap

- For Identity Providers, Federations and NRENs
  - SAML based, connected via eduGAIN
  - Two profiles that have minimal, ‘low risk’ attribute requirements
  - No personal data stored at service
  - One connection with many Services that are high value to users, but low effort for IdP
  - A pricing model which creates a revenue stream to sustain InAcademia upon success

- For Services
  - OpenID Connect interface towards Service, no SAML required
  - No need to deal with (inter) federation
  - Simplified Policy, compatible with eduGAIN CoCo
  - The pricing model allows new Services to enter the market easily
  - One connection with many trusted Identity Providers

- Allows Procurement to collaborate on pan EU scale as it provides a safe, secure and privacy preserving gateway to (potentially) all end users in Academia



Thank you

GÉANT

Networks · Services · People

www.geant.org

This work is part of a project that has applied for funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).