# InAcademia.org

**Simple affiliation validation for Academia**

Niels van Dijk, SURFnet bv

eduGAIN Townhall Meeting, Wein
December 2, 2014

# a Simple validation Service

- Many Services provide benefits or discounts for members of Academia (Student/Staff/Faculty)

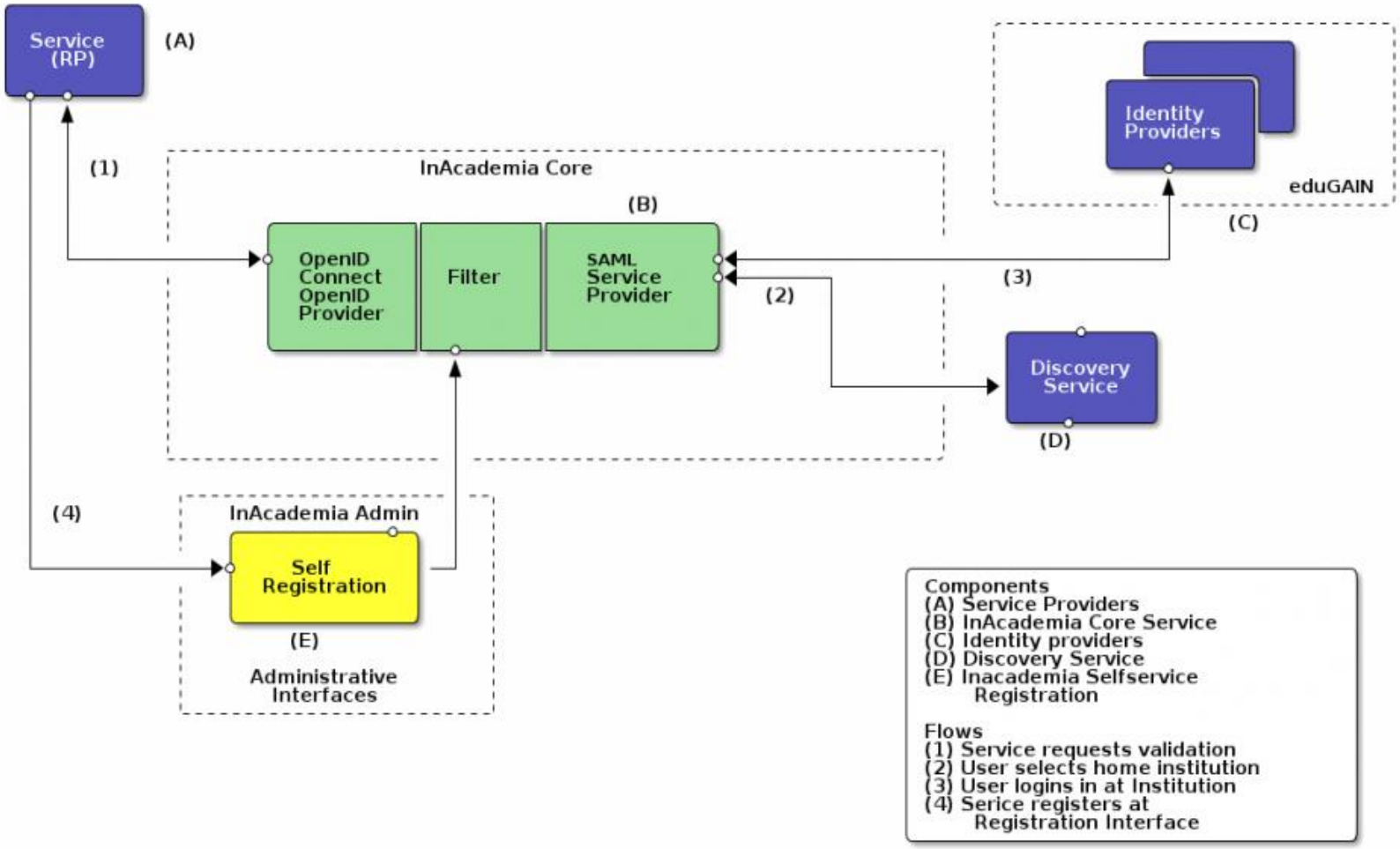
- A federated (SAML) login with the eduPersonAffiliation attribute can be used to validate membership of the academic community, but:
  - Joining a federation is a problem (policies and contracts)
  - Implementing SAML and doing federation is not easy
  - Interfederation is even harder
  - Upfront cost, but no customers

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

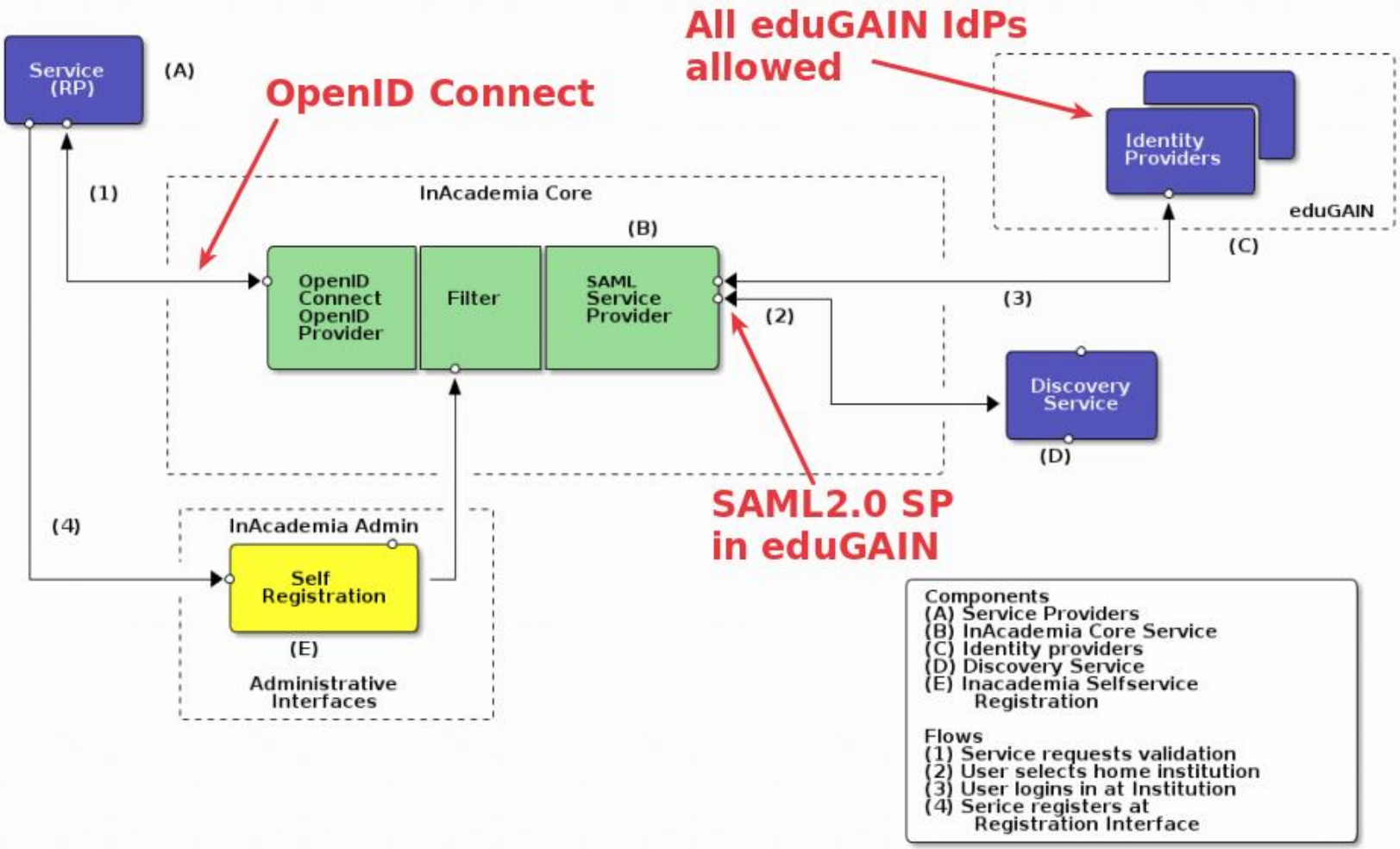
# Use cases for Affiliation validation

- Discount at web shops
- 1 Time discount at Telco (Geant3+ SA7 mobile procurement)
- ‘Free’ access to generic cloud service, e.g. Microsoft (DreamSpark, ItAcademey, Office365), Apple, Adobe, Cisco, etc
- Digital reservations for Theatres and Sports accommodations on Student Campuses
- Validate Academic affiliation on relevant ‘Social’ platforms like e.g. ORCID, Mendeley, ReseachGate, LinkedIn, etc.

# Simplified overview



# Simplified overview -2



# Benefits

- For Identity Providers
  - SAML based, connected via eduGAIN
  - Two profiles that have minimal, ‘low risk’ attribute requirements
  - No personal data stored at central service
  - One connection with many Services that are high value to users, but low effort for IdP

- For Services
  - OpenID Connect interface towards Service, no SAML required
  - No need to deal with (inter) federation
  - Simplified Policy, compatible with eduGAIN CoCo
  - Little upfront cost, only pay when a transaction is made
  - One connection with many trusted Identity Providers

# Timeline

- Public Beta available in Jan 2015
  - Technically available
  - Hosted by SURFnet & SUNET/NORDUnet
  - Start of pilots
- By March 2015
  - Legal & Policy validated
  - Bugfixes and pilot feedback done
- GEANT4 (year 1)
  - Work out operational model
  - Setup transaction fee & billing
  - Move towards fully operation service

# Thank you!


Connect | Communicate | Collaborate

www.geant.net

www.twitter.com/GEANTnews | www.facebook.com/GEANTnetwork | www.youtube.com/GEANTtv


# InAcademia.org

## Simple affiliation validation for Academia

***Bonus Slides***

Niels van Dijk, SURFnet bv

eduGAIN Townhall Meeting, Wein
December 2, 2014

# Considerations

- Can this be simplified?
  - Service gets attributes directly from user (self asserted or social)
  - Service queries a single, centralised service, the “InAcademia Simple validation Service” (SvS) to confirm affiliation
  - A simple, well understood, protocol can be used to query SvS
  - The policy barrier for using SvS is low
  - The user ‘proves’ his/her affiliation at SvS which is under control of the federations / NRENs
  - SvS is connected to eduGAIN
  - Authentication at home IdP delivers requested affiliation
  - SvS interprets the affiliation and answers the Service, but SvS *never* directly delivers attribute values to the requesting Service
  - User gets discount
  - Service pays a small transaction fee

# Project and Team

- Geant3+ JRA3-T1 project
- Team
  - Devs: Daniel, Rebecka, Roland (Umeå University)
  - Infra: Leif (SUNET), Niels (SURFnet),
  - Legal: Mikael (CSC), Evelijn (SURFnet)
  - Documentation: Remco, Niels (SURFnet)
  - Project: Niels
  - with additional support from Geant3+ SA*
- Started Sept 1, 2014 ends March 2015
- Proposed to continue in Geant4 SA5

# Design Characteristics

- One service, but nodes are geographically distributed (preferably globally). 4 nodes (2x NL, 2x SE) by March 2015
- Transactions are handle in the same zone whenever possible.
  (If Service is in the same zone as the IdP, userdata remains in that same zone)
- Two Attribute profiles (persistent & transient) with low attribute requirements
- Stateless: not storing of personal data at any time
- Log data live on local nodes and are kept in accordance with local law
- Invitation based Self-service registration for RPs
- All eduGAIN IdPs are allowed by default

# OpenID Connect
# Supported RP claims

| Claims | Description |
|---|---|
| **Affiliation Claims** | Based on [1], [2] |
| student | A student at the institution |
| faculty+staff | Institutional workers whose primary role is teaching or research and workers other than teachers or researchers |
| affiliated | This person is affiliated to the institution (Student, Faculty or Staff) |
| alum | An alumus at the institution |
| | |
| **Identifier Claims** | (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

# OpenID Connect
# Supported claims -2

| Claims | |
|---|---|
| **Other Claims** | |
| country | What is the country of the users home institution? |
| domain | What is the domain name of the institution of the user? |

Examples:
scope=affiliated
scope=affiliated persistent
scope=affiliated persistent country
scope=student persistent country
scope=student persistent country domain

# SAML SP Attribute requirements
# None persistence profile

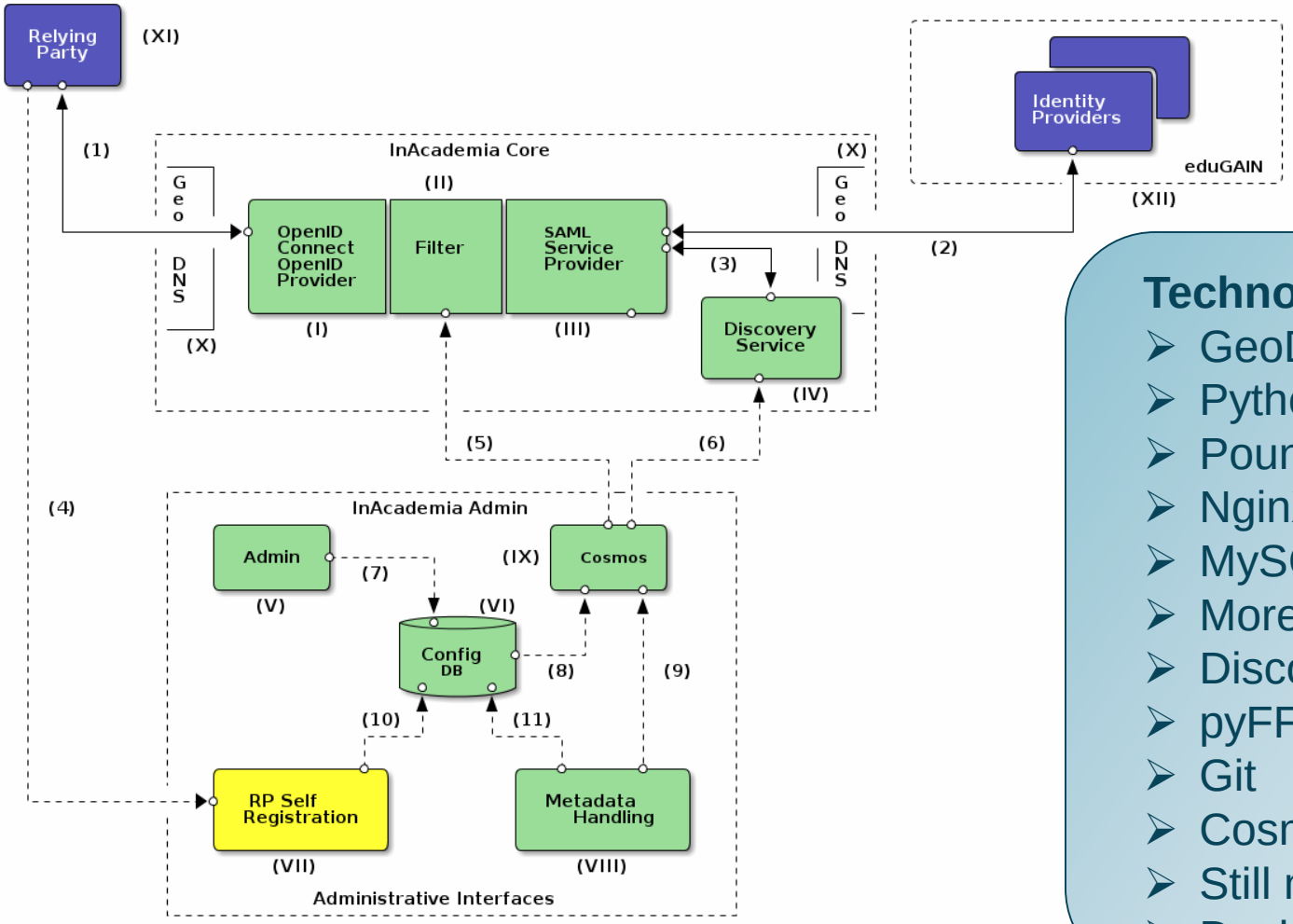
| Attribute | Description | Status |
|---|---|---|
| **transient** SAML nameID | We request a transient NameID<br>None transient NameIDs will be ignored | Required |
| eduPersonAffiliation<br>urn:oid:1.3.6.1.4.1.5923.1.1.1.1 | The home institution affiliation.<br><br>Supported values: Student, Staff, Employee, Faculty, Alum<br>Other affiliations are ignored | Required |
| schacHomeOrganization<br>urn:oid:1.3.6.1.4.1.25178.1.2.9 | RFC-1035 domain | Optional |

# SAML SP Attribute requirements
# Persistent profile

| Attribute | Description | Status |
|---|---|---|
| **persistent** SAML NameID | We prefer a **persistent** NameID | Optional* |
| eduPersonTargetedID<br>urn:oid:1.3.6.1.4.1.5923.1.1.1.10 | An eduPersonTargetedID may be used if a persistent NameID is not available | Optional* |
| eduPersonPrincipleName<br>urn:oid:1.3.6.1.4.1.5923.1.1.1.6 | An eduPersonPrincipleName may be used if all fails | Optional* |
| eduPersonAffiliation<br>urn:oid:1.3.6.1.4.1.5923.1.1.1.1 | The home institution affiliation<br>Supported values: Student, Staff, Employee, Faculty, Alum<br>Other affiliations are ignored | Required |
| schacHomeOrganization<br>urn:oid:1.3.6.1.4.1.25178.1.2.9 | RFC-1035 domain | Optional |

* Although optional, one of these ***must*** be provided.

# Technical Setup




**Technology:**

- GeoDNS
- Python
- Pound
- NginX
- MySQL
- More python
- DiscoJuice
- pyFF
- Git
- Cosmos+Puppet
- Still more python
- Docker