InAcademia

Simple Validation Service

Niels van Dijk

InAcademia lead

niels.vandijk@surfnet.nl

Mark Bevers

InAcademia business development

Mark.bevers@surfmarket.nl

eduGAIN Town Hall

Feb 21, 2017 – Vienna

InAcademia - *a Simple validation Service*

InAcademia radically simplifies affiliation validation for services, in a privacy preserving way, while at the same time leveraging existing eduGAIN infrastructure for Institutions

Microsoft wants to offer free Office365 to all students in EU

ORCID seeks to improve account quality

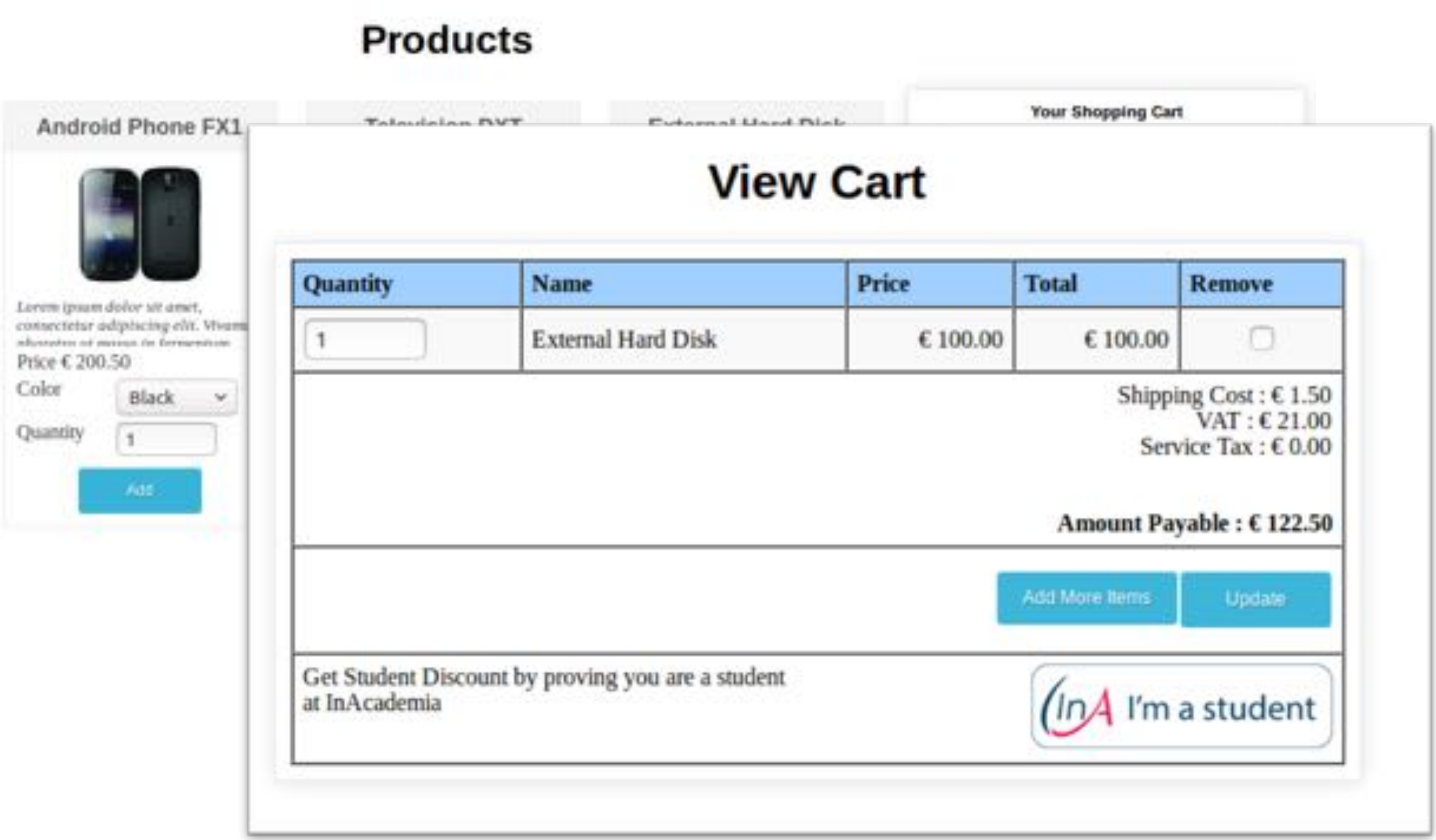
SMEs (webshops) want low barriers for leveraging digital academic Identity: a simple contract, a predictable cost model and high assurance on identity

InAcademia – *affiliation validation made easy*

How to make affiliation validation much 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 (yes or no)
- A user 'proves' affiliation by **authentication** with home IdP
- Validation service accessible for all **eduGAIN IdPs**
- A **simple protocol** is used by the Services (OpenID Connect)
- The **policy barrier** for using should be **low** (a single contract)
- Service pays a **small transaction fee** (pay per use)
- Academic services get 100% discount

InAcademia – demo: *Select a product*



Products

Android Phone FX1

Television DXT

External Hard Disk

Your Shopping Cart

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivam

Price € 200.50

Color: Black

Quantity: 1

View Cart

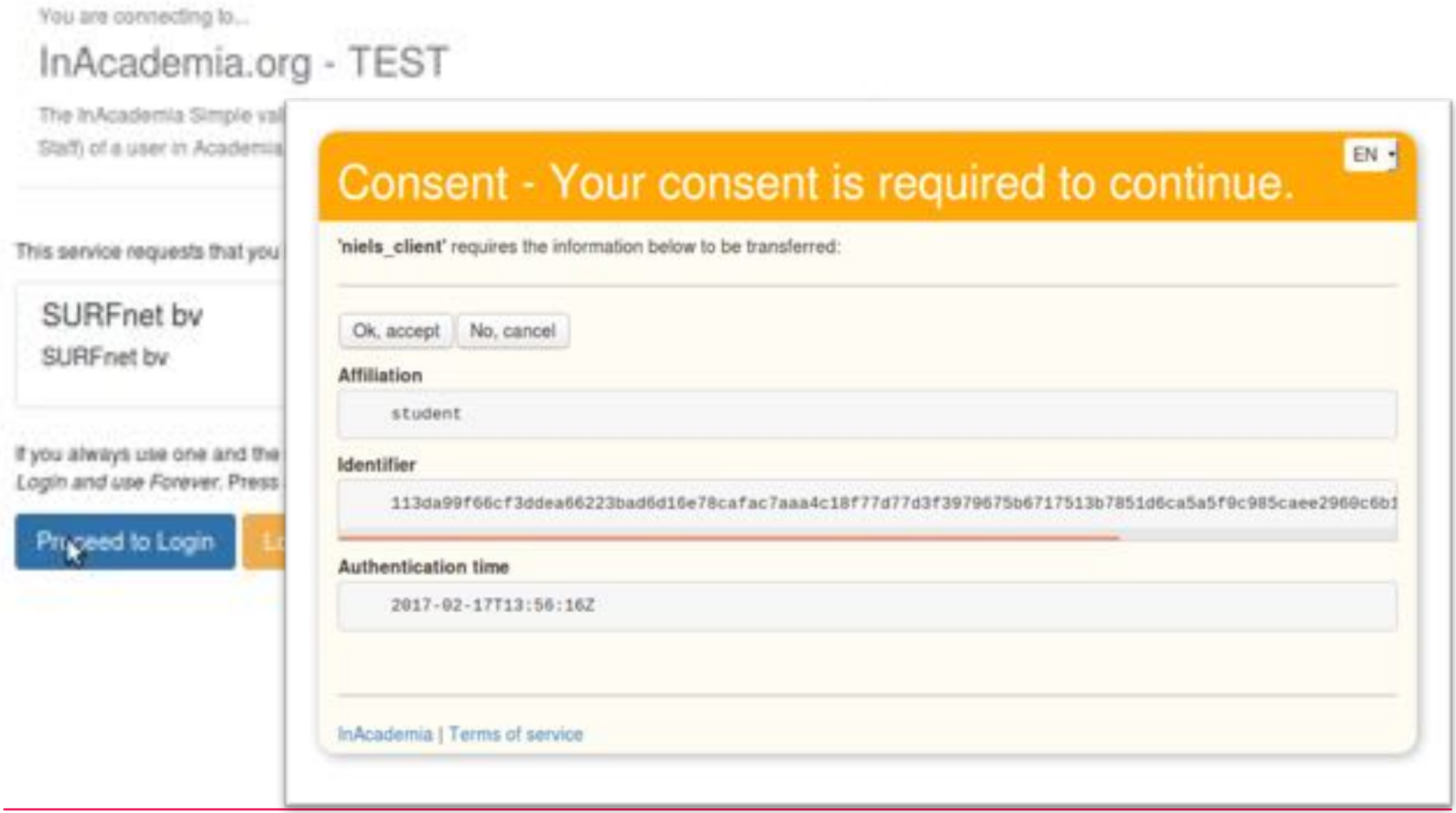
Quantity	Name	Price	Total	Remove
1	External Hard Disk	€ 100.00	€ 100.00	□

Shipping Cost : € 1.50
VAT : € 21.00
Service Tax : € 0.00

Amount Payable : € 122.50

Get Student Discount by proving you are a student at InAcademia

InAcademia – *demo: Prove affiliation*



You are connecting to...

InAcademia.org - TEST

The InAcademia Simple val

Staff) of a user in Academia

This service requests that you

SURFnet bv

SURFnet bv

If you always use one and the

Login and use Forever. Press

Consent - Your consent is required to continue.

'niels_client' requires the information below to be transferred:

Affiliation

student

Identifier

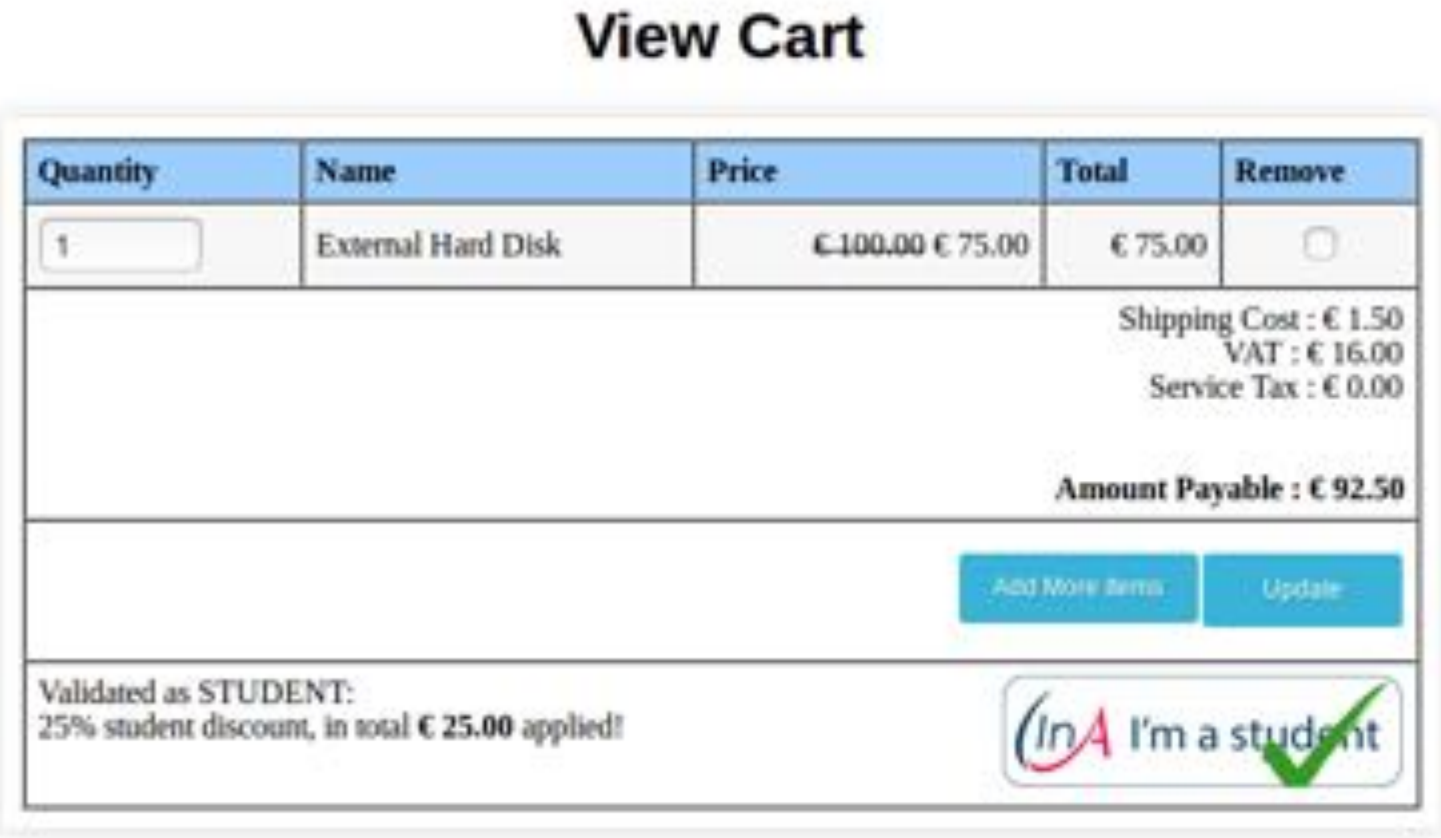
113da99f66cf3ddea66223bad6d16e78cafac7aaa4c18f77d77d3f3979675b6717513b7851d6ca5a5f9c985caee2960c6b1

Authentication time

2017-02-17T13:56:16Z

InAcademia | Terms of service

InAcademia – *demo: validated!*



View Cart

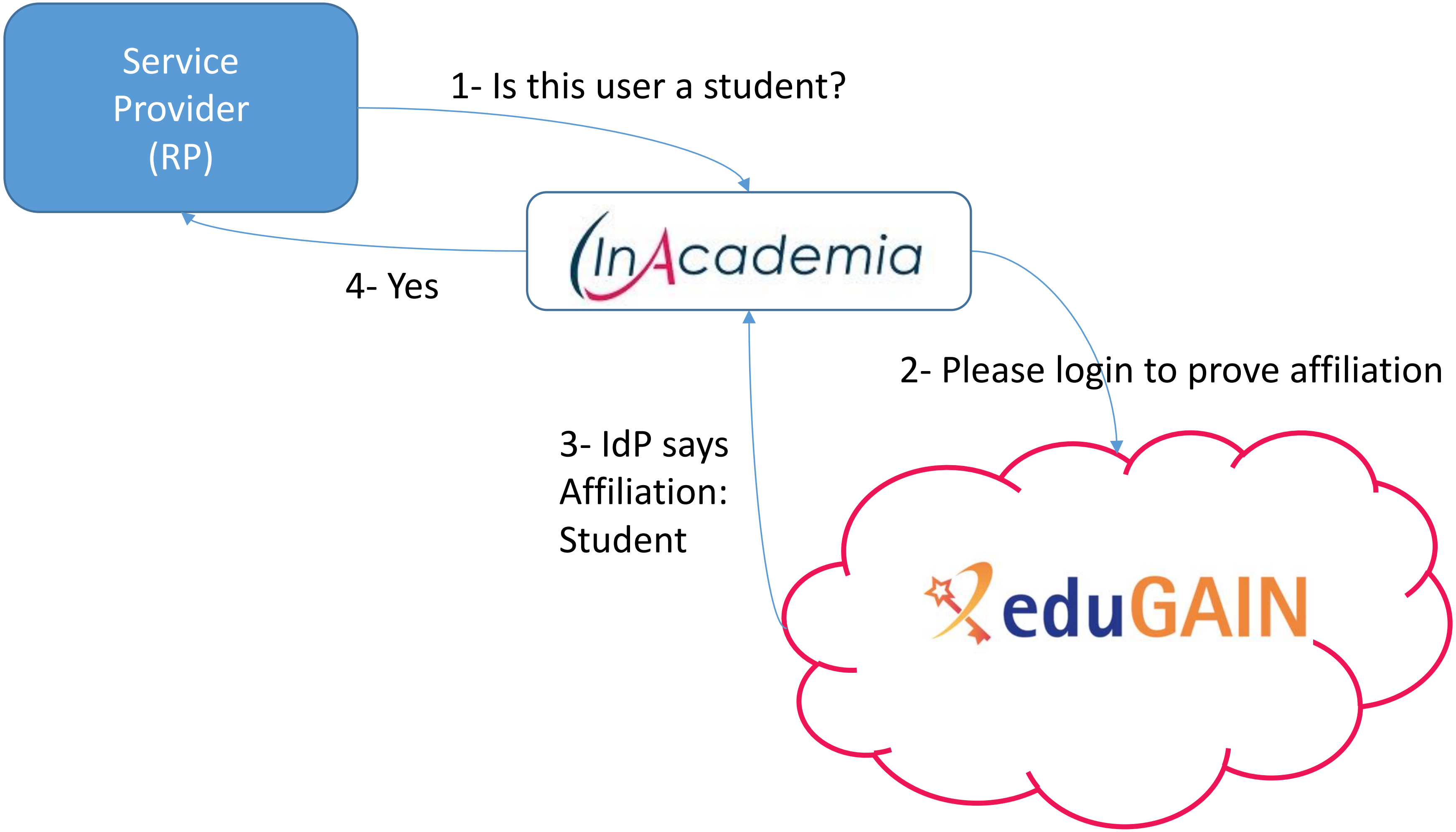
Quantity	Name	Price	Total	Remove
1	External Hard Disk	~~€ 100.00~~ € 75.00	€ 75.00	□

Shipping Cost : € 1.50
VAT : € 16.00
Service Tax : € 0.00

Amount Payable : € 92.50

Validated as STUDENT:
25% student discount, in total **€ 25.00** applied!

InAcademia – *Flow overview*



Service Provider (RP)

1- Is this user a student?

2- Please login to prove affiliation

3- IdP says Affiliation: Student

4- Yes

Services perspective

InAcademia	eduGAIN
Very easy to implement	Implement SAML SP
Common integration pattern (Google/Facebook)	SAML (federation) has learning curve
“Setup and forget”	Metadata; ARP; opt-in/opt-out
Same Terms and Conditions for all academic users in EU	Per federation differences in policy
No contracts or dealings with Institutions	Interaction w/ institutions needed
No user data; persistent identifier, country and institution domain name optional	Rich attribute set possible
No integration across services (atomic)	Good integration across services (SSO)
Small transaction fee per transaction	Free; technical knowhow is needed

Institutional perspective

InAcademia	eduGAIN
SAML SP proxy in eduGAIN	SAML SP in eduGAIN
Effort and cost free access to ‘bonus’ services for your end users	Core campus and scientific services
SAML NameID + (scoped) affiliation	Rich attribute set possible
Highly privacy preserving	Depends on attributes sent
Institution hidden behind InAcademia	Direct transaction between SP and IdP
SP and end user support covered	Support via internal IT or fed ops
CoCo complient	Per SP policy and contracts
Service sustained by fees	Institition pays for sustaining
Usage free for end users	Usage free for end users

Federation perspective

InAcademia	eduGAIN
Gateway to many services	Gateway to entities abroad
Uses existing SAML IdPs	Uses existing SAML IdP
SAML NameID + (scoped) affiliation	Rich attribute set possible
Highly privacy preserving	Depends on attributes send
SP and end user support covered	Support & coordination via fed ops (towards other fed ops & internal IT)
Infrastructure provided by GEANT	Local Infrastructure required
Usage Free	Usage Free
Zero effort tool for long tail services	Core campus and scientific services

When to suggest InAcademia over regular eduGAIN?

- When the service has no needs beyond affiliation validation
- When a service has low transaction volume
  or When a service has world domination aspirations
- When service owner is not technically adapt
- When you have no ability or willingness to provide support
- When you want user privacy guaranteed
- To reduce the amount of work required when dealing with the services
- When you feel the R&E community as a whole can get a better deal than a single institution/federation/country
- Aspirational note: InAcademia fees may help sustain other eduGAIN services also

If you are an Academic peer, e.g. a research service

- You may use InAcademia for free (best effort/ fair use)
- No user data = no data protection troubles
- Validation backed by institutional IdM
- Very easy to implement (see https://github.com/InAcademia)

Ready for Playing & Pilots

Play

- If you want to test or play, please let us know
  Have a look at https://inacademia.org/getting-started
  or try the demo shop at https://demoshop.inacademia.org/shop
- We welcome your input and feedback!

Pilots

- Ready to talk to services, with your endorsment, for pilotting InAcademia
- Currently in discussion with Amazon, Google, SheerID, Mecenat, Parantion
- For now, GEANT project partners only
- No fees charged for pilot period

We want to work with identity federations to find the best fit for InAcademia

https://inacademia.org

Technical: https://github.com/InAcademia

info@inacademia.org

Thank you

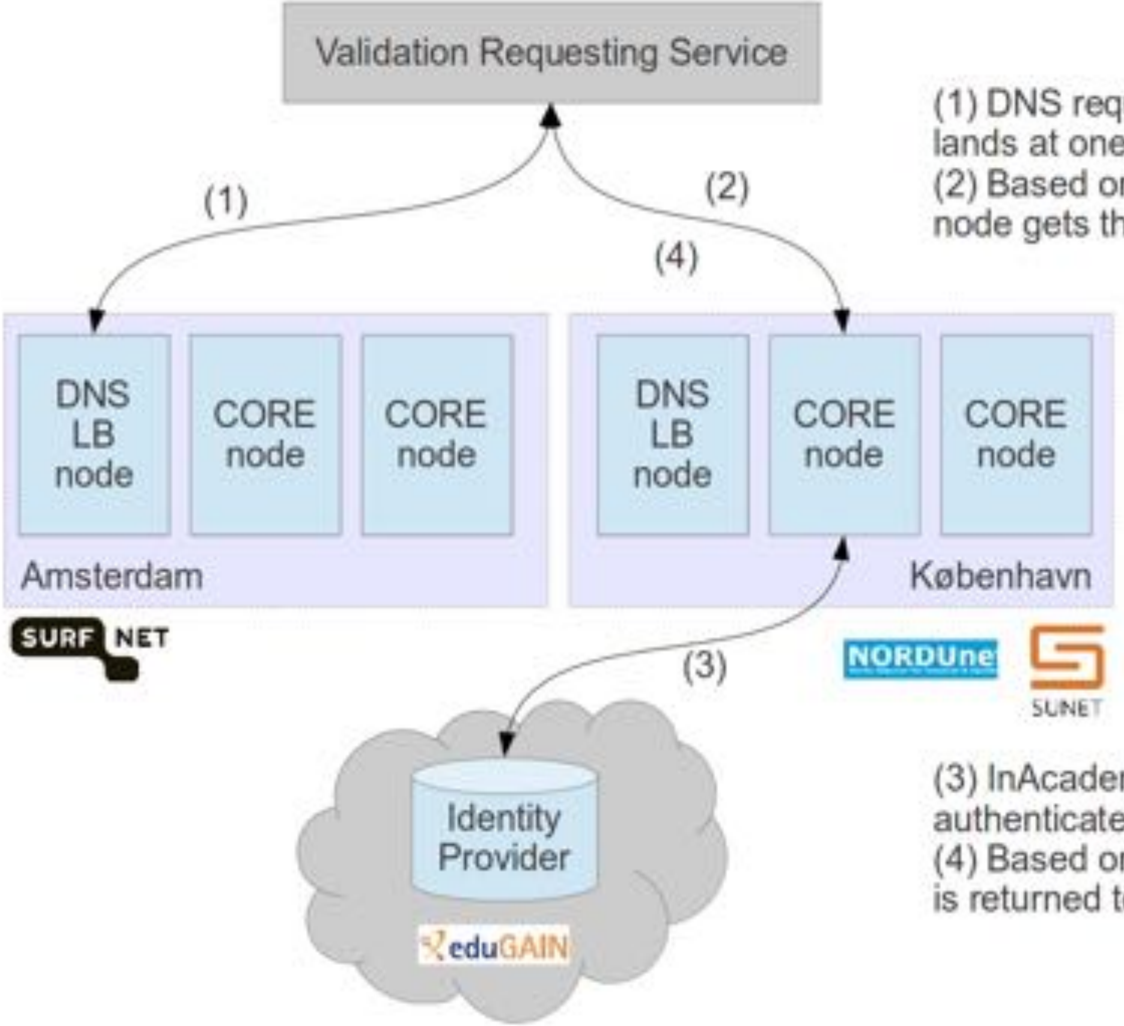
GÉANT

Networks · Services · People

www.geant.org

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

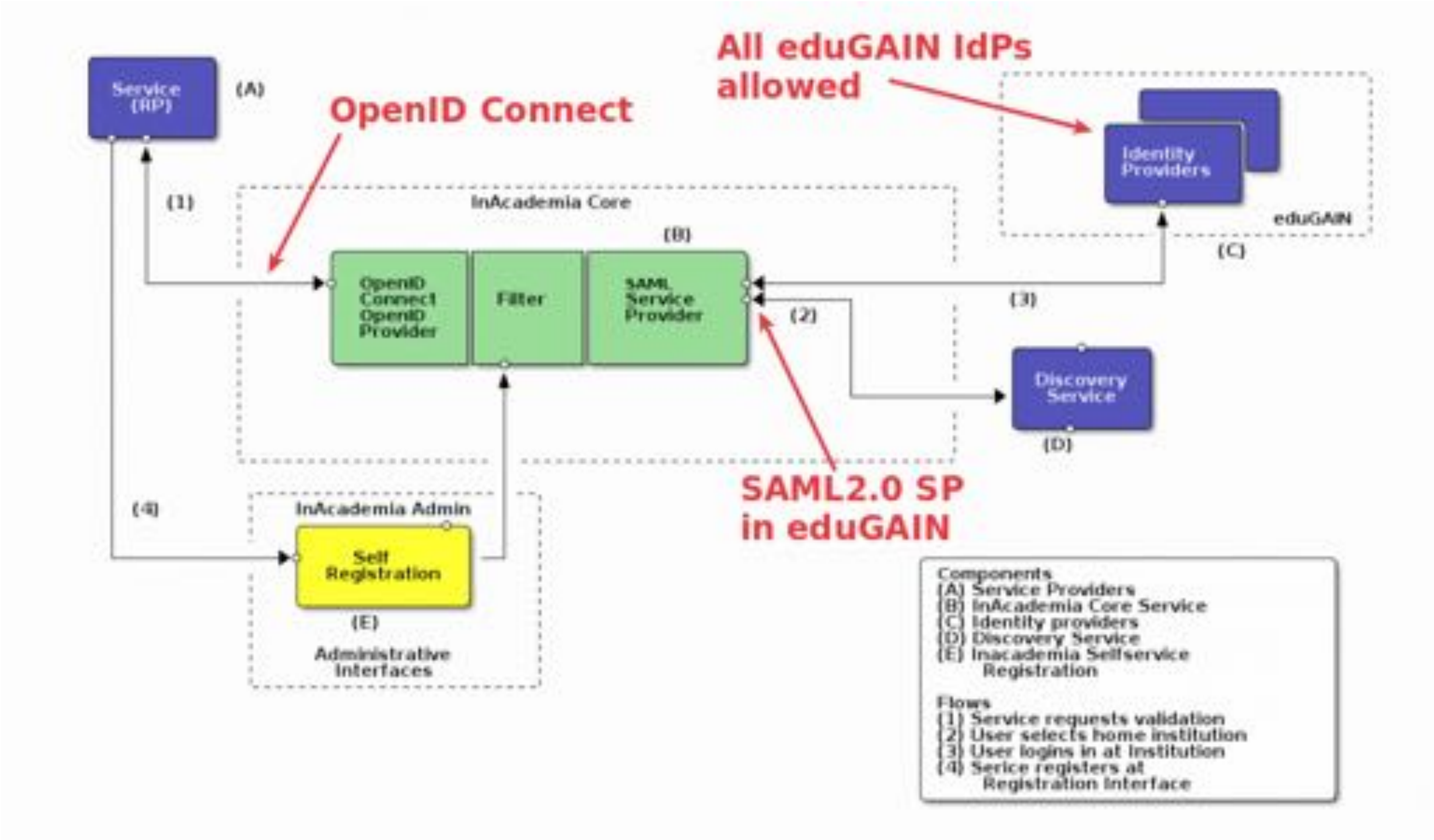
InAcademia – *Technical setup*



(1) DNS request for InAcademia.org lands at one of the DNS nodes
(2) Based on the response a core node gets the transaction

(3) InAcademia.org lets user authenticate at eduGAIN IdP
(4) Based on affiliation a response is returned to the requesting service

InAcademia – *Component overview*



OpenID Connect

All eduGAIN IdPs allowed

SAML2.0 SP in eduGAIN

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
employee	Institutional workers whose primary role is teaching or research and workers other than teachers or researchers
student	A student at the institution
faculty	Institutional workers whose primary role is teaching or research
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