

Community Tagging

Sprint Demo – June 25, 2019

Uros Stevanovic et al.

Community tagging team

TRUST & IDENTITY
INCUBATOR



Community Tagging - “Pixie Dust” - Usecase

- Research communities have a need to express and potentially share certain trust marks on IdPs and SPs. These trust marks may differ from existing trust marks issued by identity federations, or may be put in to compliment existing ones, in case the federation operator does not support these, like e.g. in the case of SIRTFI.
- This activity tries to implement a technical solution that matches the requirements as described by the SIRTFI community and investigates usability of the solution for research communities and the impact of the solution of Identity federations. It also explores potential other scenarios where a similar methodology could be used, like e.g. REFEDs MFA and in the context of the IdP self assessment tool that was developed in GN42
- It does not consider itself with the questions on where and how such a tool would be used in the context of existing trust frameworks.





Activity goals

- Create technical implementation based on SIRTFI+ Registry document
 - Distil technical requirements from SIRTFI+ Registry document;
 - Create/Describe technical design;
 - Buy or build (or modify existing);
 - Improve through sprint iterations;
 - Interact with SIRTFI working group to improve features if needed.
- Learn and discuss flows and usability in 'real world' (Collaborate with LIGO)
- Deploy working setup so it can be tested with stakeholders
- Explore and describe (& implement) authZ architecture in collaboration w/ SIRTFI working group
- Bonus: Explore other usecases

- Web portal
 - Federated login (including admin)
- Self assertion of the tag, by “invitation” only
- Flow resembling: <https://access-check.edugain.org/>
- History of taken actions/steps
- Identified issues:
 - “Official” Sirtfi support (i.e. which federations support it)
 - Signing key (storage, usage, etc.)
- https://docs.google.com/document/d/1Hwdi7iO3v2U-RrzgT_EhL7AA0xkE9Rlr_bQac2IhZ3M/edit?pli=1#
- <https://wiki.geant.org/pages/viewpage.action?pageId=120500327>

- Existing tools evaluated:
 - OpenConnex – applicable, deemed overly “unflexible”
 - Jagger – deemed applicable and acceptable
 - Access Check Tool – assessed, selected for the registration flow
- Preliminary technical solution established:
 - Access Check + Jagger
 - Access Check for the registration/invitation step
 - Jagger for the “dusting” step

- User (entity owner) access Access Check Tool (ACT)
- Selects its entity
- Tool shows the mail necessary for dusting (technical contact email)
- Invitation is sent to the selected email (containing one time token pass) and user is prompted to enter a correct token value

eduGAIN Access Check

1. Select your service provider

2. Select your email address

3. Complete email challenge

Select your service provider

Please select the service provider you want to test in one of the lists below. You must be an administrator of that service to continue afterwards.

All service providers

- <http://acesnoto.deboecksuperieur.com> (De Boeck Supérieur License Desk)
- <http://adfs.untsystem.edu/adfs/services/trust> (UNT System ADFS Service Provider)
- <http://adfs.yz.yamagata-u.ac.jp/adfs/services/trust> (SharePoint Foundation Service)
- <http://bond-wstest.imodules.com/sp> (iModules Bond University test site)
- <http://canvas.sbccc.edu/saml2> (Santa Barbara City College - Canvas)
- <http://cloudmore.com/shibboleth> (Cloudmore)
- <http://cwpub2.imodules.com/sp> (Current Work Test)
- <http://dev-us.cloudmore.com/shibboleth> (Cloudmore)
- <http://dev.cloudmore.com/shibboleth> (Cloudmore)
- <http://fse.eduuni.fi/adfs/services/trust> (Eduuni)
- <http://harvard-test.imodules.com/sp> (Harvard Chan (TEST))
- <http://harvard.imodules.com/sp> (Harvard Chan (PROD))
- <http://hotfixpub1.imodules.com/sp> (iModules Hotfix Test)
- <http://ic.imodules.com/sp> (Ithaca College)
- <http://ic.test-imodules.com/sp> (Ithaca Test)
- <http://imodarugula.imodules.com/sp> (iModules Preload: Arugula)
- <http://imodrhubarb.imodules.com/sp> (iModules Preload: rhubarb)
- <http://lawgwu.imodules.com/sp> (GWU Law)



As part of the GÉANT 2020 Framework Partnership

eduGAIN Access Check

1. Select your service provider

2. Select your email address

3. Complete email challenge

Select your email address

Before you can create test accounts at this Identity Provider, we need to ensure you are a legitimate administrator of the Service Provider <https://inacademia.org/metadata/inacademia-simple-validation.xml>.

Select the email address where an email challenge can be sent to validate your identity:

- admin@inacademia.org
- support@inacademia.org
- tech@inacademia.org

Those email addresses have been extracted from your service metadata.

Previous

Next



eduGAIN Access Check1.2.0 - [contact us](#)
As part of the GÉANT 2020 Framework Partnership Agreement (FPA), this project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2). [Disclaimer](#) [Policies](#)

eduGAIN Access Check

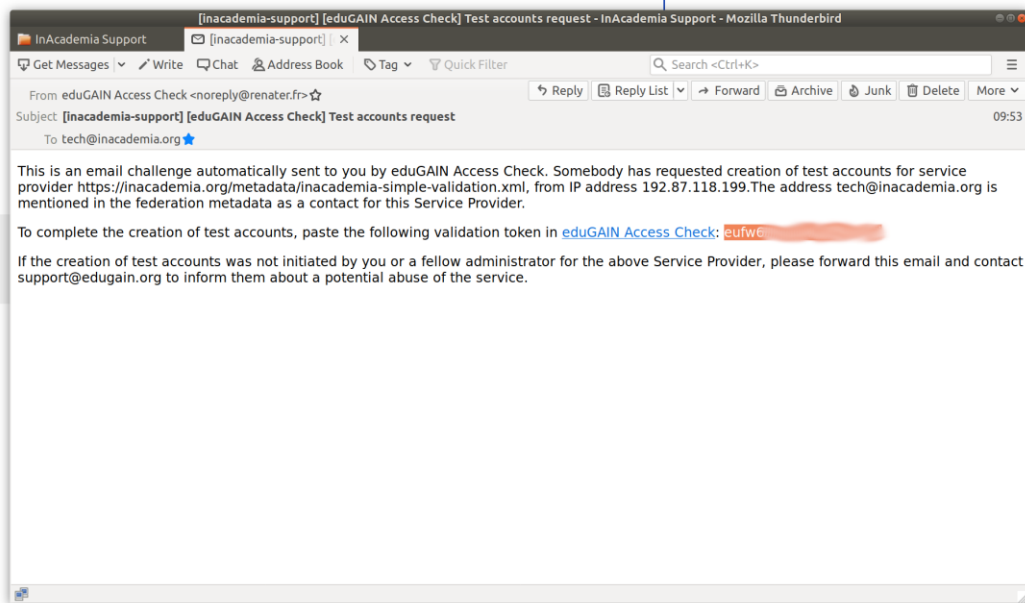
1. Select your service provider
2. Select your email address
3. Complete email challenge

Complete email challenge

An email challenge including a validation token has been emailed to you at tech@inacademia.org. Please copy and paste the validation token in the form below to prove that you are administrator of this service.
Please provide the validation token here:

eufw6tk0ouw4uedwyeti

Previous Next



Disclaimer Policies

Horizon 2020 research and innovation

eduGAIN Access Check

Success: your identity as administrator of the Service Provider <https://inacademia.org/metadata/inacademia-simple-validation.xml> has been validated!

Test accounts created

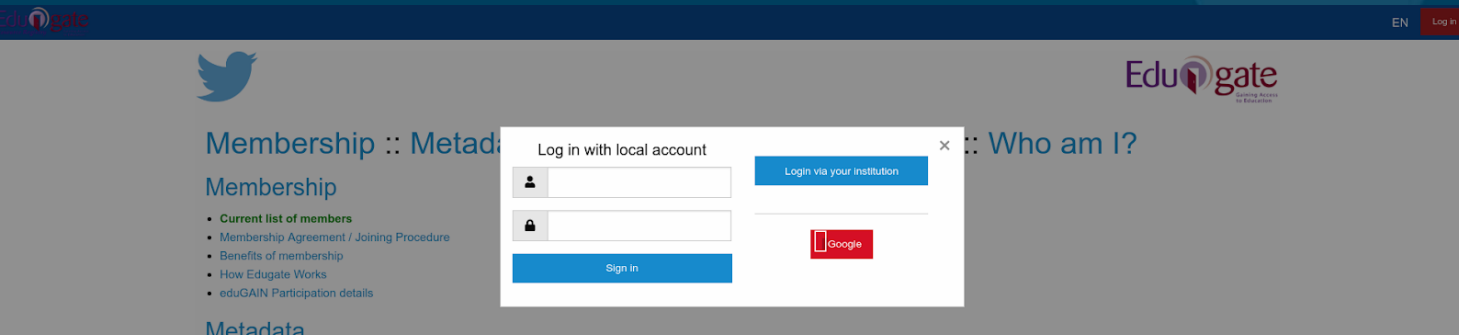
You can now use these test accounts to access your [service provider](#), using **eduGAIN Access Check** as identity provider.

This page won't be accessible again, you should either keep it open in your web browser, or [download accounts in CSV format](#).

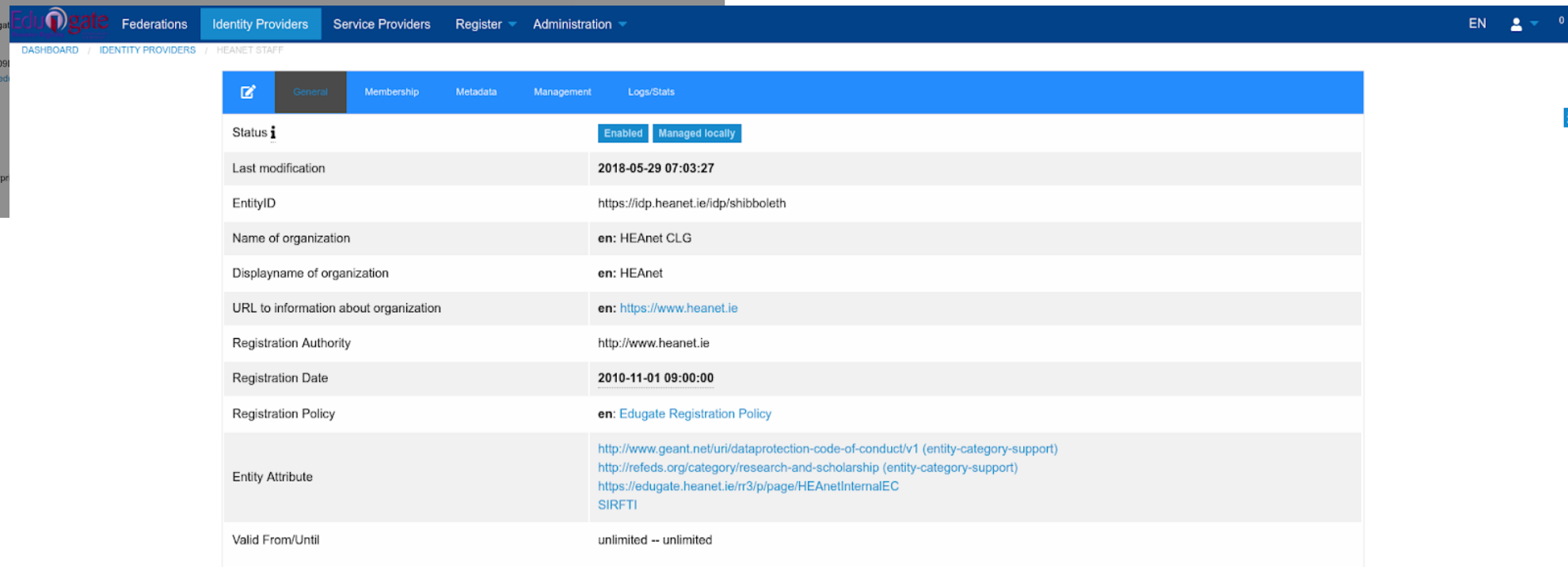
Account profile: fullset1	Account profile: limitedset1	Account profile: generic1
user name: [REDACTED]	user name: [REDACTED]	user name: [REDACTED]
password: [REDACTED]	password: [REDACTED]	password: [REDACTED]

- After successful use of Access Check tool, it is “proven” that the user controls the entity. This information is transferred to Jagger.
- Jagger prompts the user with the possibility to “dust” the entity with (hardcoded) Sirtfi value (potentially checkbox)
- Entity is dusted and new metadata is generated

Jagger flow



(images taken from <http://jagger.heanet.ie/>)



The screenshot shows the 'Identity Providers' management page in the EduGate system. The breadcrumb trail is 'DASHBOARD / IDENTITY PROVIDERS / HEANET STAFF'. The page has tabs for 'General', 'Membership', 'Metadata', 'Management', and 'Logs/Stats'. The 'General' tab is active, showing the following details:

Status	Enabled Managed locally
Last modification	2018-05-29 07:03:27
EntityID	https://idp.heanet.ie/idp/shibboleth
Name of organization	en: HEAnet CLG
Displayname of organization	en: HEAnet
URL to information about organization	en: https://www.heanet.ie
Registration Authority	http://www.heanet.ie
Registration Date	2010-11-01 09:00:00
Registration Policy	en: Edugate Registration Policy
Entity Attribute	http://www.geant.net/uri/dataprotection-code-of-conduct/v1 (entity-category-support) http://refeds.org/category/research-and-scholarship (entity-category-support) https://edugate.heanet.ie/r3/p/page/HEAnetInternalEC SIRFTI
Valid From/Until	unlimited -- unlimited