НРЕН УКРАЇНИ
АСОЦІАЦІЯ УРАН

eduGAIN – ваш ключ до міжнародних науково-освітніх сервісів

Вебінар від Асоціації УРАН

26 травня 2021 року

Про що ви почуєте?

- НРЕН України Асоціація УРАН, участь у GÉANT і EaPConnect
- Що таке eduGAIN, його історія та еволюція, для чого він потрібний, які сервіси дозволяє отримувати
- Технологія eduGAIN
- Використання eduGAIN в УРАН
- Умови надання сервісу
- Відповіді на запитання

НРЕН України Асоціація УРАН

NREN – National Research and Education Network
Національна науково-освітня телекомунікаційна мережа

НРЕН - спеціалізований інтернет-провайдер, створений для забезпечення потреб науково-освітньої спільноти країни в інформаційно-комп'ютерних технологіях.

НРЕН України - Асоціація УРАН: неприбуткова організація, засновниками є ВНЗ України IV-го рівня акредитації, установи НАН та Академія педагогічних наук України

www.uran.ua
www.panorama.uran.ua

Асоціація УРАН

- Доступ до високошвидкісних каналів пан'європейської мережі для науки і освіти GÉANT
- Цифрові послуги (власної розробки і розробки GÉANT)

система видачі та використання електронних посвідчень ідентифікаційних даних (ІД)

- ✓ авторизація за допомогою технології єдиного входу (SSO)
- ✓ доступ до світових наукових ресурсів (в т. ч. Springer, Elsevier, Scopus та електронних сервісів для студентів)

Ukrainian Research and Academic Network

Співробітництво з GÉANT

Пан'європейська мережа, яка з'єднує НРЕН всієї Європи

- Частина ініціативи EU4Digital, фінансується ЄС .
- Координатор – GÉANT
- Мета - розвиток та інтеграція 6 країн Східного партнерства та їхніх науково-освітніх спільнот до Європейського дослідного простору

- Член GÉANT
- Учасник EaPConnect
- Надає науковцям і освітянам України цифрові послуги європейського стандарту, одна з них - eduGAIN

eduGAIN: загальні відомості

Девід Вагетті
розпорядник послуги eduGAIN
GARR, НРЕН Італії

Ukrainian Research and Academic Network

eduGAIN Service

Davide Vaghetti (GARR)

eduGAIN service owner

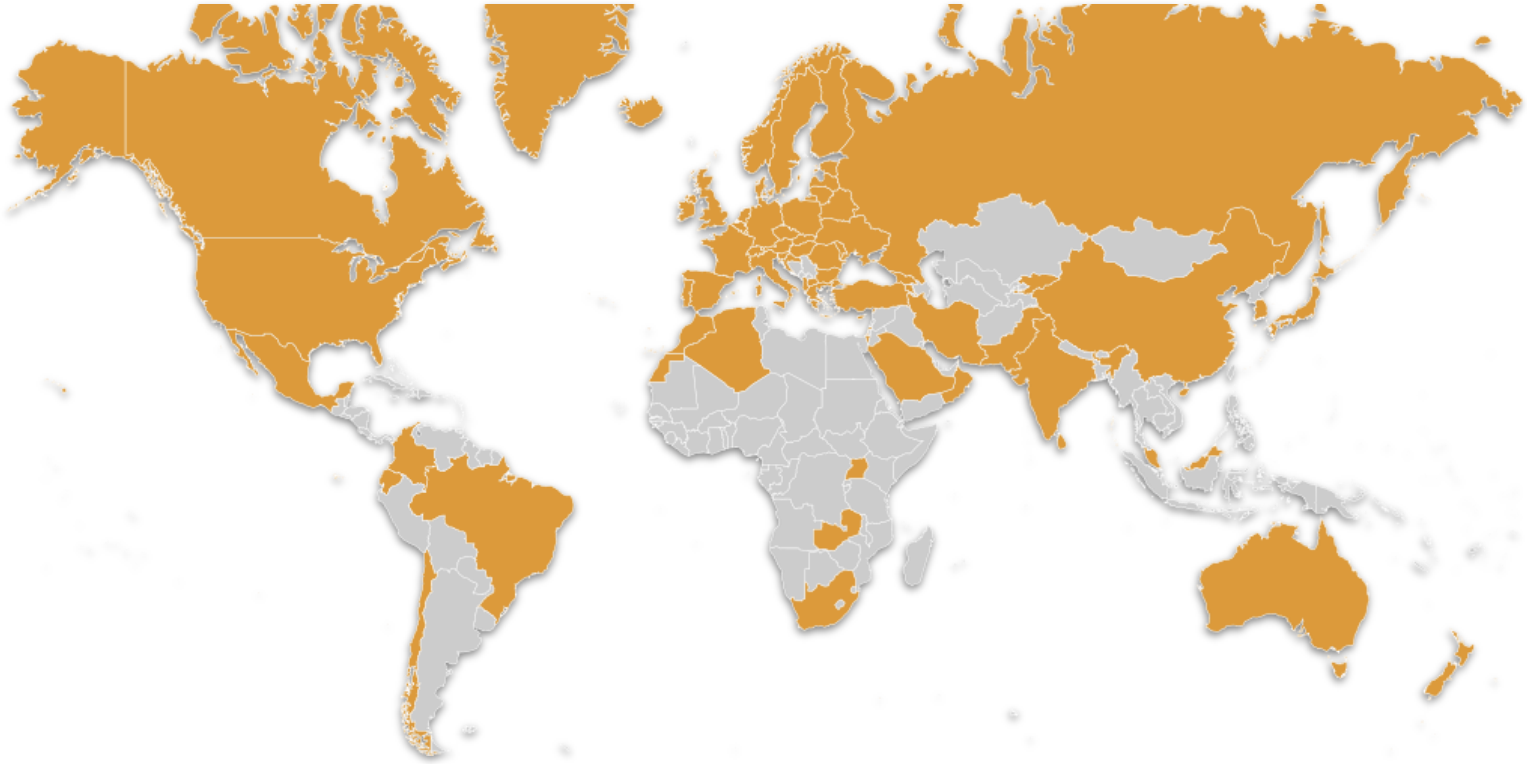
Agenda

- What is eduGAIN?
- How it started and growth?
- Federated access
- eduGAIN enabled services
- eduGAIN challenges & evolution

eduGAIN

Enabling access for the global research and education community

Federated identities enable users to access a wide range of services using their institutional account.



72 Identity Federations

4000+ Identity Providers

3000+ Service Providers

eduGAIN pilot - circa 2010

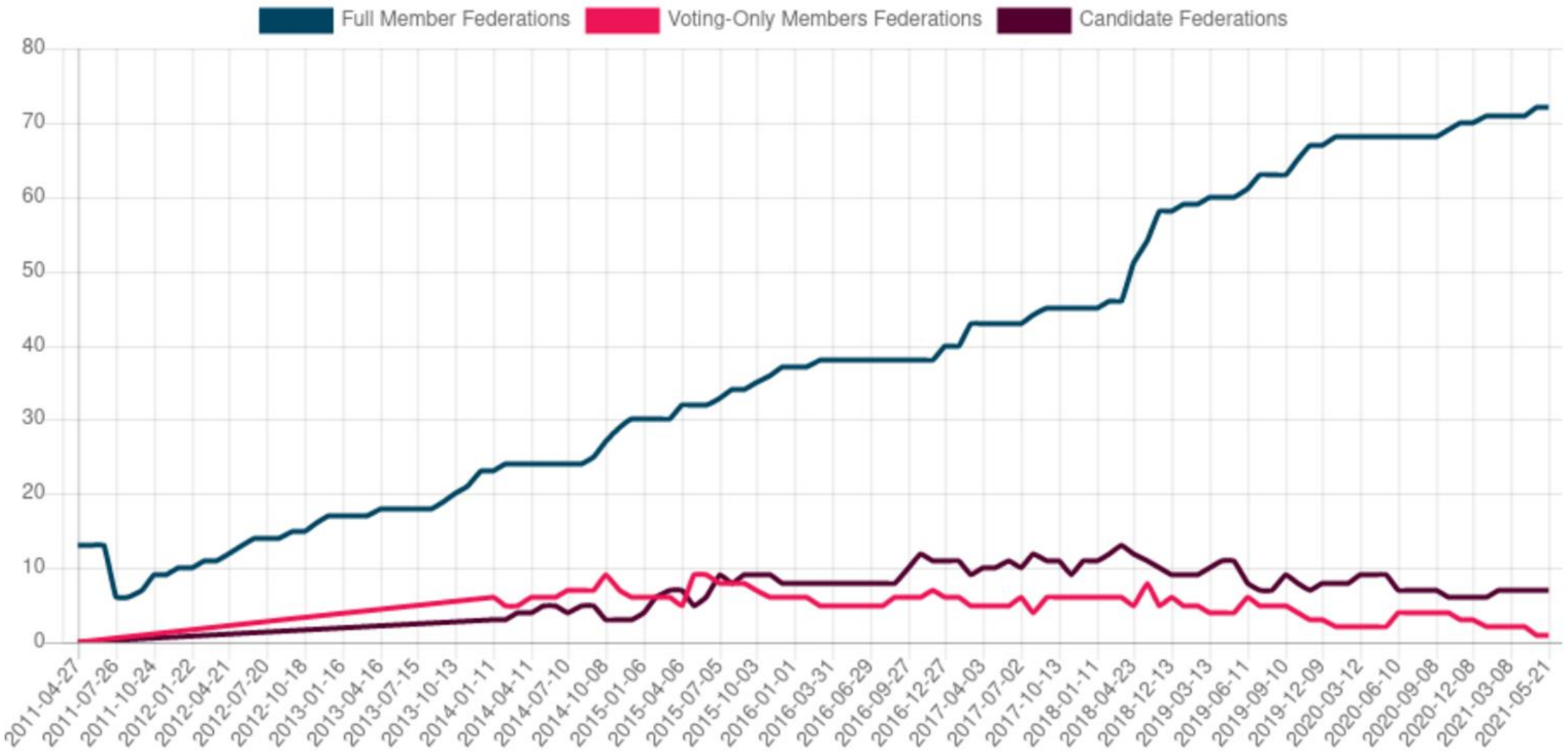
EduGAIN

eduGAIN

- Project by GÉANT
- Based on SAML
- It's not a Federation, it's a service to connect Federations
- www.edugain.org

- Pre-pilot phase:
  Croatia, Czech Republic, Finland, Germany, Poland and Switzerland

eduGAIN Growth



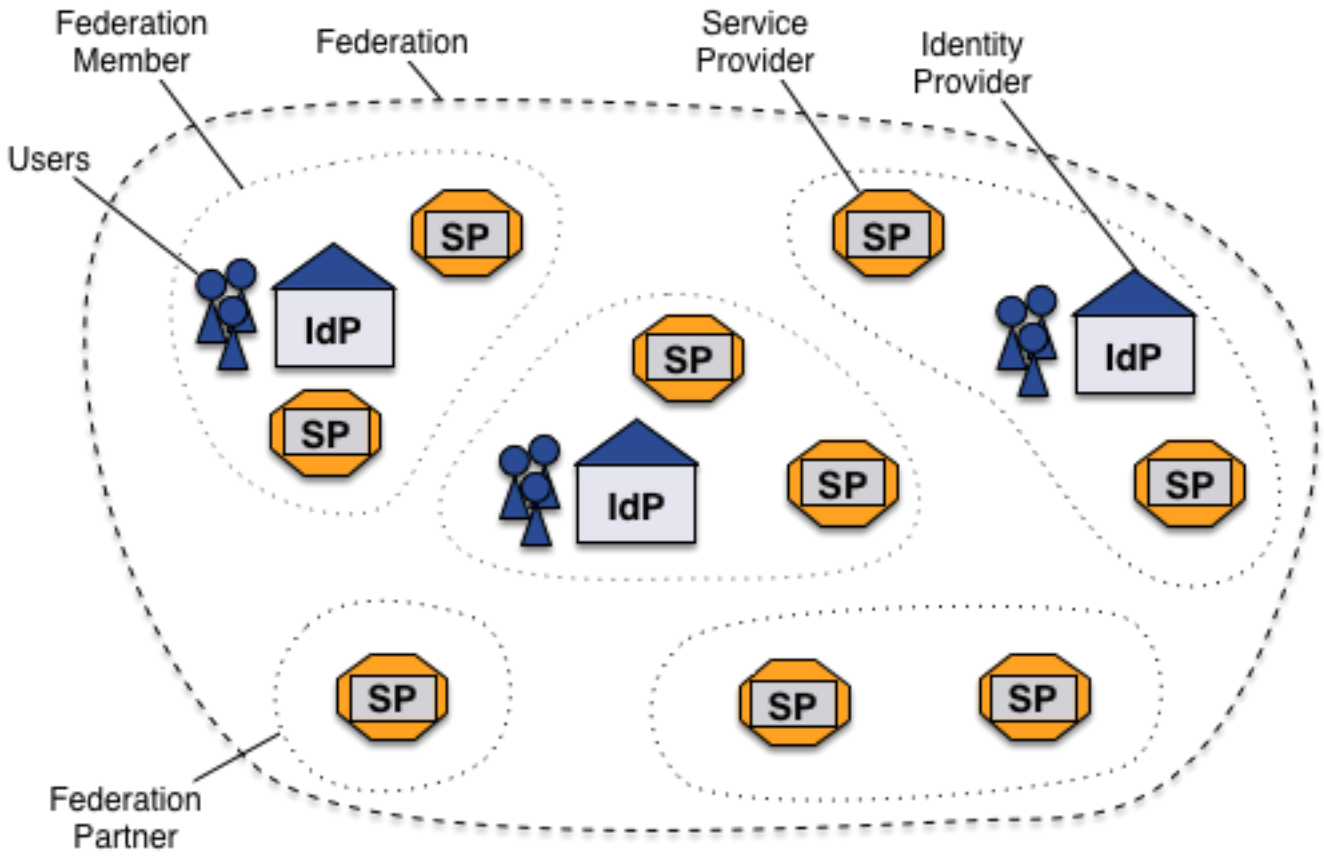
The eduGAIN many contributors

Identity Federation

An identity federation is a collection of organizations that agree to interoperate under a certain rule set.

This rule set typically consists of **legal frameworks**, **policies** and **technical profiles** and standards.

It provides the necessary **trust** and **security** to exchange home organizations' **identity** information to **access services** within the federation.



Identity Providers, Service Providers and Discovery Service

Identity Provider

The system component that authenticates a user (e.g. with username and passwords) and issues identity assertions on behalf of the user who wants to access a service protected by a Service Provider.

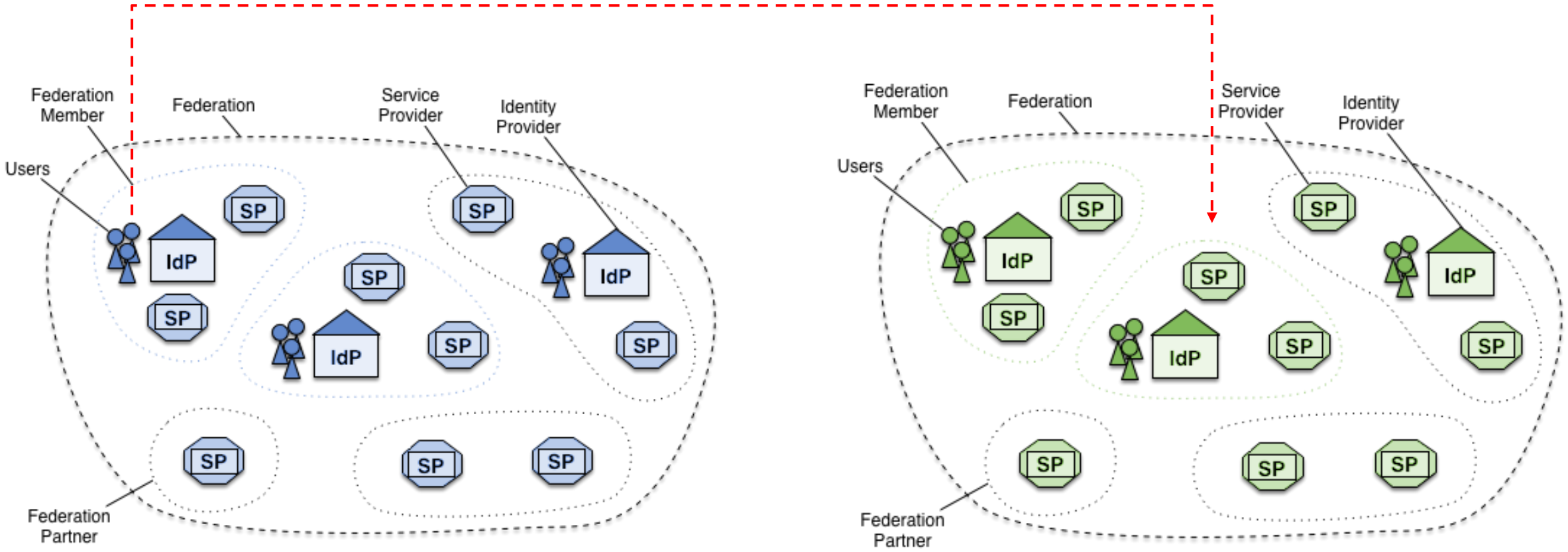
Service Provider

The system component that evaluates identity assertions from an Identity Provider and uses the information from the assertion for controlling access to protected services.

Discovery Service

The Discovery Service service, also known as "Where Are You From (WAYF)" service, lets the user choose his home institution from a list and then redirects the user to the login page of the selected institution for authentication.

Inter federation access



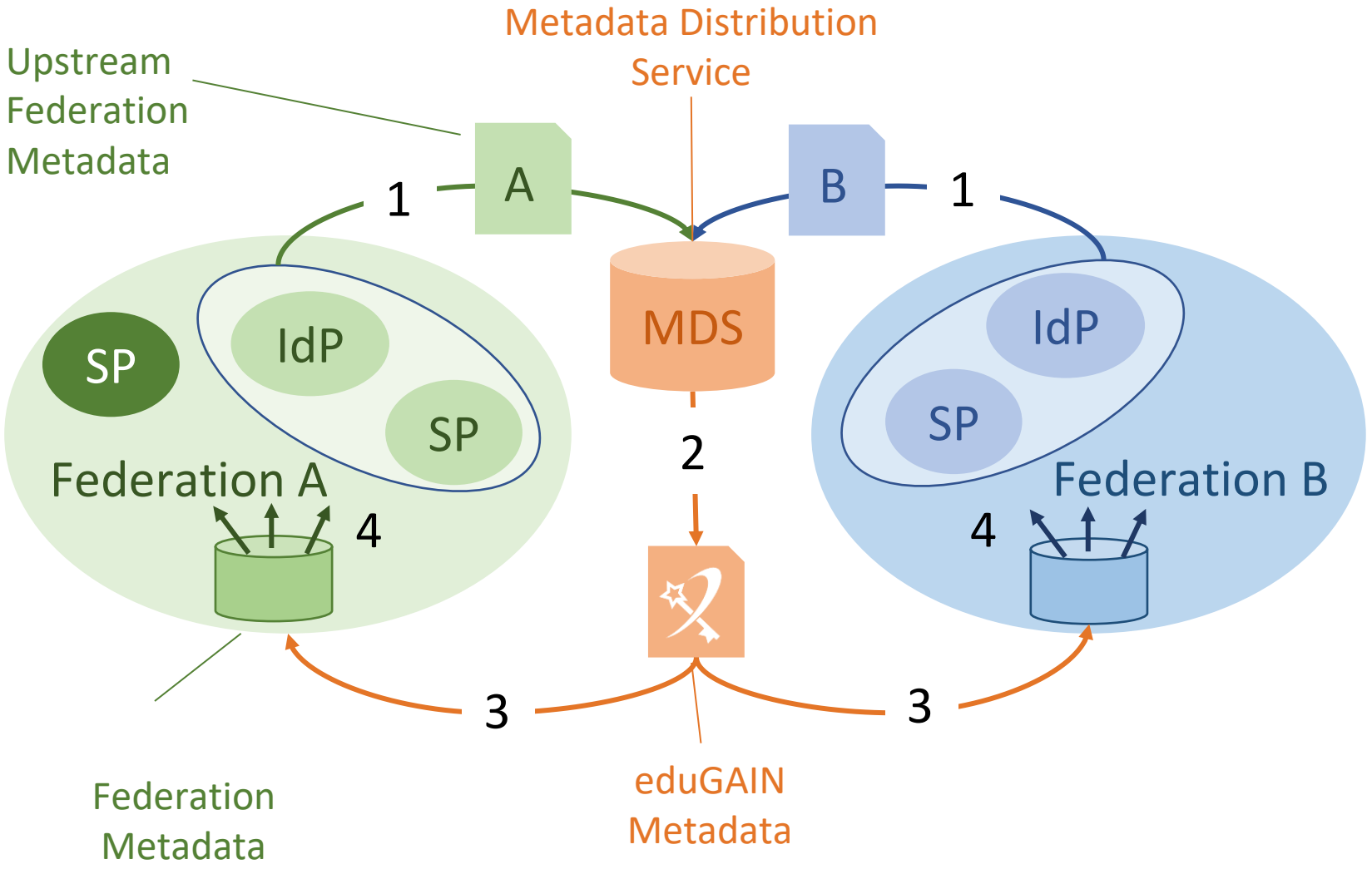
eduGAIN Metadata Distribution Service

1 - Federations' metadata upstream feed

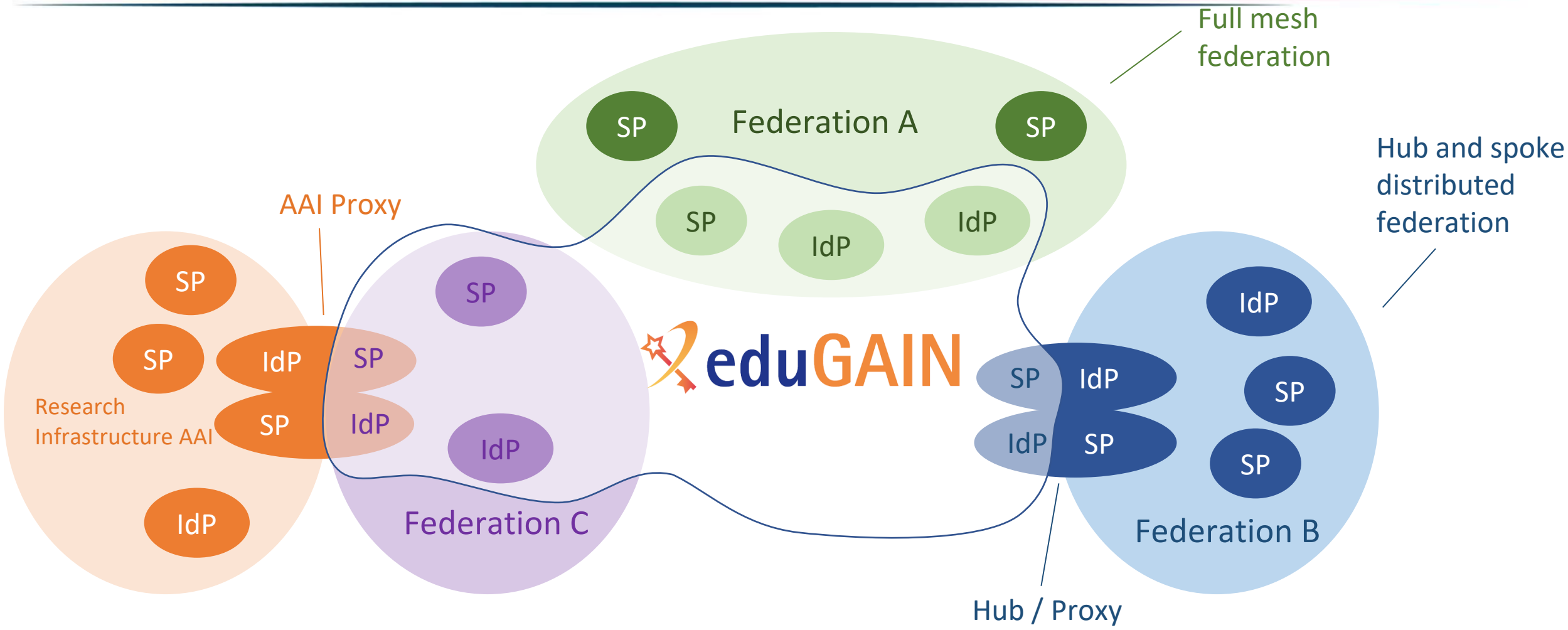
2 - eduGAIN metadata creation

3 - eduGAIN metadata signing and distribution

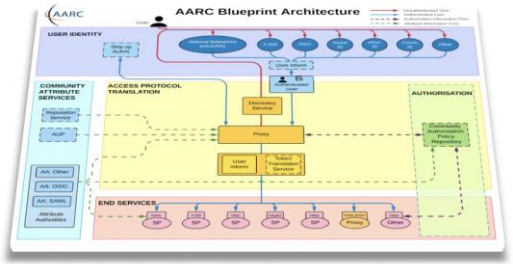
4 - Federations redistribute the eduGAIN metadata



A complex ecosystem



eduTEAMS

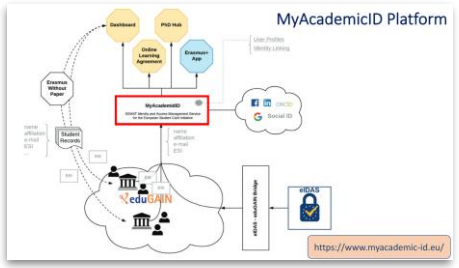


virtual teams and shared resources

InAcademia
ONLINE STUDENT VALIDATION

student validation service

MyAcademicID



student mobility Erasmus+ services

EBSCO · IEEE · Clariva Analytics · ELSEVIER · DE GRUYTER · OXFORD UNIVERSITY PRESS · SPRINGER NATURE · Wolters Kluwer

scientific publishers & academic journals

eduGAIN

haka · SWITCHaai · cafe · grnet · SWAMID · The UK Access Management Federation · COFRE Comunidad Federada REUNA · confia · arnes · GakuNin · TAAT · Carsi · RCTSaai · MiNGA · FEIDE · SURF CONEXT · Belnet R&E Federation · edu ID · SIFULAN · WAYF Where are you from · InCommon · aconet · DFN-AAI · RENATER · AUSTRALIAN ACCESS FEDERATION · idem garr aai · Tuakiri · Edugate · Colfire · AFIRE · SIR · @EduHr · edu ID cz

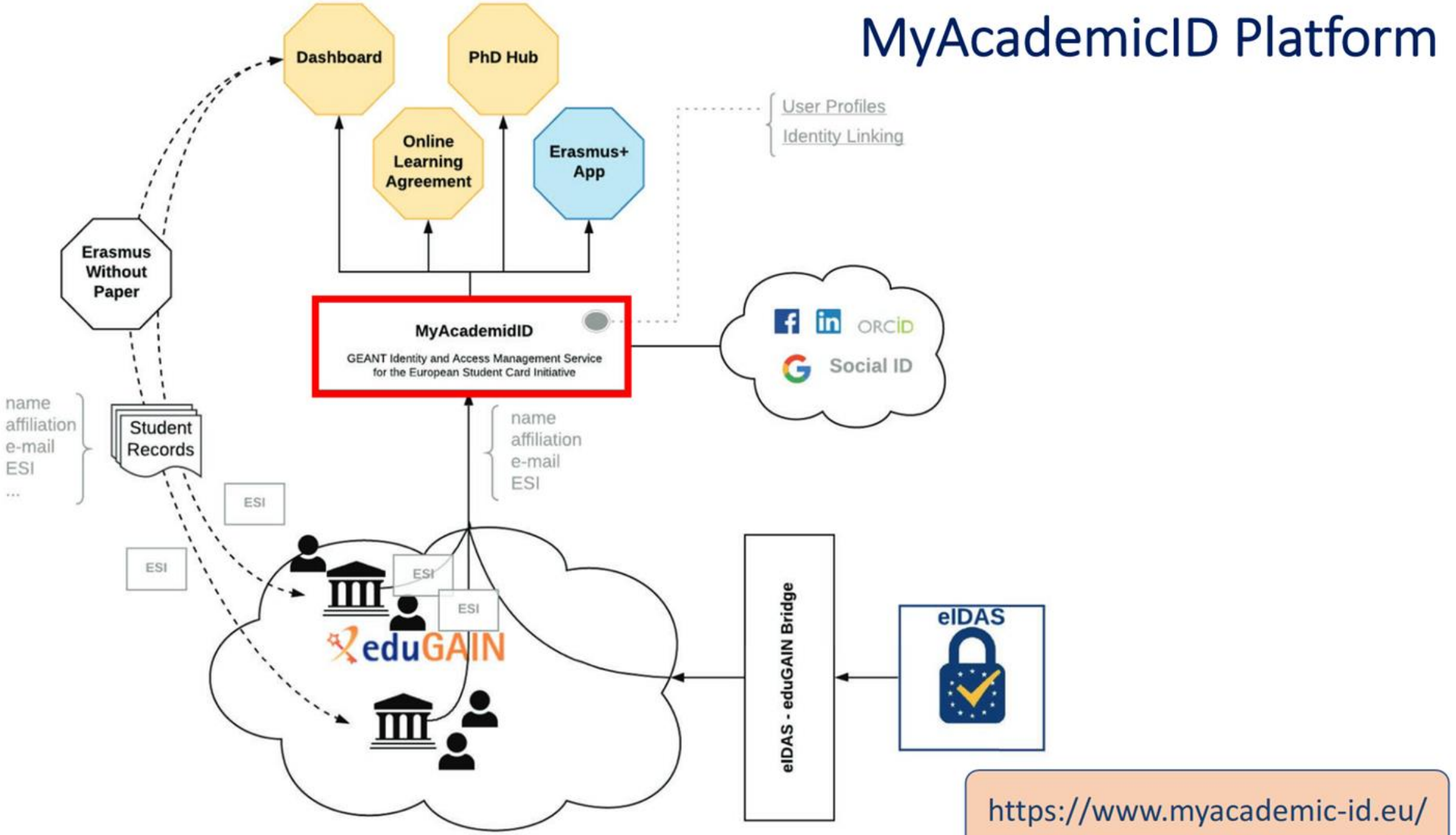
EUROPEAN STUDENT CARD INITIATIVE

Simplifying, facilitating, connecting.

MyAcademicID

enable every student to easily and safely identify and register themselves electronically at higher education institutions within Europe when moving abroad for studies, eliminating the need to complete onsite registration procedures and paper work.

MyAcademicID Platform



https://www.myacademic-id.eu/

eduGAIN Challenges

- Too few federations participate
  - Solved as more then 85% known R&E federations participate
- Too few organisations participate
  - Addressed with recommendations for opt-in/opt-out approach
- Process to address interfederated security incidents
  - eduGAIN Security team and SIRTFI Entity Category
- Too few attributes get released
  - Partially addressed with Entity Categories – R&S and CoCo

eduGAIN evolution
toward a stronger service definition

To improve the interoperation among entities, the eduGAIN community is **currently working** in the definition of **Baseline Expectations for eduGAIN**, classifying them in groups targeting:

- Identity Providers
- Service Providers
- Federation Operators

The aim is to improve user experience through a more interoperable and consistent service delivery

https://wiki.refeds.org/display/GROUPS/Baseline+Expectations+Working+Group

eduGAIN

GÉANT

Global Metadata Service

Supporting Tools

Global Policy

Identity Federation

National Metadata Service

National Policy

R&E Institution

SAML Auth Infrastructure

Identity Management

User

Can use over 3000 Web services

THANKS!

davide.vaghetti@garr.it

GÉANT

Networks · Services · People

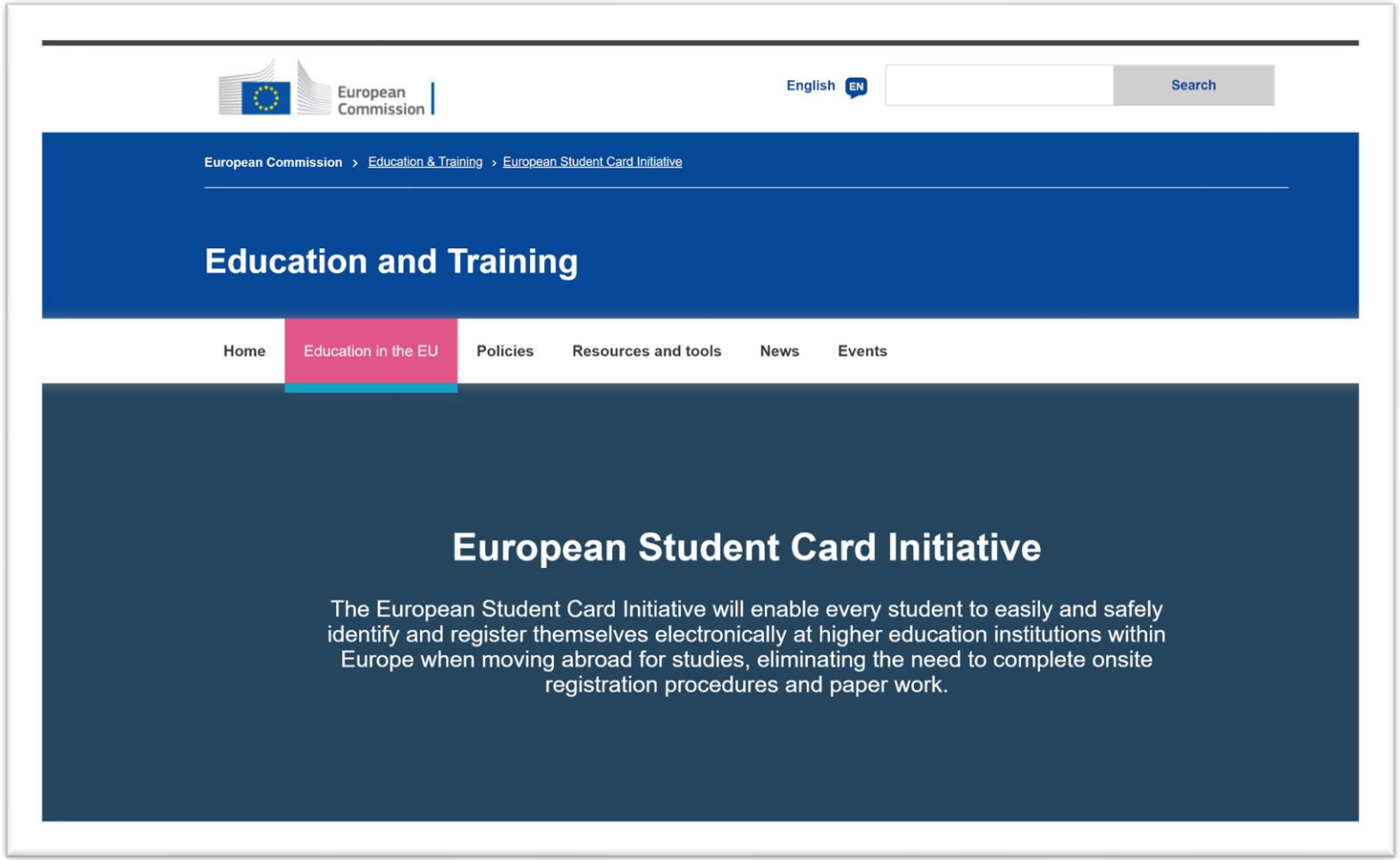
www.geant.org

eduGAIN: загальні відомості

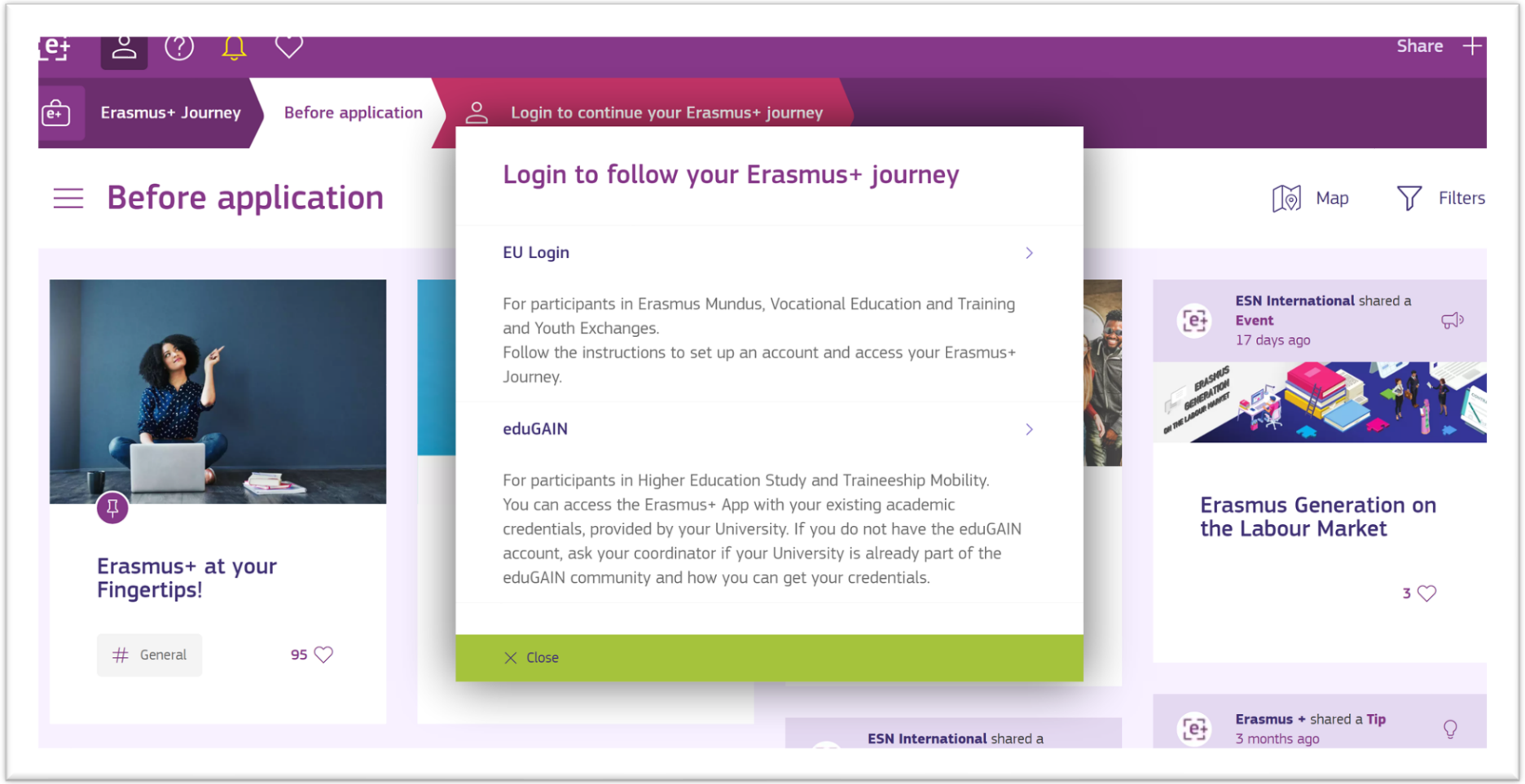
Ще декілька слів

Ukrainian Research and Academic Network

Ініціатива ЄК по створенню електронного студентського квитка



Застосунок Erasmus+



uran.ua
panorama.uran.ua

Ukrainian Research and Academic Network

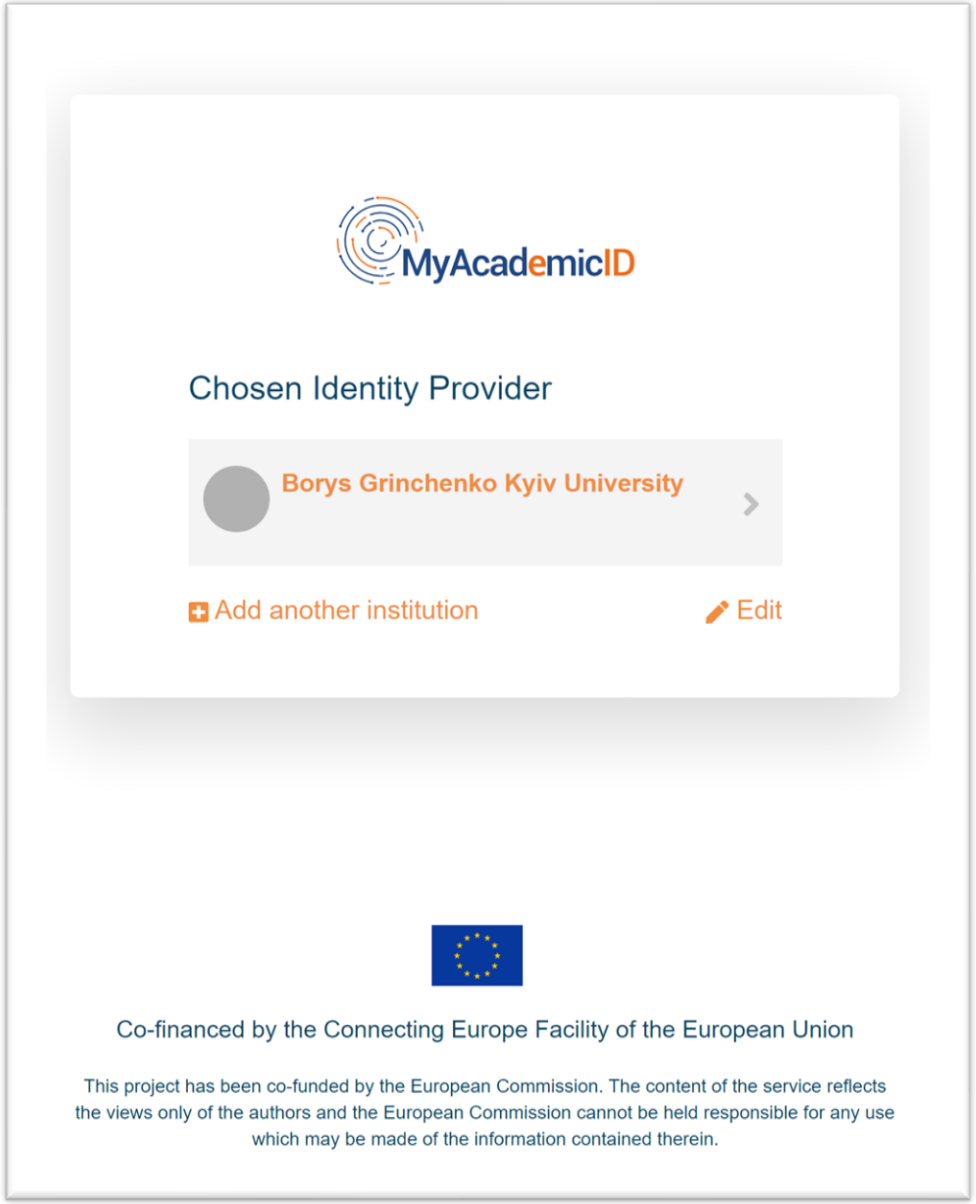
Етапи введення програми «Erasmus без паперів»

- 2021 - розпочати укладення угод про навчання в режимі онлайн
- 2022 – розпочати керування міжінституційними угодами
- 2023 – розпочати обмін студентами; приймати та розшифровувати записи, пов’язані з мобільністю студентів

Організації-учасниці повинні сприяти використанню мобільного застосунку Erasmus+, щоб забезпечити для студентів отримання вигоди від підвищення ефективності адміністративних процесів.

До 2025 року всі студенти в Європі повинні мати можливість користуватися перевагами Європейської ініціативи щодо отримання цифрових студентських квитків.

https://ec.europa.eu/education/education-in-the-eu/european-student-card-initiative_en



Університет України, що вже підключився до eduGAIN

Федерація ІД України

ПЕАНО

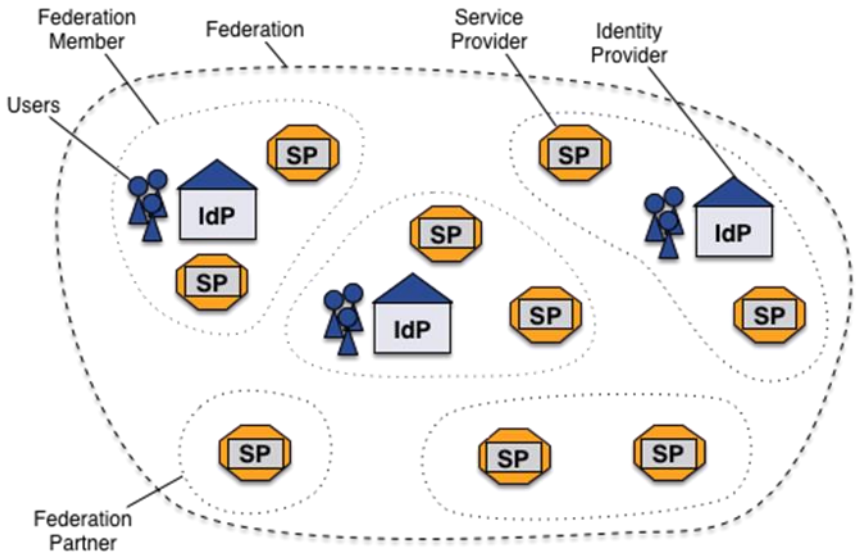
uran.ua
panorama.uran.ua

Ukrainian Research and Academic Network

Федерація **ПЕАНО**

Об’єднання постачальників ІД (IdP) та постачальників сервісів (SP) України. Оператор федерації – Асоціація УРАН

- IdP - забезпечують власникам електронних акаунтів можливість доступу до ресурсів SP.
- SP - володіють власними електронними ресурсами (бібліотеки, університети, обчислювальні центри, сховища даних тощо) і надають доступ до них власникам електронних облікових записів, справжність яких засвідчена одним з IdP ПЕАНО.



- Установи-учасниці реєструють свої метадані в ПЕАНО
- ПЕАНО перевіряє та збирає метадані всіх установ-учасниць та створює «довідник» федерації (один або декілька)
- «Довідник» (и) підписуються ключем ПЕАНО та розповсюджуються установам-учасницям

Ukrainian Research and Academic Network

Технологія eduGAIN

Ukrainian Research and Academic Network

Технологія єдиного входу Single Sign-On (SSO)

Зазвичай кожен онлайн сервіс потребує окремого облікового запису користувача. Тому постачальникам послуг доводиться керувати величезною кількістю облікових записів, а користувачі змушені оперувати декількома логінами та паролями, що створює незручності та послаблює безпеку.

Науково-освітні заклади Європи надають своїм користувачам єдину онлайн ідентифікацію (SSO) і тим самим відкривають їм доступ до всіх сервісів «домашньої» установи.

Наприклад, якщо на веб-порталі існує кілька незалежних сервісів (форум, пошта, чат, блог тощо), то, пройшовши автентифікацію в одному з сервісів, користувач автоматично отримує доступ до всіх інших, що позбавляє його від багаторазової автентифікації.

Способи автентифікації у веб-застосунках

Спосіб	Основне використання	Протоколи
За паролем	автентифікація користувачів веб-застосунків	HTTP, Forms
За сертифікатом	автентифікація користувачів в безпечних застосунках; автентифікація сервісів	SSL/TLS
За одноразовими паролями	Додаткова автентифікація користувачів (для досягнення двофакторної автентифікації)	Forms
За ключами доступу	автентифікація сервісів і застосунків	-
За токенами	Делегована автентифікація користувачів; делегована авторизація застосунків	SAML, WS-Federation, OAuth, OpenID Connect

Структура токена (SAML)

Токен (SAML) являє собою структуру даних в XML-форматі, яка містить інформацію:

- про суб'єкта, що згенерував токен,
- хто може бути отримувачем токена,
- термін дії,
- набір відомостей про самого користувача та додатковий набір даних.

Крім того, токен додатково підписується за допомогою асиметричної криптографії для запобігання несанкціонованих змін і гарантій автентичності токену (service provider (SP)).

SAML-токени містять механізм для підтвердження володіння токеном, що дозволяє запобігти перехопленню токенів через man-in-the-middle-атаки при використанні незахищених з'єднань.

Програмні продукти, що підтримують SAML (SSO)

- ✓ https://en.wikipedia.org/wiki/SAML-based_products_and_services

Найбільш відомі програмні продукти:

- ✓ Moodle
- ✓ Google Apps
- ✓ MS SharePoint
- ✓ BlackBoard

Програмне забезпечення (SAML) для інтеграції з eduGAIN

- SimpleSAMLphp (на мові PHP),
- Shibboleth MA (на мові Java)

ПЗ керування федерацією:

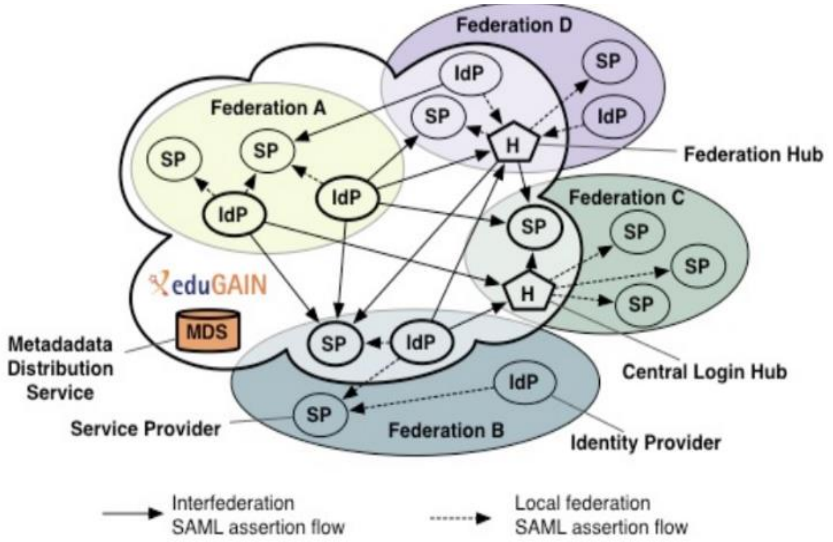
- Jagger (на мові PHP)

EDUcation Global Authentication Infrastructure

eduGAIN - сервіс **GÉANT**, який поєднує федерації інших країн, спрощуючи глобальній науково-дослідницькій та освітній спільноті доступ до контенту, послуг і ресурсів.

Технологія eduGAIN використовує «службу метаданих», яка регулярно зчитує і агрегує інформацію від федерацій про IDP та SP - і робить цю інформацію доступною для федерацій.

eduGAIN координує необхідні елементи технічної інфраструктури федерацій і забезпечує нормативну базу, яка контролює обмін інформацією між федераціями.



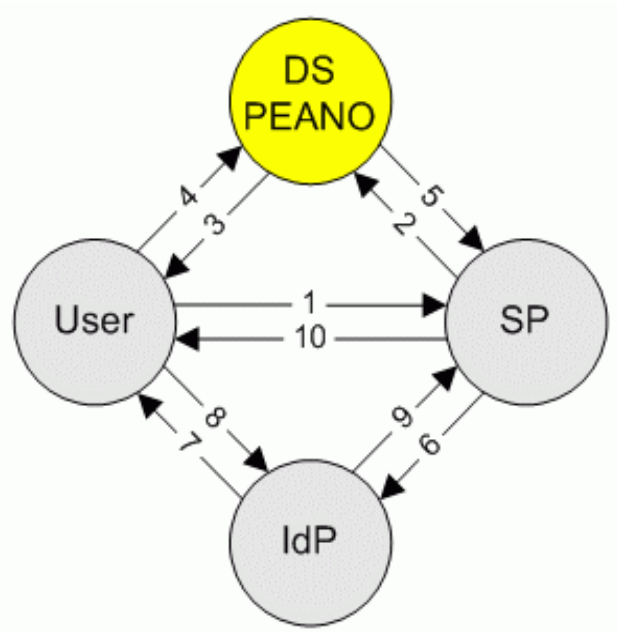
Функціонування сервісу ПЕАНО

- ✓ Користувач робить запит до веб-ресурсу (SP) **[1]**, цей запит перенаправляється до **Служби виявлення ПЕАНО** (*Service Discovery of PEANO*, DS PEANO) **[2]**, який містить перелік постачальників посвідчень (IdP) - членів Федерації.

- ✓ Сервер DS PEANO показує користувачу цей перелік **[3]**, з якого користувач вибирає свою «домашню» установу **[4]**. Сервер DS PEANO спрямовує цей вибір назад до Постачальника Послуг **[5]**, який далі пересилає запит на автентифікацію вибраному Постачальнику Посвідчень **[6]**, а той, в свою чергу, відображує інтерфейс **автентифікації** користувача **[7]**.

- ✓ Користувач вводить свої дані для доступу **[8]**. В разі успішної автентифікації Постачальник Посвідчень передає інформацію про користувача (так звані атрибути користувача) Постачальнику Послуг для **авторизації [9]**.

- ✓ Якщо користувач авторизований для доступу до ресурсу, він отримує доступ через браузер, в іншому випадку він отримує повідомлення про відмову в доступі **[10]**.



Ukrainian Research and Academic Network

Використання eduGAIN в УРАН

Ukrainian Research and Academic Network

Використання eduGAIN для контролю доступу до сховищ журналів та бібліотек (Journal and Library)

Приклади використання:

- Springer
- EBSCO
- Scopus
- ScienceDirect
- IEEE
- інші

Ukrainian Research and Academic Network

Використання eduGAIN в віртуальних платформах для навчання (VLEs -Virtual Learning Environments)

В УРАН реалізована авторизація через eduGAIN до сервису **WebClass**

Можливості сервісу:

- ✓ розрахований на велику кількість користувачів;
- ✓ загальний і приватний чат і обмін файлами;
- ✓ автоматичне перепідключення при виникненні перебоїв зв’язку;
- ✓ демонстрація робочого столу доповідача слухачам;
- ✓ завантаження і показ презентацій в стандартних форматах;
- ✓ навчальна дошка з віртуальною указкою;
- ✓ функції підйому руки і вираження емоцій смайлами;
- ✓ проведення голосування;
- ✓ функція запису лекції (доповіді, презентації) з можливістю повторного відтворення

webclass.uran.ua

Ukrainian Research and Academic Network

Використання eduGAIN в сервісі відеоконференцій (Video conferencing)

В УРАН реалізовані:

- ✓ авторизація через Gmail до сервісу edumeet (планується організувати авторизацію через eduGAIN)
- ✓ авторизація через eduGAIN до сервісу WebClass

eduMEET (https://edumeet.uran.ua) – відкрита браузерна платформа онлайн спілкування, розроблена для використання науково-освітньою спільнотою

WebClass (https://webclass.uran.ua/) – платформа для проведення відеоконференцій, онлайн семінарів, лекцій, робочих нарад, вебінарів, обговорень тощо

Ukrainian Research and Academic Network

Використання eduGAIN в сервісі eduVPN

- Сервіс eduVPN (https://www.eduvpn.org, https://github.com/eduVPN) забезпечує тунельне з'єднання з VPN-серверами, розташованими в наукових мережах інших країн, через захищений тунельний канал для доступу до внутрішніх локальних мереж.

- В УРАН реалізований захищений доступ до офісної мережі та до наукових мереж інших країн – на основі eduVPN з авторизацією через eduGAIN

- На основі сервісу eduVPN реалізована можливість під’єднатись до мережі УРАН з інших наукових мереж – наприклад, для тестування роботи сервісів з боку інших мереж

Ukrainian Research and Academic Network

Використання eduGAIN у сервісі «FileSender»

В УРАН реализований сервис FileSender з авторизацією через eduGAIN

FileSender - веб-застосунок, дозволяє авторизованим користувачам легко та надійно обмінюватись великими файлами (до 500 Гб).

Інші приклади реалізації сервісу FileSender:

- ACOnet (Austria)
- Amres (Serbia)
- Goe (UK)
- AARNet (Austria)

https://filesender.uran.ua

Ukrainian Research and Academic Network

Використання eduGAIN у сервісі OpenStack SaaS

- ✓ OpenStack в УРАН - програмне рішення, яке використовується для створення хмарних сервісів (**SaaS**). Продукт складається з відкритого безкоштовного програмного забезпечення, яке розповсюджується під ліцензією Apache.

- ✓ В УРАН ведуться роботи по впровадженню можливості авторизації користувачів eduGAIN у сервісі OpenStack - для доступу до адміністративних консолей віртуальних машин (openstack).

- ✓ Установи можуть використовувати eduGAIN для створення безпечного середовища, де користувачів можна ідентифікувати за допомогою одного посвідчення ІД на всіх серверах та сервісах

Ukrainian Research and Academic Network

Використання eduGAIN у сервісі eduroam

Сервіс eduroam забезпечує роумінг для користувачів національних науково-освітніх мереж

- Ведуться роботи з впровадження можливості авторизації користувачів eduGAIN в eduroam.
- Реалізована можливість авторизації через eduGAIN на веб-сторінці адміністрування домену eduroam https://eduroam.uran.ua/manage/login/?next=/manage/

Ukrainian Research and Academic Network

Використання eduGAIN в якості сервісу Web application login

В УРАН ведуться роботи з організації доступу до webmail, zabbix через eduGAIN

автентиікації SAML 2.0 підтримуються у версії Zabbix5

https://www.zabbix.com/documentation/current/ru/manual/appendix/install/okta

Доступ до веб-сторінки адміністрування домена eduroam здійснюється через eduGAIN

https://eduroam.uran.ua/manage/login/?next=/manage/

Ukrainian Research and Academic Network

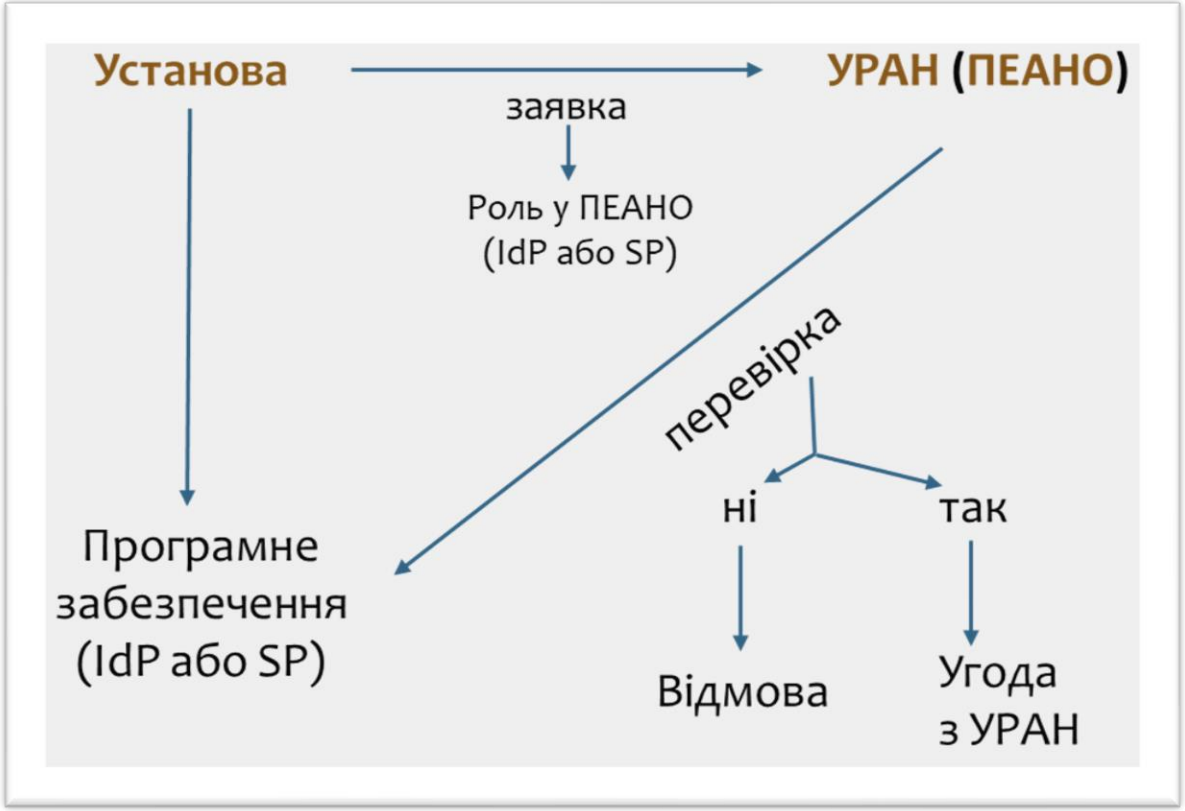
Умови надання сервісу eduGAIN

Ukrainian Research and Academic Network

Фінансові умови

- Клієнти, які користуються доступом до Інтернету від УРАН, – безкоштовно (у пакеті послуг)
- Інші клієнти – за запитом на dopomoga@uran.ua
- Обидві категорії – лише за умови членства в ПЕАНО

Процедура приєднання до eduGAIN



- ✓ Установа подає заявку на членство в Федерації, погоджуючись з її політикою в письмовій формі – за підписом офіційного представника установи.
- ✓ В заявці зазначається, в якій саме ролі заявник приєднується до Федерації - постачальник електронних посвідчень (IdP) чи постачальник сервису (SP) .
- ✓ Заявник за власний рахунок та на власних комп'ютерних ресурсах використовує програмне забезпечення відповідно до ролі, зазначеної на бланку заявки.
- ✓ Після проходження процедури перевірки програмного забезпечення установа-заявник підписує угоду з УРАН про надання послуг

Наші контакти

www.uran.ua

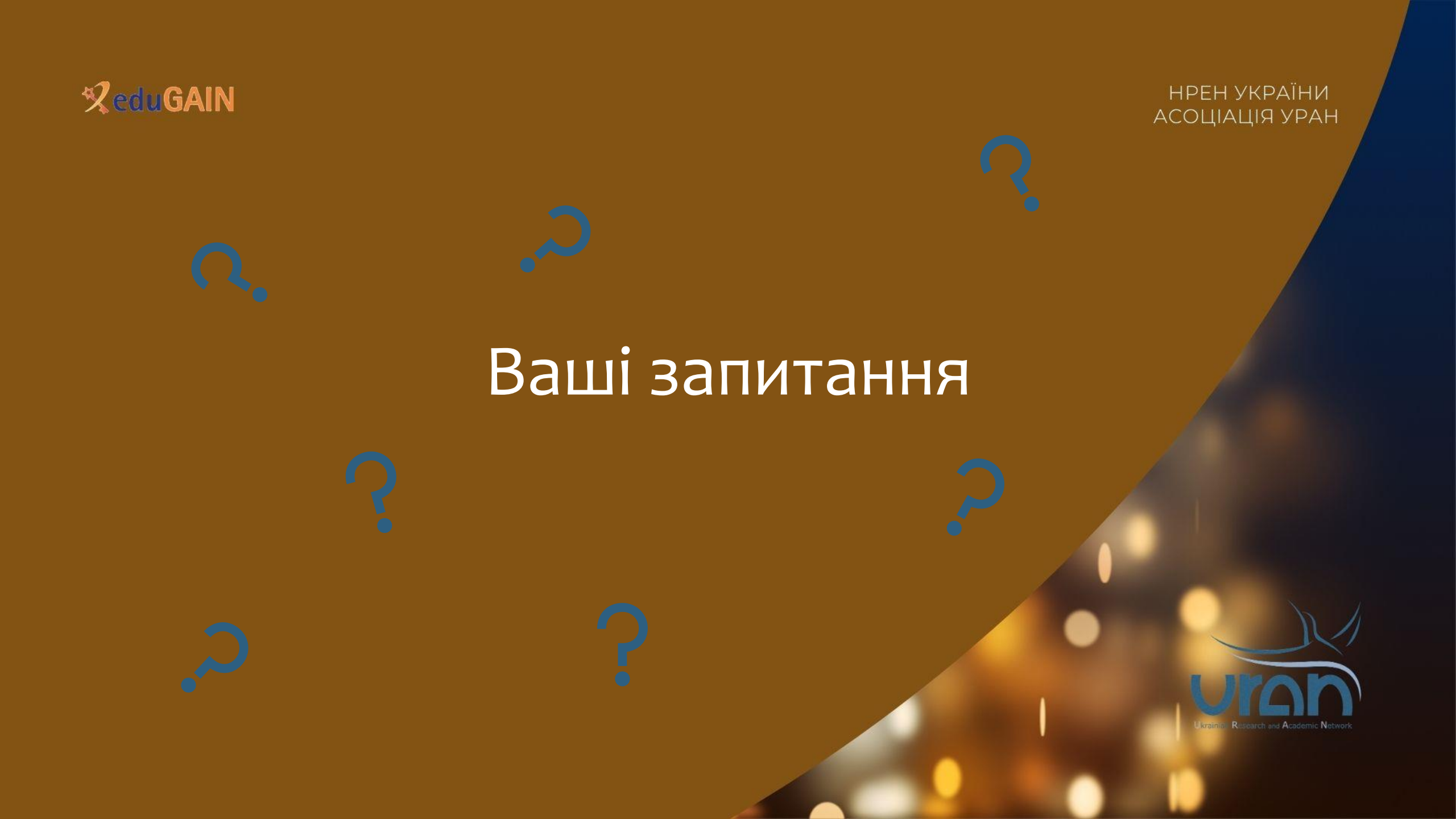
www.panorama.uran.ua

dopomoga@uran.ua

eduGAIN

НРЕН УКРАЇНИ
АСОЦІАЦІЯ УРАН

Ваші запитання



URAN
Ukrainian Research and Academic Network