R.2.1-2-3. Methodology to integrate the identified mechanisms into existing security procedures already adopted by partners

for the Project Education 4.0: Living Labs for the Students of the Future (LLSF)

Contract number 2021-1-RO01-KA220-HED-000032176

This project has received funding from the European Union's ERASMUS+ research and innovation programme under Grant Agreement no. 2021-1-RO01-KA220-HED-000032176.

Project:	Education 4.0: Living Labs for the Students of the Future (LLSF)
Action Type:	KA220-HED - Cooperation partnerships in higher education
Contract number:	2021-1-RO01-KA220-HED-000032176
Responsible:	University POLITEHNICA of Bucharest

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Erasmus+

List of participants

Participant No *	Participant organisation name	Acronym	Country
1 (Coordinator)	University POLITEHNICA of Bucharest	UPB	RO
2	Universidade NOVA de Lisboa	NOVA	PT
3	Universita Politecnica delle Marche	UPM	IT
4	Universidad Nacional de Education a Distancia	UNED	ES
5	Tel Aviv University	TAU	IL

Revision history:

Rev	Date	Partner	Description	Name
2	26/Ian/2023		Final Draft	Ciprian Dobre

Disclaimer

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Erasmus+

R.2.1. Set of Components, Extensions, and Technologies Identified to Enable Interconnection

In the context of the Education 4.0: Living Labs for the Students of the Future (LLSF) project, various components, extensions, and technologies have been identified to ensure effective interconnection between partner institutions and facilitate secure access to remote labs. Key identified solutions include:

Identity/Login Management

- eduGAIN Integration:
    - The eduGAIN interfederation service connects identity federations around the world, simplifying access to content, services, and resources for the global research and education community.
    - It enables secure authentication and authorization by connecting more than 8,000 Identity and Service Providers across 70 federations.
    - Each university's Moodle instance is integrated with its local Identity Provider (IdP) and registered with eduGAIN to allow seamless remote access for authenticated users across institutions.

Jupyter Hub Cluster

- Jupyter Hub is identified as a critical platform for running remote digital labs. It allows multiple users to access shared computing resources in a controlled environment, facilitating collaborative scientific work and remote experiment execution.
- Jupyter Hub's integration with eduGAIN further enhances security by ensuring that user authentication aligns with institutional credentials, reducing the risk of unauthorized access.

Components/elements/services to enable interconnection identified for Smart Labs

Identity/Login Management

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

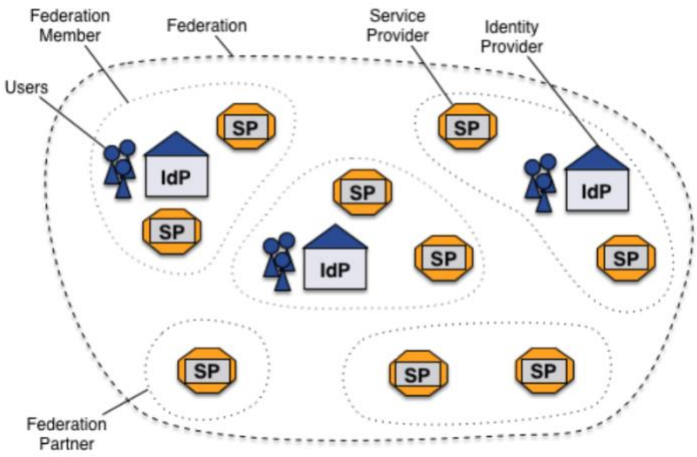
Erasmus+

As a cluster for open ideas, the technical implementation of the tools will come with the challenge of managing the authentication and access control for a big number of actors (students, teachers, researchers, and auxiliary personnel).

While manually granting access for each participant might look like a good solution for a project with a small number of participants, it can easily become an unbearable burden when we talk about 100s or 1000s of participants, with different roles in different institutions.

The eduGAIN interfederation service connects identity federations around the world, simplifying access to content, services, and resources for the global research and education community. eduGAIN connects more than 8,000 Identity and Service Providers and helps nearly 27.000.000 students, researchers, and educators access online services while minimizing the number of accounts they must manage. By interconnecting more than 70 federations around the world, eduGAIN enables more than 3,500 Service Provider to easily identify their users with minimal costs.

From a functional point of view, EduGAIN acts as an automated aggregator of metadata enabling the interoperability between multiple Research and Education Federations (REFEDS) entities founded mostly by National Research and Education Networks and the Internet Society.



This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

On the user side, EduGAIN comes as a help for both minimizing the number of accounts each user must manage as well as a technical solution for automatically proving the academic status, using the authentication source from the home organization (e.g., university, research centre, etc.).

To take advantage of the opportunity of using eduGAIN as roaming authentication method, we aim to engage the SSO (Single Sign-On) authentication for most of the services that require academic status validation and/or extended exposure to beneficiary from other academic organizations.

To achieve the goal above:

- Each institution involved should become an IdP (Identity Provider) in EduGAIN.
- Each institution offering a service should become a SP (Service provider) in EduGAIN.

Useful information about joining EduGAIN can be found in public websites such as:

- EduGAIN main website: https://edugain.org
- EduGAIN technical site: https://technical.edugain.org
- EduGAIN section of the GEANT Wiki: https://wiki.geant.org/display/eduGAIN/eduGAIN+Home

Joining EduGAIN as an IdP involves access to the internal SSO system of educational/research you want included in the inter-federation. Therefor the IdP registration is most likely to be done by the IT team in the institution.

After the SSO gateway is ready, the IdP/SP should be advertised in the EduGAIN inter-federation. Directed by the status of the EduGAIN, research/educational entities should join EduGAIN through the Federation in their country. This is usually administrated by the National Research and Education Network. A list of the current federations in EduGAIN can be found at https://technical.edugain.org/status. Each entity that wishes to join EduGAIN should contact the Federation inside the home country.

In Table 1 it is present an extract of information that can be useful for the partners in the project to get in touch with the suitable federations.

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Erasmus+

Country	Federation	Federation Page	Contact email
Romania	RoEduNetID	https://eduid.roedu.net/	eduid@roedu.net
Israel	IUCC Identity Federation	https://iif.iucc.ac.il/home/	info@iif.iucc.ac.il
Portugal	RCTSaai	http://rctsfederation.fccn.pt/	noc@fccn.pt
Italy	IDEM	https://www.idem.garr.it/index.php/en	idem-help@garr.it
Spain	SIR	http://www.rediris.es/sir/	sir@rediris.es

A set of Frequently Asked Questions and answers about EduGAIN integration:

Q1: How can I check if my organization is already federated and part of EduGAIN?

A1: Check your email/domain at https://technical.edugain.org/isFederatedCheck/.

Q2: How can I check if my organization is registered as an IdP / SP?

A2: Search the entity using EduGAIN Database Explorer: https://technical.edugain.org/entities.

Q3: How can I test the integration of the IdP in my organization?

A3: One should check the Attribute Release check at https://release-check.edugain.org

Jupyter Hub cluster for running remote living labs

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

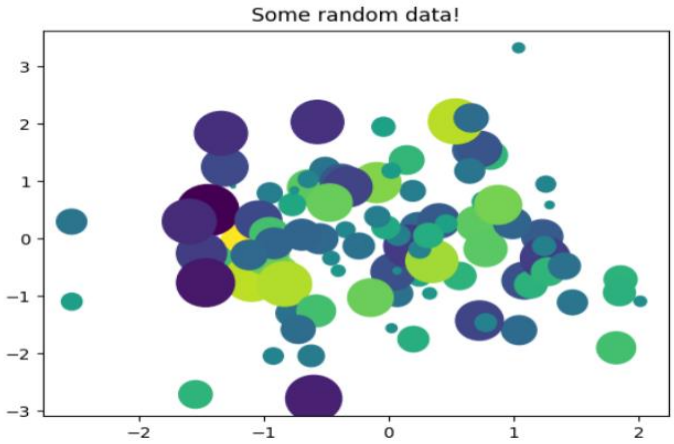
Erasmus+

Jupyter Notebook is an Open-Source software component that allows to run computational components through a web-based interface.

```
[1]: from matplotlib import pyplot as plt
     import numpy as np

     # Generate 100 random data points along 3 dimensions
     x, y, scale = np.random.randn(3, 100)
     fig, ax = plt.subplots()

     # Map each onto a scatterplot we'll create with Matplotlib
     ax.scatter(x=x, y=y, c=scale, s=np.abs(scale)*500)
     ax.set(title="Some random data!")
     plt.show()
```



This web-based GUI approach is ideal for learning laboratories since it combines the flexibility of writing code in more than 40 programming languages with the easy visualization of the results. Through a Jupyter Notebook, the students can easily interact with the code given by the instructor as well as develop new snippets of code and experiments.

Containerized **Jupyter Notebooks are also an important vector of reproducible research** since they allow the researchers to share their code along with easily accessible methods to visualize the results and create new experiments.

Running Jupyter Notebook on Windows/Linux/MacOS

Assuming you have already installed Python 3.x on Windows/Linux/MacOS workstation, running Jupyter Notebook only takes two easy steps:

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Step 1: Installing Jupyter Notebook using pip

```
pip install notebook
```

Listing 7. Installation of Jupyter Notebook.

Step 2: Running the notebook

```
jupyter notebook
```

Listing 8. Running Jupyter notebook.

The default and most used programming language for Jupyter Notebook is Python. By default, is uses the global Python environment on the machine it runs as any python script run by the current user.

Since different laboratories might have different requirements (in terms of installed libraries), it is recommended to run each Jupyter Notebook on its own Python virtual environment as in Listing 9.

```
# Create a new virtual environment
python -m venv venv
# Activate the virtual environment
source venv/bin/activate
# Install Jupyter Notebook
pip install notebook
# Install any other dependencies (requests as an example)
pip install requests
# Run jupyter notebook
jupyter notebook
```

Listing 9. Installing Jupyter Notebook using a virtual environment.

With the setup in Listing 9, resuming the work with a Jupyter notebook only takes the 2 steps in Listing 10.

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Erasmus+

```
# Reativate the virtual environment
source venv/bin/activate
# Install any other dependencies (requests as an example)
pip install requests
# Run jupyter notebook
jupyter notebook
```

Listing 10. Resuming the work on a Jupyter Notebook installed on a virtual environment.

Running Jupyter notebook using Docker Containers

Even though running Jupyter notebooks on virtual environments can help us run multiple projects asking for different dependencies, installing a large set of dependencies can still be tricky and take a lot of time.

In cases when the initial setup for a Jupyter Notebook is complex, running them using Docker containers can help work around the complexity of the initial setup.

Jupyter Docker Stacks20 offers a set of easy-to-run prebuild Docker images for different scenarios and setups and base images for creating new setups as well.

The images offered through Jupyter Docker Stack are publicly available on Docker Hub and they can be easily used by anyone. For example, the command in Listing 11 starts a Docker container running the image for the R language on port 8888 of the local machine, using the current folder as a working directory.

```
docker run -it --rm -p 8888:8888 -v "${PWD}":/home/jovyan/work jupyter/r-notebook
```

Listing 11. Running R-language notebook using Docker.

Running the command above, the latest jupyter/r-notebook image will be automatically downloaded and the Jupyter notebook container will start shortly.

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Erasmus+

Once the Jupyter server is running, a secret token will appear on the console and the user can access the instance by accessing http://<hostname>:8888/lab?token=<token> on the browser.

Adding new dependencies (libraries) to an existing Jupyter Docker Stack image is also very simple.

For example, the Dockerfile in Listing 12 adds the libraries in the requirements.txt file to the jupyter/datascience-notebook image using pip. mamba21 can also be used as in Listing 13.

```
# Start from a core stack version
FROM jupyter/datascience-notebook
# Install from requirements.txt file
COPY --chown=${NB_UID}:${NB_GID} requirements.txt /tmp/
RUN pip install --quiet --no-cache-dir --requirement /tmp/requirements.txt && \
    fix-permissions "${CONDA_DIR}" && \
    fix-permissions "/home/${NB_USER}"
```

Listing 12. Dockerfile adding requirements to jupyter/datascience-notebook image using pip (source: https://jupyter-docker-stacks.readthedocs.io/en/latest/using/recipes.html)

```
# Start from a core stack version
FROM jupyter/datascience-notebook
# Install from requirements.txt file
COPY --chown=${NB_UID}:${NB_GID} requirements.txt /tmp/
RUN mamba install --yes --file /tmp/requirements.txt && \
    mamba clean --all -f -y && \
    fix-permissions "${CONDA_DIR}" && \
    fix-permissions "/home/${NB_USER}"
```

Listing 13. Dockerfile adding requirements to jupyter/datascience-notebook image using Mamba. (source: https://jupyter-docker-stacks.readthedocs.io/en/latest/using/recipes.html)

Prebuild (custom) images can be prebuilt and uploaded to Docker Hub (or other container repository) and distributed to avoid long building times and ensure fast reproducibility of the computational environment.

Extensive tutorials on building Jupyter Docker images can be found at https://jupyter-dockerstacks.readthedocs.io/en/latest/using/recipes.html.

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Erasmus+

Jupyter Hub

Jupyter Hub is a container-based multi-user version of Jupyter Notebook which can be run on Cloud or on its own hardware to offload the burden of running the notebooks from the actual users to system administrators.

Using this approach, the location of the running code changes from the user's workstation to the location of Jupyter Hub deployment (e.g., university cluster) enabling not just the code in environments that can be close to important resources (e.g., databases, data repositories, live deployments of sensors), but also running computationally intensive tasks (by using Cloud/remote computational power) while using any convenient client (e.g., a notebook) to define the notebooks and interact with the results.

Two important ways of deploying Jupyter Hub are available:

- Zero to JupyterHub for Kubernetes (https://z2jh.jupyter.org/) deploys JupyterHub on Kubernetes using a well-maintained Helm Chart. This approach is suitable for scalable deployments when considering a large number of users.
- The Littlest JupyterHub (https://tljh.jupyter.org/en/latest/) is a simpler distribution aimed at smaller deployments using a single virtual machine.

Since the aim is to create Living Labs available for both homed and guest instructors and students, we are considering the deployment of JupyterHub deployment(s) to host the living labs with no special requirements/setups for the participants. This approach might also be required for simplified access to remotely hosted resources.

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Erasmus+

R.2.2. Authorization Mechanism for Secure Authentication and Access to Remote Labs

The technical implementation of authentication and access control for remote labs in the **Education 4.0: Living Labs for the Students of the Future (LLSF)** project presents significant challenges due to the large number of participants, including students, teachers, researchers, and administrative personnel. To address this, **eduGAIN** has been identified as a core solution.

Challenges in Managing Authentication and Access Control

- For small-scale projects with limited participants, manual authorization may be manageable. However, when scaling up to hundreds or thousands of participants across multiple institutions, this approach becomes inefficient and prone to errors.
- Different participants may have diverse roles within institutions (e.g., student, teacher, researcher), adding complexity to managing permissions and authentication.

eduGAIN as a Solution

eduGAIN is an interfederation service that simplifies secure authentication and access control across research and academic institutions. With over 8,000 Identity and Service Providers connected globally, eduGAIN serves approximately **27 million users** in academia by reducing the need for multiple account credentials.

eduGAIN's framework interconnects more than **70 national federations** and enables **3,500 Service Providers** to identify users efficiently with minimal cost.

Functional Role of eduGAIN

- **Automated Aggregation of Metadata:** eduGAIN functions as an automated aggregator, facilitating seamless integration and interoperability between various Research and Education Federations (REFEDS). These entities are typically supported by National Research and Education Networks (NREN) or related bodies.
- **Academic Status Verification:** By using the authentication system of the home organization (university, research center, etc.), eduGAIN simplifies the process of verifying a participant's academic status without requiring separate user accounts for each service.

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Implementation Plan for eduGAIN Integration

To successfully integrate eduGAIN for secure authentication in remote labs, the following steps should be followed:

1. **Each Institution as an Identity Provider (IdP):**
    - Each partner institution must register as an **Identity Provider** (IdP) within eduGAIN. This allows the institution's existing Single Sign-On (SSO) system to manage access control for participants from their organization.
2. **Each Institution as a Service Provider (SP):**
    - Institutions offering remote lab resources must register as **Service Providers** (SP) within eduGAIN. This ensures their services can securely authenticate users from partner institutions.
3. **SSO Integration Process:**
    - Institutions must prepare their internal SSO gateway to align with eduGAIN's protocols. The IT team typically manages this process, ensuring that proper attributes such as user roles, academic status, and institutional affiliations are correctly configured.
4. **Joining the National Federation:**
    - Institutions must join their respective **National Research and Education Network (NREN)** to participate in eduGAIN. Each NREN manages a national federation that facilitates eduGAIN integration.
      Examples of relevant NRENs include:
    - **Romania:** RoEduNetID - Contact: eduid@roedu.net
    - **Israel:** IUCC Identity Federation - Contact: info@iif.iucc.ac.il
    - **Portugal:** RCTSaai - Contact: noc@fccn.pt
    - **Italy:** IDEM - Contact: idem-help@garr.it
    - **Spain:** SIR - Contact: sir@rediris.es

Testing and Validation

To ensure successful integration, the following tools and resources are available for testing and validation:

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Federation Check Tool:**
  To confirm if an institution is already part of eduGAIN: Is Federated Check
- **Entity Status Verification:**
  To check whether an institution is registered as an IdP or SP in eduGAIN: eduGAIN Entity Database
- **Attribute Release Testing:**
  To test if an institution's IdP is correctly configured for attribute release: Attribute Release Check

Benefits of Using eduGAIN for Secure Authentication in Remote Labs

- **Simplified User Management:** Reduces the need for users to manage multiple accounts across institutions.
- **Automated Authorization:** Facilitates role-based access control for participants based on their academic status.
- **Scalability:** Supports projects with hundreds or thousands of participants without manual intervention.
- **Security Assurance:** Ensures secure, verified access to online resources with minimal administrative overhead.

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Erasmus+

R.2.3. Methodology to Integrate Identified Mechanisms into Existing Security Procedures

The methodology for integrating these mechanisms into the security frameworks of partner institutions includes the following steps:

Step 1: Analysis of Existing Security Procedures

- Each partner institution's current security procedures for digital resources (e.g., Moodle platforms, data repositories, Jupyter Hub) are reviewed to identify gaps and ensure compatibility with eduGAIN.
- The review process involves documenting current authentication frameworks, analyzing password management systems, evaluating encryption standards, and assessing data backup protocols.
- Specific attention is given to identifying weak points in user authentication, data storage practices, and session management.

Step 2: Framework Establishment

- An integration framework is defined to establish seamless connections between the existing security mechanisms and the newly identified solutions.
- Each institution's IdP is registered with eduGAIN, ensuring secure user identity verification.
- The framework includes defining uniform data encryption standards, session timeout settings, and user tracking mechanisms to improve security consistency across partner institutions.
- The deployment of a **Docker-Compose** stack using **Bitnami Moodle images** was identified as an effective solution for securely scaling Moodle platforms in combination with automated monitoring and load balancing configurations.

Step 3: Access Control Configuration

- User roles and permissions are mapped to align with eduGAIN's role-based security framework.
- This includes defining specific access rights for students, educators, and administrators to ensure appropriate security measures are upheld.
- Permissions are set to restrict access to sensitive data and protect critical resources. For example, student access may be restricted to course content, while educators are granted administrative rights to manage user roles and data entry.

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Erasmus+

Step 4: Awareness and Training

- Training sessions are conducted to ensure technical staff and end-users understand the newly integrated security framework.
- These sessions focus on secure login processes, data protection best practices, and troubleshooting potential issues with the integrated platforms.
- End-users are guided on identifying phishing attempts, understanding social engineering threats, and practicing secure data handling techniques to minimize risk.

Step 5: Additional Procedures for Integration from the Methodological Toolkit

- **IoT Integration:** Incorporating IoT frameworks that align with data collection, sensor integration, and real-time monitoring for remote labs. Specific mechanisms ensure secure transmission of IoT data with encryption protocols such as TLS.
- **AI-Enhanced Security Features:** The toolkit includes AI-driven security enhancements to detect and mitigate potential security threats in real-time. These systems use machine learning algorithms to detect anomalous behavior and automatically alert administrators.
- **Automated Logging and Monitoring:** Utilizing monitoring solutions that integrate with the Moodle platform to provide alerts on unauthorized access attempts or suspicious activities. Logs are collected in centralized storage to ensure comprehensive auditing.
- **Secure API Management:** Ensuring that data shared across systems follows secure protocols such as OAuth 2.0 and API Gateways to protect data transactions. The toolkit emphasizes robust key management practices to mitigate exposure risks.
- **Incident Response Planning:** Establishing response protocols to handle security breaches efficiently, including escalation procedures, forensic analysis guidelines, and recovery strategies.

Step 6: Security Assessment and Continuous Improvement

- Periodic assessments are performed to evaluate the performance and security of the integrated mechanisms.
- These assessments include penetration testing, vulnerability scanning, and data privacy audits to identify potential risks proactively.
- Identified vulnerabilities are addressed promptly to ensure compliance with evolving security standards.

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Erasmus+

- Partner institutions are encouraged to participate in collaborative security drills to improve response times and ensure readiness in the event of a security incident.

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.