**Student and Citizen Identities Linked**

# D5.2 Operational and Technical Documentation of Platform Integration with eduGAIN

| **Document Identification** | | | |
|---|---|---|---|
| **Status** | Final | **Due Date** | 13/11/2020 |
| **Version** | 1.0 | **Submission Date** | 13/11/2020 |

| | | | |
|---|---|---|---|
| **Related Activity** | Act 5 | **Document Reference** | D5.2 |
| **Related Deliverable(s)** | D2.2, D3.2 | **Dissemination Level (*)** | PU |
| **Lead Organization** | UAegean | **Lead Author** | Petros Kavassalis |
| **Contributors** | UAegean<br>ATOS | **Reviewers** | Dimitris Mitropoulos, GRNET<br>Ross Little, ATOS |

| **Keywords:** |
|---|
| eduGAIN, Authentication, Identity Provider |

This document is issued within the frame and for the purpose of the SEAL project. This project has received funding from the European Union's Innovation and Networks Executive Agency – Connecting Europe Facility (CEF) under Grant AGREEMENT No INEA/CEF/ICT/A2018/1633170; Action No 2018-EU-IA-0024. The opinions expressed, and arguments employed herein do not necessarily reflect the official views of the European Commission.

# Document Information

| List of Contributors | |
|---|---|
| Name | Partner |
| Petros Kavassalis | University of the Aegean |
| Nikos Triantafyllou | University of the Aegean |
| Pigi Karavia | University of the Aegean |
| Anastasia Constantelou | University of the Aegean |
| Miryam Villegas Jimenez<br>Nicolas Liampotis | ATOS<br>GRNET |

| Document History | | | |
|---|---|---|---|
| Version | Date | Change editors | Changes |
| 0.1 | 06/11/2020 | Petros Kavassalis | version for partner review |
| 0.2 | 13/11/2020 | Ross Little, ATOS | Review |
| 0.3 | 13/11/2020 | Eirini Degkleri, GRNET | Review |
| 1.0 | 13/11/2020 | ATOS | FINAL VERSION TO BE SUBMITTED |

| Quality Control | | |
|---|---|---|
| Role | Who (Partner short name) | Approval Date |
| Deliverable leader | UAegean | 13/11/2020 |
| Technical manager | UJI | 13/11/2020 |
| Quality manager | ATOS | 13/11/2020 |
| Project Manager | ATOS | 13/11/2020 |

# Table of Contents

# List of Figures

# List of Acronyms

| Abbreviation / acronym | Description |
|---|---|
| CEF | Connecting Europe Facility |
| CI/CD | Continuous Integration/ Continuous Development |
| DG DIGIT | Directorate-General for Informatics |
| DID | Decentralized Identifier |
| Dx.y | Deliverable number y belonging to WP x |
| EC | European Commission |
| eMRTD | Electronic Machine Readable Travel Document |
| HEI | Higher Education Institution |
| IdP | Identity Provider |
| MDS | Minimum Data Set |
| MS | Member State |
| NREN | National research and education network |
| OVF | Open Virtual Format |
| SP | Service Provider |
| WP | Work Package |

# 1.Introduction

The SEAL project has developed and deployed the required process for integration with the eduGAIN network. Specifically, the deployed process integrates the SEAL platform, deployed in GRNET in Task 5.1, with the eduGAIN network via the Greek NREN (GRNET). This, therefore, enables the required validation workflow to allow the importing of eduGAIN academic attributes to the SEAL platform with the purpose of linking them with Personal Identification Information, retrieved from the eIDAS Network, and also deriving new privacy preserving identities. Additionally, via the deployed software eduGAIN authentication can be used to support identity bootstrapping, authentication and linking to other prevalent identities (like ePassport under eMRTD specifications).

## 1.1 Purpose of the document

The presented document describes the efforts and results undertaken by the partners during Activity 5 (Linking Service deployment and integration for cross-border testing) Task 5.2 (Integration of SEAL Platform with eduGAIN Network) to deploy the required process to integrate the SEAL Platform with the eduGAIN Network and specifically to integrate the SEAL to the Greek NREN GRNET.

## 1.2 Relation to other project work

The work presented here was carried out in conjunction with Activity 3 (Linking Service Core Platform and modular interfaces development) to produce a platform for managing and verifying linked identities, as specified in the technical specification produced by Activity 2 (Linking Service Core Platform and Interfaces Design). It is also related with the Task 5.1 “Deployment of SEAL Platform and integration with eIDAS Network”.

## 1.3 Structure of the document

This document is structured in 3 major chapters

**Chapter 2** Presents the technical integration of the SEAL platform with the eduGAIN network

**Chapter 3** Provides validation results from the integration of the SEAL platform with the eduGAIN network

**Chapter 4** Reports on the conclusions of the integration efforts

# 2. SEAL eduGAIN Technical Integration

This section provides a brief overview of the eduGAIN network and the technical architecture and integration steps required to enable SEAL to offer its service over the eduGAIN federation.

## 2.1 The SEAL Service as a Service Provider towards the eduGAIN network

The SEAL platform acts as a Service Provider (SP) to the eduGAIN network. Specifically, SEAL supports an interface to the eduGAIN federation towards Higher Education Institutions (HEI) Identity providers which act as both a student authentication and identity source for SEAL. This is fully described in D2.2 [1].

### 2.1.1 eduGAIN Network

EduGAIN is a strongly established GÉANT initiative, providing the framework for interconnecting different education identity federations. These federations include Identity Providers (IdP) from the affiliated Higher Education Institutions.

The eduGAIN interfederation shares some similarities with the eIDAS-eID network (the primary identity source for the SEAL project), but there are some differences. In eduGAIN, all interactions are point to point, not involving proxies like the eIDAS-eID nodes that proxy the requests to the IdPs (although some sub-federations might choose to).

Despite offering lower grade assurances than the eIDAS identities, the fact that these assurances contain academic attributes make eduGAIN a strategic pillar of the SEAL service.

### 2.1.2 GRNET eduGAIN Proxy

The SEAL interface to the eduGAIN interfederation is provided through the GRNET eID Proxy service. The eID Proxy acts as an SP towards the external Identity Providers (IdPs) and, at the same time, as an IdP towards the SPs (e.g. SEAL platform). Through the proxy, users are able to authenticate using:

- eIDAS credentials;
- the universities and research institutes that participate in the eduGAIN interfederation;
- other social identity providers, such as Google, Facebook, LinkedIn, and ORCID.

To achieve this, the eID Proxy supports the translation between different authentication protocols, such as SAML (eIDAS and SAML2int profile), OpenID Connect and OAuth 2.0. The proxy also provides a country selector for users to select their country of origin eIDAS node (Home eIDAS Node). Figure 1 provides a high-level view of the GRNET eID Proxy service architecture illustrating the interconnections with IdPs and SPs.

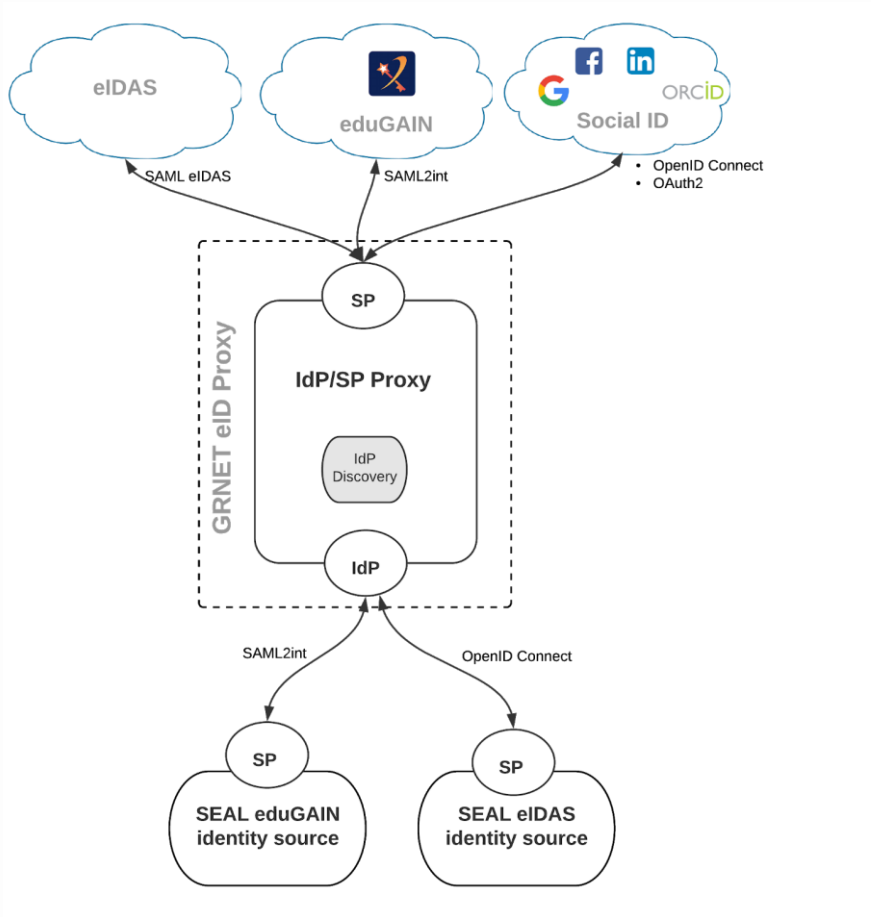



**Figure 1: GRNET eduGAIN Proxy**

There are three instances of the GRNET eID Proxy:

1. **Production** – Connected with the production instance of the Greek eIDAS Node which, in turn, is connected to a number of production eIDAS Nodes of other Member States. This allows eIDAS cross-border authentication using natural/legal person account credentials.
2. **Preproduction** – Connected with the preproduction instance of the Greek eIDAS Node which, in turn, is connected to a number of preproduction eIDAS Nodes of other Member States. This allows for testing eIDAS cross-border authentication using test natural/legal person account credentials.
3. **Test** – Connected with an eIDAS Node deployed locally at GRNET to allow testing eIDAS authentication using test natural/legal person account credentials.

The production instance of the GRNET eID Proxy has joined eduGAIN through the GRNET identity federation as a Service Provider under the REFEDS Research and Scholarship (R&S) entity category in order to ensure sufficient attribute release, including unique and non-reassignable user identifiers. The GRNET eID Proxy can enable users from more than 4000 Universities and Research Institutes to access the SEAL platform with little or no administrative involvement.

Depending on their attribute release policy, identity providers can release the following user attributes to SEAL through the eID Proxy:

| Attribute type | Friendly name | **URN** |
|---|---|---|
| User identifier | eduPersonUniqueId | urn:oid:1.3.6.1.4.1.5923.1.1.1.13 |
| | eduPersonPrincipalName | urn:oid:1.3.6.1.4.1.5923.1.1.1.6 |
| | eduPersonTargetedID | urn:oid:1.3.6.1.4.1.5923.1.1.1.10 |
| Name | cn | urn:oid:2.5.4.3 |
| | displayName | urn:oid:2.16.840.1.113730.3.1.241 |
| | givenName | urn:oid:2.5.4.42 |
| | sn | urn:oid:2.5.4.4 |
| Email | mail | urn:oid:0.9.2342.19200300.100.1.3 |
| Affiliation | eduPersonAffiliation | urn:oid:1.3.6.1.4.1.5923.1.1.1.1 |
| | eduPersonScopedAffiliation | urn:oid:1.3.6.1.4.1.5923.1.1.1.9 |
| | schacHomeOrganization | urn:oid:1.3.6.1.4.1.25178.1.2.9 |
| | schacHomeOrganizationType | urn:oid:1.3.6.1.4.1.25178.1.2.10 |

## 2.2 SEAL eduGAIN Integration Architecture and Deployment

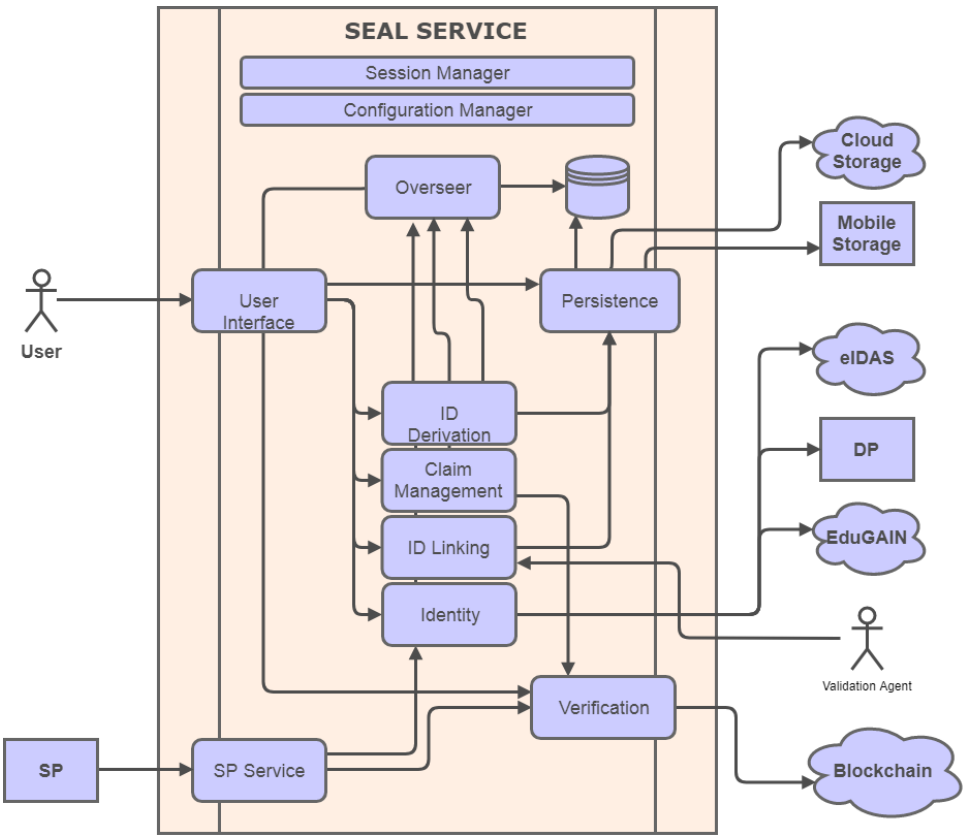



**Figure 2: SEAL Service architecture diagram**

The overall architecture of the SEAL platform can be seen in Figure 2. Interfacing to the Identity Sources (like eduGAIN and eIDAS) takes place using specially built software, denoted in the figure above as "identity" modules. During implementation a specifically built identity module was developed and deployed for each authentication source.

### 2.1.3 SEAL eduGAIN Identity Module

The SEAL Platform integration with the eduGAIN Federation takes place using a software module called the "eduGAIN Identity module". This module supports the interface to the eduGAIN federation by connecting to the GRNET eduGAIN proxy: a proxy service to the eduGAIN federation maintained by the Greek NREN GRNET allowing easy integration with the federation and consumption of academic Ids.

Specifically, the "eduGAIN Identity module" implements an internal protocol towards the SEAL platform (for more details please review D2.2 [1] and D3.2 [2]) and consumes a SAML2 interface from the eduGAIN proxy. This Identity module requests the full eduGAIN schema to be returned in the metadata so that the end user is able to fully manage their eduGAIN identity data using the SEAL service.

Two services are provided to the SEAL Platform: one for a user to be authenticated, and another for a user to query their attributes. Both of them result in a redirection towards the GRNET eduGAIN proxy where the final eduGAIN identity provider can be selected. See Figure 1: GRNET eduGAIN Proxy

Once the user has introduced their credentials, the eduGAIN provider returns the corresponding answer to the SEAL eduGAIN module (following the SAML protocol), which redirects to the related module depending on that answer (success/fail authentication).

#### 2.2.1.1 SEAL Platform deployment and eduGAIN Authentication connection

This microservice (edugain-idp) is implemented in Java code using Spring. The related github repository can be found at https://github.com/EC-SEAL/edugain-idp, where the code updates are done in the default branch (development).

The current README file is located at https://github.com/EC-SEAL/edugain-idp/blob/development/README.md. The following environment variables are used:

- ASYNC_SIGNATURE is a Boolean value, if true denotes RSA signing for JWTs, else HS256 signing is conducted.
- KEYSTORE_PATH is the path to the keystore holding the RSA certificate used for signing JWTs.
- KEY_PASS is the password for the certificate.
- STORE_PASS is the password for the keystore containing the certificate.
- HTTPSIG_CERT_ALIAS is the alias of the certificate used for the httpSig protocol.
- SIGNING_SECRET is an HS256 secret used for symmetric signing of JWTs.
- SESSION_MANAGER_URL is the location of the Session Manager microservice.
- Variables related to the SAML certificate expedited by GRNET to Atos:
    - SAML_KEYSTORE_PATH

- SAML_KEYSTORE_PASS
- SAML_KEYSTORE_ID
- SAML_KEY_PASS

- PESPONSE_SENDER_ID is the name chosen for this edugain-idp microservice in the current deployment (the same that ConfigurationManager module serves).
- CL_RESPONSE_RECEIVER_ID is the name of the APIGW microservice in the current deployment (the same that ConfigurationManager module serves).
- RM_RESPONSE_RECEIVER_ID is the name of the Request Manager microservice in the current deployment (the same that ConfigurationManager module serves).
- IDP_METADATA_URL is set to the GRNET eduGAIN proxy ( https://eid-proxy.aai-dev.grnet.gr/Saml2IDP/proxy.xml)
- Some information related to the ssl certificate has to be added:
  - SSL_KEYSTORE_PATH
  - SSL_STORE_PASS
  - SSL_KEY_PASS
  - SSL_CERT_ALIAS

The seal-idp.yaml file contains the OpenAPI (swagger) specification for this microservice. Note that this file is a part of the SEAL_interfaces.yaml (https://github.com/EC-SEAL/interface-specs) which defines all the interfaces of SEAL.

The Dockerfile file is intended for packing this microservice as container, which image will be stored in docker-hub under different tags along the development and testing (https://hub.docker.com/repository/docker/mvjatos/seal-edugain-idp )

Following the CI/CD directives agreed in the project, a file .travis.yml has been specified in order to automate the container management and its versions.

Within the source directory (src), where the code is found, there is a resources directory used to store there the keys used for signing the requests to other microservices, as Session Manager; the keys for SAML requests are kept there too. That means a resources directory has to be available as a volume within the container, as it explained following.

When the edugain-idp is to be deployed, several aspects to take into account are:

- The last version of the container image.
- The necessary environment variables to be set.
- Dependencies on the Session Manager.
- To define a volume where to keep the key stores.
- The internal port of this microservice is 8081.

After starting successfully, the related log shows these last lines:

```
2020-10-28 12:18:50.457  INFO 1 --- [           main] o.s.s.c.ThreadPoolTaskExecutor           :
Initializing ExecutorService 'applicationTaskExecutor'
2020-10-28 12:18:52.036  INFO 1 --- [           main] o.s.b.w.e.t.TomcatWebServer              : Tomcat
```

started on port(s): 8081 (https) with context path "
2020-10-28 12:18:52.044 INFO 1 --- [ main] e.s.i.Application : Started Application in 13.146 seconds (JVM running for 15.504)

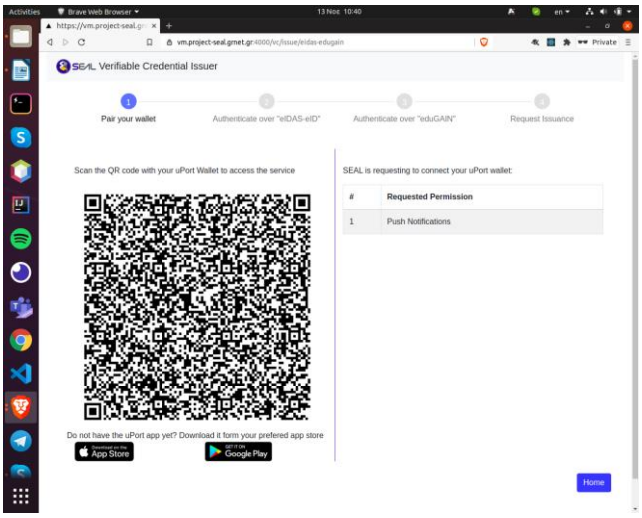
An example of how to deploy the edugain-idp using Docker is given in the following figure:

```
edugain-idp:
    image: mvjatos/seal-edugain-idp:test3
    restart: on-failure
    command:
      - "-Dorg.opensaml.httpclient.https.disableHostnameVerification=true"
    environment:
      - ASYNC_SIGNATURE=true
      - KEY_PASS=xxxxx
      - SIGNING_SECRET=xxxxx
      - JWT_CERT_ALIAS=xxxxx
      - SAML_KEYSTORE_PATH=classpath:/saml/your_site_name.jks
      - SAML_KEYSTORE_PASS=xxxxx
      - SAML_KEYSTORE_ID=xxxxx
      - SAML_KEY_PASS=xxxxx
      - STORE_PASS=xxxxx
      - HTTPSIG_CERT_ALIAS=xxxxx
      - SESSION_MANAGER_URL=http://SessionManager:8090
      - KEYSTORE_PATH=resources/testKeys/keystore.jks
      - IDP_METADATA_URL=https://eid-proxy.aai-dev.grnet.gr/Saml2IDP/proxy.xml
      #- YES: IDP_METADATA_URL=https://idp.ssocircle.com
      - TESTING=true
      - RESPONSE_SENDER_ID=edugainIDPms_001
      - CL_RESPONSE_RECEIVER_ID=CLms001
      - RM_RESPONSE_RECEIVER_ID=RMms001
      - SSL_KEYSTORE_PATH=/cert/keystoreatos.jks
      - SSL_STORE_PASS=xxxxx
      - SSL_KEY_PASS=xxxxx
      - SSL_CERT_ALIAS=xxxxx
    links:
        - SessionManager:SessionManager
    networks:
    volumes:
      - /SEAL/EDUGAIN-IDP/resources:/resources^M
      - /SEAL/ATOS-CERT/202010:/cert
    ports:
      - 10081:8081
    depends_on:
      - SessionManager
```

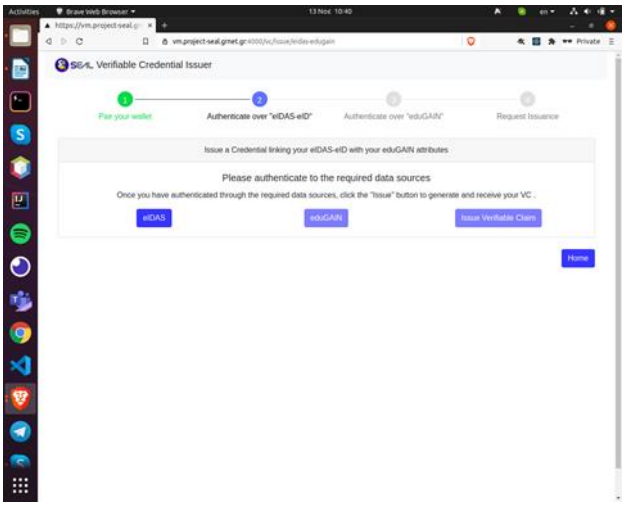
# 3. Validations Tests

This presents a validation test conducted on teh SEAL platform to prove its working integration with the eduGAIN and eIDAS netwroks respectively. Specifically, this test consists of a user using the production SEAL platform to authenticate over eIDAS and eduGAIN and finally link these identities together in order to generate a linked Verifiable Credential and store it in their mobile wallet. The following screenshots present the aforementioned flow:

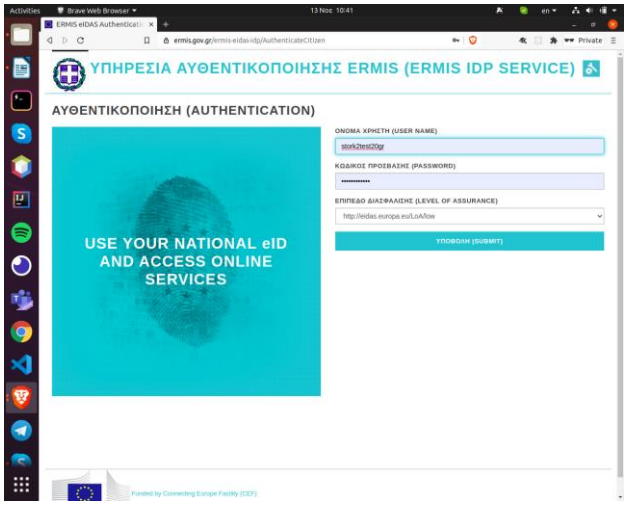
- The user accesses the SEAL platform Verifiable Credential issuer service at https://vm.project-seal.grnet.gr:4000/vc/issue/eidas-edugain and is prompted to connect their wallet by performing DID authentication

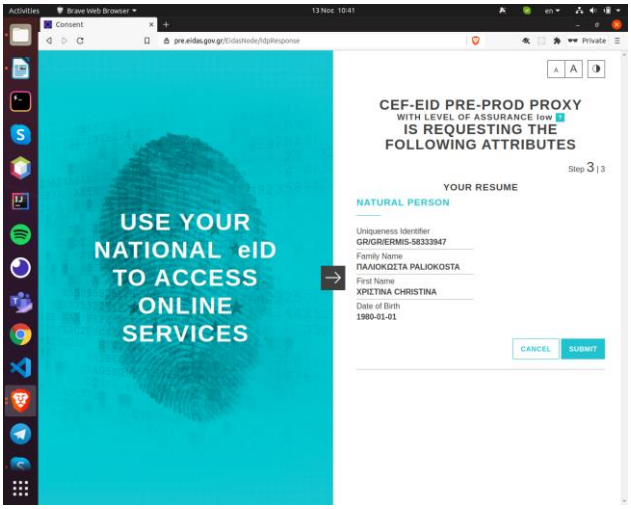



- The user is requested to authenticate over eIDAS

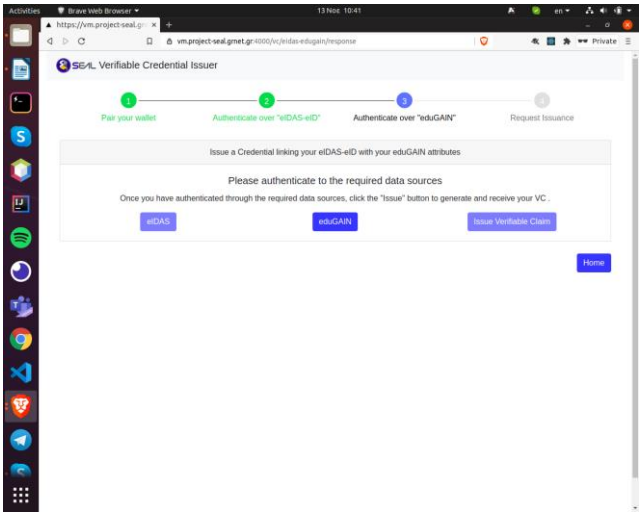


- The user authenticates over eIDAS and consents to the disclosure of their attributes to the SEAL platform

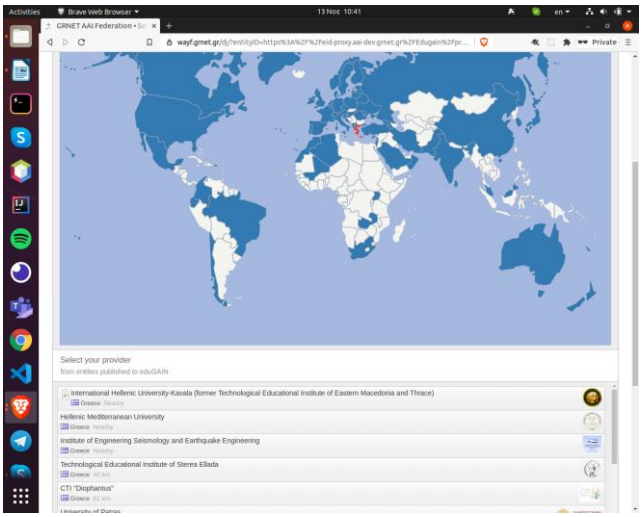


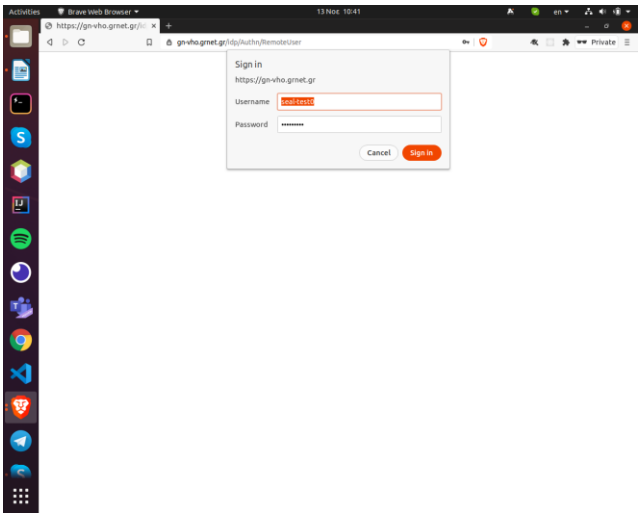




- The user in prompted to authenticate over eduGAIN

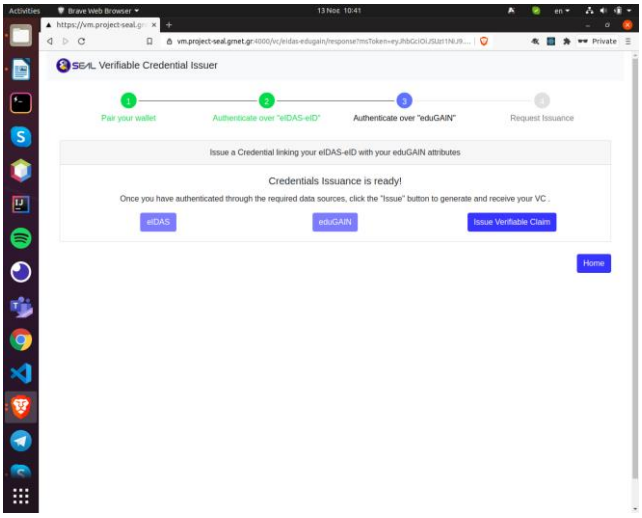


- The user authenticates over eduGAIN

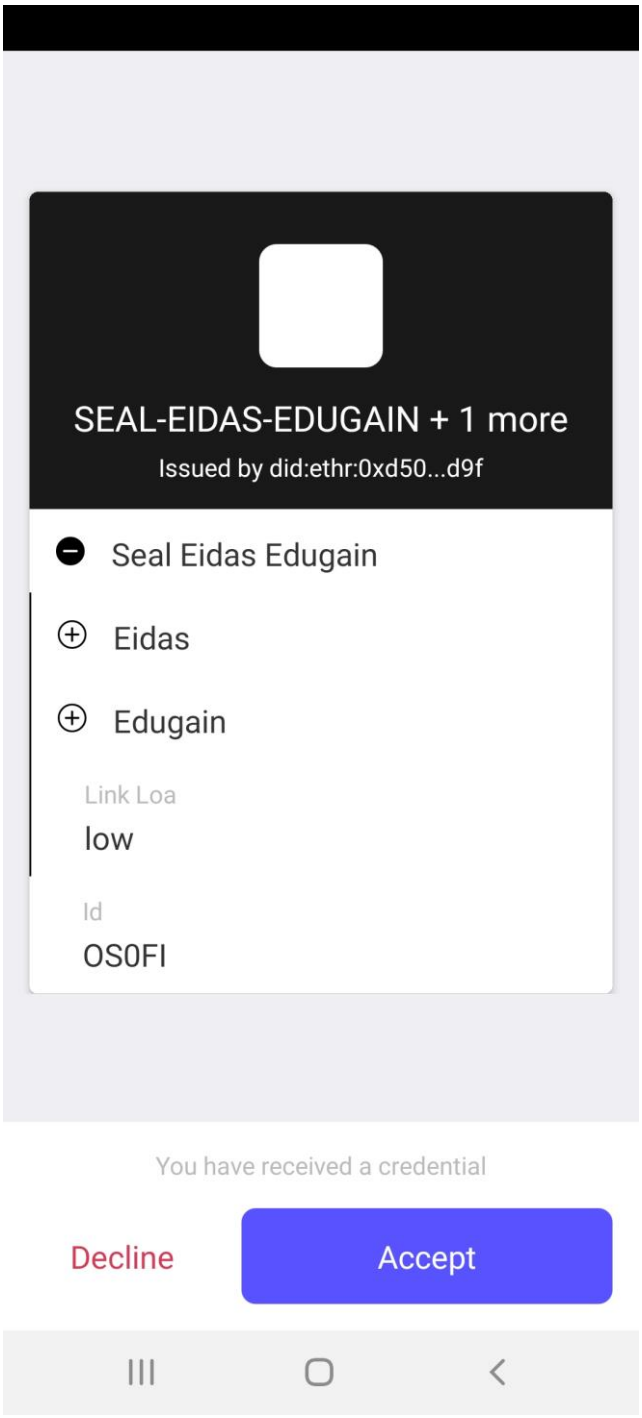


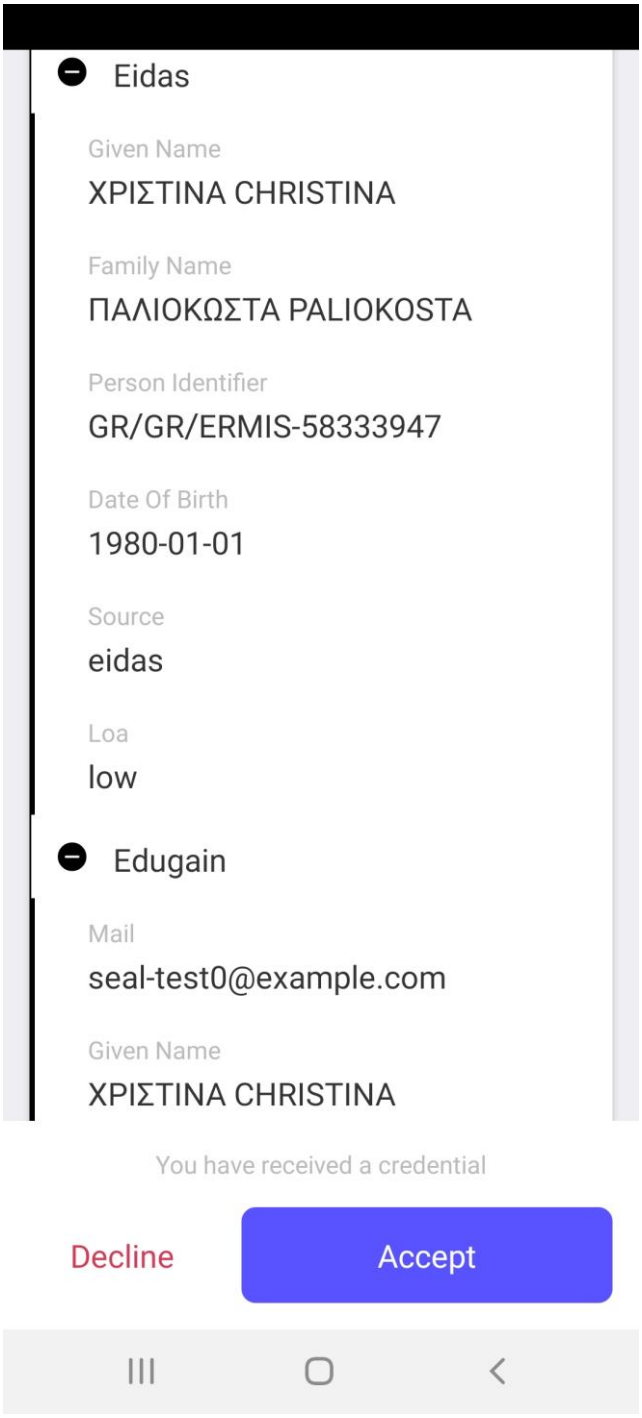




- The user is prompted to request the issuance of a linked Verifiable Credential containing the linked attributes imported from eIDAS and eduGAIN




- The user receives the linked credential on their mobile wallet


SEAL-EIDAS-EDUGAIN + 1 more
Issued by did:ethr:0xd50...d9f
Seal Eidas Edugain
Eidas
Edugain
Link Loa
low
Id
OS0FI
You have received a credential
Decline
Accept


Eidas
Given Name
ΧΡΙΣΤΙΝΑ CHRISTINA
Family Name
ΠΑΛΙΟΚΩΣΤΑ PALIOKOSTA
Person Identifier
GR/GR/ERMIS-58333947
Date Of Birth
1980-01-01
Source
eidas
Loa
low
Edugain
Mail
seal-test0@example.com
Given Name
ΧΡΙΣΤΙΝΑ CHRISTINA
You have received a credential
Decline
Accept

# 4. Conclusions

This deliverable presented the efforts and the results undertaken by the partners during Activity's 5 Task 5.2, to deploy the required process to integrate the SEAL Platform with the eduGAIN federation. As a result, at the end of this task a fully functional instance of the SEAL platform integrated with the eduGAIN federation has been deployed. The metadata of the SEAL platform have been made available to the eduGAIN federation and can be accessed from the eduGAIN registry. As a result, any HEI that accepts this metadata can be used by the users of the SEAL platform to import their academic attributes.

This deliverable presented the efforts and the results undertaken by the partners during Activity's 5 Task 5.2, to deploy the required process to integrate the SEAL Platform with the eduGAIN federation. As a result, at the end of this task a fully functional instance of the SEAL platform integrated with the eduGAIN federation has been deployed. The metadata of the SEAL platform have been made available to the eduGAIN federation and can be accessed from the eduGAIN registry[1]. . As a result, any HEI that accepts this metadata can be used by the users of the SEAL platform to import their academic attributes.

[1] https://met.refeds.org/met/entity/https%253A%252F%252Feid-proxy.aai-dev.grnet.gr%252FEdugain%252Fproxy.xml/

# 5. References


1. Deliverable: SEAL D2.2 - Identities and tokens modules technical analysis. Franciso Aragó. 2020
2. Deliverable: SEAL D3.2 - Technical documentation on modular interfaces for different