M2.2. Deliverable for the e-signature service

Stefan Liström, Konstantinos Karaoglanoglou

18/08/2023

CEF-TC-2020-3

Co-funded by the European Union

Table of Contents

1. Description

The goal of task 2.2 in activity 2 in the EDSSI L2 project was to create an eIDAS compliant eSignature solution, based on eduSign (a Swedish signature service operated by the Swedish Research Council and based on the CEF eSignature building block), and make it available to the HE community.

The eSignature service should be upgraded to be operated at European level allowing users to authenticate using the MyAcademicID proxy (with eIDAS or eduGAIN depending on the level of trust required for the signature) and electronically sign PDF or XML files. Aristotle University of Thessaloniki should make their Trust Certificate Authority available to the eSign service. The service should then be implemented on the Online Learning Agreement platform and the housing platform.

While the first use cases of the portal will be applied to the signature of rental contracts and online Learning Agreements, the development will be future-proofed to fulfil other mobility use cases in the future.

The above description is taken from the Grant agreement of the EDSSI L2 project and this document is explaining how that has been fulfilled.

2. MyAcademicID

To enable an eIDAS compliant signature solution, MyAcademicID[1] was chosen to be used as authentication service for the eduSign integration with the Aristotle University of Thessaloniki and their Trust Certificate Authority. There are several reasons for this choice. First, MyAcademicID is already used in the Erasmus Without Paper Network as authentication service towards, among other services, the Online Learning Agreement Portal[2]. However the most important reason is that MyAcademicID enables the possibility of authenticating with both accounts from the eduGAIN[3] interfederation and accounts from eIDAS nodes.

3. eduSign

3.1. Background

The eduSign e-signature service is used in Swedish higher education and research to facilitate the process of signing digital documents such as PDFs. The service was developed as an open source collaboration between the Swedish Research Council and the Swedish Agency for Digital Government, the service is based on the CEF eSignature building block.

The service consist primarily of three parts:

- The Graphical user interface (also called the frontend) where users sign in to upload documents to sign
  - URL: https://edusign.sunet.se/
  - code: https://github.com/SUNET/edusign-app
- The Signature service (also called the backend)
  - Code: https://github.com/swedenconnect/signservice
- A validation service.
  - URL: https://validator.edusign.sunet.se/
  - Code: https://github.com/swedenconnect/signature-validation

[1] https://myacademic-id.eu/
[2] https://learning-agreement.eu/
[3] https://edugain.org/

The signature service is built in a modular way with open REST APIs. Which means that it is possible to integrate other services directly into the backend of the signature service without having to use the existing eduSign graphical frontend. This is how the OLA portal and the housing contract application are integrated towards the signature service.

The validation service is used to validate both the validity of the signature on the document but also that nothing has been changed in the document since it was signed.

On the Sunet wiki there are user guides[4] for the eduSign service both in Swedish and English.

3.2. EDSSI L2 Development

To be able to reach the goals of the EDSSI L2 project the eduSign service needed to be further developed to work within a broader educational context such as Erasmus.

The upgraded EDSSI L2 eduSign service is currently running parallel with the regular eduSign service offered to the Swedish education and research community.

The updated eduSign service is currently running on the following URLs

- Service frontend:
  - URL: https://test.edusign.geant.org/
  - Code: https://github.com/SUNET/edusign-app/
- Signature backend
  - Code: https://github.com/SUNET/signservice-modules
- Validation service
  - URL: https://validator.test.edusign.sunet.se/
  - Code: https://github.com/SUNET/docker-sigval

4. Harica Integration

4.1. About Harica

HARICA is operated by the IT Center of Aristotle University of Thessaloniki and acts as a Trust Service Provider (TSP) also known as a "Certification Authority", and as a "Qualified" Trust Service Provider (QTSP).

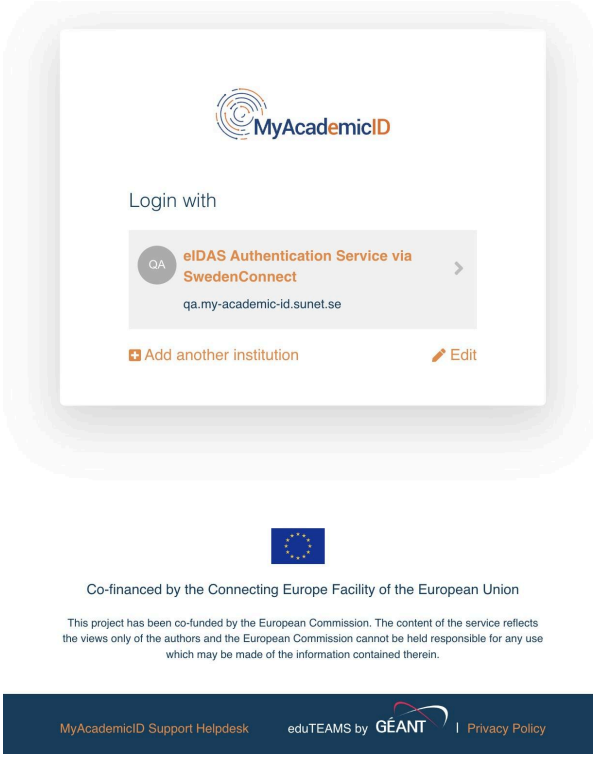
4.2. New signature flow

Below is the new signature flow created within the EDSSI L2 project. It should be noted that it was not part of the project to investigate the business use case of running a signature service including qualified signatures and there was also no funding for running such a service. In that regard, the service created within this project is now available to the HE community but the business use case and funding to offer such a service needs to be taken into account before it can be run in production. As such the current installation of the service is running in a Quality Assurance setup which means that some data and certificates are for testing purposes only. Due to expected changes in the requirements on qualified signature devices in the upcoming revisions in the eIDAS regulation we decided to focus our efforts in this project on delivering signatures with qualified certificates rather than going to the length of offering qualified signatures.

[4] https://wiki.sunet.se/pages/viewpage.action?pageId=78219313

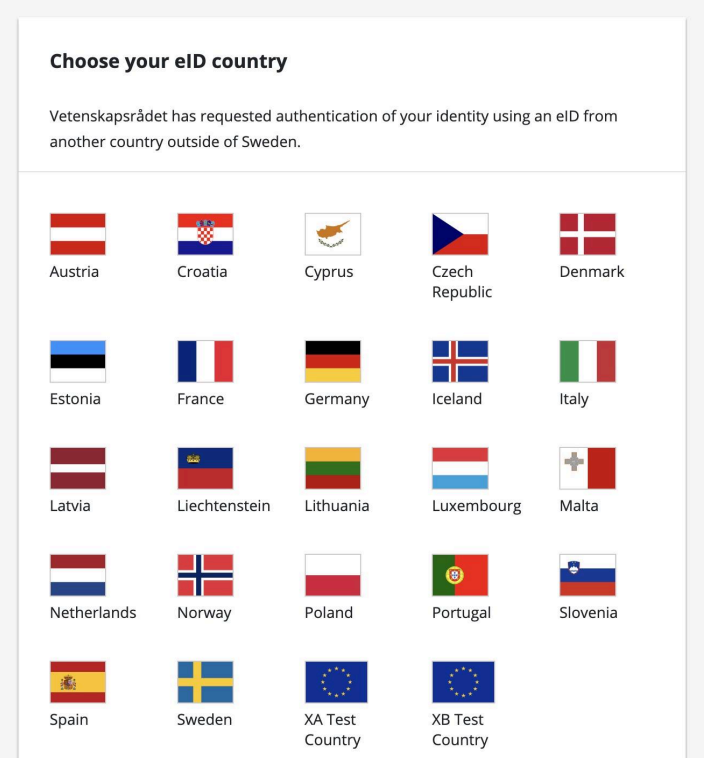
1. **Login at eduSign**
   The initial landing page for eduSign is not much different in the EDSSI L2 version. The main difference is that instead of only being able to login using a discovery service for Identity providers in the eduGAIN interfederation it is now possible to login using MyAcademicID. As mentioned earlier MyAcademicID allows both for users available in the eduGAIN interfederation and eIDAS to login.

2. **Use eIDAS at MyAcademicID to login**
   To get a signature with a qualified certificate a user needs to login using an eIDAS identity as shown below.

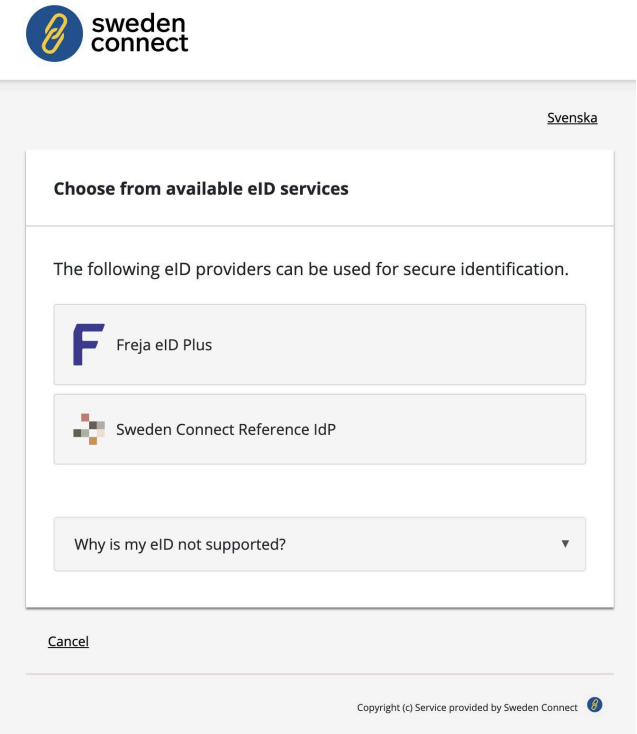


3. **Choose country for correct eIDAS login**
Once eIDAS has been chosen as an authentication method, the user is asked to choose which country identity providers they want to use to login.

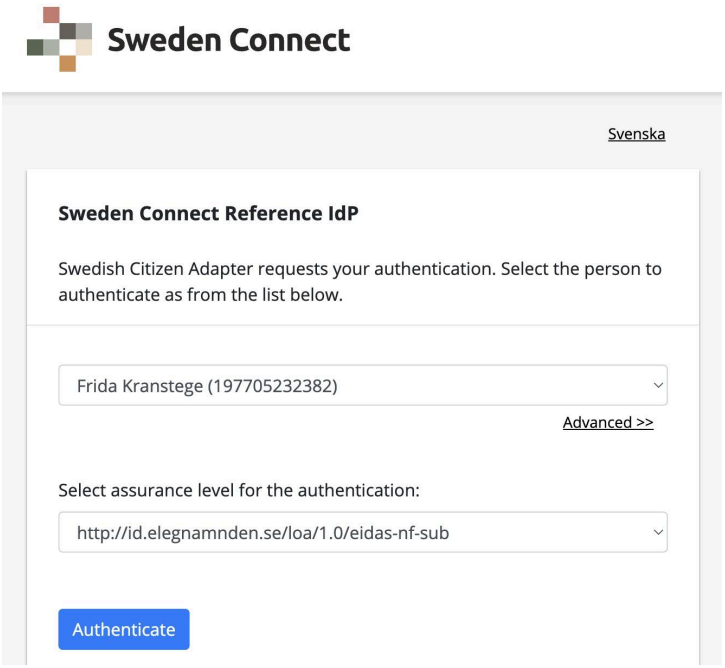
Two major issues with eIDAS today is that there are still several European member states that are not part of the eIDAS infrastructure, which means that citizens from those countries can not use any services integrated with eIDAS. A second problem is that eIDAS is primarily designed to work for national services when a person from one country uses a service in another country. As such many national eIDAS nodes do not include their own national identity providers. Which means that when an international service targeting e.g. Erasmus students in all of Europe use eIDAS; the students from the country the service connects to will not be able to use that service. E.g. the Erasmus Online Learning Agreements portal is connected to the Swedish eIDAS node which means that Swedish students can not use the Online Learning Agreements Portal.



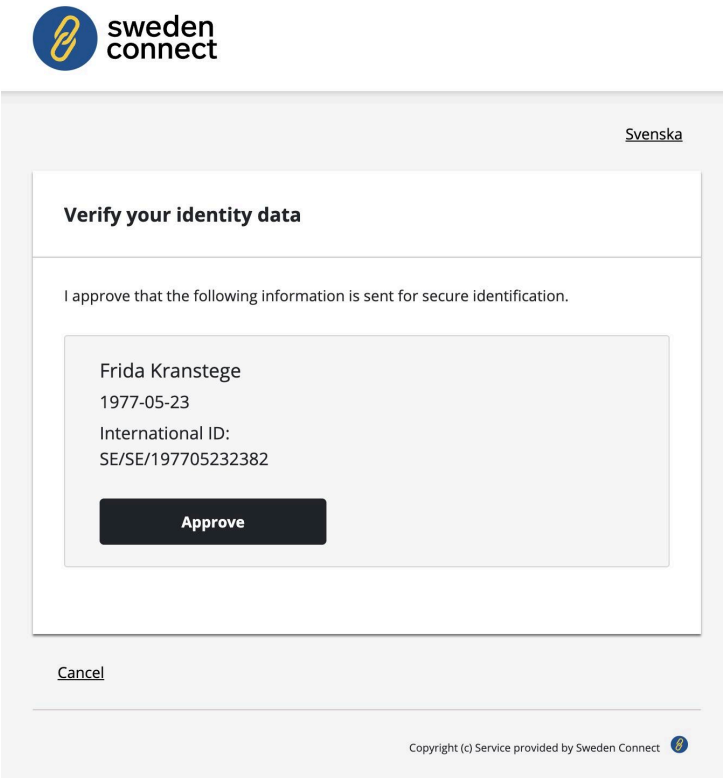
4. **Choose country Identity provider**
In the demo for this report Sweden was chosen and the user is directed to the Swedish Quality Assurance eIDAS node that contains test Identity providers as seen in the image below.



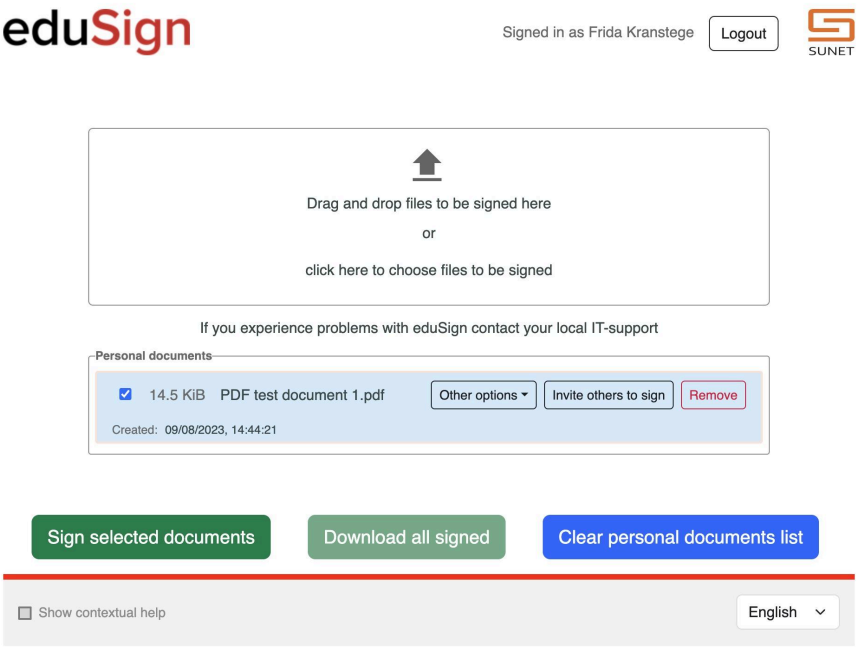
5. **Choose user at the Identity provider**
The user then can select one of the test users. In a production scenario the user would login with their own national eID.



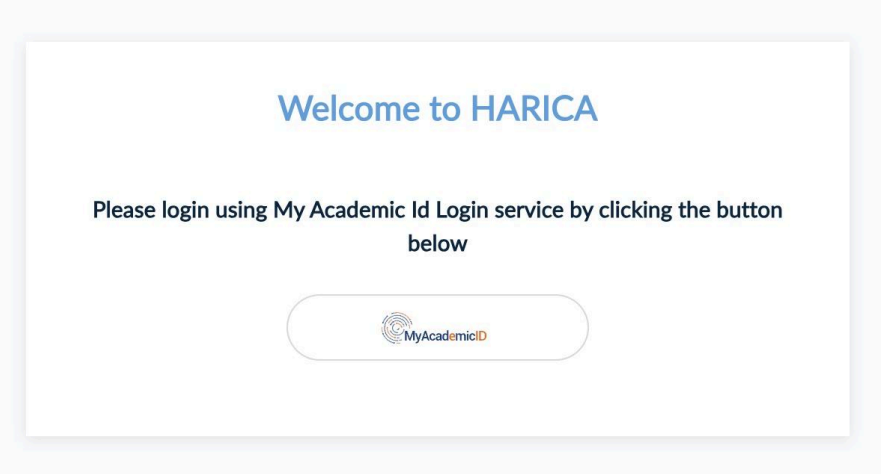
6. **Approve identity data to send to service**
The user has to approve to send certain user specific information to the service in question.



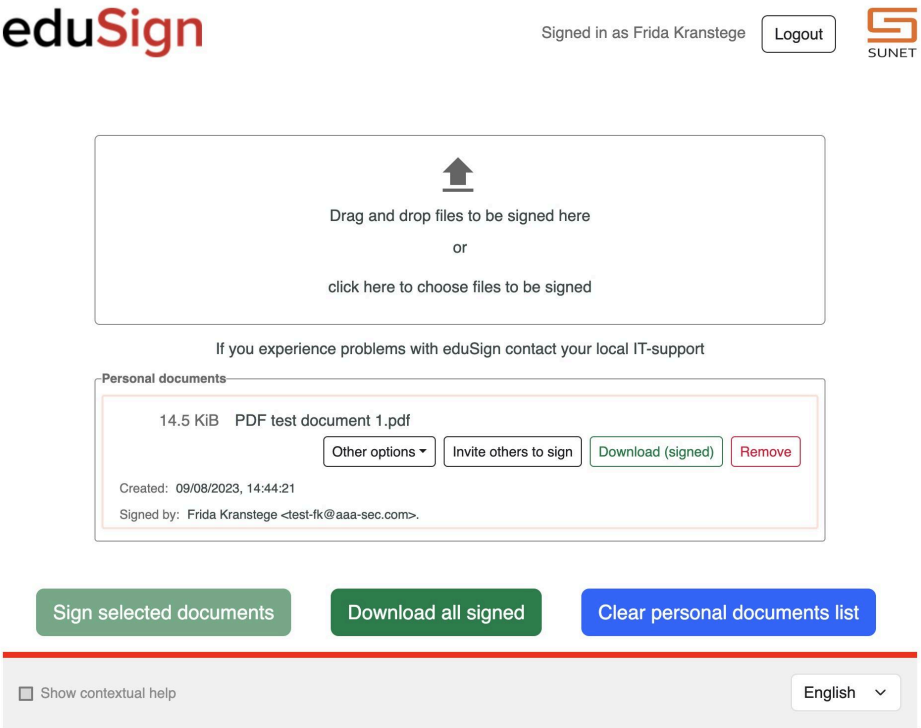
7. **eduSign document upload**
Once the user is in the eduSign system they can upload a document to sign as usual. There is a link to general user guides for eduSign in section 3.1.



8. **Sign document at Harica**
When the user in question wants to sign the document they are directed to Harica to get the qualified certificate for the signature. When directed to Harica they need to choose to authenticate again with MyAcademicID and eIDAS to ensure that they are who they claim to be also from the perspective of the Harica Certificate Authority service.



9. **Final signed document**
Once the user has authenticated again the document is signed with a qualified certificate from Harica and the user can download it from eduSign or invite others to sign it depending on their requirements.



4.3. Results of signed document

The signature page of the document looks the same as other documents signed with the regular eduSign e-signature service. The graphical representation of the signature is however not really the interesting part of the signature. The metadata added with the cryptographic information is the most interesting part and it is also fairly similar as the regular eduSign implementation, the main difference is that the certificate used to sign is a qualified certificate which means that it is part of the EU trust lists that many applications and validation services use to validate signatures.

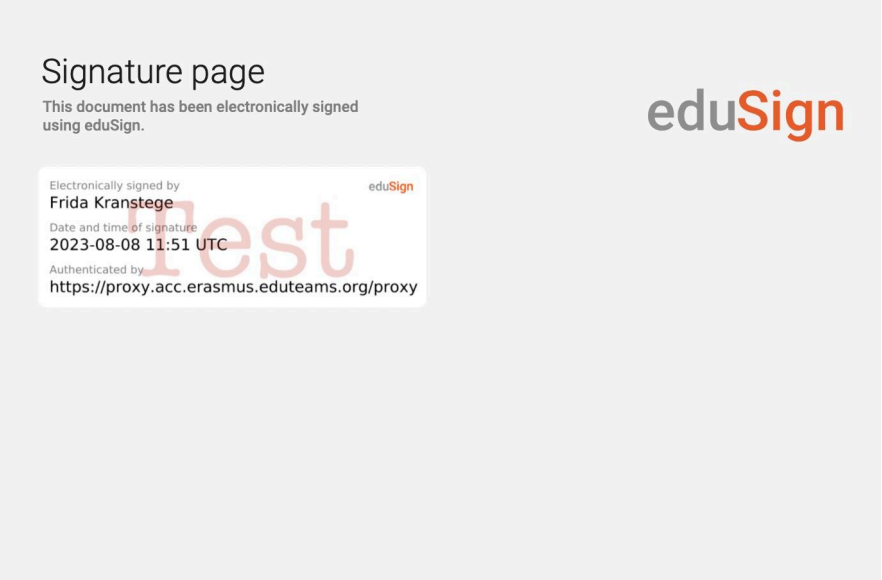


Image of the signature page of a document signed with eduSign

When viewed in e.g. Adobe Acrobat reader the signature is accepted due to the qualified certificate used to sign the document from Harica. Note that the certificate used in the current Quality Assurance setup needs to be manually added to the trust of the application used to view it to be validated correctly.

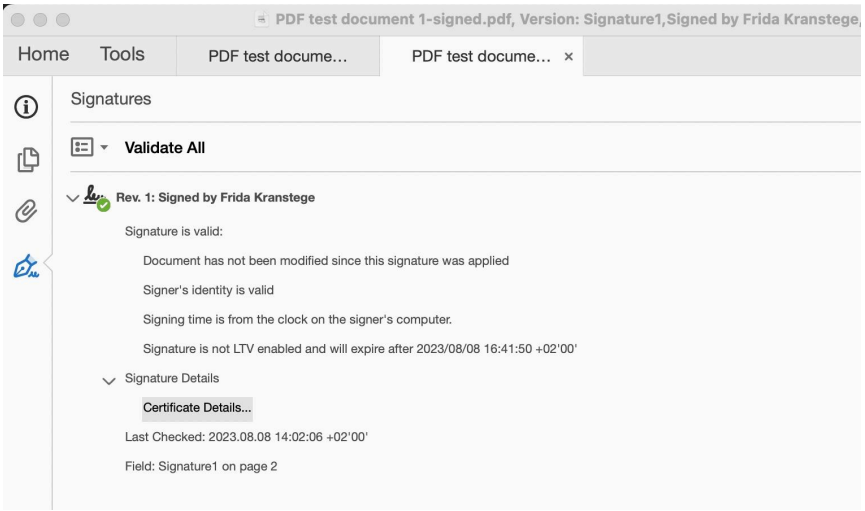
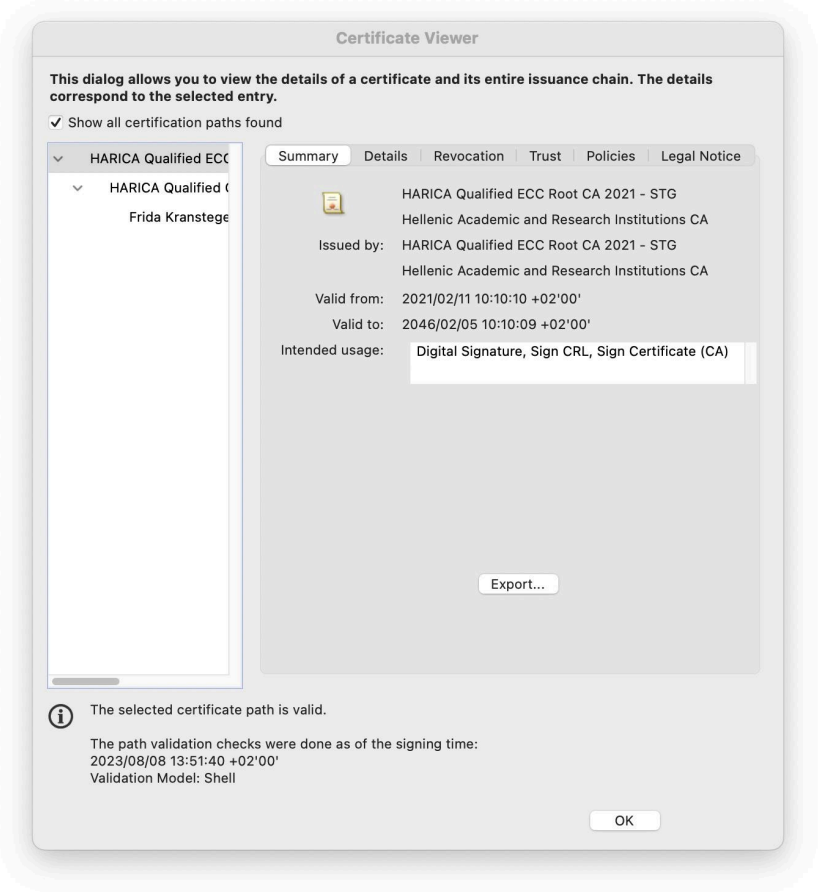


Image of a signed document in eduSign viewed in Adobe Acrobat

Finally the actual Harica certificate used to sign can also be viewed in Adobe Acrobat and in the image below it is possible to see that it is a qualified certificate.

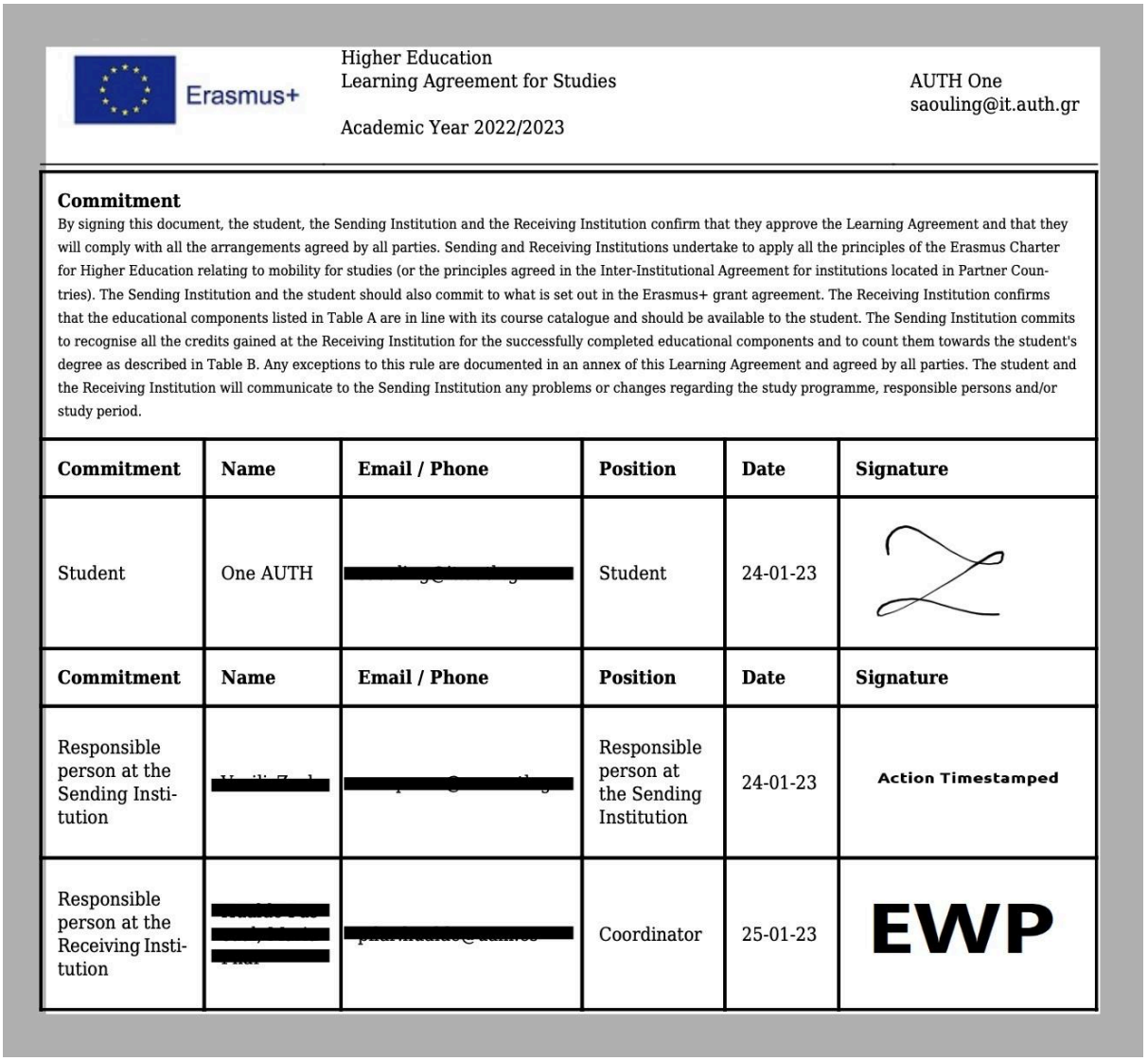


5. OLA integration

One of the goals in the EDSSI L2 project was also to integrate the Online Learning Agreement (OLA) portal[5] towards the eduSign e-signature service to be able to have more than simple signatures on the Online Learning Agreements.

PDF exports from the OLA portal carry a simple e-signature that the user attaches to the document via a signature pad integrated in the application.

[5] https://learning-agreement.eu/



Erasmus+

Higher Education
Learning Agreement for Studies

Academic Year 2022/2023

AUTH One
saouling@it.auth.gr

Commitment

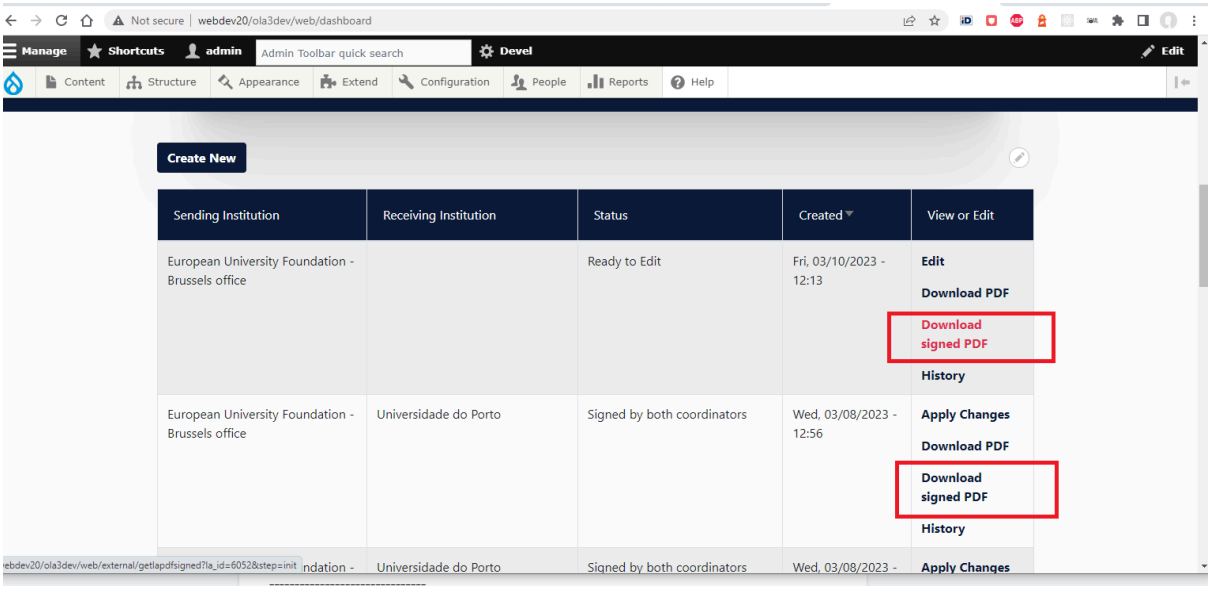
By signing this document, the student, the Sending Institution and the Receiving Institution confirm that they approve the Learning Agreement and that they will comply with all the arrangements agreed by all parties. Sending and Receiving Institutions undertake to apply all the principles of the Erasmus Charter for Higher Education relating to mobility for studies (or the principles agreed in the Inter-Institutional Agreement for institutions located in Partner Countries). The Sending Institution and the student should also commit to what is set out in the Erasmus+ grant agreement. The Receiving Institution confirms that the educational components listed in Table A are in line with its course catalogue and should be available to the student. The Sending Institution commits to recognise all the credits gained at the Receiving Institution for the successfully completed educational components and to count them towards the student's degree as described in Table B. Any exceptions to this rule are documented in an annex of this Learning Agreement and agreed by all parties. The student and the Receiving Institution will communicate to the Sending Institution any problems or changes regarding the study programme, responsible persons and/or study period.

Commitment	Name	Email / Phone	Position	Date	Signature
Student	One AUTH	[redacted]	Student	24-01-23	
Commitment	**Name**	**Email / Phone**	**Position**	**Date**	**Signature**
Responsible person at the Sending Institution	[redacted]	[redacted]	Responsible person at the Sending Institution	24-01-23	Action Timestamped
Responsible person at the Receiving Institution	[redacted]	[redacted]	Coordinator	25-01-23	EWP

Currently OLA documents are signed with simple e-signatures

In the EDSSI L2 project Aristotle University of Thessaloniki (that are maintaining the OLA portal) integrated their staging environment towards the eduSign signature service backend using the API. This was successful and it has now been shown that it is possible to show that the authenticity, identity and authentication of the signatory can be proven and the integrity of the signed document is intact.

The procedure is initiated by the user from the OLA portal by clicking the Download signed PDF action button available next to the correspondent Learning Agreement, and after a sequence of steps that handle the backend communications (detailed below), a signed pdf document is returned to the user displaying the authenticity, identity and authentication of the signatory, and the overall integrity of the document.



User initiating the procedure from the OLA portal

1. Prepare PDF document - POST /v1/prepare/{profile}
Post request to the `prepare` endpoint of the API.
Post fields:

- the pdf document in base64 form
- list of signer idp attributes ('urn:oid'), the values of which will be posted in a next step
- the url of the idp

Result:

- a reference to the pdf document (an id, e.g. "ef49b295-2ff7-43fc-b62d-2016be9b4623")
- the signature properties requirements for its visible representation - needed in a next step (e.g. the final signer idp attributes ('urn:oid'), the position of the signature)

2. Create a SignRequest message - POST /v1/create/{profile}
Post request to the `create` endpoint of the API.

Post fields:

- the reference to the pdf document (received in step 1)
- the signature properties requirements for its visible representation (also received in step 1)
- a return url, the url where the esign service will post the final signed pdf
- the requested signer attributes values (information leak here: our service will send user info from our Idp to their esign service. we leak the 'displayName')

Result:

- the sign request in xml (base64)
- the request id
- the request url that the next step will redirect the user to (i.e. the "https://signservice.edusign.sunet.se/cs-sigserver/request")

3. Submit the signing request - POST destination url (from the previous step)
The user submits the final post to the signing service, given the return values from the 'create' step.

An html form is created for the user to make this last post (usually the user does not have to do anything, as javascript onload will submit the form on behalf of the user).

4. User Authentication

The user is being redirected by the esign service to login to their idp.

The idp must release certain attributes to the esing service:

- displayName
- eduPersonPrincipalName
- givenName
- eduPersonAssurance
- sn
- mail

Result:

- the esign service compares the user's attributes given by OLA in the previous step with the ones returned by the IdP (i.e. the 'displayName'), and proceeds to the addition of the digital signature.

5. esign service posts back signed response to OLA
POST to the destination url from the previous step. The esign service posts back the sign response.

The post fields:

- the request id
- the sign response in base64 form

6. Process the sign response - POST /v1/process
Post request to the `process` endpoint of the API.

Post fields:

- the sign response, from previous step
- the request id

Result:

- the signed document in base64 form

7. User gets the signed document

User gets the signed document. The pdf document is decoded from the base64 form and we return it to the user.

Erasmus+

Higher Education
Learning Agreement for Studies

Academic Year 2023/2024

[redacted]

Commitment

By signing this document, the student, the Sending Institution and the Receiving Institution confirm that they approve the Learning Agreement and that they will comply with all the arrangements agreed by all parties. Sending and Receiving Institutions undertake to apply all the principles of the Erasmus Charter for Higher Education relating to mobility for studies (or the principles agreed in the Inter-Institutional Agreement for institutions located in Partner Countries). The Sending Institution and the student should also commit to what is set out in the Erasmus+ grant agreement. The Receiving Institution confirms that the educational components listed in Table A are in line with its course catalogue and should be available to the student. The Sending Institution commits to recognise all the credits gained at the Receiving Institution for the successfully completed educational components and to count them towards the student's degree as described in Table B. Any exceptions to this rule are documented in an annex of this Learning Agreement and agreed by all parties. The student and the Receiving Institution will communicate to the Sending Institution any problems or changes regarding the study programme, responsible persons and/or study period.

Commitment	Name	Email / Phone	Position	Date	Signature
Student	[redacted]	[redacted]	Student	19-01-23	
Commitment	**Name**	**Email / Phone**	**Position**	**Date**	**Signature**
Responsible person at the Sending Institution	[redacted]	[redacted]	Responsible person at the Sending Institution	19-01-23	Action Timestamped
Responsible person at the Receiving Institution	[redacted]	[redacted]	coordinator	19-01-23	EWP

Signature page

This document has been electronically signed using eduSign.

eduSign

Electronically signed by [redacted]
eduSign
Date and time of signature
2023-03-08 07:11 UTC
Authenticated by
https://login.auth.gr/saml2/idp/metadata.php
Test

The document signed with eduSign returned to the user

6. Housing application integration

The housing application platform proof of concept has been integrated with the eduSign back-end signature service API. This allows users of the housing application to sign housing contracts with the help of the eduSign e-signature service.

The results of the work with the housing application and the integration towards the eduSign service is explained in more detail in the Milestones report for Task 2.5 - Student housing Web-Application in Activity 2.

7. Summary

In summary, the existing eduSign e-signature service has been upgraded in the EDSSI L2 project to work on a European level where users can sign with both identities that are part of the eduGAIN interfederation and their national eIDAS identities. Even though the project did not reach the ambition of having qualified signatures, the eIDAS signatures done in the EDSSI L2 version of eduSign are now done with qualified certificates from the Harica Certificate Authority.

The project did also show that it is possible to integrate both the Online Learning Agreement portal and a completely new application such as the housing contract application with the eduSign e-signature service to achieve more than simple e-signatures according to the eIDAS regulation.

www.edssi.eu