Student and Citizen Identities Linked

D5.1 Operational and Technical Documentation of Platform Integration with eIDAS node

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

Related Activity	Act 5	**Document Reference**	D5.1
Related Deliverable(s)	D2.2, D3.2	**Dissemination Level (*)**	PU
Lead Organization	UAegean	**Lead Author**	Petros Kavassalis
Contributors	UAegean	**Reviewers**	Victoriano Giralt, UMA
			Francisco Aragó,UJI

Keywords:

eIDAS, 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.

(*) Dissemination level.-**PU**: Public, fully open, e.g. web; **CO:** Confidential, restricted under conditions set out in Model Grant Agreement; **CI:** Classified, **Int =** Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

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

Document History			
Version	Date	Change editors	Changes
0.1	06/11/2020	Petros Kavassalis University of the Aegean	version for partner 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
DG DIGIT	Directorate-General for Informatics
Dx.y	Deliverable number y belonging to WP x
EC	European Commission
IdP	Identity Provider
MDS	Minimum Data Set
MS	Member State
OIDC	OpenID Connect
OVF	Open Virtual Format
SP	Service Provider
WP	Work Package

1.Introduction

The SEAL project has developed and deployed the required process for integration of the SEAL platform developed in Activity 3 (Linking Service Core Platform and modular interfaces development) with the eIDAS Network. The process permits the identity bootstrapping and authentication (both for the user interfaces and for the service provider interfaces) via the eIDAS Network. Specifically, the deployed process integrates the SEAL platform with the Greek eIDAS Node, as was the preferred option during the project's design. In this capacity, the interoperability testing in both production and pre-production environments with eIDAS eID identities from all the connected Member States connected to the Greek eIDAS node is enabled.

1.1 Purpose of the document

This document presents the efforts undertaken and the results achieved by the partners during Activities' 5 (Linking Service deployment and integration for cross-border testing) Task 5.1 (Deployment of SEAL Platform and integration with eIDAS Network). These presented efforts were required to integrate the SEAL Platform with the elDAS Network and specifically with the Greek eIDAS Node (in both production and pre-production environments).

1.2 Relation to other project work

The work presented here was carried out as part of the SEAL Activity 3 (Linking Service Core Platform and modular interfaces development) to produce a platform for managing and verifying linked identities -- following the technical specification produced by Activity 2 (Linking Service Core Platform and Interfaces Design).

1.3 Structure of the document

This document is structured in 2 major chapters:

Chapter 2 Presents the technical integration of the SEAL platform with the eIDAS Network

Chapter 3 Reports on the conclusions of the integration efforts

2. SEAL eIDAS Technical Integration

This section provides a brief overview of the eIDAS-eID network architecture and infrastructure and provides an overview of the technical architecture and integration steps of SEAL with eIDAS-eID.

2.1 The SEAL Service as a Service Provider towards the eIDAS network

The SEAL platform acts as a Service Provider (SP) to the eIDAS network. Specifically, the SEAL platform is capable of authenticating users using their national eIDs over the eIDAS-eID network by integrating with the Greek eIDAS node.

2.1.1 eIDAS Infrastructure

2.1.1.1 eIDAS Regulation

The eIDAS Regulation No 90/2014[1] addresses the electronic identification and recognition and governance of trust services for electronic transactions in the internal market, so as to boost confidence and trust towards digital world by adopting the following principles among others:

- mutual acceptance of national e-ID;
- common framework for secure interaction between citizens, companies and public administration;
- interoperability solutions reduce fragmentation of digital market;
- technological neutrality is required in order to avoid security requirements to be restricted to specific technological solutions;
- interoperability of digital signatures is necessary to increase trust in business online transactions;
- the level of trust in national electronic identity can be defined by a certain e-ID quality level;
- each member state must define one or more supervision organisations in order to verify the adoption of the Regulation and to interact with the European Commission;
- supervision organisations should interact with authorities for data privacy, so as to avoid abuses and misuse of personal data.

The eIDAS Regulation Implementing Act of 8 September 2015[2] has laid down requirements on the implementation of the regulation in European member states.

2.1.1.2 Proxy model architecture of the eIDAS-Network

The eIDAS interoperability architecture is strongly influenced by the outcomes of the STORK project, building a federation for the governance of electronic identity inside the single digital market.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782373783&uri=OJ:JOL_2015_235_R_0001

Specifically, the architecture defines a national gateway, called the eIDAS-Node, for each member state involved. These eIDAS nodes serve as the single point of contact for all transactions with eIDs originating from the member state and are composed of the following two components (serving different roles during an authentication process, as depicted in the following figure):

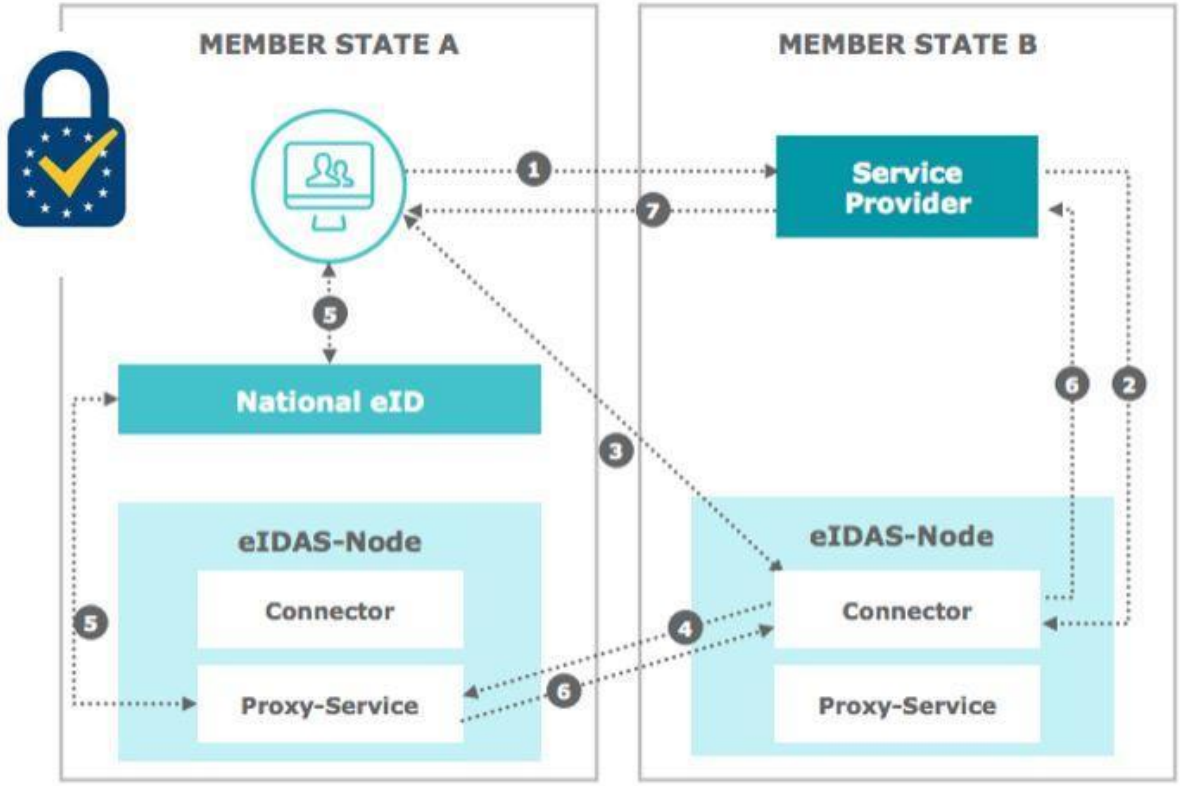

Figure 1: eIDAS Network Architecture

- eIDAS-Connector, if it requests a cross-border authentication for a person;
- eIDAS-Proxy-Service, if it provides cross-border authentication for a person.

A typical eIDAS authentication flow is as follows:

1. An eIDAS Service Provider (SP) asks for user authentication using the eIDAS-eID network. The SP does so by requiring one or more qualified eIDAS attributes of the citizen in order to provide their services.
2. The authentication request is sent from the SP to the eIDAS-Connector it is configured to interact with,
3. The user is queried about their country of origin
4. The eIDAS Node connector, contacts the eIDAS proxy-service of the user's country of origin
5. Next, the eIDAS proxy-service delegates authentication to (one of the available) eIDAS Identity Provider (eIDAS-IdP). Authentication takes place over the users national e-ID solution. Authentication may be performed with different technologies and security assurance, depending

on the legally accredited e-ID systems of the member state. After the user authentication the user attributes are propagated back to the eIDAS proxy-service

6. Next, the eIDAS proxy service transfers the user's attributes to the eIDAS Node Connector that requested them in step 4
7. Finally, the eIDAS Node connector receives and propagates the user's attributes to the SP that requested them in step 1

2.1.1.3 Middleware architecture of the eIDAS-Network

An alternative model for the eIDAS-Network is based on the eIDAS-Middleware-Service component as an alternative to the eIDAS-Proxy-Service. In this case, the member state has to provide a middleware to other member states, which is operated by the operators of the eIDAS-Connectors, in order to interact directly with the local e-ID scheme.

The member state notifying a middleware-based eID is responsible to provide the necessary Middleware. According to the regulation in such a case the member state must meet the following requirements:

1. provide the middleware as a pre-configured virtual machine in Open Virtualization Format (OVF);
2. make it configurable via scripts for both test and production environments;
3. should expose logging information via a syslog-interface and health information via an SNMP-interface;
4. build it in such a way that the host is in charge of performing the generation of cryptographic keys;
5. provides the middleware to DG DIGIT for bundling with CEF implementation and to other member states, if requested;
6. document instructions for how to access administrative roles, install keys and certificates and configuration steps;
7. ensure the middleware is supported by its notifying member state.

In this scenario, there is a one-to-one correspondence between eIDAS-Connector and eIDAS-Middleware-Service.

2.1.2 Greek eIDAS Node

Greece supports the eIDAS network in both production and pre-production environments. Specifically, in Greece two eIDAS nodes are deployed (one for each environment) running eIDAS node software at version 1.4.3[3], maintained by the Greek Ministry of Digital Governance[4]. The metadata urls of the nodes are the following:

- pre-production: https://pre.eidas.gov.gr/EidasNode/ConnectorResponderMetadata

[3] https://ec.europa.eu/cefdigital/wiki/download/attachments/82773765/eIDAS-Node%20Installation%20Manual%20v1.4.3.pdf?version=1&modificationDate=1536823008963&api=v2

[4] https://mindigital.gr/

- production: https://eidas.gov.gr/EidasNode/ConnectorResponderMetadata

The existing governance policy for the eIDAS nodes allows both public and private Service Providers (SPs) to connect to the Greek eIDAS nodes, enabling them to seamlessly authenticate cross-border users from any of the connected Member States (MS). Greece, at the moment of this report, does not have a notified eID scheme. This results in the situation that although citizens from any third party MS connected to the Greek node can authenticate to any SP service connected to it, Greek citizens are unable to authenticate to SP service connected to other MS´s eIDAS nodes (at a production level). In details, at the moment the connectivity of the Greek eIDAS node reported by the Ministry of Digital Governance is as follows[5]:

- pre-production:
  - Greece
  - Cyprus
  - Estonia
  - Spain
  - Italy
  - Lithuania
  - Portugal
  - Malta
  - Poland
  - Slovenia
- production:
  - Estonia
  - Italy
  - Lithuania
  - Greece
  - Spain

Additionally, we report that the Greek eIDAS strategy is being revisited as part of the creation of a national eID scheme (this is also an immediate result of the fact that the custody of the Greek eIDAS nodes has been passed over to the Greek Ministry of Digital Governance). Thus, it is expected that in the near future the connectivity of the Greek eIDAS node will improve significantly.

[5] The Ministry of Digital Governance is currently updating the Greek eIDAS node infrastructure, as a result the reported connections in this document are subject to change

2.2 SEAL eIDAS Integration Architecture and Deployment

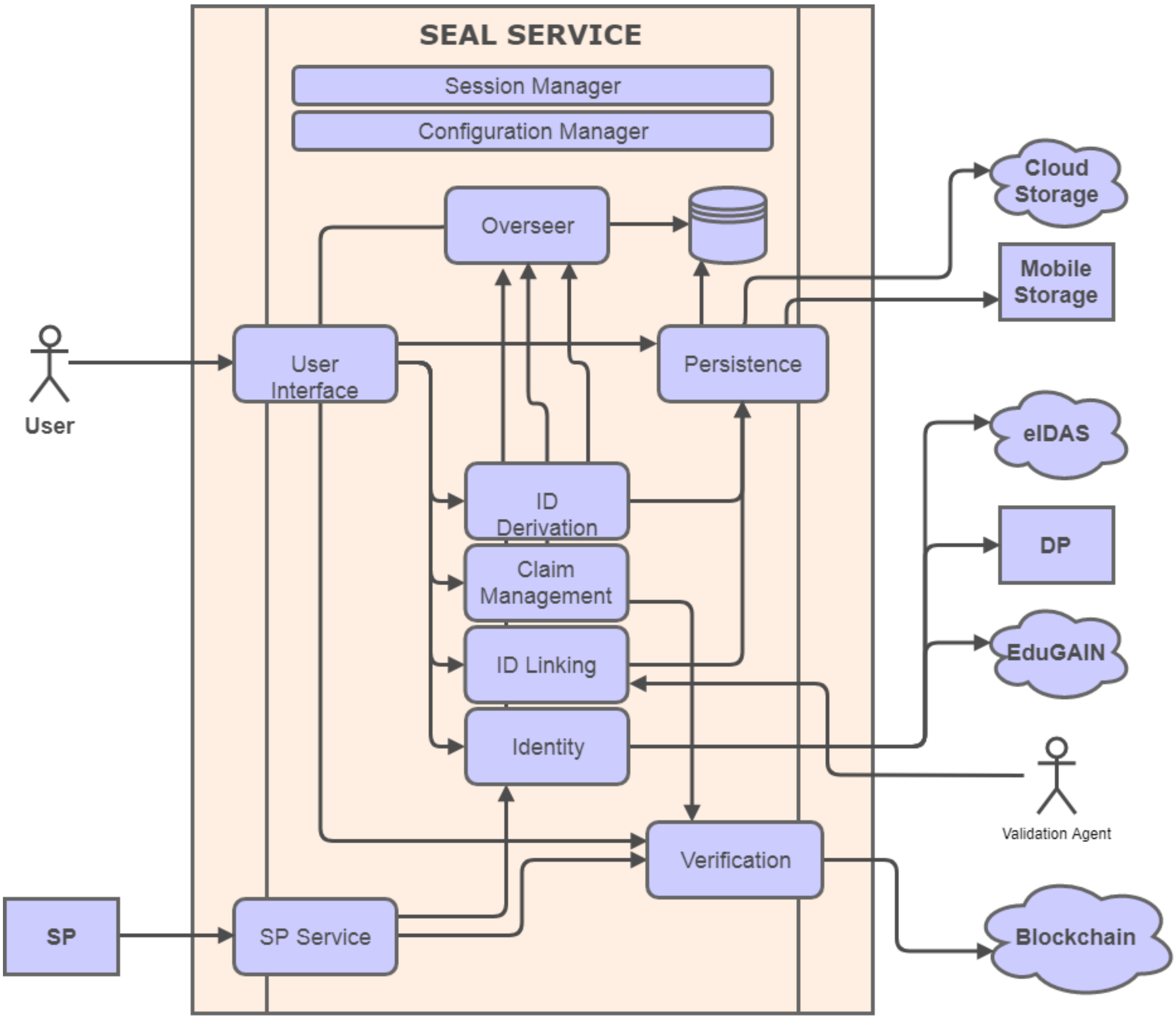

Figure 2: SEAL Service architecture diagram

The overall architecture of the SEAL platform can be seen in Figure 2. Interfacing to the Identity Sources (like 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 eIDAS Identity Module

The SEAL Platform integration with the eIDAS Network takes place using a software module called the "eIDAS Identity module". This module supports the interface to the eIDAS network by connecting to the Athens ESMO Gateway[6] (an OIDC eIDAS proxy maintained by the Ministry of Education in Greece). The technical details of this interface are fully described in D2.2 and D3.2.

[6] https://esmo-gateway.eu/about/

Specifically, the “eIDAS Identity module” implements an internal protocol towards the SEAL platform (for more details please review D2.2 and D3.2) and consumes an OpenID Connect (OIDC) interface from the Athens ESMO Gateway which acts as a proxy to the Greek eIDAS node[7], allowing the querying of the eIDAS minimum dataset (MDS) as OIDC scopes.

In order to authenticate users over eIDAS-eID the “eIDAS identity module” submits an authorization request to the Athens ESMO GW using the authorization code flow as that is defined in RFC 6749[8]. The complete flow is shown in Figure 3 below.

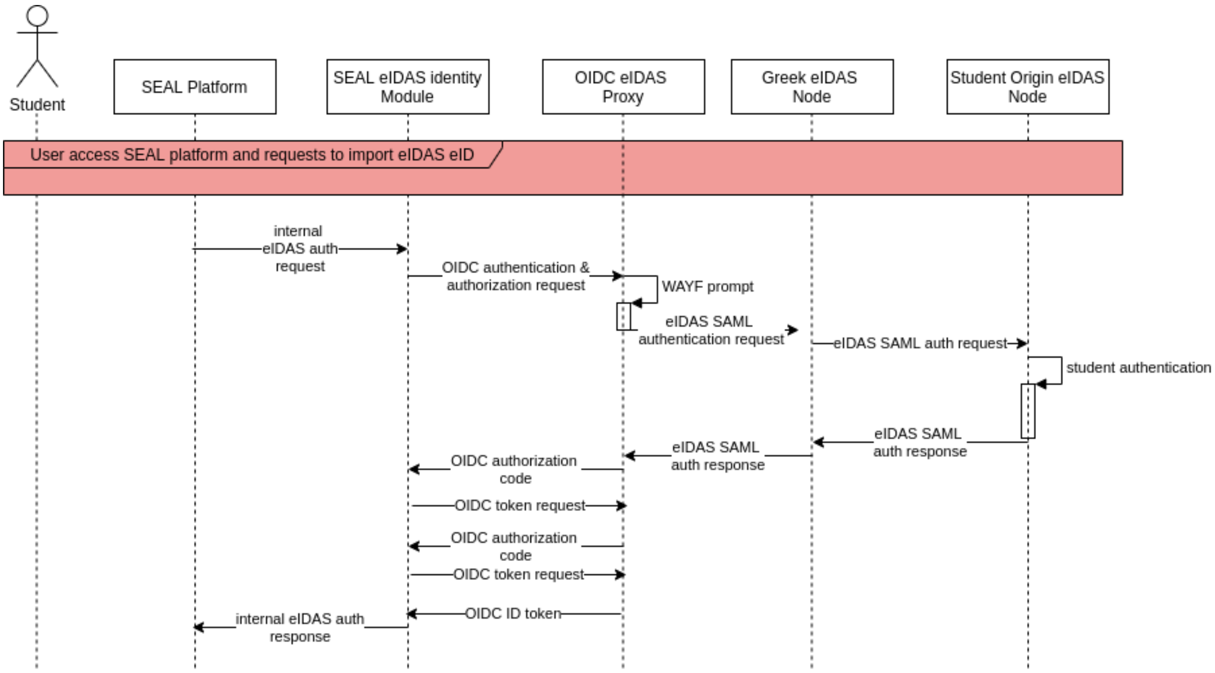

Figure 3: SEAL eIDAS authentication

The SEAL eIDAS identity module has been designed for the specific Greek eIDAS connection infrastructure case. Other modules could be developed to connect to eIDAS though other MS infrastructures if deployed in other countries.

2.1.4 SEAL Platform deployment and eIDAS Authentication connection (Pre-production and Production)

The SEAL eIDAS identity module (eidas-idp) has been implemented in Java code using Spring boot. The related github repository can be found at https://github.com/EC-SEAL/eidas-idp-ms, where the code updates are done in the default branch (development).

[7] In more details the Athens ESMO Gateway, integrates to the Greek eIDAS Node via GRNet eIDAS proxy (https://eid-proxy.aai-dev.grnet.gr/.well-known/openid-configuration), for the purposes of SEAL. The integration takes place over OIDC.

[8] https://tools.ietf.org/html/rfc6749#section-4.1

The following environment variables are used:

- EIDAS_PROPERTIES, comma (“,”) separated eIDAS attributes friendly names used to request the corresponding attributes from the connected eIDAS node
- AUTH_DURATION, integer denoting in milliseconds the authentication session to the eIDAS node proxy
- SESSION_MANAGER_URL, absolute url of the SEAL platform session manager
- KEY_PASS, password for the SSL certificate used
- KEYSTORE_PATH, path to the keystore holding the SSL certificate
- STORE_PASS, keystore password
- RESPONSE_SENDER_ID, string denoting the name of the eIDAS microservice in the SEAL platform
- SEAL_EXPOSE_URL, string containing the url path for the module metadata
- SEAL_ENTITY_ID, the id of the module to include in the metadata
- SEAL_DEFAULT_NAME, default name of the module to include in the metadata
- CLIENT_ID, the id in the OIDC connection for the module
- CLIENT_SECRET, the secret of the OIDC client
- ISSUER_URI, the uri of the OIDC server

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/r/endimion13/seal-eidas-idp)

2.2.1.1 Pre-production deployment

The pre-production SEAL platform contains a fully functional instance of the “eIDAS identity module” that is connected to the Greek pre-production eIDAS node. The SEAL pre-production platform containing this identity module is deployed at https://vm.project-seal.eu/

The integration with the pre-production Greek eIDAS node has been completed successfully and all functional tests have been successful.

2.2.1.2 Production Deployment

The production SEAL platform also contains a fully functional instance of the “eIDAS identity module”. However, this instance is connected to the Greek production eIDAS node. The production platform containing this identity module is deployed at https://vm.project-seal.grnet.gr/

3. Conclusions

This deliverable presented the efforts and the results undertaken by the partners during Activity's 5 Task 5.1, to deploy the required software to integrate the SEAL Platform with the elDAS Network and specifically to integrate the SEAL platform with the Greek eIDAS Node (in both production and pre-production environments).

As a result, at the end of this task a fully functional instance of the SEAL platform integrated with the Greek eIDAS Node has been deployed in both pre-production and production environments. This results in the SEAL platform being ready for interoperability testing in preproduction and production with elDAS identities from all the Member States available to the Greek eIDAS Node (in both environments).