



Co-financed by the Connecting Europe Facility of the European Union



increasing tRust with eld for Developing buSiness

D3.3 eIDAS node report

Document Identification			
Status	Final	Due Date	31/12/2020
Version	1.0	Submission Date	22/12/2020

Related Activity	Act 3	Document Reference	D3.3
Related Deliverable(s)	D2.1, D2.2		
Lead Participant	UAEGEAN	Lead Author	Petros Kavassalis (UAEGEAN)
Contributors	KOMPANY	Reviewers	1 st reviewer – Dominik Tiefenbacher (KOMPANY)
			2 nd reviewer - Juan Carlos Pérez Baún, ATOS

Keywords
eIDAS, SSO,OIDC

This document is issued within the frame and for the purpose of the GRIDS 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/A2019/1926018; Action nº 2019-EU-IA-0044. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

This document and its content are the property of the GRIDS Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the GRIDS Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the GRIDS Partners.

Each GRIDS Partner may use this document in conformity with the GRIDS Consortium Grant Agreement provisions.

Document Information

List of Contributors	
Name	Partner
Petros Kavassalis	UAEGEAN
Nikos Triantafyllou	UAEGEAN
Dominik Tiefenbacher	KOMPANY
Peter Bainbridge-Clayton	KOMPANY

Document History			
Version	Date	Change editors	Changes
0.1	14/12/2020	Petros Kavassalis	first version
0.2	16/12/2020	Juan Carlos Pérez Baún (ATOS)	Proof-reading + Content check
0.3	17/12/2020	Dominik Tiefenbacher (KOMPANY)	Proof-reading + Content check
0.4	19/12/2020	Peter Bainbridge-Clayton (KOMPANY)	Content check
1.0	22/12/2020	Carmen San Román (ATOS)	Final quality assurance review

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	UAEGEAN	14/12/2020
Peer reviewers	ATOS, COMPANYY	19/12/2020
Quality Manager	ATOS	22/12/2020

Document name:	D3.3 eIDAS node report	Page:	2 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

Table of Contents

Document Information.....	2
Table of Contents	3
List of Figures.....	4
List of Acronyms	5
Executive Summary	6
1 Introduction.....	7
1.1 Purpose of the document	7
1.2 Reference to other project work	7
1.3 Structure of the document	7
2 GRIDS Architecture Overview.....	8
2.1 The role of the SP Hub within the GRIDS architecture	9
3 SP Hub Architecture and components	10
3.1 SP Hub Components.....	10
4 The functionality of the SP Hub.....	12
5 Deployment	15
6 Testing through GR and ES credentials	17
6.1 Greek User Authentication	17
7 Conclusions.....	20
8 References	21

Document name:	D3.3 eIDAS node report	Page:	3 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

List of Figures

<i>Figure 1: GRIDS architecture overview</i>	8
<i>Figure 2: GRIDS SP Hub architecture</i>	10
<i>Figure 3: GRIDS authentication flow</i>	12
<i>Figure 4: Mock SP authenticate prompt</i>	17
<i>Figure 5: SP Hub WAYF interface</i>	18
<i>Figure 6: Greek pre-production eIDAS IdP authentication</i>	18
<i>Figure 7: Greek pre-production eIDAS Node consent form</i>	19
<i>Figure 8: Mock SP authenticated user interface</i>	19

Document name:	D3.3 eIDAS node report	Page:	4 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

List of Acronyms

Abbreviation / acronym	Description
BAA	Business Attribute Aggregator
DC	Data Consumer
DP	Data Provider
Dx.y	Deliverable number y belonging to Activity x
JWT	JSON Web Token
IdP	Identity Provider
KYC	Know Your Customer
MDS	Minimum Data Set
OIDC	OpenID Connect
PII	Personal Identification Information
SSO	Single Sign On
SP	Service Provider
SPI	Service Provider Interface
WAYF	Where are you from

Executive Summary

Deliverable “D3.3 – eIDAS node report” is related to Activity 3 of the GRIDS project (increasing trust with eID for Developing business). The goal of this deliverable is to present the design and actual details of the integration of the GRIDS platform with the Greek eIDAS node, as those were carried out in the context of the GRIDS project. With the completion of the presented activities, 360kompany is capable of becoming a Service Provider connected to the Greek eIDAS node via the business gateway facility of ADACOM.

Document name:	D3.3 eIDAS node report	Page:	6 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

1 Introduction

1.1 Purpose of the document

This document reports on the development and deployment of the Service Provider Hub (SP Hub) of the GRIDS platform. These tasks were performed under Activity 3 (“Business Attributes Aggregator, 360kompany services customization and Integration with the eIDAS Infrastructure”) and are a result of the design implemented under Activity 2 (“Business Requirements, Technical Design and Integration Planning”). The SP Hub was designed and implemented to provide eIDAS authentication functionality (i.e. act as a relying party for the eIDAS Network). Through it the GRIDS platform becomes a consumer of the eIDAS eID Network to enable authentication for its end users (natural persons representing a business entity).

Specifically, the SP hub generates an identification token containing the eIDAS received identity attributes that can be transmitted back to the Business Attribute Aggregator (BAA), in such a way that any service under the same domain can reuse it (in other words it provides full SSO functionality). As a result, any service provider (SP) integrated with the BAA will be capable of consuming eIDAS eID Identities as part of a GRIDS flow. Finally, the SP Hub was developed by the University of the Aegean (UAEGEAN) and is operated by ADACOM in collaboration with the UAEGEAN.

1.2 Reference to other project work

This deliverable is an immediate result of the business requirements of the GRIDS platform (as those were presented in D2.1 “Business Service Definition”) and the architecture design of the GRIDS platform (as that is being finalized under Activity’s 2 Task 2.2 and will be described in detail in the deliverable D2.2 “Technical Specifications and Architecture”), due to the fact that the eIDAS integration module described here (i.e. the SP Hub) is a direct implementation of the aforementioned design, aimed at satisfying the original business requirements.

1.3 Structure of the document

This document is structured in 7 major chapters

Chapter 2 presents a high-level overview of the GRIDS architecture and the role of the SP Hub within the GRIDS architecture.

Chapter 3 presents the SP Hub Architecture and its components.

Chapter 4 presents the main functionality of the SP Hub.

Chapter 5 presents the deployment details of the SP Hub.

Chapter 6 presents tests conducted to verify the connectivity of the SP Hub to the Greek eIDAS node

Chapter 7 presents the conclusions of the deliverable.

Document name:	D3.3 eIDAS node report	Page:	7 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

2 GRIDS Architecture Overview

The GRIDS platform (presented in Figure 1 below) supports the integration of various Data Providers (DP) enabling them to expose their APIs via this Platform to authorized Data Consumers (DC). The GRIDS platform is composed of the following high-level entities:

- ▶ The Business Attribute Aggregator(s) (BAAs)
- ▶ The GRIDS Registry Service
- ▶ The SP Hub.

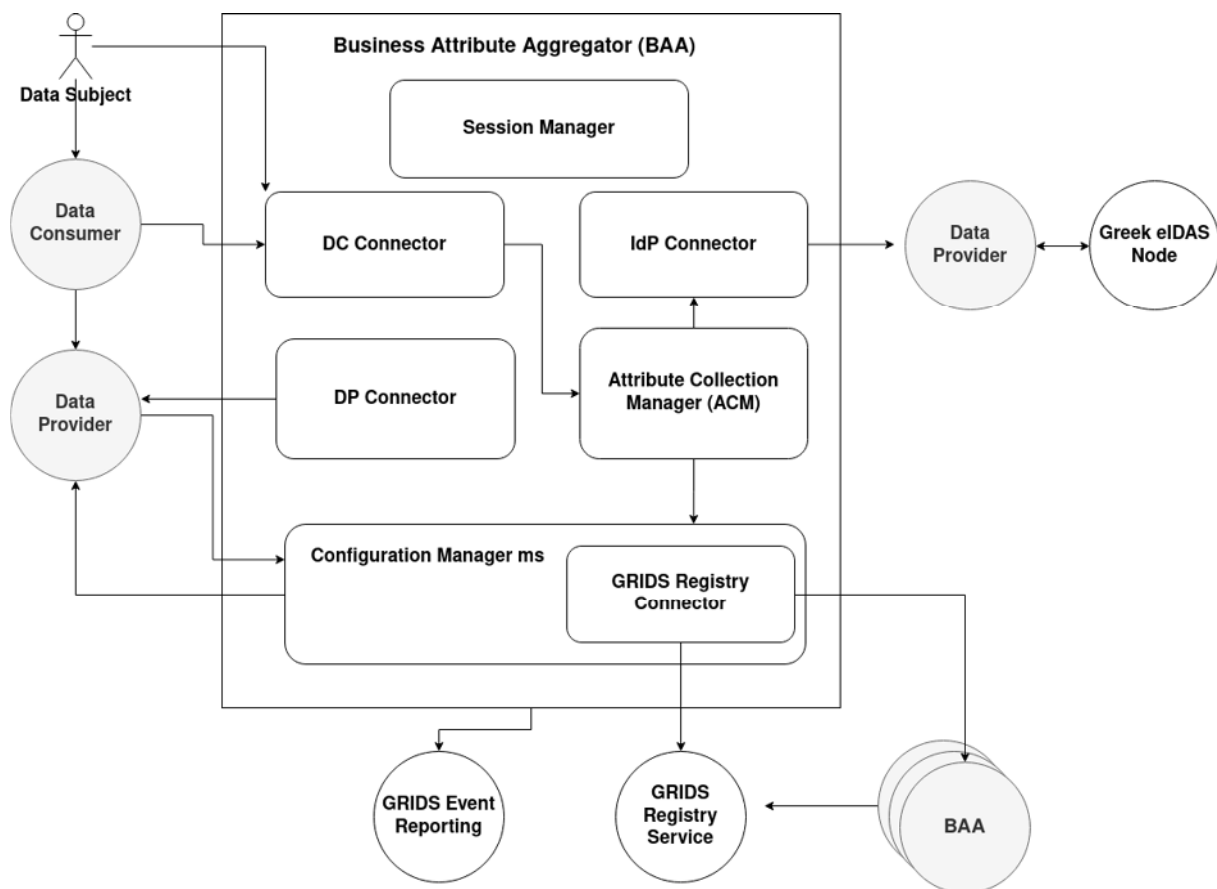


Figure 1: GRIDS architecture overview

Specifically, the **Business Attribute Aggregator (BAA)** provides the main functionality of the GRIDS platform. It enables through a single standardized API, various Data Consumers to query KYC information from the connected Data Providers (KYC-providers) for a user identified using eIDAS eID, thus enhancing the level of assurances and simplifying the process. Specifically, the BAA is designed to contain the following components/microservices:

1. Session Manager; this microservice implements the “memory” of the BAA, caching the required metadata to generate the appropriate requests to the EIDAS eID network and KYC providers and handle their responses by making them available to the appropriate BAA components. Finally, this component provides API authentication supports for the various calls between the microservices of a BAA

Document name:	D3.3 eIDAS node report	Page:	8 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

2. DC Connector; this microservice permits the various clients of the GRIDS platform to integrate with GRIDS over a standardized and easy to consume REST API (specifically over OpenID Connect (OIDC)).
3. IdP Connector; this microservice integrates with the Service Provider Hub (that is presented in detail in this deliverable) to request the eIDAS eID authentication and Identification of the users of the clients connected to the platform.
4. DP Connector; this microservice integrates with the various Data Providers connected to the BAA service, providing the required metadata to query them for KYC information of a user identified over eIDAS eID.
5. Attribute Collection Manager; this component acts as the orchestrator for the platform, propagating the eIDAS+KYC request from the platform's clients (as those were received by the DC Connector module) to the IdP Connector and DP Connector module, and transforms them to a coherent response capable of satisfying the original request.
6. Configuration Manager; this component main functionality is that of connecting to the GRIDS Registry. Additionally, it enables microservice discovery within the same BAA.

The **GRIDS Registry Service** acts as the trust anchor of the GRIDS architecture. It enables the discovery of the DPs registered to the potentially multiple BAAs of the architecture¹ and provides the necessary cryptographic assertions to enable their query by DC connected to different BAAs.

2.1 The role of the SP Hub within the GRIDS architecture

The SP Hub enables the authentication and identification, via eIDAS eID, of the users of the DCs connected to a BAA by acting as a proxy service to the (Greek) eIDAS node. Essentially, this service is designed to hide the complexity of the eIDAS Node integration by exposing a much simpler to consume REST API, over OIDC.

As a result, the BAA becomes a relying party of the Greek eIDAS node by becoming a client of the SP Hub (operated jointly by ADACOM and UAEGEAN).

¹ At the end of the project one BAA is going to be deployed and operated by 360kompany. However, the architecture envisions the integration of multiple BAAs each onboarding each own set of Data Providers to the system

Document name:	D3.3 eIDAS node report	Page:	9 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

3 SP Hub Architecture and components

The architecture of the SP Hub is displayed in Figure 2. Specifically, the SP hub is realised via a lightweight, production ready, stable and scalable OpenIdConnect (OIDC) Server (Keycloak) complemented by a Memcached instance and that has been augmented for the purposes of GRIDS (via the Greek eIDAS Node Connector ms) to be capable of authenticating the users of the connected clients over the eIDAS eID network by integrating with the Greek eIDAS node. Additionally, by employing a composable microservice architecture the SP Hub can be easily expanded to integrate with additional eIDAS Nodes, or even simultaneously integrate with multiple eIDAS nodes (if such a need arises) with no modification of the core OIDC server (and as a result with no down time).

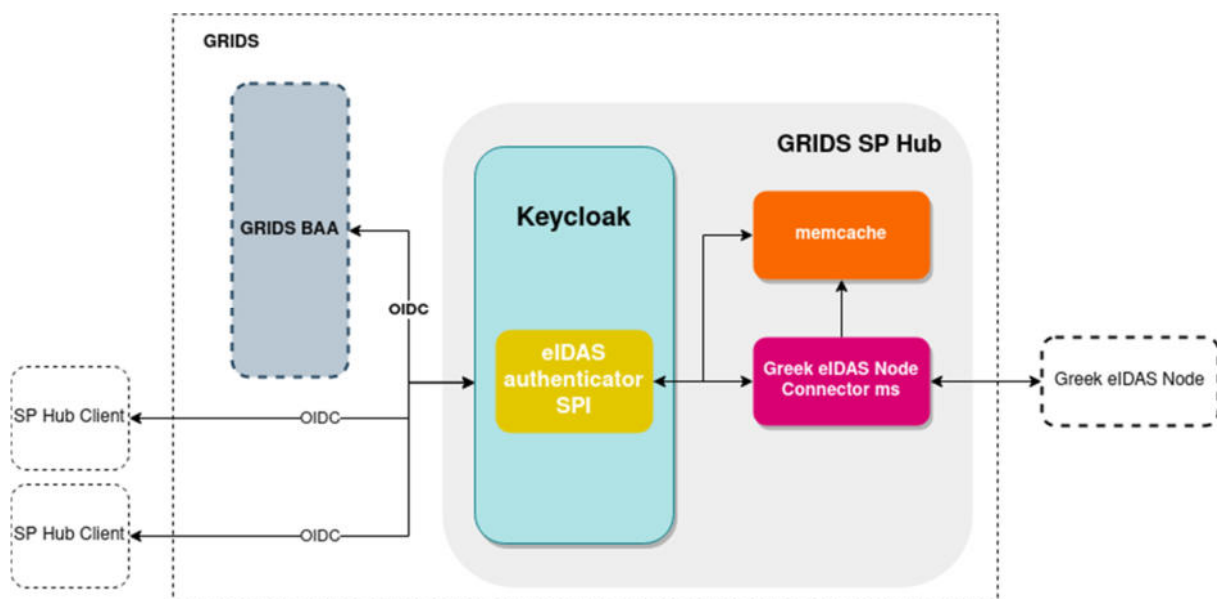


Figure 2: GRIDS SP Hub architecture

3.1 SP Hub Components

The SP Hub is composed of:

1. The core OIDC server (i.e. Keycloak).
2. The eIDAS authenticator Service Provider Interface (SPI).
3. The Greek eIDAS Node connector microservice.
4. An instance of Memcached.

These components are analysed in detail below.

1. **Core OIDC Server:** This component implements the main functionality of the SP Hub, i.e., that of an OpenID Connect Server. It is implemented using the open-source software Keycloak. Keycloak is an open-source Identity and Access Management solution that fully supports Single Sign On (SSO) and Logout functionality. This enables users to only authenticate once in order to access any connected service (and likewise only need to logout once to logout from all connected services). Finally, Keycloak is based on standard protocols and provides support for OpenID Connect, OAuth 2.0, and SAML.

Document name:	D3.3 eIDAS node report	Page:	10 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

2. **eIDAS authenticator Service Provider Interface (SPI):** While Keycloak is capable of handling many external authenticator providers with no code modifications required, this is not the case for connecting to an eIDAS Node. The eIDAS authenticator SPI, is a specifically build Keycloak module (implemented in the context of GRIDS) that:
 - a. enables a user to select their country of origin (via appropriate user interfaces)
 - b. integrates with the Greek eIDAS Node Connector to propagate the OIDC authentication request to the Greek eIDAS node so as to authenticate the user over the eIDAS eID network.
 - c. receives the authentication response, after the user's authentication is completed, and restores the original OIDC authentication session with the client (i.e., the BAA service), by incorporating the user as the authenticated principal of the session.
3. **Greek eIDAS Node Connector microservice:** This component is responsible for the integration with the Greek eIDAS node. Specifically, this component receives an authentication request (containing the user's country of origin) from the eIDAS authenticator SPI (in a secure back channel call) and builds an appropriate SAML authentication request which is propagated to the Greek eIDAS node. After the user authenticates, the Greek eIDAS node sends the appropriate SAML assertions to the Greek eIDAS Node Connector microservice, which in turn parses it, retrieves the users attributes and sends them (via a secure back channel call) to the eIDAS authenticator SPI. Finally, this microservice exposes the SAML metadata that is required to integrate with the Greek eIDAS node.
4. **Memcached microservice:** This microservice acts as the cache of the architecture, specifically using it the eIDAS authenticator SPI caches the original client OIDC request parameters (before sending the request to the connector microservice), in order to revitalize the authentication session once the response is received and thus finally propagate the eIDAS assertions back to the client (i.e. the BAA service).

Document name:	D3.3 eIDAS node report	Page:	11 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

4 The functionality of the SP Hub

OIDC is an identity layer built on top of the OAuth 2.0 protocol. It defines a sign-in flow that enables a client application to authenticate a user, and to obtain information (or "claims") about that user. User identity information is encoded in a secure JSON Web Token (JWT), called ID token. OpenID Connect defines a discovery mechanism, called OpenID Connect Discovery, where an OpenID server publishes its metadata at a well-known URL. The SP Hub implements a fully functional OpenID connect server. Its main functionality is displayed in Figure 3.

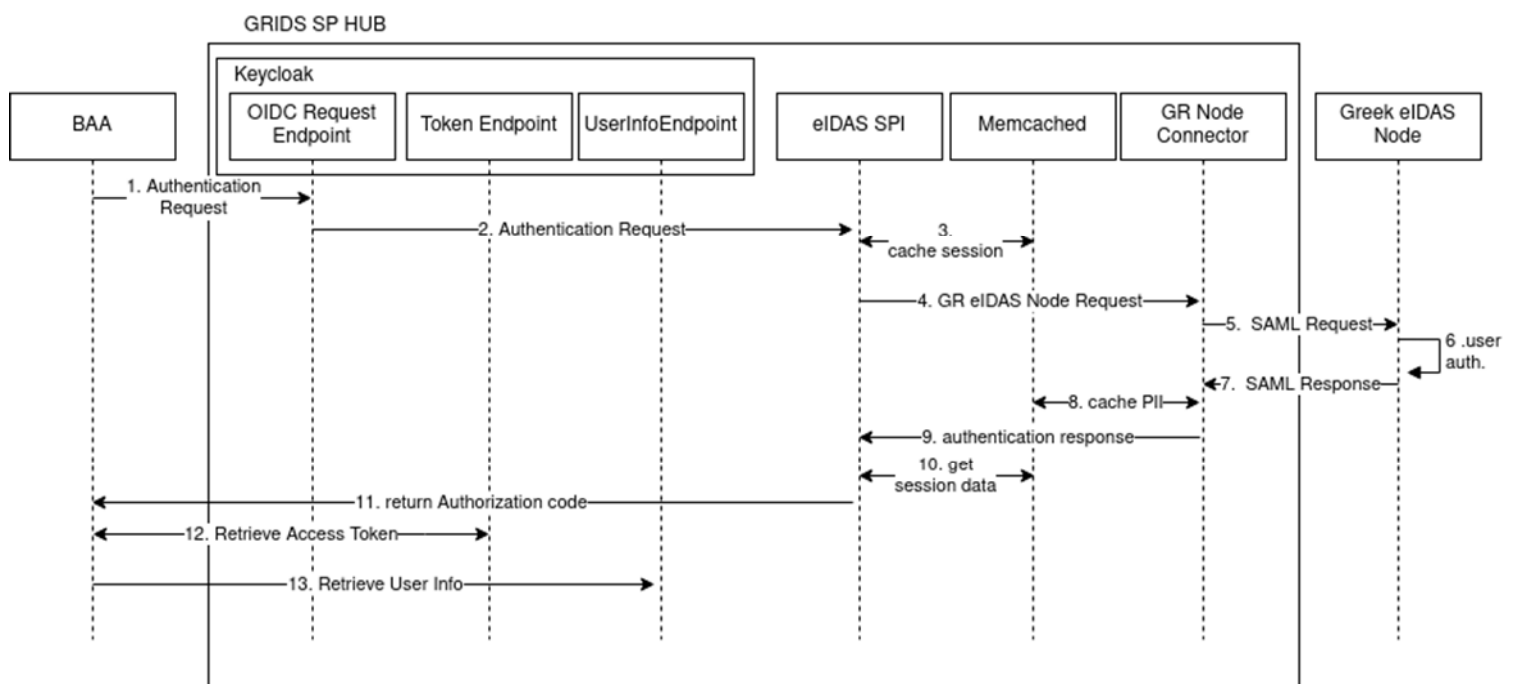


Figure 3: GRIDS authentication flow

Specifically, the functionality of the SP Hub is to authenticate users over the eIDAS Network (via the Greek eIDAS node) after a request made by the Business Attribute Aggregator component of the GRIDS Architecture. For this end the BAA will be registered as an OIDC Client at the SP Hub.

Additionally, the SP Hub supports the authentication of both Legal and Natural persons via the eIDAS Network. This is supported by the addition of two custom OIDC scopes (natural, legal respectively) which can be included in the original OIDC request. Each of these scopes will result in the request of the respective minimum data sets (MDS) to be retrieved from the eIDAS network (as those are defined in the eIDAS specification). SPs that require additional eIDAS attributes to be requested during the user authentication can add as additional OIDC scopes the eIDAS friendly names of these attributes (e.g., Gender). However, to ensure the highest possible success rate of authentication these attributes will only be requested as optional. The SP is responsible for terminating their service in case they do not retrieve any of those attributes.

Document name:	D3.3 eIDAS node report	Page:	12 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

Assuming the existence of such a registration, the flow that implements the functionality of the SP Hub is follows:

1. The BAA is (using its IdP Connector module) performs an OIDC authentication request, with the aforementioned OIDC scopes, towards the SP Hub (including client_id, redirect uri etc. as defined in the OIDC specification).
2. The SP hub propagates this request to the eIDAS SPI module.
3. The eIDAS SPI module, first creates a unique session Id, produces and displays a Where Are You From (WAYF) interface for the user, retrieves their selection and finally caches it together with the OIDC authentication request parameters under the generated sessionId.
4. The eIDAS SPI module sends an authentication request to the Greek eIDAS Node Connector microservice. This request contains the newly generated sessionId and the users selected country of origin.
5. The eIDAS Node Connector, generates an appropriate eIDAS SAML request and sends it to the Greek eIDAS node.
6. The user is redirected from the Greek eIDAS node to their country of origin eIDAS node, and from there to their national IdP. Next, the user authenticates at the national IdP and the response is sent to the eIDAS node of their country-of-origin. Next, the users Personal Identification Information (PII) is sent from the user country of origin to the Greek eIDAS node.
7. Next, the Greek eIDAS node propagates the PII of the user to the eIDAS Node Connector of the SP Hub.
8. The eIDAS Node Connector microservice caches the response.
9. The eIDAS Node Connector redirects to the eIDAS SPI module using the session Id generated in step 3.
10. The eIDAS SPI module retrieves from the cache the users PII and the original OIDC request parameters.
11. The eIDAS SPI recreates the OIDC authentication request and binds it to the retrieved user attributes and generates an authorization code to retrieve them. The code is sent to the BAA (IdP Connector).
12. The BAA uses this code together with its client Id and secret (as those were generated during its registration) to request from the SP Hub's token endpoint and access token
13. The exchanges this access token (at the SP Hub's user info endpoint) for the user attributes which are sent to the BAA encoded as a Json Web Token (JWT).

The JWT returned to the BAA (apart from the necessary cryptographic material that can be used to verify that it is indeed send form the SP Hub, and that it has not been tampered with) contains the following attributes (identifying the user and providing metadata related to the user authentication session):

► In the case of natural person authentication:

```
{
  CurrentFamilyName: xxx,
  CurrentGivenName: xxx,
  DateOfBirth: xxx,
  PersonIdentifier: xxx,
  loa: xxx,
  timeStamp: xxx,
```

Document name:	D3.3 eIDAS node report	Page:	13 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

```
eIDASSAMLresponse: xxx,  
eIDASnotBefore: xxx,  
eIDASnotAfter:xxx,  
eIDASIssueAt: xxx.  
eIDASExpiration: xx  
}
```

► While In the case of legal person authentication:

```
{  
LegalName: xxx,  
LegalPersonIdentifier: xxx,  
loa: xxx,  
timeStamp: xxx,  
eIDASSAMLresponse: xxx,  
eIDASnotBefore: xxx,  
eIDASnotAfter:xxx,  
eIDASIssueAt: xxx.  
eIDASExpiration: xx  
}
```

In the above responses the metadata retrieved directly from the eIDAS response (i.e., eIDASSAMLresponse, eIDASnotBefore, eIDASnotAfter, eIDASIssueAt, eIDASExpiration) are provided as evidence of the successful authentication of the user over the eIDAS network. Please note that no party other than the SPHub may read the plain text content of the eIDASSAMLresponse attribute as those are encrypted with the SP Hubs public key (as defined in the eIDAS specification²)

² <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/10/29/Release+of+CEF+eIDAS-Node+version+2.3.1>

Document name:	D3.3 eIDAS node report	Page:	14 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

5 Deployment

The SP hub was deployed at the premises of ADACOM with the support of the University of the Aegean. Specifically its OIDC well-known URL is available at:

<https://eidas.adacom.com/auth/realms/eidas/.well-known/openid-configuration>

The SP Hub is built as a set of container images built with Docker [1] and an additional WILDFLY [2] “ear” file that is deployed inside the Keycloak container (implementing the eIDAS authenticator SPI as specified by Keycloak [3]). This implementation minimises the deployment effort and seamlessly integrates with the development environments. A deployment of the SP hub can be easily created using the following docker-compose file [4].

```

version: '3'

volumes:
  mysql_data:
    driver: local

services:
  eidas-proxy:
    image: endimion13/eidas-proxy:0.0.1d
    environment:
      SP_CONFIG_REPOSITORY: /configEidas/
    volumes:
      - /home/user/configEidas:/configEidas
    ports:
      - 8082:8081
    links:
      - memcached

  mysql:
    image: mysql:5.7
    volumes:
      - mysql_data:/var/lib/mysql
    environment:
      MYSQL_ROOT_PASSWORD: ***
      MYSQL_DATABASE: keycloak
      MYSQL_USER: ****
      MYSQL_PASSWORD: ****

  keycloak:
    image: jboss/keycloak:latest
    environment:
      _JAVA_OPTIONS: -Dlogback.configurationFile=/logs/config.xml
      PROXY_ADDRESS_FORWARDING: 'true'
      SP_CONFIG_REPOSITORY: /configEidas/
      DB_VENDOR: MYSQL
  
```

Document name:	D3.3 eIDAS node report	Page:	15 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

```

DB_ADDR: mysql
DB_DATABASE: keycloak
DB_USER: ****
DB_PASSWORD: ****
KEYCLOAK_USER: ****
KEYCLOAK_PASSWORD: ****
EIDAS_PROXY_SAML_ENDPOINT: http://deploymentServer/proxy/makeRequest
EIDAS_NODE_URI: https://eidas.gov.gr/EidasNode/ServiceProvider
ports:
- 8081:8080
volumes:
- ./keyConfig:/keyConfig
- ./logs2:/opt/jboss/keycloak/logs
- ../certs:/opt/jboss/keycloak/certs
depends_on:
- mysql
- memcached
links:
- memcached:memcached

memcached:
image: sameersbn/memcached:1.5.6-2
ports:
- 11111:11211

```

Extensive instruction on the deployment server requirements, configuration and deployment of the SP Hub can be found in the following guide:

https://docs.google.com/document/d/1dCYIiioxWBrDxwPB_AI_Pj8dYO6AJvXCsbTzJglsQI/edit?usp=sharing

Document name:	D3.3 eIDAS node report	Page:	16 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

6 Testing through GR and ES credentials

This section contains the validation results produced during the testing of the successful integration of the GRIDS SP Hub to the Greek eIDAS Node.

To implement these tests a Demo Service Provider was implemented. This Demo SP integrates with the GRIDS SP Hub via OIDC (in exactly the same way that the BAA will integrate as well) and issues an OIDC authentication request, which according to the functionality of the SP Hub is transformed into an eIDAS authentication request.

The SP Hub is currently connected to the pre-production environment of the Greek eIDAS node. All integration tests have been concluded successfully and the SP Hub is expected to be connected to the production environment of the Greek eIDAS node within the next few days.

The following screenshots provide the required validation of the correct integration of the GRIDS SP Hub to the Greek eIDAS node, by demonstrating the authentication of a user from Greece.

6.1 Greek User Authentication

The user first reaches the SP interface (Mock ADACOM SP), and is requested to authenticate as demonstrated in the following screenshot

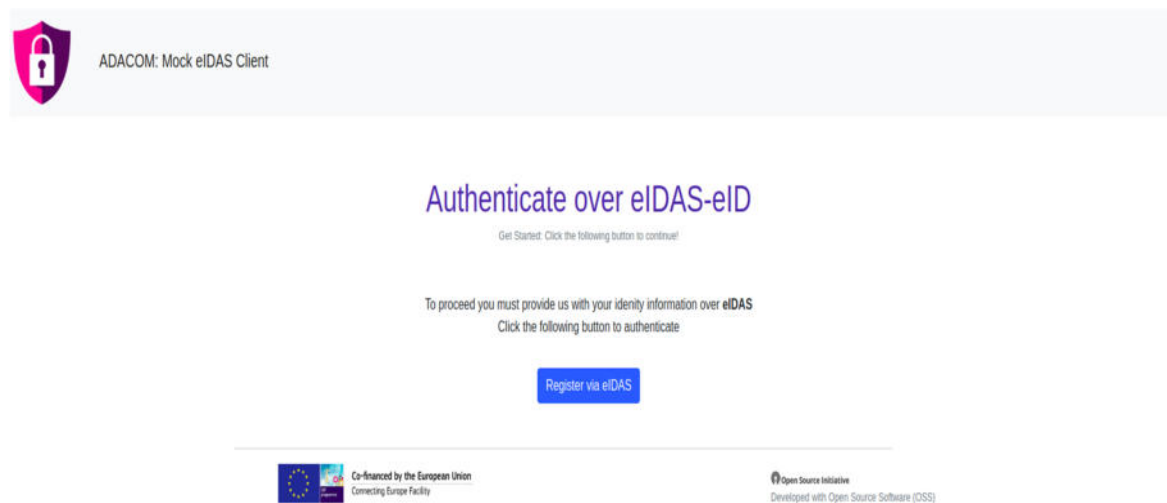


Figure 4: Mock SP authenticate prompt

Next, by clicking the Register via eIDAS button, the SP sends a suitable OIDC authentication request to the SP Hub. The SP Hub receives this request and displays the user a WAYF interface

Document name:	D3.3 eIDAS node report	Page:	17 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

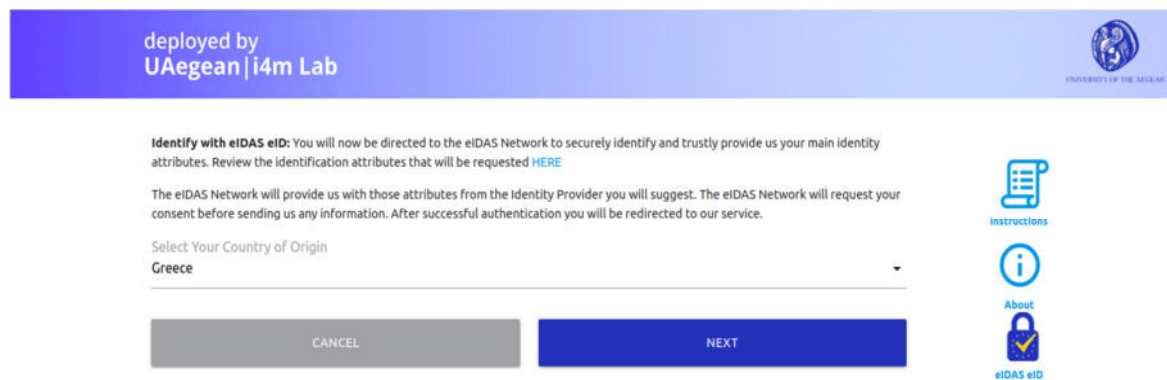



Figure 5: SP Hub WAYF interface

The user selects Greece as their country-of-origin and clicks next. As a result, the SP Hub generates an appropriate eIDAS SAML request and sends it to the Greek eIDAS node. Next, the user proceeds to the normal eIDAS authentication flow as shown in the following screenshots:

EIDAS AUTHENTICATION SERVICE (IDP)

AUTHENTICATION



**USE YOUR NATIONAL eID
AND ACCESS ONLINE
SERVICES**

USERNAME Test user

PASSWORD

LEVEL OF ASSURANCE

IP ADDRESS FOR SUBJECTCONFIRMATIONDATA

SUBMIT

Figure 6: Greek pre-production eIDAS IdP authentication

Document name:	D3.3 eIDAS node report	Page:	18 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

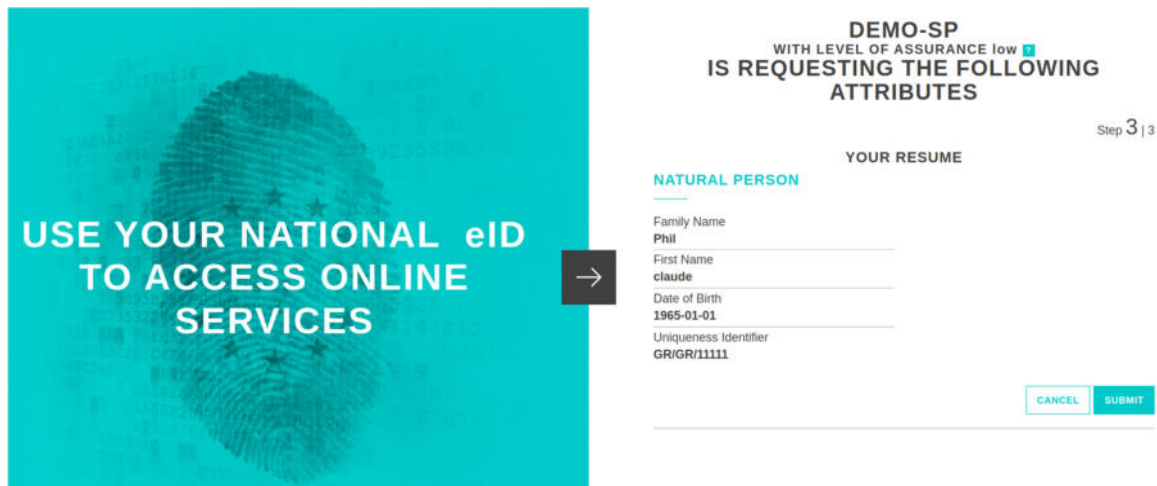


Figure 7: Greek pre-production eIDAS Node consent form

Finally, the user's attributes are sent the SP Hub, which in return redirects to the SP including those attributes as part of the OIDC response



Figure 8: Mock SP authenticated user interface

Document name:	D3.3 eIDAS node report	Page:	19 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

7 Conclusions

This document presented the main outcomes of the efforts that took place as part of Activity's 3 Task 3.3. As a result of these efforts, the GRIDS SP Hub was implemented by UAEGEAN and was deployed at the premises of ADACOM (where it will be jointly managed by ADACOM and UAEGEAN). Additionally, the aforementioned deployment of the SP Hub was successfully connected to the Greek eIDAS node in the pre-production environment.

All integration tests were concluded successfully. Thus, within the next few days the SP Hub will be integrated to the production environment Greek eIDAS node (currently pending the whitelisting of the SP Hub in the production environment from the Greek eIDAS Node operators). As a result, citizens from any EU Member state connected to the Greek Node will be capable of authenticating to any service provider connected to the SP Hub. Subsequently, 360Kompany is capable of becoming a Service Provider connected to the Greek eIDAS node using the business gateways facility (with SSO-support) of ADACOM (i.e., the GRIDS SP Hub).

Document name:	D3.3 eIDAS node report	Page:	20 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final

8 References

- [1] <https://www.docker.com/>
- [2] <https://www.wildfly.org/>
- [3] https://www.keycloak.org/docs/latest/server_development/#_auth_spi
- [4] <https://docs.docker.com/compose/>

Document name:	D3.3 eIDAS node report	Page:	21 of 21
Reference:	D3.3	Version:	1.0
		Status:	Final