Leveraging eID in the Private Sector

D4.3 Operational and Technical Documentation of SP (ATHEX, Hellenic Post) integration (production)

Document Identification			
Status	Final	**Due Date**	30/07/2018
Version	1.0		27/08/2018

Related Activities	Activity 4, Activity 5	**Document Reference**	D4.3/D5.3
Related Deliverable(s)	D2.1, D3.3, D4.1/D5.1, D4.2/D5.2, D3.1	**Dissemination Level (*)**	PU
Lead Participant	UAegean	**Lead Author**	Petros Kavassalis, Katerina Ksystra, Nikolaos Triantafyllou, Maria Lekakou
Contributors	UAegean, ATHEX , ELTA	**Reviewers**	Elena Torroglosa. UMU / Loukia Demiri (HMIAR)

Keywords
eIDAS, eID, SP e-services, Greek eIDAS Node, eIDAS API Connectors

This document is issued within the frame and for the purpose of the *LEPS* 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/A2016/1271348; Action No 2016-EU-IA-0059 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	UAegean
Katerina Ksystra	UAegean
Nikolaos Triantafyllou	UAegean
Maria Lekakou	UAegean

Document History			
Version	Date	Change editors	Changes
0.1	13/06/2018	UAegean	Initial draft version with ToC
0.2	9/07/2018	UAegean	Updated ToC.
0.3	16/07/2018	UAegean	Updated ToC. Guide lines for each section.
0.4	17/07/2018	UAegean	Updates on sections: Introduction, List of figures, List of tables
0.5	24/07/2017	UAegean	Updates on sections: Executive Summary, Introduction, Conclusion, Requirements
0.6	26/07/2017	UAegean	Updates on sections: Tests (according to ATHEX feedback), Interoperability tests, Methodology
0.7	27/07/2017	UAegean	Updates on sections: Integration, Requirements, Evaluation
0.9	31/07/2017	UAegean	Updates on sections: Tests, Evaluation (after receiving ATHEX and ELTA contribution)
1.0	03/08/2018	UAegean	Version sent to Reviewers
1.1, 1.2 and 1.3	21/08/2018	UAegean	Versions incorporating reviewers' comments (UMU, HMIAR, ATOS)
1.4	27/08/2018	UAegean	Final version sent to quality review
1.5	03/09/2018	ATOS	Quality review
FINAL	04/09/2018		FINAL VERSION TO BE SUBMITTED

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
CEF	Connecting Europe Facility
Dx.y	Deliverable number y belonging to WP x
EC	European Commission
eID	Electronic Identification
eIDAS	electronic IDentification, Authentication and trust Services
IdP	Identity Provider
GDPR	General Data Protection Regulation
JSON	JavaScript Object Notation
JWT	JSON Web Token
LEPS	Leveraging elD in the Private Sector
LEPS eIDAS API Connectors	(SP-side) APIs allowing a Service Provider to easily integrate with the eIDAS Network
LoA	Level of Assurance
OTP	One Time Password
REST	REpresentational State Transfer
SAML	Security Assertion Mark-up Language
SOAP	Leveraging elD in the Private Sector
SP	Service Provider
TWA	Thin Web Apps
WP	Work Package

List of Terms

Abbreviation / acronym	Description
authRequest	Authentication Request that will be sent to the eIDAS Node
authResponse	Authentication Response sent from the eIDAS Node

Executive Summary

The main goal of the Deliverable "D4.3 Operational and Technical Documentation of SP (ATHEX, Hellenic Post) integration (production)" is to provide a precise description of the actions performed by Hellenic Post (ELTA) and Athens Stock Exchange Services Group (ATHEX Group) during the process of integration of their e-Services with the Greek elDAS Node. This integration has been developed in the objective to allow EU cross-border users to access ATHEX and ELTA services via an elDAS Network-based authentication request (with mandatory and optional attributes that have been defined in Activity 2). Obviously, this phase follows an activity of customization and adaptation of ATHEX and ELTA e-Services to the needs of the integration with the eIDAS Network (Activity 4 and 5, Tasks 4.1 and 5.1, respectively).

As stated in the Grant Agreement, the integration of ATHEX and ELTA services with the eIDAS Network will use a SP-tailored interconnection service, which is now called "LEPS eIDAS API Connectors". It is a specific software suite developed in previous Tasks (Tasks 4.2 and 5.2 – reported in Deliverable D4.2/D5.2), therefore, this deliverable includes only a short description of the LEPS eIDAS API Connectors. LEPS API Connectors simplify and optimize the decision of a Service Provider to join the eIDAS infrastructure. Furthermore, this deliverable includes: a) the technical, operational and legal requirements of the services that are connected to eIDAS Network via LEPS eIDAS API Connectors and, b) a detailed overview of the technical infrastructure, based on LEPS eIDAS APIs Connectors, that allows for service integration with the eIDAS infrastructure. Yet, the deliverable provides a complete description of the activities performed for the integration of ATHEX and ELTA services with the Greek elDAS Node and presents a number of test cases that prove the success of the integration (a more extended testing procedure will take place in the last months of the project).

As a conclusion, we report that ATHEX and ELTA services which are part of LEPS project, have been successfully and at a reasonable effort integrated with the eIDAS Network. They do now interoperate with the Greek eIDAS Node via LEPS eIDAS API Connectors and, therefore, can provide the same functionality to local and cross-border users (with cross-border users being able to automatically access them via their national eID credentials). After the detailed tests conducted in the context of the last project operation (Activity 7: "Testing of cross-border authentication and access to electronic Services"), and the necessary final adjustments and service business logic modifications, these services will be functional parts of the pan-european eIDAS infrastructure. Finally, it is worth to notice that ATHEX and ELTA may further benefited from the interconnection infrastructure they have deployed in the context of LEPS project (relying on LEPS eIDAS API Connectors), to easily integrate with the eIDAS Network other services they may want to make available to cross-border customers, at a minimal technical and operational cost (Chapter 9).

The results included in this deliverable will be compared with those obtained in the context of Activity 3 "Customization of Spanish Postal Services and Integration with eIDAS Infrastructure" which encompasses the actions performed in the objective to integrate Spanish Correos Postal services with the Spanish eIDAS Node through a similar eIDAS adapter. This comparison will be valuable for SPs of other EU member states that wish to integrate their services with the eIDAS Network. This

comparison will be valuable to other EU member states and SPs that are searching for eIDAS Network integration solutions that are well adapted to their strategies, needs and IT infrastructures.

1 Introduction

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014 provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities[1].

In this regard, the eIDAS Regulation:

- Ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available.
- Creates a European internal market for electronic trust services – namely electronic signatures, electronic seals, time stamp, and electronic delivery service and website authentication – making these services interoperable across borders, while guaranteeing an equivalent legal status with traditional paper-based processes.

After entering into force eIDAS regulation[2] in September 2014, and since 29 September 2018, the EU public organizations offering e-services to citizens are obliged to recognize notified eID schemes from other EU member states. The next challenge for the businesses offering digital services will be the accelerated use of trusted eIDs issued by EU governments for accessing electronic services and making secure electronic transactions. The LEPS project which is funded by CEF Telecom Programme[3] promotes this perspective. It envisages at the standardization and and simplification of the integration of European Service Providers (SPs) to the eIDAS Network, enabling them able to make their offerings accessible across EU countries borders while enjoying the legal coherence and online safety requirements of the eIDAS framework. The project re-uses parts of the eID software (called eID building block) provided by the European Commission[4] to develop APIs and interconnection strategies and solutions that allow private Service Providers to connect their offerings to the eIDAS Network at the minimum possible effort and cost.

This Deliverable reports on the work performed within LEPS Tasks 4.3 and 5.3, ATHEX and ELTA Integration to Greek PEPS/eIDAS Node Connector, respectively. The process of integration with the eIDAS Network includes: a) the generation of an eIDAS authentication request containing both mandatory and optional attributes, b) the processing of the authentication response (after user's authentication with her/his national IdP) and the translation from SAML 2.0 to common enterprise standards (JSON, SOAP, etc.) and, c) the smooth insertion of this processed information into SP back-end systems and authorization processes, that means the appreciation of the received identity attributes and LoA level and the use of this information to enable effective user authentication and grant access privileges (similarly to any local authentication process).

[1] https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

[2] https://ec.europa.eu/inea/sites/inea/files/c_2017_696_f1_annex_en_v3_p1_875665.pdf

[3] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom

[4] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID

1.1 Purpose of the document

The purpose of this document is to provide a complete description of the activities achieved within:

- Activity 4: Customization of Greek Financial Services and Integration with elDAS Infrastructure – Task 4.3: Integration to Greek PEPS/eIDAS Node Connector
- Activity 5: Customization of Greek Post Electronic Services and Integration with elDAS Infrastructure: Task 5.3: Integration to Greek PEPS/eIDAS Node Connector

This Deliverable is related to milestone 7 "Integration of Hellenic Post and ATHEX services to PEPS/eIDAS Node connector (production)" (Mean of Verification: Operational and Technical Documentation of SP integration (production)".

1.2 Relation to other project work

The activities described in this document have received input mostly from:

- Activity 2: Business Requirements, Integration and Testing Planning
  - Task 2.1 "Project Operations and Architecture Design"
- Activity 4: Customization of Greek Financial Services and Integration with elDAS Infrastructure
  - Task 4.1 "Customization of Greek Financial Services"
  - Task 4.2: "Develop elDAS Interconnection Supporting Service"
  - Task 4.3: "Integration to Greek PEPS/elDAS-Node Connector"
  - Task 4.4: "Mobile authentication"
- Activity 5: Customization of Greek Post Electronic Services and Integration with elDAS Infrastructure
  - Task 5.1 "Customization of Hellenic Post Services Portal"
  - Task 5.2: "Develop elDAS Interconnection Supporting Service"
  - Task 5.3: "Integration to Greek PEPS/elDAS-Node Connector"
  - Task 5.4: "Mobile authentication"

The activities described in this document will provide input to:

- Activity 6: Testing of cross-border authentication and access to Correos electronic Services and to Hellenic (Financial and Post) electronic Services
- Activity 7: Maximizing eID uptake in private sector, sustainability and road-mapping.

1.3 Structure of the document

This document is structured in the following chapters:

Chapter 2 provides a short view on the integration with the eIDAS Netwiork methodology used by ATHEX and ELTA, that is based on the deployment of an API infrastructure (LEPS eIDAS API Connectors) as a bridge between their services and applications and the eIDAS Network.

Chapter 3 describes the technical, operational and legal requirements that have been considered prior to integration of ATHEX and ELTA Services with the Greek eIDAS Node, and further with the eIDAS Network.

Chapter 4 presents in brief LEPS eIDAS API Connectors (they have beeb extensively presented in a previous deliverable) and how their use modifies and consolidates typical eIDAS authentication flows.

Chapter 5 provides a detailed description of how ATHEX and ELTA have used, in practice, these APIs in order to interconnect their services with the Greek elDAS Node.

Chapter 6 presents the test cases that were used to verify the effective integration of SP services with the eIDAS Network.

Chapter 7 provides the interoperability operations with other EU countries, to be developed next.

Chapter 8 evaluates the activities related to integration of Greek Financial Services and Greek Post Electronic Services with the Greek eIDAS Node, suggests future improvements and presents lessons learnt.

Chapter 9 concludes the document.

2 Challenges to meet and methodology

Based on previous European projects such as STORK 1.0, STORK 2.0[5] and eSENS[6], an eID infrastructure has been deployed across Europe. The initiative undertaken by CEF has allowed for the development of several building blocks (also known as Digital Service Infrastructures | DSI) which provide a European digital ecosystem for cross-border interconnection of citizens/customers and Service Providers from different European countries. The eIDAS Network is created specifically by leveraging the potential of CEF building blocks, mainly eID, and by applying eIDAS regulation principles in the design of the eIDAS Network authentication and attributes transfer functionality. The network is made by the interconnected eIDAS Nodes of the different Member States[7], which embrace common standards and operation principles. Essentially, it enables the interoperation of the different national eID schemes to allow for the cross-border use of national eIDs. In fact, when a citizen or customer requires access to electronic services provided by Service Providers located in countries that are different from the country of origin of the requester, the user is redirected to the eIDAS Network which basically acts as a trusted third-party service for user authentication. Putting it in another way, the eIDAS Network transports (across borders) the identity attributes that a Service Provider (SP) has requested for authenticating a user (for example, name, surname, country of origin, unique ID, etc.), from the authoritative source that hosts the eID of this user (also called Identity Provider | IdP) to the Service Provider;s IT infrastructure -- under the condition that the user has provided consent to such an information transfer.

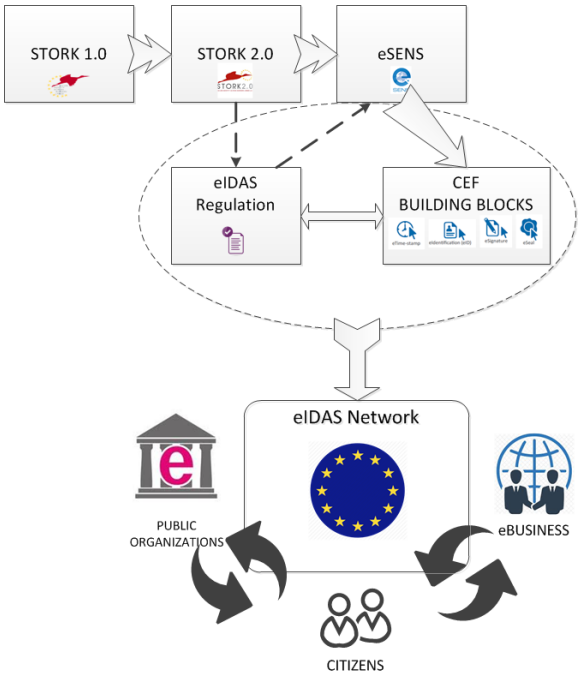

Figure 2-1: eIDAS Background

For a Service Provider (SPs), the interconnection with a national eIDAS Node requires the deployment of software module that is programmed to create and send to eIDAS Node an authentication request and receive, from the eIDAS Node, and process an authentication response. LEPS project has

[5] https://www.eid-stork2.eu/

[6] https://www.esens.eu/

[7] See: eIDAS Interoperability Architecture, available at https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile?preview=/46992719/47190130/eidas_interoperability_architecture_v1.00

introduced the concept of a stand-alone API Connector that can be easily deployed within SP's premises, to interoperate with SP existing applications and operations modes, but also transparently integrate with a proxy-based eIDAS Node (Figure 2-2). Essentially, LEPS eIDAS API Connectors implement a gateway between SP's IT premises and the eIDAS Node to provide a two-fold functionality: on one hand, they translate SAML 2.0 protocol requirements to common enterprise standards; on the other hand, they implement a business process model that is able to manage the different stages of the authentication flow via a third-party provider, such as the eIDAS Network. It is implied that LEPS eIDAS API Connectors follow the eIDAS technical specifications for generating and processing authentication messages in terms of signing, encrypting, decrypting etc[8].

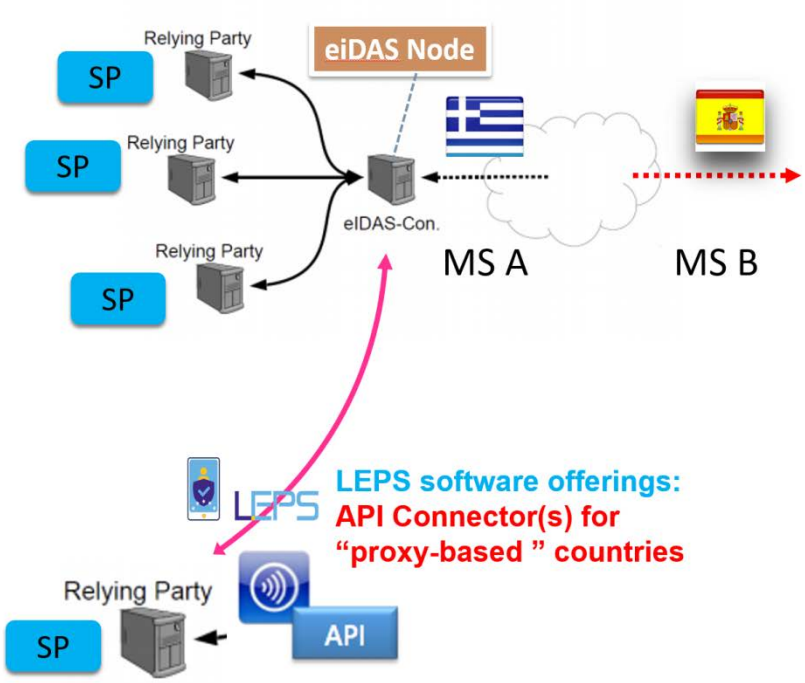

Figure 2-2: eIDAS API Connectors

The successful deployment of LEPS eIDAS APIs within ATHEX and ELTA Service Systems and the realization of a clear operational efficiency (in terms of technological simplicity and cost decrease) were the main methodological challenges for the integration of ATHEX and ELTA Services with the Greek eIDAS Node. As explained in the following chapters, both challenges have been awarded with success. This Deliverable will demonstrate the effectiveness of the integration of ATHEX and ELTA Service Systems with the eIDAS Node via LEPS eIDAS APIs. In terms of the obtained cost and operational gains, we will report in detail in one of the Deliverables of the Activity 7 (Maximizing eID uptake in private sector, sustainability and road-mapping – D7.2: Cost-benefit assessment report).

[8] For a detailed presentation of LEPS eIDAS APIs, see: LEPS D4.2/5.2: "eIDAS Interconnection Supporting Service"

At the end of Activity 4 and 5 (Customization of Greek Financial and Postal Services and Integration with the eIDAS Infrastructure), the following services of ATHEX and ELTA are integrated with the Greek eIDAS Node, thus allowing for single-sign-on on cross-border access from users coming from other EU and EEA countries.

ATHEX:

Application/Service	Functionality
ATHEX Sign (Remote eSignature Service)	(Customer) Registration
ATHEX AXIAweb (Receive electronic information on an Investor's positions in Greek Central Securities Repository)	(Customer) Registration / Login

ELTA:

Application/Service	Functionality
ELTA eDelivery Hybrid Service (cross-border exchange of electronic documents)	(Customer) Register / Login
ELTA Online Postal Services **ELTA portal / eShop**	(Customer) Register / Login
ELTA Online Postal Services **Parcel Delivery Voucher**	(Customer) Login
ELTA Online Postal Services **Online Zip Codes for Business Users**	(Customer) Login / Register

Additionally, ATHEX Identity Provider (IdP) providing a higher LoA level has been also integrated with the eIDAS Network, by following eIDAS Network specifications. A specific interface has been created that implements an eIDAS IdP application workflow, augmented with a two-factor authentication validation service.

ATHEX:

Application	Functionality
ATHEX Identity Service Provider (ATHEX IdP)	Integrate with GR eIDAS Node

3 Definition of Requirements

This section provides a short list of the requirements that should be taken in consideration while implementing ATHEX and ELTA services integration with the Greek eIAS Node. These requirements derive from the operational modes of the eIDAS Network and the technical specifications of the Greek eIDAS Node, but they are also determined by the eIDAS regulation. In addition, the specific application/service requirements in terms of requested attributes, as defined in Tasks 4.1 and 5.1 (Customization of Athens Stock Exchange Services Portal and Customization of Hellenic Post Services Portal), have been considered in this phase of integration work[9].

3.1 Technical and Operational Requirements

Table 3-1 describes the technical requirements derived from the eIDAS Network applying to eIDAS API Connectors development and deployment.

Table 3-1: eIDAS Network (NE) and Node (NO) Interconnection Assumptions (A) and Requirements (R)

Id	Name	Description	Satisfied?
EINEA-1	Interoperability Assumption	The Greek eIDAS Node MUST be able to connect with the Spanish counterpart to provide cross-border authentication.	Yes (GR eIDAS Node)
EINER-1	Integration	eIDAS interconnection tools **MUST** be able to connect with the Greek eIDAS Node and manage the SAML request and response the eIDAS network accepts and provides, respectively.	Yes (LEPS eIDAS API Connectors)
EINER-2	Secure data exchange	eIDAS interconnection tools **MUST** establish secure communication between the SP and the eIDAS network, encrypting messages using secure protocols (TLS or SSH) in the latest version available.	Yes (LEPS eIDAS API Connectors)

Table 3-2 describes the technical requirements derived from the Greek eIDAS Node applying to eIDAS API Connectors dep development and deployment.

[9] See, LEPS D4.1/5.1: "Operational and Technical Documentation of SP customization"

Table 3-2: Greek eIDAS Node Requirements (R)

Id	Name	Description	Satisfied?
EINOR-1	SAML Protocol	eIDAS interconnection tools **MUST** follow SAML2.0 protocol as the rest of the eIDAS network does**.**	Yes (LEPS eIDAS API Connectors)
EINOR-2	Connection	eIDAS interconnection tools **MUST** connect directly to the Greek eIDAS Node.	Yes (LEPS eIDAS API Connectors)
EINOR-3	SP Metadata	eIDAS interconnection tools **MUST** offer a service providing the SP metadata for validation.	Yes (LEPS eIDAS API Connectors)
EINOR-4	Trust	The SP and the eIDAS interconnection tools **MUST** be registered in advance on Greek eIDAS system.	Yes (LEPS eIDAS API Connectors)
EINOR-5	Signing Request	eIDAS interconnection tools **MUST** sign the authentication request to the Greek eIDAS Node.	Yes (LEPS eIDAS API Connectors)
EINOR-6	Signed Response	The signed SAML response provided by the Greek eIDAS Node **MUST** be validated by the eIDAS interconnection tools. If the SAML assertion is signed it **MUST** also be validated.	Yes (LEPS eIDAS API Connectors)
EINOR-7	Cipher	The ciphered SAML assertions, containing user personal data, provided by the Greek eIDAS Node **MUST** be deciphered.	Yes (LEPS eIDAS API Connectors)
EINOR-8	Integrity and authenticity	eIDAS interconnection tools **MUST** verify the integrity and the authenticity of the SAML messages before processing the SAML response provided by the eIDAS Node.	Yes (LEPS eIDAS API Connectors)

3.2 Legal Requirements

Table 3-3 describes the legal requirements derived from the eIDAS regulation[10] and the General Data Protection Regulation (GDPR)[11] (approved by the EU Parliament on 14 April 2016, with enforcement date on 25 May 2018) applying to eIDAS API Connectors development and deployment.

Table 3-3: Legal Requirements (R)

Id	Name	Description
LR-1	Data Minimization	The SP or the eIDAS interconnection tools **MUST** request the minimal data set, needed by the SP for authentication purposes.
Satisfied?	- ATHEX and ELTA services require the minimum eIDAS data set (mandatory attributes: Uniqueness Identifier, Current Family Name, Current First Name, Date of Birth) - Only ATHEX Sign requires a larger set of attributes (both mandatory and optional) since it implements a pre-activation procedure, a sort of customer registration for ATHEX remote e-Signature Service.	
LR-2	User Consent	The SP or the eIDAS interconnection tools **MUST** inform to the user about the requested data
Satisfied?	Yes (LEPS eIDAS API Connectors: Country Selection e-Form) (*) The management of the user consent for data disclosure (i.e. the transfer of identity attributes from the IdP to the requester SP) is part of the eIDAS Node functionality.	
LR-3	Data Protection	The eIDAS interconnection tools **MUST** provide to the user information about the use of his/her data, and **MUST** provide information on how to exercise his/her rights
Satisfied?	Yes (LEPS eIDAS API Connectors: Country Selection e-Form/information part on the right of the page).	

[10] European Commission, eIDAS Observatory, see:

https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014. Retrieved date 2018/05/23

[11] EUR-Lex, Access to European Union law, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, see:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

4 LEPS eIDAS API Connectors: a functionality overview

The eIDAS Network defines and deploys a pan-European infrastructure for cross-border user authentication purposes that enables the interoperability of national eID schemes and the interconnection between SPs and IdPs located in different EU countries. The communication between the various parties involved is defined over SAML 2.0. By integrating with the eIDAS Network, a SP acts as an eIDAS Network Relying Party. A SP can therefore use a trusted and secure federated environment through which cross-border user authentication to the services it provides to customers, is conducted seamlessly.

However, for the SPs to be willing to adopt and deploy eIDAS solutions as part of their business models, the integration must be made as easy as possible, and efficient in terms of operational requirements and investment costs. Additionally, the resulting system must be mobile friendly and designed with user experience in mind.

Specifically, for an SP to successfully connect to a (proxy-based) eIDAS Node the following tasks must be undertaken:

1. Familiarization with SAML communication (protocol understanding and implementation).
2. Implementation of the required web interface (User Interface / UI) for User interaction with the eIDAS-enabled services.
3. Formulation and proper preparation of an eIDAS SAML Authentication Request.
4. Processing of an eIDAS Node SAML Authentication Response and provision of the appropriate authentication process end events for success or failure.
5. Publishing of the SP's metadata, as is required by the CEF eIDAS Specifications.

To facilitate the execution of the above tasks, LEPS provides a cost and operation effective strategy that consists of using a standardized, open source, off-the-shelf Connection Facility to make SP applications *de facto* interoperable with an eIDAS Node (proxy-based)[12].

4.1 LEPS API Connectors: components and functionality

The following figure illustrates the usage of this facility (called LEPS eIDAS APIs) within the eIDAS Network infrastructure.

[12] For a detailed presentation of LEPS eIDAS APIs, see: LEPS D4.2/5.2: "eIDAS Interconnection Supporting Service"

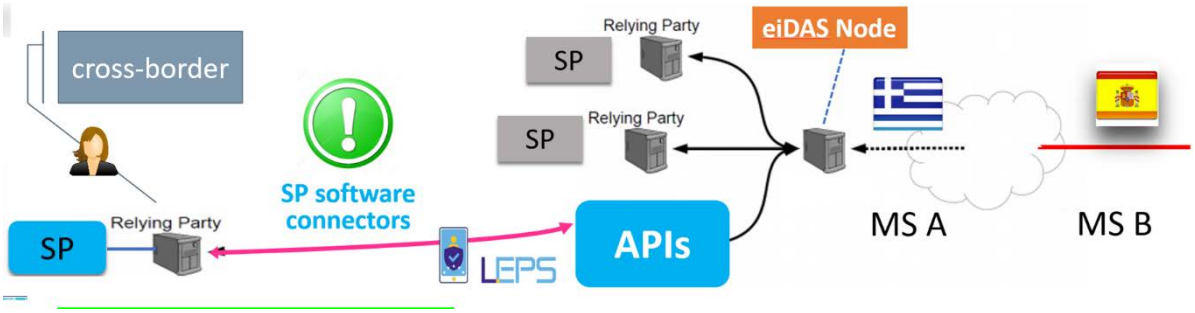

Figure 4-1: SP Integration with eIDAS Node using Connector(s)

It is a stand-alone API Connector that can be easily deployed within SP's hosting environment reducing the complexity of communication with the eIDAS network to that of consuming a REST API (a task similar to integrating with Open ID Connect standards). Once deployed this API connector handles for the SP the tasks that appear in the following Table.

Table 4-1: Overview of functionality of LEPS eIDAS API Connectors

Manage requests to eIDAS Node
Provide next-to-login authRequest-UI (includes country e-Form and SP-requested attributes list)
Construct and propagate SAML 2.0 authRequest
Publish SP metadata
Manage responses from eIDAS Node
Process authResponse (as received from eIDAS Node)
(On success) Provide authResponse translated from SAML 2.0 to common enterprise standards (JSON, SOAP), and redirect user to SP
eIDAS authentication failure report
Support SP authentication policy (optional)

Yet, LEPS API Connectors provide a method to connect to an eIDAS (proxy-based) Node depending on specific SP requirements. Three efficient solutions (presented in next Table) with different characteristics are provided. In the integration of ATHEX and ELTA services, two of them have been extensively used: eIDAS Interconnection Supporting Service 2.0 (eIDAS ISS 2.0) and eIDAS SP WebApp 2.0

Table 4-2: LEPS eIDAS API Connectors used in the integration of ATHEX and ELTA services

LEPS eIDAS API Connectors		Used in the integration of ATHEX and ELTA Services?
1	eIDAS SAML Tools Lib	No
2	eIDAS Inteconnection Supporting Service 2.0 (eIDAS ISS 2.0)	Yes
3	eIDAS SP WebApp 2.0	Yes

4.1.1 LEPS eIDAS ISS 2.0

The eIDAS ISS 2.0 solution simplifies the connection of any SP, regardless whether it is Java-based or not. It provides the following list of functionalities to the SP.

1. Enables SPs to communicate with the eIDAS Node without using SAML 2.0.
2. One ISS 2.0 installation can support multiple services within the same SPs.
3. Simple public web access to the log file of all requests served by the ISS 2.0.
4. Endpoint communication method: JSON.
5. Each request can be parameterized (explained below) by:
    a. the Attributes requested.
    b. the Citizen/User Nationality.
    c. the Level of Assurance Requested.
6. On Authentication failure, two "Attributes" are provided ("StatusCode" and "StatusMessage"), providing the SP with information on the cause. These are provided and defined by the eIDAS infrastructure.

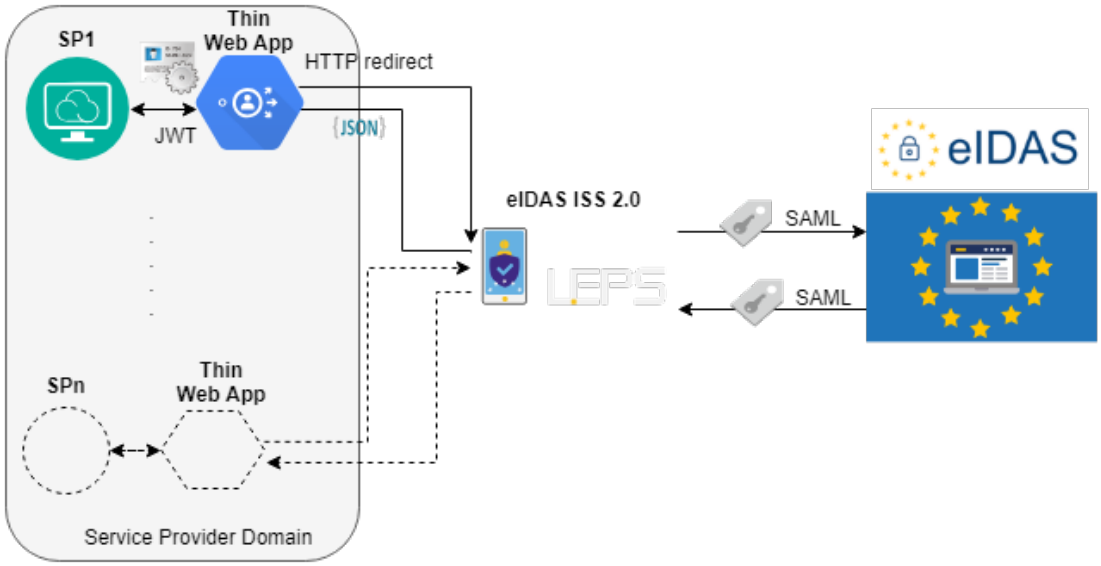

Figure 4-2. eIDAS ISS 2.0 (plus this WebApp)

A (thin) WebApp User Interface complements the ISS 2.0 functionality by containing a prebuilt UI that the SPs can use and also require from the SPs to build fewer end points in order to retrieve the identification attributes from the eIDAS Node (Figure 4-2).

Specifically, the Thin WebApp acts as a proxy between the actual SP service and the ISS 2.0. It handles all the interaction with the ISS 2.0 and requires from the SP to build only one new endpoint to receive the identification attributes. These attributes are next bundled as a JSON Web Token (JWT) signed by the Thin WebApp for increased security. This JWT finally reaches the SP either as an HTTP only cookie, as an HTTP header or finally as a URL parameter.

4.1.2 LEPS eIDAS WebApp 2.0

The eIDAS WebApp 2.0 offers to the SP identical interfaces as the Thin WebApp, but has embedded the ISS 2.0 functionality. The eIDAS WebApp 2,0 is intended for use by SPs that either wish to connect only a single application to eIDAS or wish to connect a service that is expected to handle significant traffic, or requiring a tailored solution, and is thus better served by a dedicated eIDAS interconnection web application. Specifically, the eIDAS WebApp 2.0 facilitates the integration of a SP with the eIDAS Node by:

1. Allowing the SP to avoid development time for processing SAML messages.
2. Completely handling an eIDAS-based authentication flow (including UIs).
3. Being SP infrastructure independent; operates over a simple REST API.
4. Providing strong security assertions in the form of JSON Web Token, JWT (RFC 7519).

Specifically, the eIDAS WebApp 2.0 handles all communication with a proxy-based eIDAS Node (generation and parsing of SAML messages, publication of SP metadata and out-of the box UIs). At the end of an eIDAS authentication process the eIDAS WebApp 2.0 receives the identification attributes from the eIDAS Node and generates a JWT token containing those attributes. An example of such a token can be seen on the table below.

```
{
"sub":"{\"firstName\":\"ΑΝΔΡΕΑΣ, ANDREAS\",\"eid\":\"GR/GR/ERMIS-
11076669\",\"familyName\":\"ΠΕΤΡΟΥ,
PETROU\",\"personIdentifier\":\"GR/GR/ERMIS-
11076669\",\"dateOfBirth\":\"1980-01-01\"}",
"origin": "eIDAS"
}
```

This JWT token is signed from the eIDAS WebApp 2.0 either using HS256 or RSA (after exchange of public keys with the SP). Finally, the token is sent back to the SP either as an HTTP only cookie, or as a URL parameter or finally as an HTTP header. All options are available using the appropriate configuration.

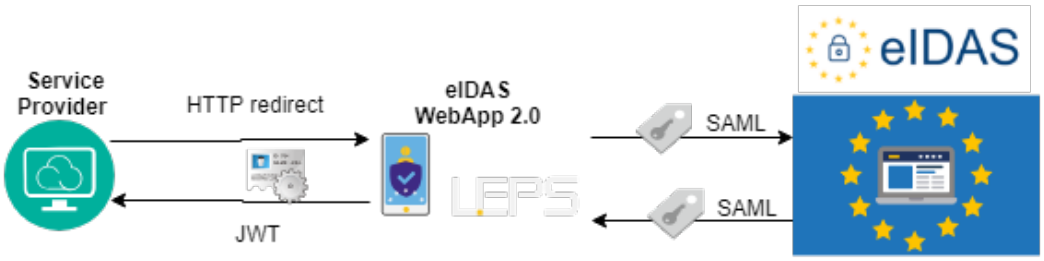

Figure 4-3. eIDAS WebApp 2.0

4.2 Authentication flows: Service Provider – LEPS APIs – eIDAS Network

For all SPs using LEPS eIDAS API connectors, the main steps of an eIDAS Network-based authentication using the provided are the following:

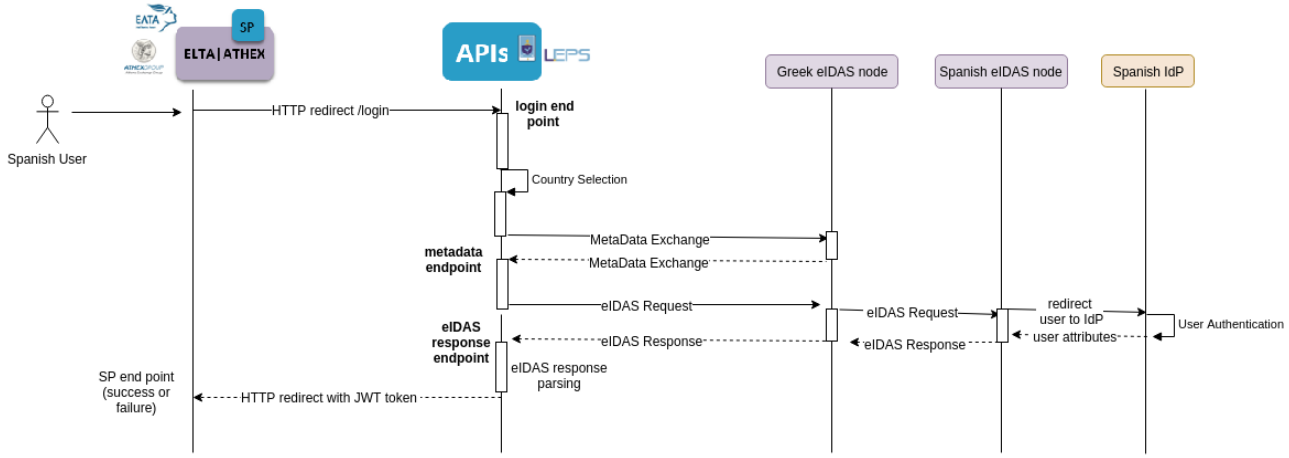

Figure 4-4: Integration Flow (SP -eIDAS API Connectors - eIDAS Node)

The main components involved in this process are playing the following role:

- Services: ATHEX and ELTA services where the user initiates the authentication process.
- LEPS eIDAS API Connectors: The connector modules (eiDAS ISS 2.0 plus Thin Web App - eIDAS WebApp 2.0) handling the authentication of the user over eIDAS.
- eIDAS Network: Connecting each country eIDAS Node developed by the EU Member State.
- The IdP: Performing the user authentication.

1. The **Service Provider** configures and deploys an API Connector with a UI instance (ISS 2.0 with Thin WebApp, or eIDAS WebApp 2.0)
2. The **Service Provider** redirects authentication requests from the application login page (Login with eID_EU) to the deployed **API Connector/UI**.

a. Redirection is a simple browser redirection to the "Country e-Form" (no parameters are required).
b. The User selects "Country".

3. The **API Connector/UI** transfer to the **API Connector**: <listOfRequestedAttributes> and the <selectedCountty>
4. The **API Connector** takes as input what it receives and formulates as output an appropriate eIDAS SAML authentication request.

User's Country

5. The SAML authentication request is next transmitted to the near (proxy) **eIDAS Node** (GR in occurrence) and, then to the eIDAS infrastructure of the Country the User has dispatched the authentication process (ES in occurrence).
6. The User is authenticated using the eIDAS flow (eIDAS Node – IdP – back to eIDAS Node); the output of the eIDAS authentication flow an eIDAS SAML authentication response.
7. The **eIDAS Node** of the Country the User has dispatched the process (ES in occurrence) forwards the eIDAS SAML authentication response to the eIDAS Node that has initiated the authentication request (GR in occurrence).

Back to SP's Country

8. The **eIDAS Node** which receives the authentication response (GR in occurrence) forwards it to the **API Connector**
9. The **API Connector** processes and decrypts the authentication response and asks from the **API Connector/UI** to generate a JWT token that contains all the retrieved eIDAS attributes (plus the UUID of the session, generated in the beginning of the process). Essentially, the API Connector/UI creates the appropriate identification assertions for the eIDAS authenticated User, so that the SP service can easily consume them.
    a. If an "error" occurred during authentication, such as a failure in the authentication of the User to the IdP, the Connector/UI handles it by displaying an appropriate message to the user.
10. The JWT token is forwarded to **SP's** Service Point[13], to the Service Point "success endpoint" if the authentication was successful, or to the Service Point "failure endpoint" in case an error occurred. The SP retrieves the JWT from the *http request* and acts accordingly (verifies its signature and authenticates the User or handles the error).
    a. The User is redirected to the SP application/service, where she had submitted a "Login with eID_EU" request (or to an "Authentication Terminate" page, in the case of an authentication error).

[13] We define a Service Point as: a) the minimal SP configuration that redirects a user's login request to an API (Connector), when the user selects "register/login via eID_EU" and, b) the sum of endpoints where the API (Connector) will forward to SP application/service the *authResponse* data received from the eIDAS Node (*auth* success or failure report). A more detailed presentation of the concept of Service Point will include in chapper 5 of this document.

4.3 Technologies

For the implementation of the LEPS eIDAS API connectors presented in this document several technologies as well as standards and protocols were used. Specifically, the implementation of the all offered APIs took place using the Java language (version 8.0). Additionally, several frameworks and tools were required.

- Spring Boot[14]: Creates stand-alone Spring applications, embedding Tomcat as application server, avoiding the war files deployment (used in the Web App 2.0 and Thin Web App implementations)
- Struts 2[15]: Framework for creating Java EE web applications, based on the "ModelView Controller" architectural model (MVC), extending Java Servlet API, managing the authentication process flow. As drawbacks the use of this technology is decreasing, and some vulnerabilities have been found recently (used in the ISS 2.0 implementation)
- JWT[16]: Industry standard method (RFC 751), defining a self-contained object to securely transmit information between the SP and the eIDAS adapter. This token includes the user data (used in the Web App 2.0 and Thin Web App implementations)
- SAML 2.0[17]: XML-based framework for transmitting user authentication between the eIDAS adapter and the eIDAS network, in both ways (used in the Web App 2.0 and ISS 2.0 implementations)
- eIDAS Technical Specifications[18]: During the implementation process these specifications have been taken into consideration and used. This European standard, which includes cryptography and cyphering, is based on SAML 2.0 standard; (used in the Web App 2.0 and ISS 2.0 implementations)
- Maven[19]: Software project management tool for managing dependencies with java code libraries for developing code and project's build ;(used in all API implementations)
- Apache Tomcat[20]: Web application server where the eIDAS adapter is running; (used in all implementations)
- Docker[21]: This platform facilitates the application deployment, avoiding dependencies between application and infrastructure (used in the Web App 2.0 and Thin Web App implementations)

[14] https://spring.io/projects/spring-boot

[15] https://struts.apache.org/

[16] https://jwt.io/introduction/

[17] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[18] European Commission, eIDAS Technical Specifications v.1.1, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2016/12/16/eIDAS+Technical+Specifications+v.+1.1

[19] https://maven.apache.org/

[20] http://tomcat.apache.org/

[21] https://www.docker.com/

- GitHub[22]: Repository for uploading the project source code or the artefacts created during the implementation process. Also used for bug tracking (used in all implementations).

4.4 Deployment

The ISS 2.0 is offered as a Java web application bundled in a *".war"* file and thus need to be deployed in an appropriate application server such as Tomcat. The *Web App 2.0* and *Thin Web App* are built as Spring Boot applications (with embedded Tomcat). Also, these two offerings are published as Docker images and can thus be deployed in any host running a Docker machine.

For more information regarding the deployment and configuration of these API connectors please refer to their Github page at: https://github.com/uaegeani4mlab/LEPS-APIs.

[22] https://www.github.com/

5 Interconnection of ATHEX and ELTA Services with the Greek eIDAS Node

In this section we present the interconnection of ATHEX Group and Hellenic Post services with the Greek eIDAS Node using LEPS eIDAS API Connectors. First a brief description of the services that have been integrated with the eIDAS Node is given. Next the high-level architecture of ATHEX and ELTA Connection to Greek eIDAS Node via LEPS eIDAS API Connectors is presented as well as the proposed architecture solutions. Finally, we describe ATHEX and ELTA architecture in detail and we give an overview of the mobile integration of the services.

SP e-services that have been integrated with the eIDAS Network are presented in the following table.

Table 5-1. ELTA & ATHEX: List of e-Services integrated with the eIDAS Network

ELTA & ATHEX: List of e-Services integrated with the eIDAS Network		
	ELTA	**ATHEX**
1	**ELTA eDelivery Hybrid Service** Cross-border exchange of electronic documents Functionality: (Customer) Register / Login	**ATHEX Sign** Remote eSignature Service Functionality: (Customer) Registration
2	**ELTA Online Postal Services** ELTA portal / eShop Functionality: (Customer) Register / Login	**ATHEX AXIAweb** Receive electronic information on an Investor's positions in Greek Central Securities Repository Functionality: (Customer) Registration / Login
3	**ELTA Online Postal Services** Parcel Delivery Voucher Functionality: (Customer) Login	**ATHEX IdP** Identity Service Provider
4	**ELTA Online Postal Services** Online Zip Codes for Business Users Functionality: (Customer) Register / Login	

A brief summary of the functionality of these services is provided below in the objective to explain the business logic of the integrated services. A detailed presentation of the functionality of these services is included in the deliverable D4.1[23].

5.1.1 ATHEX Services

- **ATHEX Sign** is the service of remote e-signature provided by the Athens Exchange Group (ATHEX Group). As stated within "D2.1 LEPS Service Design Document" and "D4.1/D5.1 Operational and Technical Documentation of SP (ELTA, ATHEX) customization", the scope

[23] See, LEPS D4.1/5.1: "Operational and Technical Documentation of SP customization"

of the project includes integration with the eIDAS Network for two e-services services: ATHEX Sign (Registration) & ATHEX AXIAweb (Registration and Login). This integration will allow European users coming through the MS eIDAS Nodes to connect to the ATHEX e-services.

  - The service requires a pre-activation procedure, a sort of customer registration. Customers get ATHEX IdP credentials (username/password or digital certificate) when they complete successfully the physical identification process against the ATHEX Certificate Authority
  - Upon successful registration, a User can process with the main service and digitally sign documents "on the go". ATHEX automates the pre-activation procedure with support from the eIDAS Network. As a result, the users will not be requested to deliver the Subscriber Agreement together with a validated copy of their identity card, as it happens today, but to authenticate and register via eID_EU (with obvious benefits from both the users and the company).

- **ATHEX AXIAweb** is the service providing information on the positions of an investor in the Greek Central Repository Group. ATHEX integrates the AXIAweb service with the eIDAS Network. As a result, a user can both register and login AXIAweb site to review her portfolio in the Greek Stock Exchange Market ("Portfolio Access" page).
- Additionally, **ATHEX IdP** is integrated with the eIDAS Network via a specific that implements an eIDAS IdP application workflow augmented with a two-factor authentication validation service. **ATHEX Identity Service Provider (ATHEX IdP)** delivers an eIDAS compliant identity provision service for all customers of Athens Stock Exchange (ATHEX) who have issued a qualified digital certificate from its certificate authority infrastructure[24]. ATHEX IDP is therefore available to every Service Provider (both in Greece and cross-border) using the eIDAS authentication infrastructure.

5.1.2 ELTA Services

- **eDelivery Hybrid Service**: This service merges the functionality of Document Management and Workflow System (DMWS) with the Hybrid Mail Service of ELTA. The users, after registration, will be able to:
  - Send electronic documents using both the ELTA eDelivery network and the Hybrid Mail Service (sender functionality)
  - Receive documents (recipient functionality)
    - If customers are part of eDelivery network: receive electronic documents and manage delivery evidence through an eDelivery personalized inbox
    - If customers are not part of eDelivery network but they have a physical address: receive a physical letter that includes a URL link from where they can download the electronic document that a sender has addressed to them while the application keeping track and providing evidence on the details of

both postage and reception (day and time, secure copy of the original document etc.).

- **ELTA Portal / e-Shop**: ELTA Portal / e-shop offers to both individuals and corporate customers online postal services and e-shop services such as (indicatively): Letter mail services, Parcel services, Prepaid envelopes, Letter mail products, Packaging, Fragile items envelopes, Telephony products, MailBoxes, Philatelic Products etc.
- **Online Parcel Voucher**: Online Parcel Voucher is an e-service provided by ELTA, available to both individual customers and business, but mostly used by SMEs as a B2C service. Users can print online the accompanying vouchers for parcels. The service is vastly used from companies selling through e-Commerce (part of the eltab2b service offerings).
- **Online Zipcodes for Business Users**: This is an on-line service offered by ELTA to corporate customers, allowing them to obtain the current version of Zip codes of Greece. These codes are available in two languages (Greek and English) -- he downloadable files are updated by the Hellenic Post whenever a new version is publishing. ELTA augments the existing service functionality with integration with the eIDAS Network while simplifying the application logic to create a "fast-track" e-shop, thus improving service customer experience. The user is able to register and login via the eIDAS Network (as well as through local credentials). Upon successful completion of the authentication process, the user is redirected back to service web page, to access an e-payments page. After verification of the payment, the user can download the Zipcodes file (part of the eltab2b service offerings).

5.2 ATHEX and ELTA connection to Greek eIDAS Node via LEPS eIDAS APIs: high level architecture

The use of LEPS eIDAS API Connectors from a Service Provider (SP) requires the deployment of the appropriate API Connectors and the creation of a Service Point which serves as the anchor for the LEPS eIDAS APIs within the IT infrastructure of a Service Provider (SP). LEPS supports SP application/service integration with eIDAS Node thanks to Service points and API Connectors (Figure 5-1).

The use of LEPS eIDAS API Connectors from a Service Provider (SP) requires the deployment of the appropriate API Connectors and the creation of a Service Point which serves as the anchor for the LEPS eIDAS APIs within the IT infrastructure of a Service Provider (SP). We define a Service Point as:

1. The minimal SP configuration that redirects a user's login request to an API (Connector), when the user selects "register/login via eID_EU"
2. The sum of endpoints where the API (Connector) will forward to SP application/service the authResponse data received from the eIDAS Node (authentication success or failure report)

In the case of a SP providing multiple services, each service is connected to a different Service Point.

Obviously, the SP infrastructure use the Service Point to redirect the user to LEPS eIDAS APIs interfaces (1-2) and receive the authentication response (5-6) -- (Figure 5-1). The essential of the interconnection with the Greek eIDAS Node, including the creation of the authentication request and the process of the authentication response, is taken in charge by the API Connector (3-4).

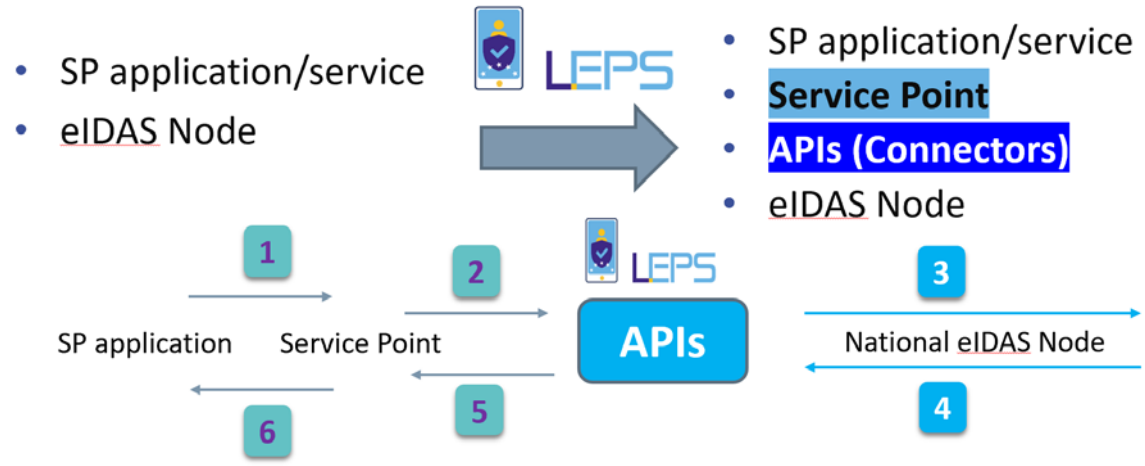

Figure 5-1. LEPS eIDAS API Connectors and Service Points – a generic view

The following table presents the list of the Service Points (with their corresponding endpoints) as those were deployed per service for the needs of the project by each SP. Since ATHEX IdP service does not use an API Connector it is not included in the table below. A description of the interconnection of ATHEX IdP with the Greek eIDAS Node is provided in the end of this section.

Table 5-2. LEPS eiDAS API Connectors and Service Points (ELTA - ATHEX)Service	**Service Point**	**Endpoints**
ELTA eDelivery Hybrid Service	http://www.e-post.gr	• Success Endpoint: http://safas/portalRedirect.jsp • Fail Endpoint: http://asdffsdaf/portalLogin.jsp?disconnected=1
ELTA Portal/e-shop	http://www.elta.gr	• Success Endpoint: http://www.elta.gr/el-gr/eidaslogin.aspx • Fail Endpoint: http://www.elta.gr
ELTA Online Parcel Voucher	http://www.eltab2b.gr	• Success Endpoint: http://www.eltab2b.gr/plugins/authentication/eid/login.php • Fail Endpoint: http://www.elta.gr

ELTA Zipcodes for Business Users	http://www.eltab2b.gr	• Success Endpoint: http://www.eltab2b.gr/plugins/authentication/eid/login.php • Fail Endpoint: http://www.eltab2b.gr
ATHEX Sign	https://athex-sign.athexgroup.gr	• Success Endpoint: https://www.sp-gw.eidas.athexgroup.gr/regAthexSign • Fail Endpoint: https://athex-sign.athexgroup.gr
ATHEX AXIAweb	https://www.axiaweb.gr/AXIAWeb/gr/login	• Success Endpoint: https://www.axiaweb.gr/AXIAWeb/gr/EidasResponse.jsp • Fail Endpoint: https://www.axiaweb.gr/AXIAWeb/gr/login

5.3 Connection to Greek eIDAS Node: eIDAS ISS 2.0 vs eIDAS WebApp 2.0 architecture solutions

The Service Providers, ATHEX and ELTA, took into consideration the special requirements for each offered service and decided on the deployment of two Architecture Solutions:

1. **Architecture Solution 1** (ISS 2.0 plus Thin Web App): Integrates a **set of SP services** to the eIDAS Network **under a common "umbrella"**, i.e. the eIDAS ISS 2.0 API Connector
2. **Architecture Solution 2** (eIDAS WebApp 2.0): Integrates a single SP service to the eIDAS Network, in the case of **a service having special needs like supporting heavy traffic or needing a tailored interconnection** to the eIDAS Network.

Specifically, in the case of ATHEX it was decided that all of the offered services (apart from the ATHEX IdP which naturally follows a different interconnection architecture) to be integrated to eIDAS using the same eIDAS ISS 2.0 instance. Additionally, each service was coupled with its own Thin Web App removing the need for UI development and reducing the endpoint development needs. This situation is presented in the next figure (ATHEX services have been deployed using the Architecture Solution 1).

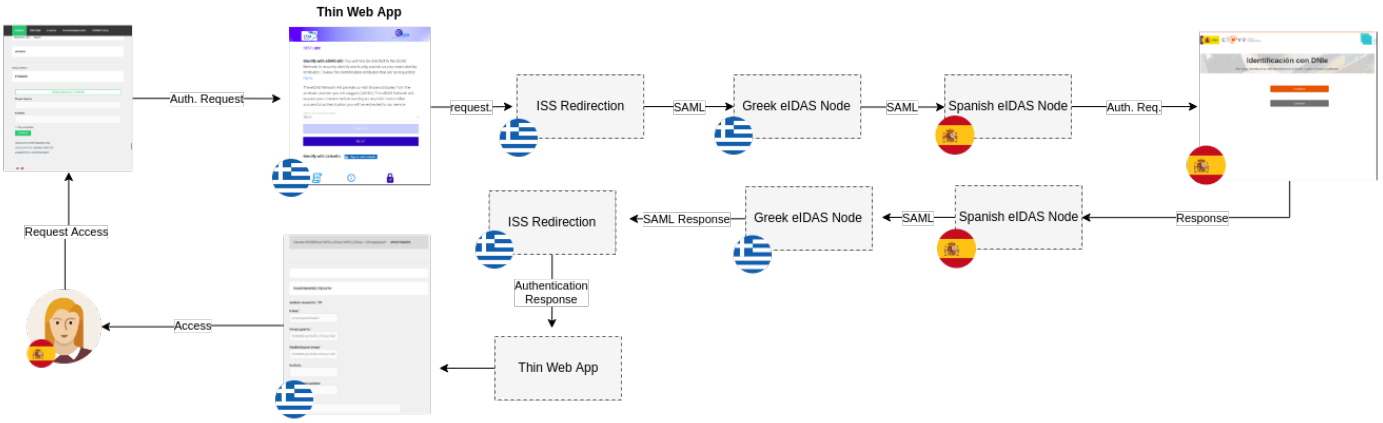

Figure 5-2. ATHEX Services Authentication User Screen Flow (based on Architecture Solution 1)

ELTA's architecture is slightly different. In the context of LEPS, ELTA has upgraded one of its services into a new service called "ELTA eDelivery Hybrid Service". This service is expected to serve a great volume of requests and thus it was decided that a separate connection to the eIDAS Node would serve its needs better. For this reason, the integration with the Greek eIDAS Node took place with the *eIDAS Web App 2.0* (Architecture Solution 2). The screen Authentication flow for this service can be seen in the following figure.

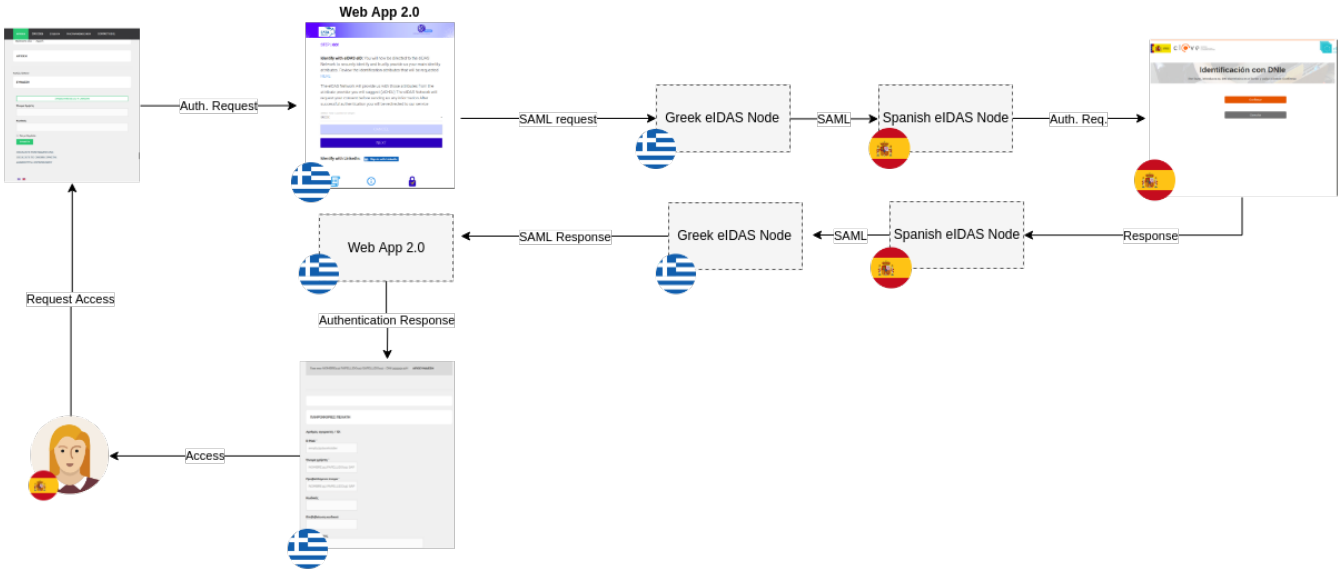

Figure 5-3. ELTA eDelivery Hybrid Service Authentication User Screen Flow (based on Architecture Solution 2)

The rest of the services offered by ELTA were developed using the Architecture solution 1 (i.e. *eIDAS ISS 2.0* with *Thin Web App*).

From the previous analysis it should be made clear that the authentication flows of the services of the SPs present many similarities. Specifically, there exist two different authentication flows depending on

the Architecture solutions. ATHEX has employed Architecture Solution 1 that is depicted in Figure 5-4.

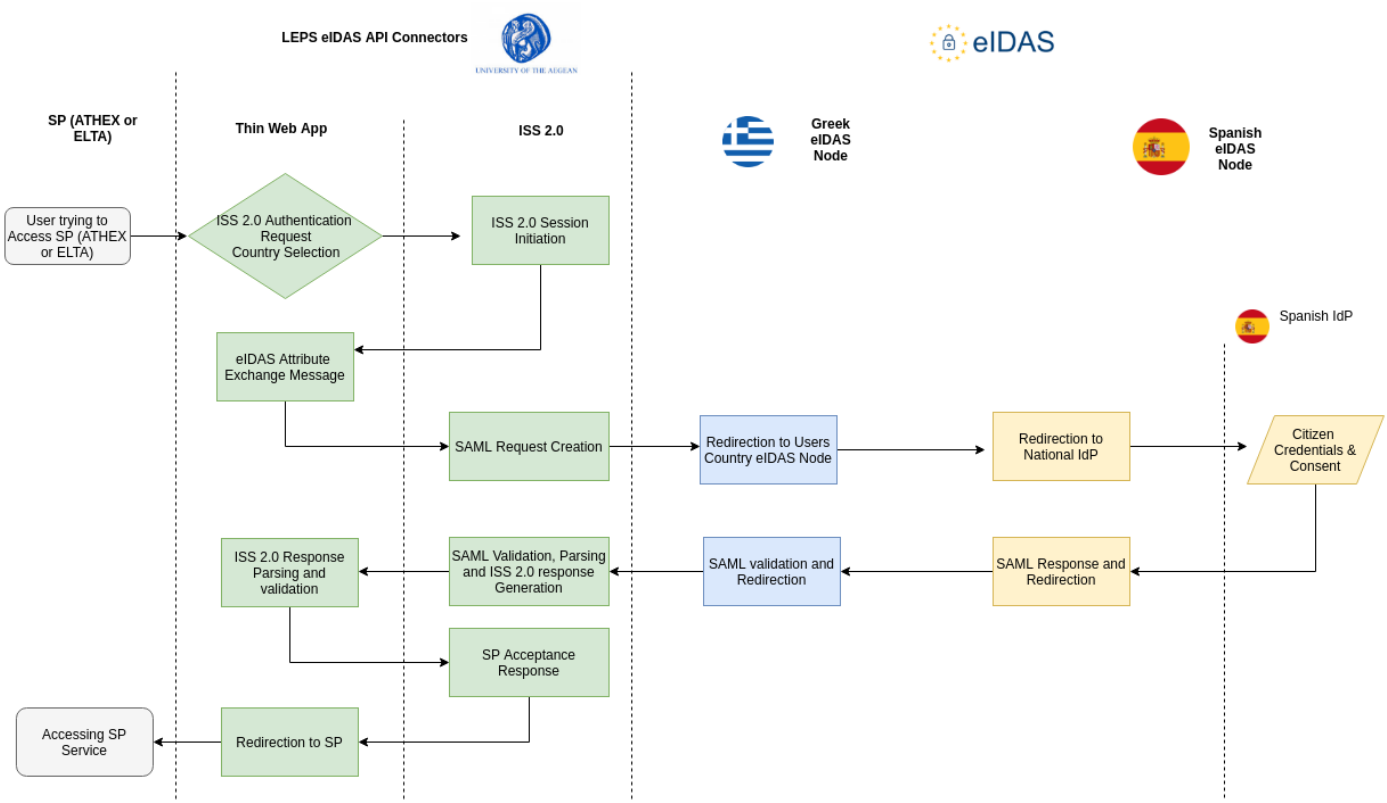

Figure 5-4. Architecture Solution 1 - high level sequence diagram

ELTA has employed both Architecture Solutions 1 and 2. A high level sequence diagram for Architecture Solution 2 is depicted in Figure 5-5.

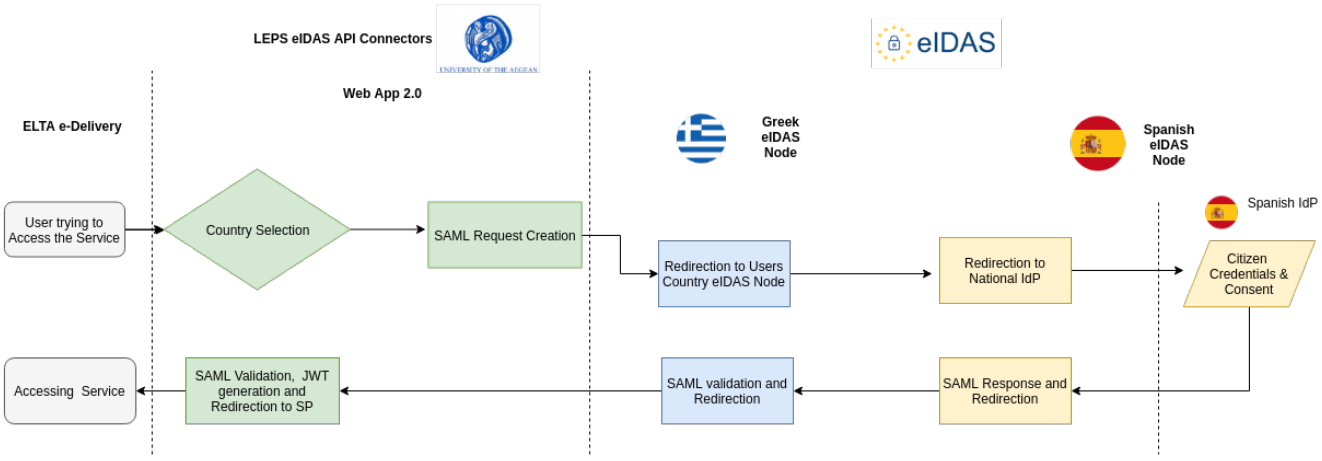

Figure 5-5. Architecture Solution 2 - high level sequence diagram

The actual sequence diagrams for both architecture approaches are similar. The most important differentiation is the interaction between the ISS 2.0 instance and the *Thin Web App* in Architecture 1, which is not present in Architecture 2 since the functionality of ISS 2.0 and the necessary UIs are natively integrated in the same application, can be seen in the following sequence diagrams.

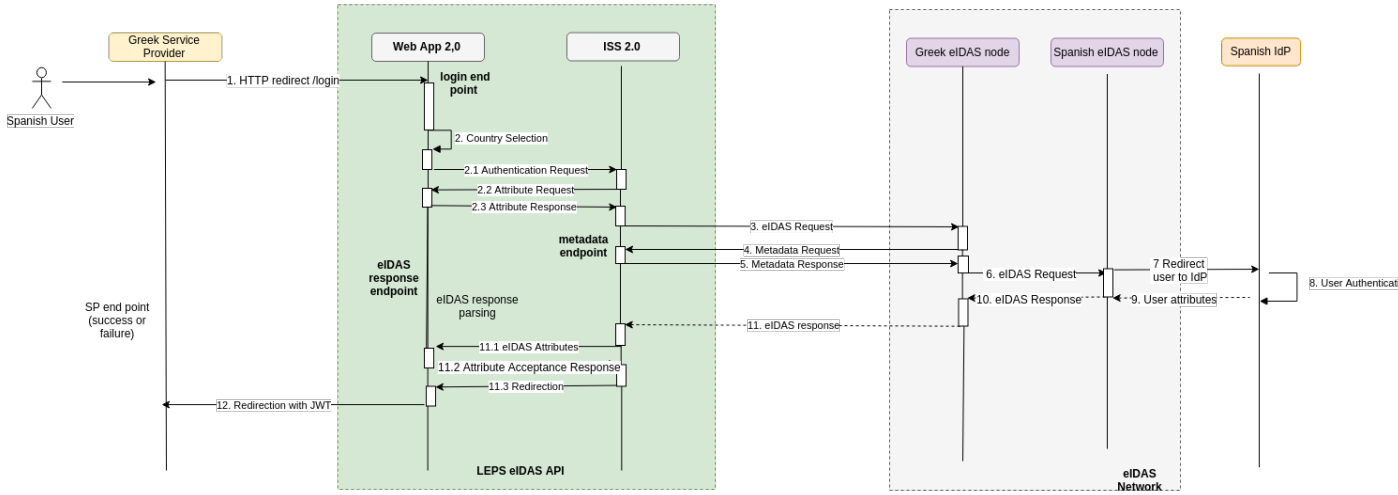

Figure 5-6. Sequence Diagram for Architecture Solution 1

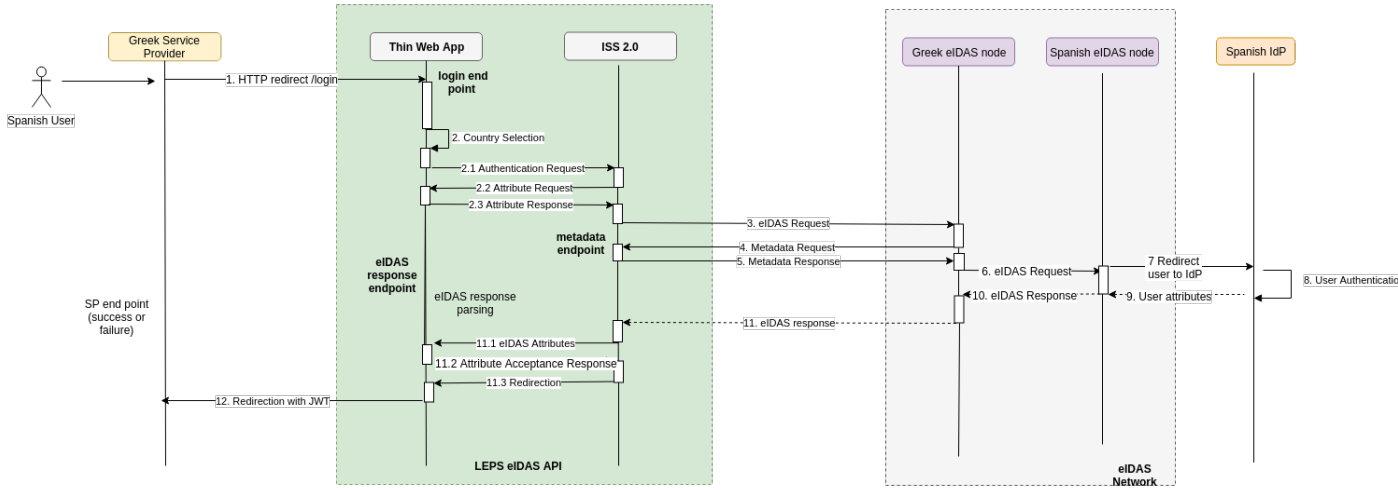

Figure 5-7. Sequence Diagram for Architecture Solution 2

Specifically, for the case of Architecture 1 (Figure 5-6) we have the following steps:

1. The SP service redirects the user authentication request to the *Thin Web App* (country selection page).
2. The user selects her country of origin
    a. The *Thin Web App* sends an authentication request to ISS 2.0.
    b. ISS 2.0 request from the *Thin Web App* which attributes will be requested from the eIDAS network.
    c. The *Thin Web App* responds with which attributes it needs to request.

3. ISS 2.0 generates the appropriate SAML request and forwards it to the Greek eIDAS Node.
4. The Greek eIDAS Node requests (if not cached) the metadata published by ISS 2.0.
5. ISS 2.0 responds with the appropriate metadata.
6. The Greek eIDAS Node generates an appropriate request for the Spanish eIDAS Node.
7. The User is redirected to the Spanish IdP.
8. The User presents her credentials.
9. The Spanish IdP sends the identification attributes to the Spanish eIDAS Node.
10. The Spanish eIDAS Node generates an appropriate attribute response and sends it to the Greek eIDAS Node
11. The Greek eIDAS Node sends the response to ISS 2.0:
    a. ISS 2.0 sends the attributes to the *Thin Web App* (back-channel communication).
    b. The *Thin Web App* responds if some error occurred.
    c. ISS 2.0 redirects flow to the Thin Web App.
12. Thin Web App formulates a JWT containing the attributes received and forwards it to the SP service.

The sequence diagram for the Architecture Solution 2 (Figure 5-7) is almost identical to that of the first solution (the only difference is that there exist no steps 2.1, 2.2, 2.3 and 11.1, 11.2, 11.3) and that the communication in steps 3, 4, 5 and 11 takes place between the WebApp 2.0 and the Greek eIDAS Node.

5.4 ATHEX architecture in detail

In the case of the ATHEX Services, the Architecture Solution 1 was deployed. In other words, a single instance of the eIDAS ISS 2.0 service was used to connect all of the offered services combined with two *Thin Web Apps* (TWA). This architecture solution was decided because it provides the ability of a single API Connector (eIDAS ISS 2.0) to connect with the Greek eIDAS Node, effectively acting as a "proxy" service for the internal ATHEX services (i.e. ATHEX Sign and ATHEX AXIAweb), as shown on the table below.

Table 5-3: ATHEX Services and corresponding Module

Application/Service	eIDAS API Connector
ATHEX Sign (Remote eSignature Service) Customer registration (pre-activation procedure)	eIDAS ISS 2.0
ATHEX AXIAweb (Receive electronic information on an Investor's positions in Greek Central Securities Repository) Customer registration (pre-activation procedure) a and Service login	

Figure 5-8 illustrates the architecture that was used in the ATHEX case

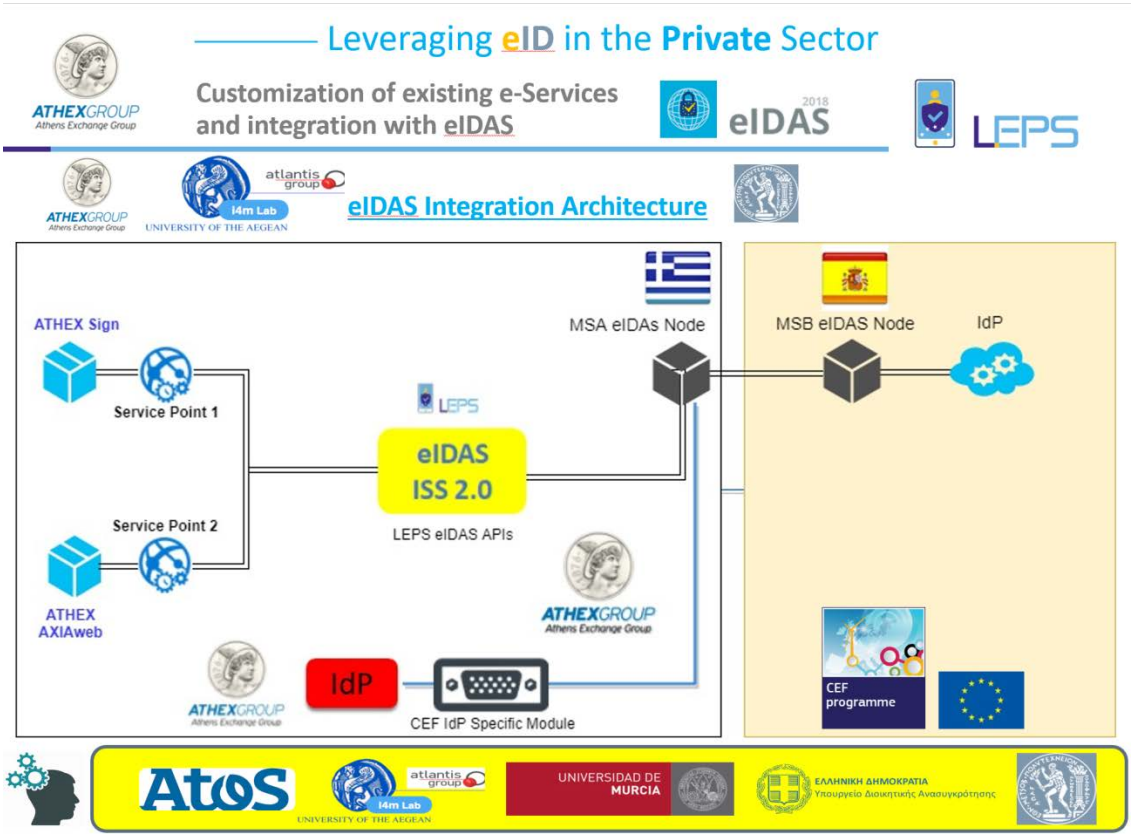

Figure 5-8: ATHEX Services Architecture

For each service connected using this Architecture Solution, the SP built a single Service Point with several Endpoints (see Figure 5-8). These endpoint extracts the JWT from an HTTP only cookie ("access_token") generated by the TWA containing the user authentication attributes and authorizes the access to the service accordingly, or manage the authentication failure process.

The ATHEX hosting machines Operating System made the deployment of Docker Machine problematic. While this posed no problems in deploying eIDAS ISS 2.0, deployment of the TWAs was not possible out of the box. Additionally, the TWA is built as a Spring Boot application with an embedded Tomcat server. While this approach is ideal for dockerizing an application (since configuration of the Docker file becomes simply the definition of the execution of the appropriate ".jar" file), it is not ideal for a production deployment of a service. Embedded Tomcat is more difficult to parameterize and does not offer out of the box deployment standards such as restart on system reboot for example.

For these reasons, the TWA source code was retrieved from the relative repository and its configurations were altered so that instead of the project being built to an embedded Tomcat service, for it to build it as a simple ".war" file deployable in any application server (e.g. Tomcat). This allowed ATHEX to simply deploy these two TWA instances in a per-existing Tomcat instance.

5.5 ELTA Architecture in detail

As in the case of the ATHEX Services, the ability of a single eIDAS ISS 2.0 to support multiple Services makes it a prime candidate for its adoption in the services provided by the ELTA, as seen in the following Table:

Table 5-4: Hellenic Post Services and corresponding Module

Applicatiion/Service	eIDAS API Connector
ELTA eDelivery Hybrid Service (cross-border exchange of electronic documents)	eIDAS SP WebApp 2.0
ELTA Online Postal Services **ELTA portal/e-shop**	eIDAS ISS 2.0
ELTA Online Postal Services Parcel Delivery Voucher	
ELTA Online Postal Services Online Zip Codes for Business Users	

5.5.1 ELTA eDelivery Hybrid Service

The *eDelivery Hybrid Service* however is a service that is expected to support a significant number of user requests. For this reason, the stateless nature of authentication provided by the second Architecture Solution (i.e. integration using the eIDAS WebApp 2.0), that allows vertical scalability by simply increasing the number of Docker Containers of the eIDAS WebApp 2.0 and using a load balancer, was considered as the optional of the available alternatives.

The overall integration strategy deployed by ELTA can be seen in Figure 5-9.

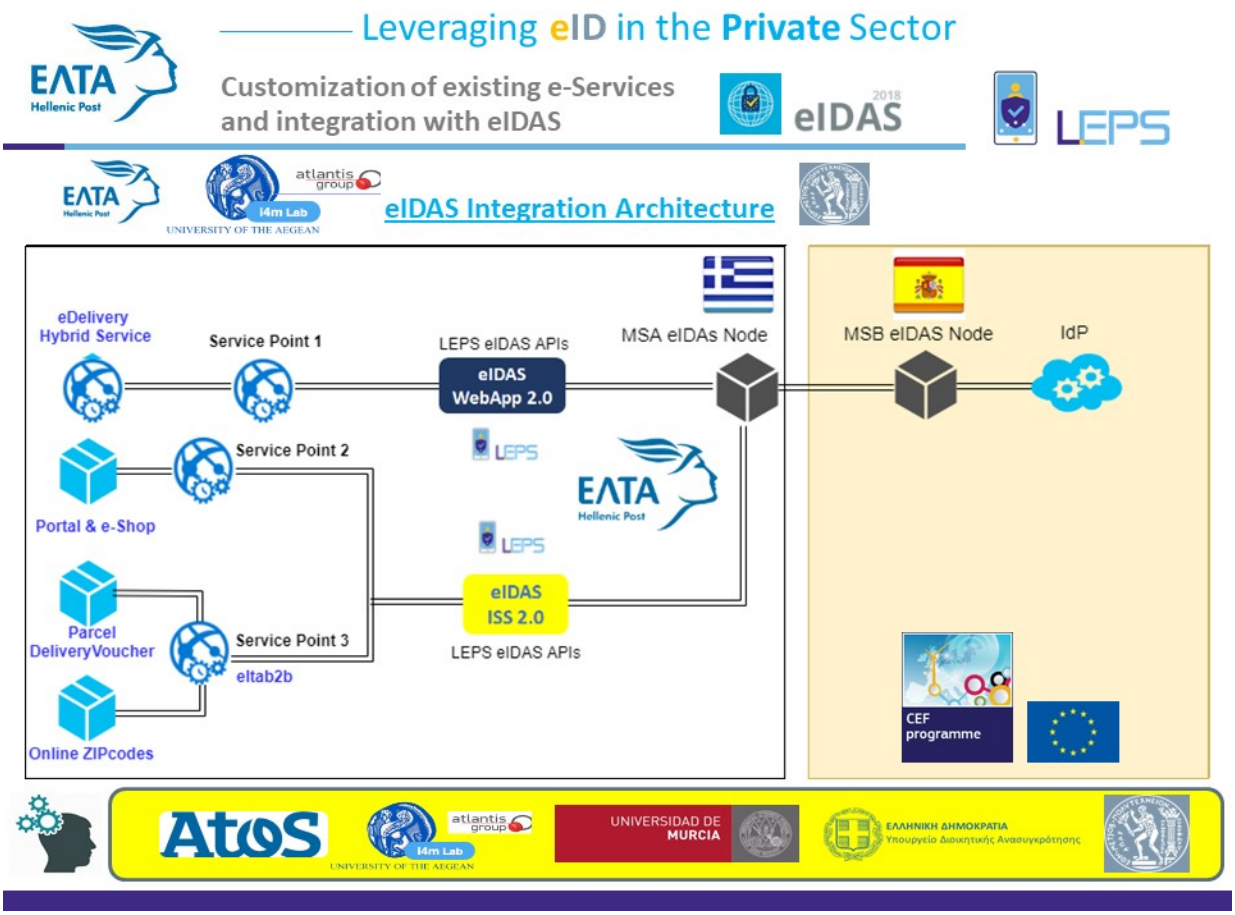

Figure 5-9: ELTA Services Architecture

The customization of the ELTA services was a little more extensive. This was due to two reasons, being the first the nature of the services being integrated:

- The ELTA e-shop/portal and the parcel Voucher were legacy systems built with outdated proprietary software frameworks that did not support the integration of new libraries like JWT.
- The ELTA b2b portal (hosting Parcel Delivery Voucher and Online Zip Codes for Business Users) service was built with a CMS system (JOOMLA) that restricted the retrieval of the JWT token

For these reasons the TWA was considerably modified to permit the integration with the services. In the case of the *ELTA Online Zip Codes for Business Users service* the required changes were considered valuable additions to the API and were merged to the API connector.

ELTA b2b services API Connector customization

The first addition made to the TWA as a result of its integration with the *ELTA Online Zip Codes API Connector* was the support for signing of the JWT token with RSA certificates. This was a requirement for increased security. Due to this customization before deploying the TWA a X.509 certificate must be generated. The certificate must be mapped to the TWA container and its public key shared to the SP service. By using the appropriate configuration parameters (as seen in the next table)

the TWA instead of signing the JWT with a symmetric signature signs it with the provided certificate and sends it to the SP service.

Finally, due to the CMS framework used the service was unable to retrieve the JWT token from a cookie (and neither could it be retrieved from an HTTP header as was initially planned). For this reason, the option of sending the JWT as a path parameter (**login**) was added to the TWA ("*URL_ENCODED*" variable in the configuration example of the following table)

```
enviroment:
    …
    - ASYNC_SIGNATURE=true
    - SP_JWT_CERT=/certificates/keystore.jks
    - STORE_PASS=keystorepass
    - KEY_PASS=selfsignedpass
    - CERT_ALIAS=selfsigned
    - URL_ENCODED=true
volumes:
   - /zipcodesCertificates:/certificates
```

For more information on the configuration of the TWA and a detailed explanation of these configuration variables please refer to the UAegean LEPS API repository[25]

5.5.2 ELTA Portal/eSAhop

As mentioned above the ELTA Portal and eShop are legacy systems built with an older technological stack. As a result, the consumption of the JWT token was not possible. For this reason, the TWA implementation was significantly altered support these services.

The redirection of the authentication flow to the TWA does not start with a simple redirection but a parametric one. The services send to the login endpoint of the TWA the following parameters:

Parameter name	Explanation
1) returnUrl	1) The service URL where the TWA will redirect the user's browser to in the end of a successful authentication process (mandatory)
2) email	2) A pseudo email account that is generated by

[25] https://github.com/uaegeani4mlab/LEPS-APIs/tree/master/eIDAS-SP-WebApp-2.0

	the SP service to identify the user that initiates the process (optional)
3) redirectUrl	3) A service url that the browser of the user will be redirected to by the returnUrl endpoint, to maintain the session of the user in case the user has begun a process at the portal/e-shop prior to eIDAS authentication
4) token	4) a nonce that is to be returned to the SP service slated and hashed appropriately to validate that the response is indeed originated from the TWA

Using these parameters, the eIDAS authentication flow is altered as follows:

1. The **Service Provider** configures and deploys a (API Connector) UI instance (TWA)
   a. The configuration requires the definition of which attributes will be requested from the eIDAS Network
2. The **Service Provider** redirects authentication requests from the application login page (Login with eID_EU) to the deployed **API Connector/UI**.
   a. Redirection contains the parameters described in the table above
   b. The User selects "Country"
3. The **API Connector/UI** transfer to the **API Connector**: <listOfRequestedAttributes> and the <selectedCountty> with a freshly generated UUID string
4. The **API Connector** takes as input what it receives and formulates as output an appropriate eIDAS SAML authentication request

User's Country

5. The SAML authentication request is next transmitted to the near (proxy) **eIDAS Node** (GR in occurrence) and, then to the eIDAS infrastructure of the Country the User has dispatched the authentication process (ES in occurrence)
6. The User is authenticated using the eIDAS flow (eIDAS Node – IdP – back to eIDAS Node); the output of the eIDAS authentication flow an eIDAS SAML authentication response
7. The eIDAS Node of the Country the User has dispatched the process (ES in occurrence) forwards the eIDAS SAML authentication response to the eIDAS Node that has initiated the authentication request (GR in occurrence).

Back to SP's Country

8. The **eIDAS Node,** which receives the authentication response (GR in occurrence), forwards it to the **API Connector**
9. The **API Connector** process and decrypts the authentication response and asks from the **API Connector/UI** to generate a JSON containing the identification attributes. Next the TWA **salts** the token received in step 2.1 using a predefined string shared between the SP and the TWA and hashes it using the ***HmacSHA256*** *algorithm*. Finally, the attributes the token and the rest

of the parameter received in step 2.1 are bundled together is a JSON and are POSTed on the SP endpoint received from the original request (*returnUrl*) with the parameter name **login**. The format of the JSON message posted is the following:

{eidasAttributes: “list of key value pairs”, returnUrl: “the SP url that the TWA redirects the user to “, token: “the salted and hashed token”, redirectURL : “the url provided in step 2.1 that the SP service will finally redirect the user to”}

10. The SP service upon receiving such a request validates the token (by calculating the salted hash of the original token and comparing them), reads the authentication values of the user from the JSON and authorizes the user according to its business logic.

5.6 Mobile Integration

Most modern Identity Providers, such as Google or PayPal offer authorization and authentication service that can be easily consumed by (native) mobile applications. However, the eIDAS specification requires the exchange of SAML messages in HTTP POST binding (as opposed to Artefact binding) format.

This restriction impacts heavily the implementation of a mobile solution for SPs and its integration as that is offered by LEPS. Specifically, the restriction from the eIDAS specification together with the fact that the Spanish eIDAS IdP offers authentication using X.509 certificates (accessed either as software certificates or Spanish DNIe 3.0 with NFC support) led to the decision to implement a native Android app that offers a simplified embedded browser to access any SP webpage, with support for authentication using either username/password, or software certificates and Spanish DNIe 3.0 through the mobile NFC interface.

Additionally, the SPs participating in LEPS have redesigned their offered services so as to be responsive, i.e. adapted them for use in mobile devices. The offered services described in this document were tested for compatibility with the LEPS Mobile ID App and were adjusted accordingly. By adopting the offered solution together with the redesigned services, any user can seamlessly use any of the provided SP services from his/her mobile device and authenticate himself/herself easily over the eIDAS network[26].

5.7 ATHEX IdP

An Identity Provider (IdP) provides user identification information as a service to remote Service Providers (SPs). Benefiting from LEPS, ATHEX developed ATHEX IdP as part of eIDAS Network, to provide identification services with higher level of assurance to eIDAS connected SPs. ATHEX IdP

[26] For more details on the implemented solution please refer to the Deliverable D3.1: “M5 & M9 – Mobile ID App and its integration results with the Industrial Partners”.

is acting as a connection and validation point for ATHEX-registered users, between the Greek eIDAS Node and the ATHEX User Registry.

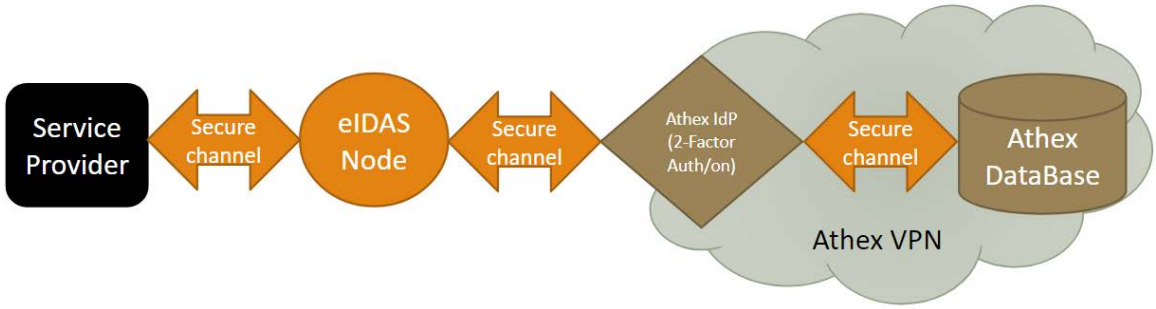

Figure 5-10: ATHEX IdP positioning in the eIDAS value chain

5.7.1 Design principles

To do so, a specific interface has been created that implements an eIDAS IdP application workflow, based on CEF software[27], augmented with a two-factor authentication validation service. The development of the ATHEX IdP interface follows a "high confidence design constraint" founded on the defintiion of three (3) specific core design principles:

1. Confidence in identifying communication through the exchange of digital certificates (the entity consuming the identification information should be confident that the information comes from the particular IdP that the SP trusts).
2. Secure communication of IdP with the user identification information management database.
3. Strong user authentication through safer identification methods.

The deployment of ATHEX IdP covers all three core design principles in the following ways:

1. A powerful identification and encryption certificate for IdP (3072 bits) was used. IdP's digital ID has been added to the list of certificates for the Greek node eIDAS that the node trusts. The corresponding process has also taken place in the list of certificates entrusted by IdP. This certificate is both used by the eIDAS Node to identify the validity of incoming IdP responses and to additionally encrypt sensitive parts of the SAML communication.
2. The communication with the ATEHX User Registry takes play within a secure VPN without external access. ATHEX IdP uses a second digital identification certificate for this communication, without which it is impossible to communicate with it.
3. User authentication is enabled by a two (2) factor authentication process, through a temporary One-Time-Password | OTP (Extended Password) additional to the user's persistent password (issued by ATHEX during the registration process). For this by OTP, the process makes use of

[27] eIDAS Node version 1.4.2 available at https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Node+version+1.4.2

Google Authenticator (Proof of Possession)[28]. Each generated OTP is coupled with that user's persistent credentials only[29].

5.7.2 Developemnt

As already mentioned, the implementation of the ATEHX IdP was based on the Demo-IdP sample code provided by CEF. Additionally, the implenmentation has used: a) a Java Cryptography Extension lib and, b) an Apache Tomcat Application Server. The provided by CEF code was modified and enriched to:

1. Allow the user to provide additional authentication information for an increased Level of Assurance (One-Time-Password) – 1st Requirement
2. Allow the IdP to validate the authentication of this information with the ATHEX User Database and retrieve the necessary attributes information – 2nd Requirement.

To satisfy the first requirement, the web interface of the IdP was modified in order to allow the user to provide his/her username, password, as well as the current, valid One-Time-Password. An illustration of the new Athex IdP interface is presented below:

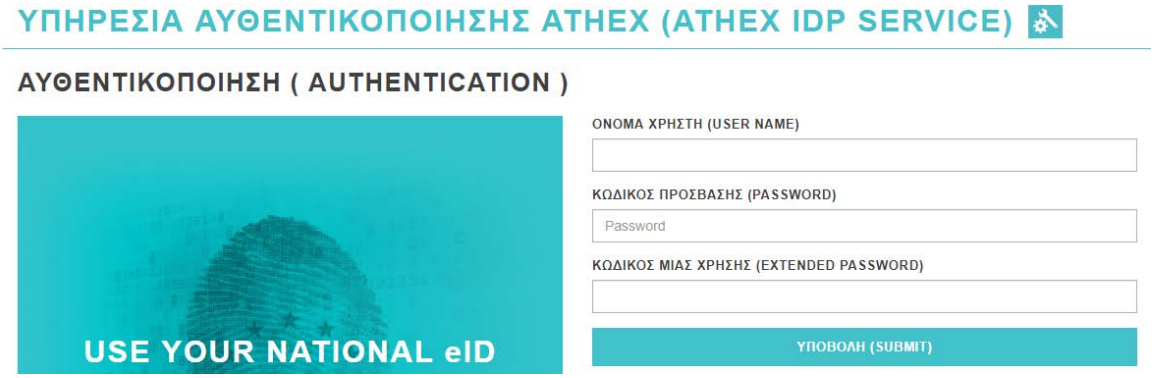

Figure 5-11: ATHEX IdP User Interface

The second requirement is accomplished by using a REST service endpoint provided by the ATHEX User Database. A back-channel communication was implemented, in a secure fashion, between the IdP and the User Database. A POST REST request is sent through the channel containing the user-provided credentials. A response is received with the result of the request. In detail:

The POST REST request of the Database endpoint requires the following parameters to be provided:

Object	Description	Type	Behaviour

[28] See. https://github.com/google/google-authenticator

[29] In addition, the communication of the browser of the user with the IdP is only via TLS (https).

Username	Username of end User at DocuSign appliance	String	Obligatory
Password	User's current password at DocuSign appliance	String	Obligatory
ExtendedPassword	One Time Password generated number from end user's device	String	Obligatory
BufferToSign	A temporary/random string converted to Base64 (not used by the IdP)	String	Obligatory

An example of a POST REST Request is as follows:

```
{
  "Username":                                   "JDOE",
  "Password":                                   "Ab1cde2f34",
  "ExtendedPassword":                           "123456",
  "BufferToSign":                               "ABCDE"
}
```

The User Database endpoint may reply to the request in two ways.

1. The credentials provided (username, password, OTP) were checked and NOT validated (ie: there was a mismatch of the username to either the password or the OTP). In this case, an error message is provided to the IdP as a reply. An example of such an error message is presented below:

```
{
 "Success":                                    false,
 "ErrorMessage": "(0X90020133) Invalid user name or password., at ValidateCredentials",
 …
}
```

   In such a case, the appropriate eIDAS error message is contructed and returned to the requesting eIDAS Proxy Service.
2. The credentials provided are validated successfully. The ATHEX User Database endpoint replies with a success message containing the attribute values (personal indormation) of the specific user. Such an example is presented below:

```
{
 "Success": true,
 "ErrorMessage": "",
 "AccountName": "John Doe",
 "Email": "an.email@example.com",
```

```
  "GivenName": "John",
  "Surname": "Doe",
  "ParentName": "Alex",
  "BirthDate": "1973-01-29T00:00:00",
  "Country": "GR",
  "UserIdentifier": "MJ0091",
  "SerialNo": "AXTST12344",
  "SignatureAlgorithm": "sha256RSA",
  "Subject": " T=John Doe, OID.2.5.4.45= #030C005350444556454C4F504552 , CN=John
Doe ",
  "Version": 3,
  "Issuer": "CN=ATHEX General Certificates CA TEST, O=ATHEX, C=GR",
  "NotBefore": "2016-10-20T13:09:09+03:00",
  "NotAfter": "2018-10-20T13:09:09+03:00",
  "Thumbprint": "C880FFCD51456650F826DB48F85748A234330725",
  "SerialNumber": "27B8",
  "FriendlyName": "",
  "PublicKey": "MIIB...AQAB",
  "PublicKeyFormated": "30 82...00 01",
  "BufferSignature": "MIIGEgY...QQ=="
}
```


The relevant to the eIDAS Request information is extracted from the successful reply and used in order to construct the eIDAS SAML Authentication Response which will be provided to the requesting eIDAS Proxy Service.

ATHEX IdP as part of the eIDAS Node, provides the four core eIDAS Personal Attributes. The following table presents the matching between the ATHEX User Database provided attributes (also highlighted in the example) and the core eIDAS Personal Attributes:

ATHEX Attribute	eIDAS Attribute
GivenName	http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName
Surname	http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName
BirthDate	http://eidas.europa.eu/attributes/naturalperson/DateOfBirth
UserIdentifier	http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier

5.7.3 Operational Flow

1. End User requests access via eIDAS Node (through browser redirection)
2. IdP validates the SAML Authentication Request as per CEF eIDAS specifications
3. End User provides credentials in webapp form: Username, password, extendedPassword (generated OTP)

4. eIDAS IdP gathers the credentials and performs a POST REST request towards the 2FA Validation Service endpoint
5. eIDAS IdP gathers the response from the 2FA Validation Service and decides whether the user is valid or invalid
6. The appropriate SAML Authentication Response is created
7. The user is redirected back to the requesting Proxy Service along with the SAML Authentication Response.

5.7.4 Deployment

The IdP was deployed on the Athex premises, secured by the Athex VPN infrastructure. As per Greek eIDAS infrastructure (and CEF) specifications, the IdP was provided with two 3072-bit digital certificates, one for Encryption and Assertion Signing and one for Metadata Signing and Identification. The configuration files of the IdP were also modified in order to specify the deployment details:

Idp.properties
idp.metadata.url=http://t-leps-idp.inet.helex.gr:8080/IdP/metadata idp.ssos.redirect.location=http://t-leps-idp.inet.helex.gr:8080/IdP/AuthenticateCitizen idp.ssos.post.location=http://t-leps-idp.inet.helex.gr:8080/IdP/AuthenticateCitizen

EncryptModule_IdP.xml/SignModule_IdP.xml
<entry key="response.sign.assertions">false</entry> <entry key="keyStorePath">../../keystore/AthexIdP.jks</entry> <entry key="keyStorePassword">...</entry> <entry key="keyPassword">...</entry> <entry key="issuer">CN=ATHEXIDP, OU=IDPAUTH, O=ATHEX, L=ATHENS, ST=ATTICA, C=GR</entry> <entry key="serialNumber">ce50ad9442ef4999</entry> <entry key="keyStoreType">JKS</entry> <entry key="metadata.keyStorePath">../../keystore/AthexIdP_METADATA.jks</entry> <entry key="metadata.keyStorePassword">...</entry> <entry key="metadata.keyPassword">...</entry> <entry key="metadata.issuer">CN=ATHEXIDPMETADATA, OU=IDPAUTH, O=ATHEX, L=ATHENS, ST=ATTICA, C=GR</entry> <entry key="metadata.serialNumber">ca3dc9e80b4b3fd4</entry> <entry key="metadata.keyStoreType">JKS</entry>

6 Greece eIDAS Node integration

This section presents the test use cases performed to demonstrate the effective integration of the SP e-services to the Greek eIDAS Node. A more extended testing procedure will take place in the last months of the project.

6.1 ATHEX

The test cases for ATHEX Group services (ATHEX, ATHEX AXIAweb and ATHEX Identity Service Provider) are presented below.

6.1.1 ATHEX Sign (Registration)

ATHEX Sign	
Start Testing Event	https://athex-sign.athexgroup.gr
End Testing Event	User registers and then accesses the ATHEX Sign Service

ATHEX Sign	
Test Case	User Registration Flow | A non-registered user registers to the ATHEX Sign Service

6.1.1.1 Test Case | Title: User Registration Flow (ATHEX Sign – Greek User)

Test with a Greek User

Description	A non-registered user with a Greek eIDAS eID wants to register with the service
Preconditions	The user is not registered to the service

Process	1. The User accesses the service via visiting: https://athex-sign.athexgroup.gr 2. User selects apply via eIDAS 3. User authenticates via eIDAS 4. User fills in non eIDAS provided registration details (email, fathers name) 5. System responds with an appropriate message 6. User receives mail with Qualified Digital Certificate Offer from ATHEX Digital Signature Services and payment information. 7. User proceeds with the payment for the service 8. User sends an email to the service with the payment receipt 9.User receives information on how to proceed the enrolment with the device 10. User enrols to the service 11. User accesses the service
Result	The User accesses the service

Step 1: Type URL: https://athex-sign.athexgroup.gr and click apply via eIDAS Sign Up.

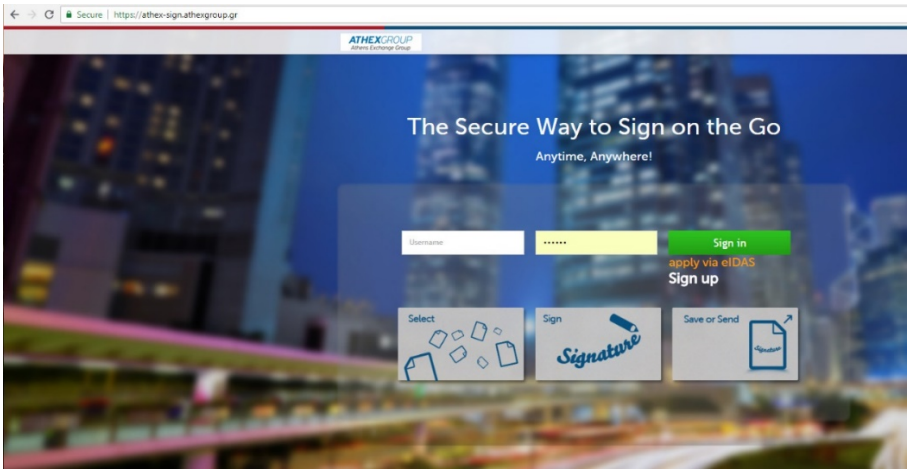

Figure 6-1. ATHEX Sign home page

Step 2: User accesses Greek Service Provider (ATHEX Sign) and selects "GREECE" as his/ her Country of Origin and clicks "NEXT" button.

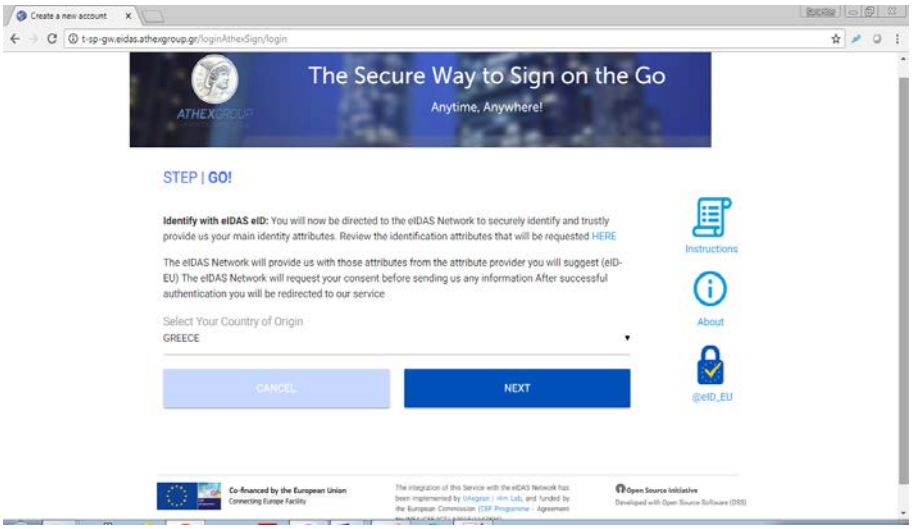

Figure 6-2. Country Selection page

Step 3: User is redirected to ATHEX IdP and is asked to provide credentials (user name, password, One Time Password) in order to authenticate.

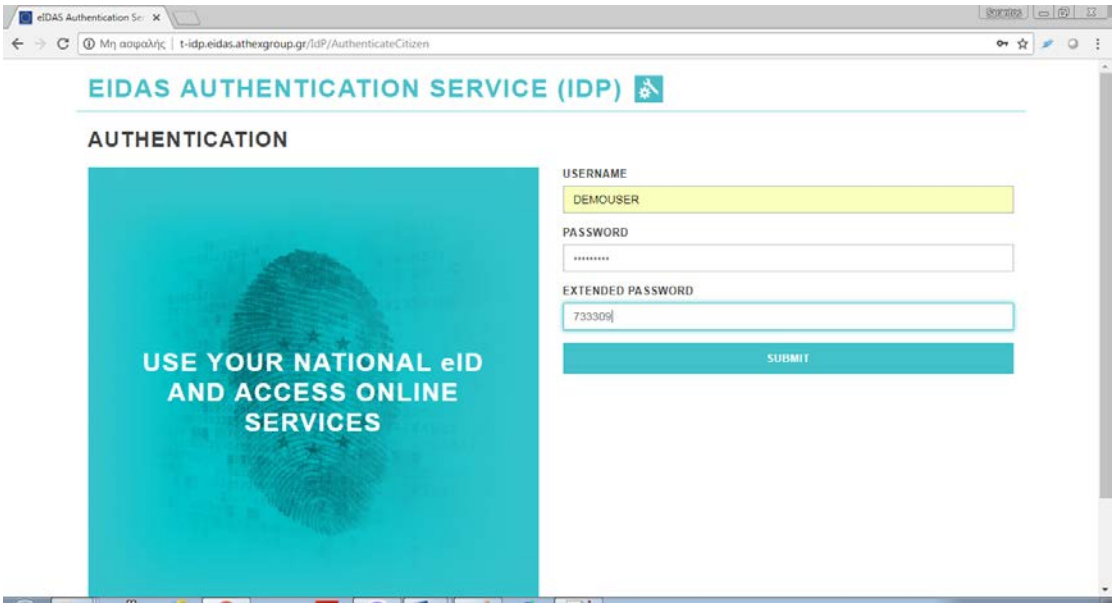

Figure 6-3. ATHEX Idp Authentication page

Step 4: User is redirected to Greek eIDAS Node and is informed about the attributes requested (Basic Information) from Greek Service Provider (ATHEX Sign). User clicks “SUBMIT” button.

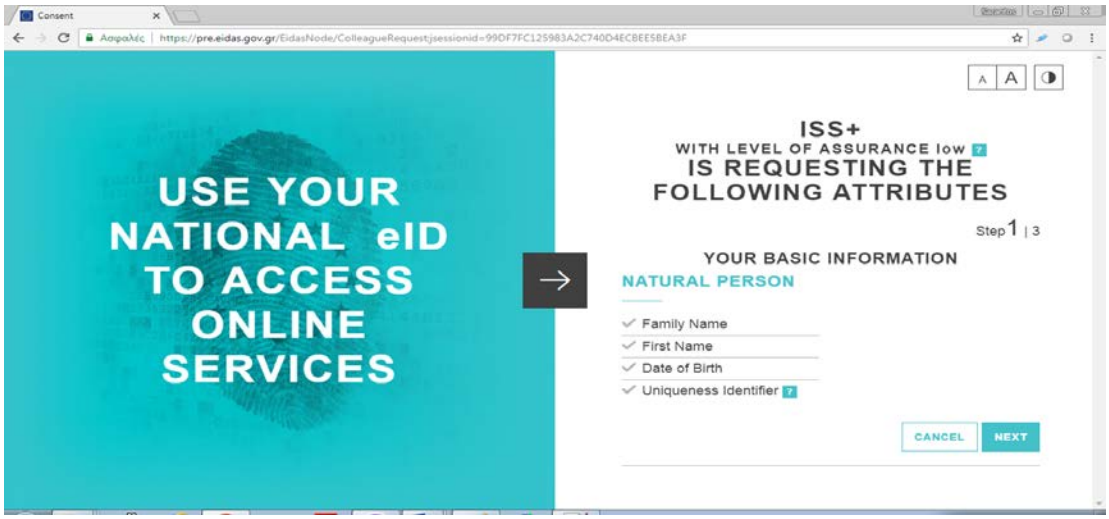

Figure 6-4. Attributes Pre Consent page

Step 5: User is also informed about the attributes requested (Additional Information) from Greek Service Provider (ATHEX Sign) and clicks «NEXT» button.

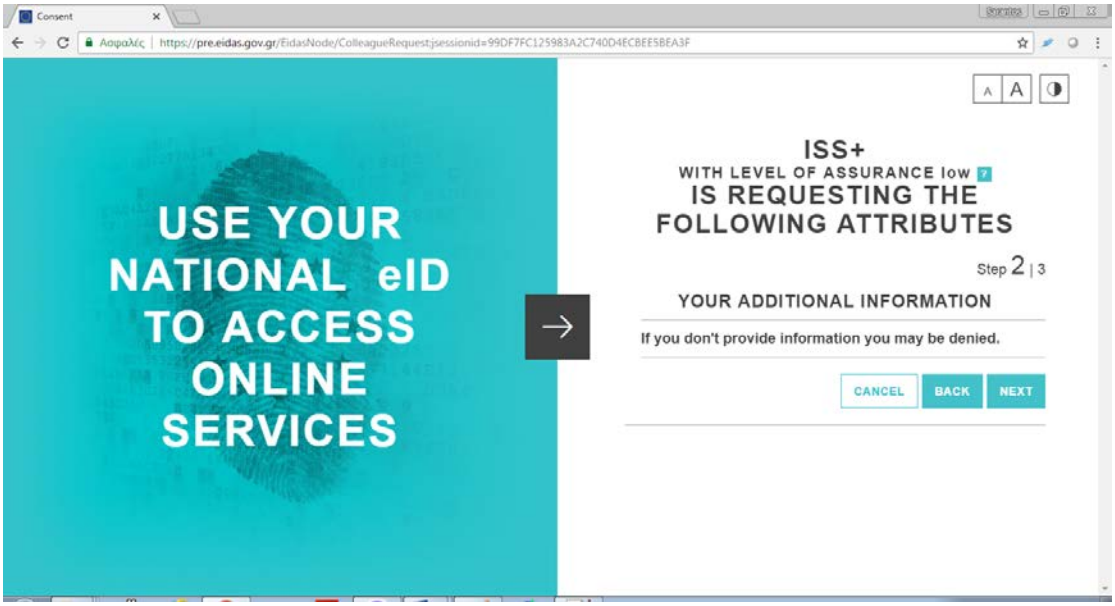

Figure 6-5. Optional Attributes Pre Consent page

Step 6: User is forwarded to Greek Service Provider and some mandatory personal Information provided by Greek eIDAS Node are automatically filled in ATHEX Sign Registration Form and is required to fill in “Father Name” and “Email” and clicks “SUBMIT” button.

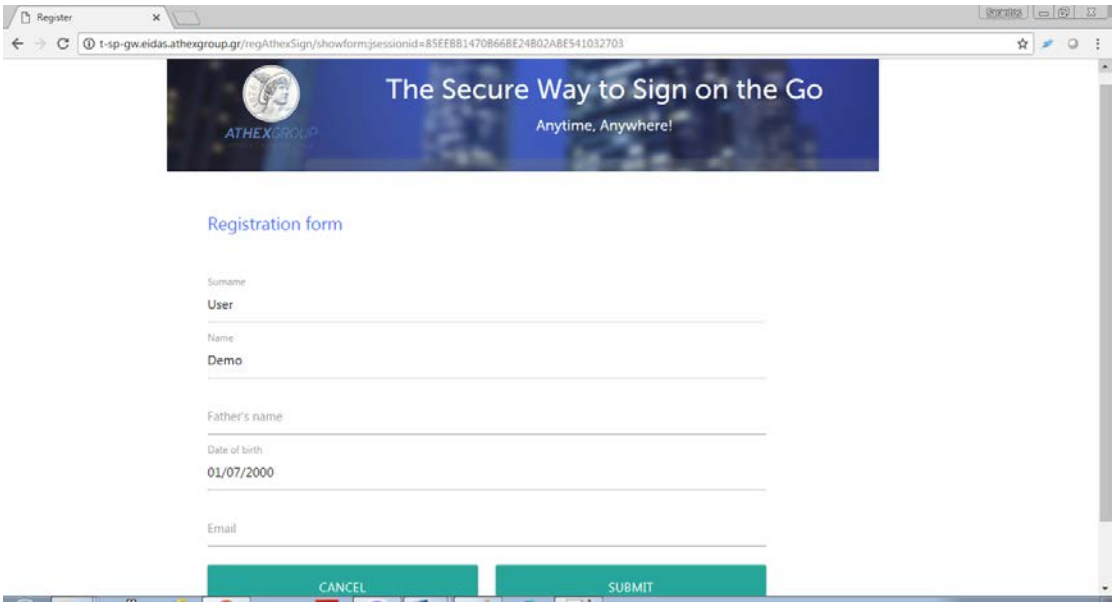

Figure 6-6. ATHEX Sign Registration form

The registration has been completed succesfully

Figure 6-7. Successful registration message

After initial registration procedure is completed, user receives mail with Qualified Digital Certificate Offer from ATHEX Digital Signature Services and payment information.

Attached Smart-Sign v1_0 - Subscriber Application Agreement.pdf 410 KB

We thank you very much for the interest you showed in the products and the services of our company.
After our communication and your inquiry, we are happy to submit to you our offer for the provision of the qualified digital certificates (remote e-signatures)

Specifically for the needs you mentioned regarding the qualified Digital certificates our financial offer is as follows:

A/A	Product description	Price per piece
1	Qualified digital certificates for one Year (1)	90 € **(VAT Included)**

For the issuing of the certificate we need you to fill in the attached subscribers contract application and return it to us together with the receipt payment and send to us the email address PKICA-Services@athexgroup.gr .

The time of issuance after the receipt of the application is (1) one business day.

We remain at your disposal for any additional inquiry concerning this matter.

We would also want to advise you along with the application you should send a copy of the bank transcript of the deposit to the amount for the certificate.

The deposit can be made in one of the following accounts and banks.

BANK	IBAN	BIC
ALPHA BANK	GR56 0140 1010 0200 2012380	CRBAGRAAXXX
NATIONAL BANK OF GREECE	GR18 0110 0400 0000 0404 7254 505	ETHNGRAA
EUROBANK	GR98 0260 1040 0009 5020 0125 765	ERBKGRAA
PIREAUS BANK	GR66 0172 0320 0050 3201 7505570	PIRBGRAA

Figure 6-8. Email with Qualified Digital Certificate Offer and payment information

Once the payment is completed, the user sends an email with a copy of the receipt of the payment and the completed Subscriber Application Agreement.

In order to receive the One Time Password (OTP) the user receives the information in his e-mail how to proceed the enrollment with the device. More specifically :

In order to activate the OTP Click https://athex-sign.athexgroup.gr/selfservice/enrollotp.aspx .

1. Fills User Name (xxxxxxxx), Activation Password (xxxxxxx) and click Submit.

Figure 6-9. One time password credentials

2. Open Google Authenticator application in mobile device. Fill in User Name (xxxxxxxx), Activation Password (xxxxxxx) scan the QR Code and click next.

Figure 6-10. One time password QR code

4. Fill in User Name, Activation Code, New Code, Verification Code, fill in the OTP number generated by your mobile Authenticator app and click submit.

Figure 6-11. Account Activation

5. Your Account has been activated.
6. Click https://athex-sign.athexgroup.gr/ to Upload and digitally sign a document.

6.1.1.2 Test Case | Title: User Registration Flow (ATHEX Sign – Spanish User)

Test with a Spanish User

Description	A non-registered user with a Spanish eIDAS eID tries to register to the service
Preconditions	The user is not registered to the service

Process	1. The User accesses the service via visiting: https://athex-sign.athexgroup.gr 2. User selects apply via eIDAS 3. User authenticates via eIDAS 4. User fills in non eIDAS provided registration details (email, fathers name) 5. System responds with an appropriate message 6. User receives mail with Qualified Digital Certificate Offer from ATHEX Digital Signature Services and payment information. 7. User proceeds with the payment for the service 8. User sends an email to the service with the payment receipt 9.User receives information on how to proceed the enrolment with the device 10. User enrols to the service 11. User access the service
Result	The User accesses the service

Step 1 and Step 2 are the same as the previous Test case.

Step3: User selects “SPAIN” as his/ her Country of Origin and clicks “NEXT” button.

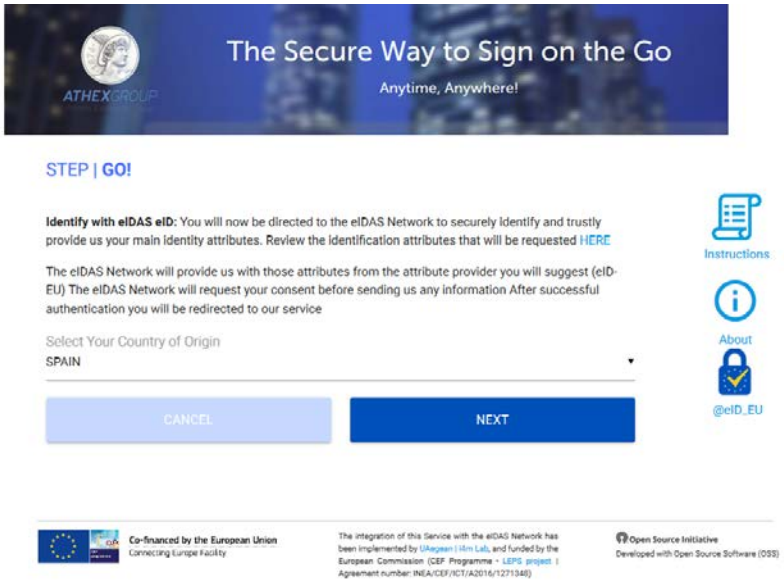

Figure 6-12. Country selection page

Step 4: User is redirected to Spanish IdP and is asked to confirm the use of the DNIe as credentials. The user clicks on “Confirmar” button.

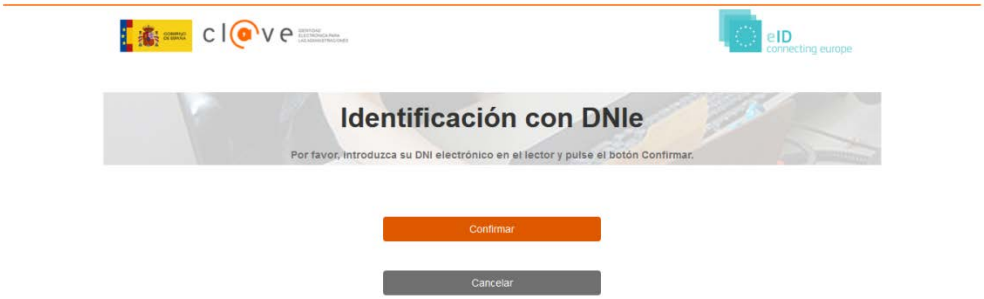

Figure 6-13. Spanish Idp page

Step 5: The browser (requested by the Spanish IdP) displays a pop-up asking the user to select the certificate to use as credential. The user selects the certificate and clicks on “Aceptar” button.

Once the user is authenticated, the citizen is redirected to the Spanish eIDAS Node, which redirects to the Greek eIDAS Node.

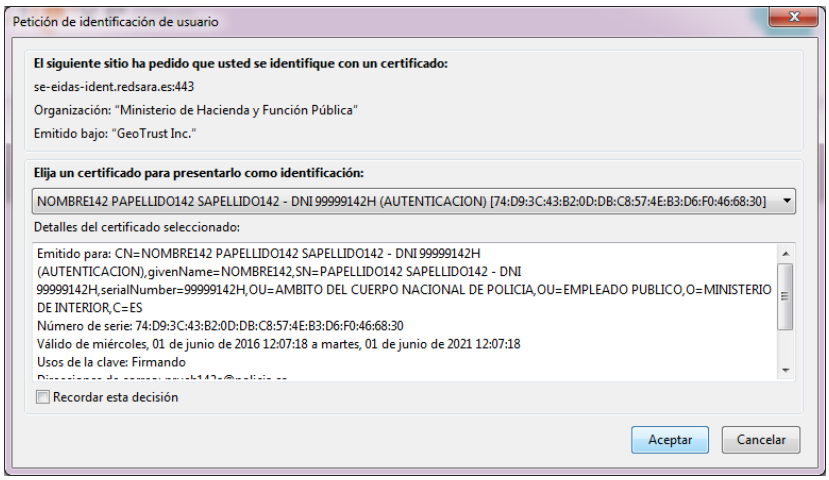

Figure 6-14. Certificate selection page

Step 6: Finally, the user is forwarded to Greek Service Provider and some mandatory personal Information provided by Spanish eIDAS Node are automatically filled in ATHEX Sign Registration Form and is required to fill in “Father Name” and “email” and clicks “SUBMIT” button.

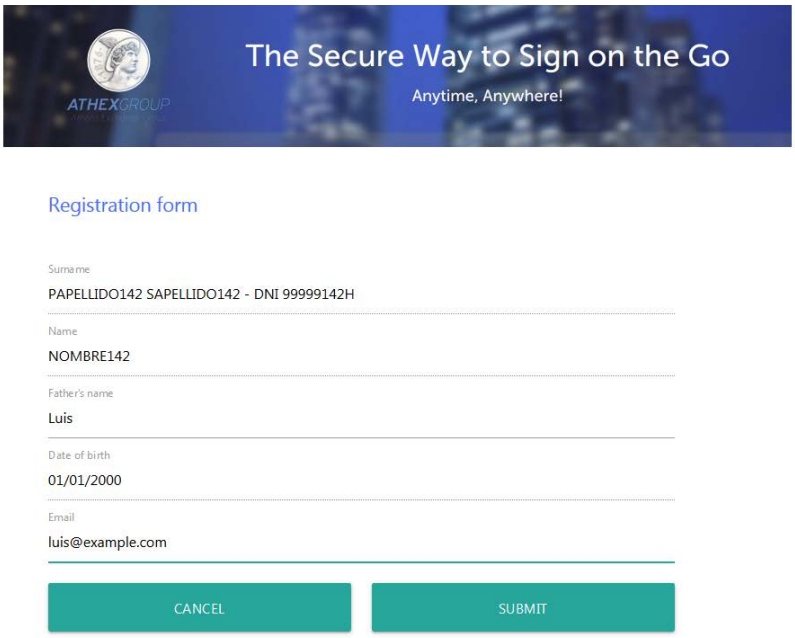

Figure 6-15. ATHEX Sign registration form

Step 7: The registration has been completed succesfully.

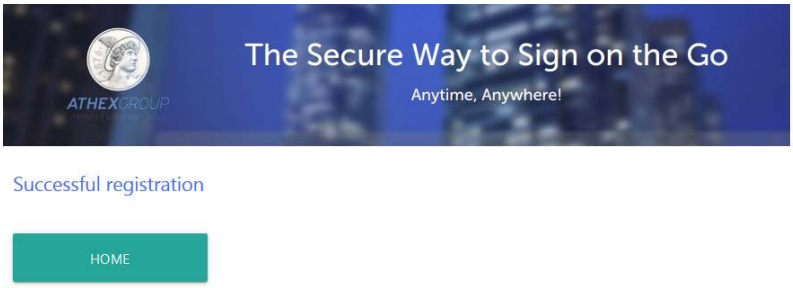

Figure 6-16. Successful registration message

6.1.2 ATHEX AXIAweb

ATHEX AXIA Web	
Start Testing Event	https://www.axiaweb.gr/AXIAWeb/gr/login.htm
End Testing Event	User registers and then accesses the ATHEX Sign Service

ATHEX AXIA Web	
Test Case	User Registration Flow | A non-registered user tries to register to the ATHEX Sign Service
Test Case	Registered not logged-in User Accessing Service Flow | A registered but not logged-in user tries to access the AXIA Web service
Test Case	Registered logged-in User Accessing Service Flow | A registered and logged-in user tries to access the AXIA Web service

6.1.2.1 Test Case | User Registration Flow (ATHEX Axia Web – Greek User)

Test with a Greek User

Description	A non-registered user with a Greek eIDAS eID tries to register to the service
Preconditions	Existing portfolio with ATHEX
Process	1. The User accesses the service via visiting: https://www.axiaweb.gr/AXIAWeb/gr/login.htm 2. The User selects eIDAS Login 3. The User authenticates via eIDAS 4.The User receives an email containing information on how finalize the registration
Result	The User receives an email containing further instructions, to finalize the registration process

Step 1: Type URL: https://www.axiaweb.gr/AXIAWeb/gr/login.htm and click eIDAS Login.

Figure 6-17. AXIA Web home page

Step 2: User accesses Greek Service Provider (Axia Web) and selects “GREECE” as his/ her Country of Origin and clicks “NEXT” button.

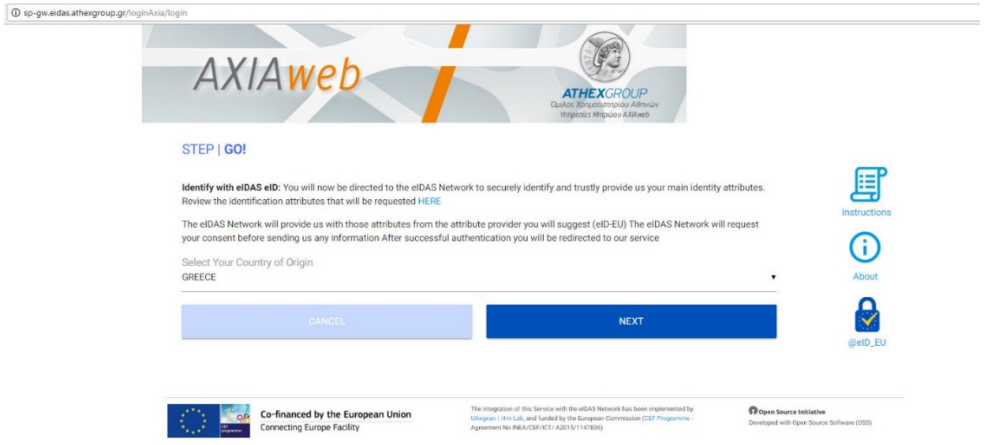

Figure 6-18. Country selection page

Step 3: User is redirected to ATHEX IdP and is asked to provide credentials (user name, password, One Time Password) in order to authenticate.

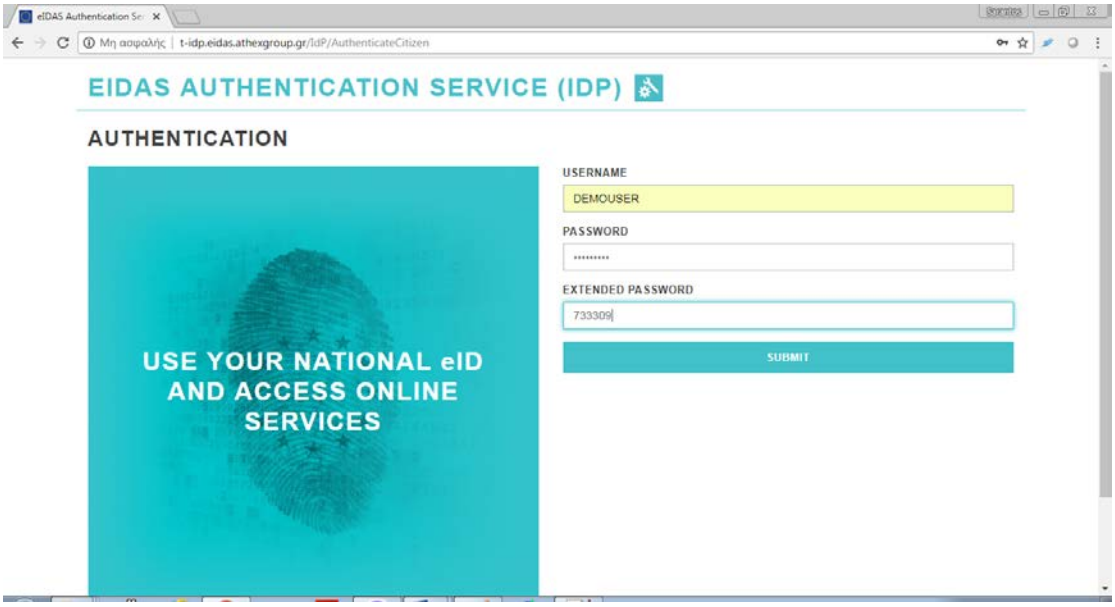

Figure 6-19. ATHEX Idp page

Step 4: User is redirected to Greek eIDAS Node and is informed about the attributes requested (Basic Information) from Greek Service Provider (Axia Web). User clicks “SUBMIT” button.

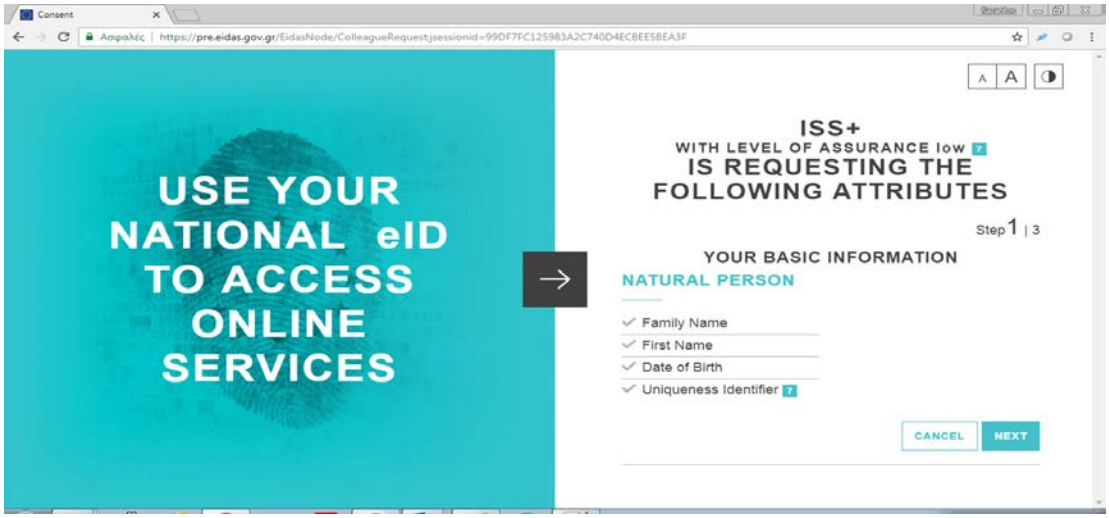

Figure 6-20. Attributes Pre Consent form

Step 5: User is also informed about the attributes requested (Additional Information) from Greek Service Provider (Axia Web) and clicks «NEXT» button.

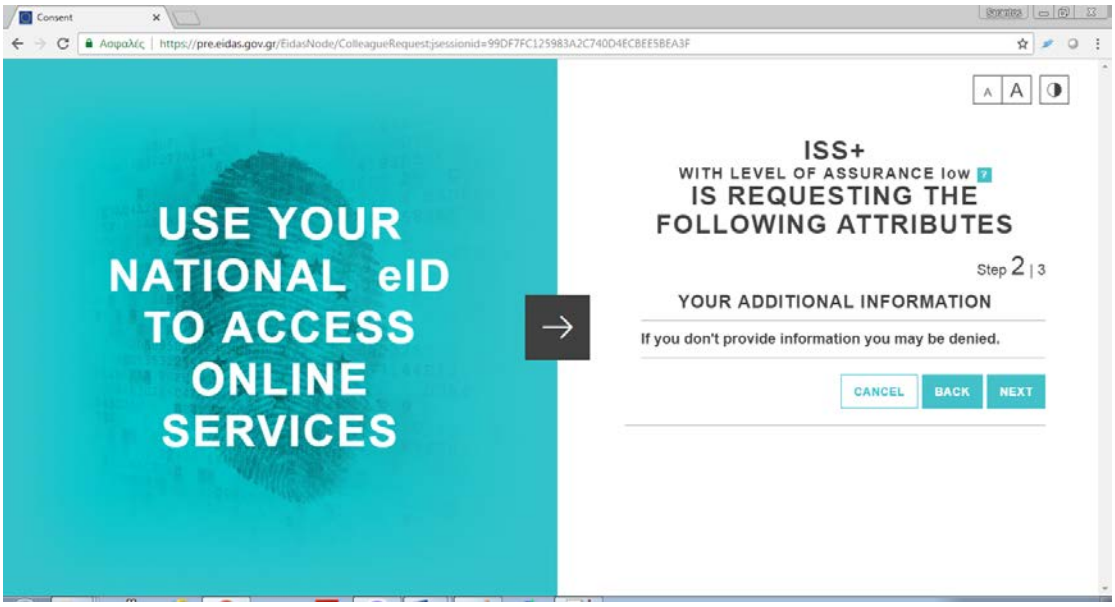

Figure 6-21. Optional Attributes Pre Consent form

Click Submit the registration successful.

Figure 6-22. Successful registration message

The User Registration Flow with a Spanish User is similar to the test case described in 6.1.2.1.

6.1.3 ATHEX Identity Service Provider (ATHEX IdP)

Service Start and End Events

ATHEX Identity Provider Service (ATHEX IDP)	
Start Testing Event	https://athex-sign.athexgroup.gr/.
End Testing Event	User is successfully authenticated from ATHEX Identity Provider and he/she is ready to consume a service provided by Greek Service Provider (ATHEX – Sign)

Test Cases

ATHEX Identity Provider Service (ATHEX IDP)	
Test Case	User Authentication Flow | A non-authenticated user asks to authenticate in order to consume a service provided by Greek Service Provider (ATHEX Sign)
Test Case	User Authentication Flow | A non-authenticated user asks to authenticate in order to consume a service provided by Spanish Service Provider.

6.1.3.1 Test Case | User Authentication Flow (ATHEX IdP - Greek Service Provider)

Description	A non-registered user tries to consume a service provided by Greek Service Provider (ATHEX Sign) and he/she is asked to authenticate him/herself. The user uses ATHEX IdP service in order to authenticate him/herself.
Preconditions	The user is not authenticated but has an account in ATHEX IdP service.
Process	1. The user accesses Greek Service Provider (ATHEX Sign) through the following url: https://athex-sign.athexgroup.gr/. User selects "Sign up" in order to register through eIDAS. 2. User selects his /her country of origin and also gets informed about the attributes requested by ATHEX Sign Service Provider. 2.1 User selects "GREECE" as his/ her Country of Origin and clicks "NEXT" button.

	2.2 User is redirected to Greek eIDAS Node and he/she is informed about the attributes requested (Basic Information) from Greek Service Provider (ATHEX Sign). User clicks «NEXT» button. 2.3. User is also informed about the attributes requested (Additional Information) from Greek Service Provider (ATHEX Sign). User clicks «NEXT» button. 3. User is redirected to ATHEX IdP and he/she is asked to provide his/her credentials. (user name, password, One Time Password) in order to authenticate him/herself. 3.1 User fills in his/her username and password. 3.2 User retrieves the One time Password (OTP) from his/her smartphone, by opening Google Authenticator Application which is already installed in his/her smartphone and fills in the "Extended Password" field. 3.3 User clicks "Submit" button. 4. Upon successful authentication, user is asked to give his/her consent in order his/her personal information to be forwarded to Greek Service Provider (ATHEX Sign). User clicks "SUBMIT" button. 5. User is forwarded back to Greek Service Provider and his/her personal Information provided by Greek eIDAS Node are automatically filled in ATHEX Sign Registration Form.
Result	The user is authenticated from ATHEX IdP and can access the service provided from Greek Service Provide (ATHEX Sign).

Step 1: The user accesses Greek Service Provider (ATHEX Sign) through the following url: https://athex-sign.athexgroup.gr/. User selects "Sign up" in order to register through eIDAS.

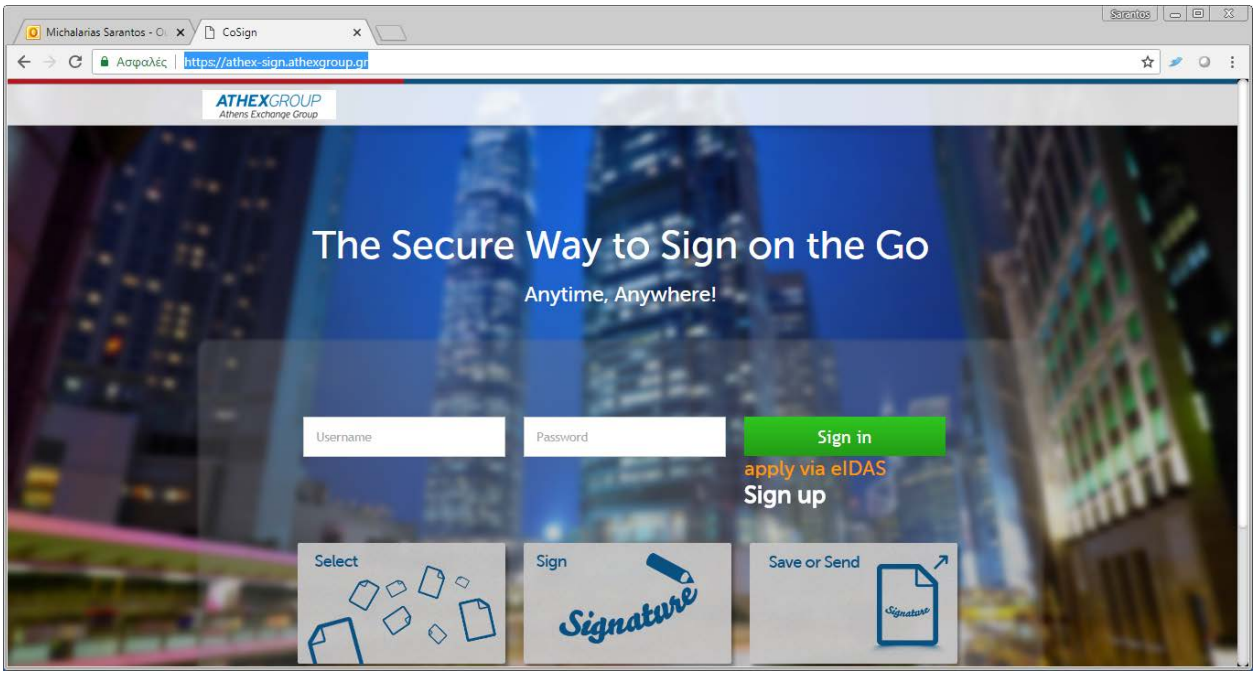

Figure 6-23. ATHEX Sign home page.

Step 2: User selects his /her country of origin and also gets informed about the attributes requested by ATHEX Sign Service Provider

2.1 User selects “GREECE” as his/ her Country of Origin and clicks “NEXT” button

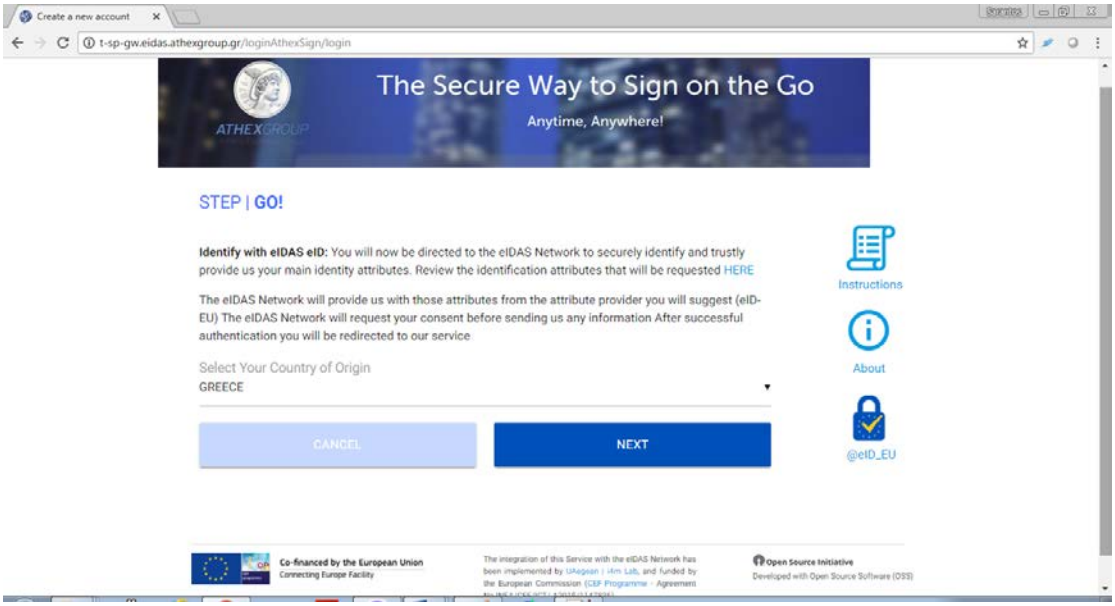

Figure 6-24. Country Selection page

2.2 User is redirected to Greek eIDAS Node and he/she is informed about the attributes requested (Basic Information) from Greek Service Provider (ATHEX Sign). User clicks “NEXT” button.

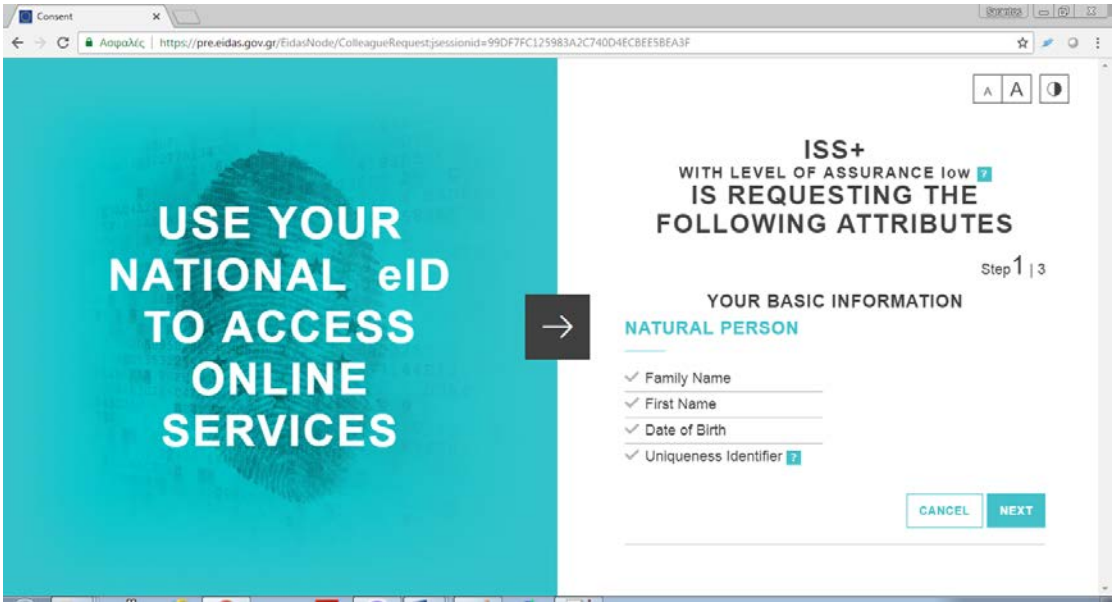

Figure 6-25. Attributes Pre Consent Form

2.3 User is also informed about the attributes requested (Additional Information) from Greek Service Provider (ATHEX Sign) and clicks «NEXT» button.

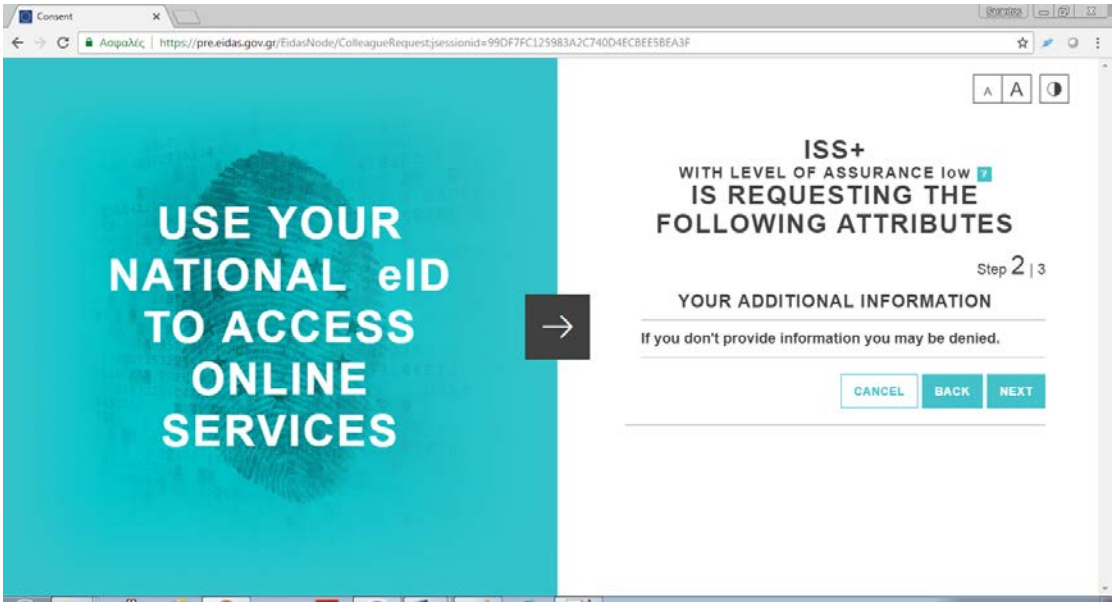

Figure 6-26. Optional Attributes Pre Consent Form

Step 3: User is redirected to ATHEX IdP and he/she is asked to provide his/her credentials. (User name, password, One Time Password) in order to authenticate him/herself.

3.1 User fills in his/her username and password

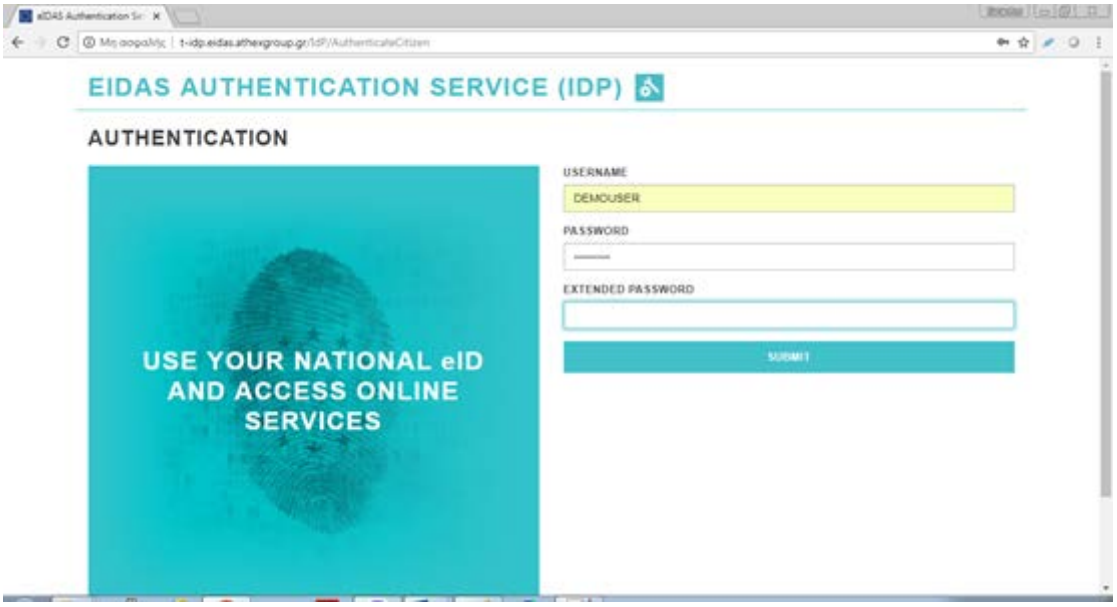

Figure 6-27. ATHEX IdP Page

3.2 User retrieves the One Time Password (OTP) from his/her smartphone, by opening Google Authenticator Application which is already installed in his/her smartphone and fills in the "Extended Password" field.

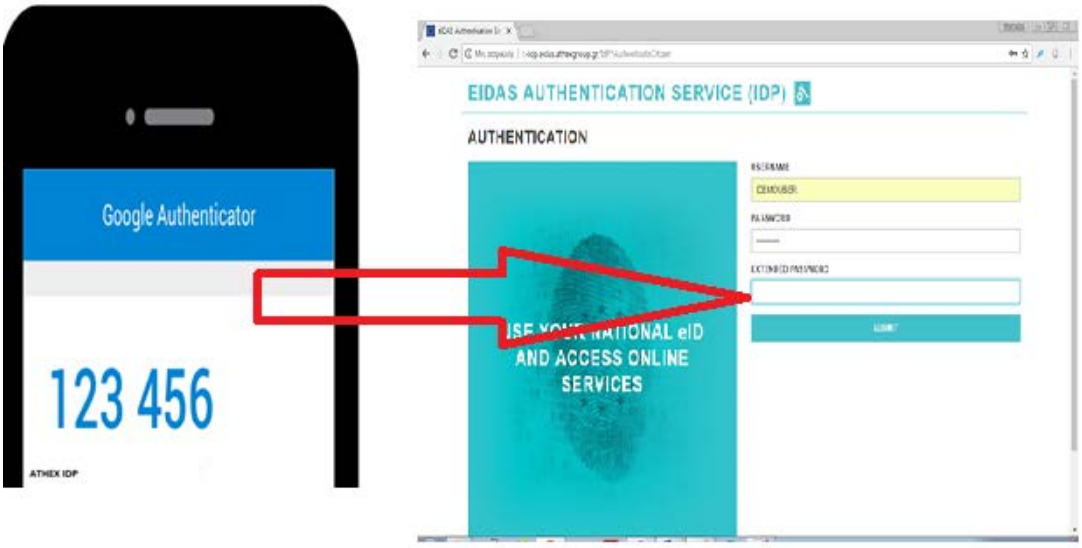

Figure 6-28. User receives OTP from Google Authenticator

3.3 User clicks "Submit" button.

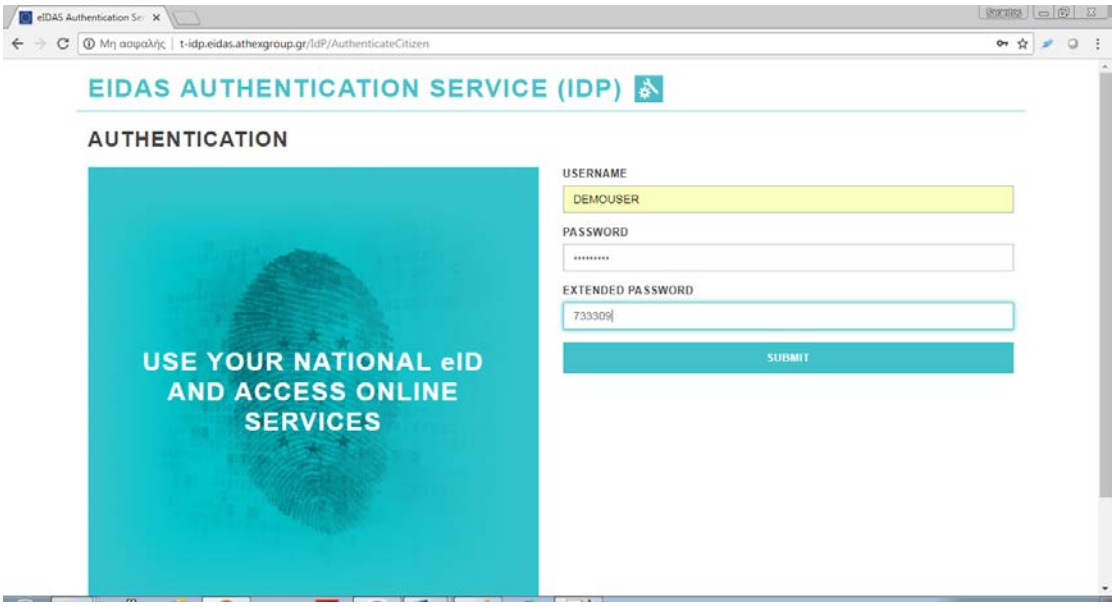

Figure 6-29. User fills in OTP in ATHEX IdP Page

Step 4: Upon successful authentication, user is asked to give his/her consent in order his/her personal information to be forwarded to Greek Service Provider (ATHEX Sign). User clicks "SUBMIT" button

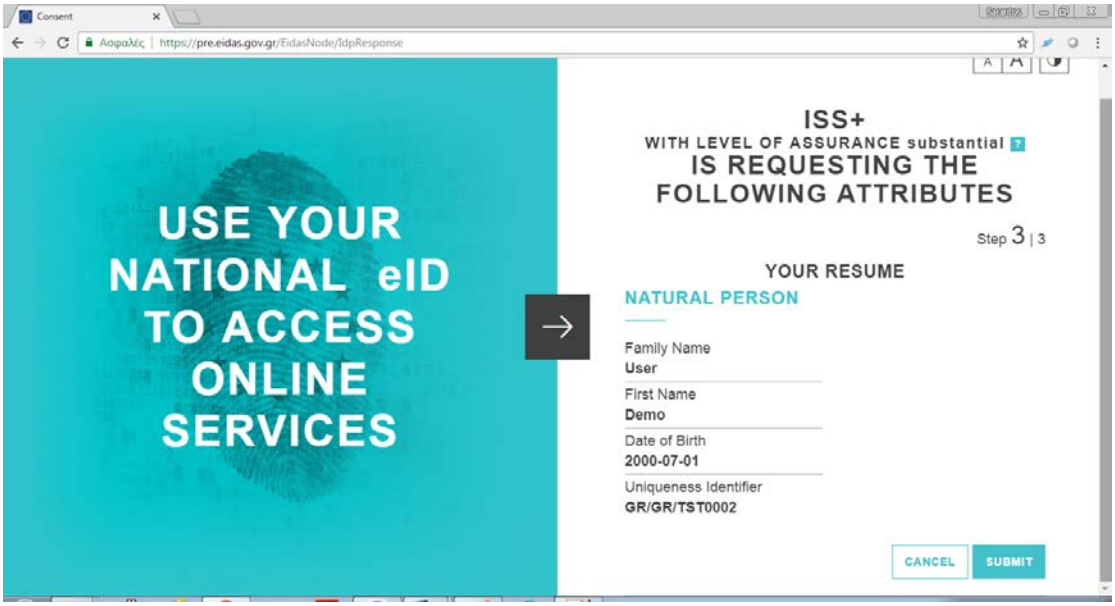

Figure 6-30. Attributes Consent Page

Step 5: User is forwarded back to Greek Service Provider and his/her personal Information provided by Greek eIDAS Node are automatically filled in ATHEX Sign Registration Form.

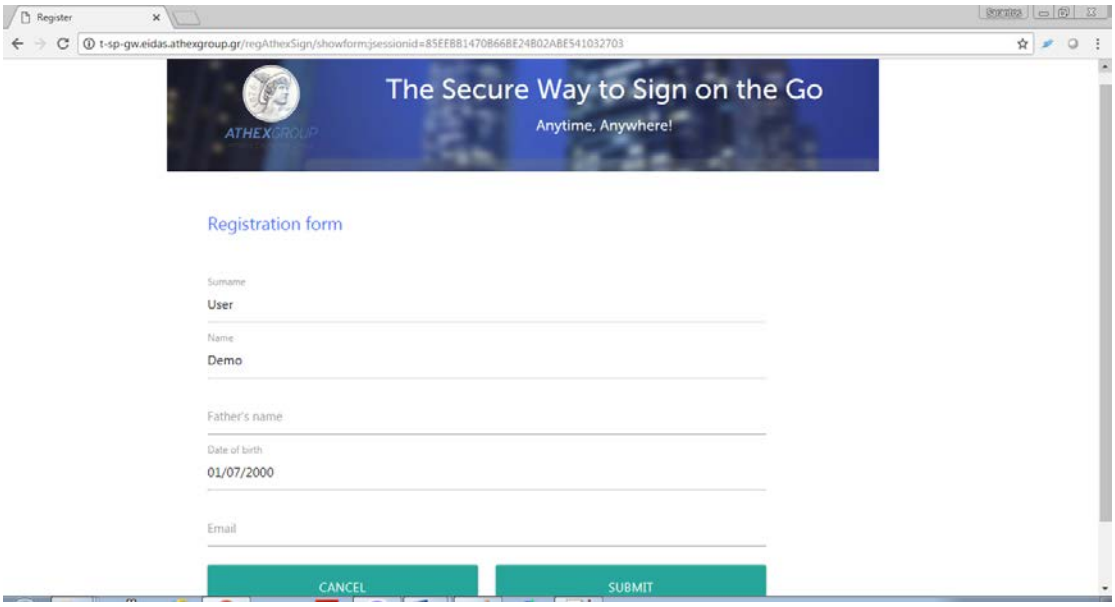

Figure 6-31. ATHEX Sign Registration Form with prefilled eIDAS attributes

6.1.3.2 Test Case | User Authentication Flow (ATHEX IdP - Spanish Service Provider/eIDAS demo SP)

Description	A non-registered user tries to consume a service provided by Spanish Service Provider and he/she is asked to authenticate him/herself. The user uses ATHEX IdP service in order to authenticate him/herself.
Preconditions	The user is not authenticated but has an account in ATHEX IdP service.
Process	1. The user accesses Spanish Service Provider through the following url: https://se-eidas.redsara.es/SP/populateIndexPage 2. User selects his /her country of origin and also gets informed about the attributes requested by Spanish Demo Service Provider. 2.1 User selects “ES” in “SP COUNTRY” drop-down list, “GR” in “CITIZEN COUNTRY” drop-down list and press “SUBMIT” button. 2.2 User press “SUBMIT” button in order to send the SAML request to Spanish eIDAS Node. 2.3 User is asked from Spanish eIDAS Node to choose the country from where his /her eID is issued. User selects “Greece” from the drop –down list and clicks “Login” button. 2.4 User is redirected to Greek eIDAS Node and he/she is informed about the attributes requested (Basic Information) from Spanish

	Service Provider. User clicks «NEXT» button. 2.5 User is also informed about the attributes requested (Additional Information) from Spanish Service Provider. User clicks «NEXT» button. 3. User is redirected to ATHEX IdP and he/she is asked to provide his/her credentials. (username, password, One Time Password) in order to authenticate him/herself. 3.1 User fills in his/her username and password. 3.2 User retrieves the One time Password (OTP) from his/her smartphone, by opening Google Authenticator Application which is already installed in his/her smartphone and fills in the "Extended Password" field. 3.3 User clicks "Submit" button. 4. Upon successful authentication, user is asked to give his/her consent in order his/her personal information to be forwarded to Spanish Demo Service Provider. User clicks "SUBMIT" button. 5. User is redirected back to Spanish Service Provider. 5.1 User can view SAML response from Greek eIDAS Node. User clicks "SUBMIT" button. 5.2 User is successfully logged in Spanish Service Provider.
Result	The user is authenticated from ATHEX IdP and can access the service provided from Spanish Service Provider.

Step 1: The user accesses Spanish Service Provider through the following url: https://se-eidas.redsara.es/SP/populateIndexPage.

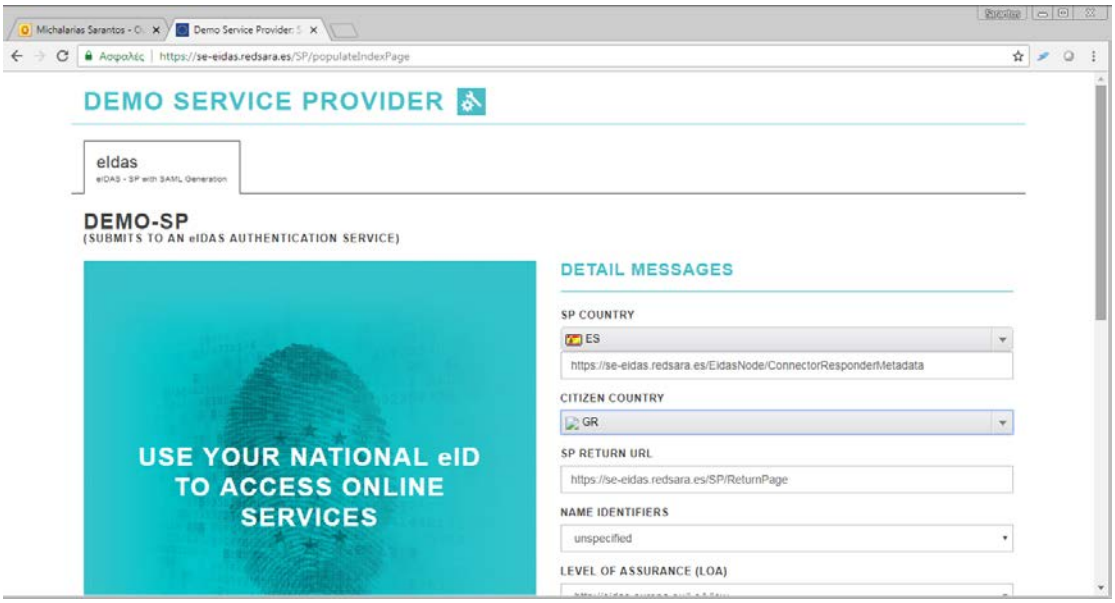

Figure 6-32. Demo Spanish Service Provider Page

Step 2: User selects his /her country of origin and also gets informed about the attributes requested by Spanish Demo Service Provider.

2.1 User selects “ES” in “SP COUNTRY” drop-down list, “GR” in “CITIZEN COUNTRY” drop-down list and press “SUBMIT” button.

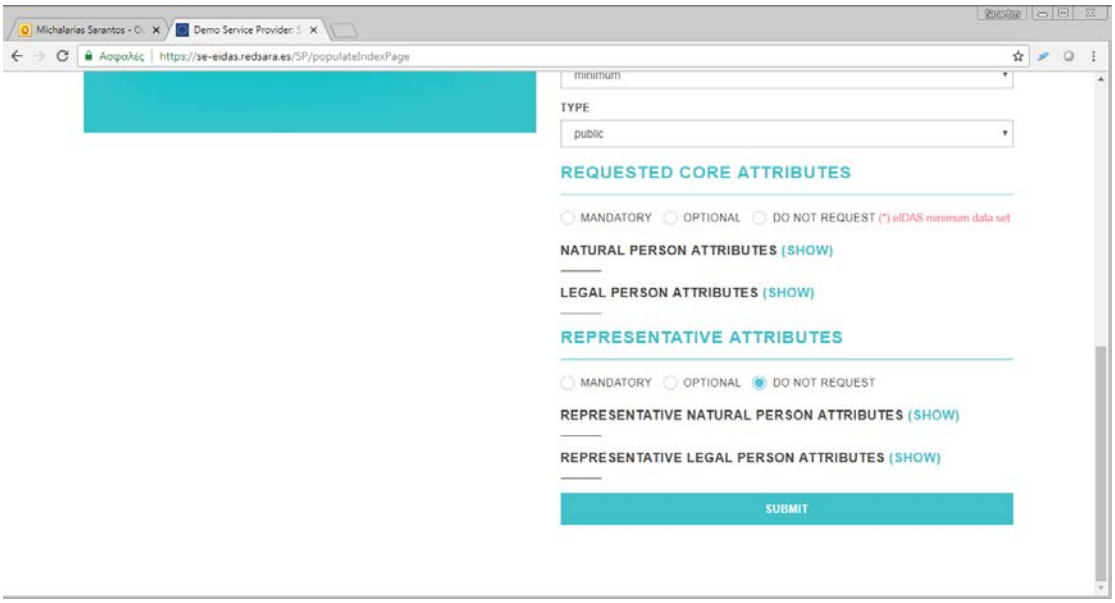

Figure 6-33. User Request eIDAS authentication from demo Spanish Service Provider Page

2.2 User press “SUBMIT” button in order to send the SAML request to Spanish eIDAS Node.

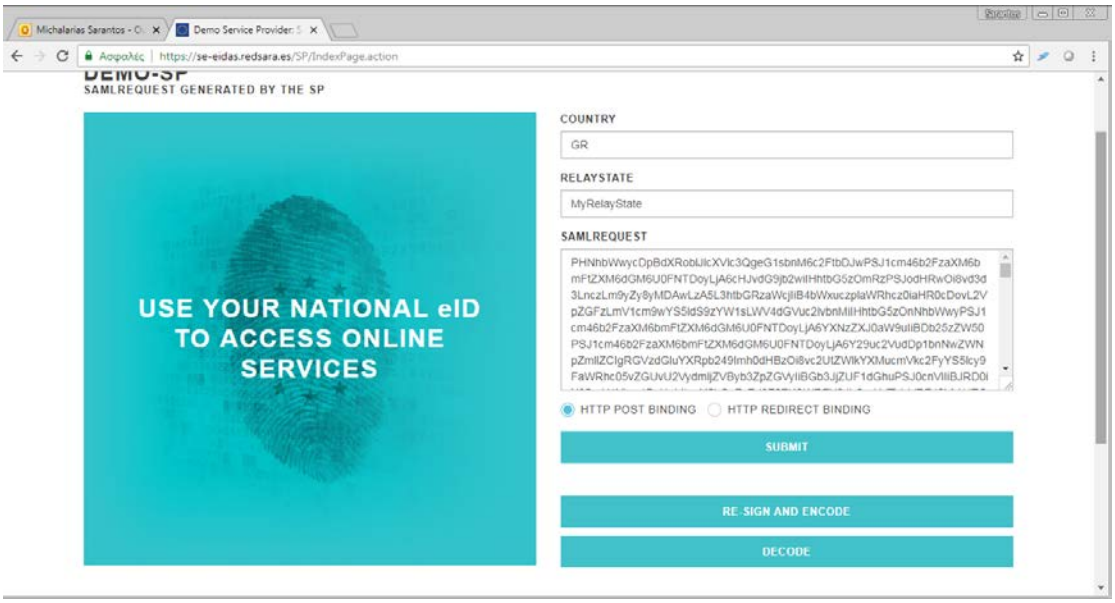

Figure 6-34. Demo Spanish Service Provider SAML Request preview

2.3 User is asked from Spanish eIDAS Node to choose the country from where his /her eID is issued. User selects “Greece” from the drop –down list and clicks “Login” button.

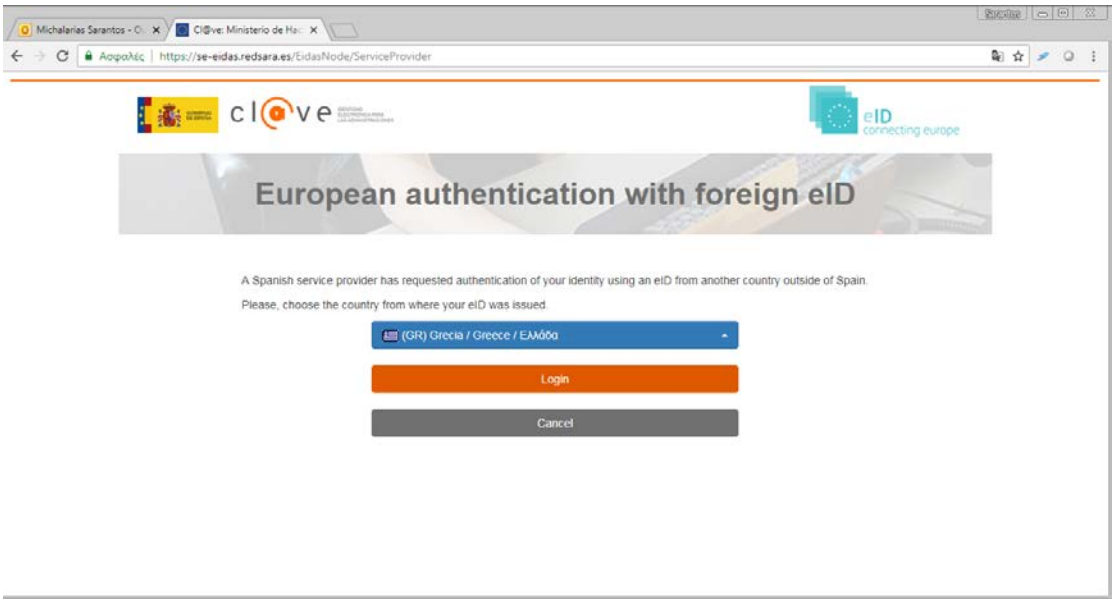

Figure 6-35. Country selection page

2.4 User is redirected to Greek eIDAS Node and he/she is informed about the attributes requested (Basic Information) from Spanish Service Provider. User clicks «NEXT» button.

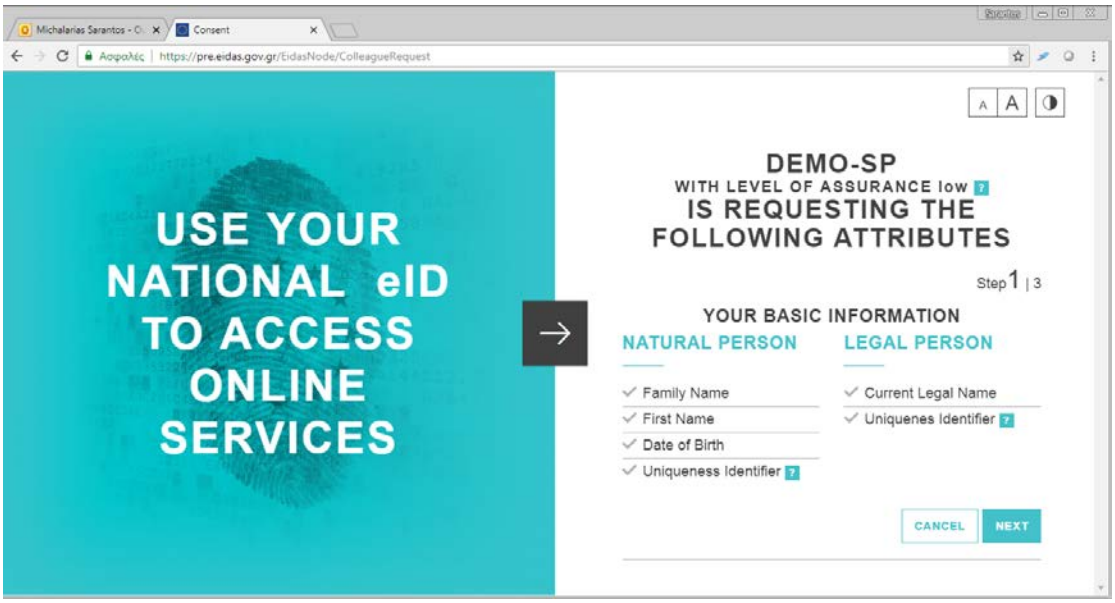

Figure 6-36. Attributes Pre Consent Page

2.5 User is also informed about the attributes requested (Additional Information) from Spanish Service Provider. User clicks «NEXT» button.

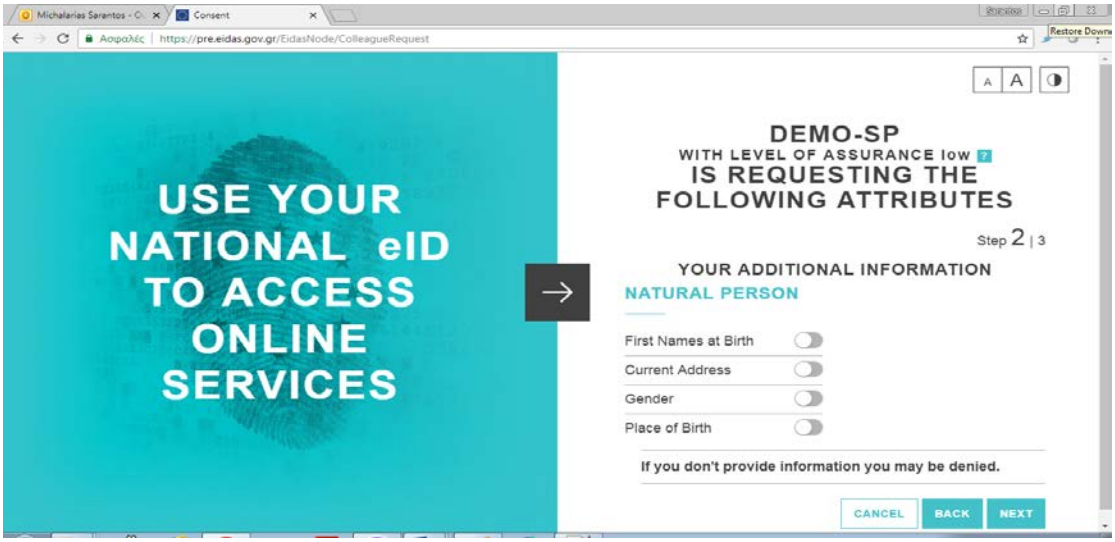

Figure 6-37. Optional Attributes Pre Consent Page

Step 3: User is redirected to ATHEX IdP and he/she is asked to provide his/her credentials. (User name, password, One Time Password) in order to authenticate him/herself.

3.1 User fills in his/her username and password

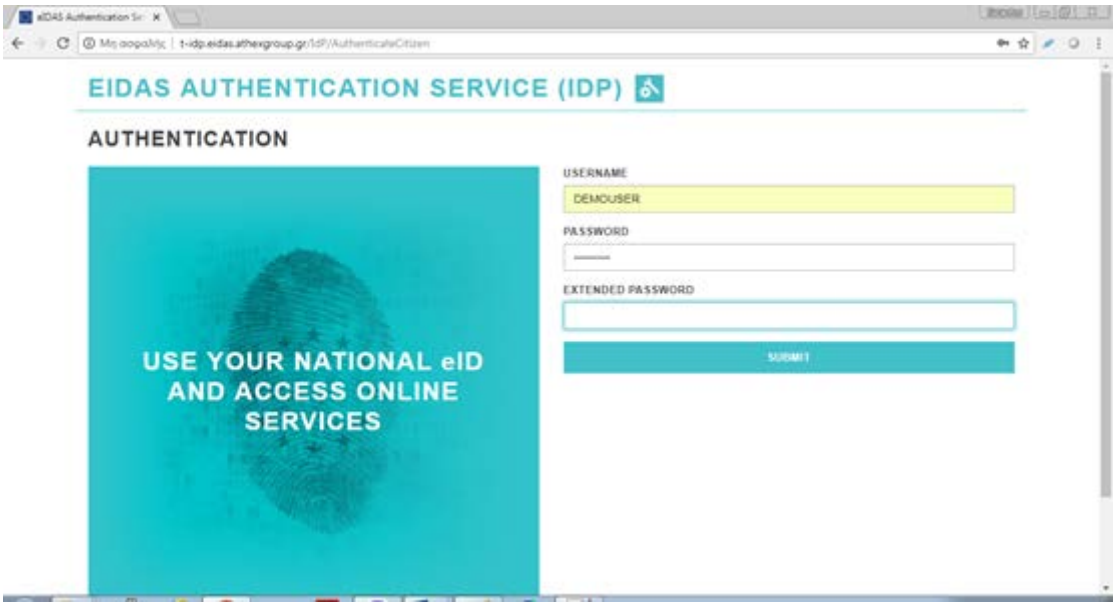

Figure 6-38. ATHEX IdP Page

3.2 User retrieves the One Time Password (OTP) from his/her smartphone, by opening Google Authenticator Application which is already installed in his/her smartphone and fills in the "Extended Password" field.

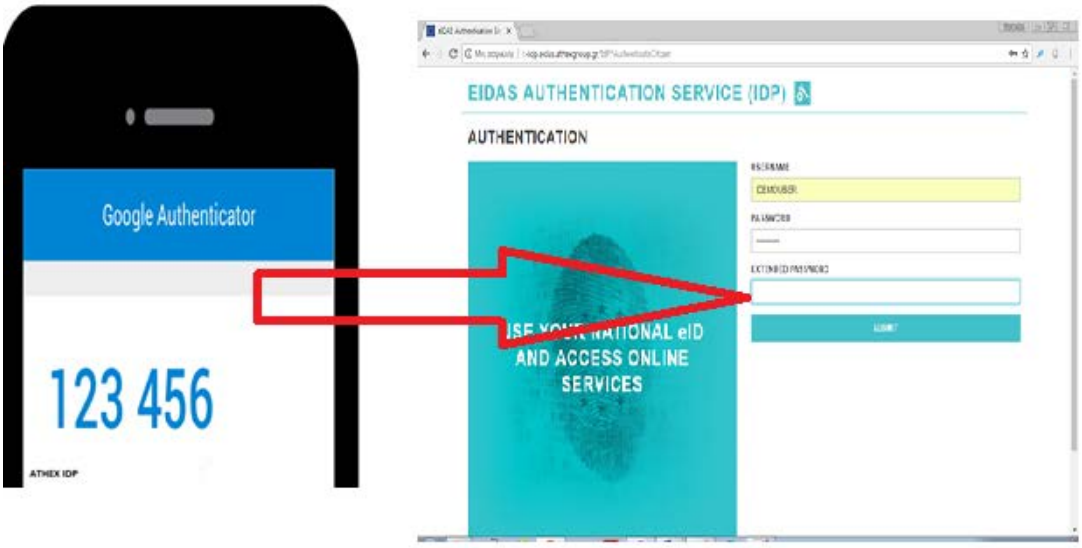

Figure 6-39. User receives OTP from Google Authenticator

3.3 User clicks "Submit" button.

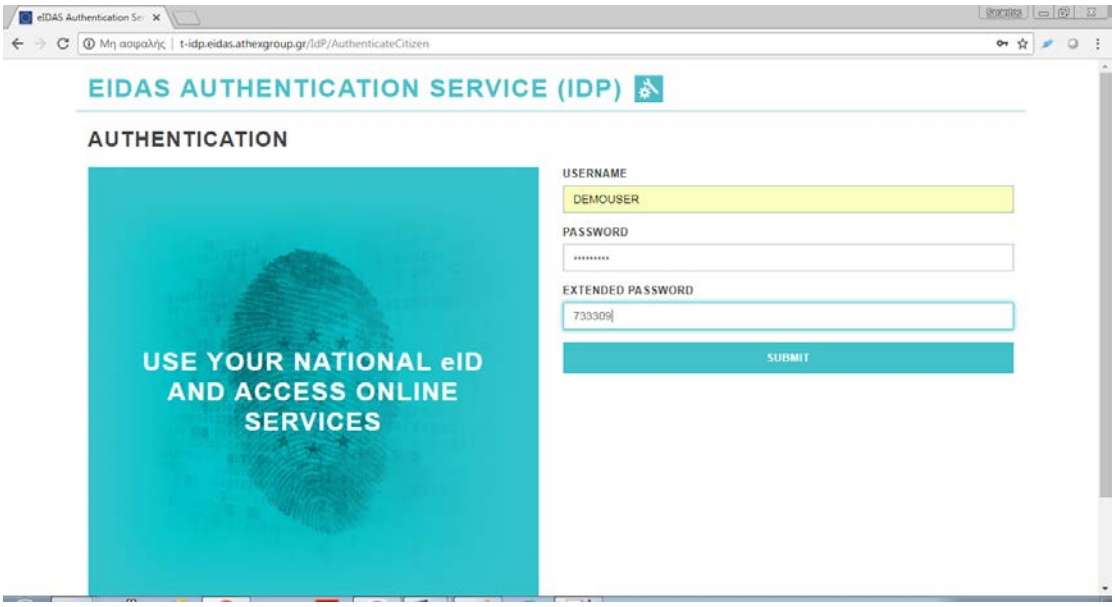

Figure 6-40. User fills in OTP in ATHEX IdP Page

Step 4: Upon successful authentication, user is asked to give his/her consent in order his/her personal information to be forwarded to Spanish Demo Service Provider. User clicks “SUBMIT” button.

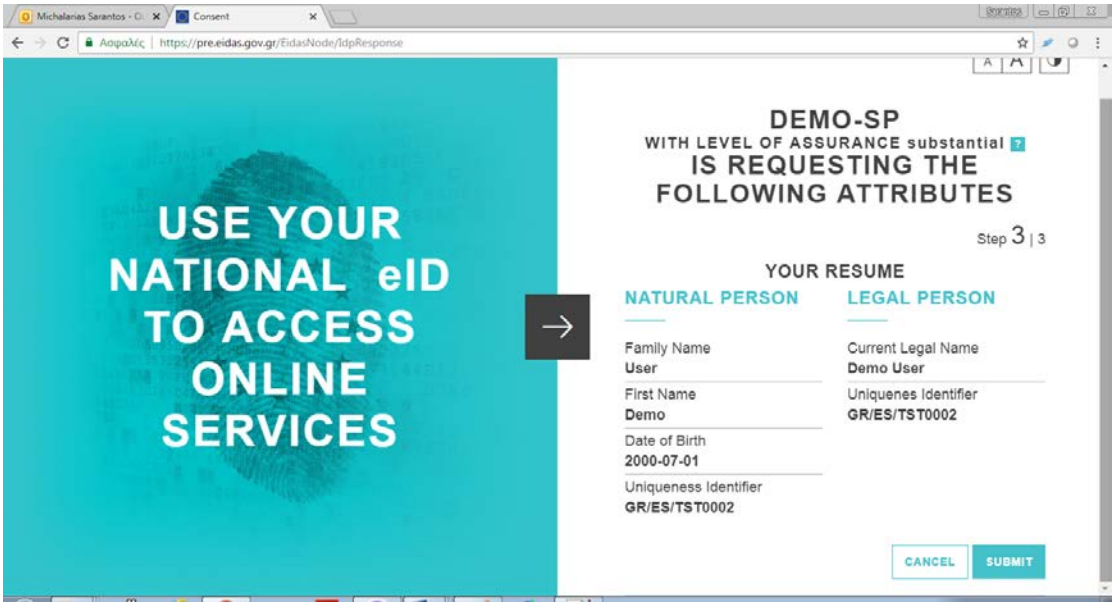

Figure 6-41. Attributes Pre Consent Page

Step 5: User is redirected back to Spanish Service Provider. User can view SAML response from Greek eIDAS Node.

5.1 User can view SAML response from Greek eIDAS Node. User clicks “SUBMIT” button.

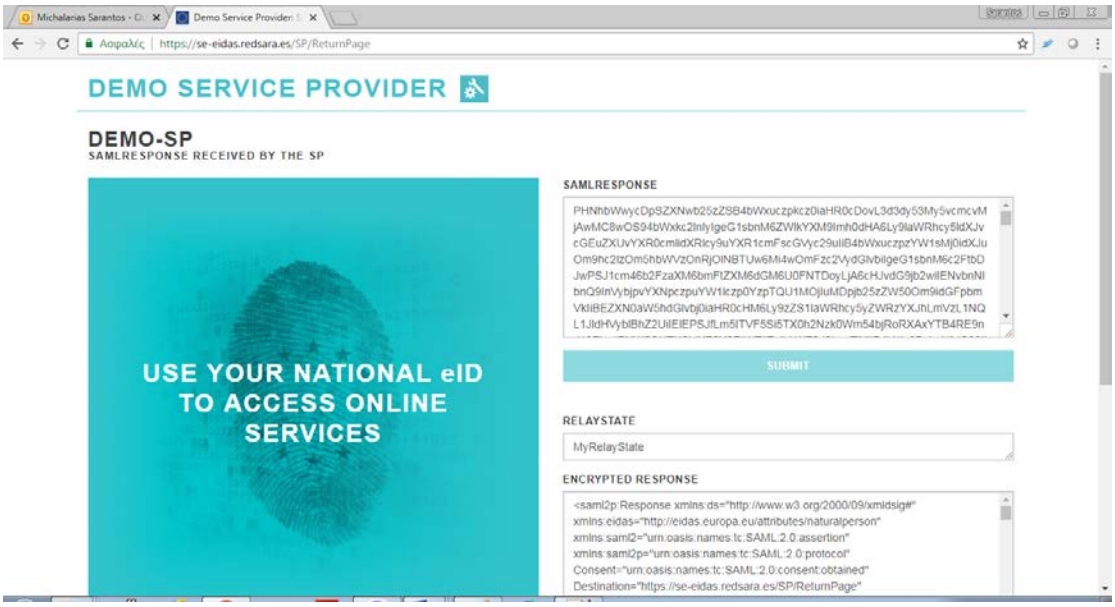

Figure 6-42. SAML response from Greek eIDAS Node

5.2 User is successfully logged in Spanish Service Provider.

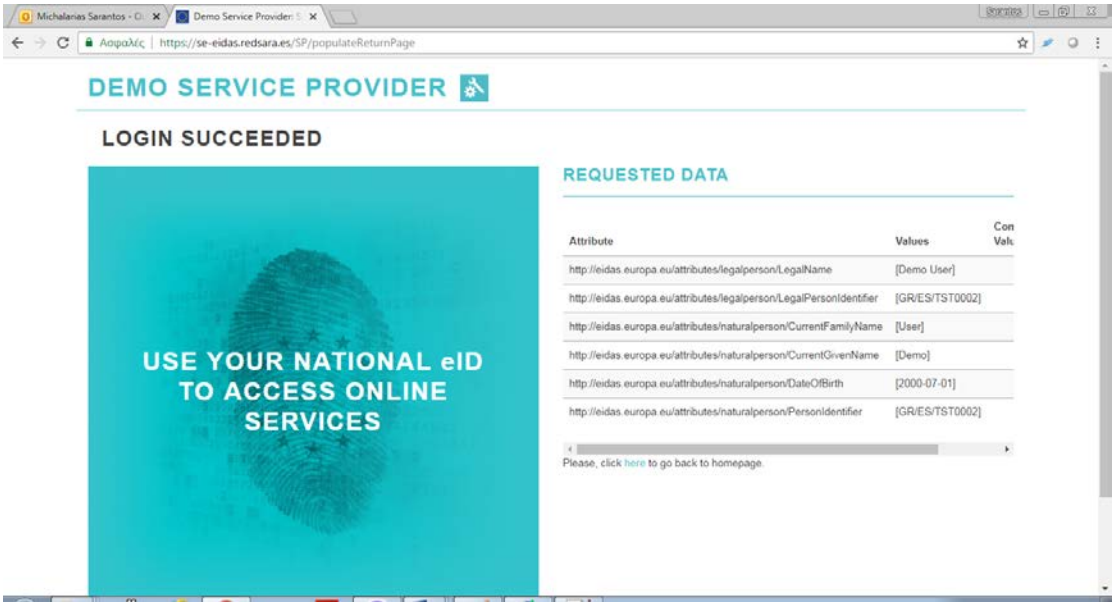

Figure 6-43. Successful login in Spanish SP

6.2 ELTA

The test cases for Hellenic Post services (ELTA eDelivery Hybrid service, ELTA portal/eShop, Parcel Delivery Voucher and Online Zip Codes for Business users) are presented below.

6.2.1 ELTA eDelivery Hybrid Service

Service Start and End Events

ELTA eDelivery Hybrid Mail Service	
Start Testing Event	http://212.205.82.119/portalLogin.jsp?disconnected=1
End Testing Event	A user registers and then logs into to the system using eIDAS

Test Cases

ELTA eDelivery Hybrid Mail Service	
Test Case	User Registration Flow | A non-registered user tries to register to the Service
Test Case	Registered not logged-in User Accessing Service Flow | A registered but not logged-in user tries to access the service

6.2.1.1 Test Case: User registration

Test with a Greek User

Description	A non-registered user register with the Service
Preconditions	The user has eIDAS credentials
Process	1. The user accesses the Greek Service Provider through the following URL (http://212.205.82.119/portalLogin.jsp?disconnected=1) 2. User selects "Σύνδεση" to login to the system 3. User Selects her country of origin 4. User Authenticates using eIDAS 5. User is requested to f ill in additional non eIDAS provided attributes 6. User registers to the service 7. System redirects valid users to the service page

Result	User is registered

Step1. The user accesses the service page and selects the “Σύνδεση” button

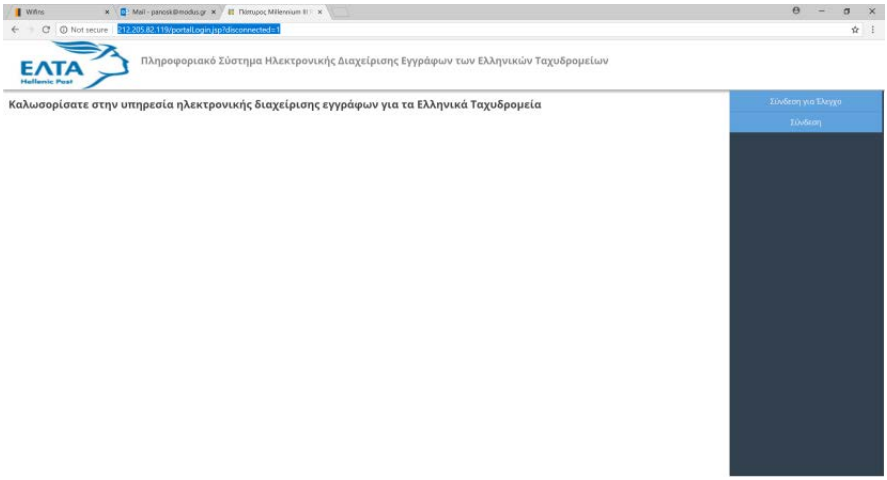

Figure 6-44. ELTA eDelivery Hybrid Mail Service Home Page

Step 2. User completes the login process by inserting the right credentials

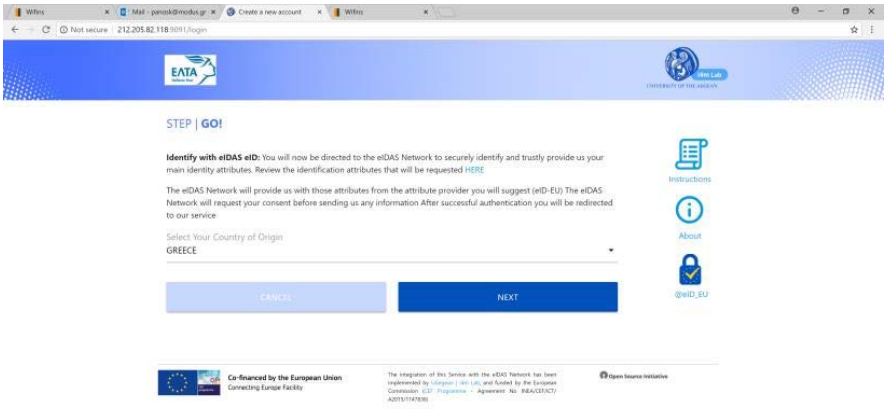

Figure 6-45. Country Selection Page

Step 3. User is presented with the eIDAS attributes that will be returned to the service provider.

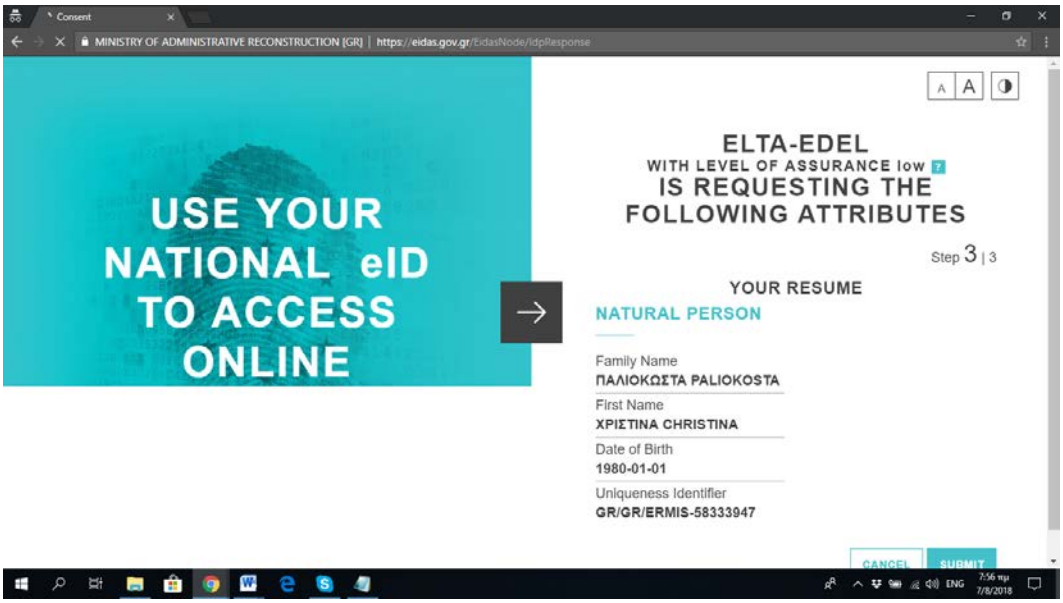

Figure 6-46. Attributes Consent Page

Step 4. User is required to fill in additional non-eIDAS provided identification attributes

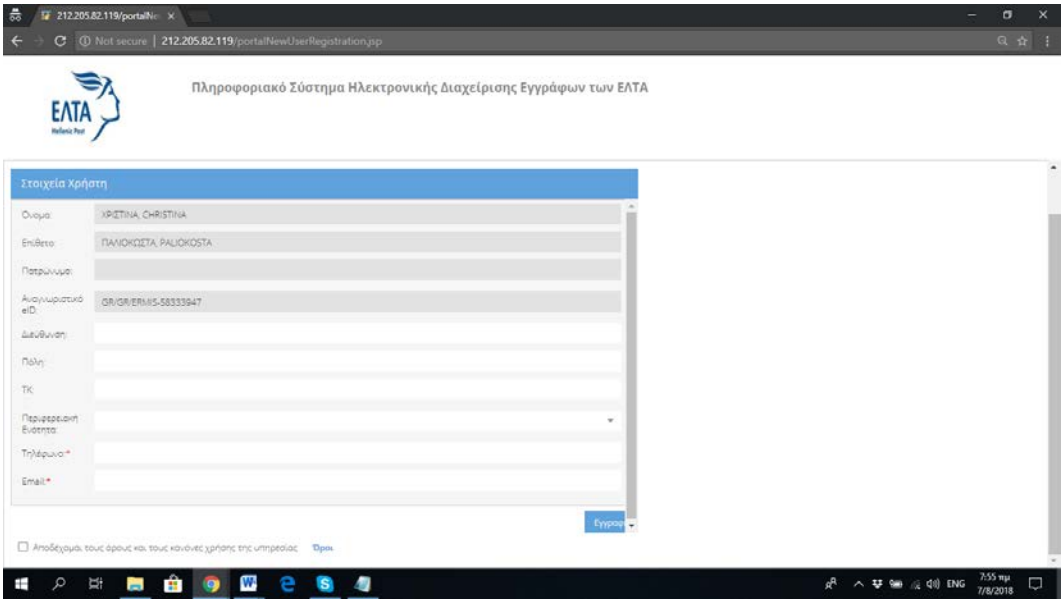

Figure 6-47. Registration Form with prefilled eIDAS attributes

Step 5. The User accesses the service

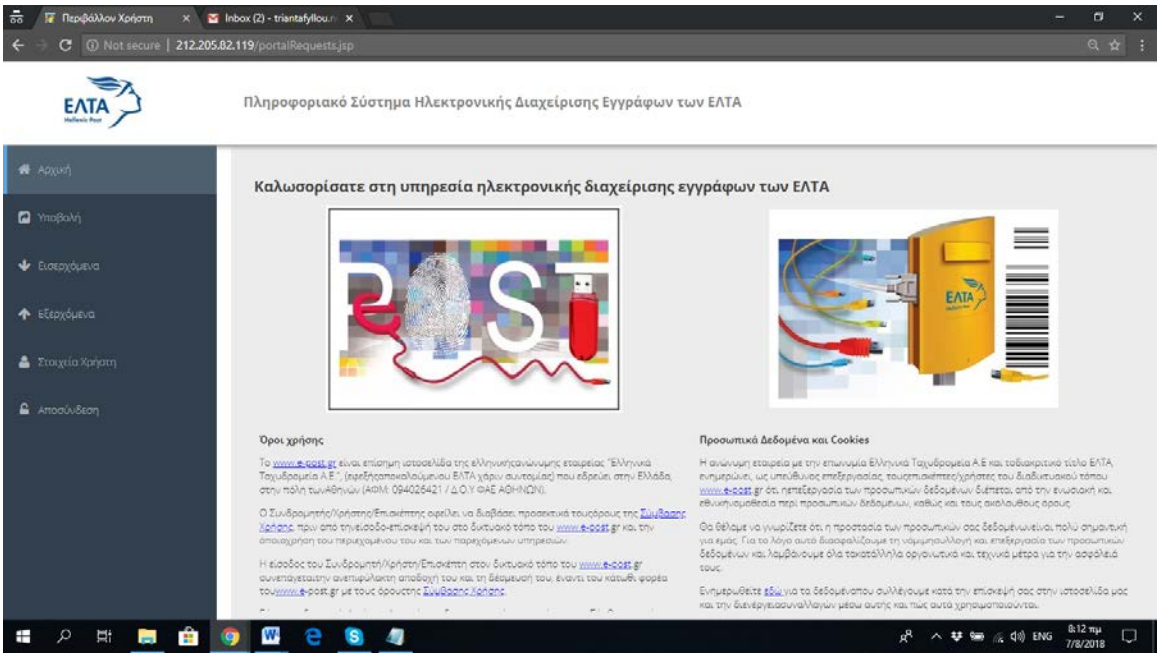

Figure 6-48. User accesses the service

6.2.1.2 Test Case: (Registered) User login

Test with a Greek User

Description	Registered eIDAS user login into the system using his/her credentials
Preconditions	The user has eIDAS credentials
Process	1. The user accesses the Greek Service Provider through the following URL (http://212.205.82.119/portalLogin.jsp?disconnected=1) 2. User selects "Σύνδεση" to login to the system 3. User Selects her country of origin 4. User Authenticates using eIDAS 5. User accesses the service
Result	Registered user login to portal service page

The user accesses the service page and selects the "Σύνδεση" button

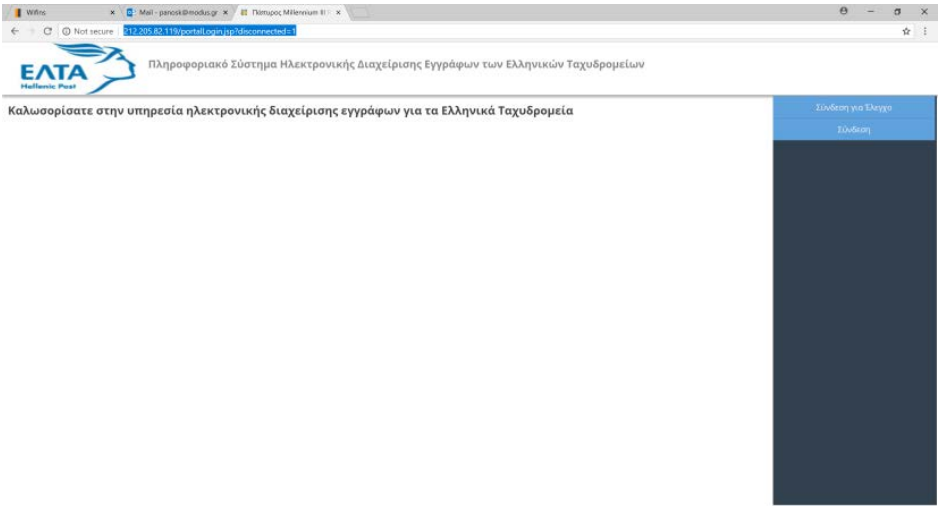

Figure 6-49. Service Login page

User completes the login process by inserting the right credentials

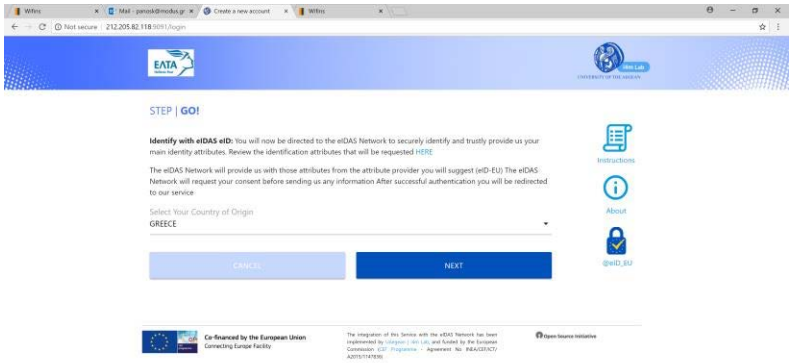

Figure 6-50. Country selection page

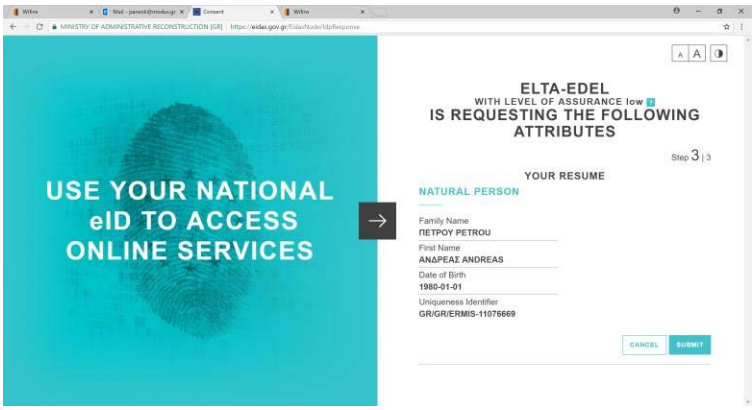

Figure 6-51 Attributes Consent form

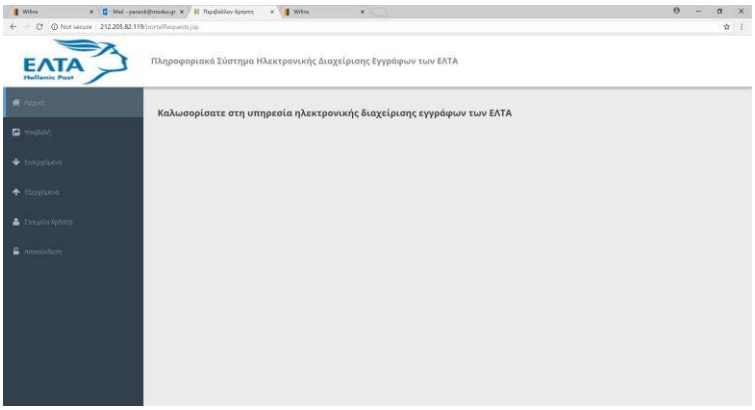

Figure 6-52. User accesses the service

6.2.2 ELTA portal /eShop

Service Start and End Events

ELTA portal /eShop	
Start Testing Event	http://www.elta.gr
End Testing Event	A user registers and then logs into to the system using eIDAS.

Test Cases

ELTA eDelivery Hybrid Mail Service	
Test Case	User Registration Flow | A non-registered user registers with the Service

Test Case	Registered not logged-in User Accessing Service Flow | A registered logs into the Service

6.2.2.1 Test Case: User registration

Test with a Greek User

Description	A non-registered user registers with the Service
Preconditions	The user has eIDAS credentials
Process	1. The user accesses the Greek Service Provider through the following URL (http://www.elta.gr) 2. User selects “Login with eIDAS” 3. User Selects her country of origin 4. User Authenticates using eIDAS 5. User is requested to f ill in additional non eIDAS provided attributes 6. User registers to the service 7. System redirects valid users to the service page
Result	User is registered to the service

Step 1: On the top right corner of elta.gr, exists a new option of login: “Login with eIDAS”

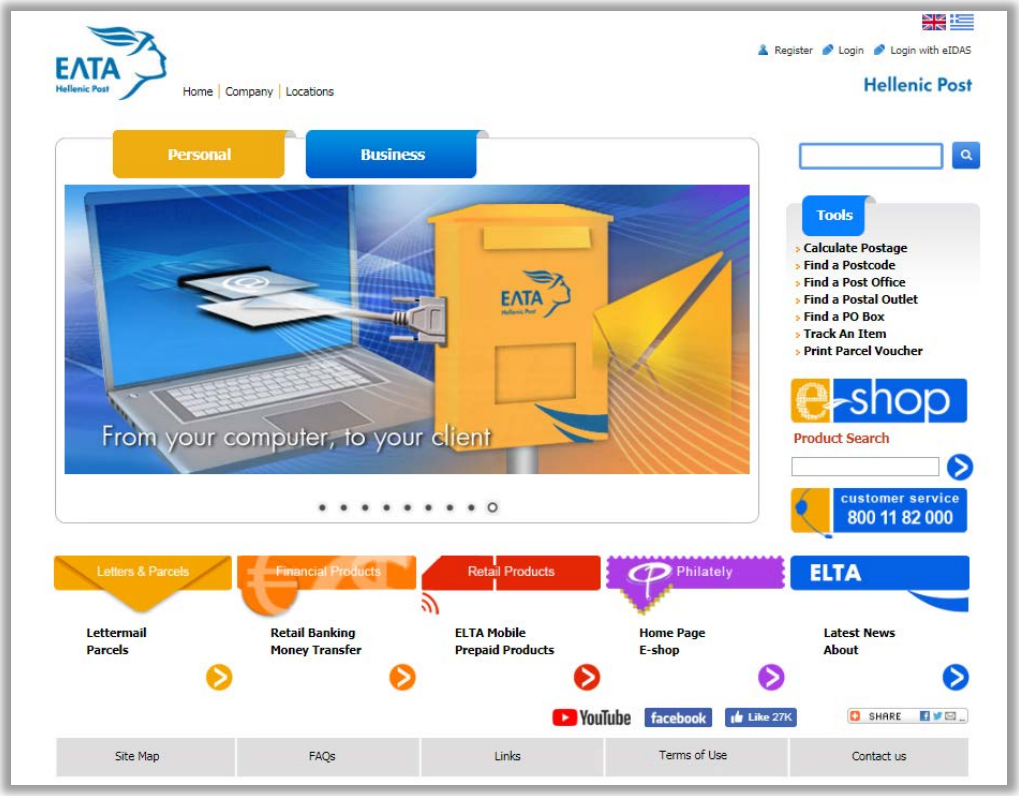

Figure 6-53. Service Home Page

Step 2: When selecting "Login with eIDAS" option, user's browser is redirected to the page:

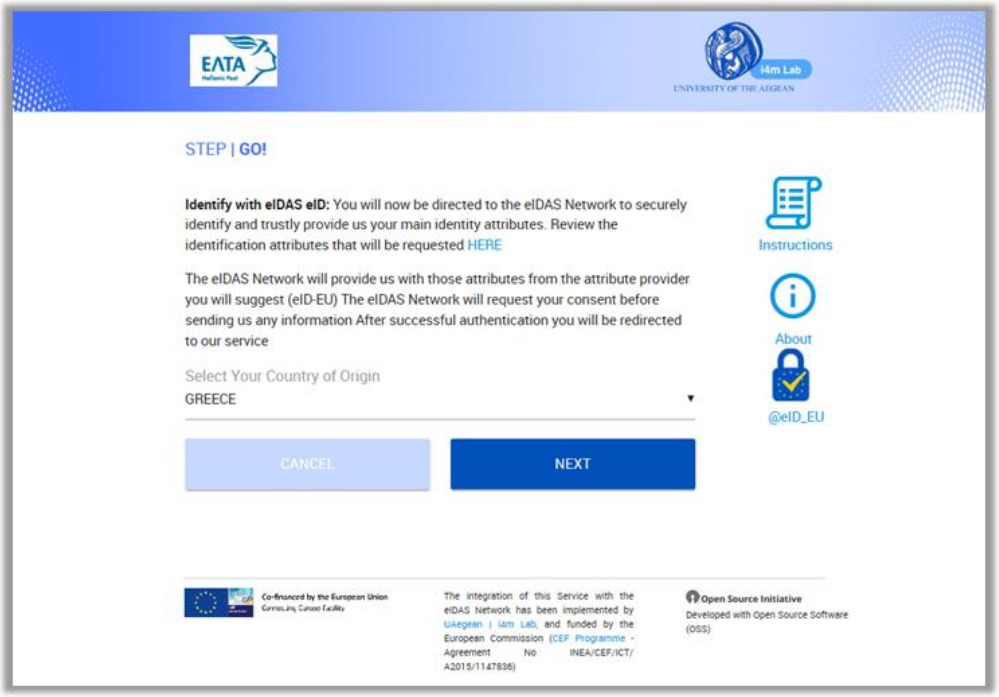

Figure 6-54. Country Selection Page

Here the user can select his Country of Origin. Pre-Selected Option is GREECE.

Step 3: Having selected Greece as Country of Origin, and pressing "Next" button, user's browser is redirected to ERMIS IDP Service:

Figure 6-55. ERMIS IdP Page

Step 4: After entering Username & password (correctly), when pressing "Submit" button, a confirmation page appears, about what attributes are going to be exposed to ELTA:

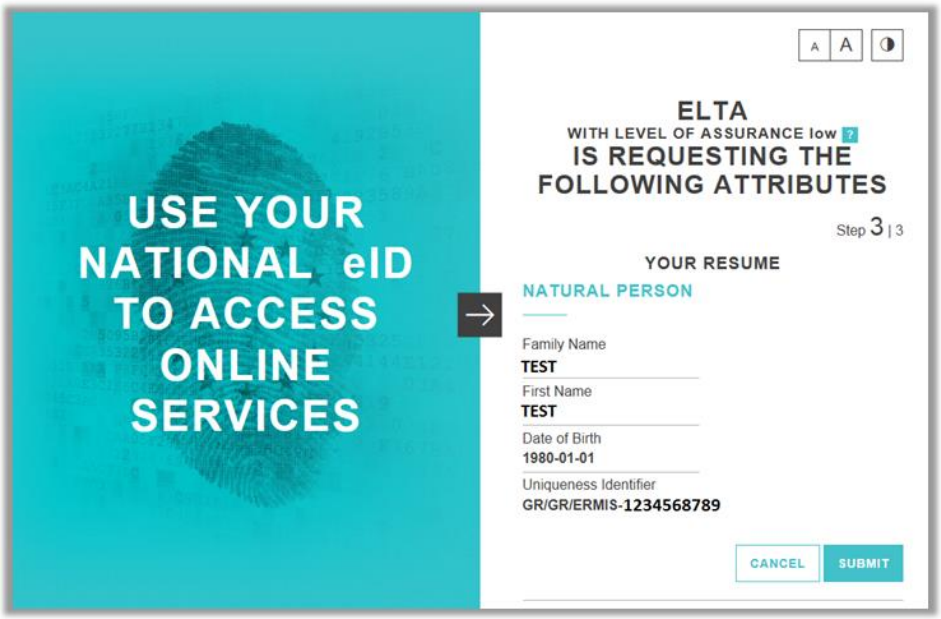

Figure 6-56. Attributes Consent page

Step 5: Pressing “Submit” button on previous page, user is redirected (first to controller page of user origin and then automatically) to elta.gr. Elta.gr Checks if the user with the specific Unique identifier is already registered, and if not prompts a registration page:

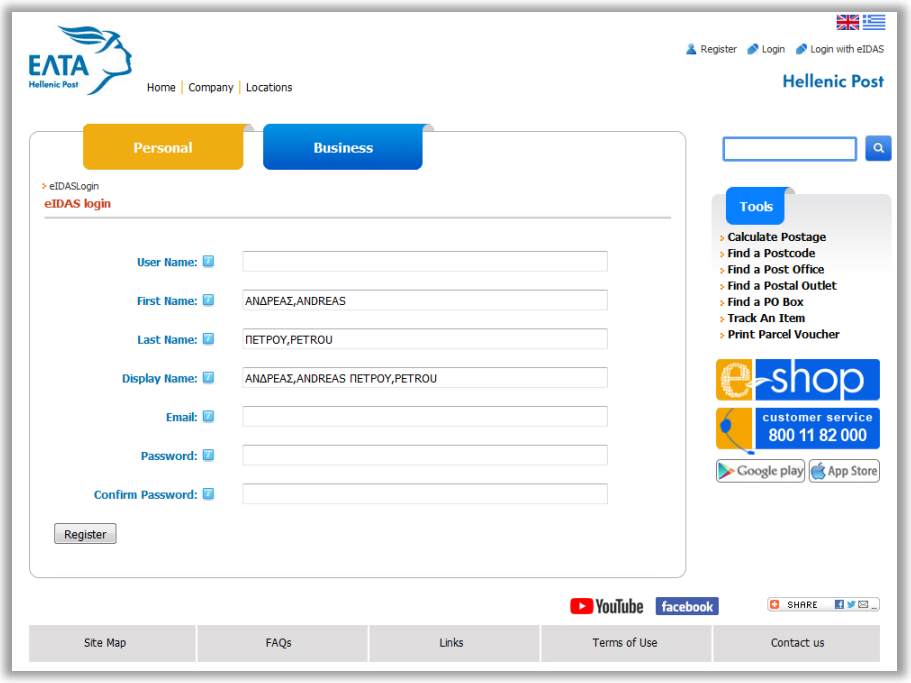

Figure 6-57. Registration Form, eIDAS attributes prefilled

Step 6: Registration page fields: First Name & Last Name are locked (user can't change them):

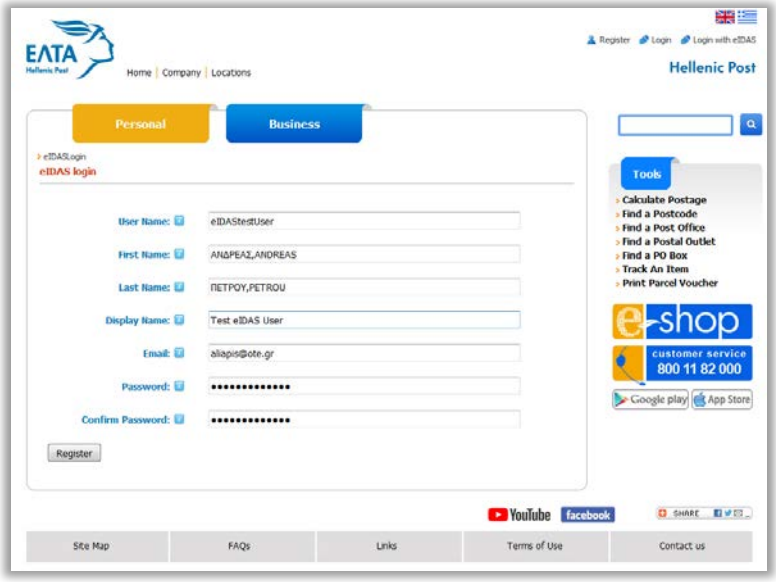

Figure 6-58 User completes registration Form

Step 7. Having completed all other fields correctly and pressed button "Register", ELTA portal creates a local account combined with user's eIDAS account and returns to the page that the process began

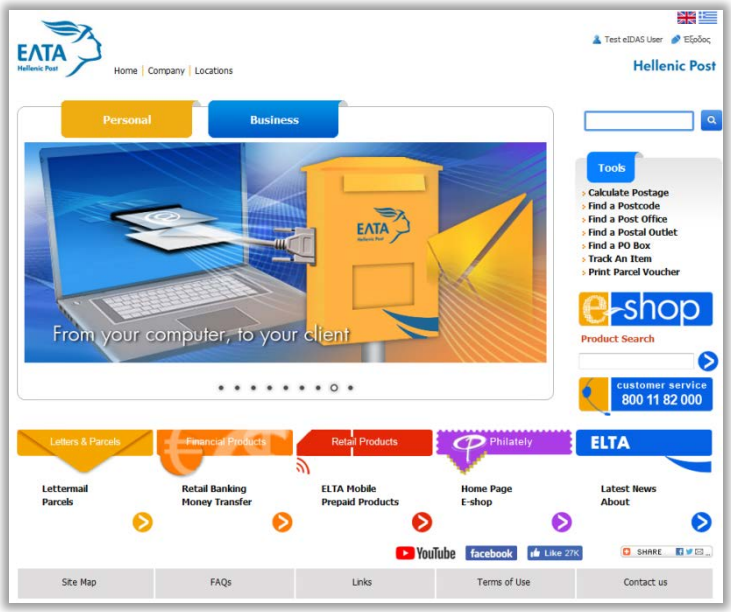

Figure 6-59 User successfully logged in using eIDAS

Test with a Spanish User

Description	A non-registered user registers with the Service
Preconditions	The user has eIDAS credentials
Process	1. The user accesses the Greek Service Provider through the following URL (http://www.elta.gr) 2. User selects “Login with eIDAS” 3. User Selects the country of origin 4. User Authenticates using eIDAS 5. User is requested to fill in additional non eIDAS provided attributes 6. User registers to the service 7. System redirects valid users to the service page
Result	User is registered to the service

Step 1: On the top right corner of elta.gr, exists a new option of login: “Login with eIDAS”

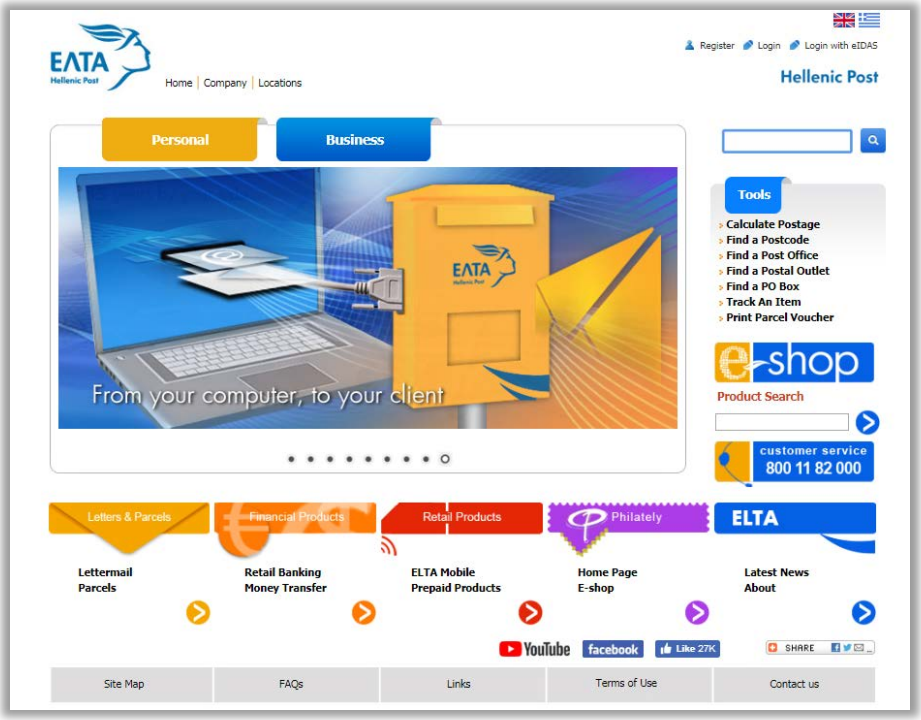

Figure 6-60. Service Home Page

Step 2: When selecting "Login with eIDAS" option, user's browser is redirected to the page:

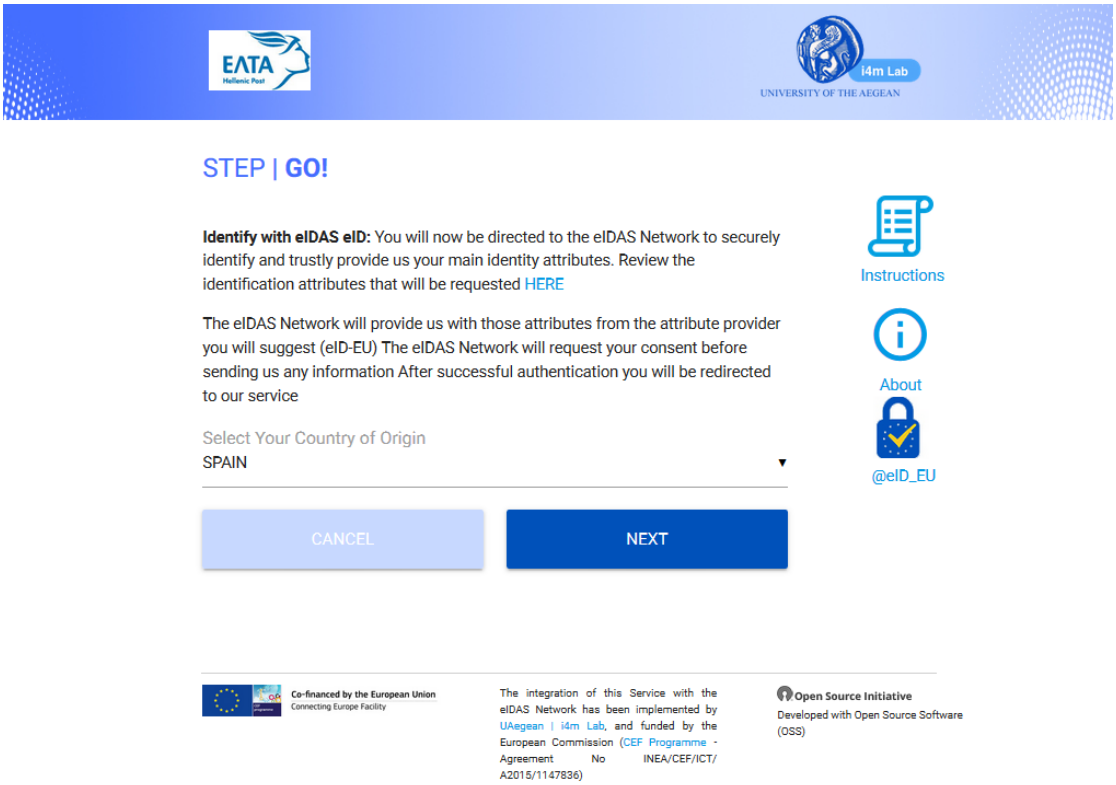

Figure 6-61. Country Selection Page

Here the user can select his Country of Origin (Spain)

Step 3. Selecting "SPAIN" and pressing NEXT, we are transferred to Spanish eIDAS Node:

Figure 6-62. Spanish IdP Page

Step 4. Selecting "Confirmar", a message box appears that mentions the usage of certificate use for authenticating the user:

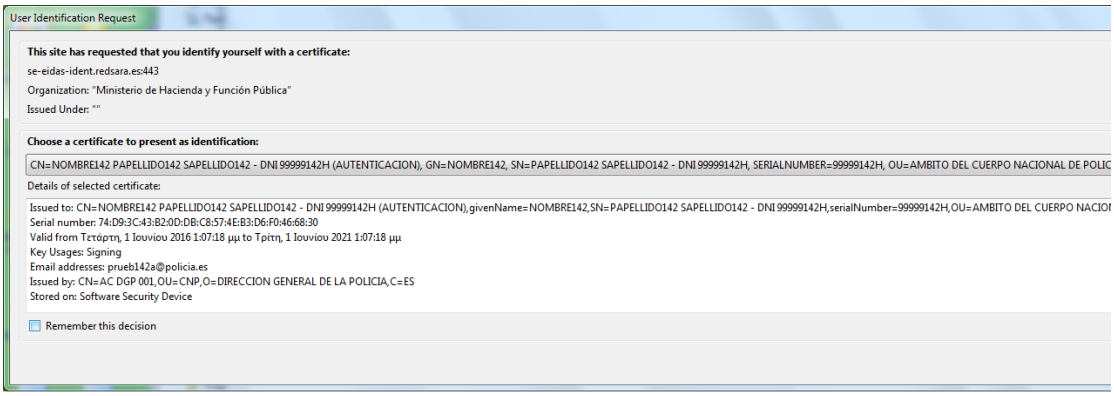

Figure 6-63 Certificate Selection

Step 5. Selecting "OK" at the message box user is redirected (first to controller page of user origin and then automatically) to elta.gr. Elta.gr Checks if the user with the specific Unique identifier is already registered, and if not prompts a registration page:

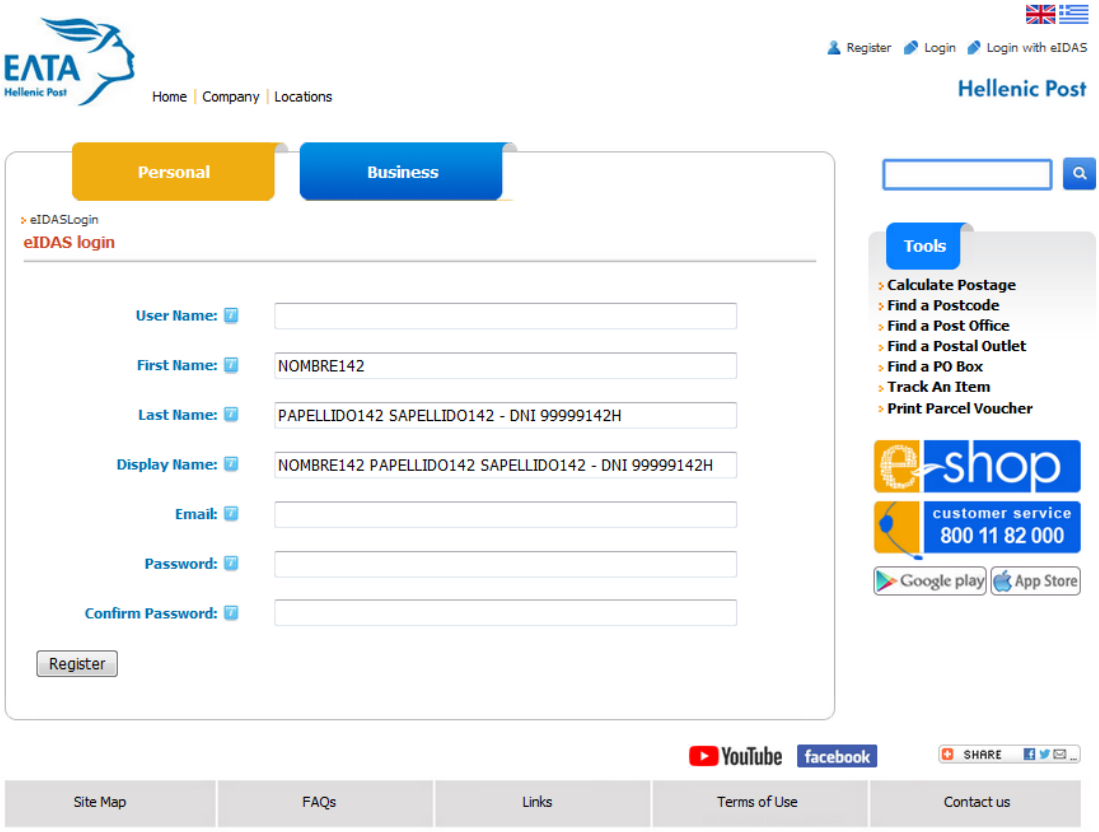

Figure 6-64 Registration form, eIDAS attributes prefilled

Step 6. Registration page fields: First Name & Last Name are locked (user can't change them).

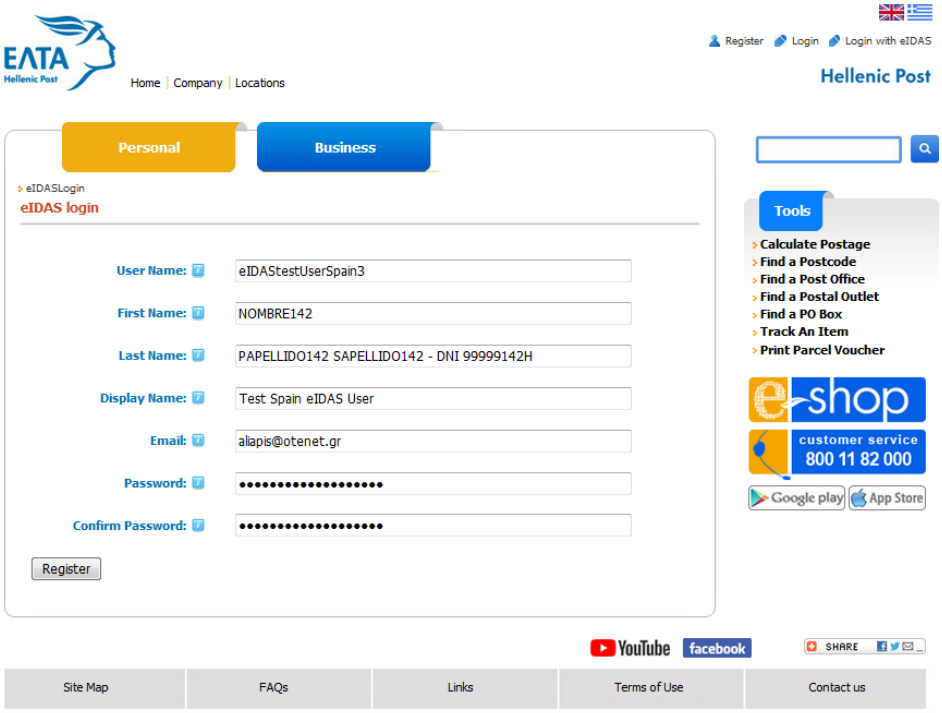

Figure 6-65 User completes registration form

Step 7. Having completed all other fields correctly and pressed button "Register", ELTA portal creates a local account combined with user's eIDAS account and returns to the page that the process began

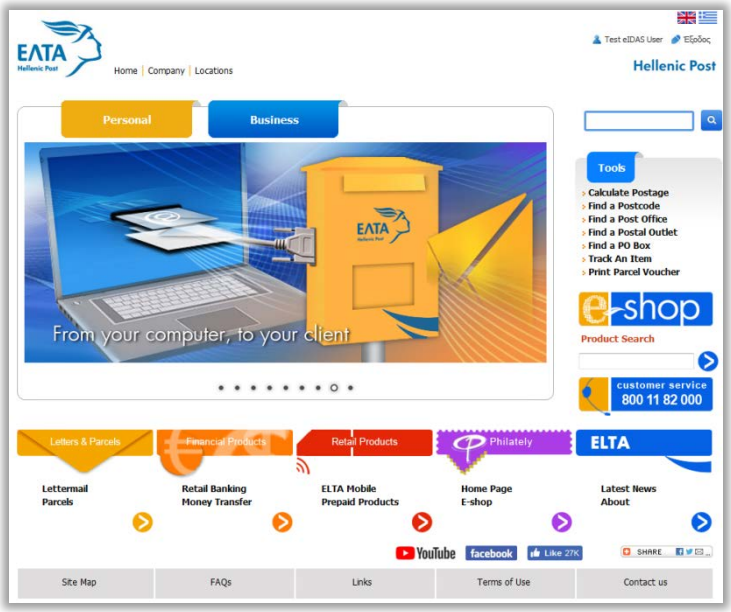

Figure 6-66. User successfully logged in using eIDAS

6.2.2.2 Test Case: (Registered) User Login

Test with a Greek User

Description	A registered user logs into the Service
Preconditions	The user has eIDAS credentials
Process	1. The user accesses the Greek Service Provider through the following URL (http://www.elta.gr) 2. User selects “Login with eIDAS” 3. User Selects her country of origin 4. User Authenticates using eIDAS 5. User accesses the service
Result	User is registered to the service

Step 1: On the top right corner of elta.gr, exists a new option of login: “Login with eIDAS”

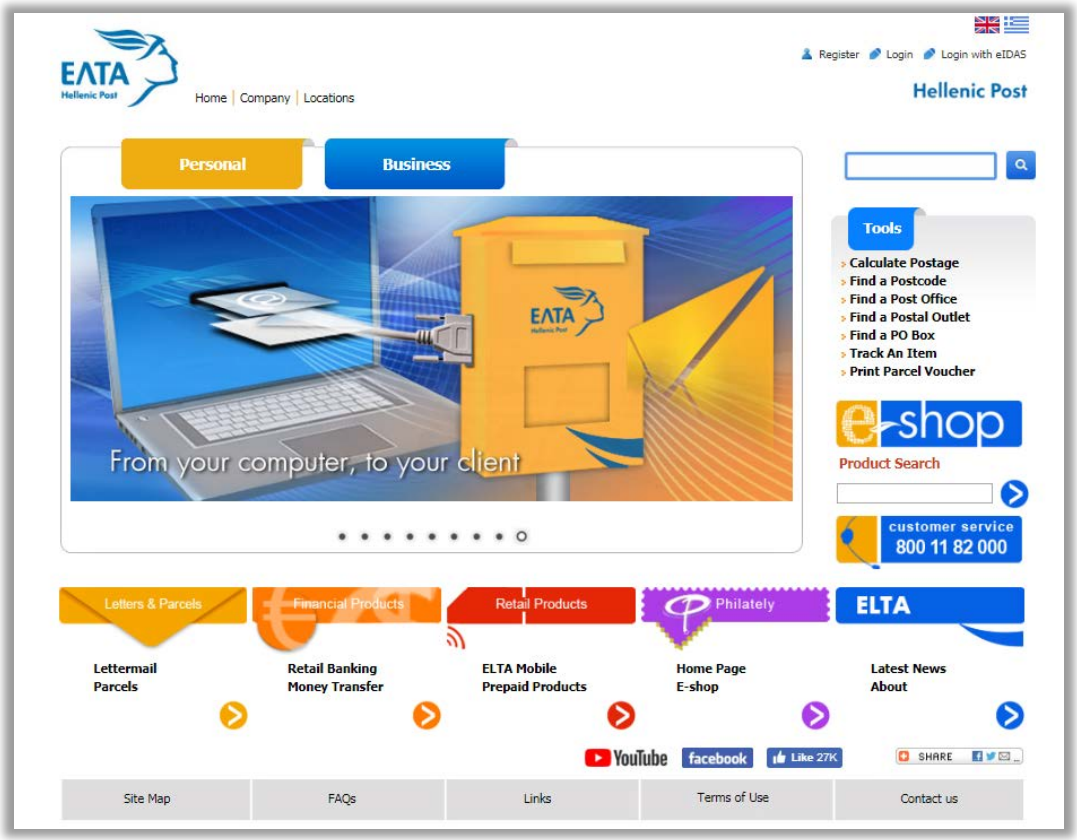

Figure 6-67. Service home page

Step 2. When selecting “Login with eIDAS” option, user’s browser is redirected to the page:

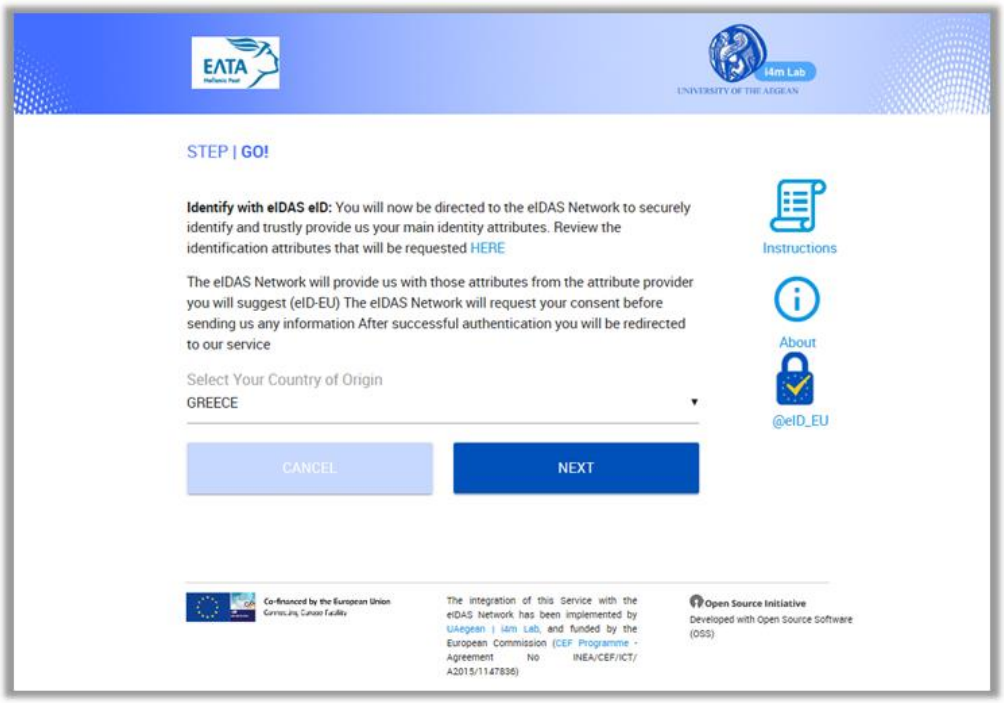

Figure 6-68. Country selection page

Here the user can select his Country of Origin. Pre-Selected Option is GREECE.

Step 3: Having selected Greece as Country of Origin, and pressing “Next” button, user’s browser is redirected to **ERMIS IDP Service**:

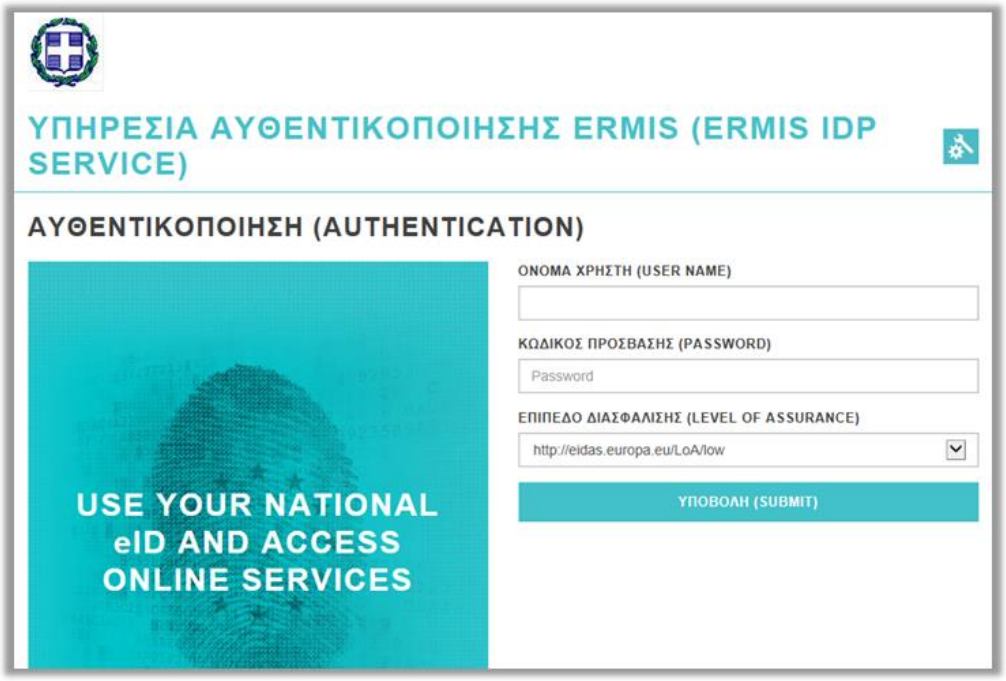

Figure 6-69. ERMIS IdP Page

Step 4: After entering Username & password (correctly), when pressing "Submit" button, a confirmation page appears, about what attributes are going to be exposed to ELTA:

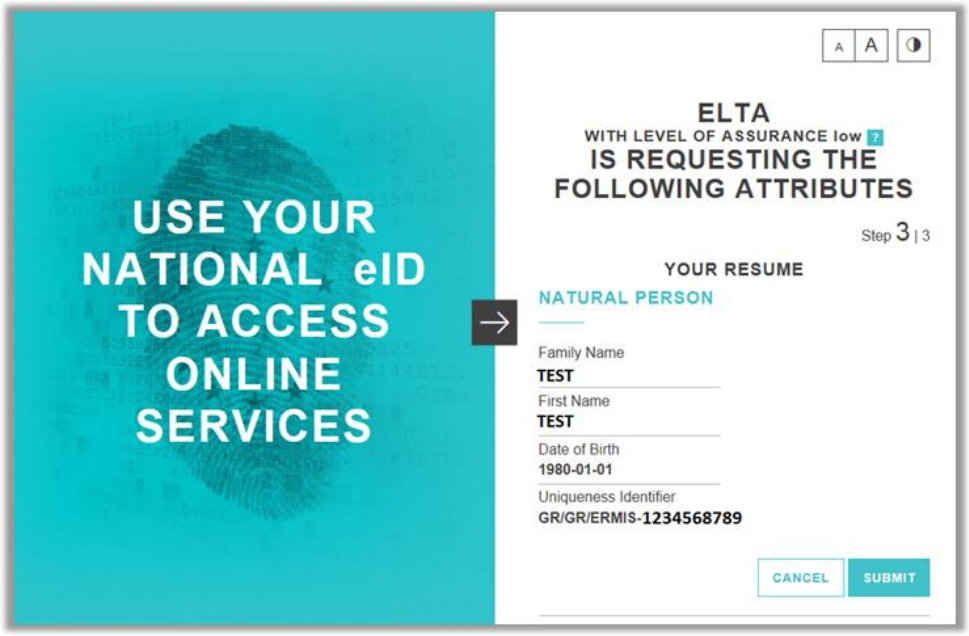

Figure 6-70. Consent Page

Step 5: Pressing "Submit" button on previous page, user is redirected (first to controller page of user origin and then automatically) to elta.gr. Elta Portal checks if the user with the specific unique identifier is already registered, and if local account with this unique identifier exists, then logs in the user and returns to the page that the process began:

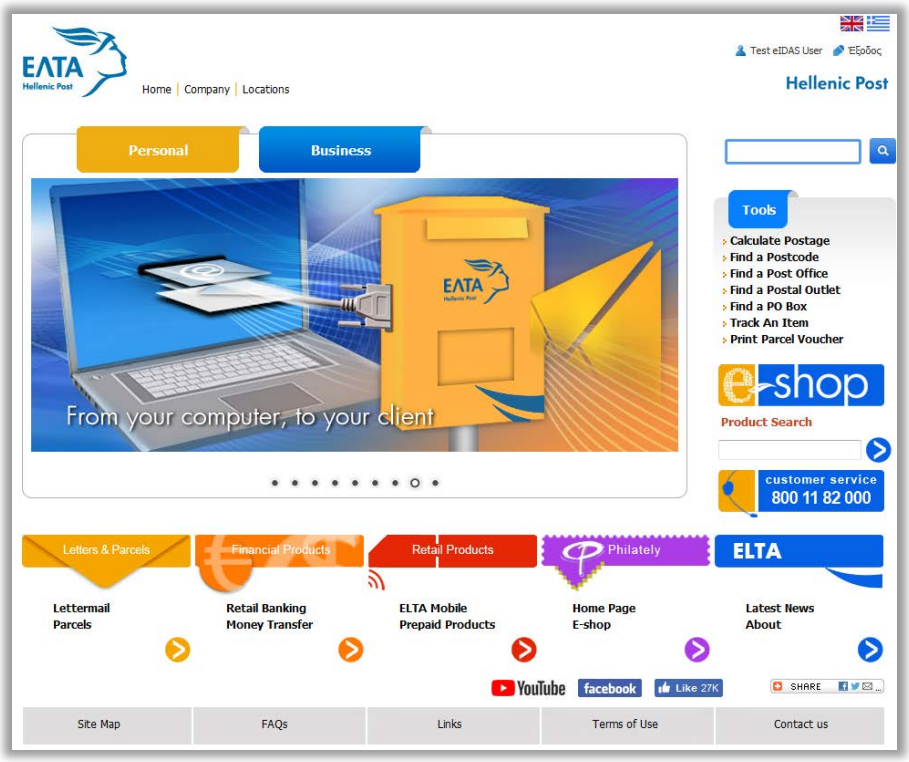

Figure 6-71. User successfully logged in using eIDAS

The test case with a Spanish User is similar to the test case described in page 92 (section 6.2.2.1 Test Case: User registration, Test with a Spanish User).

6.2.3 Parcel Delivery Voucher

Service Start and End Events

ELTA Parcel Voucher Service	
Start Testing Event	http://www.eltab2b.gr/index.php?lang=en
End Testing Event	The user receives a Voucher for his/her parcel

Test Cases

ELTA Parcel Voucher Service

Test Case	User Registration Flow | A user registers with ELTA eltab2b.gr website where she can access the Parcel Voucher Service
Test Case	Registered User Accessing Service Flow | A registered User logins to the Parcel Voucher service

6.2.3.1 Test Case: User registration

Test with a Greek User

Description	A non-registered user tries to register with the ELTA eltab2b.gr website
Preconditions	The user is not authenticated and is not registered to eltab2b.gr and has valid eIDAS credentials
Process	1. User accesses the service via (http://www.eltab2b.gr/index.php?lang=en) 2. User selects Login with eIDAS 3. User is redirected to the page where he is informed that he can Identify with eIDAS eID. 4. User is authenticated via eIDAS 5. User is redirected to the eltab2b 6. User fills-in the registration form 7. User can use the Service
Result	The user is registered to the service.

Step 1. User accesses the service via (http://www.eltab2b.gr/index.php?lang=en). User selects Login with eIDAS.

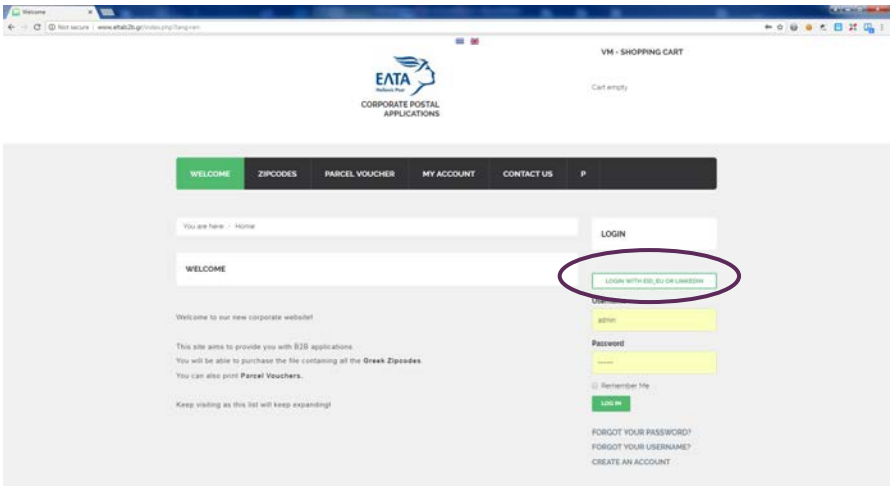

Figure 6-72. Service home page

Step 2. User selects “Country of Origin” GREECE and clicks NEXT.

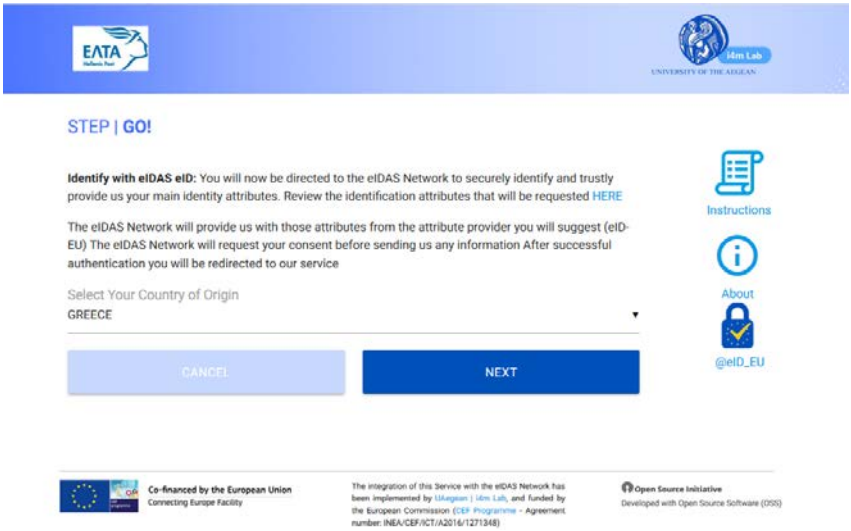

Figure 6-73. Country selection page

Step 3. User is redirected to the ERMIS IDP service where she authenticates with her credentials.

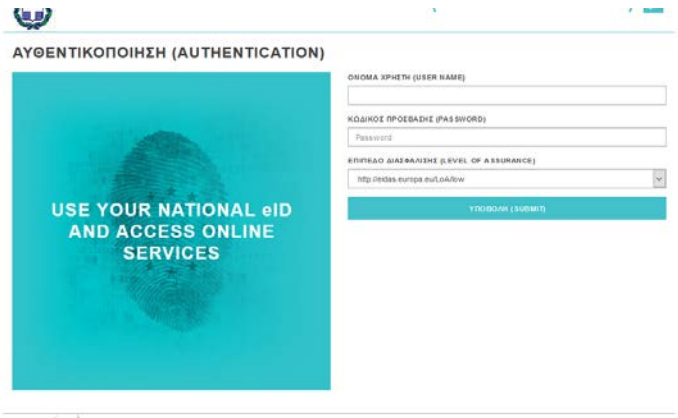

Figure 6-74. ERMIS IdP page

Figure 6-75. Consent Page

Step 4. User is redirected to the eltab2b.gr

User registers by completing the registration form.

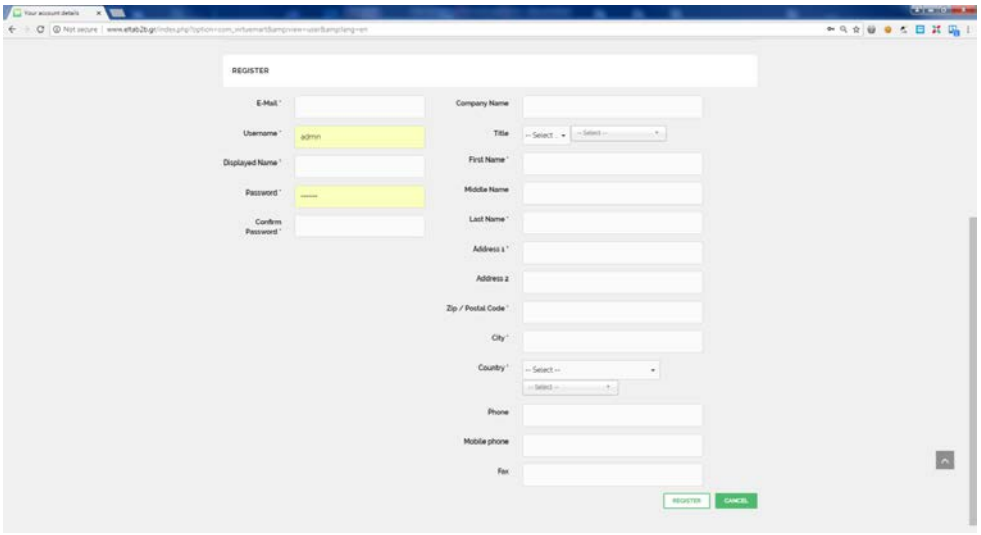

Figure 6-76. Registration form, eIDAS attributes prefilled

User can now use the services of eltab2b.gr.

The test case with a Spanish User is similar to the test case described in page 92 (section 6.2.2.1 Test Case: User registration, Test with a Spanish User).

6.2.3.2 Test Case: (Registered) User login

Test with a Greek User

Description	A registered User of the eltab2b website user logs into and accesses the Service
Preconditions	The user is registered to the service and has valid eIDAS credentials
Process	1. The user accesses service URL (http://www.eltab2b.gr/index.php?lang=en) 2. User proceeds to login 3. User selects Parcel Voucher service 4. User accesses the service

Result	User accesses the service

Step 1. The user accesses eltab2b URL.

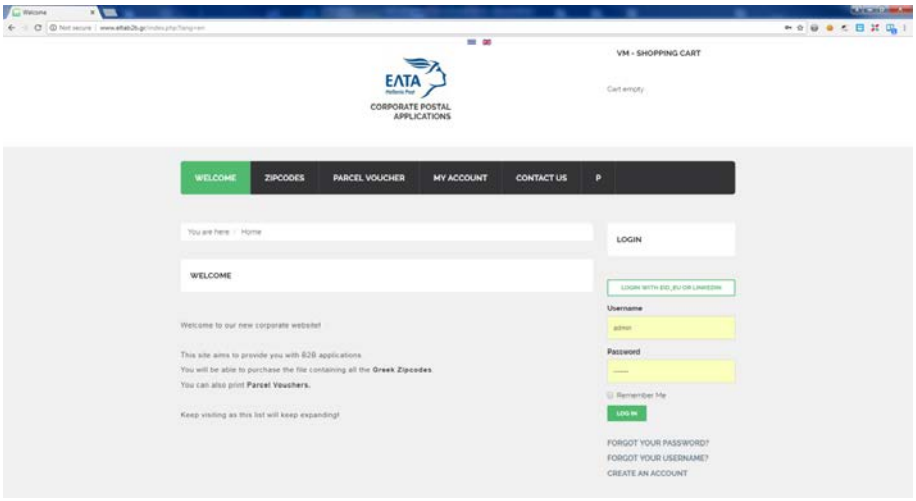

Figure 6-77. Service Home Page

Step 2. The user proceeds with the login, by clicking login with eID_EU.

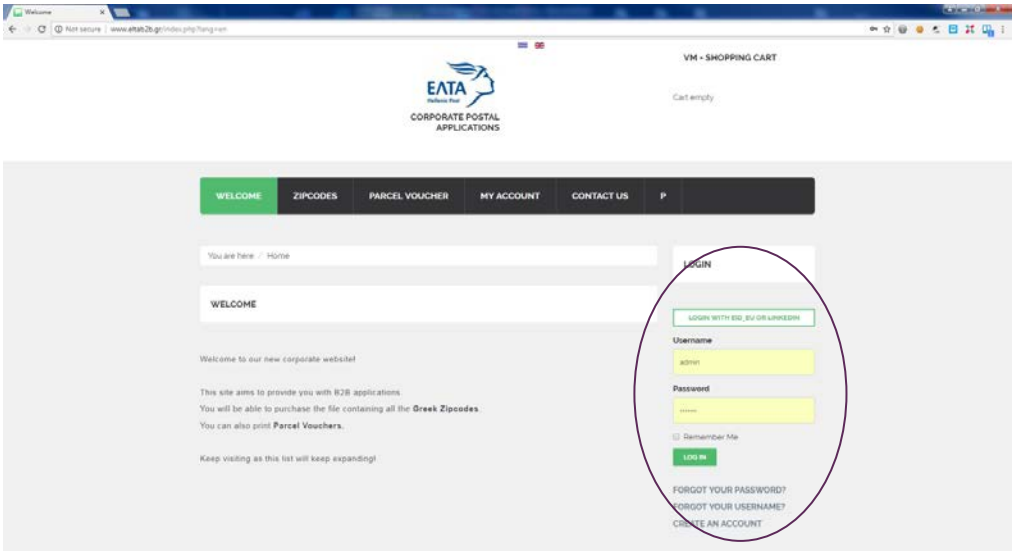

Figure 6-78. User requests login with eIDAS

Step 3. User selects “Country of Origin” GREECE and clicks NEXT.

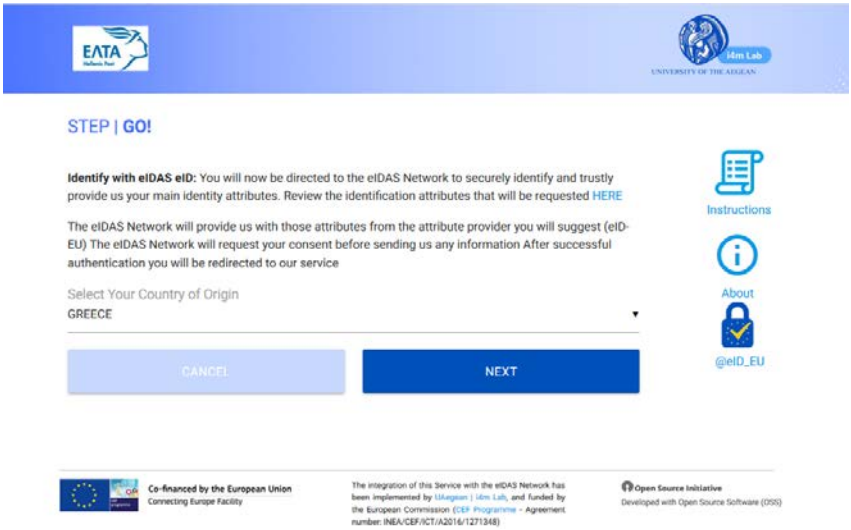

Figure 6-79. Country selection page

Step 4. User is redirected to the ERMIS IDP service where she authenticates with her credentials.

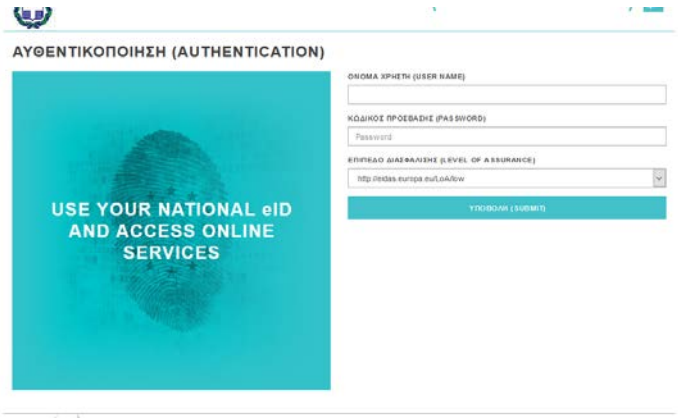

Figure 6-80. ERMIS IdP page

Figure 6-81. Consent page

Step 5. User selects “Parcel Voucher”, fills-in the form and clicks “Print Voucher”.

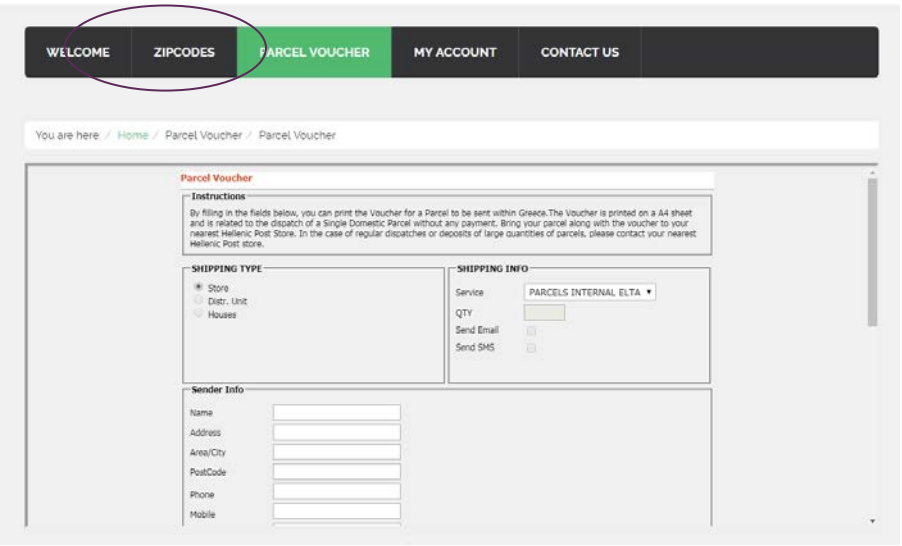

Figure 6-82. User fills-in the form

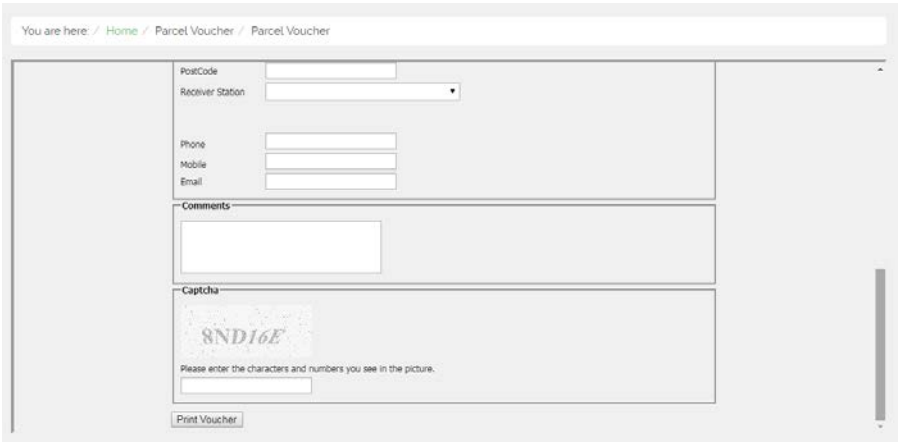

Figure 6-83. User clicks “Print Voucher”.

Step 6. System responds upon successful completion of the form and captcha with a .pdf file containing the parcel voucher. The user prints the voucher and attaches it to their parcel.

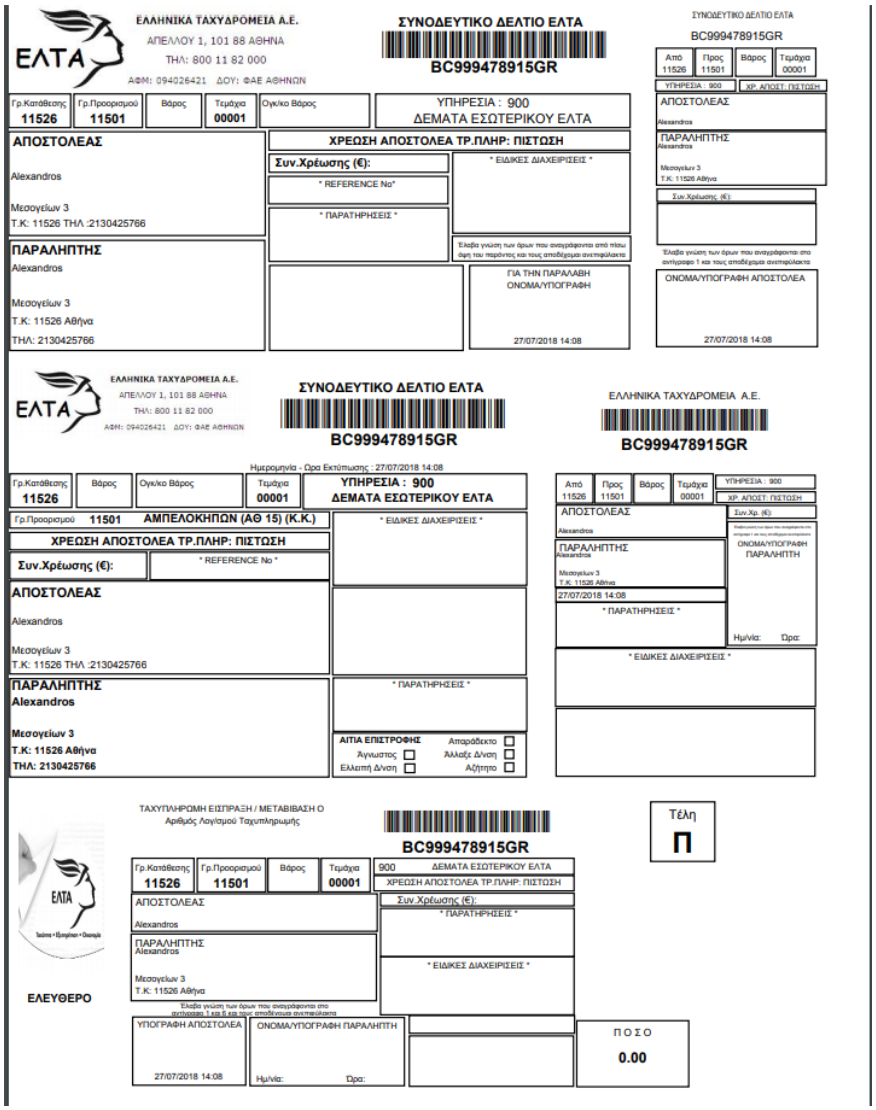

Figure 6-84. Printed Parcel Voucher

The test case with a Spanish User is similar to the test case described in page 92 (section 6.2.2.1 Test Case: User registration, Test with a Spanish User).

6.2.4 Online Zip Codes for Business Users

Service Start and End Events

ELTA Zipcodes Service	
Start Testing Event	http://www.eltab2b.gr/index.php?lang=en

End Testing Event	The order is completed and user receives a confirmation email

Test Cases

ELTA Zipcodes Service	
Test Case	User Registration Flow | A non-registered user registers with the ELTA eltab2b.gr website
Test Case	Registered User Accessing Service Flow | A registered user logs into and accesses the ELTA Zipcodes service

6.2.4.1 Test Case: User registration

Description	A non-registered user registers with eltab2b.gr and then access the ELTA Zipcodes service
Preconditions	The user is not authenticated and is not registered to eltab2b.gr
Process	1. User accesses the service via (http://www.eltab2b.gr/index.php?lang=en) 2. User selects Login with eIDAS 3. User is redirected to the page where he is informed that he can Identify with eIDAS eID. 4. User is authenticated via eIDAS 5. User is redirected to the eltab2b 6. User can use the Zipcodes service
Result	The user is registered to the service. User accesses the services.

Test with a Greek User

As this service is available through the eltab2b.gr website this test case is identical with the test case presented in section 6.2.3

Test with a Spanish User

As this service is available through the eltab2b.gr website this test case is identical with the test case presented in section 6.2.3

6.2.4.2 Test Case: (Registered) User login

Test with a Greek User

Description	A user tries to access the ELTA Zipcodes service
Preconditions	The user is registered to eltab2b.gr and has valid eIDAS credentials
Process	1. User accesses the service via (http://www.eltab2b.gr/index.php?lang=en) 2. User selects Login with eIDAS 3. User is redirected to the page where he is informed that he can Identify with eIDAS eID. 4. User is authenticated via eIDAS 5. User is redirected to the eltab2b 6. User selects the Zipcodes service 7. User completes the remaining fields of the order details 8. User proceeds with electronic payment 9. System responds with order confirmation
Result	The user receives order confirmation.

Step 1. The user accesses eltab2b URL.

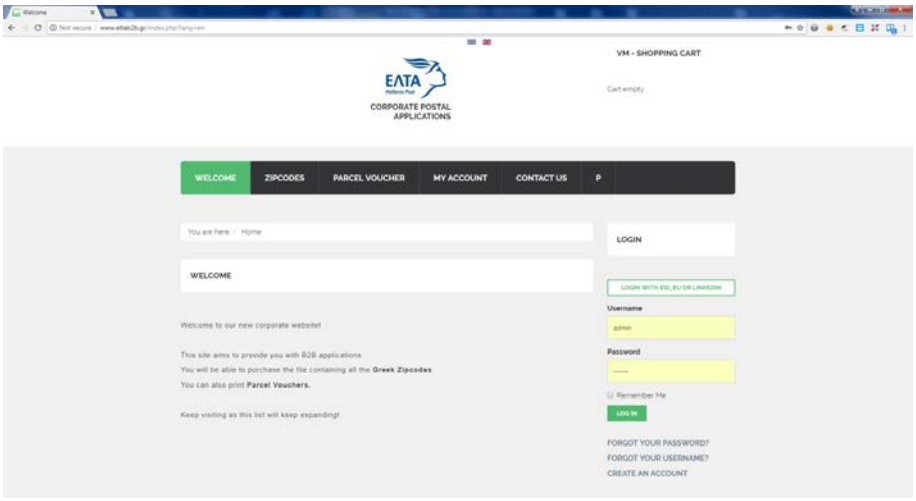

Figure 6-85. Service Home Page

Step 2. The user proceeds with the login, by clicking login with eID_EU.

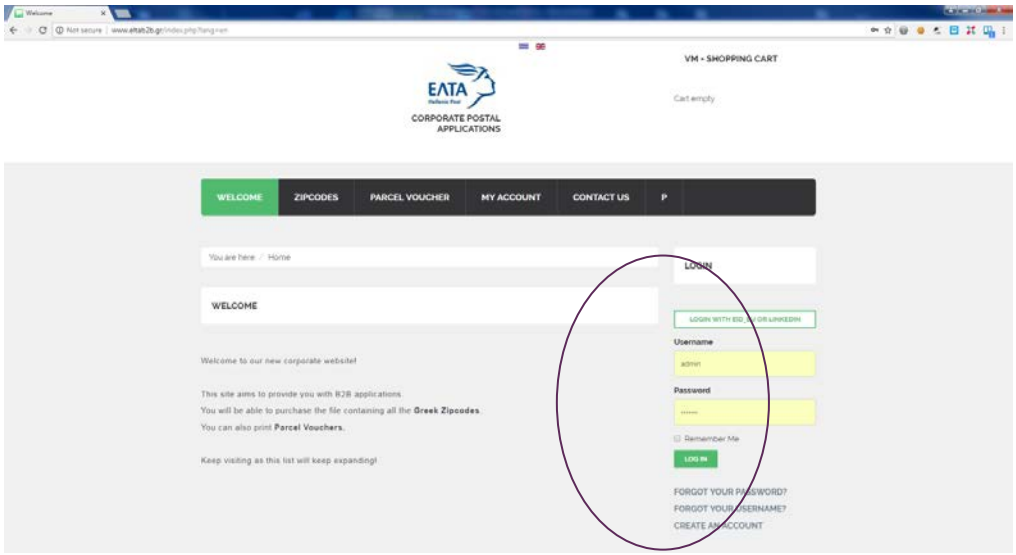

Figure 6-86. User selects eIDAS authentication

Step 3. User selects “Country of Origin” GREECE and clicks NEXT.

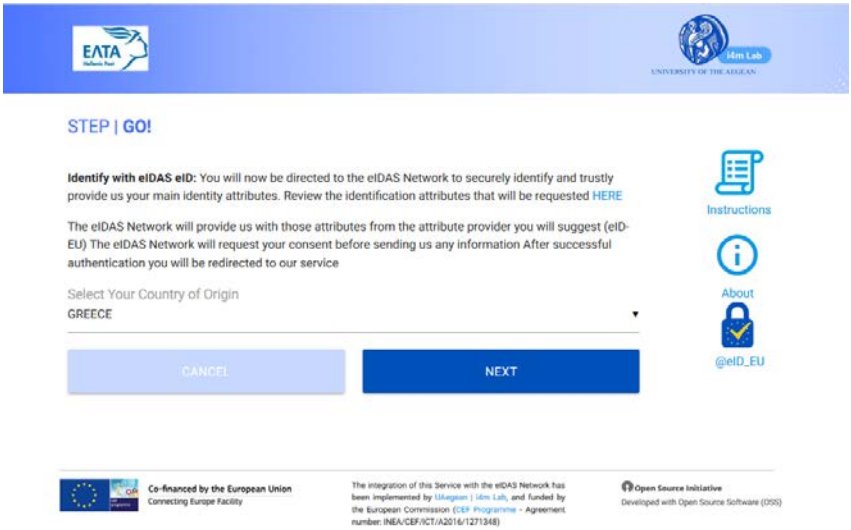

Figure 6-87. Country selection page

Step 4. User is redirected to the ERMIS IDP service where she authenticates with her credentials.

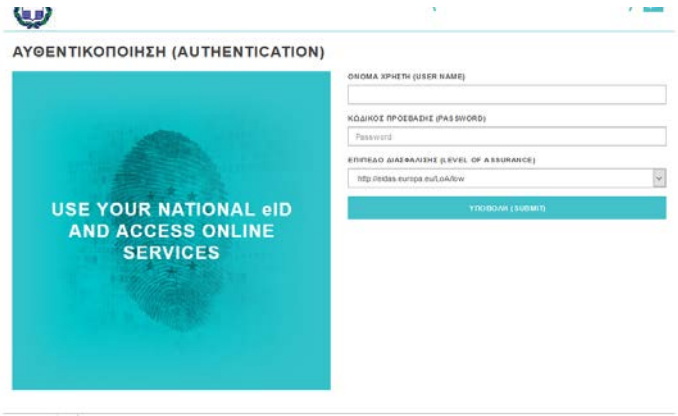

Figure 6-88. ERMIS IdP Page

Figure 6-89. Consent page

Step 4. User selects the Zipcodes service and adds a product to her basket.

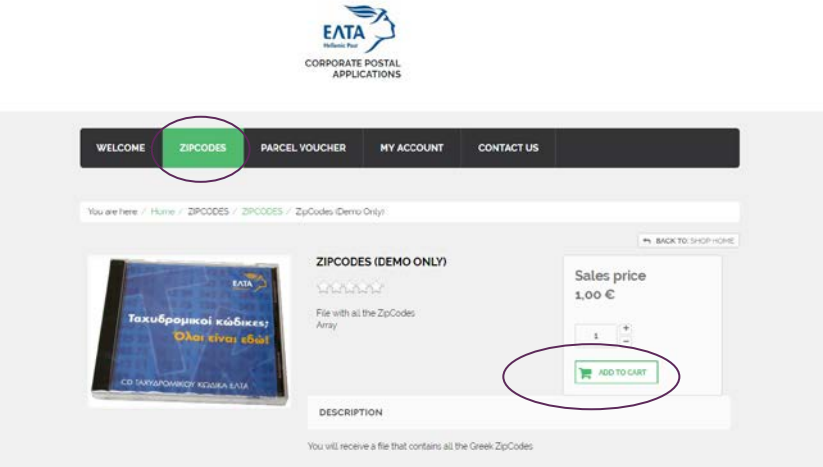

Figure 6-90. User adds products to her basket

Step 5. User completes the remaining fields of the order details form and clicks CHECK OUT NOW after having accepted the Terms and Conditions.

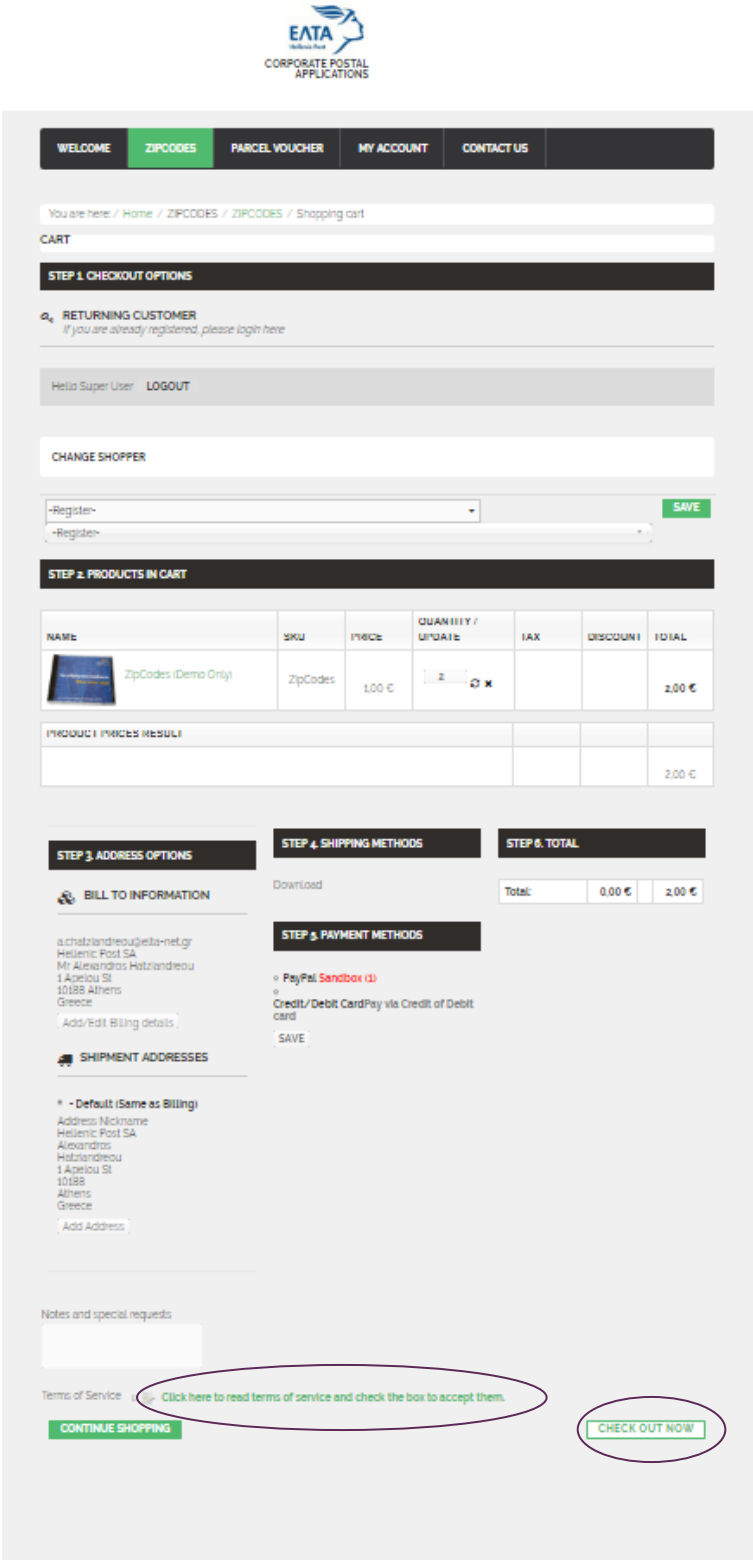

Figure 6-91. User complete order form and checks out

Step 6. After user click on CONFIRM PURCHASE they are being redirected to (depending on their choice of payment method) either Paypal or the Banking institutions clearance page.

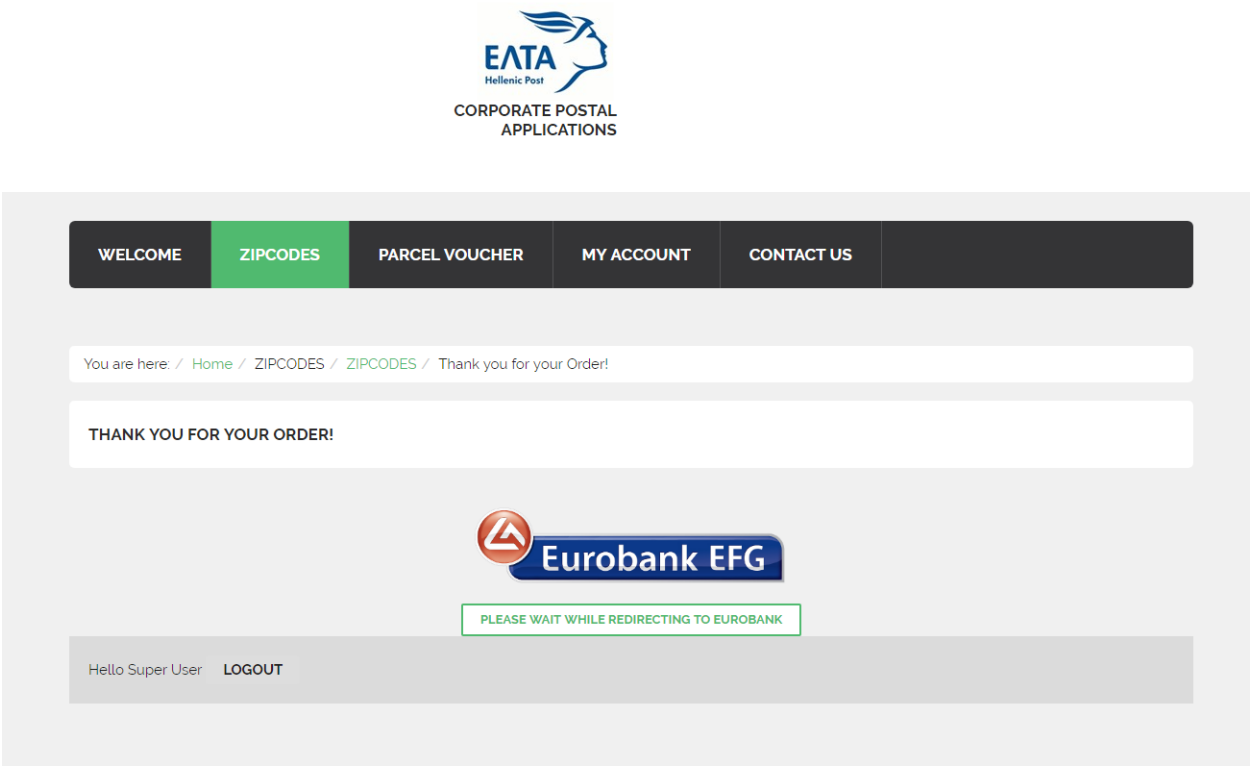

Figure 6-92. User successfully purchased the product

Step 7. System responds upon successful order with order confirmation. The order is completed and user receives a confirmation email.
The test case with a Spanish User is similar to the test case described in page 92 (section 6.2.2.1 Test Case: User registration, Test with a Spanish User).

7 Interoperability tests

The interoperability tests will be developed in Activity 6 “Testing of cross-border authentication and access to Correos electronic Services and to Hellenic (Financial and Post) electronic Services” and will be included in deliverable D6.1 (Milestone 10) of Activity 6. After an agreement concluded with the Greek public authority that is in charge of the Greek eIDAS Node (Hellenic Ministry of Administrative Reconstruction – HMAR), ATHEX and ELTA services will be tested against users in two ways:

- via the pre-production Greek eIDAS Node with Italy, Czech Republic and Estonia;
- via the production Greek eIDAS Node with Italy

8 Evaluation & Lessons learned

This section summarizes the main results of the tasks 4.3 and 5.3 “Integration to Greek PEPS/elDAS-Node Connector” and presents some lessons learnt. As already mentioned in Chapter 3, the integration of ATHEX and ELTA services with the eIDAS Networks has met the challenged and requirements that have been initially defined. Furthermore:

ATHEX

- ATHEX has successfully adopted and deployed eIDAS API Connectors provided by the University of the Aegean, with no major modifications.
- eIDAS API Connectors are Operating System independent and can be deployed in any network zone.
- The development effort that is required in order to create Service Points that implement a bridge between eIDAS API Connectors and SP own IT premises, is rather minimal and easily adapted to the needs of the application supporting the service that integrates with the eIDAS Network.

During the integration of ATHEX e-services with the Greek eIDAS Node, the following problems were discovered:

- It was very difficult to integrate the eIDAS API Connectors as docker containers.
- In order to achieve full
- WebApp Look’n’Feel homogenization with the service, ATHEX needwed to perform extended refactoring of the WebApp HTML templates. This was not a problem as WebApp is open sourced.

ELTA

- Production of software based on already existing/operating software is time-consuming process especially when it has to be implemented in “closed environments” that are characterized as “black boxes”.
- However, in services that have been re-designed to be integrated with the eIDAS Netwoek, there were not any significant problems reported in terms of implementation, connectivity or architectural design.
- During the implementation phase, there is frequently the need to work in close collaboration with third party IT providers and external to organization collaborators. This introduces an additional organizational cost in the integration with the eIDAS Network.

In the case of ELTA in particular, most services needed to be redesigned to a certain extent. The initial planning for the customization had to go through a number of amendments in order to be consistent with the extra work that emerged step after step. This caused delays and required more development and testing effort that is usually needed.

Finally, based on the gained experience so far, the following improvements for the future are suggested:

- Externalization of the ISS 2.0 configuration files, so that subsequent re-deploys, would not overwrite them.
- Externalization of the WebApps HTML templates, so that an SP can freely modify them without the need of rebuilding the executables.
- A successful dockerization of the components, would address both above issues.

9 Conclusions

The implementation of the integration of ATHEX and ELTA services with the Greek eIDAS Node has undertaken the following steps:

a) Service customization: service re-engineering to adapt to the requirements of an authentication through a "third part system", i.e. eIDAS Network. This phase encompasses the specific tasks of customization design, development and deployment.
b) Effective service integration with the eIDAS Network via the Greek eIDAS Node. Specific tasks related to this phase are: integration design, API for the interconnection of the application supporting a service with the eIDAS Node, UIs to support effective user navigation to eIDAS Network and back, insertion of the authentication data obtained from eIDAS into the back-end of the application/service.
c) Service integration verification: testing of the integration of SP services with the GR eIDAS Node.
d) Documentation and Training: creation of the necessary explications and guidelines for the needs of the technical team overseeing eIDAS Network integration support and service maintenance.

Eventually, the necessary effort and costs for service customization and new components development are underestimated in the phase initial design. The preparation of a service to be integrated with the eIDAS Network is not a trivial task; it requires a deep understanding of the related authentication and identity attributes transfer data flows. Further, it is very probable that the task of service customization will introduce the occasion for a broader service re-design that may ultimately lead to a major upgrade of service functionality. In the case of ELTA for example, this integration implicated an important re-design of the existing e-services (including UIs and flows) and collaboration with third-party providers to achieve this. As a result, major delays in the initial time-plan were presented.

As a conclusion, we report that ELTA and ATHEX services which are part of LEPS project have been successfully integrated with the eIDAS Network. They do now interoperate with the Greek eIDAS Node via LEPS eIDAS API Connectors and, therefore, can provide their functionality to both local and cross-border users, with cross-border users being able to automatically access them via their national eID credentials. After the detailed tests conducted in the context of the last project operation (Activity 7: "Testing of cross-border authentication and access to electronic Services"), and the necessary final adjustments and service business logic modifications, these services will be functional parts of the paneuropean eIDAS infrastructure. Finally, it is worth to notice that ATHEX Group and ELTA may further benefited from the interconnection infrastructure they have deployed in the context of LEPS project (relying on LEPS eIDAS API Connectors), to easily integrate with the eIDAS Network other services they may want to make available to cross-border customers, at a minimal technical and operational cost.

References

1. *LEPS D4.1/5.1: "Operational and Technical Documentation of SP customization".*

2. *LEPS Deliverable D3.1: "M5 & M9 – Mobile ID App and its integration results with the Industrial Partners".*