Leveraging eID in the Private Sector

D3.3 Operational and Technical Documentation of SP integration

Document Identification			
Status	Final	**Due Date**	30/06/2018
Version	0.10	**Submission Date**	31/07/2018

Related Activity	Activity 3	**Document Reference**	D3.3
Related Deliverable(s)	D2.1, D3.1, D3.2, D6.1	**Dissemination Level (*)**	PU
Lead Participant	Atos	**Lead Author**	Juan Carlos Pérez Baun
Contributors	Atos, Correos, UMU	**Reviewers**	Petros Kavasalis, UAEGEAN
			John Balafas, ATHEX

Keywords:
eIDAS, eID, CEF Building Block, SP Integration, Cross-Border Authentication, SAML 2.0

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
Juan Carlos Pérez Baún	Atos
Raquel Cortes Carreras	Atos
Nuria Ituarte Aranda	Atos
Elena Torroglosa Garcia	UMU
Adrian Fernandez Vega	Correos

Document History			
Version	Date	Change editors	Changes
0.1	24/05/2018	Atos	Initial draft version with ToC
0.2	15/06/2018	Atos	Guide lines on content for each section. Updates on Introduction and Methodology sections.
0.3	21/06/2018	Atos	Updates on following sections: Methodology, Requirements and Architecture.
0.3	22/06/2018	UMU	Updates on Mobile service section.
0.4	25/06/2018	Atos	Updates on eIDAS adapter components section,
0.5	18/07/2018	Atos	Updates on Introduction, eIDAS adapter components, lessons learnt sections and Annexes. Adjusting document's structure.
0.6	23/07/2018	Atos	Updates on Executive Summary, Requirements, eIDAS adapter Integration, Interoperability tests and Evaluation & lessons learnt sections,
0.6	23/07/2018	Correos	Updates on Integration with Correos Services Updates section.
0.7	24/07/2018	Atos	Updates on Interoperability tests, Evaluation & lessons learnt and Conclusion sections,
0.8	25/07/2018	Atos	Update on Conclusions section and final polishing.
0.9	25/07/2018	Atos	For review process
0.10	28/07/2018	Atos	Updates on Introduction section. Addressing Atos quality process. Addressing reviewers' comments.
1.0		Atos	FINAL VERSION TO BE SUBMITTED

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
API	Application Programming Interface
CEF	Connecting Europe Facility
EC	European Commission
Dx.y	Deliverable number y belonging to Activity x
eID	Electronic Identification
eIDAS	electronic IDentification, Authentication and trust Services
GDPR	General Data Protection Regulation
IDE	Integrated Development Environment
IdP	Identity Provider
JASON	JavaScript Object Notation
JWT	JASON Web Token
LEPS	Leveraging elD in the Private Sector
MVC	Model-View-Controller (Web Application Framework)
OS	Operating System
REST	REpresentational State Transfer
SAML	Security Assertion Mark-up Language
SP	Service Provider
UI	User Interface
URL	Uniform Resource Locator
UX	User eXperience

Executive Summary

This document describes the work performed in Activity 3 “Customization of Spanish Postal Services and Integration with eIDAS Infrastructure”. This activity aims at boosting the use of eID through the pan-European eIDAS network for cross-border identification and authentication. Namely, this document fits within the context of Task 3.3 “Integration to Spanish eIDAS node”, where the IT infrastructure supporting e-services from Correos are connected to eIDAS infrastructure.

The following tasks have been performed during the integration of the Correos’ services to the eIDAS network:

- Compile the requirements from the integration of the Correos’ services with the eIDAS adapter from D3.2 [10], and the derived requirements from the Spanish eIDAS node and the eIDAS infrastructure;
- Provide a rationale for the eIDAS adapter design and architecture. Describe the implementation of the eIDAS adapter to connect the Correos e-services with the Spanish eIDAS node;
- Provide details about the deployment of the eIDAS adapter;
- The authentication flow completed when a Greek citizen tries accessing to a protected Correos’ service;
- The steps performed, as well as the modifications and updates developed during the integration of Correos services with the eIDAS Network;
- The performed tests during the integration and the developed actions preparing the interoperability tests;
- Finally, a section describing the lessons learnt along the integration process and some hints for developers and integrators, is also provided.

The main achieved results within the course of this task are firstly the creation of an eIDAS adapter based on an integration package provided by the Spanish Ministry for integrating e-services from the private sector with the Spanish eIDAS node in a pre-production environment. Secondly, the validation of the ability of this adapter for allowing EU citizens to authenticate cross-border, and access these online services. Initially the process has been tested with Greek citizens accessing Spanish e-services, and then it will be tested with citizens from other EU countries connected to the eIDAS network.

These results will be compared with those obtained from the counterpart tasks developed in Activity 4 “Customization of Greek Financial Services and Integration with eIDAS Infrastructure” and Activity 5 “Customization of Greek Post Electronic Services and Integration with eIDAS Infrastructure”, which integrates Greek online services (ATHEX and ELTA services respectively) with the Greek eIDAS node through different integration approaches than the Spanish side.

This comparison will be valuable to the rest of EU member states and SPs for deciding the up taking of the option which fits best to their needs. This will allow the different stakeholders to reduce time and effort for the integration with the eIDAS network.

1 Introduction

After entering into force eIDAS regulation [11] in September 2014, from 29 September 2018, the EU public organizations offering e-services to citizens are obliged to recognize notified eID schemes from all EU member states. Then, the next challenge for the businesses offering digital services is the uptake of using trusted eIDs issued by EU governments for enrolment, and for secure electronic transactions.

The European Commission in the context of the Digital Single Market strategy is trying to improve the access for citizens and businesses to online services in a secure way [17]. Based on the eID and eSignature building blocks delivered by CEF [5] and the eIDAS regulation [11], the EC launched the CEF Telecom call on eIdentification (eID) & eSignature[1] where LEPS project has been granted by CEF[2] .

The planned actions agreed under the Grant Agreement Consortium to be developed within this task T3.3, aimed to integrate the Spanish eIDAS node generating eIDAS authentication request containing both mandatory and optional attributes. Then the eIDAS authentication response obtained after the cross-border user authentication will be integrated into the authorization process of Correos portal for taking authorizations decisions founded on features such as the LoA required for the attributes.

To carry out these planned actions the following tasks have been developed, and described in this document, starting with the compilation of the requirements affecting the development of the eIDAS adapter. These requirements will be grouped in two categories, Technical and operational requirements and Legal requirements. Based on these requirements the eIDAS adapter will be implemented based on a modular design leveraging the SP integration package provided by the Spanish Ministry. Once deployed on Atos premises the integration with the Spanish eIDAS node will be tested for user cross-border authentication. Finally, the evaluation of the developed processes will be performed against the initial gathered requirements.

1.1 Purpose of the document

The purpose of this document is to provide a complete description of actions developed during the task 3.3 “Integration to Spanish eIDAS node” in the context of Activity 3 “Customization of Spanish Postal Services and Integration with eID Infrastructure”. This document is related to milestone 4 “Integration to Spanish PEPS/eIDAS-Node connector (production)”.

1.2 Relation to other project work

The architectural design activities described in this document are based on those developed in task 2.1 “Project Operations and Architecture Design” from Activity 2 (included in D2.1 “Business and

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

[2] The LEPS project has received funding from the European Union's Connecting Europe Facility under grant agreement No INEA/OEF/ICT/A2016/1271348

Technical Design for the Effective Use of eID DSI Report", due on month 15/Milestone 2 at the end of the project) and task 5.1 "Customization of Hellenic Post Services Portal" in activity 5.

Moreover, the implementation and integration activities continuing these activities performed on task 3.2 (described in D3.2 "Operational and Technical Documentation of Correos Services Customization", already submitted on Month 6/Milestone 3), implementing and integrating the eIDAS Adapter to the eIDAS network.

In parallel with the reported activities in this document, is developed the implementation of a mobile app in the context of task 3.1 "Mobile Authentication" (to be described in D3.1 "Mobile ID App Final Version"), which will be used for authenticates Spanish citizens using NFC eID through the mobile.

Finally, the components and infrastructure developed in the context of this task will serve for developing Activity 6 "Testing of cross-border authentication and access to Correos electronic Services and to Hellenic (Financial and Post) electronic Services".

1.3 Structure of the document

This document is structured in eight major chapters

Chapter 2 presents the methodology followed for developing the eIDAS adapter, based on previous developments, standards and protocols.

Chapter 3 describes the requirements derived from the eIDAS network, the specific Spanish eIDAS node and the derived from the eIDAS regulation. The requirements compiled in D3.2 from Service Provider integration have also been considered.

Chapter 4 presents the eIDAS Adapter architecture and their main features.

Chapter 5 provides a detailed description on the eIDAS Adapter components, the associated functionalities and the involved technologies. Also, the complete user authentication flow is described.

Chapter 6 describes how the eIDAS Adapter has been integrated with the eIDAS network through the Spanish eIDAS node, and the updates on the eIDAS Adapter required during this process. A description of the performed tests during the integration process, is also included.

Chapter 7 provides the interoperability operations with third countries, to be developed during the test execution tasks.

Chapter 8 finally, compiles the results of the activities developed, the lessons learnt during the implementation task and the evaluation of the process.

2 “Methodology”

Based on previous European projects such as STORK 1.0 [1] and STORK 2.0 [2] an eID infrastructure was created across Europe. This work continued by the eSENS project [3], and the collaboration with Connecting Europe Facility (CEF) Digital [4] have allowed the creation of different building blocks (also known as Digital Service Infrastructures (DSI)) providing a European digital ecosystem for cross-border interoperability and interconnection of citizens and services between European countries.

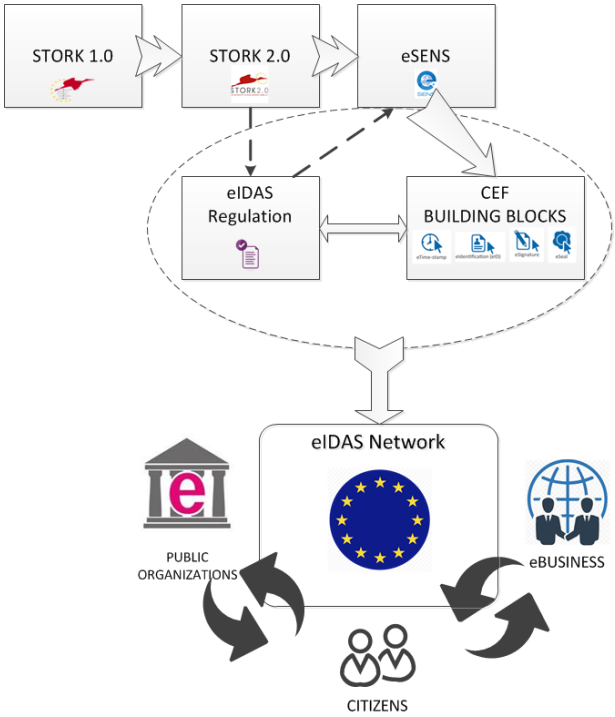

Figure 1: eIDAS Background

These building blocks [5] eDelivery, eInvoicing, eID, eSignature and eTranslation, are generic and reusable components, which offering functionalities easing the use of cross-border online services not only on public sector, but also on private sector (see Figure 1).

The eIDAS network is created leveraging the delivery of the CEF building blocks, mainly eID, and taking into consideration the eIDAS regulation [6] (entered into force on 17 September 2014), with the aim to boost the use of eID for accessing cross-border digital services in Europe. This technical infrastructure is connecting the national eID schemes facilitating to European citizens the use of eIDs, in a secure way, when accessing online services from different European countries. The eIDAS infrastructure is made by the different connected country eIDAS nodes [7].

In the case of Spanish services provided by Correos, the integration with the eIDAS infrastructure has a twofold utility:

- A user strong authentication for accessing the Correos services;
- Leveraging the trusted eIDAS infrastructure and the Spanish eID scheme for user registration purposes.

In both cases an element which will be able to provide a direct connection with the eIDAS network has been envisaged, and called eIDAS Adapter. As can be seen in Figure 2 this adapter acts as a hub or proxy service between the SP and the Spanish eIDAS node.

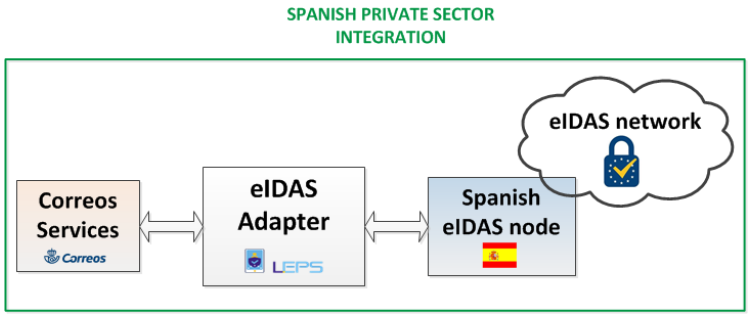

Figure 2: eIDAS Adapter Integration

Following the approach of reusing the building blocks provided by CEF, the Spanish Ministry has created an integration package based on the integration package delivered by the EC [9].

This integration package follows the eIDAS technical specifications, including signing, encryption and the SAML 2.0 standard. Also, the use of federated identity allows the adapter do not store none of the user authentication data, providing a SSOs system.

This integration package is provided in three flavours covering different technologies the SPs can support:

- Java
- PHP
- ASP.NET

Based on the Java package the eIDAS Adapter is created adapting the already existing services, improving the existing ones and adding new functionalities, technologies, protocols and standards, covering the integration needs of the SPs, not only those related with the services provided by Correos, but also preparing the adapter for future integration of SPs which need different interfaces and use different technologies. There has been also took into consideration how to facilitate the deployment on different environments.

Figure 3 shows the process followed for creating the eIDAS Adapter. A more detailed information on technologies, protocols, standards and functionalities included are provided in oncoming sections.

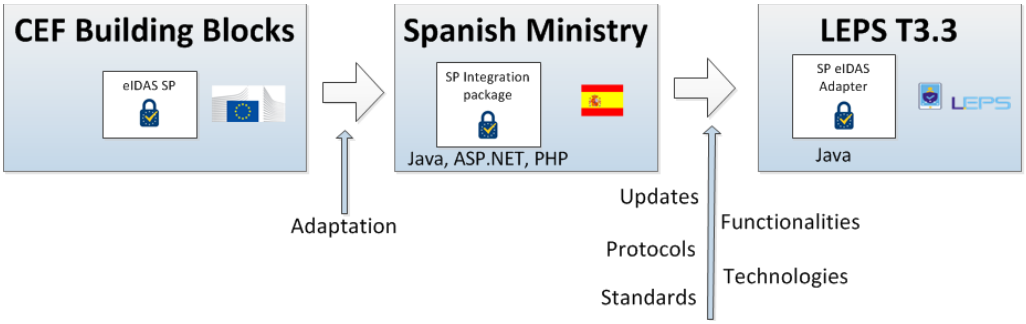

Figure 3: eIDAS Adapter Development Strategy

3 "Requirements"

This section provides the requirements derived not only from the eIDAS network operation, but also from the specific Spanish eIDAS node operation and, additionally, those determined by the eIDAS regulation. Beside these new applying requirements, the already determined requirements from D3.2 (described in section 2.5) [10], are also considered.

3.1 Technical and Operational Requirements

The eIDAS network is based on a circle of trust, where the European countries are connecting each other, allowing European citizens accessing online services using the eID schemes established in each country. The eIDAS infrastructure has established secure channels of communication encrypting messages and using secure protocols.

Table 1 describes the technical requirements derived from the eIDAS network applying to eIDAS Adapter development.

Table 1: eIDAS Network Requirements

Id	Name	Description
EINER-1	Interoperability	The Spanish eIDAS node **MUST** be able to connect with the Greek counterpart (or any other country in eIDAS with which interoperability must be fulfilled), for providing cross-border authentication.
EINER-2	Integration	The eIDAS adapter **MUST** be able to connect with the Spanish eIDAS node and manage the SAML request and SAML response the eIDAS network accepts and provides, respectively.
EINER-3	Secure data exchange	The eIDAS adapter **MUST** establishes secure communication between the SP and the eIDAS network, encrypting messages using secure protocols: TLS or SSH in the latest version available.
EINER-4	Integrity	User data provided by the eIDAS network **MUST NOT** be altered in any sense by the eIDAS adapter. The eIDAS adapter **MUST** play a role as a data intermediary.

The Spanish Ministry ("Ministerio de Hacienda y Función Pública") in charge of managing and maintenance of the Spanish eIDAS node provides different access to this node for public and private organizations:

- For public administrations[3], the access is made through the called Cl@ve gateway[4],

[3] https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2018/Marzo/Noticia-CTT-2018-03-20-Finalizado-proyecto-europeo-conexion-servicios-publicos-nodo-eIDAS.html#.WydyLIq-nIU

[4] https://trustindigitallife.eu/wp-content/uploads/2016/06/gomez-munoz-f.pdf

- In the case of private sector, a direct access is enabled to the Spanish eIDAS node for the SPs.

The protocols followed in both cases are similar and based on SAML 2.0 [8]. It means that switching from one to the other will be just a configuration matter.

The SP, or the eIDAS Adapter acting in behalf of the SP, will create a well-formed eIDAS SAML Request.

The SP/eIDAS Adapter should be registered in the Spanish eIDAS node system in advance, in order to be considered as trusted party.

The SAML responses provided by the eIDAS network are signed and must be validated by the eIDAS Adapter. Moreover, the assertions containing the user information are ciphered. This is a ciphering additional to the ciphering provided by SSL/TLS communication channel.

In addition, the Spanish eIDAS node verifies the integrity and authenticity of the SAML messages provided by the rest of the eIDAS nodes: the eIDAS Adapter takes this accordingly into account.

Table 2 describes the technical requirements derived from the Spanish eIDAS node applying to eIDAS Adapter.

Table 2: Spanish eIDAS Node Requirements

Id	Name	Description
EINOR-1	SAML Protocol	The eIDAS Adapter **MUST** follow SAML2.0 protocol as the rest of the eIDAS network does**.**
EINOR-2	Connection	eIDAS Adapter **MUST** connect directly to the Spanish eIDAS node.
EINOR-3	SP Metadata	The eIDAS Adapter **MUST** offer a service providing the SP metadata for validation.
EINOR-4	Trust	The SP and the eIDAS Adapter **MUST** be registered in advance on Spanish eIDAS system.
EINOR-5	Signing Request	The eIDAS Adapter **MUST** signs the authentication request to the Spanish eIDAS node.
EINOR-6	Signed Response	The signed SAML response provided by the Spanish eIDAS node **MUST** be validated by the eIDAS Adapter. If the SAML assertion is signed it **MUST** be also validated.
EINOR-7	Cipher	The ciphered SAML assertions, containing user personal data, provided by the Spanish eIDAS node **MUST** be deciphered.
EINOR-8	Integrity and authenticity	The eIDAS Adapter **MUST** verify the integrity and the authenticity of the SAML messages before processing the SAML response provided by the eIDAS node.
EINOR-9	Ports	The eIDAS Adapter **MUST** use standard ports (http 80 or https 443) for connecting to Spanish eIDAS node.

Apart from the requirements compiled in D3.2 [10] (included in "Annex 1: SP Requirements", with the aim to provide all the requirement in the same document), new requirements, compiled in the Table 3, have been derived from the integration of the SP with the eIDAS network.

Table 3: SP New Requirements

Id	Name	Description
SPR-4	Mapping	The eIDAS Adapter **MUST** provide a mapping between the SP and the eIDAS network for the attributes required by the SP in order to maintain end-to-end interoperability.

3.2 Legal Requirements

The eIDAS Adapter development must be accomplished with the legal requirements according to the eIDAS regulation [6] and the General Data Protection Regulation (GDPR) [11] approved by the EU Parliament on 14 April 2016, with enforcement date on 25 May 2018, Table 4 describes the legal requirements derived from these regulations applying to eIDAS Adapter.

Table 4: Legal Requirements

Id	Name	Description
LR-1	Data Minimization	The SP or the eIDAS Adapter **MUST** request the minimal data set, needed by the SP for authentication purposes.
LR-2	User Consent	The SP or the eIDAS Adapter **MUST** inform the user about the requested data, and **MUST** ask the user consent for data disclosure.
LR-3	Data Protection	The eIDAS Adapter **MUST** provide to the user information about the use of her data, and **MUST** provide information on how to exercise her rights

4 “eIDAS Adapter Architecture”

During the architectural design of eIDAS Adapter different aspects have been taken into consideration as follows:

- The technical and legal requirements described in section 3;
- The architectural design features inherited from the integration package the Spanish Ministry provided;
- The SP requirements and scenarios for user authentication, described in D3.2 [10].

Therefore, the main objective is developing a single component which will integrate the SP with the Spanish eIDAS node, fulfilling the following features:

- Simple;
- Reusable;
- SP infrastructure independent;
- SP client programming language independent;
- Able to connect with different SP services in the same or from different domains.

With this aim an eIDAS Adapter component has been designed, providing two main interfaces:

- SP interface
- eIDAS interface

Figure 4 displays a high-level overview of the eIDAS Adapter, and the interactions (thanks to the provided interfaces) with both, the SP domain (e.g. Correos services) and with the IdP domain through the eIDAS network. In the case of LEPS project, the adapter will redirect the user to the proper IdP:

- The Spanish police for Spanish citizens;
- The Ermis IdP (Greek governmental IdP) or to ATHEX IdP (Greek private IdP).

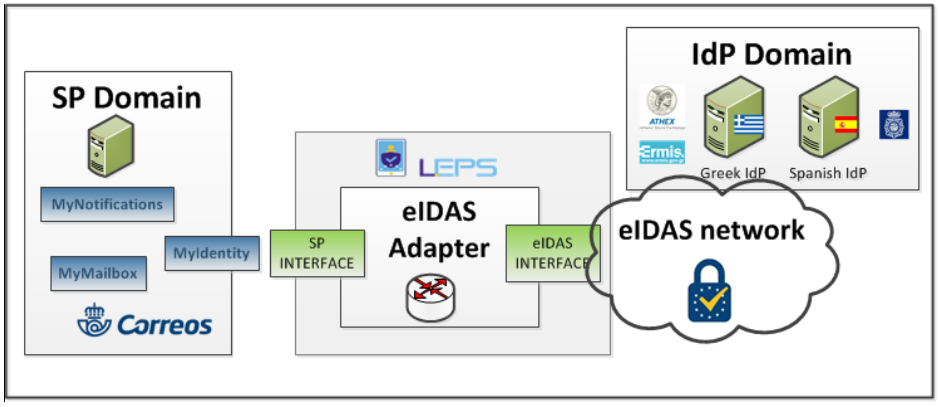

Figure 4: eIDAS Adapter Architecture General Overview

With the aim to accomplish with the aforementioned requirements, considerations and features, the eIDAS Adapter has been developed containing the following components:

- **SP interface**: Establishes interaction with the integrated services. Contains a single endpoint which receives the authentication request from the SP;

- **eIDAS interface**: Connects to the country eIDAS node, Comprises two endpoints:
  - Metadadata endpoint: Provides SP metadata;
  - ReturnPage endpoint: Receives the SAML response from the country eIDAS node.
- **UI module**: Interacts with the end user;
- **Manager service**: Orchestrate the authentication process inside the eIDAS Adapter;
- **Translator service**: Translates in both ways from the SP to eIDAS node:
  - The authentication request from the SP to a SAML request;
  - The SAML response from eIDAS node to an authentication response to SP;
- **Mapping service**: Maps the SP attribute names to SAML eIDAS attribute names, doing the semantic translation;
- **SAML Engine**: Manages the SAML request and response, encrypting/decrypting and signing.
- **Metadata service**: Creates SP metadata;
- **Mobile service**: Optional component able to detect the device where the authentication process is performed.

Figure 5 depicts the eIDAS Adapter components.

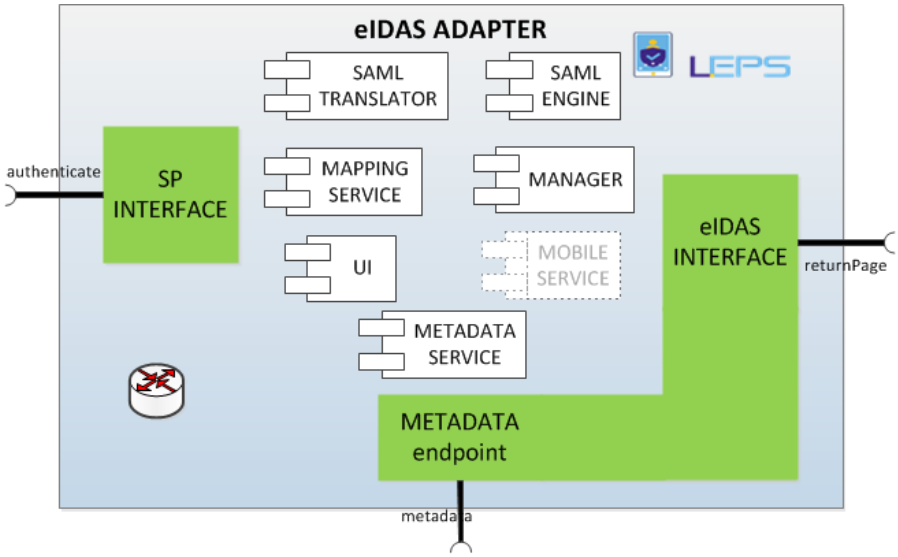

Figure 5: eIDAS Adapter Components

A complete description on these components and its functionalities is provided on following sections.

5 “eIDAS Adapter Components”

This section presents a detailed description of each eIDAS Adapter components, the functionalities provided, the technologies used during the implementation, deployment and testing phases and the complete authentication process involving the eIDAS adapter components. Finally, a description on how to deploy and configure the adapter, and some guide lines for developers for the integration, are also included.

5.1 Components and Functionalities

The eIDAS Adapter comprises the following components as indicated in section 4 and displayed in Figure 5. Next are provided the functionalities and futures offered by the main components.

5.1.1 Interfaces

The eIDAS Adapter offers interfaces based on servlets in two folds, as Figure 6 shows:

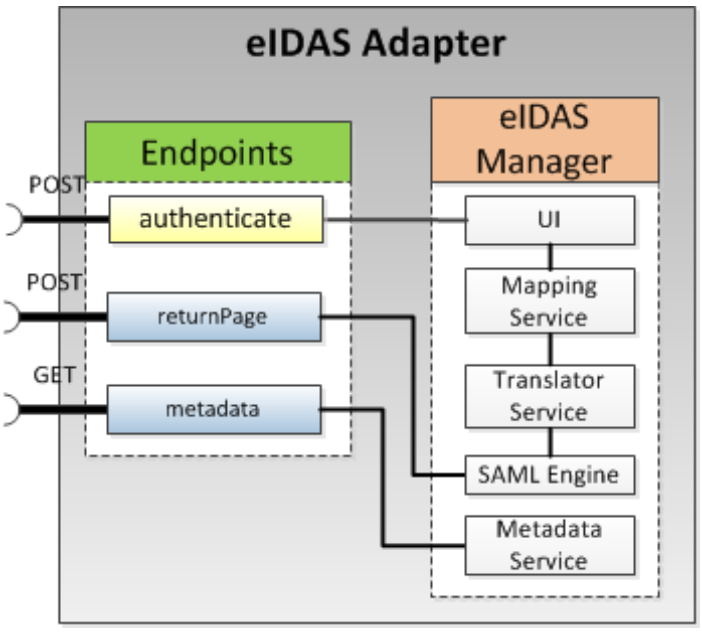

Figure 6: eIDAS Adapter Enpoints

- **To the SP**: A unique endpoint is offered to the SP for starting the authentication process:

  POST /authenticate {“token”: String}

  This endpoint allows an easy SP integration of the SP to trigger the authentication process providing a signed JASON Web Token (JWT), which includes information about the SP, the attributes the SP needs for user authentication. As this is an Asynchronous process the JWT also provides and the call back URL where the user data must be provided at the end of the authentication process (detailed information on the endpoint and triggering process is included in D3.2 “Operational and Technical Documentation of Correos services customization” [10]).

- **To the eIDAS network:** 2 endpoints are provided:
  - Metadata: Public endpoint where the eIDAS node can retrieve the metadata from the SP.

    GET /metadata

    The SP metadata are provided in a xml file including the public certificate, which will be validated against the trusted services registered in the Spanish eIDAS node system.
  - ReturnPage: Endpoint for receiving the SAML response the Spanish eIDAS node sends:

    POST /ReturnPage

    This servlet receives an asynchronous SAML response, which must be validated and deciphered.

5.1.2 User Interface

The User Interface (UI) is a single jsp provided by the eIDAS Adapter, which shows to the user the following information:

- List of requested attributes, both mandatory and optional, the SP needs for authentication purposes;
- Country selector: where the citizen selects her origin country;
- Button Submit for sending the authentication request to the Spanish eIDAS node. A Cancel button is also included.
- Links to privacy info on Correos as a SP and LEPS project.

A screenshot of the displayed screen is shown in Figure 7.

Figure 7: eIDAS Adapter UI

5.1.3 Manager service

This component plays a main role orchestrating the complete authentication process inside the eIDAS Adapter. Basically, once the authentication request reaches the eIDAS Adapter, the received JWT is processed, and the following actions will be performed by this component:

1- Validates the JWT (see document for validation: signed, time, issuer, etc.)

2- Extracts information for creating the SAML request, leveraging the Translator and the Mapping services;
3- Creates the SAML request using the SAML Engine service;
4- Sends the SAML request to the Spanish eIDAS node;
5- Receives the SAML response from the Spanish eIDAS node;
6- Validates the SAML response using the SAML Engine;
7- Creates the authentication response with the JWT format, using the Translator and the Mapping services;
8- Sends the authentication response to the SP.

Sequence diagram in Figure 8 depicts the described process.

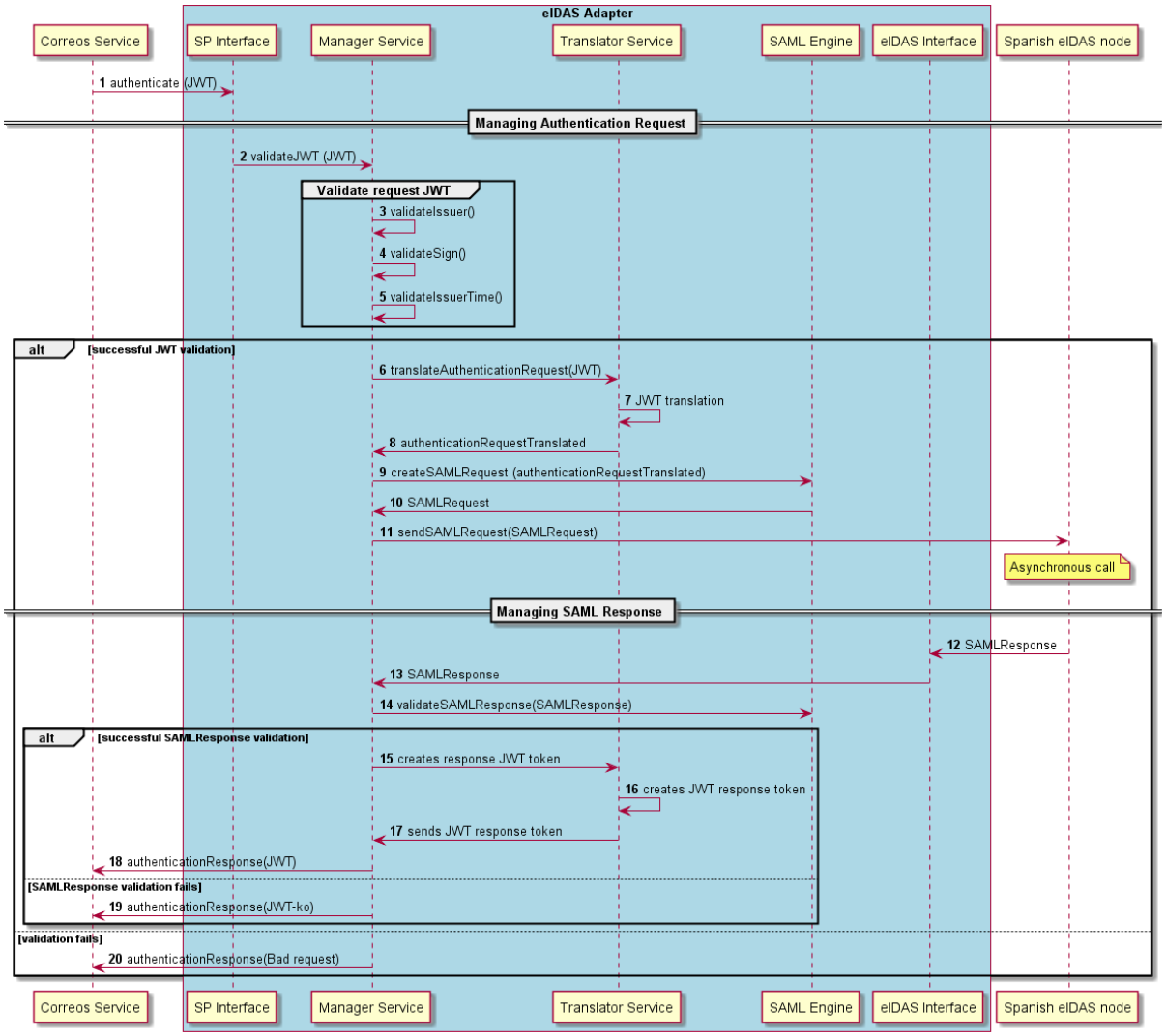

Figure 8: Manager Module Flow

The steps indicated in Figure 8 are described next:

1- The Correos service sends an authentication request containing the JWT request token;
2- The SP Interface calls the Manager module for validating the received JWT;

3-5 The issuer, the issuer time and the signed JWT are validated;

If the JWT validation is successful:

6. The Manager module asks the Translator service to translate information contained in the JWT to understandable eIDAS information;
7. The Translator service translate the provided JWT;
8. The Translator service provides the translated authentication request;
9. The Manager module asks the SAML Engine module to create the SAML Request using the translated request;
10. The SAML Request is provided by the SAML Engine;
11. The Manager module sends the SAML Request to the Spanish eIDAS node;
12. As the eIDAS authentication is an asynchronous process, after the user authentication the eIDAS node provides a SAML Response to the eIDAS Interface;
13. The SAML Response reaches the Manager module;
14. The Manager module validates the SAML Response against the SAML Engine;

If the validation is successful:

15. The Manager module asks the Translator module for creating a JWT response token;
16. The Translator service creates the response JWT;
17. The Translator service provides the response JWT to the Manager module;
18. The Manager module sends the authentication response to the Correos service;

Otherwise:

19. An authentication response is provided to the Correos service including a signed JWT with a KO message;
20. An authentication response including Bad request message is provided to the Correos service.

5.1.4 Translator service

The Translator service plays a key role during the user authentication process easing the integration of the SP with the eIDAS network. This component executes two main tasks:

1- Translates the authentication request, sent by the SP, to a SAML request the eIDAS network understands. For providing the information to create the SAML request the following actions must be performed by the Translator service:

- Extracting information from the JWT request token, needed for creating the SAML request. The following information included in the JWT will be sent to the Spanish eIDAS node:
  - The attributes needed by the SP, the Mapping service described in previous section 5.1.3 helps with this process;
  - The level of assurance the SP needs regarding the attributes;
- Retrieving the following information from the JWT request token, to be used for sending the JWT response token to the SP:
  - The URL where the user must be redirected after the authentication process and the JWT response token should be returned;

- Authentication request identifier. for the authentication request from the SP to a SAML request;
- Information needed for validating the JWT request token validation and entries to be returned with the JWT response token for security reasons;

2- Translates the SAML response, sent by the Spanish eIDAS node, to an authentication response to be sent to the SP. To create the JWT included into the authentication response the Translator service execute the next actions:

- Extracts user data from the SAML eIDAS response, using the SAML Engine;
- Maps the attributes from eIDAS format to SP format using the Mapping service;
- Fills the JWT response token with the user data;
- Includes the security entries retrieved from the JWT request token into the JWT response token;
- Signs the JWT response token;

Sequence diagram in Figure 9 depicts the described process.

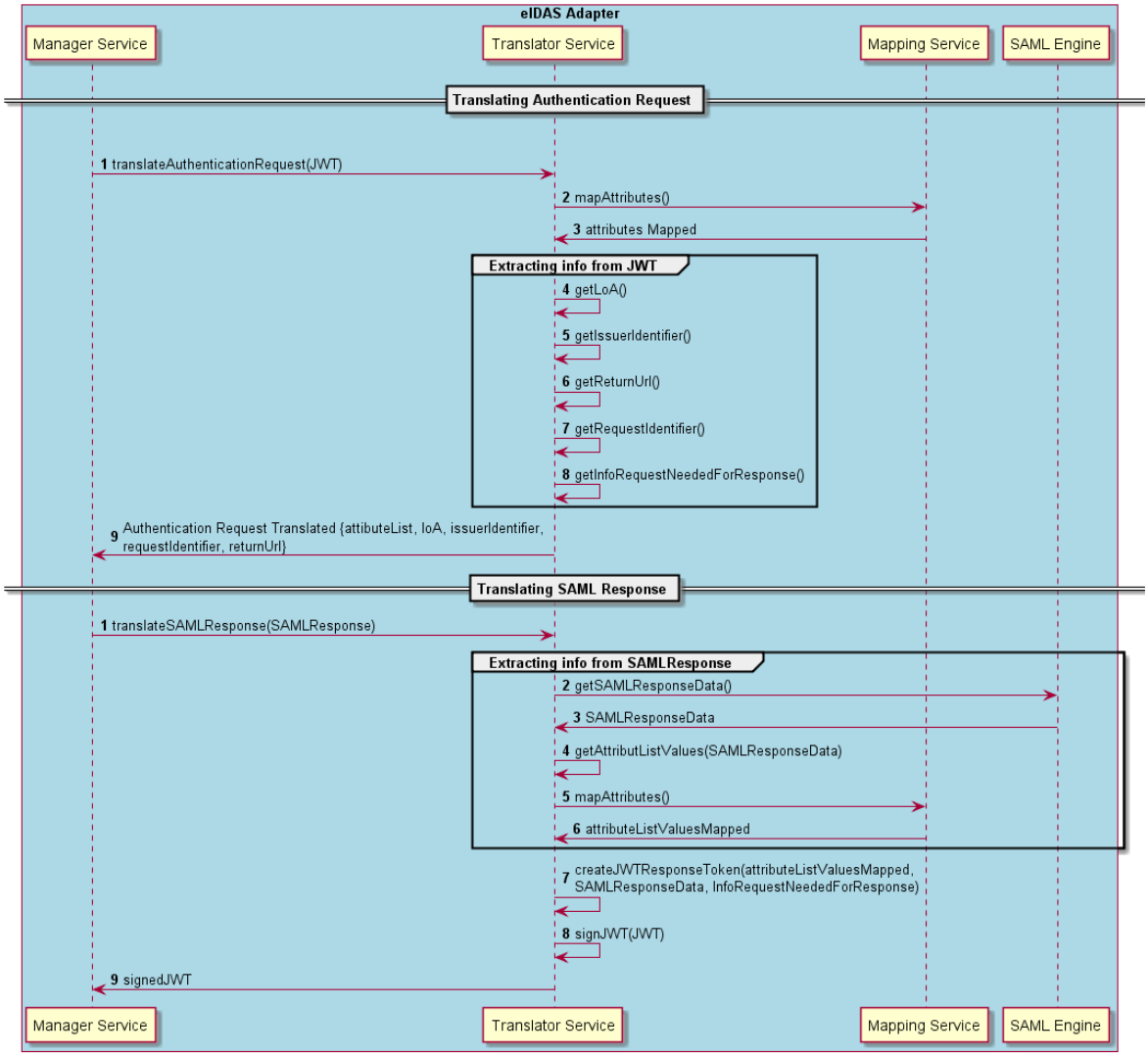

Figure 9: Translator Service Flow

The two tasks developed by the Translator service displayed in Figure 9 are described next:

A. Translating the authentication request:
   1- The Manager service sends the JWT to the Translator service for retrieving authentication request information;
   2- The Translator service maps the SP attribute names using the Mapping service;
   3- The Mapping service provides the eIDAS attribute names requested;

   4-8 The Translator service obtain the LoA, the Issuer Identifier, the Return URL, the Request Identifier and the information needed to create the authentication response later;

   9- The Translator service provides the authentication request translated to the Manager service.

B. Translating the SAML response:
   1- The Manager service sends the SAML Response to the Translator service for retrieving authentication response information from the SAML Response;
   2- The Translator service uses the SAML Engine for retrieving the user data contained in the SAML Response;
   3- SAML Engine provides the user data;
   4- The Translator service gets the user attribute values;
   5- The Translator service maps the eIDAS attribute names using the Mapping service;
   6- The Mapping service provides the SP attribute names requested;
   7- The Translator service creates the JWT response token with the previously retrieved information, which includes the user attribute values and the info required for response retrieved during the authentication request translation task (A);
   8- The Translator service signs the JWT response token;
   9- The Translator service sends the signed JWT response token to the Manager service.

5.1.5 Mapping service

The Mapping service has as main objective get interoperability between the different SPs and the Spanish eIDAS node. For achieving this objective, it will be necessary to harmonize the attribute name formats. Therefore, the mapping service provides a semantic mapping of user attributes defined in both domains: Correos SP and eIDAS network.

The authentication request is based on a JWT token generated by the SP. This JWT contains the list of attributes the SP needs for authenticate the user. With the aim to ease the mapping process the JWT contains a parameter called *scope* where is defined the attributes to be requested.

The scope entry accepts two different values:

"scope":"profile"

"scope":"address"

The scope values can be merged separated by a space:

"scope":"profile address"

In this manner a direct mapping between the SP attribute names and eIDAS attribute names, which would be more complex to implement and maintain is avoided.

Table 5 shows the mapping defined for the scope entry.

Table 5: Mapping attributes

Scope	SP Attribute Name	Description	eIDAS Attribute FriendlyName
profile	user_identifier	Unique user identifier	PersonIdentifier
	given_name	Name	FirstName
	family_name	Surname	FamilyName
	birthdate	Date of birth	DateOfBirth
	gender	Gender	Gender
address	address	Current address	CurrentAddress

In the future new scopes could be added for additional data set.

The scope values have been included in a configuration file allowing the attribute mapping works in a friendly way.

The mapping between scopes and eIDAS user attributes is stored in a configuration file and can thus be customized for choice. The Mapping service ensures that the user attributes that are mapped to the requested scopes as part of the JWT token returned to the SP.

5.1.6 SAML Engine

SAML Engine is a Java library eidas-saml-engine-1.4.0.jar provided by CEF[5] responsible for managing the SAML request and SAML response, providing the following functionalities:

- Create the SAML request;
- Validate the SAML response;
- Generate the SP metadata;
- Participate in the encrypting and decrypting of SAML request and response;
- Participate on signing SAML request.

5.1.7 Metadata service

The Metadata service is a servlet where the SP metadata are publicly published, and the involved stakeholders (e.g. Spanish eIDAS node or the Spanish IdP) can access for establishing a trust relationship between them. These metadata include:

- SP identifier
- Certificates
- Cryptographic details
- Security and privacy policies

[5] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+-+All+releases

A signed xml file is created leveraging the functionalities provided by the SAML Engine, and following the OASIS standard for metadata[6]. An example of xml file with SP metadata is included in Annex 2: sp-metadata.xml.

5.1.8 Mobile service

This Mobile service is an optional service, envisaged to facilitate the user experience detecting the device where the authentication process is performed, when the citizen is using a mobile device for accessing the services offered by the SPs.

This functionality is not implemented yet, but planned to be included in the future.

Information on the Mobile app design and implementation is provided in D3.1 “Mobile ID App” [13].

5.2 Authentication flow

This section provides a description of the Correos service login authentication integrated with the eIDAS infrastructure. The main components involved in this process are playing the following role:

- **Correos service**: Triggering the authentication process;
- **The eIDAS Adapter**: Linking the initial authentication request with the eIDAS network;
- **eIDAS network**: Connecting each country eIDAS node developed by the EU member state.
- **The IdP**: Performing the user authentication.

Figure 10 displays the sequence of screens the system is showing to the user.

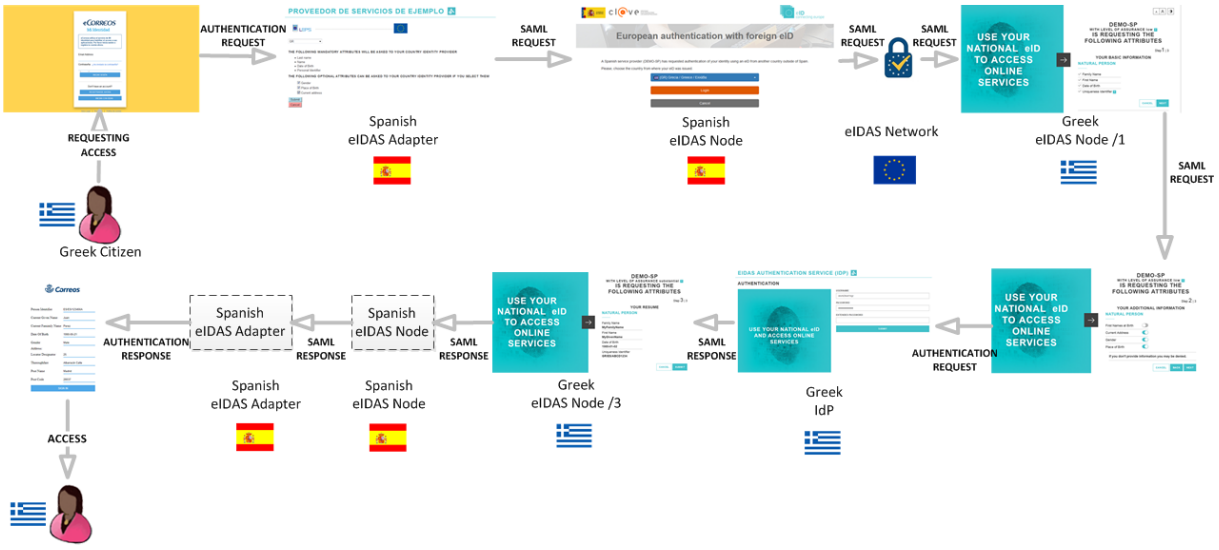

Figure 10: eIDAS Authentication Screen flow

Figure 11 shows the authentication diagram flow including the high-level actions performed by each component behind the screens displayed in Figure 10.

[6] https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

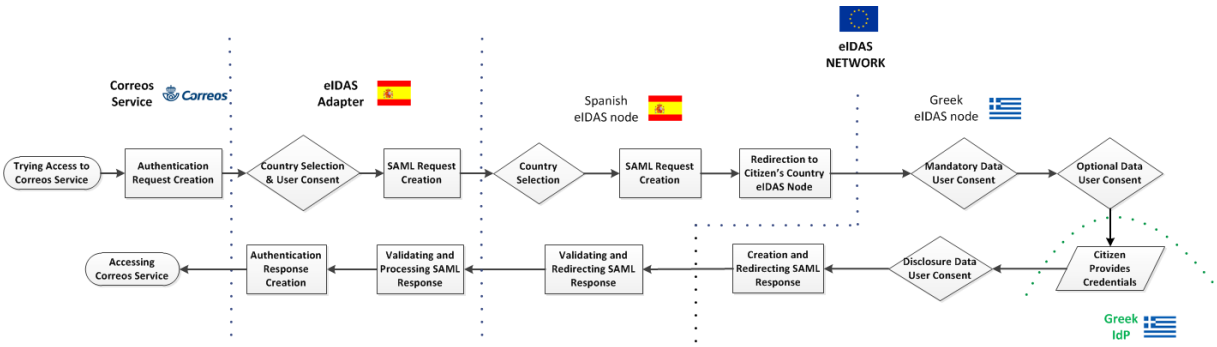

Figure 11: eIDAS Authentication Diagram flow

Figure 12 depicts the sequence diagram detailing the performed actions by each single component.

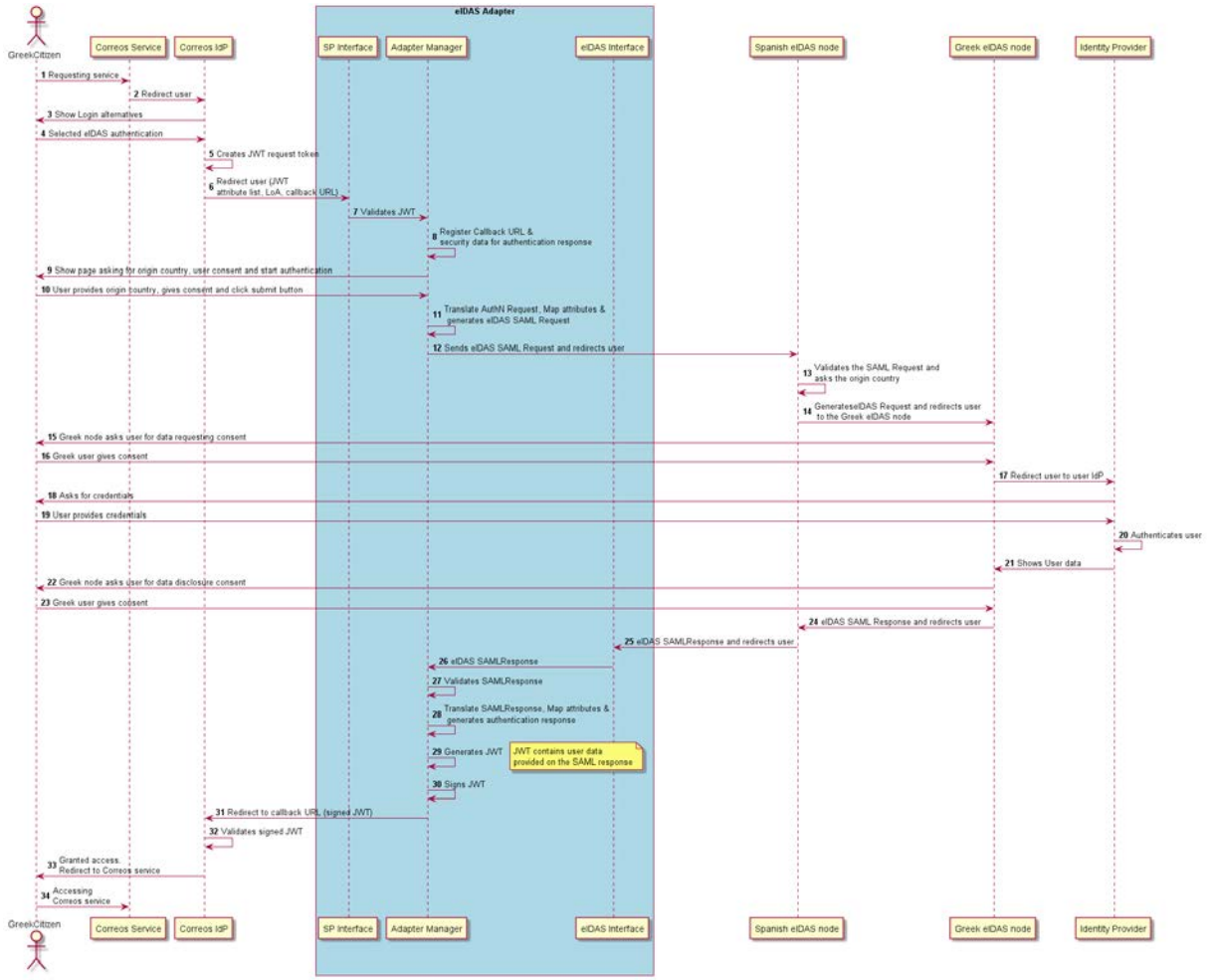

Figure 12: eIDAS Authentication Sequence Diagram

A detailed description of these steps is provided next.

1- A Greek citizen tries to get access the Correos service;
2- The Correos service redirects the user to the Correos IdP;
3- The Correos IdP displays different login options to the user;
4- The user selects the eIDAS authentication option;
5- The Correos IdP creates a JWT request token;

6- The Correos IdP redirects the user to the SP Interface providing the JWT request token which includes the requested attributes, the LoA and the callback URL where the response should be provided;
7- The SP Interface receives the authentication request and validates the JWT;
8- Register the call back URL and the security data for the authentication response;
9- The user is asked to provide her origin country and gives the consent for the requested data;
10- The user gives consent and the eIDAS authentication is triggered;
11- The Manager service translates the JWT retrieving the list of requested attributes, maps the attributes to the eIDAS format and generate an eIDAS SAML request;
12- The user is redirected to the Spanish eIDAS node and the SAML request is sent;
13- The SAML Request is validated and the user origin country is asked;
14- The user is redirected to the Greek eIDAS node and the SAML Request is sent;
15- The user is asked to give data request consent;
16- The user give consent;
17- The user is redirected to the Greek IdP and SAML authentication request is sent;
18- The IdP asks the user credentials;
19- The user provides credentials;
20- The IdP authenticates the user;
21- The Greek node shows the user data;
22- User consent for data disclosure is required;
23- User gives consent;
24- The Greek eIDAS node redirects the user to the Spanish eIDAS node, and sends a SAML Response containing the user data;
25- The Spanish eIDAS node redirects the user to the Adapter eIDAS Interface;
26- The SAML Response reach the Adapter Manager;
27- The SAML Response is validated;
28- The SAML Response is processed, the attributes are mapped and an authentication response is created;
29- A JWT is generated including the user information and the data retrieved from the authentication request for security checking;
30- The JWT response token is signed;
31- The user is redirected to the callback URL and the JWT is sent;
32- The IdP validates the signed JWT response token;
33- The IdP grants user access to the service;
34- The user is redirected to the requested service.

5.3 Technologies

During the implementation, deployment and test of the eIDAS adapter several technologies, standards and protocols have been used for these purposes.

The eIDAS adapter is implemented in Java[7] programming language version 8.0. On top of this during the design and implementation process the following frameworks, technologies, standards and protocols have been used.

[7] http://www.oracle.com/technetwork/java/index.html

- Spring Boot[8]: Creates stand-alone Spring applications, embedding Tomcat as application server, avoiding the war files deployment;
- Swagger[9]: For designing, build and testing API REST for both SP and eIDAS interfaces, which are included into the eIDAS Adapter;
- Servlets[10]: Provides the endpoints for both SP and eIDAS node for sending the authentication response and receives the SAML response respectively;
- Struts 2[11]: Framework for creating Java EE web applications, based on the 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;
- JWT[12]: 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;
- SAML 2.0[13]; XML-based framework for transmitting user authentication between the eIDAS adapter and the eIDAS network, in both ways;
- eIDAS Technical Specifications [14]: 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;
- Maven[14]: Software project management tool for managing dependencies with java code libraries for developing code and project's build;
- Apache Tomcat[15]: Web application server where the eIDAS adapter is running;
- Docker[16]: This platform facilitates the application deployment, avoiding dependencies between application and infrastructure;
- Eclipse[17]: The selected IDE for source code management is Eclipse Oxygen[18];
- GitLab[19]: Repository for uploading the project source code or the artefacts created during the implementation process. Also used for bug tracking.

Figure 13 depicts at a glance the different technologies used during the implementation and deployment of the eIDAS Adapter.

[8] https://spring.io/projects/spring-boot
[9] https://swagger.io/
[10] https://docs.oracle.com/javaee/7/tutorial/servlets.htm
[11] https://struts.apache.org/
[12] https://jwt.io/introduction/
[13] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
[14] https://maven.apache.org/
[15] http://tomcat.apache.org/
[16] https://www.docker.com/
[17] https://www.eclipse.org/
[18] https://www.eclipse.org/oxygen/
[19] https://about.gitlab.com/product/

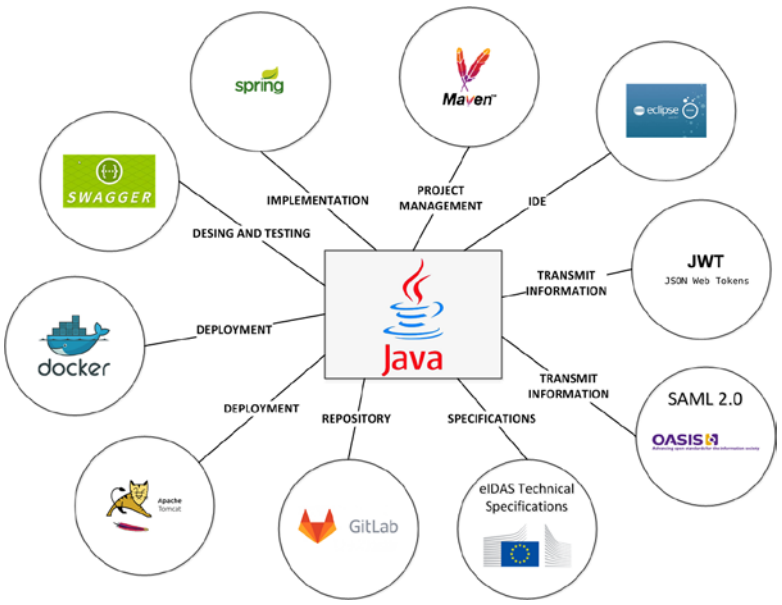

Figure 13: Technologies used during the eIDAS Adapter Implementation and Deployment

5.4 Deployment

The eIDAS Adapter is built as a Java Web Application Archive (war file[20]) that must be deployed in a Web Application Container like Apache Tomcat.

The Tomcat version 8.0.46. used is configured on server.xml file. Exposed ports and context are provided in Annex 3: Deployment Configuration.

For deployment of the eIDAS adapter deployment Docker[21] and Docker Compose[22] are used. The Dockerfile is provided in Annex 3: Deployment Configuration, and includes the following information:

- The Tomcat server version to be used;
- The exposed port;
- The path to the server.xml file with the Tomcat configuration;
- The path to the war file;
- The path to the application configuration files and the certificates needed for the crypto functionalities.

The initial deployment of the eIDAS adapter will be on Atos premises with the aim of facilitate the development, debugging and testing process. Correos is evaluating the possibility of deployment on their premises, taking into account security matters and final cost for hosting and maintenance.

The server machine where the eIDAS adapter is running has Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-121-generic x86_64) as OS:

Additional info about the main features of the server machine is provided in Annex 4: Server Machine Features.

[20] https://en.wikipedia.org/wiki/WAR_(file_format)
[21] https://www.docker.com/
[22] https://docs.docker.com/compose/overview/

6 “Spanish eIDAS node Integration”

In Task 3.2 “Customization of Spanish Correos Services Portal” developed the customization of Correos e-services, the implementation of the SP interface the eIDAS adapter is exposing to the external users, and the integration tests between the SP and the eIDAS adapter. These actions where described in D3.2 “Operational and Technical Documentation of Correos services customization” [10]. The next step, the integration with the eIDAS node, is performed in T3.3, and described in this document D3.3. In previous sections, it was described the eIDAS adapter architecture (section 4) and the functionalities implemented (section 5.1). This section, also, describes how the integration of the eIDAS adapter with the Spanish eIDAS node through the eIDAS interface is made, and the updates and modifications developed on the adapter component and the Correos SP.

6.1 Integration with Correos Services Updates

The main adaptations and modification needed on Correos’ services were described in D3.2 “Operational and Technical Documentation of Correos Services Customization” [10]. With the objective of make easier the integration with the eIDAS adapter was developed a mock up for simulating the process. The only action taken is modifying the path to the final version of the adapter once the integration with the eIDAS node is ready.

As indicated in section 6.3 the path where the eIDAS adapter is deployed has changed due to eIDAS node port restrictions.

6.2 “Integration with Spanish eIDAS node”

The eIDAS adapter component is linking the SP and eIDAS node, allowing the connection with the eIDAS infrastructure. As described in sections 4 and 5 this component is built of several sub-components (see Figure 4 and Figure 5).

This phase is focused on the developed of the eIDAS interface based on servlets, that interact with HTTP requests and HTTP responses in order to communicate with the end-user, with eIDAS node and with the IdP. In this context, the main effort has been made for generating the SAML request (to be sent to the Spanish eIDAS node) and create the authentication response (to be sent to the Correos service) using the user data retrieved from the SAML response.

Next is explained the **integration strategy** followed with the aim to reduce time and effort during eIDAS adapter implementation, configuration and deployment, and create a RESTful application up and running in a faster way, the use of Spring Boot framework was decided as first approach.

The Spanish Ministry has different eIDAS network access policy for public and private sector.

The public sector is accessing to Spanish eIDAS node through the Cl@ve[23] gateway, while the private sector access directly to the eIDAS node. For the later purpose, the Spanish Ministry has delivered a SP integration package in three flavours, Java, PHP and ASP:NET (see Figure 14).

[23] http://clave.gob.es/clave_Home/clave.html

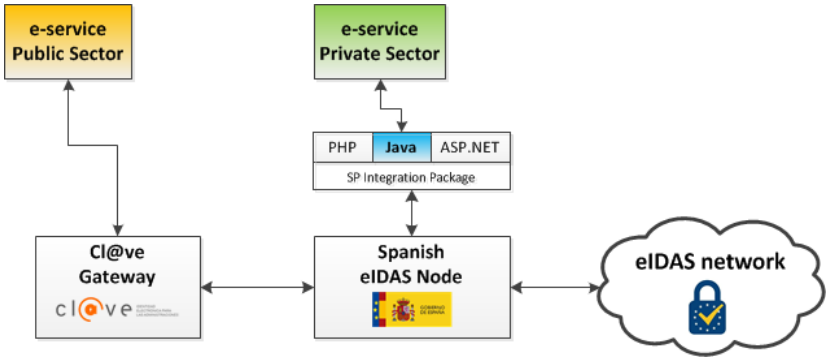

Figure 14: Spanish eIDAS Node Integration

The first decision taken for developing the eIDAS adapter was reuse the SP Integration package provided by the Spanish Ministry or implement the adapter from the scratch, leveraging eidas-saml-engine library [15] (eIDAS module for managing SAML messages following eIDAS specification). Both alternatives have pros and cons, Table 6 displays some of them.

Table 6: Pros and Cons Implementing eIDAS adapter

	Pros	Cons
SP Integration Package	Reuse already developed code can speed up the process and reduce effort and implementation time.	Inherited technologies and dependencies when reuse code.
	Code already tested by the Spanish Ministry. Hints and specific documentation is provided.	Only general documentation could be used.
	After meeting with the Spanish Ministry, some support can be provided by the technical team, supporting the integrating to the eIDAS node	Full availability of the technical team is not guarantee, as the Spanish Ministry is not a project partner.
eIDAS Module	Developers can use familiar technologies.	Support on the technologies selected would be not guarantee.
	Customization can be quicker	Connection with the eIDAS node can take more time than expected.
	No dependencies with inherited code or technologies.	Implementation from the scratch would imply more time and effort on the process.

As the decision for acquiring one or the other alternative depends on the particular SP needs. and considering the Greek side of the project is implementing different alternatives based on the eIDAS module, the Spanish side decide to follow the implementation of the eIDAS adapter, leveraging the SP implementation package provided by the Spanish Ministry, with the aim to provide more alternatives to the SPs for taking a right decision,

The next decision to take is which flavour to choose. As the Atos technical team is used to manage Java language and the eIDAS adapter is offering a RESTful endpoint accessible by all kind of SP implementation, the Java package is selected.

Once decided the use of the Java integration package provided by the Spanish Ministry, the following step is the **integration process** itself. The different modules already designed and partially implemented for integrating the SP and for managing the authentication process are implemented in full, including all the functionalities needed for completing the authentication process through the eIDAS infrastructure using the user eID. It means that the following services, basically, the SP Interface, the Mapping service, the Translator service, the Orchestrator module and the User Interface, can be updated or modified.

The following sub-components have been updated:

- The initial endpoint developed was based on Spring technology, due to some compatibility problems with Struts 2 technology, the authenticate endpoint was updated and changed by a servlet based service;
- Mapping service, which does the semantic translation (i.e. mapping) of user attributes between the SP side and the eIDAS node side, and the way back
- The Translator service includes the translation, basically from SAML response to JWT response token;
- The Manager service have been updated: including orchestrator steps, for completing the user authentication process;
- The User Interface: The list of countries can be removed as the Spanish eIDAS node includes a new screen with the list of the available countries connected from the Spanish eIDAS node.

The SAML Engine as legacy library, the Metadata service and the eIDAS interface are kept as is, only the configuration files where these components are referred are updated.

Figure 15 shows which components are modified or keep as is during the eIDAS node integration process.

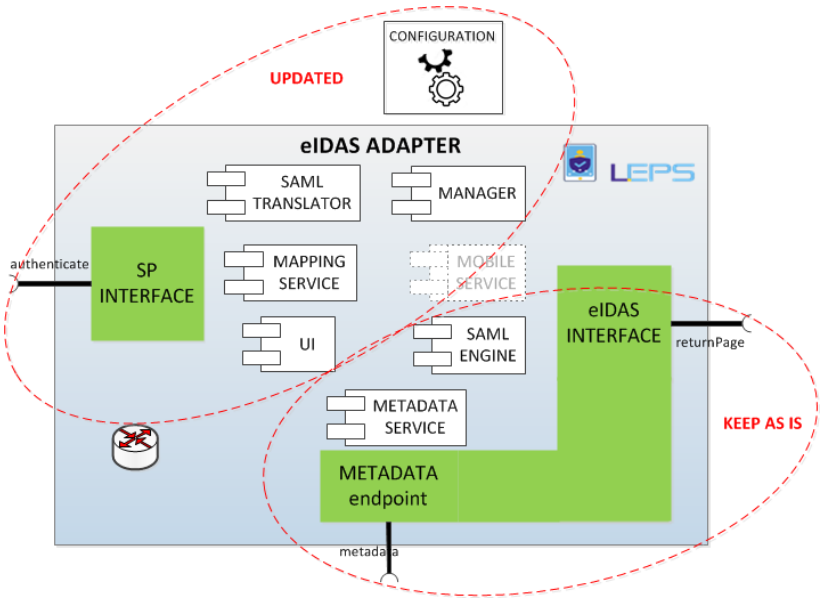

Figure 15: Spanish eIDAS Integration Updates

During the design, implementation and integration phases some **issues** have arisen affecting the completion of the performed tasks and the preparation of this document. The main issues found are compiled in Table 7. The found issues where overtaken for completing the planned tasks and this document. In section 8.2 some mitigation actions are suggested.

Table 7: Issues Found During the eIDAS Adapter Implementation

Issue	Description	Actions Performed
1	Technologies used: Java integration package is using Struts 2 and not all the developing team was familiar with this technology, but with Spring.	Initial learning period took place for being familiar with this framework. Finally, the complete development of the eIDAS adapter took more time than expected.
2	Technology compatibility: Some compatibility problems were found between Spring and Struts 2.	Some Spring services were changed by services based on servlets.
3	Delay granting access to the Spanish eIDAS node: The procedure for accessing to the Spanish eIDAS node got long in time.	Despite the procedure for accessing the Spanish eIDAS node started before finalizing the eIDAS adapter implementation, the procedure took more time than expected.
4	Constraint on port use: Once the eIDAS adapter was implemented the exposed ports for services was inadequate. Use of port 80 or 443 are compulsory.	The contact with the Spanish eIDAS node technical team finally fixed the issue.

In Annex 5: Notes for developers are provided some hints to developers facilitating the future implementation of this kind of adapters for integrating SPs with the eIDAS infrastructure.

6.3 eIDAS Adapter Updates

During the tests performed for integrating the Spanish eIDAS node the following updates on eIDAS adapter have been performed:

- Update the port where the eIDAS adapter is deployed due to Spanish eIDAS node port constraints. Standard ports http 80 and https 443 must be used. This update fulfils the requirement EINOR-9 (Table 2) on Ports used.
  This change has affected both exposed services, the metadata service and the eIDAS interface;
- Updates on the configuration file the paths where the services are exposed.

6.4 “Integration Tests”

In spite of this document should cover the integration with the Spanish eIDAS node in production environment, the integration of Correos’ services will be performed only against “Servicios Estables” (the pre-production environment). due to restrictions on ruled by The Spanish Ministry, who rules the

Spanish eIDAS node, set operational restrictions to SPs from the private sector, which are only allowed to access the pre-production environment. There exists the possibility the private SPs can integrate through Cl@ve gateway on a production environment in the future, but this is a political decision that will not be taken during the project lap time.

The tests performed during the integration process have been introduced in 5.2 and in Figure 10. These tests are basically the authentication flow. The following screenshots shows the process followed during the complete process. A short explanation on the actions performed is also provided.

Step 1- Correos login

A Greek citizen access a protected Correos service[24] and a pop up is displayed asking her to login using eIDAS among other alternatives (Figure 16).

Actions: Click on "INICIAR CON EIDAS" button.

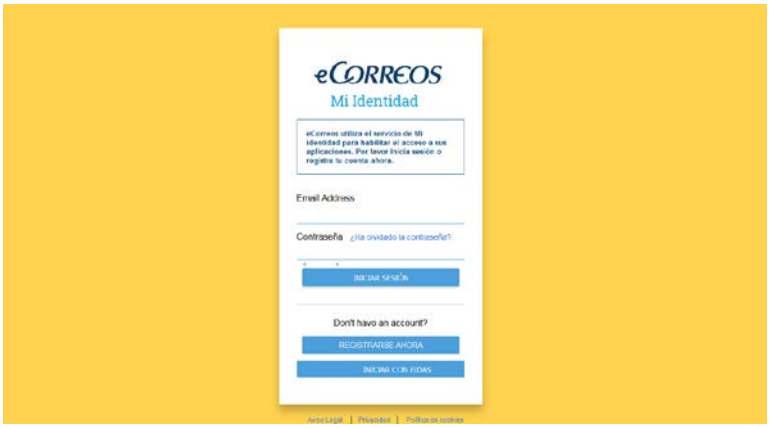

Figure 16: Correos Login

Step 2 - eIDAS Adapter List Attributes

The user is redirected to the eIDAS adapter[25] which presents to the user a screen where the list of both mandatory and optional attributes (Figure 17). Additionally, links to the privacy policy from the SP and LEPS are included.

Actions: User selects country and optional attributes. Clicks on Submit button to proceed with the authentication or Cancel button otherwise.

24 https://login.ecorreos.post/IdPCloudCorreosPRE.onmicrosoft.com/oauth2/v2.0/authorize?p=B2C_1_mi_identidad_signup_signin_eidas_test&client_id=6751b126-cfe3-4ccc-b65f-23c48386d0d9&nonce=defaultNonce&redirect_uri=https%3A%2F%2Fmiidentidadpre.azurewebsites.net&scope=openid&response_type=id_token&prompt=login

25 http://loge.atosresearch.eu/eIDASConn/authenticate

Figure 17: eIDAS Adapter Screen

Step 3 - Spanish eIDAS node Select country

The user is redirected to the Spanish eIDAS node[26] and a list of countries is provided (Figure 18).

Actions: User selects her origin country. Clicks on Login button to proceed with the authentication or Cancel button otherwise.

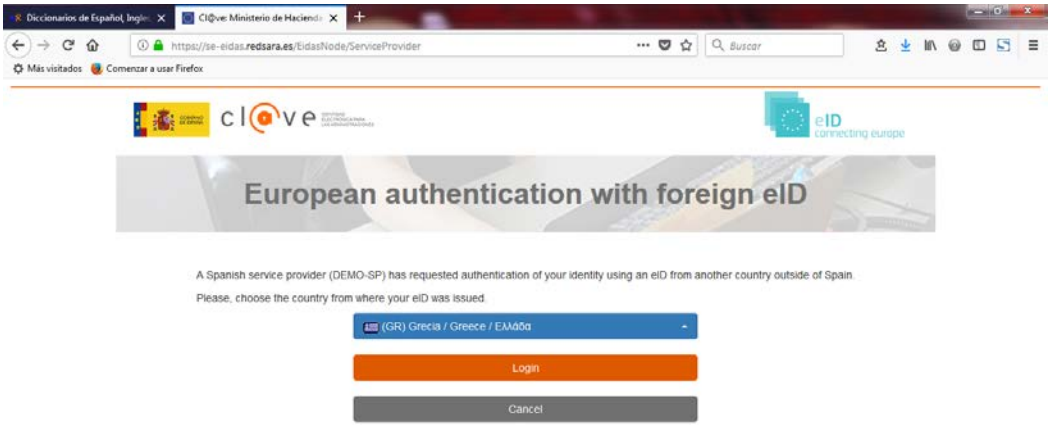

Figure 18: Spanish eIDAS Node Country Selector

Step 4 - Greek eIDAS node Step 1

The Greek citizen is redirected to the Greek eIDAS node[27] where the list of mandatory attributes is displayed (Figure 19).

Action: The user clicks on NEXT button to proceed with the authentication or Cancel button otherwise.

[26] https://se-eidas.redsara.es/EidasNode/ServiceProvider
[27] https://pre.eidas.gov.gr/EidasNode/ColleagueRequest

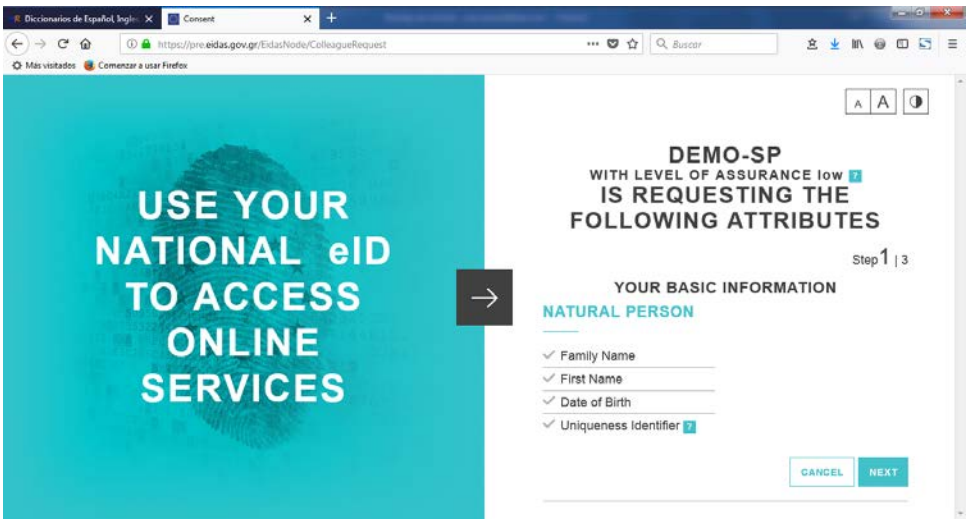

Figure 19: Greek eIDAS Node Compulsory Attributes

Step 5 - Greek eIDAS node Step 2

The user is redirected to Step 2[28] on Greek eIDAS node displaying the requested optional attributes (Figure 20).

Actions: The Greek citizen selects the optional attributes to be requested to the IdP. Clicks on NEXT button to proceed with the authentication or Cancel button otherwise. BACK button allows the user to go back to the previous step 1.

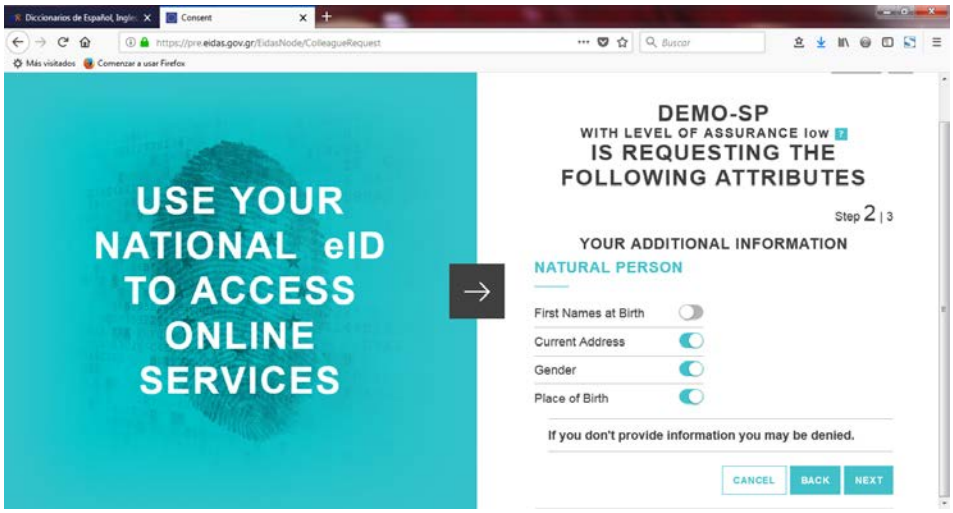

Figure 20: Greek eIDAS Node Optional Attributes

Step 6 - Greek IdP Credentials

The Greek citizen is redirected to the Greek IdP[29] asking the user for introduce credentials (Figure 21).

Actions: User introduces user and password. Clicks on SUBMIT button.

[28] https://pre.eidas.gov.gr/EidasNode/ColleagueRequest
[29] http://t-leps-idp.inet.helex.gr:8080/IdP/AuthenticateCitizen

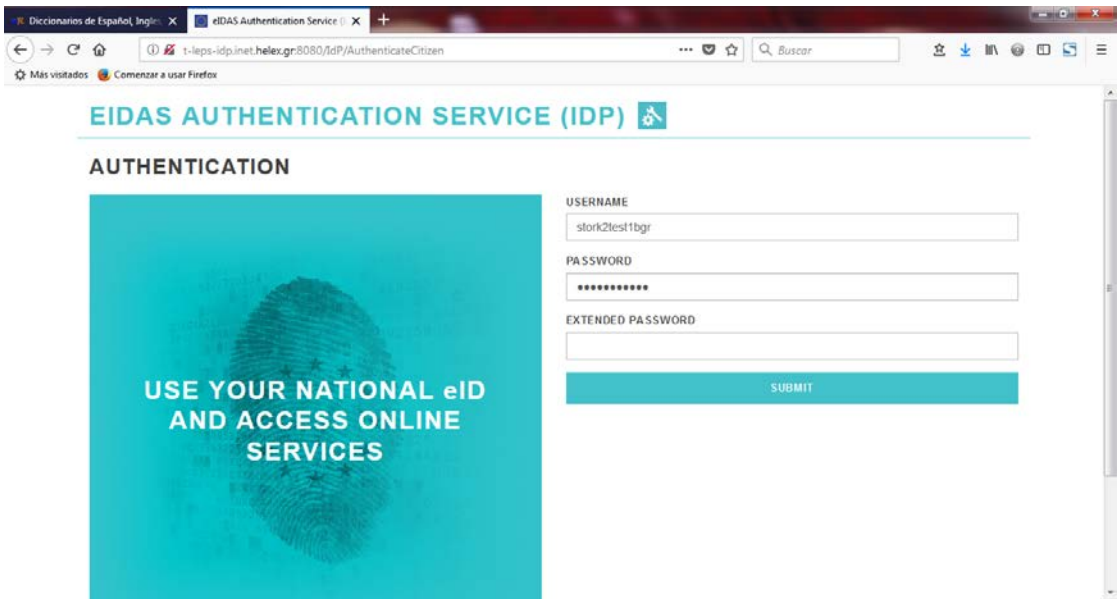

Figure 21: Greek IdP Asking User Credentials

Step 7 - Greek eIDAS node User Data

The Greek citizen is redirected to the Greek eIDAS node[30] and the requested data are displayed (Figure 22).

Actions: User clicks on SUBMIT button for accepting data disclosure to the Spanish eIDAS node or clicks the CANCEL button otherwise.

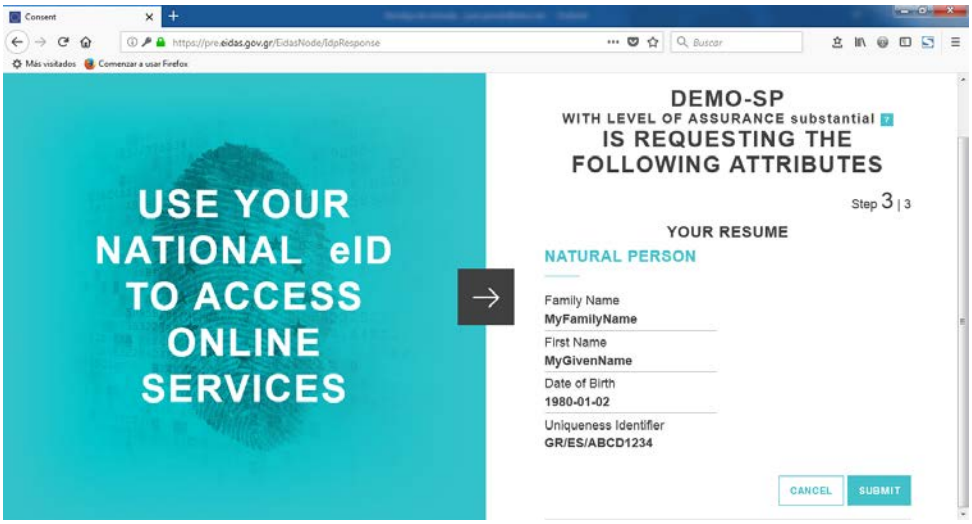

Figure 22: Greek eIDAS Node Asking User Acceptance

Step 8 - Correos Enrolment Page

The user is redirected to the Spanish eIDAS node, then to the eIDAS adapter and finally to the Correos service enrolment page[31] (Figure 23).

Actions: Greek citizen clicks on SIGN IN button for completing the enrolment process.

[30] https://pre.eidas.gov.gr/EidasNode/IdpResponse

[31] https://miidentidadpre.azurewebsites.net

This screen (mock up) can be modified by the final one.

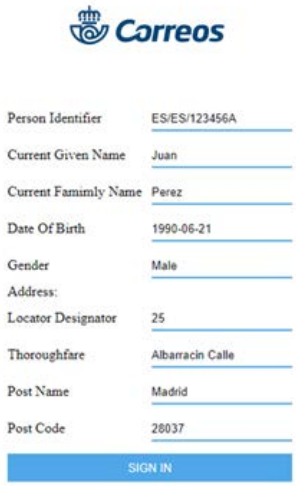

Figure 23: Correos enrolment Screen

7 “Interoperability tests”

Interoperability tests will be developed by Activity 6 “Testing of cross-border authentication and access to Correos electronic Services and to Hellenic (Financial and Post) electronic Services”. But, the initial contacts with other Member States than Greece have been started during the process of eIDAS adapter integration with the Spanish eIDAS node. The contacts were made, under the umbrella of the Spanish Ministry, with the countries already connected with the Spanish eIDAS node or those planned on the near future before the end of this project.

Additionally, contacts with the Hellenic Ministry of Administrative Reconstruction (HMAR) have been made in order to not overlap the contacted countries and try to cover wide number of Member States, for performing the interoperability tests.

Considering these premises, the contacted countries by the Spanish side will be Italy, The Netherlands, Iceland and Sweden.

The interoperability tests will be described and performed during the development of Activity 6 and will be included in deliverable D6.1 for Milestone 10.

8 “Evaluation & Lessons learnt”

This section provides the main results achieved during the integration of the Spanish services with the Spanish eIDAS node. It is also included the lessons learnt during the implementation, deployment and testing processes. This will support future private SP’s integration in other European countries that can help and diminish the needed effort.

8.1 Evaluation

The main results reached in the course of this task T3.3 are listed next:

- Demonstrate the feasibility of the SP Integration package the Spanish Ministry has provided for SP integration with the Spanish eIDAS node;
- The modular design of the eIDAS adapter allows an easy integration with different SP protocols;
    - The developed eIDAS adapter provides a single endpoint (SP Interface) for interconnection of many SP services in the same domain;
    - The eIDAS adapter is able to send SAML request to eIDAS node, translate SAML response from SAML 2.0 to JSON and forward it to the relevant SP service;
- Integrate security features for transmitting user information between different domains (i.e. eIDAS infrastructure to SP domain) using secure JWT tokens. The included claims are encoded as a JSON object and digitally signed. User data are encrypted with a secret Key, which is updated regularly;
- The eIDAS adapter is SP infrastructure independent.
- The use of Docker framework for deployment allows:
    - The use of any kind of OS such as Linux or Windows;
    - Cloud deployment;
    - Ease the large-scale deployment;
    - Increase the security;
    - Enable portability. This means that the eIDAS adapter can be hosted on the Correos infrastructure or in an external hosting/cloud provider;
- The eIDAS adapter component fulfils with the technical and operational requirements, and also with the legal requirements compiled in section 3.
  Table 8 shows the fulfilment of the compiled requirement in section 3.

Table 8: Requirements fulfilment

Requirement	Yes	No	Partially	Comments
EINER-1	X			
EINER-2	X			
EINER-3			X	Not at this moment, https protocol will be implemented before the end of the project.

Requirement	Yes	No	Partially	Comments
EINER-4	X			
EINOR-1	X			
EINOR-2	X			
EINOR-3	X			
EINOR-4	X			
EINOR-5	X			
EINOR-6	X			
EINOR-7	X			
EINOR-8	X			
EINOR-9	X			Use of port 80 at the moment, port 443 will be enabled before the end of the project. Related with EINER-3.
SPR-1	X			
SPR-2	X			
SPR-3	X			
SPR-4	X			
LR-1	X			
LR-2	X			
LR-3			X	Complete information on data protection will be included before the end of the project.

8.2 Lessons Learnt

During the implementation, deployment and test of eIDAS adapter some problems were found, in this section some actions and decision to be taken in advance are suggested, for avoiding or mitigating those problems.

The initial approach for **designing and implementing** this component was based on the idea of reuse as much as possible the integration package the Spanish Ministry delivered for the private SP connection. In one hand this approach would help to reduce the implementation time and effort for generating the final component. Moreover, this option guarantee that the connection to eIDAS node has been checked and assured, and just effort on integrating SP service should be done. In the other hand the use of legacy code and the used technologies for creating this integration package can limit the possibility to use more familiar technologies to the development team. In the particular case of the Spanish eIDAS adapter implementation, the experience mixing different technologies (e.g. Struts 2 and Spring) was causing some problems, and it took more time than expected. It was necessary to carry out some changes and the developer team had to acquire some knowledge on Struts 2

framework. For these reasons the use of generic eIDAS library with the more familiar technology the development team is used to manage, is recommended.

One point to take also into consideration is about the **documentation** needed for the integration. The documentation provided by the Spanish eIDAS node technical team seems complete. Some information on error messages and their management would be helpful for understanding the real error and, therefore, speed up the connectivity process.

Beside the documentation, the **technical support** is another important point to be considered. The Spanish Ministry created a communication channel for contacting to the eIDAS node technical team. The connectivity tests to the Spanish eIDAS node was being at the same time the eIDAS technical team was performing interoperability tests with the rest of European countries joined to the eIDAS network. This caused some delays on the technical support. The involvement of the Spanish Ministry as project partner of this kind of projects is recommendable.

In any case, the results obtained by following this choice would provide relevant information for those countries to take a decision on the way to proceed with the private SP connection.

8.3 Future Improvements

After the design and the implementation process some improvements can be suggested for the future.

- **The user authentication with the mobile devices using eID supporting NFC**. As indicated in section 5.1.8 a Mobile module has been suggested to be included for improving the user experience. This would be a first approach, but it would be worth to include this functionality on the eIDAS node side or even better on the Spanish IdP side for managing in a nice way the eID supporting NFC technology.
- **New eIDAS node 2.0 release[32] delivered by the European Commission.** The European Commission has released a new version 2.0 on 28 March 2018 of software for eIDAS-Node [16]. The main changes included in this new version are summarized next [16]:
    - Provided in two kinds of deployment;
    - Architectural changes "enabling seamless upgrades of the eIDAS-Node in the future" [16], and splitting the country eIDAS node component in two modules, the Proxy Service and the Connector;
    - JSON protocol defined for demo-SP application;
    - Use of OpenSAML 3.0;
    - Look and feel.

  The objective of this new release is to improve the user eID experience. As indicated the version 2.0 replace the SAML 2.0 protocol by JSON protocol, and each MS should take the decision for selecting the security protocol and how to implement the interfaces with the SPs and the IdPs. An interesting study made by Estonian authorities named "Migration to eIDAS Node 2.0 – Technical Analysis", comparing different options to follow afterwards, would be worth to be checked by both Spanish and Greek authorities. A short-term solution is suggested maintaining the version 1.4 to accomplish with the 2018 September deadline, and moving from eIDAS node version 1.4 to 2.0 as a long-term option [18].

[32] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2018/04/04/Release+of+eIDAS-Node+software+version+2.0

Despite of the current deployment of the Spanish eIDAS node is based in version 1.4, the technical team is working on the new version. This could affect the eIDAS adapter and a new updated version of this component would be necessary to deliver.

- **Private sector SPs connected to Cl@ave gateway.** In case the Spanish Ministry decides the private e-services will be connected to Spanish eIDAS node through Cl@ve instead of making a direct connection, the eIDAS Interface module must be updated to fit with the new situation.

9 Conclusions

The main output of the actions performed during the integration process in T3.3 is the design and implementation of an eIDAS adapter able to integrate SP from private sector with the eIDAS network, allowing a Greek citizen accessing to Spanish digital services using her Greek eID.

The design and implementation of this component has demonstrated the feasibility of reusing tailor-made solutions provided by the Member States (SP integration package delivered by the Spanish authorities), and including additional security features (secure JWT token) for user data transmission on top of this. Additionally, the generated component permits the connection with different SPs which are built in with different technologies. Also, the selected form of deployment gives the possibility of deployment in different environments and OS.

The modular design and implementation allows the functional enhancement in the future.

The results of this activity performed in the Spanish side, beside the results produced in Activity 4 and Activity 5, will be the basis for the guide lines and alternatives to provide at the end of the project, for helping other European countries the way to integrate SPs from the private sector with the particular country eIDAS node. In summary, thanks to the achievements reached within this Task 3.3 the following targeted objectives for this action have been fulfilled:

a) Connecting the IT infrastructure of Correos' end-user to Spanish eIDAS node, allowing the Correos' services to use the eIDAS network (i.e. eID common building block).
b) Demonstrate the usability of eIDAS specifications and the Spanish eIDAS node in the private sector.
c) Using and testing the Correos' services for cross-border user authentication against eIDAS network, providing guidelines of the process helping to other European countries.
d) Boosting the growth of eID uptake within the private sector.

The unique objective not covered in full by the project has been the user authentication across borders in production environment for accessing the e-services provided by Correos. As indicated in section 6.4, the Spanish Ministry only allows the connection between private SPs and the "Servicios Estables" (the pre-production environment) for accessing the Spanish eIDAS node. The Spanish authority decision restricts the use of Correos' services to a pre-production environment. For security reasons, this forces Correos to connect only their pre-production e-services to pre-production Spanish eIDAS node.

References

[1] European Commission, STORK: Take your e-identity with you, everywhere in the EU, https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu/, retrieved date 2018/05/23

[2] STORK 2.0, https://www.eid-stork2.eu/. retrieved date 2018/05/23

[3] eSENS, Moving Services Forward, https://www.esens.eu/, retrieved date 2018/05/23

[4] European Commission, e-SENS and Connecting Europe Facility: how do they work together?, https://ec.europa.eu/digital-single-market/en/news/e-sens-and-connecting-europe-facility-how-do-they-work-together. Retrieved date 2018/05/23

[5] European Commission, About CEF building blocks, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/About+CEF+building+blocks. Retrieved date 2018/05/23

[6] European Commission, eIDAS Observatory, https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014. Retrieved date 2018/05/23

[7] European Commission, eIDAS Profile: eidas_interoperability_architecture_v1.00.pdf, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile?preview=/46992719/47190130/eidas_interoperability_architecture_v1.00.pdf. Retrieved date 2018/05/23

[8] Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 15 March 2005, http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf. Retrieved date 2018/06/18

[9] European Commission, eIDAS-Node integration package, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Node+integration+package. Retrieved date 2018/06/18

[10] LEPS deliverable lead author: Juan Carlos Pérez Baún, D3.2 Operational and Technical Documentation of Correos services customization. Deliverable of the LEPS project, 2018. http://leps-project.eu/node/344.

[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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG, Retrieved date 2018/06/19

[12] Cuerpo Nacional de Policia, DNI y Pasaporte, Descripción DNI 3.0, https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_103&id_menu=1, retrieved date 2018/06/27

[13] LEPS deliverable lead author: Elena Torroglosa, D3.1 Mobile ID App. Deliverable of the LEPS project, 2018. To be submitted on June 2018.

[14] 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, retrieved date 2018/07/18.

[15] European Commission,, , eIDAS.Node and SAML 2.1, version 2.1, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiHr4GklrXcAhVrJMAKHcqqDnYQFggwMAE&url=https%3A%2F%2Fec.europa.eu%2Fcefdigital%2Fwiki%2Fdownload%2Fattachments%2F46992189%2FeIDAS-Node%2520and%2520SAML.pdf%3Fversion%3D1%26modificationDate%3D1523458236833%26api%3Dv2&usg=AOvVaw0hHc6ZRIPFIy0IBoCU_KJA , retrieved date 2018/07/23.

[16] European Commission, Release of eIDAS-Node software version 2.0, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2018/04/04/Release+of+eIDAS-Node+software+version+2.0, retrieved date 2018/07/25.

[17] European Commission, Digital Single Market, https://ec.europa.eu/digital-single-market/e-identification, retrieved date 2018/07/26.

[18] Estonian Information System Authority, Migration to eIDAS Node 2.0 – Technical Analysis, https://e-gov.github.io/TARA-Doku/Migration, retrieved date 2018/07/27

Annexes

Annex 1: SP Requirements

SP Requirements compiled in D3.2 [10]:

Id	Name	Description
SPR-1	Attributes	eIDAS infrastructure **MUST** provide name, surname, person identifier and date of birth as mandatory attributes to complete the register and the login processes. eIDAS infrastructure **MAY** provide additional user data such as address, gender or fiscal code if user gives consent and the eIDAS platform is able to provide.
SPR-2	Adapter	eIDAS adapter **MUST** provide a connector to eIDAS infrastructure in order to retrieve user attributes to SP.
SPR-3	Authentication request	SP **MUST** agree with the eIDAS adapter implementer partner the content of the JWT provided by the adapter and the structure of the JWT provided by Correos services to the adapter. These tokens are the base of the trust chain for triggering the authentication process.

Annex 2: sp-metadata.xml

The metadata included into the xml provided by the eIDAS Adapter metadata endpoint is included next. Signature and certificate parts have been hidden for security reasons.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://loge.atosresearch.eu:8185/eIDASConn/metadata" validUntil="2018-06-06T08:43:40.710Z">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"/>
            <ds:Reference URI="">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
                <ds:DigestValue>IRKmTXOfd … </ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
```

```
<ds:SignatureValue>J7KMZV …</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIDSzCCAjMCBF…</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIDSzCCAjMCBF… </ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIDSzCCAjMCBF …</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://localhost:8080/ceic/ReturnPage" index="0" isDefault="true"/>
</md:SPSSODescriptor>
<md:Organization><md:OrganizationName xml:lang="en"/>
<md:OrganizationDisplayName xml:lang="en"/>
<md:OrganizationURL xml:lang="en"/></md:Organization>
<md:ContactPerson contactType="support"/>
<md:ContactPerson contactType="technical"/>
</md:EntityDescriptor>
```

Annex 3: Deployment Configuration

This annex provides the configuration files needed to eIDAS adapter deployment. Basically, the Apache Tomcat configuration, and the Dockercompose file for creating the Docker container where the adapter is running.

Only the relevant information such as exposed ports and context is provided.

- server.xml file

<! -- A "Connector" represents an endpoint by which requests are received
and responses are returned. Documentation at:
Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
Java AJP Connector: /docs/config/ajp.html APR (HTTP/AJP) Connector: /docs/apr.html
Define a non-SSL/TLS HTTP/1.1 Connector on port 8080 -->
<Connector connectionTimeout="20000" port="80" protocol="HTTP/1.1" redirectPort="8443"/>
….
<Context docBase="eIDASConn" path="/eIDASConn" reloadable="true" source="org.eclipse.jst.j2ee.server:eIDASConn"/>

- Dockefile

FROM tomcat:8.0.46-jre8

MAINTAINER Leps
EXPOSE 80

ENV LOG_HOME /usr/local/tomcat/logs

ADD config /LEPS/config
ADD certificates /LEPS/certificates

COPY server.xml /usr/local/tomcat/conf/server.xml
COPY eIDASConn.war /usr/local/tomcat/webapps/

Annex 4: Server Machine Features

Architecture: x86_64
CPU op-mode(s): 32-bit, 64-bit
Byte Order: Little Endian
CPU(s): 2
On-line CPU(s) list: 0,1
Thread(s) per core: 2
Core(s) per socket: 1
Socket(s): 1
NUMA node(s): 1
Vendor ID: GenuineIntel
CPU family: 6
Model: 44
Model name: Intel(R) Xeon(R) CPU E5645 @ 2.40GHz
Stepping: 2
CPU MHz: 2400.118
BogoMIPS: 4800.23
Hypervisor vendor: vertical
Virtualisation type: full
L1d cache: 32K
L1i cache: 32K
L2 cache: 256K
L3 cache: 12288K
NUMA node0 CPU(s): 0,1

Annex 5: Notes for developers

The following notes will support developers to ease the integration and deployment processes.

- The use of eidas-saml-engine library [15] (eIDAS module for managing SAML messages following eIDAS specification) and the Spring Boot framework can ease the implementation and testing process.
- Designing of the REST interfaces with Swagger framework will help developers and integrators to easily develop clients for accessing the component.
- The use of Docker infrastructure for deployment and testing is highly recommended.