



Leveraging **eID** in the Private Sector

## D3.2 Operational and Technical Documentation of Correos services customization

Document Identification			
Status	Final	Due Date	28/02/2018
Version	1.0	Submission Date	28/02/2018

Related Activities	Activity 3	Document Reference	D3.2
Related Deliverable(s)	D2.1, D3.3, D3.1	Dissemination Level (*)	PU
Lead Participant	Atos, Correos	Lead Author	Juan Carlos Pérez Baún
Contributors	Atos Correos	Reviewers	Petros Kavasalis UAEGEAN
			George Christakeas & Sarantos Michalarias ) ATHEX

### Keywords:

Correos' services, eIDAS, customization, integration

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.

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

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

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

## Document Information

List of Contributors	
Name	Partner
Juan Carlos Pérez Baún	Atos
Victor Martin	Correos
Javier Salazar	Correos
Carlos Balot	Correos
Rogelio Méndez	Correos
Ramón Castrejón	Correos
Pedro Gómez	Correos
Raquel Cortes Carreras	Atos

Document History			
Version	Date	Change editors	Changes
0.1	04/12/2017	Atos	Initial ToC and integration draft
0.2	15/12/2017	Atos/Correos	Updates after Correos feedback
0.3	19/02/2018	Atos	Executive summary and updates through the document chapters
0.4	21/02/2018	Atos Correos	Updates on chapters 2, 3, 4 and 5 Updates on chapters 2, 3 and 4
0.5	21/02/2018	Atos	Polishing document for review
0.6	23/02/2018	Atos/Correos	Added Introduction and Conclusions and updates on sections 2, 3, 4 and 5
0.7	27/02/2018	Atos/Correos	Polishing document updating figures and content across document
0.8	28/02/2018	Atos	Final polishing
0.9	28/02/2018	Atos	Quality Check
1.0			FINAL VERSION TO BE SUBMITTED

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	2 of 28
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final

# Table of Contents

Document Information .....	2
Table of Contents .....	3
List of Tables.....	4
List of Figures .....	5
List of Acronyms.....	6
1 Executive Summary .....	7
2 Introduction.....	8
2.1 Purpose of the document .....	8
2.2 Relation to other project work.....	9
2.3 Structure of the document .....	9
3 “Customization preparation”.....	10
3.1 “Correos Services Portal to integrate”.....	10
3.2 “Register Use Case” .....	11
3.3 “Login Use Case” .....	12
3.4 “Metrics” .....	12
3.5 “Correos Services Requirements” .....	12
3.6 “Technical infrastructure preparation” .....	14
3.6.1 “Architecture”.....	14
3.6.2 “Environment”.....	14
4 “Customization Implementation”.....	16
4.1 “Customization time plan” .....	16
4.2 “Interface definition” .....	16
4.2.1 Correos Digital Services.....	16
4.2.2 eIDAS Adapter .....	21
4.3 “Integration flow”.....	23
5 “Tests”.....	25
5.1 “Test Cases Definition” .....	25
6 Conclusions.....	27
References .....	28

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	3 of 28		
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

## List of Tables

---

<i>Table 1: SP Requirements</i>	13
<i>Table 2: Customization Time plan</i>	16
<i>Table 3: TC1: New user tries to log in on Correos services</i>	25
<i>Table 4: TC2: Existing user tries to log in on Correos services</i>	26

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	4 of 28		
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

# List of Figures

<i>Figure 1: My Identity service</i>	10
<i>Figure 2: My Notifications service</i>	10
<i>Figure 3: My Mailbox service</i>	11
<i>Figure 4: Architecture General Overview</i>	14
<i>Figure 5: My Identity service login page</i>	17
<i>Figure 6: POST call to My Identity service</i>	17
<i>Figure 7: POST call sent to eIDAS adapter endpoint</i>	17
<i>Figure 8: JWT sent to eIDAS adapter endpoint</i>	18
<i>Figure 9: Mock up of eIDAS adapter page for testing purposes</i>	19
<i>Figure 10: JWT sent to My Identity service from eIDAS adapter</i>	19
<i>Figure 11: My Identity protected page</i>	20
<i>Figure 12: eIDAS adapter REST endpoint</i>	21
<i>Figure 13: Screen displayed to the user by the eIDAS connector</i>	22
<i>Figure 14: JWT content</i>	23
<i>Figure 15: Integration flow</i>	24

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization				<b>Page:</b>	5 of 28
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

# List of Acronyms

Abbreviation / acronym	Description
API	Application Programming Interface
CEF	Connection Europe Facility
CPU	Central Processing Unit
EC	European Commission
eID	Electronic Identification
eIDAS	<u>e</u> lectronic <u>I</u> dentification, <u>A</u> uthentication and trust <u>S</u> ervices
GB	<u>G</u> iga <u>B</u> yte
GHz	<u>G</u> iga <u>H</u> erz
HD	<u>H</u> ard <u>D</u> isk
IdP	<u>I</u> ntity <u>P</u> rovider
JWT	JASON Web Token
LEPS	Leveraging eID in the Private Sector
LTS	Long Term Support
OAuth	Open Authorization
OTP	One Time Password
RAM	Random Access Memory
REST	REpresentational State Transfer
SAML	Security Assertion Mark-up Language
SP	Service Provider under the definition of eIDAS SPs
UI	User Interface
UPU	Universal Postal Union
URL	Uniform Resource Locator
UX	User eXperience

Document name:	D3.2 Operational and Technical Documentation of Correos services customization	Page:	6 of 28				
Reference:	D3.2	Dissemination:	PU	Version:	1.0	Status:	Final

# 1 Executive Summary

The main goal of this deliverable D3.2 “Operational and Technical Documentation of Correos services customization” is providing a complete description of the process performed for the customization of the services provided by Correos (My Identity, My Mailbox and My Notifications) during the integration process in the context of LEPS project.

With this aim a summary of the services to integrate is provided. Taking into account the entry points the eIDAS Adapter can offer to the Correos’ services for connecting to the eIDAS infrastructure, an analysis of the detected aspects and points to be modified on the service side is developed. Then the interfaces between the services and the eIDAS adapter are established and agreed.

As a result of this analysis the service Correos ID (based on Correos IdP: MyIdentity) is identified to be customized for connecting to the eIDAS adapter. It implies to adapt the log-in page in order allowing to the users the authentication with eIDAS. The interfaces the eIDAS adapter is offering to MyIdentity service are described, and also the call-back entry point offered by MyIdentity service to the eIDAS adapter is provided.

The interaction between MyIdentity service and eIDAS adapter is described in both ways:

- MyIdentity triggers the user authentication process making an authentication request to the eIDAS adapter;
- The eIDAS adapter will ask to the user to give consent to disclosure personal user data to the Correos service. The user acceptance will trigger the authentication process through eIDAS network. As the connection between eIDAS adapter with the eIDAS node is part of the oncoming developments, this process is not covered by this deliverable.
- The eIDAS adapter will provide to MyIdentity service the user data according to the protocol and format established in advance.

A description of the use case for the authentication process where the user, the Correos services and the eIDAS adapter are involved is also described.

An overview of the technical infrastructure needed for the customization and the integration with the eIDAS adapter is provided as a generic guide for future integration of services with the eIDAS infrastructure.

Metrics, test cases definition and an initial evaluation e.g. lessons learnt, of the customization and the eIDAS adapter integration are finally provided.

The activities performed during the development of this task 3.2 will allow the Correos’ services to be fully integrated with the eIDAS adapter and afterwards with the eIDAS infrastructure itself.

As final conclusion the three services provided by Correos have been successfully integrated with the entry point to the eIDAS infrastructure. After the final implementation of eIDAS adapter and the integration with the Spanish eIDAS node the services provided by Correos will be totally integrated with the eIDAS network, easing to European citizens a cross-border authentication for accessing to those services.

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	7 of 28	
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

## 2 Introduction

In the context of emerging the Digital Single Market in Europe, the EU Innovation and Networks Executive Agency through the Connection Europe Facility (CEF) Telecom program [2], is providing Digital Service Infrastructure (DSI) building blocks, trying to ease the connection with citizens, business and public administrations in a cross-border way.

According Ecommerce Foundation<sup>1</sup> the eCommerce in Europe<sup>2</sup> has reaching more than 600 € in 2017. Additionally the cross-border availability of public on-line services is growing in Europe<sup>3</sup>. The improving of these services is based on, among others, the availability of eID issued by European trusted authorities.

The use of eID for accessing digital services is a secure method, preventing fraud and facilitating the user data protection. Electronic Identification (eID) solutions allow European citizens to authenticate themselves and sign documents through e-signatures. These solutions can be integrated not only for accessing public digital services but for private online services.

Regarding the private sector the eCommerce in southern Europe is on the rise<sup>4</sup>. Namely in Greece grew in 2017 by 8% to €4.4 billion<sup>5</sup>. Also in Spain grew by 8% to €28 billion<sup>6</sup>. But as the Eurostat indicates the cross-border transactions accross the EU is not exploited by business in deep<sup>7</sup>.

The Correos services are customized in the context of the LEPS project, to validate the use of eID in private sector, integrating the eIDAS infrastructure, LEPS project has been granted for validating and facilitating the connection between European citizens and private digital services in Greece and Spain. Also ease the uptake of eID on the private sector for cross-border transactions.

### 2.1 Purpose of the document

This deliverable D3.2 Operational and Technical Documentation of Correos services customization is the verification of the Milestone 3 of the LEPS project, associated with the task 3.2 Customization of Spanish Correos Services Portal.

This document provides a technical report containing description of the customization of the selected Correos services environment for integration with CEF eID.

The actions reported across the document are embedded in the context of the Activity 3 Customization of Spanish Postal Services and Integration with eIDAS infrastructure.

<sup>1</sup> <http://www.ecommercefoundation.org/>

<sup>2</sup> <https://ecommercenews.eu/e-commerce-europe-e602-billion-2017/>

<sup>3</sup> <https://ec.europa.eu/digital-single-market/en/news/new-study-egovernment-services-europe-improving-cross-border-availability-services>

<sup>4</sup> [https://www.r-trends.ru/netcat\\_files/526/459/C\\_European\\_Ecommerce\\_Report\\_2017\\_v170623\\_published\\_28basic\\_29.pdf](https://www.r-trends.ru/netcat_files/526/459/C_European_Ecommerce_Report_2017_v170623_published_28basic_29.pdf)

<sup>5</sup> [https://www.ecommercewiki.org/Global\\_Ecommerce\\_Figures/Europe/Greece](https://www.ecommercewiki.org/Global_Ecommerce_Figures/Europe/Greece)

<sup>6</sup> [https://www.ecommercewiki.org/Global\\_Ecommerce\\_Figures/Europe/Spain](https://www.ecommercewiki.org/Global_Ecommerce_Figures/Europe/Spain)

<sup>7</sup> [http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce\\_statistics#Cross-border\\_web\\_sales\\_within\\_the\\_EU\\_not\\_fully\\_exploited\\_by\\_enterprises](http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics#Cross-border_web_sales_within_the_EU_not_fully_exploited_by_enterprises)

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	8 of 28		
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final



The activities performed during this task 3.2 are the starting point for the integration of the SP with the eIDAS infrastructure, which is being developed in task 3.3 Integration to Spanish eIDAS node.

## 2.2 Relation to other project work

---

The activities described in this document are related to those developed in task 4.1 “Customization of Athens Stock Exchange Services Portal” from activity 4, and task 5.1 “Customization of Hellenic Post Services Portal” in activity 5.

These three tasks are running in parallel and their main objectives, as the Grant Agreement states, are “to provide a seamless integration with the user interface for authentication process of eIDAS-specific elements like country selector or updates to privacy notices and identity reconciliation between eIDAS Uniqueness Identifier and the services internal user identifiers”.

## 2.3 Structure of the document

---

This document is structured in 5 major chapters.

**Chapter 2** presents the activities performed before starting the customization implementation. A general overview of the services to be integrated is provided. Also a description of the envisage use cases and metrics are included. Additionally the specific service requirements are collected, and finally a technical view of the infrastructure and environments is outlined.

**Chapter 3** describes the activities performed during the customization of the Correos’ services and how these services are integrated with the eIDAS adapter. Interfaces in both sides the services and the eIDAS adapter are provided. Also a detailed flow of the authentication process involving the aforementioned components is included.

**Chapter 4** includes the description of the test use cases for testing the integration process and the achieved results.

**Chapter 5** finally presents the conclusions and main achievements reached during the customization and integration process of the Correos’ services.

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	9 of 28	
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

## 3 “Customization preparation”

This section provides a comprehensive view of the Correos customization preparation based on agreement achieved between Correos as Service Provider (SP) and Atos as technical coordinator of the activity and creator of the adaptor to which the Correos services will connect.

Section 2 is organized in seven subsections as follow:

- A description of the Correos as SP end user and Correos e-services to be integrated with the eIDAS Network;
- A description of the scopes of the two use cases (registration and login) developed during the integration process;
- The metrics agreed;
- The requirements compiled such as the minimum data set needed by Correos for authentication purposes, also the reconciliation between eIDAS identifier and Correos internal user identifier is provided;
- The integration architecture using the eIDAS adaptor. It includes a high level overview of the Correos and Atos environment.

### 3.1 “Correos Services Portal to integrate”

As stated within the “D2.1 LEPS Service Design Document” [1], the scope of the project is to integrate and eNotification (*My Notifications*) and an eDelivery service (*My Mailbox*). This integration goes through Correos ID, service based on *My Identity* IdP of Correos, and will allow European users coming from the eIDAS nodes to connect to the Correos Digital Services.

Below brief descriptions of the services mentioned before; for further information, the reader can refer to D2.1 [1]:

- **Correos ID - My Identity** (“*Mi Identidad*”): provides secured digital identities to citizens, businesses and governments (Figure 1). Therefore, acting as a trusted third party to validate identity attributes, raising third parties trust on individuals. It acts as a gateway eCorreos services and even non-Correos applications.



Figure 1: My Identity service

- **My Notifications** (“*Mis Notificaciones*”): is a digital service (Figure 2), within the eCorreos suite, aiming to centralize and manage governmental notifications for one or several individuals or legal entities.



Figure 2: My Notifications service

Document name:	D3.2 Operational and Technical Documentation of Correos services customization			Page:	10 of 28		
Reference:	D3.2	Dissemination:	PU	Version:	1.0	Status:	Final

- **My Mailbox** (“*Mi Buzón*”): is meant to be a space where citizens, companies and governments will be able to send & receive relevant documentation (like a digital version of the physical mailbox. Figure 3). Information will be stored with all legal guarantees & high security standards. Moreover, sender and receiver are validated and uniquely identified by Correos. Individuals can subscribe to any verified business/government agency to start receiving trusted information.

Even so this is only part of a whole suite of digital services, these represent the best fit sample to be used within the LEPS pilot. Plainly explained, Correos ID (and My Identity) is the gateway to My Notifications and My Mailbox. The last two represent different perspectives on the matter of using digitally trusted communications in between two parties.



Figure 3: My Mailbox service

### 3.2 “Register Use Case”

A detailed description of the registration process into the Correos services is provided next.

1. An unknown customer (not registered yet) tries to get access to the Correos website. Correos is offering the *users* the possibility to register with eIDAS network for a more secure and stronger authentication through eIDAS network provided by the LEPS project.
2. The user selects Register with eIDAS instead of Correos option.
3. Correos sends a Register Request (within the Open ID Connect Protocol) to the LEPS Adapter.
4. The LEPS Adapter shows to the user the list of attributes (mandatory and optional) needed by Correos. Before accepting or rejecting to disclosure the data, the user must provide the origin country (through a dropdown menu or an European map). Additionally this screen will provide links to SP general info, links to privacy matters for SP, LEPS and eIDAS regulation. See Figure 131 below.
5. Once the request is submitted, the LEPS Adapter creates and sends a **SAML Authentication Request** to the SP eIDAS node, containing the attribute names Correos needs and the user origin country.
6. The user is redirected to the origin country eIDAS node, which connect to the origin country IdP.
7. The IdP asks credentials to the user.
8. The user enters the eID card and the PIN.
9. The IdP authenticates the user and provides **SAML Authenticate Response** (with the attribute values) to origin country eIDAS node.
10. The SAML Authenticate Response reaches the SP eIDAS node through the eIDAS network.

Document name:	D3.2 Operational and Technical Documentation of Correos services customization			Page:	11 of 28		
Reference:	D3.2	Dissemination:	PU	Version:	1.0	Status:	Final

11. The SP eIDAS node redirects the user to the LEPS Adapter providing the SAML Response.
12. LEPS Adapter checks and manages the SAML Response, providing a signed **JWT** (OAuth 2.0 with Open ID Connect) to the Correos SP with the user info and set a valid user session.
13. The user is redirected to the register page provided by Correos. The user fills-in the remaining fields Correos needs for a full registration.
14. Correos registers the user in the system (Correos: to discuss).

The steps 5 to 11 are out of the scope of the integration process.

### 3.3 “Login Use Case”

---

1. A detailed description of the login process into the Correos services is provided next. An already registered customer tries to get access to the service website provided by Correos. Correos provides to users achieving strong authentication using eID through eIDAS network.
2. The user selects login with LEPS instead of Correos login (to be still discussed and determined if such a button will be the same one).
3. Correos sends an Authentication Request to the eIDAS (LEPS) Adapter.
4. From now the follow the steps 4 to 12 from the Register scenario.
13. Once the LEPS Adapter provides the user info through a signed **JWT** (OAuth 2.0 with Open ID Connect) to Correos, the user validation process will check the attributes provided.
14. The user gets access to the services provided by Correos.

### 3.4 “Metrics”

---

As a result of the several meetings held between the Correos and Atos during the development of task 3.2, has been agreed to use the following user credentials for the testing phases, and the number of users involved during the integration process:

- Test credentials will be used for the first phase.
- Real credentials must be used for the second phase.
- The number of users testing the integration will be more than 5 people, taking into account the developers and testers from Correos and Atos.

### 3.5 “Correos Services Requirements”

---

This section describes the compiled requirements from the Correos services customization, and the Correos Identity reconciliation needed after the integration with eIDAS Network will be made.

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	12 of 28		
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

The following general requirements generated in Activity 2 Business Requirements, Integration and Testing Planning document [1] (to be submitted at the end of the project) will affect the Correos services customization and are covered by this pilot:

The list of user attributes required by MyIdentity service for a natural person from eIDAS network includes:

- Name
- Surname
- Person identifier
- Date of Birth

Optional data such as user address or fiscal code can be requested, but its availability will depend on the eIDAS infrastructure. The format of the message as will be seen below will be prepared to provide all optional attributes to Correos.

The specific requirements compiled from the Correos services are indicated in Table 1:

**Table 1: SP Requirements**

Number	Name	Description
SPR-1	Attributes	eIDAS infrastructure <b>MUST</b> provide name, surname, person identifier, fiscal code and date of birth as attributes to complete the register and the login processes. eIDAS infrastructure <b>MAY</b> provide additional user data such as address or fiscal code if user gives consent and the eIDAS platform is able to provide.
SPR-2	Adapter	eIDAS adapter <b>MUST</b> provide a connector to eIDAS infrastructure in order to retrieve user attributes to SP.
SPR-3	Authentication request	SP <b>MUST</b> 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.

### **Correos Identity reconciliation**

Once the integration will be done, there are specific requirements regarding the users accounts and attributes reconciliation.

If it is the first time the user connects to the service, a new account will be created with the information received from the eIDAS adaptor plus the information required by the system and that has to be fulfilled in a specific form of the app.

Further on, after registering is done, Correos infrastructure will check whether the eIDAS identifier exists within the system and is associated to an account or not. When associated already, system will check if information has been updated; if so, system would do so too.

Additionally, it will be analysed within the project how to treat the verified attributes coming from eIDAS, “against” the attributes verified by My Identity Correos service. It has to be thought and

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	13 of 28		
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

analysed, as the LoA affects which attribute might be saved and which information may be prioritized over previous information loaded.

### 3.6 “Technical infrastructure preparation”

Following subsections describe the architecture of the Correos services portal and how the Correos services are integrated with the eIDAS infrastructure. Also, technical details about the infrastructure preparation in Correos environment are provided and finally how the different components have been deployed is described.

#### 3.6.1 “Architecture”

Figure 4 shows a general view of the eIDAS-Correos service portal integration architecture containing the different components involved in the process. Red dotted line remarks the scope of this task 3.2 in the context of Activity 3.

- The SP domain contains the services to be integrated with the eIDAS network: MyIdentity, MyMailbox and MyNotifications.
- The eIDAS adapter provided by the LEPS project, which will connect the services with the eIDAS network
- The IdP domain contains the eIDAS nodes from the SP country and the Citizen country, namely Spain and Greece respectively. The IdP domain is out of the scope of this deliverable.

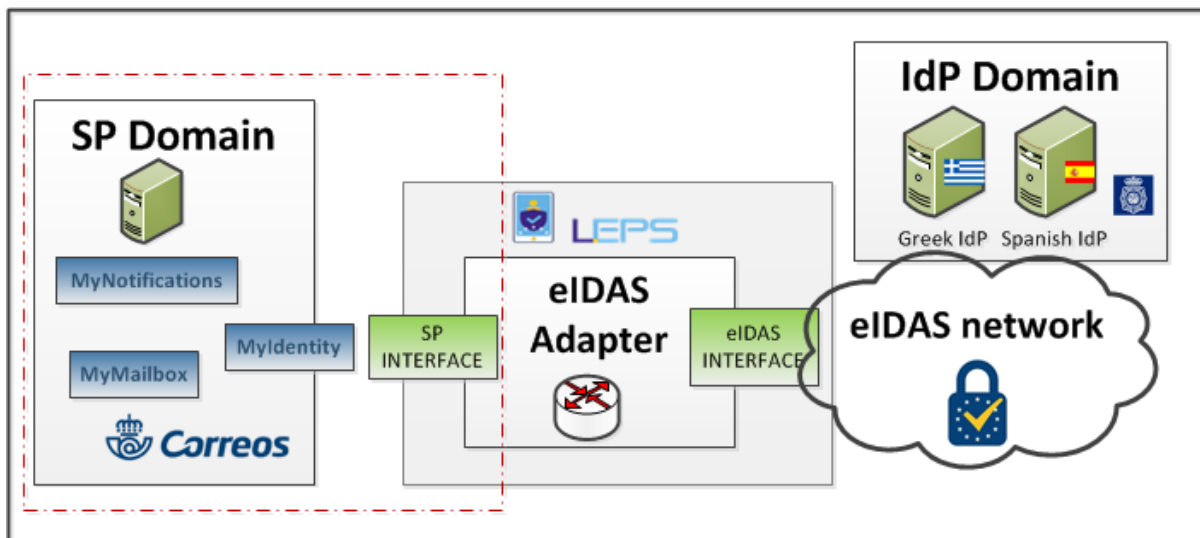


Figure 4: Architecture General Overview

#### 3.6.2 “Environment”

The integration of Correos services with the eIDAS network comprises two environments:

- Correos environment, where the selected services are currently deployed;

Document name:	D3.2 Operational and Technical Documentation of Correos services customization	Page:	14 of 28	
Reference:	D3.2	Dissemination:	PU	
	Version:	1.0	Status:	Final

- eIDAS Adapter environment, where the adapter will be running. Depending on the SP needs and requirements, the adapter could be deployed at SP environment (in this case the Correos infrastructure) or outside. As the eIDAS adapter is developed by Atos, for the integration process has been decided to run the adapter on the Atos infrastructure. This will ease the integration development in order to speed the bug fixing process and the future integration with the eIDAS infrastructure.

### 3.6.2.1 Correos Environment

Within a secured cloud-based platform, the Correos digital services are hosted under a .post domain. .Post project was developed with high standards of security (including DNSSEC) and sponsored by the Universal Postal Union (UPU) agency of the United Nations.

The environment includes usage of OTPs and a specification of *OAuth2* with *Open Id Connect*. Interaction within the Correos digital services suite or external apps is done using specific APIs. Bearing this in mind, it was offered a public development URL for interacting with the adaptor using JWT messages.

### 3.6.2.2 eIDAS adaptor environments (at ATOS and on-premises)

With the aim to facilitate the development and deployment of the eIDAS adaptor, Atos has created and deployed the adapter leveraging the following technologies:

- The eIDAS adapter offers an interface to MyIdentity service as Spring Boot<sup>8</sup> REST endpoint;
- The adapter is deployed as a Docker<sup>9</sup> container to improve portability and fast deployment;
- Server used runs on Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86\_64);
- Server features:
  - RAM : 16 GB System memory;
  - Processor: Intel(R) Xeon(R) CPU E5645 @ 2.40GHz;
  - HD: 40 GB memory;

<sup>8</sup> <https://projects.spring.io/spring-boot/>

<sup>9</sup> <https://www.docker.com/>

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	15 of 28		
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

## 4 “Customization Implementation”

This section describes the interfaces developed for the integration of the Correos services with the eIDAS adapter and a time plan for the process performance.

As part of the implementation there are two differentiated sets of interfaces.

### 4.1 “Customization time plan”

For the development of the customization of the Correos services, the activities needed were scheduled and the following time plan depicted in Table 2 was created.

**Table 2: Customization Time plan**

Phase	Task	Deadline
Pilot preparation	<ul style="list-style-type: none"> <li>Use case description and pilot scope definition</li> <li>Number of users and metrics definition</li> <li>Requirement definition. Attributes needed. Privacy matters</li> </ul>	December 2017
Pilot infrastructure preparation	<ul style="list-style-type: none"> <li>Set up pilot environment: server, service.</li> <li>Interfaces definition between pilot and LEPS adapter</li> </ul>	January 2018
Piloting	<ul style="list-style-type: none"> <li>Interfaces implementation + Integration on LEPS platform</li> <li>Start testing</li> </ul>	January/February 2018
Test and validation	<ul style="list-style-type: none"> <li>Data Collection and analysis based on defined metrics</li> </ul>	February 2018

### 4.2 “Interface definition”

#### 4.2.1 Correos Digital Services

Within the context of the project, it was necessary to develop several changes on the main “screens” or interfaces of Correos ID (My Identity). Below a brief description of the changes/implementations done:

##### **Sign-in interface:**

A button is added for registration/authentication. This button sends a message to the specifically developed component MyIdentity-eIDAS that generates the message and redirects to LEPS adaptor. Image shown below is not final, just as an example of future look.

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	16 of 28
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final









In the token is included the following data:

- Sub: containing the PersonIdentifier.
- State: Information included in the token and has to be given back untouched.
- redirectUri: address to which the LEPS adaptor has to answer back.
- aud: identity of the receiver of the token.
- nbf: Date since when the token is valid.
- exp: Date until when the token is valid.
- iss: identity of the creator of the token (My Identity).
- iat: date and time of creation of the token, in this case will be the same as the claim nbf.
- jti: message identifier.
- nonce: security string created to avoid “reply-attacks”. It has to be given back.
- given\_name: CurrentGivenName.
- family\_name: CurrentFamilyName.
- Birthdate: DateOfBirth.
- Gender.
- Loa: Level of Assurance (LoA) with one of the following values:
  - low.
  - substantial.
  - High.
- Address: CurrentAddress, with the structure:
  - locator\_designator: LocatorDesignator.
  - street\_address: Thoroughfare.
  - Locality: PostName.
  - postal\_code: PostalCode.

### Sign-in/Sign-up interface:

The following interface shows the check of email that will decide whether is a sign-in or a sign-up in My Identity. The button shown is just an example, final UI is to be decided.



Figure 11: My Identity protected page

Document name:	D3.2 Operational and Technical Documentation of Correos services customization			Page:	20 of 28		
Reference:	D3.2	Dissemination:	PU	Version:	1.0	Status:	Final

## 4.2.2 eIDAS Adapter

The API implemented by ATOS has the next endpoint to allow MyIdentity service to make a redirect authentication request:

/eIDASconn/connector/authenticate/

In Figure 12 is depicted the Swagger<sup>10</sup> specification for this endpoint.

**eIDAS-SP**

**POST** /connector/authenticate/

Endpoint for starting the authentication process against eIDAS infrastructure. Offers to the user a screen where the attributes requested are listed.

**Response Class (Status 200)**  
Authentication successfull

Model

```
{
  "token": "string"
}
```

**Parameters**

Parameter	Value	Description	Parameter Type	Data Type
token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwIiwibmFTZ....	A JWT with the authentication request info from the SP	formData	string

**Response Messages**

HTTP Status Code	Reason	Response Model	Headers
201	Created		
206	Authentication successfull. Some optional attributes are not provided	Model	
		<pre>{   "token": "string" }</pre>	
400	Missing/invalid properties		
401	Authentication failed		
403	Invalid identifier		
404	Not Found		
406	Invalid signature		
415	Unsupported media type. Only 'application/json' or 'application/xml' is supported		
502	Authentication failed due to server problems		

**Figure 12: eIDAS adapter REST endpoint**

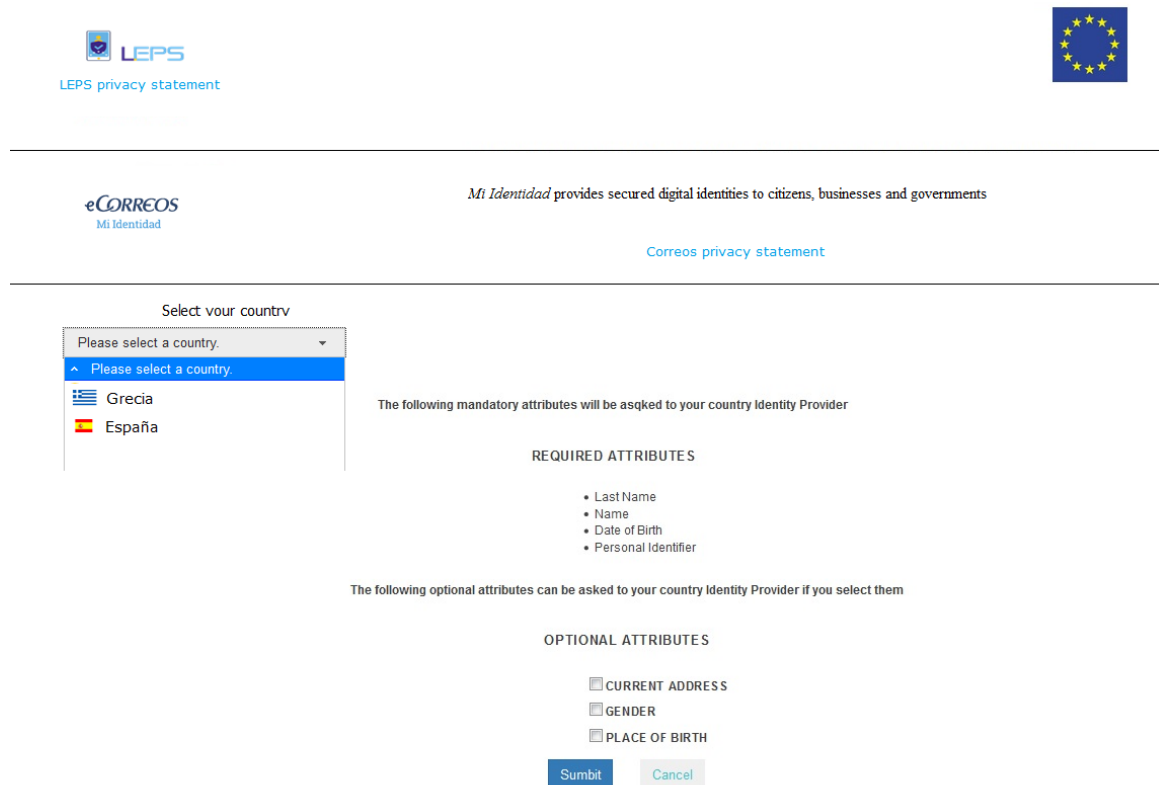
The signed JWT provided by MyIdentity is included in the body POST request.

Once the JWT is validated and the list of attributes, among other information, is extracted, the adapter shows the user the following page, displaying the list of mandatory attributes the My Identity service needs for user authentication, beside a list of optional attributes the service asks for user consent to delivery. The user can select all, some of them or none. The user is also requested to provide the origin country and finally click on the Submit button to trigger the cross-border authentication process or Cancel the operation.

<sup>10</sup> <https://swagger.io/>

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	21 of 28
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final

Links to the privacy policy from My Identity service and LEPS project are provided. All of these elements can be shown in [Figure 13](#).



The screenshot shows a user interface for selecting a country. At the top left is the LEPS logo and 'LEPS privacy statement'. At the top right is the European Union flag. Below this is the eCORREOS logo and 'Mi Identidad' text. In the center, it says 'Mi Identidad provides secured digital identities to citizens, businesses and governments' and 'Correos privacy statement'. The main content area is titled 'Select your country' and features a dropdown menu with 'Please select a country.' and options for 'Grecia' and 'España'. To the right of the dropdown, it states 'The following mandatory attributes will be asked to your country Identity Provider' and lists 'REQUIRED ATTRIBUTES': Last Name, Name, Date of Birth, and Personal Identifier. Below this, it says 'The following optional attributes can be asked to your country Identity Provider if you select them' and lists 'OPTIONAL ATTRIBUTES': CURRENT ADDRESS, GENDER, and PLACE OF BIRTH. At the bottom are 'Submit' and 'Cancel' buttons.

Figure 13: Screen displayed to the user by the eIDAS connector

When the eIDAS adapter receives the SAML request from the Spanish eIDAS node, redirects the user to the requested service and provides a signed JWT token to My Identity service containing the user information. The content is shown in Figure 14. The exact content is hidden for security reasons but the structure displayed follows the real JWT structure.

Document name:	D3.2 Operational and Technical Documentation of Correos services customization			Page:	22 of 28		
Reference:	D3.2	Dissemination:	PU	Version:	1.0	Status:	Final

```

HEADER: ALGORITHM & TOKEN TYPE
{
  "alg": "HS256",
  "typ": "JWT"
}

PAYLOAD: DATA
{
  "iat":
  "sub": "ES/ES/123456A",
  "given_name": "Juan",
  "family_name": "Perez",
  "birthdate": "1990-06-21",
  "gender": "Male",
  "nonce":
  "jti":
  "nbf": 1517267450,
  "exp": 1517269250,
  "iss":
  "aud":
  "address": {
    "locator_designator": "25",
    "street_address": "Albarracin Calle",
    "locality": "Madrid",
    "postal_code": "28037"
  },
  "state": {
    "state": null,
    "policy":
    "client_id":
    "nonce": "defaultNonce",
    "redirect_uri": '
    "scope": "openid",
    "response_type": "id_token"
  }
}

```

Figure 14: JWT content

### 4.3 “Integration flow”

Figure 15 displays the complete flow for the integration process. This flow is based on the registration use case and login use case described in section 2.2 and section 2.3 respectively. The screens displayed to the user can be seen in section 3.2.1 and section 3.2.2. It is also included the steps where the eIDAS nodes are involved for a better understanding of the authentication process, but are out of scope of this task.

Document name:	D3.2 Operational and Technical Documentation of Correos services customization			Page:	23 of 28		
Reference:	D3.2	Dissemination:	PU	Version:	1.0	Status:	Final

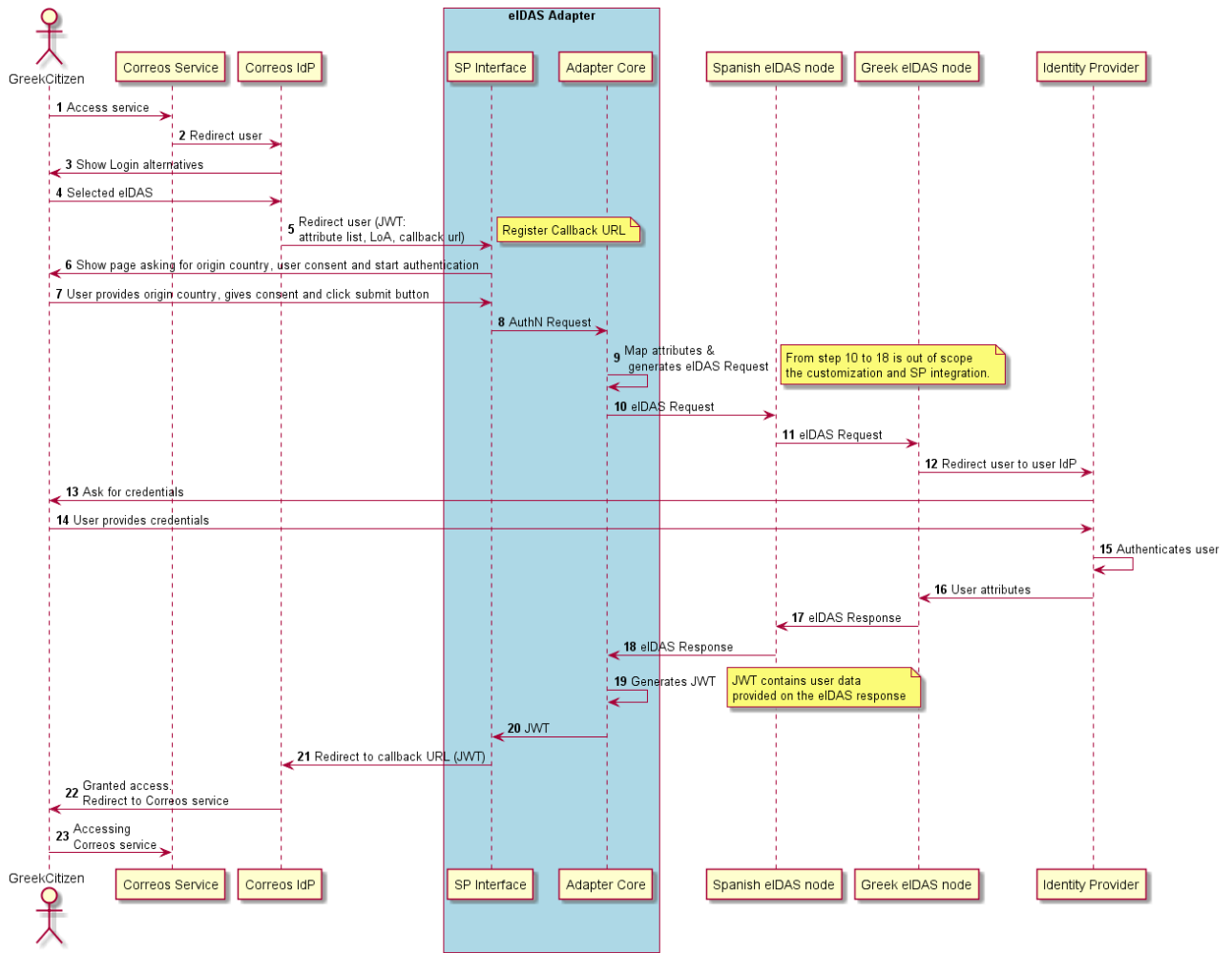


Figure 15: Integration flow

Document name:	D3.2 Operational and Technical Documentations of Correos services customization	Page:	24 of 28
Reference:	D3.2	Dissemination:	PU
	Version:	1.0	Status:
			Final



## 5 “Tests”

This section gives a description of tests performed during the integration process. Two phases has been scheduled, an initial test phase in pre-production environment and a second one on a more realistic environment<sup>11</sup>. Test cases have been described for this purpose.

Test made included daily controls reviewed in a weekly basis on a team meeting. There were two technical users testing and two functional analysts per team (Correos & Atos) to review periodically the flow of the integration (including both UX and UI).

Testing of the integration was done within 2 frameworks

- Internally with a self-created mock-up simulating the eIDAS answer (either the adaptor or the nodes themselves).
- Asynchronous test with the adaptor, sending the communication request and confirming by email with ATOS the reception of the token. Is yet to be tested a bilateral communication.

Once the nodes are integrated with the adaptor, further and more realistic tests will be done.

### 5.1 “Test Cases Definition”

With the aim to develop the testing phase of the customization and integration of the Correos services into the eIDAS infrastructure a set of test cases has been defined:

These test cases involve a user accessing My Mailbox and/or My Notifications web services.

**Table 3: TC1: New user tries to log in on Correos services**

Description	Expected Response	Remarks
A non-registered user tries to access My Mailbox or My Notification service. None authentication was performed before, so there is no session stored for the user. CorreosID/My Identity service offers to the user the possibility to authenticate through the eIDAS infrastructure among others. The user	Once the user clicks on the eIDAS button, she is redirected to eIDAS adapter. eIDAS adapter will show to the user a page containing the list of mandatory and optional attributes requested by Correos. A dropdown menu including the available countries on eIDAS infrastructure is also displayed. Additionally links to privacy policy from Correos and LEPS project are provided  The user selects her country and checks the optional attributes she wanted to share with the SP. Then she clicks on the Submit button for accepting eIDAS authentication.  The user authentication is mocked-up and the user	eIDAS adapter provides a JWT to My Identity service with all requested user attributes.

<sup>11</sup> At this moment we are waiting for the availability of the production environment for the Spanish eIDAS node.

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	25 of 28
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
		<b>Status:</b>			Final

Description	Expected Response	Remarks
tries to log in through eIDAS and start using one of the services.	<p>is redirected to My Identity service.</p> <p>As this is the first time the user access the Correos services, a form is shown to the user for filling the additional information that is not provided by the eIDAS nodes. If the user already had an account of CorreosID, both accounts will be linked and no information will be needed to fulfil.</p> <p>Once the registering process is done, the user is redirected to the specific service that was trying to access.</p>	

**Table 4: TC2: Existing user tries to log in on Correos services**

Description	Expected Response	Remarks
<p>An already registered and eIDAS-CorreosID linked user access My Mailbox or My Notification service. None authentication was performed before, so there is no session stored for the user. My Identity service offers the user the possibility to authenticate through the eIDAS infrastructure among others. The user tries to log in through eIDAS and complete a transaction.</p>	<p>Once the user clicks on the eIDAS button, she is redirected to eIDAS adapter. eIDAS adapter will show to the user a page containing the list of mandatory and optional attributes requested by Correos. A dropdown menu including the available countries on eIDAS infrastructure is also displayed. Additionally links to privacy policy from Correos and LEPS project are provided</p> <p>The user selects her country and checks the optional attributes she wanted to share with the SP. Then she clicks on the Submit button for accepting eIDAS authentication.</p> <p>The user authentication is mocked-up and the user is redirected to My Identity service.</p> <p>Once the user login is validated by My Identity the user is redirected to the specific service.</p>	<p>eIDAS adapter provides a JWT to My Identity service with all requested user attributes.</p>

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	26 of 28
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final

## 6 Conclusions

Correos has successfully created the pages to be shown to the users in order to access the selected services, including the eIDAS button option for authentication.

The CorreosID/My Identity service has successfully been adapted to the registration and login processes using eIDAS infrastructure:

- Generating a simple authentication request to the eIDAS adapter using JWT (OAuth 2.0 with Open ID Connect);
- Adapting the Correos registration process accepting the minimum data set eIDAS infrastructure provides and completing the additional information with a form filling when signing up;
- Creating an endpoint for receiving the user information provided by the eIDAS adapter through a JWT (OAuth 2.0 with Open ID Connect).

The eIDAS adapter successfully developed by Atos has performed the following tasks:

- Created the REST service interface for the integration with My Identity service, receiving the Correos authentication request.
- Created the page shown to the user which includes the list of mandatory and optional attributes requested by Correos services and asking the user consent for proceeding with the eIDAS authentication process;
- Generating a simple authentication response to My Identity service through a JWT (OAuth 2.0 with Open ID Connect).

The time plan scheduled in section 3.1 has been followed with no significant deviations, allowing performing the testing phase on time. Thus, Correos and Atos have tested the integration process between My Identity service and the eIDAS adapter performed successfully the test use cases described in section 4.1. Meaning that the oncoming phase for the final integration with the Spanish eIDAS node is ready to be completed.

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	27 of 28		
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

## References

- [1] LEPS deliverable lead author (Petros Kavasalis) (ed.):, D2.1 LEPS Service Design Document. Deliverable of the LEPS project will be submitted in September 2018.
- [2] [CEF Telecom-European Commission], [Connecting Europe Facility],[<https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom>], [retrieved on 2018/02/21]

<b>Document name:</b>	D3.2 Operational and Technical Documentation of Correos services customization			<b>Page:</b>	28 of 28		
<b>Reference:</b>	D3.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final