Leveraging eID in the Private Sector

M5 & M9 - Mobile ID App and its integration results with the Industrial Partners

Document Identification			
Status	Final	**Due Date**	May/June 2018
Version	1.0	**Submission Date**	12/07/2018

Related WP	Activity 3.4,5	**Document Reference**	ML5&9
Related Deliverable(s)	D3.2, D3.3, D4.1, D5.1, D4.2	**Dissemination Level (*)**	PU
Lead Participant	UMU	**Lead Author**	Elena Torroglosa
Contributors	ATOS Correos UAEGEAN ELTA ATHEX	**Reviewers**	ATOS
			UAEGEAN
			NTUA

Keywords:
eIDAS, mobile authentication, Android, NFC, eID, DNIe 3.0, integration tests

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
Elena Torroglosa	UMU
Antonio Skarmeta	UMU
Juan Carlos Pérez Baún	ATOS
M. Nuria Ituarte Aranda	ATOS
Javier Salazar	Correos
Carlos Balot	Correos
Harris Papadakis	UAegean
Petros Kavassalis	UAegean
John Belafas	ATHEX
George Christakeas	ATHEX
Stelios Sifnaios	ELTA
Thomas Macheras	ELTA

Document History			
Version	Date	Change editors	Changes
0.1	18/01/2018	UMU	Initial ToC
0.2	14/03/2018	Atos	Comments on ToC
0.3	23/05/2018	Correos	Comments & information added on draft.
0.4	24/05/2018	ATOS	Updated sections: 2.1 eIDAS architecture, 2.2 eIDAS authentication, 4.2 Requirements, Acronyms and References.
0.5	30/05/2018	UMU, UAegean	New content. New ToC for chapter 8 and 9
0.6	11/06/2018	UMU	Sections 5 and 6
0.7	26/06/2018	UMU	ELTA, ATOS, UAegean contributions, section 8, Introduction and Conclusions
0.8	02/062018	UMU, ELTA, ATHEX, Correos, UAEGEAN	Chapter 9
0.9	03/07/2018	UMU	Final version pre-revision
0.91	06/07/2018	UAegean-ATHEX, NTUA, ATOS	Review
0.92	09/07/2018	UMU	Final version candidate
0.99	11/07/2018	ATOS	Final review and quality
1.0			FINAL VERSION TO BE SUBMITTED

Table of Contents

List of Figures

List of Tables

List of Acronyms

Abbreviation / acronym	Description
ATHEX	Hellenic Exchanges - Athens Stock Exchange S.A.
EC	European Commission
CEF	Connecting Europe Facility
Dx.y	Deliverable number y belonging to Activity x
DNIe	Documento Nacional de Identidad electrónico (electronic Identity National Document)
eID	electronic IDentification
eIDAS	electronic IDentification, Authentication and trust Services
ELTA	Hellenic Post S.A.
FNMT	Fábrica Nacional de Moneda y Timbre
HMIAR	Hellenic Ministry of Administrative Reconstruction
IdP	Identity Provider
LoA	Level of Assurance
MS	Member State
NFC	Near Field Communication
NTUA	National Technical University of Athens
SAML	Security Assertion Mark-up Language
SP	Service Provider
UAEGEAN	University of the Aegean
UMU	University of Murcia

Executive Summary

Milestone 5+9 contains the description of the work performed within LEPS Project Task 3.1, Mobile authentication. The main objective of the Task 3.1 is to offer mobile support for Greek SP (Service Provider) services (ATHEX Group and ELTA) to enable authentication of Spanish citizens, using the eIDAS (electronic IDentification, Authentication and trust Services) infrastructure and Spanish DNIe 3.0 (electronic Identity National Document). The performed work on Task 4.4 and Task 5.4, Mobile Authentication, has been also included in this document.

This document describes the tasks of analysis, design and development of a mobile solution for eIDAS-based authentication that covers all principles and requirements of LEPS project, proposes guidelines for the installation and use of the developed solution designed and reports on initial integration and testing results of the eIDAS mobile authentication with pilot services, offered by Greek and Spanish SPs.

It is important to highlight that the resulting mobile application is SP agnostic and can work any SP offering eIDAS authentication for Spanish users. Additionally, other authentication methods beyond the Spanish DNIe could be easily integrated in the same code base, thus extending the implementation of the application to other EU Member States.

Given the generic properties of the developed solution, the requirements for SPs to integrate the mobile application are practically minimal and limited to the global requirements of operating in a mobile environment, i.e. providing responsive interfaces and use standard components such as HTML and JavaScript.

Finally, the process of integration and testing of the mobile application with real services demonstrates the compatibility and inter-operation capacity of the application with different service technologies, the eIDAS infrastructure and Spanish authentication methods. The performed integration tests of the mobile application with the services provided by each partner are satisfactory. The services work according the defined specifications and the authentication process through the eIDAS infrastructure, by using username/password, software certificates and the Spanish DNIe 3.0, is executed successfully, returning appropriately the expected authentication information to the intermediate eIDAS nodes as well as to the end-services.

1 Introduction

LEPS Project (Leveraging eID in the Private Sector) is developed under the Connecting Europe Facility (CEF) in the objective of contributing to the development of the EU Digital Single Market (DSM).

The main project's objectives are to allow existing SP services, such as e-Delivery and e-Notifications (Correos Group), e-Delivery, portal, e-shop and b2b postal services (ELTA - Hellenic Post S.A.) and signing and portfolio monitoring services (Athens Exchange Group), to use the pan-European eID (electronic Identification) infrastructure for cross-border electronic identification and authentication. LEPS offerings use eIDAS (electronic IDentification, Authentication and trust Services) specifications and rules, to connect the IT infrastructure of the project end-users to the eIDAS Network, thus demonstrating the usability of eIDAS specifications and their applicability in the private sector. LEPS offerings improve the interconnection of Services Providers to eIDAS Network with a number of supporting tools and services (a mobile interface for authentication attributes delivery and APIs for interconnection to eIDAS Nodes), demonstrate and test the effective use of the above-mentioned extensions across borders, against the eIDAS core service platform production environment, and provide guidelines for the application of these supporting tools and services to other countries. As a result, LEPS project contributes to increase eID uptake and use in the private sector and improve eIDAS interconnection service sustainability through several road mapping studies and policy guidelines, and the diffusion of results to other EU Member States (MS).

With these aims, the project follows the principles of interoperability and interconnection service flexibility while offering strong means of secure electronic identification and authentication, based on the legal framework provided by the eIDAS Regulation and the eIDAS Network.

This project integrates with the eIDAS Network electronic services from two postal services companies in Spain and Greece (Sociedad Estatal de Correos y Telégrafos S.A. and Hellenic Post - ELTA), thus opening a path to deliver cross-border eIDAS-compliant trust services, based mostly on eDelivery, another CEF building block (eventually in the perspective of becoming Qualified Trust Service Providers). Another SP in Greece, Athens Exchange Group, offers to EU customers the possibility to register for a remote electronic signatures service via eIDAS and to monitor a portfolio of actions. In all cases, private sector services develop commercial solutions by leveraging the potential of eIDAS established substantial/high levels of authentication assurance and the effective interoperability of mutually recognised means of electronic identification and authentication which are available in the different EU Member States.

This document is focused on explain how LEPS has solved the problem of eIDAS authentication and service integration in a mobile environment, following and adapting the guidelines of the project, which are:

- Improved online service and customer experience offering a mobile solution adapted to the new market;
- Substantial savings through the design of reusable and generic components;
- Data quality as the key attributes related to identity that are transported cross-border are certified by official MS eIDAS node and obtained from authoritative sources;
- Following the eIDAS Regulation [11] that provides the needed legal certainty and common legal basis for Member States to recognise and accept eID means issued in other Member States.

With this aim, it is necessary the development of a user mobile interface for authentication-attributes delivery management. This task is mainly in charge of the Spanish members of LEPS Consortium with University of Murcia (UMU) being the responsible partner for the development of the mobile eID application. In Greece, University of the Aegean (UAEGEAN) works with Hellenic Ministry of Administrative Reconstruction (HMIAR) and National Technical University of Athens (NTUA) to make all the necessary modifications of the Greek eIDAS node to support mobile ID enable citizen/customer authentication. They provide also support to the two Greek private companies participating in the LEPS Consortium the Hellenic Post S.A. (ELTA) and the Athens Stock Exchange S.A. (ATHEX) to update their infrastructures, so to interconnect with LEPS mobile eID app.

In addition to the interoperation with the eIDAS infrastructure, the mobile interface must offer support to the Spanish eID card. The DNIe 3.0 (electronic Identity National Document) is the new version of Spanish identity card [9], which makes use of near field communication (NFC) technology to facilitate its use in smartphones and tablets, is certified as a valid form of identification using an electronic signature, giving it the same juridical value as a signature on paper.

The use of smartphone and tablets in the use interaction with public administrations and private companies becomes in those days an increasingly common practice, therefore it is necessary to offer mobile solutions that integrate mobile eIDAS authentication in the SP service ecosystem. The design of an efficient solution for mobile devices can be the key for a successful adoption by both companies and users who use their services.

1.1 Purpose of the document

The objective of the eIDAS Mobile Authentication Task is to offer mobile support for Greek services to authenticate Spanish citizens, using the eIDAS infrastructure and their Spanish DNIe 3.0, when they access to Greek services.

This document includes the process of analysis, design and printing of a mobile solution that covers all the requirements and principles of the LEPS project, as well as a guide to the installation and use of the solution designed and the first results of the integration and testing process with the pilot services, both Greek and Spanish.

1.2 Relation to another project work

The Mobile Authentication Task is transversal to most of the other project tasks since it requires the interaction with adapted Greek services (D4.1 and D5.1 [8]) and eIDAS adaptors (D3.3 [7]) as well as works with several eIDAS nodes and identity providers.

These characteristics make this Task a valuable component of all project tasks and a reference to evaluate the current state of the project.

1.3 Structure of the document

This document is structured in 10 major chapters:

Chapter 2 presents the eIDAS overview including the architecture, the Greek and Spanish authentication methods and the services integrated with eIDAS in this project by industrial partners.

Chapter 3 presents the description of the eIDAS Mobile Authentication Scenario with the requirements derived from eIDAS architecture and components.

Chapter 4 presents a detailed analysis of possible approaches to solve the mobile authentication problem.

Chapter 5 presents the mobile application technical design of the chosen solution including the use case description, the user interface and internal designs.

Chapter 6 presents the mobile application implementation details.

Chapter 7 presents the guides and tools to install and test the mobile application.

Chapter 8 presents the description of the adaptation requirements for SPs.

Chapter 9 presents the initial results of the integration and preproduction tests of the mobile application with the SPs.

Chapter 10 presents document conclusions.

2 eIDAS Overview

This section provides a general overview of eiDAS infrastructure and a short description of the components, also a description of the authentication flow through eIDAS network and finally a summary of the services provided by Correos integrated with the eIDAS infrastructure.

2.1 eIDAS architecture

eIDAS infrastructure is based on CEF building blocks provided by the EC (European Commission) [1]. The CEF eID building block is the basis for the web authentication and allows both public and private companies to use the eID card for cross-border authentication purposes when a user, holder of such an eID card in one country, accesses digital services provided by other European countries.

In the case of LEPS project the eIDAS network will allow private SPs, such as Correos, ELTA and ATHEX to extend the use of their digital services to European citizens beyond Spain and Greece.

Figure 1 depicts the eIDAS basic infrastructure [2], the main stakeholders and the building components.

The main stakeholders involved are:

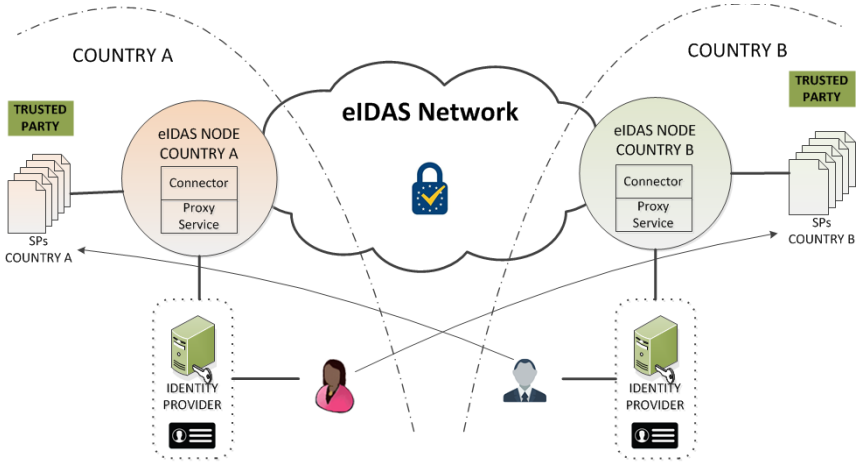


Figure 1: eIDAS Architecture

- The trusted parties: the SPs;
- The citizens: the users trying to access services provided by the SPs;
- The Identity Providers (IdPs): in charge of authenticate the citizens, supporting the national eID scheme;
- eIDAS node: the interconnected country eIDAS nodes in charge of the cross-border authentication.

A circle of trust is created between the different stakeholders, therefore each country eIDAS node establishes a trust relationship with the different European nodes under the umbrella of the eIDAS regulation [3] and the guidelines provided by the EC. The country eIDAS nodes are allowing the digital services across Europe to use the national eID schemas [4].

In order to the SPs allow the citizens get access to the provided digital services, it will be necessary to generate an authentication request triggered by the SP. With the aim to facilitate the SP integration with the eIDAS network and in order to avoid additional effort during the SP integration process, an intermediary component called eIDAS adapter has been developed. More information about technical details on eIDAS adapter can be found on document D3.2 [5] and D3.3 [7]. This eIDAS adapter will act in behalf of the SP receiving the authentication request from the SP and translating this request in a SAML 2.0 (Security Assertion Mark-up Language) request the eIDAS node understand, this new component is depicted in Figure 2.

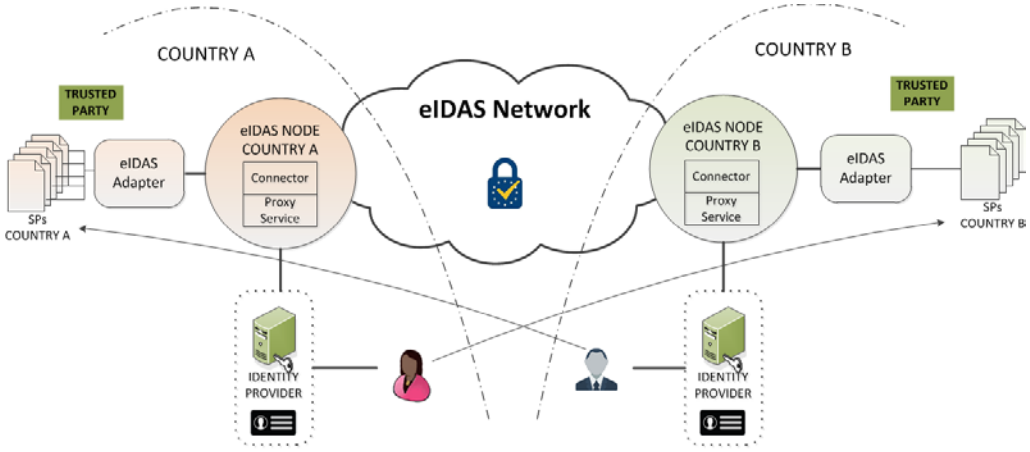


Figure 2: eIDAS Architecture in LEPS

Therefore, when the citizen from the country B, tries to get access a SP from the country A, is recognized by the adapter, and an authentication request is sent to the eIDAS node from country B through the eIDAS network. the citizen is redirected to the IdP located in the country B to authenticate. In the following section is provided a more detailed description of the authentication process.

2.2 eIDAS authentication

As indicated in previous section the cross-border authentication is performed through the eIDAS nodes. Each node contains two elements [2]:

- The eIDAS connector: in charge of request the cross-border authentication, acting on the eIDAS node from the country SP requesting the authentication;
- The eIDAS service in charge of provide a cross-border authentication (personal identification data), acting on the eIDAS node from the country user. There are two alternatives for this service the Proxy service and the Middleware service.

In the case of the countries involved in the LEPS project (Greece and Spain) the cross-border authentication will be Proxy to Proxy [6] is depicted in Figure 3.

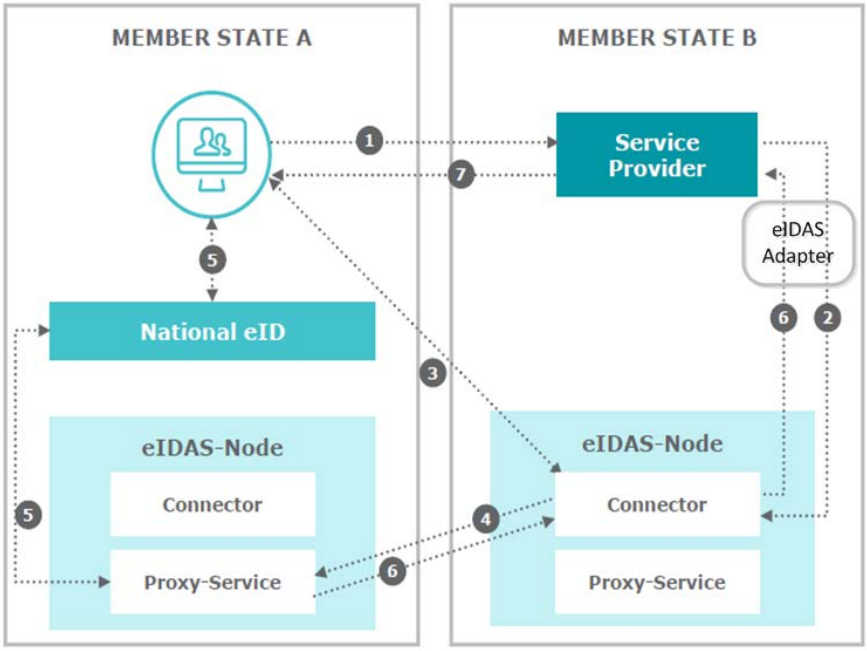


Figure 3: eIDAS Authentication Process in LEPS [6]

A detailed description of the process follows.

1. A citizen of country A requests access to a SP in country B.
2. The SP in country B sends the custom authentication request to the adapter, which sends the SAML request to the eIDAS Connector.
3. Once the request reaches the node, the Connector asks the citizen for their country of origin (this step can also be made on the Adapter component).
4. After the country of origin is selected by the citizen, the SAML Request is forwarded by the Connector to the eIDAS-Node Proxy Service of the citizen's Member State
5. The eIDAS-Node Proxy Service sends the SAML Request to the Identity Provider for authentication. The citizen authenticates using their eID. Once authenticated, this identity (personal data) is returned to the eIDAS-Node Proxy Service. Depending on the implementation there may be two additional steps within step 5:
    a. for the citizen to select the attributes to be provided (therefore given consent)
    b. for the citizen to agree the values of the attributes to be given.
6. The eIDAS-Node Proxy
7. Service sends a SAML Assertion to the requesting Connector, which forwards the response to SP through the Adapter.
8. The SP grants access to the citizen.

2.2.1 Spanish eIDAS authentication

The Spanish eID schema is based on a single IdP, the Spanish Policy. Spanish eIDAS IdP focuses the offered authentication methods on X.509 certificates that covers the high-level security requirements of eIDAS infrastructure. This kind of certificates can be stored by different methods such as P12 files, the

operating system or web browser keystore or even in physical devices like security (smart) cards (e.g. Spanish DNIe and DNIe 3.0). Below is a detailed description of this technologies.

2.2.1.1 Certificates

Client X.509 certificates installed or available on the Android device issued by the official Spanish CA (FNMT - “Fábrica Nacional de Moneda y Timbre”). The certificates are used to authenticate users at their national identity providers in the eIDAS platform.

2.2.1.2 Spanish DNIe 3.0

The first version of Spanish Electronic Identity National Document (DNIe) was presented in 2006. Physically it is a plastic card similar in size and shape to bank payment cards and with a chip where the digital certificate of the user is stored [9].

DNIe 3.0 [10] is the updated version of DNIe. Its main novelty (and advantage) is its compatibility with NFC technology, available on smartphones and tablets, which allows wireless reading of their content for identifying user in administrative formalities, payments, etc. [9]

2.2.2 Greek eIDAS authentication

The Greek eIDAS infrastructure offers two identity providers, one at the production level and another one at the pre-production level. The Ermis IdP (on the production level) provides authentication information from the Taxisnet system. The user is authenticated using his/her ERMIS credentials (username/password). As a result, the LoA (Lever of Assurance) offered by Ermis IdP is “low”. On the pre-production level, the ATHEX IdP provides authentication information for the subscribers to the Athens Exchange Group services (ATHEX). The user is authenticated using a username and password, but also receives an One-Time-Password of time-limited lifespan. Thus, the LoA offered by this IdP is “substantial”.

2.3 Service Providers description

This section provides a short description of the industrial SP involved in LEPS project, with the aim of offering an overview of the chosen services to be integrated in eIDAS.

2.3.1 Correos services

As stated within “D2.1 LEPS Service Design Document” (to be delivered at the end of the project) and "D3.2 Operational and Technical Documentation of Correos services customization" [5], the scope of the project includes integration with eNotification (My Notifications) and an eDelivery (My Mailbox) services. This integration goes through Correos ID, service based on My Identity IdP of Correos, and will allow - 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:

- Correos ID - My Identity ("Mi Identidad"): provides secured digital identities to citizens, businesses and governments. Therefore, acting as a trusted third party to validate identity attributes, raising third parties trust on individuals. It acts as a gateway to Correos digital services and even non-Correos applications.
- My Notifications ("Mis Notificaciones"): is a digital service, within the eCorreos suite, aiming to centralize and manage governmental notifications for one or several individuals or legal entities.
- 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. 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.

All applications are hosted within a cloud-based platform (eCorreos) and interconnected by an ecosystem of APIs. More specifically:

- Correos ID is a web based (responsive to any device) service.
- My Mailbox is web and native iOS and Android app based.
- My Notifications is desktop based, with a web consultation frontend.

2.3.2 ATHEX services

As stated within "D2.1 LEPS Service Design Document" and "D4.1/D5.1 Operational and Technical Documentation of SP (ELTA, ATHEX) customization", the scope of the project includes integration with the eIDAS Network for two e-services services: ATHEX Sign (Registration) & ATHEX AXIAweb (Registration and Login). This integration will allow European users coming through the MS eIDAS nodes to connect to the ATHEX e-services.

Below brief descriptions of the services mentioned before; for further information, the reader can refer to D4.1/D5.1:

- **ATHEX Sign** is the service of remote e-signature provided by the Athens Exchange Group (ATHEX Group). The service requires a pre-activation procedure, a sort of customer registration. Upon successful registration, a User can process with the main service and digitally sign documents "on the go". ATHEX automates the pre-activation procedure with support from the eIDAS Network. As a result, the users will not be requested to deliver the Subscriber Agreement together with a validated copy of their identity card, as it happens today, but to authenticate and register via eID_EU (with obvious benefits from both the users and the company).
- **ATHEX AXIAweb** is the service providing information on the positions of an investor in the Greek Central Repository Group. ATHEX integrates the AXIAweb service with the eIDAS Network. As a result, a user can both register and login AXIAweb site to review her portfolio in the Greek Stock Exchange Market ("Portfolio Access" page).

All applications these services are hosted within ATHEX premises and integrated with the eIDAS Network via LEPS APIs developed by UAegean.

ATHEX digital services are all web based and responsive to any device. Besides, AXIAweb service can be accessed from Spanish citizens with a mobile device, using the eIDAS infrastructure and their Spanish DNIe 3.0, in the context of LEPS eIDAS Mobile Authentication Task.

2.3.3 ELTA services

As stated within "D2.1 LEPS Service Design Document" and "D4.1/D5.1 Operational and Technical Documentation of SP (ELTA, ATHEX) customization", European users coming from the eIDAS nodes will be able to connect and access a set of 4 well-defined digital services provided by ELTA namely:

1. ELTA eDelivery Hybrid Service (cross-border exchange of electronic documents)
2. ELTA Online Postal Services | ELTA portal / eShop
3. ELTA Online Postal Services | Parcel Delivery Voucher
4. ELTA Online Postal Services | Online Zip Codes for Business Users

Note: Parcel Deliver Voucher and Online Zip Codes for Business Users are both accessed via http://eltab2b.gr web site

- A brief description of the above services is provided below; for further information, the reader can refer to D4.1 & D5.1.
- **eDelivery Hybrid Service**: This service merges the functionality of Document Management and Workflow System (DMWS) with the Hybrid Mail Service of ELTA. The users, after registration, will be able to:
  - Send electronic documents using both the ELTA eDelivery network and the Hybrid Mail Service (sender functionality)
  - Receive documents (recipient functionality)
    - If customers are part of eDelivery network: receive electronic documents and manage delivery evidence through an eDelivery personalized inbox
    - If customers are not part of eDelivery network but they have a physical address: receive a physical letter that includes a URL link from where they can download the electronic document that a sender has addressed to them while the application keeping track and providing evidence on the details of both postage and reception (day and time, secure copy of the original document etc.).
- **ELTA Portal / e-Shop**: ELTA Portal / e-shop offers to both individuals and corporate customers online postal services and e-shop services such as (indicatively): Letter mail services, Parcel services, Prepaid envelopes, Letter mail products, Packaging, Fragile items envelopes, Telephony products, MailBoxes, Philatelic Products etc.
- **Online Parcel Voucher**: Online Parcel Voucher is an e-service provided by ELTA, available to both individual customers and business, but mostly used by SMEs as a B2C service. Users can print online the accompanying vouchers for parcels. The service is vastly used from companies selling through e-Commerce.
- **Online Zipcodes for Business Users**: This is an on-line service offered by ELTA to corporate customers, allowing them to obtain the current version of Zip codes of Greece. These codes are

available in two languages (Greek and English) -- he downloadable files are updated by the Hellenic Post whenever a new version is publishing. ELTA augments the existing service functionality with integration with the eIDAS Network while simplifying the application logic to create a “fast-track” e-shop, thus improving service customer experience. The user is able to register and login via the eIDAS Network (as well as through local credentials). Upon successful completion of the authentication process, the user is redirected back to service web page, to access an e-payments page. After verification of the payment, the user can download the Zipcodes file.

All applications are hosted within ELTA premises and integrated with the eIDAS Network via LEPS APIs developed by UAegean.

ELTA digital services are all web based with “Parcel Deliver Voucher” and “Online Zipcodes for Business Users” being responsive to any device. These two services can be accessed from Spanish citizens with a mobile device, using the eIDAS infrastructure and their Spanish DNIe 3.0, in the context of LEPS eIDAS Mobile Authentication Task.

3 eIDAS Mobile Authentication

The objective of the eIDAS Mobile Authentication Task is to offer mobile support for Greek services to authenticate Spanish citizens, using the eIDAS infrastructure and their Spanish DNIe 3.0, when they access to Greek services. Towards this objective a mobile application will be developed.

The first aspect to take into account when considering the design of a mobile solution is the operating system on which it will work. Each of the available OS has its particularities, its advantages and its drawbacks. Given that one of the main objectives of the project is to show the feasibility of a mobile solution to the problem of integrating mobile private services with eIDAS, it was not intended from the beginning to support all existing mobile systems. As mentioned in both the proposal and the GA, the project has opted for using Android Operating System because it has the largest adoption at European level (see Figure 4), and because it has a more open philosophy regarding its internal architecture that makes easier the communication with the NFC hardware.

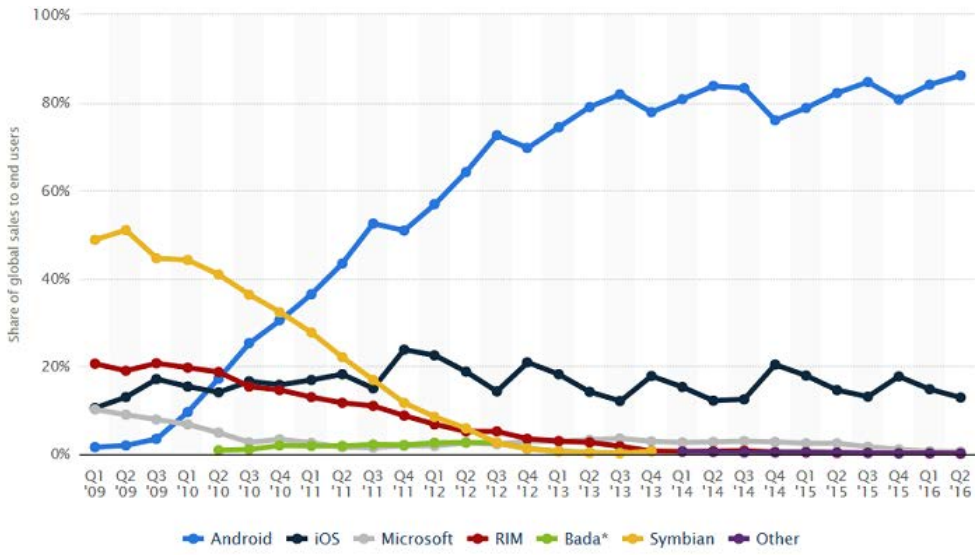


Figure 4: Mobile ecosystem evolution (2009-16)

As we have already explained in Section 2.2.1 depicts, the Spanish Identity Provider (IdP) connected to the eIDAS infrastructure offers two different methods to authenticate users: software certificates and the Spanish DNIe 3.0 with NFC support. The support of NFC access from a mobile device implies the use of native code in Android devices, which must be taken in consideration when defining the appropriate solution.

Besides, an important additional constraint is defined by the eIDAS architecture. The user interaction implies the user redirection from the SP web page, to the SP's eIDAS node, to the user's eIDAS node, to his national IdP, and back again until access to the SP service. This flow is shown in Figure 5. In each redirection, from one node to another, the user's request and the node's response, includes additional information such as the SAML Request and the SAML Response, respectively (by using a HTTP POST request. This information is relatively "heavy", which conditions the way it should be sent between the nodes through the mobile device, in this case it implies the use of HTTP POST request, that as it be shown later, affects the final design of the mobile solution.

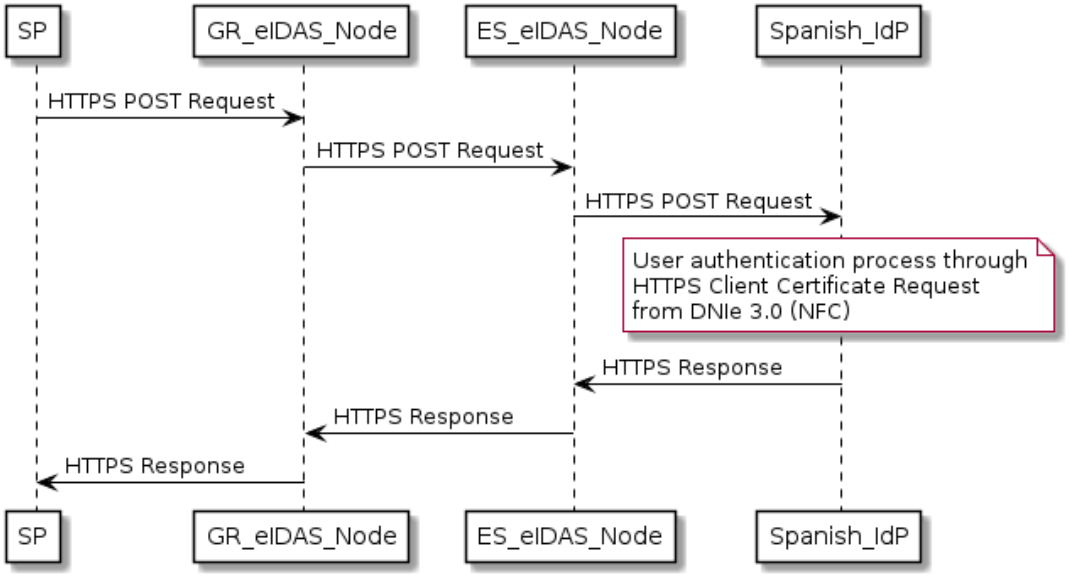


Figure 5: eIDAS interaction flow

Initially, the objective was to design and implement a specific mobile application for each Greek service because this is the usual way of offering mobile services. In the analysis phase, which will be explained in detail in the next sections, we have considered more carefully the requirements derived from the eIDAS architectural as well as the SPs requirements. Also, we have in particular focused on the evaluation of the costs and the functionality to be included in the mobile application. We have asked the question if it makes sense that a SP from a country A should be concerned with the particularities of the authentication system of a country B. In this case, why a Greek SP should be concerned with the specific authentication system of Spanish users?

Based on this assumption, we had to find a way to produce a more generic solution that does not create a non-justified overhead for the Greek Services Providers (or for any foreign SP). Obviously, these Providers should have only to guarantee that their services are provided correctly in a mobile browser, that means that their services have native responsive interfaces that are adapted to the different mobile devices.

To summarize the requirements derived from the mobile scenario, the required features from the mobile authentication app are the following:

Number	Name	Description
eIDMoApp-1	Authentication	The mobile app **MUST** be able to allow user authentication through these eIDAS methods: username/password, software certificates, Spanish DNIe 3.0 (through NFC interface)
eIDMoApp -2	JavaScriptSupport	The mobile app **MUST** be compatible with LEPS SP services, offering JavaScript support
eIDMoApp -3	Authentication request	Mobile app **MUST** support eIDAS heavy web redirections (HTTP POST)

Table 1: Requirement for the Mobile Application

3.1 Requirements derived from eIDAS architecture, eIDAS adapter and Service Providers

This section provides a list of the requirements derived from the eIDAS architecture, the eIDAS adapter in use and the SP services characteristics related to a mobile authentication.

3.1.1 eIDAS architecture requirements

From the eIDAS architecture requirements compiled in "D3.3 Operational and Technical Documentation of SP integration" (to be submitted at the end of June) [7] the following requirements are derived considering the use of mobile app for authentication purposes:

Number	Name	Description
eIDASR-1	Interoperability	The Mobile App **MUST** be able to allow connection between the Spanish eIDAS node with the Greek counterpart, for providing cross-border authentication.
eIDASR-2	HttpPost	The Mobile App **MUST** support HTTP POST redirection to transport eIDAS SAML messages between nodes

Table 2: Requirements derived from the eIDAS architecture

3.1.2 eIDAS adapter requirements

From the specific eIDAS adapter requirements compiled in D3.3 [7] the following requirements are derived taking into account the use of mobile app for authentication purposes:

Number	Name	Description
eIDASAdR-1	Integration	The Mobile App **MUST** be able to allow direct connection between eIDAS adapter and the Spanish eIDAS node.
eIDASAdR-2	HttpPost	The Mobile App **MUST** support HTTP POST redirection to transport eIDAS SAML messages between nodes

Table 3: Requirements derived form the eIDAS adapter

3.1.3 Service Providers Requirements

From the specific requirements compiled (SPR-1, SPR-2 and SPR-3) for Correos as SP on "D3.2 Operational and Technical Documentation of Correos services customization" [5] the following requirements are derived taking into account the use of mobile app for authentication purposes:

Number	Name	Description
MASPR-1	Attributes	The mobile app **MUST** be able to allow the requested attributes provided by the IdP, i.e. name, surname, person identifier, date of birth, and other optionally requested attributes, to reach the SP, so the user can complete the registration and the login processes.
MASPR-2	Adapter	The mobile app **MUST** be able to interoperate with the eIDAS adapter that connects a SP to eIDAS infrastructure.
MASPR-3	Authentication request	Mobile app **MUST** be able to allow the JWT provided by the SP and the JWT generated by the eIDAS adapter are transferred during the authentication process.
MASPR-4	HttpPost	The Mobile App **MUST** support HTTP POST redirection to transport eIDAS SAML messages between nodes
MASPR-5	JavaScript	The Mobile App **MUST** support JavaScript components to allow dynamic content for SP webpages.

Table 4: Requirements derived from SPs

4 Analysis of the solution

The Android mobile platform has specific characteristics that require an analysis in depth. In general, the eIDAS Network assumes interactions between the different entities based on web scenarios using web redirections to transfer the user from one entity to other. An Android browser offers advanced functionalities that allows to work in different environments (including a laptop or a desktop PC), but there are also limitations in terms of hardware integration and use. Particularly, it does not allow to use the NFC interface to interact with user certificates in the Spanish DNIe 3.0.

The use of certificates stored in NFC resources for user authentication is not supported natively by the standard Android browser, so it is needed the use native code to interact with the NFC interface for recovering user certificates stored inside the DNIe 3.0. This leads us to explore alternatives to address the integration of DNIe 3.0 as a valid authentication mechanism in mobile devices.

4.1 Native Android App for each Service Provider

This is the common way of offering mobile services in Android. Each SP usually design and implement native apps to offer their services adapted to the mobile users. These apps run all the flow between all the entities involved, from the SPs to the Identity Providers' authentication service.

In the eIDAS case, the application must be able to offer the SP's service with an interface adapted to the peculiar characteristics of the mobile device, and at the same time interact with the intermediate eIDAS nodes and the Identity Providers, offering the possibility of authenticating with digital certificates, as well as with the DNIe 3.0 in the case of Spanish users.

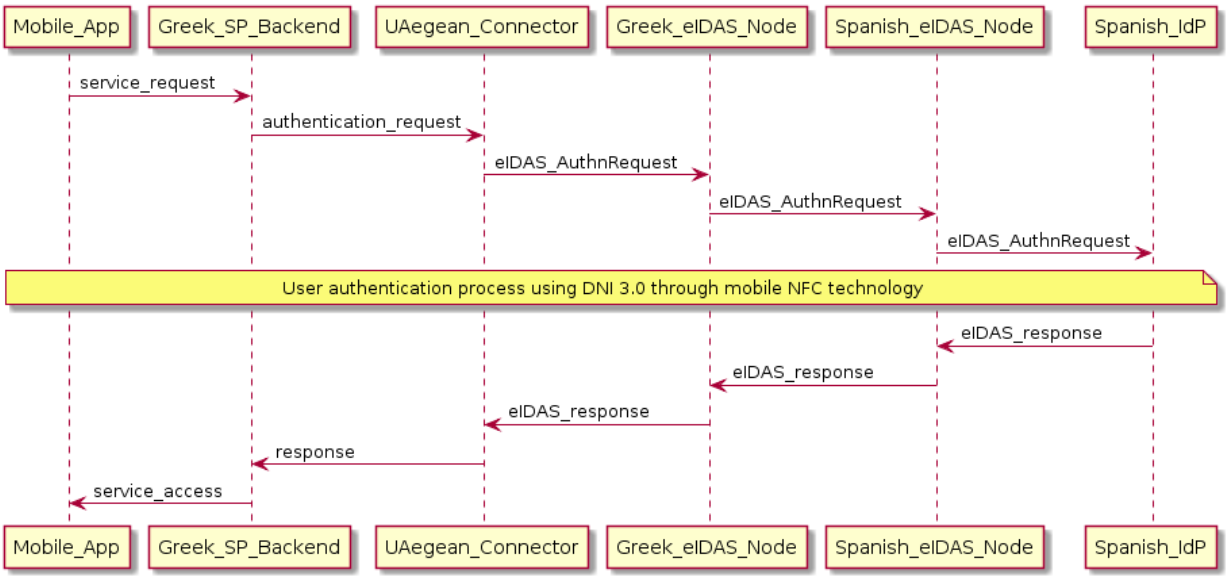


Figure 6: Native Android App for each SP diagram

4.2 Native Android browser plus (specific) native Android app to interact with the Spanish eIDAS IdP

This second option related to the use of a standard Android browser (i.e. Chrome) to organize the user's interaction with all the entities involved (i.e. SP, eIDAS nodes, IdP). The native Android browser supports the user authentication using username/password and client SSL authentication (certificates).

In the specific case that the eIDAS must be authenticated by the Spanish IdP using the Spanish DNIe 3.0, it is required the use of native code to interact with the NFC interface to recover the user certificates.

The use case is as follows:

- *A Spanish user wants to access to Greek SP, so she opens the SP's webpage and indicates that she wants to be authenticated through the eIDAS infrastructure.*
- *The SP asks for her home country and redirects her (through her browser) to the Spanish IdP, through the Greek eIDAS node and the Spanish eIDAS Node.*
- *When she tries to access to the Spanish IdP, the Android systems detects the specific access to the Spanish IdP and launch the app selector to offer the option of choosing the specific eIDAS app to complete the authentication process.*
- *This application is able to interact with the user and obtain the DNIe 3.0 certificates through the NFC interface of the mobile and to present these to the IdP to complete the authentication.*
- *After completing the authentication process and ask for user consent, the app return the flow/response to the native Android browser.*
- *It applies the redirections through the eIDAS nodes to the SP, where the user gets access to the service.*

Next Figure 7 depicts the use case sequence flow:

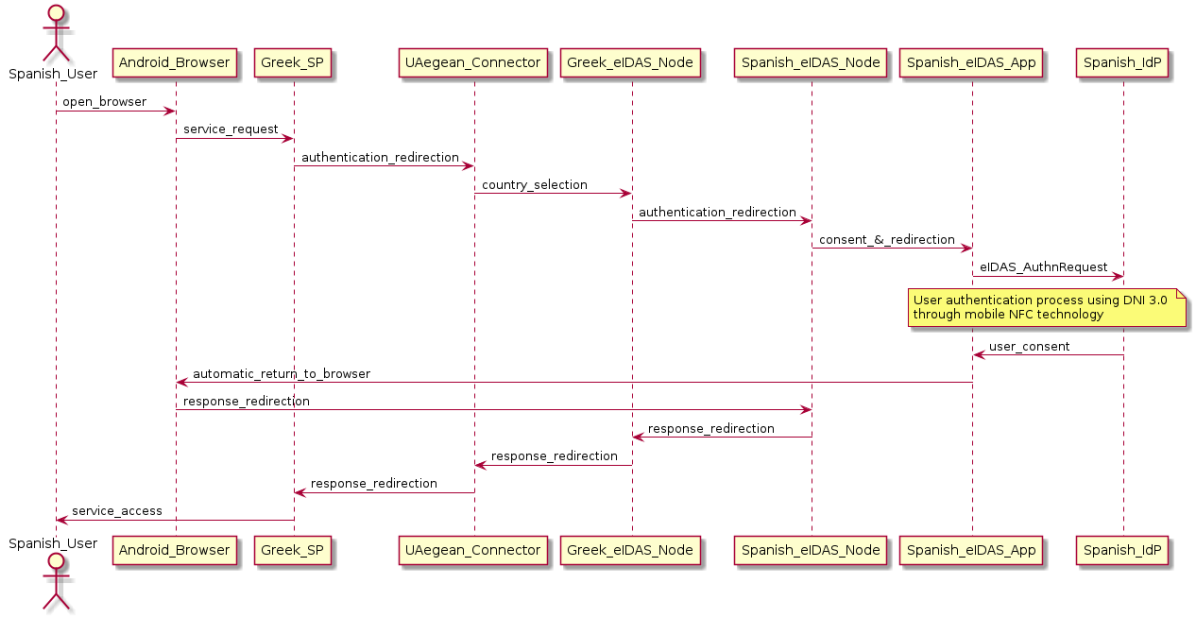


Figure 7: Native Android browser plus (specific) native Android app to interact with the Spanish eIDAS IdP diagram

This option generates several technical difficulties due to the switch between Android applications (between the Android browser and the eIDAS mobile application). They mostly related to the browser management of the web sessions in the SP and the eIDAS nodes, or to the transfer off the necessary information between the Android browser and the eIDAS application. In addition, because of the complexity of the approach many unforeseen problems may arise that may complicate or even make this solution impossible.

4.3 Native Android browser App to run the complete process from SP to IdP

A third option considers the possibility of designing an Android application that includes all the functionality of a web browser, extended with the extra functionalities required to support authentication through Spanish DNIe 3.0.

This solution has the advantage of being independent of the SPs, but it is much more complex technically and from the raises some usability concerns. More specifically, it requires a larger application size and implies the obligation of the user to launch the application in advance before starting authentication and access the service via this browser. On the other hand, this approach solves the issues mentioned in the previous approach (section 4.2) since the whole authentication process is managed inside the app, offering a homogeneous interface for all eIDAS services and a trusted single app to authenticate Spanish eIDAS users.

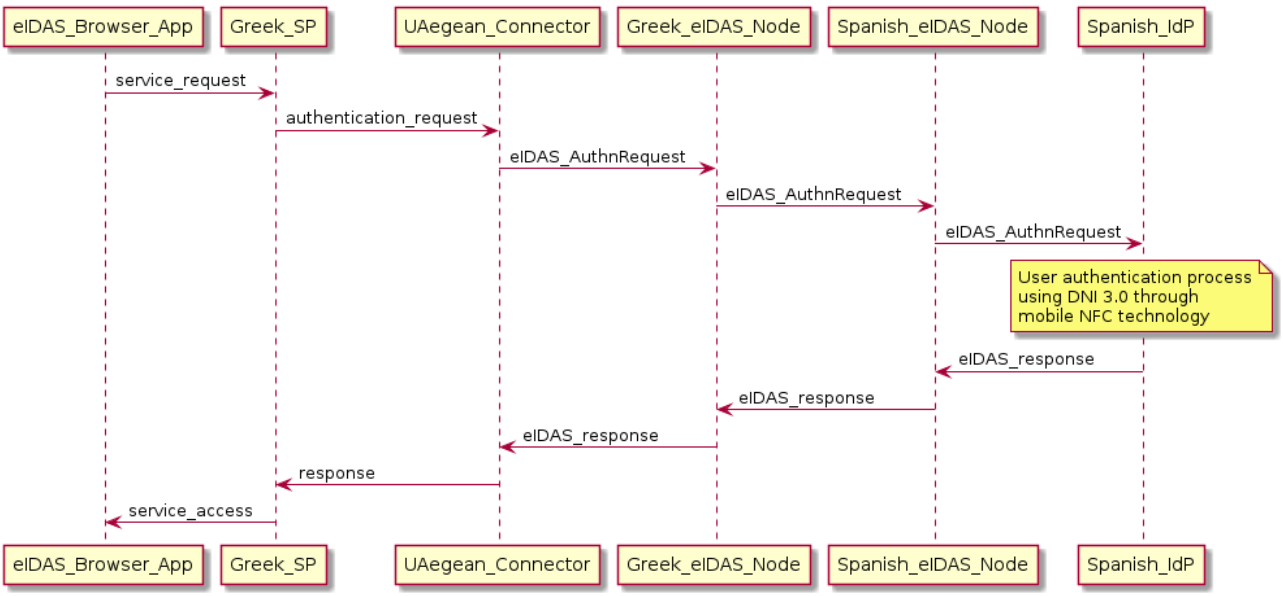


Figure 8: Native Android browser App to run the complete flow

4.4 Native Android App to catch the internal keystore/certificates request

This option merges from both last approaches. The idea is the design of a native application that only deals with the interaction with the DNIe when an authentication request based on certificates is detected.

Essentially, this option captures the user certificate request made by the IdP to the browser and process this request through a specific application that generates a new keystore with the contents of DNIe 3.0.

After an initial analysis of Android APIs, this solution does not does not seem to work in practice, since certificates and private keys are very sensitive information and well protected by the Android operating system.

4.5 Selected option

As result of the analysis, the third approach has been adopted for the final design: a native Android browser App to run the complete process from SP to IdP. This approach has clear advantages compared to other alternatives described above. Firstly, it allows for "isolating" SPs from the particularities of the authentication mechanisms of each eIDAS country. In addition, this solution does not require the explicit participation of the eIDAS or IdP nodes. Secondly, it is considered as a unified tool for authenticated access to eIDAS services. This design makes easy the support of other authentication methods and facilitates the localization process in other EU countries, for example, for allowing Greek users accessing and authenticating Spanish SP via a mobile device.

The only real drawback to this approach is that the user must require access to the service directly within the mobile application, which requires a minimum initial knowledge of the eIDAS authentication mechanisms and the tools necessary to use it.

The idea for LEPS project is to offer a single mobile app focused on the Spanish market that allows the authentication of Spanish citizens, using the eIDAS infrastructure and their DNIe 3.0, when they access to any services of the eIDAS network. This application can be used, also, by the Greek citizens accessing Spanish services, using other types of credentials for authentication, such as username/password.

5 Technical Design

The starting point for the technical design is the design of a native Android app that offers a simplified embedded browser to access any SP webpage, by using any available credential, simple username/password, a software certificate, as well as Spanish DNIe 3.0 through the mobile NFC interface.

This process implies several design steps and requires the definition in depth of the functionality of the mobile app. At first, a clear Use Case description that will allow for defining the operations that support interaction between the user and the participating services in the case of use. Based on this, it will be necessary to clearly define all user interfaces. Finally, the solution design needs to describe all the internal functional distribution required to cover the needs of the mobile solution.

5.1 Use Cases description

The application basically must execute a single use case that consists in allowing user access to an eIDAS service through the eIDAS infrastructure by using national credentials. When a citizen holding a Spanish eID accessing a Greek Service, the app must support the use of software certificates and the interaction with the Spanish DNIe (through its NFC interface). Due that there are two different methods to authenticate Spanish users, the use case can be divided in two sub-cases: a) use of software certificates and, b) use of the Spanish DNIe. In both cases, both the software certificates and the DNIe can be pre-configured in the system/app or not. The four possible use cases are described below.

5.1.1 Use Case 1: Spanish citizen using a not installed software certificate

Description	Citizen holding a Spanish eID accessing a Greek service through the eIDAS infrastructure, using a not-installed software certificate as identity proof.
Preconditions	• The SP is registered as a valid eIDAS service • The user has a valid software certificate stored in the mobile device • The user has already installed the required app (the eIDAS Browser)
Process	1. The user opens the eIDAS Browser app in his/her mobile device 2. The user enters the service provider URL in the text box that is shown in the app and press the “Go!” button. 3. The user must try accessing the service, and in the case of authentication is required, makes click on eIDAS authentication. In function of the service, the user may have to confirm, authorize or choose information relative to the service. 4. Once the eIDAS flow is launched, the user must indicate which is her country of origin and press the corresponding button to continue. 5. The app redirects the user until arrive to the Spanish IdP, where the app automatically detects that a User Certificate Request is required by the IdP server. Then, the app automatically shows a menu with three options: Digital certificate, DNIe 3.0 or Cancel.

	6. The user has to click on Software certificate. 7. The app shows a new window to manage user certificates. Since the user does not have installed a certificate yet, the user must click on “Instalar” button to add a new one. 8. The Android system opens a File Explorer windows where the user has to find and choose (clicking on) the certificate file (usually with .p12 extension). 9. Then a small new window is shown, where the user must enter the password to allow the certificate installation and click on “Aceptar” to complete the installation process. 10. Now the Certificate Manager windows already depicts the new user certificate. The user should choose the right one and click on “Permitir”. 11. The app use this to authenticate the user at the IdP and redirect the user to the SP webpage where the user can now access to the service.
Result	The SP grants access to the user.

Table 5: Use Case 1 - Spanish citizen using a not installed software certificate

5.1.2 Use Case 2: Spanish citizen using installed software certificate

Description	Citizen holding a Spanish eID accessing a Greek service through the eIDAS infrastructure, using a software certificate as identity proof. The software certificate is already configured in the mobile operating system.
Preconditions	• The SP is registered as a valid eIDAS service • The user has a valid software certificate installed in the mobile device • The user has already installed the required app (the eIDAS Browser)
Process	1. The user opens the eIDAS Browser app in his/her mobile device 2. The user enters the SP URL in the text box that is shown in the app and press the “Go!” button. 3. The user must try accessing the service, and in the case of authentication is required, clicks on eIDAS authentication. In function of the service, the user may have to confirm, authorize or choose information relative to the service. 4. Once the eIDAS flow is launched, the user must indicate which is his/her country of origin and press the corresponding button to continue. 5. The app redirects the user until arrive to the Spanish IdP, where the app automatically detects that a User Certificate Request is required by the IdP server. Then, the app automatically shows a menu with three options: Digital certificate, DNIe 3.0 or Cancel. 6. The user must click on Software certificate. 7. The app shows a new window to manage user certificates with the list of available user certificates. The user should choose the right one and click on “Permitir”.

	8. The app uses the certificate to authenticate the user at the IdP and redirect the user to the SP webpage where user can now access to the service.
Result	The SP grants access to the user.

Table 6: Use Case 2 - Spanish citizen using installed software certificate

5.1.3 Use Case 3: Spanish citizen using her Spanish DNIe 3.0 not installed

Description	Spanish user accessing a Greek service through the eIDAS infrastructure, using a Spanish DNIe 3.0 (not configured in the mobile app) as identity proof.
Preconditions	• The SP is registered as a valid eIDAS service • The user has a valid DNIe 3.0 not configured in the app. • The user uses a mobile device with NFC support (and it is active) • The user has already installed the required app (the eIDAS Browser)
Process	1. The user opens the eIDAS Browser app in his/her mobile device 2. The user enters the SP URL in the text box that is shown in the app and press the “Go!” button. 3. The user must try accessing the service, and in the case of authentication is required, makes click one IDAS authentication. In function of the service, the user may have to confirm, authorize or choose information relative to the service. 4. Once the eIDAS flow is launched, the user will have to indicate which is her country of origin and press the corresponding button to continue. 5. The app redirects the user until arrive to the Spanish IdP, where the app automatically detects that a User Certificate Request is required by the IdP server. Then, the app automatically shows a menu with three options: Digital certificate, DNIe 3.0 or Cancel. 6. The user has to makes click on DNIe 3.0. 7. The app shows a menu with a list of available DNI with the title “Selección de CAN”. Since the user wants to install a new one, she should click on “Installar nuevo DNIe”. 8. In the new window, the user must enter the CAN code that is shown in the main face of the DNIe and make click on “Aceptar”. 9. The app requires the user to put the DNIe attached to the mobile NFC reader without moving it to read the public information and save the registration within the application. 10. Back to the “Selección de CAN” window, the user can now click on the right DNIe can code. 11. The app requires again that the user to put the DNIe attached to the mobile NFC reader without moving it to stablish the connection. Once established the link, the app requires the user to introduce the private password and to click on “Aceptar” button to access the protected information (the private key) in the DNIe.

	12. The app uses the recovered information to authenticate the user at the IdP and redirect the user to the SP webpage where user can now access to the service.
Result	The SP grants access to the user.

Table 7: Use Case 3 - Spanish citizen using her Spanish DNIe 3.0 not installed

5.1.4 Use Case 4: Spanish citizen using her Spanish DNIe 3.0 (already configured)

Description	Spanish user accessing a Greek service through the eIDAS infrastructure, using a Spanish DNIe 3.0 (already configured in the mobile app) as identity proof.
Preconditions	• The SP is registered as a valid eIDAS service • The user has a valid DNIe 3.0 already configured in the app. • The user uses a mobile device with NFC support (and it is active) • The user has already installed the required app (the eIDAS Browser)
Process	1. The user opens the eIDAS Browser app in his/her mobile device 2. The user enters the SP URL in the text box that is shown in the app and press the “Go!” button. 3. The user tries to access the service, and if the authentication is required, clicks on eIDAS authentication button. 4. Once the eIDAS flow is launched, the user must indicate which is her country of origin and press the corresponding button to continue. 5. The app redirects the user until arrive to the Spanish IdP, where the app automatically detects that a User Certificate Request is required by the IdP server. Then, the app automatically shows a menu with three options: Digital certificate, DNIe 3.0 or Cancel. 6. The user must click on DNIe 3.0. 7. The app shows a menu with a list of available DNI with the title “Selección de CAN”. The user has to click on the right DNIe CAN code. 8. The app requires the user to put the DNIe attached to the mobile NFC reader without moving it to stablish the connection. 9. Once established the link, the app requires the user to introduce the private password and to click on “Aceptar” button to access the protected information (the private key) in the DNIe. 10. The app uses the recovered information to authenticate the user at the IdP and redirect the user to the SP webpage where user can now access to the service.
Result	The SP grants access to the user.

Table 8: Use Case 4 - Spanish citizen using her Spanish DNIe 3.0 (already configured)

5.2 User Interface Design

Using as guide the previous Use Case descriptions, the user interface should be designed to cover all the required functionality. The following images depict the user interfaces designed to cover each main step of the use cases, most of them are common to all the use cases.

- Initial access to the service (UI-1). This user interface (Figure 9) is the first window that the user sees after opening the app. It allows for inserting the SP's URL and shows a button 'Go' to start the navigation process.

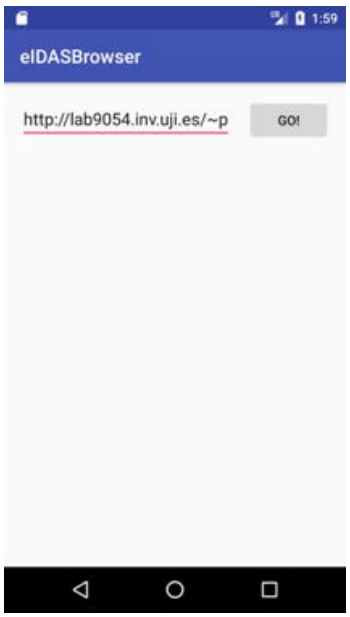


Figure 9: UI-1 Initial access to the service

- eIDAS internal browser (UI-2): the user can navigate (Figure 10) the SP's webpage, start the eIDAS authentication, navigate through the eIDAS nodes until he/she arrives to the Identity Provider, where the user authentication is required through a user certificate.

Figure 10: eIDAS internal browser (UI-2)

- Menu to choose the user authentication method (UI-3). It consists of a pop-up menu (Figure 11) that is shown superimposed on the last page opened in the internal browser and shows two possible options to provide the required certificate to the user authenticate: software certificate or DNIe 3.0. There is a third option to cancel the authentication process.

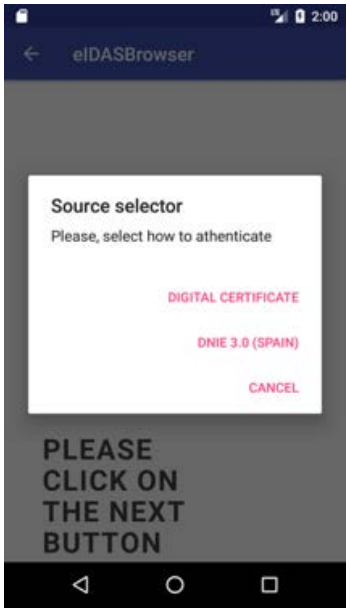


Figure 11: Menu to choose the user authentication method (UI-3)

- Certificate Manager window (UI-4). It is launched when the user chooses "Digital Certificate" in the previous menu. The pop-up menu (Figure 12) shows the certificate manager tool of Android OS. If the user has already installed some certificate, they will be listed in the menu. There is also the option of the install a new one making click on the button located in the lower right corner. Ones the user has chosen one, the user must click on "Allow" to authorize the use of this certificate in the authentication process with the IdP referred in the first paragraph.

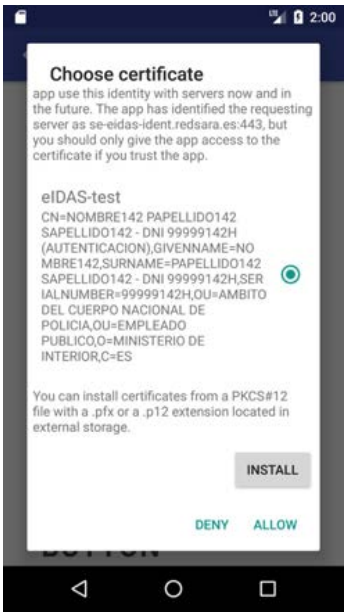


Figure 12: Certificate Manager window (UI-4)

- Android File Explorer menu to install a new certificate (UI-5). This window (Figure 13) is shown when the user need to install a new certificate. The window shows an specific Android file explorer menu with an activated filter that only allows choosing files that contain certificates (e.g. .P12, .PFX extensions). Depending on the type of file, the introduction of a password may be required through a pop-up menu.

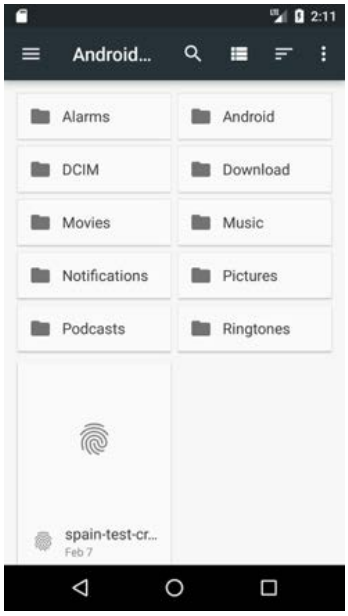


Figure 13: Android File Explorer menu (UI-5)

- eIDAS internal browser (UI-6): It shows the successful access to the service, after authentication (Figure 14) – or the failure of the authentication process. Internally it could be the same windows shown at point 2.

Figure 14: eIDAS internal browser showing the successful access to the service (UI-6)

- DNIe 3.0 use and CAN selection (UI-7): This window is displayed (Figure 15) when the user selects to authenticate through his / her DNIe. It shows the list of DNIe registered in the app, showing its associated CAN number and the name of the DNI holder. It also allows the possibility of adding a new DNIe to the app, clicking on the button "Añadir nuevo DNIe".

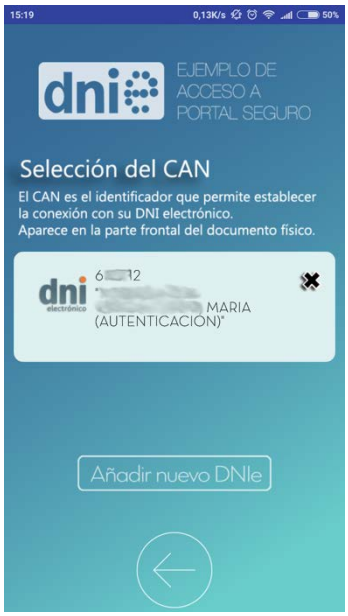


Figure 15: DNIe 3.0 use and CAN selection (UI-7)

- New DNIe and CAN code (UI-8): This window (Figure 16) is displayed when the user wants to add a new DNIe to the app. It shows a text box where the user should enter the CAN code associated to the new DNIe (the code is in the lower right corner of the main face of the DNIe). To complete the registration process, the user should click on "Aceptar".

Figure 16: new DNIe and CAN code (UI-8)

- Establishing the access to the DNIe (UI-9): after the registration of a new CAN code, the mobile app must request the user to bring the DNIe to the mobile phone (Figure 17) to establish the initial connection with it and verify that the CAN code is correct. When the mobile device detects the NFC communication, the DNIe image changes from grey scale to colours (Figure 18) and the app shows a pop up with information messages about the status of the connection.

Figure 17: Establishing the access to the DNIe: step 1 (UI-9)

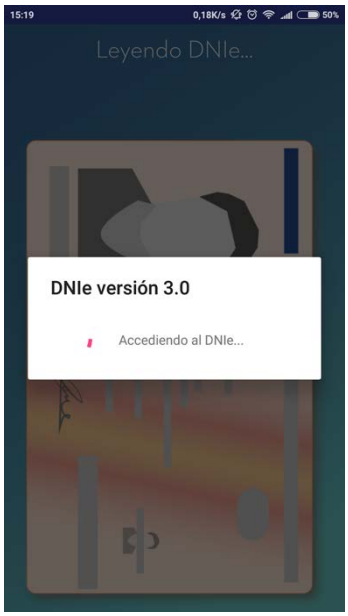


Figure 18: Establishing the access to the DNIe (step 2)

- Input of secret password to access DNIe (UI-10). This window (Figure 19) is displayed when the user selects to use an already configured DNIe. In this case, after the app request the user to bring the DNIe to the mobile device and once the NFC link is established, the app shows a pop-up windows asking for the private password that protect the private information of the DNIe.

Figure 19: secret password input form (UI-10)

- Loading internal user certificates and the private key to sign the connection (UI-11). This window (Figure 20) shows information during the process of recovery the protected information inside the DNIe. When the process is completed, the app establishes the secured connection with the IdP based on the user certificate obtained and then shows the resulting web of the authentication process.

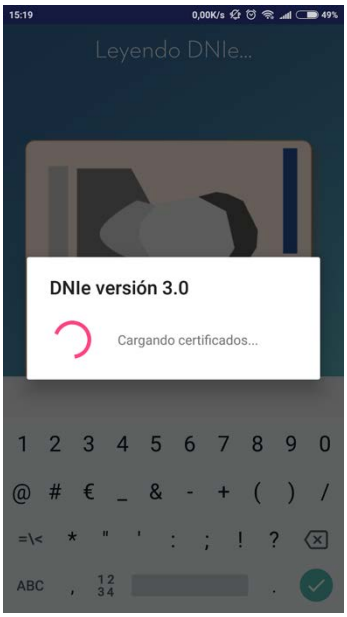


Figure 20: Loading internal DNIe data (UI-11)

5.3 Internal Design

The design of an Android mobile application is conditioned by the design of Android OS and the design guidelines for its applications, the need to have clean and user-friendly interfaces and the organization of the application functionality and structure into *Activities*.

Using as guide the functionality required by the use cases and the defined user interfaces, it is necessary to the organize this functionality between activities. The design process should in particular take care of the interaction of the user with the navigation process between eIDAS services and nodes, and also the interaction between the user and the possible sources for obtaining the certificate.

Figure 21 shows the Activity Diagram including the interaction flow between activities. The first step of the app is the *MainActivity* that shows the user interface defined in UI-1 (Figure 9). The *DisplayURLActivity* is in charge of managing the internal browser described in UI-2 (Figure 10) and UI-6 (Figure 3), basing its operation on the *MyWebViewClient* class, which is the one that marks the behaviour of the embedded browser. This client class handles the authentication request made by the Identity Provider through obtaining the client certificate and therefore initiating the process that allows choosing between software certificate or DNIe (menu UI-3 - Figure 11) and launching the corresponding activity.

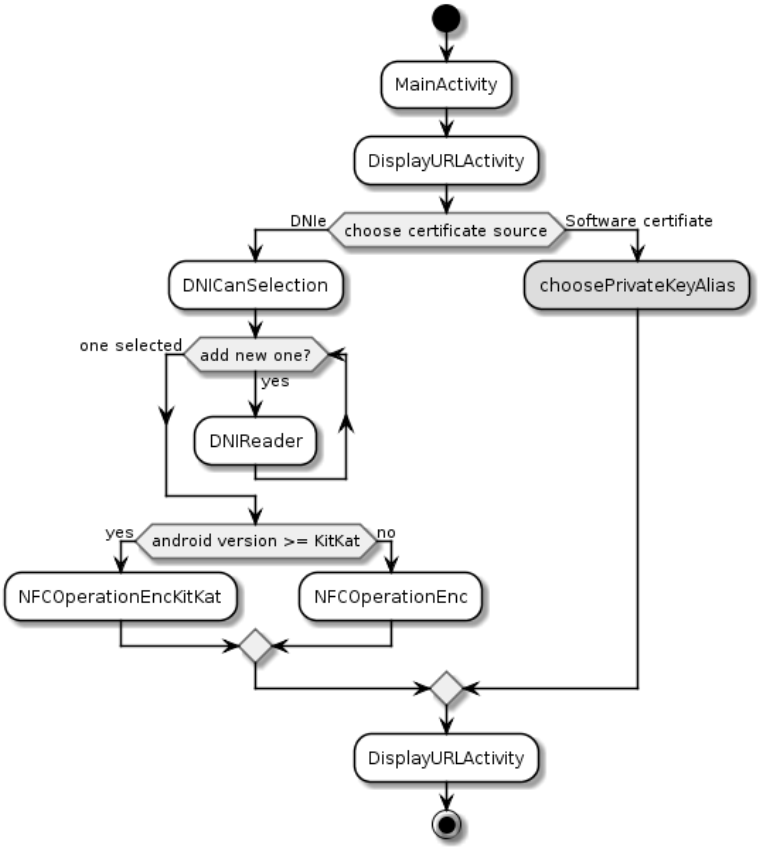


Figure 21: Mobile application activity diagram

If the user chooses to authenticate using a software certificate, the *MyWebViewClient* class launches a system activity (UI-4 -Figure 12) that determines which certificate the user wants to use by returning its alias (the name in the system) or even allows the installation of new certificates (UI-5 - Figure 13). Once the certificate has been decided, it is recovered, and the process is continued within the *DisplayURLActivity* activity (UI-6 - Figure 14).

In the case of the user chooses to authenticate using her DNIe, the *MyWebViewClient* class launches the *DNICanSelection* Activity (UI-7 - Figure 15). This activity is in charge of offering the user a list of already configured DNIes or install a new one. If it is necessary to install a new one, the *DNIReader* Activity is launched and the UI-8 (Figure 16) is shown. This activity asks the user for the CAN code of the DNIe and register it in the app, after a linking phase (UI-8 - Figure 16) through the NFC interface. Once the user chooses her DNIe from the list, and in function of the Android SO version, the Activity in charge of the interaction with the DNIe through the NFC interface is launched (it could be *NFCOperationEncKitKat* or *NFCOperationEnc*). These activities establish the connection with the DNIe, ask the user her personal password (UI-10 - Figure 19) used to protect the private information inside the DNIe, and use it to recover (UI-11 - Figure 20) the private key and protected certificates in order to use them to establish the authenticated connection. After establishing the identity of the user with the use of the certificate, the activity returns the successful result through the activity flow to the *DisplayURLActivity* that shows the navigation results in the embedded browser (UI-6 - Figure 14).

To solve part of the complexity involved in the interaction through the NFC hardware of the mobile device, the application makes internal use of the *DNIeDroid* library, which will be explained in more detail in Section 6 - Implementation Details.

6 Implementation Details

To understand the internal operation of the application it is necessary to explain, beyond the activity structure, the user interfaces and generic rules of operation, the different internal components and technical details that affect the operation and design of the application. This section will present the libraries on which the project depends as well as dependent factors on the Android operating system, which condition the application and limit the devices on which the application can be executed.

6.1 Libraries and dependencies

In order to facilitate the use of the Spanish DNIe on Android platforms, the Spanish Ministry together with Spanish National Police Service provide a library, named *DNIDroid*, and example applications to help developers to create new apps to expand the scope of use of the DNIe. These apps have different scopes: reading, signature and authentication.

The *DNIDroid* library has been adapted to be use as an external library. This middleware existed previously for the use in Java of the DNIe versions with contacts. And now it has been adapted for its proper functioning in Android and the contactless interface via NFC.

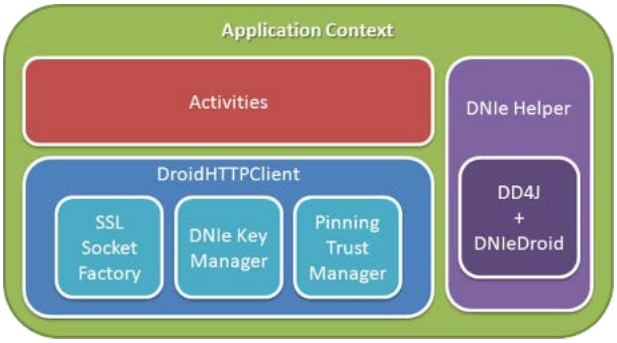


Figure 22: DNIDroid Library internal components

Figure 22 shows how the library is integrated into an Android application. In an Android application the point of contact with the user are the Activities. The *DNIeHelper* component is available for all of them, and it manages the interaction with the DNIe and the dialog boxes that are shown to the user during this interaction. On the other hand, those Activities that require the use of the DNIe for signing and authentication on third-party servers, can make use of the *DroidHTTPClient* component, which manages this problem and it is also based on the interaction component with the DNIe.

As a further step of abstraction, Android allows you to use applications such as libraries, to reuse components, interfaces, activities and graphic elements. In this way, for the implementation of our application the authentication application example provided by the Spanish Ministry has been used as a library, in such a way that screens, activities and images related to the interaction with the DNIe can be reused. The resulting component is defined as *dniedroid* and included as project dependency. Internally, the authentication app also depends of relevant libraries such as *jsoup*, which is a Java parser for *DOM*, *CSS* and *Jquery*; On the other hand, it also depends of a well-known cryptographic library as *Bouncy*

Castle Provider (bcprov). Specifically, among the reused components are the screens and their graphic components to interact with the DNIe: CAN selection, linking and reading the DNI, and password entry form.

6.2 Android version

The Android Operating System has evolved since its appearance in 2008 (Figure 23), publishing new versions and with each one of them, offering new functions, improving its security and offering compatibility with the new hardware components that were added to mobile devices.

Figure 23: Android versions release dates

Due to the short lifetime of a mobile phone, manufacturers usually do not update their terminals beyond a few versions of the operating system. This causes that many versions of Android coexist at the same time, problem known as fragmentation, the application developers should try to support the largest number of terminals and Android versions possible.

Figure 24 shows the volume of devices that are supported based on the minimum version of Android SDK to which the application supports. As it was said at the beginning, each new Android version not only improves aesthetic and security aspects but also affects the hardware supported. In our case, for the developed application, it has been determined that the minimum supported SDK is 21, known as Android 5.0 - Lollipop, being the latest version published at June 2018, Android 8.1 Oreo. This decision is basically focused on improving the NFC hardware support that is given in version 19 and the improved support of the certificate management provided in version 21. This SDK version allows the application to be installed on 71.3% of existing Android mobile devices. It is important to highlight at this point that this percentage is much greater than that of compatible devices by hardware, i.e. devices that have an NFC interface, necessary to interact with the DNIe 3.0.

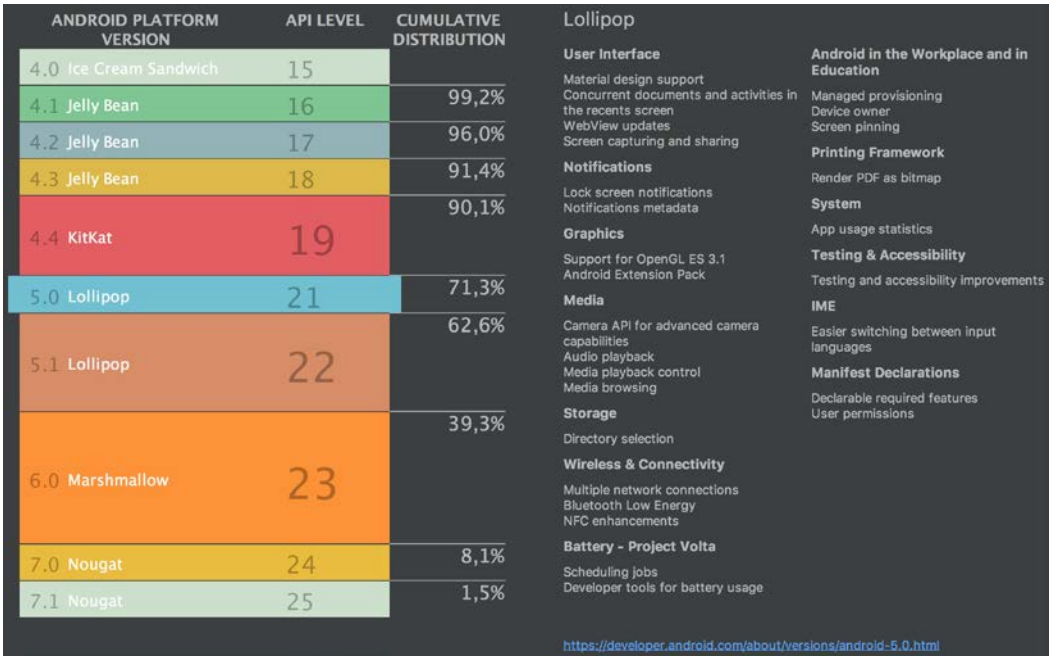


Figure 24: Android level of adoption (2018 May)

7 Mobile App installation and use

After completing the mobile application, the testing and interoperability testing phase begins with services and the eIDAS infrastructure. In order to execute the necessary tests, the binaries, test files and installation and usage guides are available to all project members so that they can execute the mobile applications with their services autonomously and independently.

This section focuses on guiding the process of installing the corresponding mobile application package, as well as downloading and using the necessary material (test certificates) to work with the preproduction environments that are active and functioning in this phase of the project. In addition to the set-up of the test environment in Section 7.1; Section 7.2 shows a brief guide to use the application based on screenshots.

Finally indicate that it is expected that at the end of the test phase in production the mobile application will be uploaded to the official Android store, Google Play, to make it available to the public in general.

7.1 Mobile application installation and test environment configuration

The description of the mobile app installation process is based on the use of *LEPS Project Repository*[1][2] based on OwnCloud software. In it, there are available all the needed files to test the mobile environment with Partners' services. The list of the available files is the following:

- README.txt: with the instructions of download and install the mobile app and the testing credential in your Android devices, that are included below after this list.
- eIDASBrowser.apk: the eIDAS Browser installation file.
- spain-test-credential.pfx: the Spanish test credential to use with the app (it must be installed in the device).
- spain-test-credential-password.pfx: the password required to access/install the credentials
- TestCasesUMU_v1.docx: use case description.
- LEPS_201805_Madrid_UMU_Activity3_mobileApp.pptx: with the slides from Madrid with the report and screenshots of the mobile app.

These are the steps to install and configure the testbed environment in a mobile device:

1. Enable third-party app installation on the Android Test Device (unknown sources)
    a. For Android OS version 2.3 and earlier:
        i. Step 1 – Go to Settings.
        ii. Step 2 – Go to Applications.
        iii. Step 3 – Tap and check "Unknown sources" box.
        iv. Step 4 – Tap 'OK" when it shows the warning.

    b. For Android OS version 4.0+:
        i. Step 1 – Go to Settings.

[1] At the time of publication of this deliverable, the development of services and mobile application are in the pre-production phase. It is expected that at the end of the project, the mobile app code and final binaries will be upload to public repositories and to the Play Store to be accessible for the general public.
[2]Restricted access

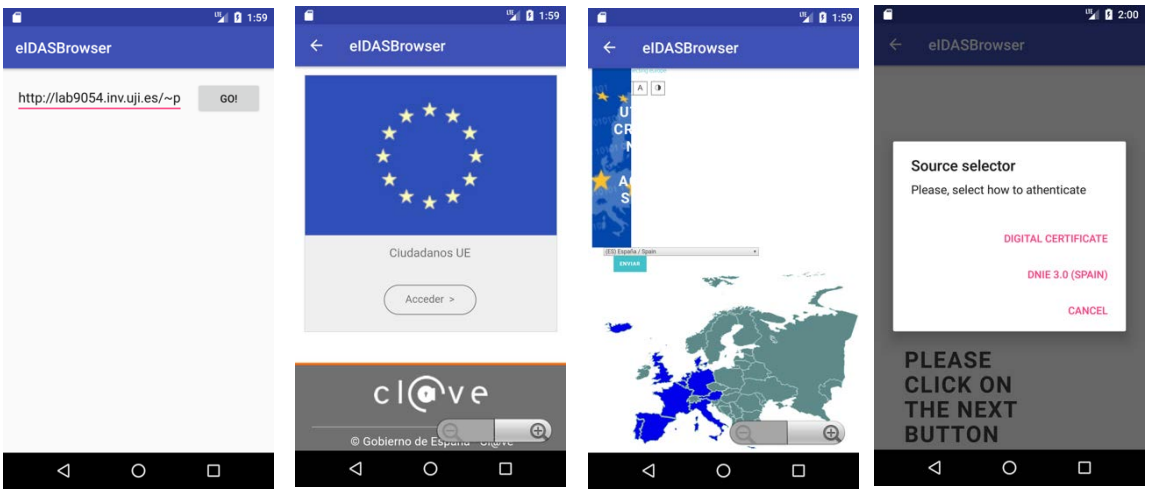
ii. Step 2 – Go to Security.
iii. Step 3 – Scroll down and check “Unknown sources” box.
iv. Step 4 – Tap ‘OK” when it shows the warning.

2. Download the eIDASBrowser app (APK file) in the test device from the repository. LEPS Owncloud Repository/LEPS/Activities/Activity 3.../T3.1 Mobile Authentication/Mobile App/eIDASBrowser.apk
3. Install the app in the device. By default, it is download to the Download folder of your device. Make click in the apk file to install it.
4. Download and install the eIDAS test credentials from the repository.
    a. Download LEPS Owncloud Repository/LEPS/Activities/Activity 3.../T3.1 Mobile Authentication/Mobile App/spain-test-credential.pfx
    b. Download LEPS Owncloud Repository/LEPS/Activities/Activity 3.../T3.1 Mobile Authentication/Mobile App/spain-test-credential-password.pfx
    c. To install the PFX file, open it with a file explorer app, make click on the file, and use the password to install the credentials in the android device.
5. Run the eIDASBrowser app and run the test cases related to software certificates using your respective SPs URL.

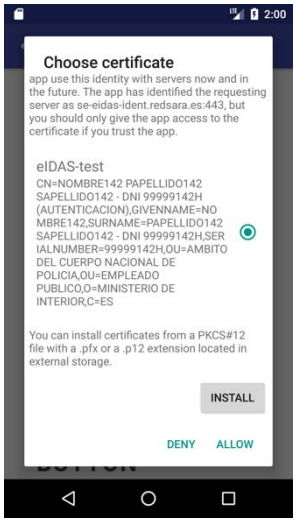
7.2 User interface and example of use

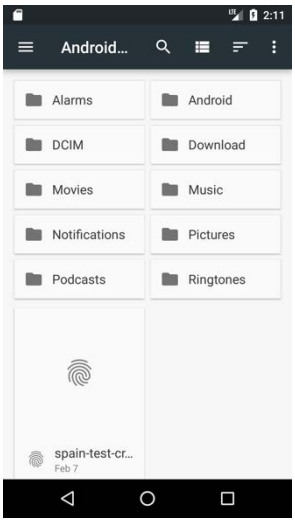
This section provides a general description of the user interface as well as a guide to the steps to follow to execute access to a service through the application.

- Accessing to the service: The first screenshot shows the entering point of the app, i.e. the first window that the user sees after opening the app. To start the access to the service, the user has to enter the SP’s URL to access and click in the 'Go' button in order to start the navigation process. Then, the user can navigate the SP's webpage, start the eIDAS authentication, and reach the involved eIDAS Network nodes until she arrives to the Identity Provider (2nd and 3rd screenshots), where the user authentication is required through a user certificate. To solve this, the application asks the user what source of certificates she wants to use: if she wants a digital certificate or wants to extract it from her DNIe.

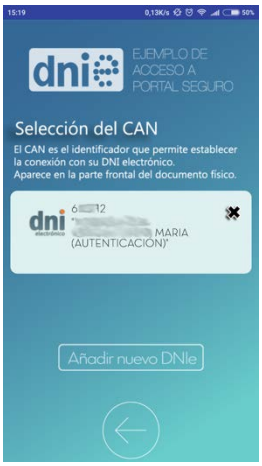


- Software certificate authentication: if the user chooses "Digital Certificate" in the previous menu, the pop-up menu shows the certificate manager tool of Android OS (1st screenshot). If the user has already installed some certificate, they will be listed in the menu. There is also the option of the install a new one (2nd screenshot) making click on the button located in the lower right corner. Ones the user has chosen one, the user must make click on "Allow" to authorize the use of this certificate in the authentication process. The 3rd screenshot shows the final access to the SP after a successful authentication.



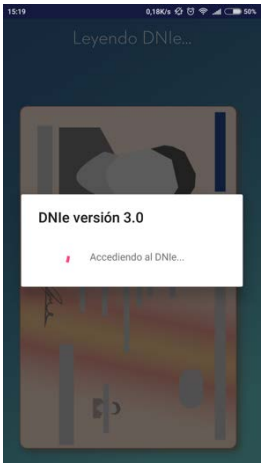


- Spanish DNIe 3.0 (NFC interface) authentication: this set of screenshots shows the successful use of Spanish DNIe to authenticate the user in the eIDAS IdP. In first place, the user has the option of select an already configured DNIe from the list. If the user needs to add a new one, she must enter the CAN code of the new DNIe which is going to be used to establish the secured channel through the NFC interface. Once selected the DNIe, the user has to bring the DNIe to the mobile NFC reader as is indicated by the application, so that the connection between the two can be established. Once established, the user is asked to enter the personal password that protects access to the private DNIe information (private key and user certificates with protected information). Once that information has been recovered, the application establishes a secure channel with the Identity Provider that guarantees the identity of both the user and the server, and subsequently the user is able to access the already authenticated service.

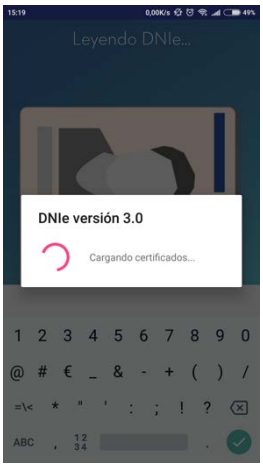

EJEMPLO DE ACCESO A PORTAL SEGURO
Selección del CAN
El CAN es el identificador que permite establecer la conexión con su DNI electrónico.
Aparece en la parte frontal del documento físico.
MARIA
(AUTENTICACIÓN)"
Añadir nuevo DNIe


EJEMPLO DE ACCESO A PORTAL SEGURO
POLICIA CNP
Introduzca el CAN de su documento de identidad
Introduzca CAN
CANCELAR
ACEPTAR


Aproxime DNIe al dispositivo


Leyendo DNIe...
DNIe versión 3.0
Accediendo al DNIe...


Leyendo DNIe...
Introduzca PIN.
Introduzca contraseña
Contraseña
Mostrar contraseña
CANCELAR
ACEPTAR


Leyendo DNIe...
DNIe versión 3.0
Cargando certificados...


2:00
eIDASBrowser
Authentication Success

8 Adaptation Requirements for Service Providers

The final solution proposed for the mobile application is focused on offering a generic mobile application that offers an embedded generic browser enriched with additional functions to support the specific requirements of the authentication of Spanish citizens based on the use of either software certificates and Spanish DNIe 3.0. These particularities initially required the design of a specific application for each service that would like to support Spanish users, since it was necessary to use native code.

Thanks to the proposed solution, it has been possible to centralize in one single application the integration of the authentication with the Spanish DNIe 3.0 and the access through the eIDAS infrastructure. In this sense, the application does not require from the SPs to know the particularities of the Spanish or other authentication scheme.

Naturally, each SP must adapt its services to the operation of eIDAS, either directly modify its services or using gateways or adapters such as those provided in LEPS by ATOS and UAEGEAN. This adaptation is independent of whether the service is accessed through a standard desktop browser or a mobile device.

For the case of accessing through a mobile device, the only requirements imposed are those of a mobile device: smaller screen size and access through a touch interface. Most SPs are already concerned about themselves, to offer friendly interfaces adapted to the different devices that users use to access their services. The embedded browser used inside the mobile app, offers support for the most common elements used in web design such as HTML and dynamic elements like JavaScript.

The navigation of web pages through mobile devices is generally limited to light components due to the limitations of mobile devices, which are generally smaller. That is why, in addition to issues of support and licensing, that the components based on flash and other specific technologies are not supported by our application and in general by Android applications, being a requirement to be used correctly through mobile devices.

To summarize, the list of requirements impose for the eIDAS mobile environment is:

- eIDAS support.
- Responsive service interface.
- Limit the web components to JavaScript and common HTML components: avoid Flash or other kind of proprietary components.

From the user point of view, it is necessary the use of a mobile device with Android version Lollipop (5.0) or superior. In the specific case of wanting to interact with the Spanish DNIe 3.0, a mobile device with NFC capabilities it is also required.

9 Integration and preproduction tests by Service Providers

This chapter provides the description of test cases for pre-production environment taking into account the use of mobile app supporting software certificates and the Spanish DNIe 3.0 through NFC interface.

The objective of the integration and testing phase is to check the mobile application compatibility:

- With Greek and Spanish services
- Using different hardware devices
- With different Android versions

This chapter offers a specific section to each industrial partner to report the compatibility status between their services and the mobile application. Since the project is currently involved in the testing process and it is possible that some services will require to be evolved in base of the results of the tests done, the result analysed in this chapter is focus on only one service per partner.

9.1 ATHEX services

This section focuses on explaining the correct compatibility of the mobile application designed with the ATHEX services described in Section 2.3.2. For this, the use case "Accessing a portfolio of stock" has been selected, on which its current status and testing environment will be explained, and finally the results of the integration test carried out.

9.1.1 Use case overview

The selected use case to test the mobile application compatibility with ATHEX services is the user access to a portfolio of stocks. The following table shows the use case description in detail:

Description	An already registered User with an ATHEX e-Service wants to login. ATHEX e-Services offer the User the possibility of authenticating with her national eID, by using the eIDAS Network (eID-EU). The User proceeds to Login with the e-Service.
Preconditions	The user is a valid user for eIDAS. Holds a valid eID card. Is already registered to the ATHEX SP.
Process	1. The User clicks on the "Login with eID_EU" button. 2. The User is redirected to "Country Selection e-Form" (eIDAS API Connector UI). 3. In this page, the User selects the EU "country of origin". The same page also shows to the User, on a pop-up window, the list of personal attributes (mandatory and optional) requested by ATHEX e-Service. Instructions on how to use eIDAS for authentication and information on the privacy policy of ATHEX and LEPS project are provided in the margins of this page. 3. The User clicks on the "Next" button of the "Country Selection e-Form".

	4. The User is redirected to the ISP of her country of origin (or, before getting there, to other pages that show in detail the requested attributes). 5. The User successfully authenticates to this IdP (IdP e-Form). 6. The User provides consent on transferring the attributes obtained by this IdP to ATHEX (Consent e-Form). 7. (Upon authentication processing, operated by the eIDAS API Connector, transferring of data from the Connector to ATHEX, and information validation by the ATHEX application/service) The Use is redirected to the requested protected resource. 8. End of Test. (*) Protected resource: ATHEX AXIAweb: “Portfolio Access” page
Result	Successful access user’s shares

Table 9: ATHEX test use case

9.1.2 Preproduction test procedure

Conducting the preproduction cross-border tests of the ATHEX service (on a Xiaomi MI 5 device, using Android version 7.0 (MIUI 9.5.5.0)) is comprised of the following steps:

1. Installation of the eIDAS Browser app following the instructions of Section 7.1
2. Installation of the Spanish citizen test certificate on the device, following the instructions of Section 7.1
3. Launching the application and accessing the Service starting URL: https://test-axiaweb.athexgroup.gr/gr/login.htm
4. Performing the necessary steps as described in the test scenario.
    a. Using the “eIDAS Login” button.
    b. Selecting Citizen Country of Origin
    c. Authenticating via eIDAS
    d. Accessing the service

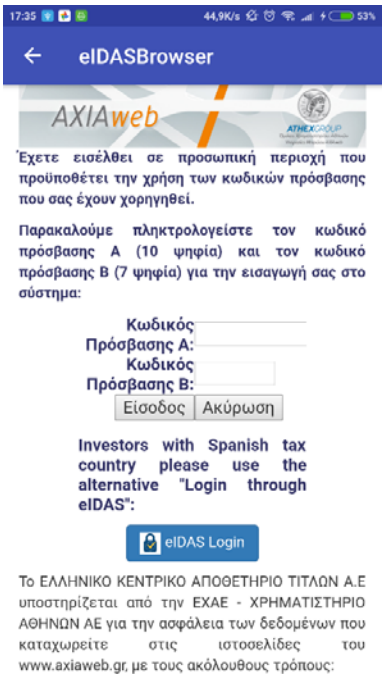
The cross-border test was conducting by authenticating the Spanish test user to the (Greek) ATHEX service. The test was made using the Spanish test user digital certificate, due to the unavailability of Spanish DNIe card to the tester. Therefore, the test showcases how a user (Spanish citizen) can use eIDAS to access the Greek ATHEX service.

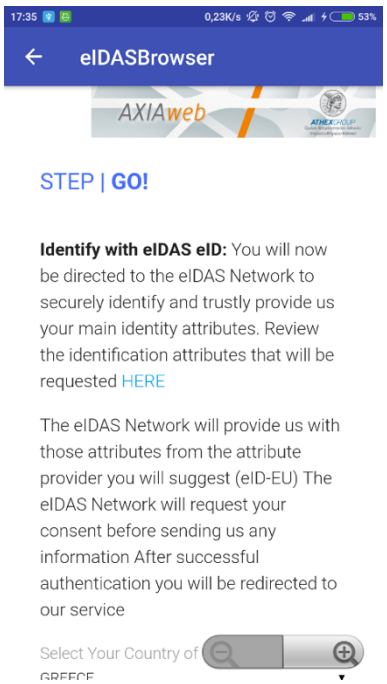
The system, in its entirety, is hosted by a Linux Server with the following hardware specifications:

- Intel(R) Xeon(R) X5650 @ 2.67GHz (4 cores)
- RAM: 4GB
- Disk: 100Gb

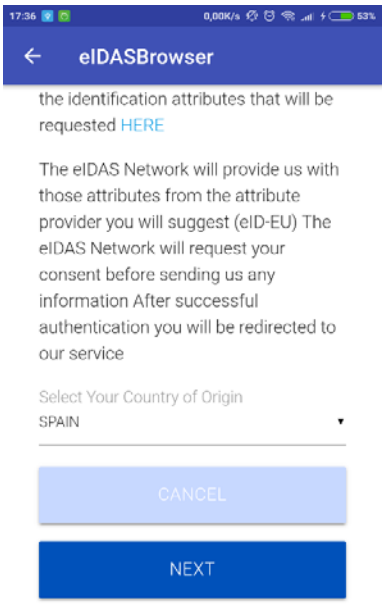
9.1.3 Screenshots of the running testcase

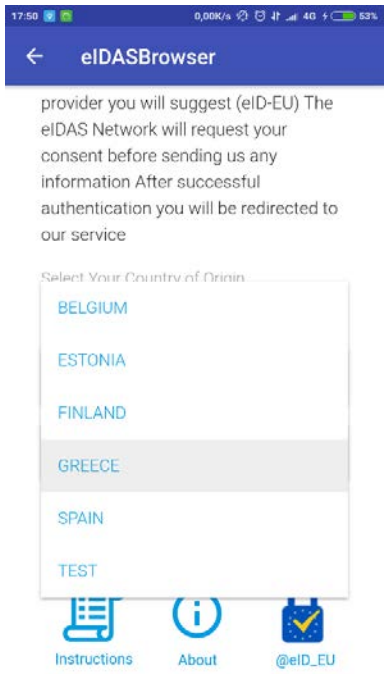
- The Spanish user accesses the ATHEX AXIAWeb service page and selects the “eIDAS Login” button



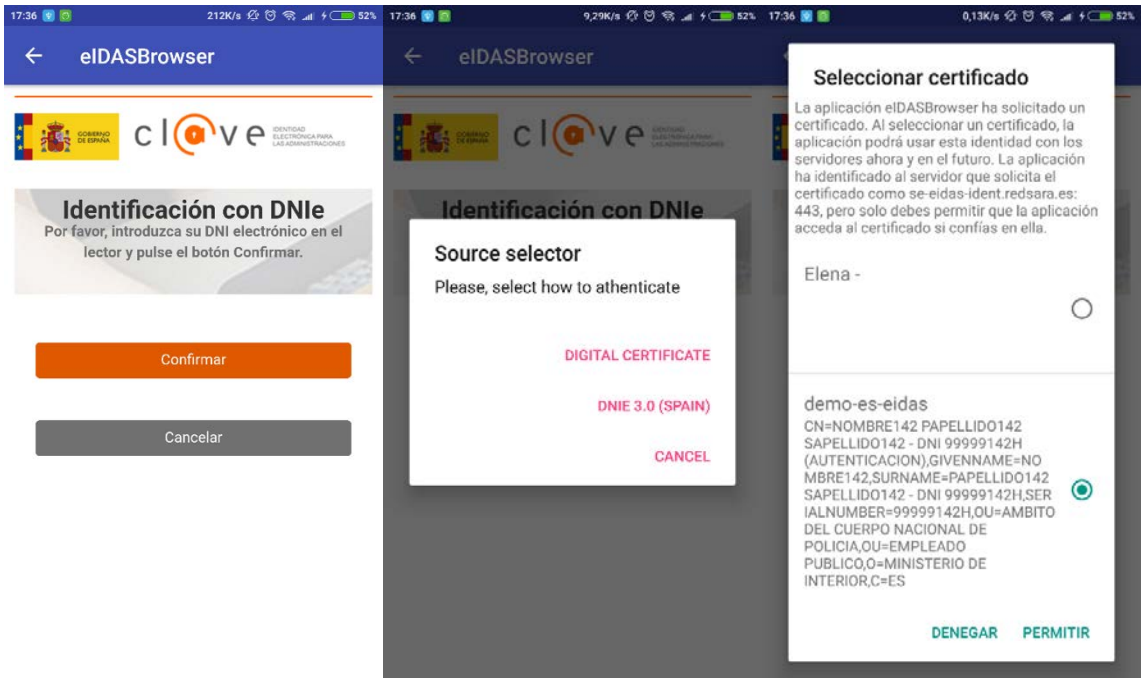


- The user is redirected to the Country selection page where Spain is selected as Citizen Country and clicks “Next”.

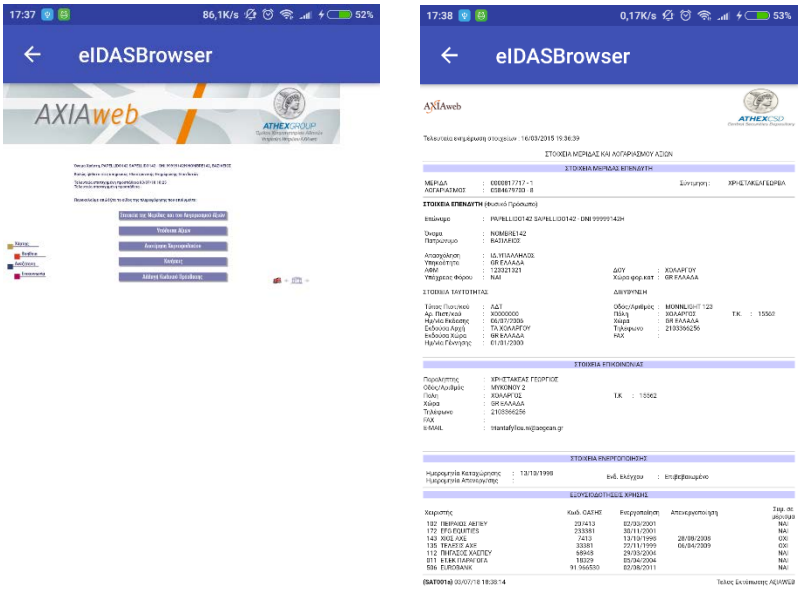




- The user is prompted by the LEPS eIDAS Browser App to select a method of authentication. In this scenario, the “Digital Certificate” Method is selected. The user is presented with a list of his/her pre-installed digital certificates and selects the appropriate one.



- The user is given access to his/her portfolio of stocks.



9.2 ELTA services

This section focuses on explaining the correct compatibility of the eIDAS Browser with the ELTA services described in Section 2.3.3. The selected use case in this case is “Zipcodes for Business Users“, on which its current status and testing environment will be explained, and finally the results of the integration test carried out.

9.2.1 Use case overview

The selected use case to test the mobile application compatibility with ELTA services is the user access to the Zipcodes for Business services. The following table shows the use case description in detail:

Description	A user connects to eltab2b.gr using eIDAS credentials in order to buy the Zipcodes file
Preconditions	The user is a valid user for eIDAS. Holds a valid eID card.
Process	1. The user accesses to **www.eltab2b.gr** and logs in using correct eIDAS credentials. 2. System responds upon successful login. 3. The user asks for the service pressing on “ZIPCODES”. 4. System responds showing the page with relative information. 5. The user selects to buy the product through selection “Add to Cart”. 6. The user selects to pay through the predefined “payment methods”.
Result	Successful buy of the product (zipcodes file).

Table 10: ELTA test use case

9.2.2 Preproduction test procedure

Conducting the preproduction cross-border tests of the ELTA service (on an LG G3-D855 device, using Android version 6.0) is comprised of the following steps:

1. Installation of the eIDAS Browser app following the instructions of Section 7.1
2. Installation of the Spanish citizen test certificate on the device, following the instructions of Section 7.1
3. Launching the application and accessing the Service starting URL: https://www.eltab2b.gr
4. Performing the necessary steps as described in the test scenario.
    a. Accessing the English version of the page
    b. Using the “LOGIN WITH EID_EU OR LENKEDIN” button.
    c. Selecting Citizen Country of Origin
    d. Authenticating via eIDAS
    e. Using the newly activated (after successful authentication) ZIPCODES button to access the service.

The cross-border test was conducting by authenticating the Spanish test user to the (Greek) ATHEX service. The test was made using the Spanish test user digital certificate, due to the unavailability of

Spanish DNIe card to the tester. The test showcases how a user (Spanish citizen) can use eIDAS infrastructure to access the Greek ELTA service (in this case, order the Zipcodes file).

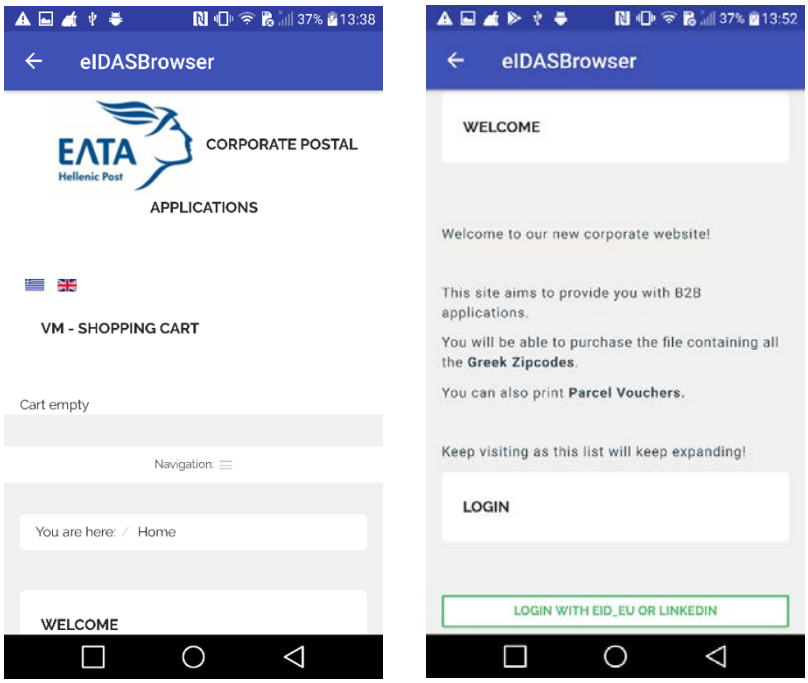
Pending work for this ELTA service is focus on adding real product content to the service. Only demo products currently exist in the service.

The specifications of the hosting environment are as follows:

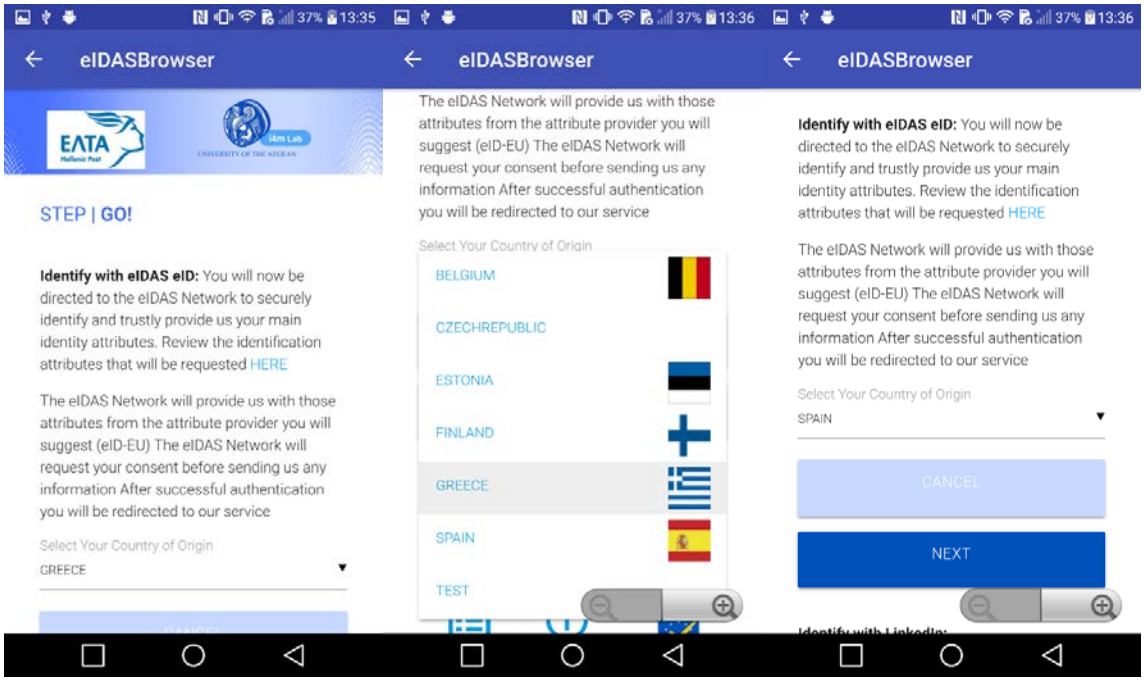
- the service itself (www.eltab2b.gr) is hosted on the Shared Hosting of Cosmote, on a Linux server.
- The software itself used the following software services:
  - PHP 5.6
  - Mysql 5.5.
- The eIDAS authentication module is hosted by a Linux virtual server (4.4.0-87-generic #110-Ubuntu) which is run by the vSphere 5.5 infrastructure, having the following hardware specifications:
  - CPU: 4 cores, Intel Westmere i7
  - RAM: 4 GB
  - Disk: 60 GB SAS, 15.000 rpm

9.2.3 Screenshots of the running testcase

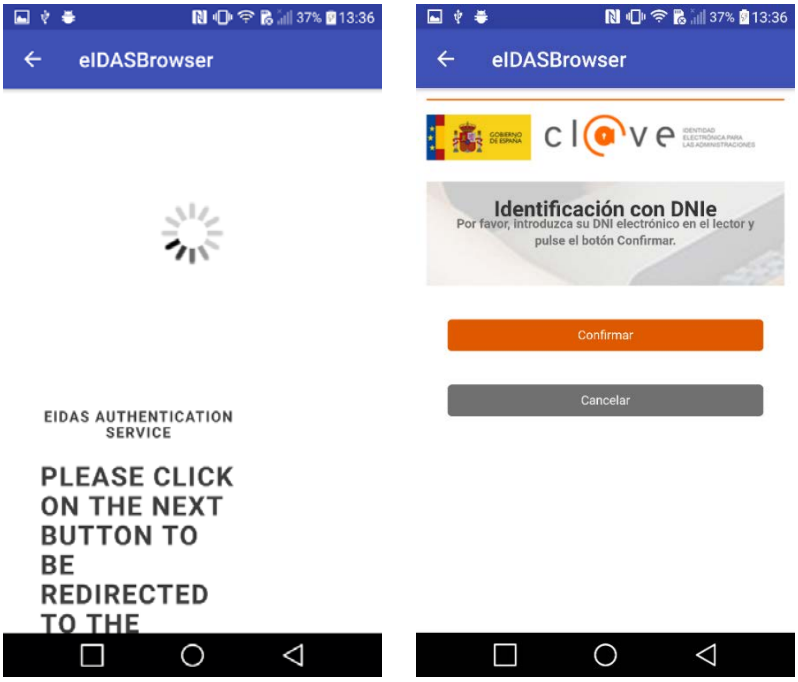
- The Spanish user accesses the English version of the ELTA page and clicks on the “LOGIN WITH EID_EU OR LENKEDIN” button



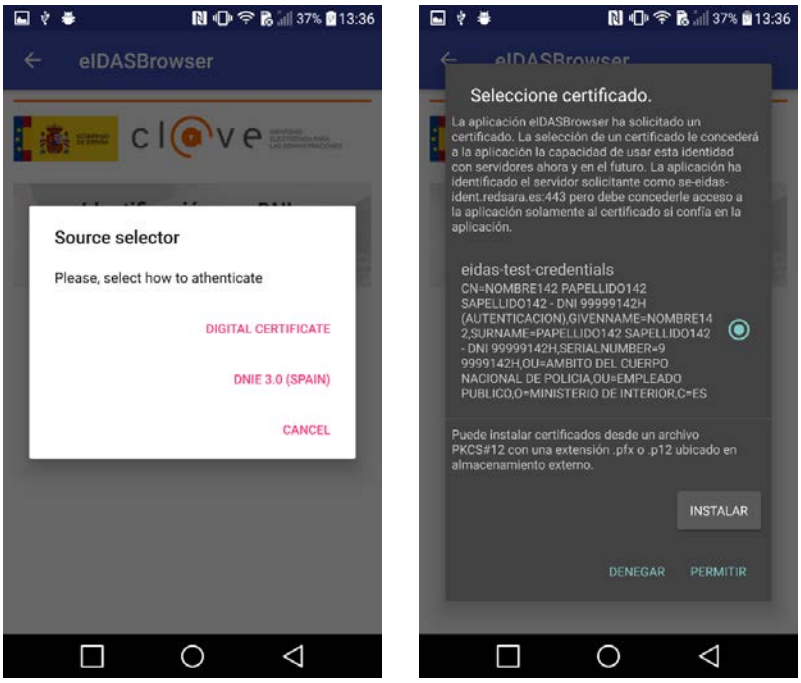
- The user is redirected to the Country selection page where Spain is selected as Citizen Country and clicks “Next”.



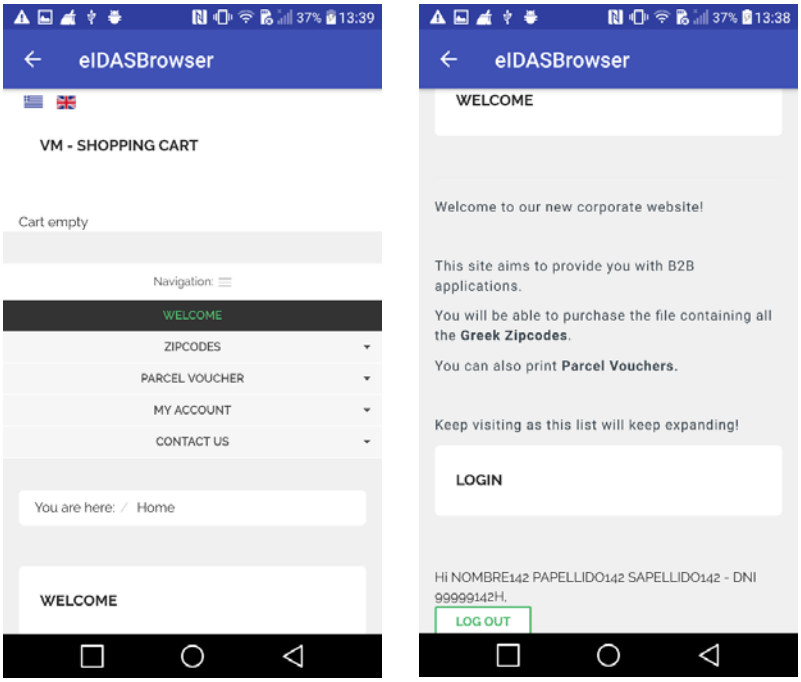
- The user is then redirected to the Greek eIDAS Connector which transparently redirects to the Spanish eIDAS Service



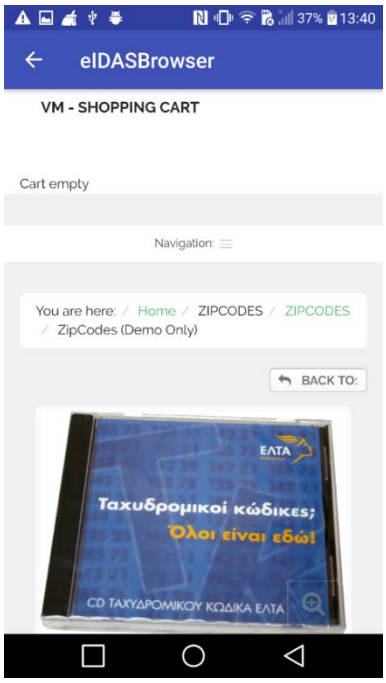
- The user is prompted by the LEPS eIDAS Browser App to select a method of authentication. In this scenario, the “Digital Certificate” Method is selected. The user is presented with a list of his/her pre-installed digital certificates and selects the appropriate one.

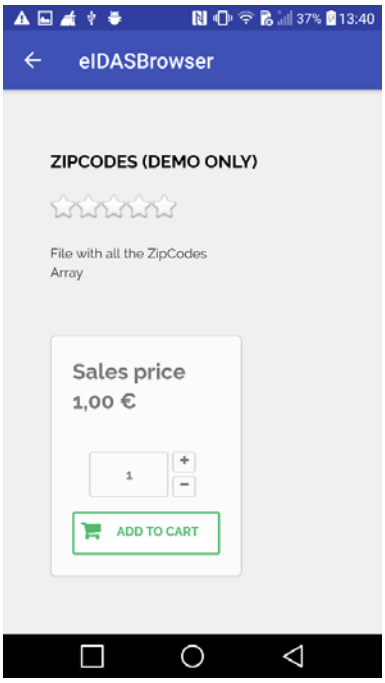


- The user is transparently redirected back to the Greek eIDAS Connector and then back to the ELTA Service page, as an authenticated user. The page has identified the user, displaying in this case, a greeting using the information provided by the authentication (Name, Surname).



- The user is now able to purchase the Zip Codes package.





9.3 Correos services

Within this section will specifically explained the test cases conducted on preproduction associated to the Correos digital services explained at chapter "2.3.1 Correos Services". Test cases are focused on Correos ID registration and login, as once done that, any due digital service of Correos will be accessible.

eIDAS IdP information has been uniquely linked to one Correos IdP (Correos ID). Like so, once the user is registered and accounts linked, user will be able to login with eIDAS at any moment.

9.3.1 Use case overview

The use case chosen to be tested with the mobile applications is the "basic login (SP & eIDAS registered user):

Description	A user from MS A (Greece) requests access to Correos Digital services (SP) in MS B (Spain). The user was previously registered in the SP. The user gets access to the SP successfully and access a specific service: "*Servicio B*" (called Service B).
Preconditions	The SP is registered in MS B (Spain) eIDAS node. The user from MS A (Greece) is a valid user for eIDAS. The user from MS A (Greece) was previously registered in the SP.

Process	1. Access to the service and then is redirected to Correos ID for login or directly access to Correos ID (https://miidentidadpre2.azurewebsites.net/) and click on “eIDAS login”. 2. The user is redirected to eIDAS adapter. 3. The eIDAS adapter page asks the user for the country and user consent. The page is showing the right requested data and the user performs the selection correctly and clicks submit. 4. The user is redirected to the Spanish eIDAS node. 5. The Spanish eIDAS node displays a list of countries and ask the citizen for providing the origin country. 6. Once the citizen selects the country and click on Login button, she is redirected to the eIDAS network. 7. The user authenticates with his electronic identity a. The MS A (Greece) IdP asks for credentials, b. the user provides right credentials. 8. The user is redirected to eIDAS network and eIDAS adapter which validates the response and the SP checks that the user was previously registered in the SP and grants access to the user. 9. User moves to Services section within Correos ID and access to Service B.
Result	User has been granted access to Service B and navigates on it.
Preproduction particularities	At the time of the execution of the tests, steps 2-6 are emulated by a mock-up service since the connection with the Spanish node through ATOS connector is not yet authorized.

Table 11: Correos test use case

9.3.2 Preproduction test report

Environments preparation has been done in parallel by Correos (Correos Digital services customization) and ATOS (development of eIDAS adapter and connection to Spanish eIDAS node). Customization (already done and finished) of Correos services was done in preproduction and a specific mock-up was created to mimic the functioning of the adapter (steps 3 to 6). Customization included the so-called “sign with eIDAS” button at the front web of Correos ID (IdP) and then an “update with eIDAS” button at the profile page of each user.

Connection between adapter and Spanish eIDAS node is not stablished yet due to some delays for granting official access to private services, as it was not possible to connect to the Spanish ministry eIDAS node yet. Moreover, full process testing had to be done in 2 separated parts: Correos side with the mock-up and ATOS side with the adapter. Once the Spanish ministry allows ATOS to connect their LEPS adapter to the Spanish eIDAS node, integration tests will be done covering the full flow of information together.

Furthermore, tests were conducted manually and Selenium code was sent to UAegean for automatisation, but again, full process can’t be tested until Spanish ministry allows us to access preproduction. Moreover, the service accessed within the preproduction phase and without the full flow completed is “Service B” (*Servicio B*). It is a service designed specifically for testing purposes and

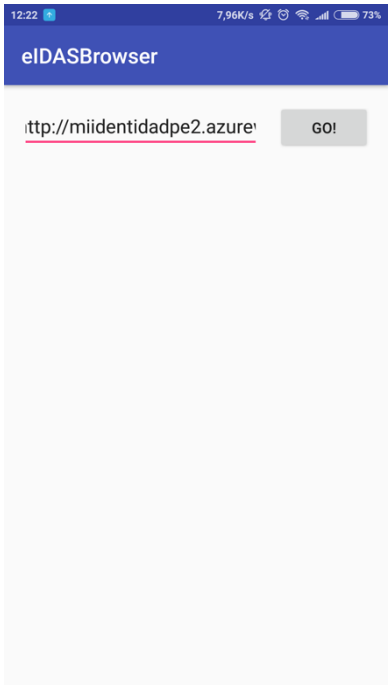
available in development environments. These tests were successfully conducted manually and all components are tested and validated, awaiting for the last integration “re-check”. Correos ID successfully grants access to users with eIDAS login tokens.

9.3.3 Screenshots of the running testcase

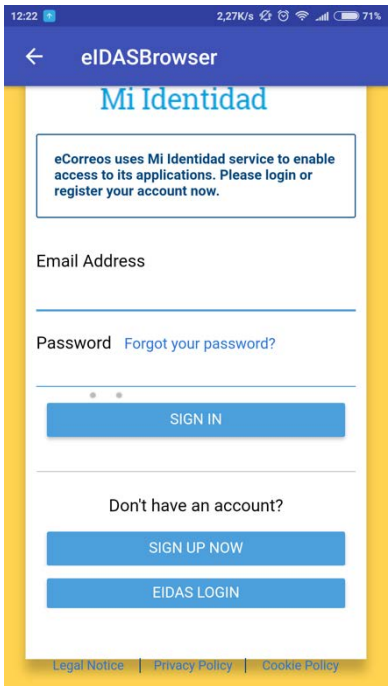
This section offers the proof of the successful use of Correos services functionality through mobile device. The screenshots cover the use case of opening the Correos Digital service within the mobile framework of LEPS project. Due to the delays in the registration process of the ATOS eIDAS Connector in the Spanish eIDAS node, the flow cannot be displayed completely and the demonstration of compatibility with the mobile application is limited to the interaction with Correos service. The connection to the eIDAS infrastructure is simulated by a mock-up service.

The order is settled by how the user will need to navigate:

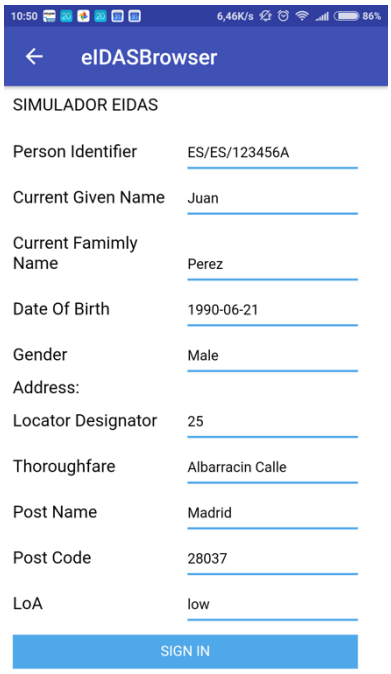
1. User opens the mobile app: “eIDAS browser”.
2. Search and access Correos ID preproduction webpage: https://miidentidadpre2.azurewebsites.net/.



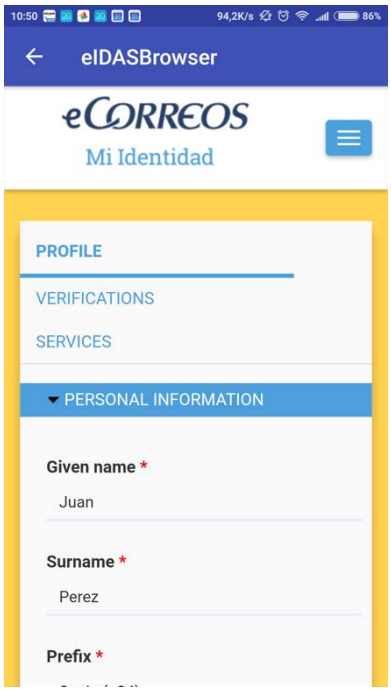
3. Clicks on “eIDAS login”.

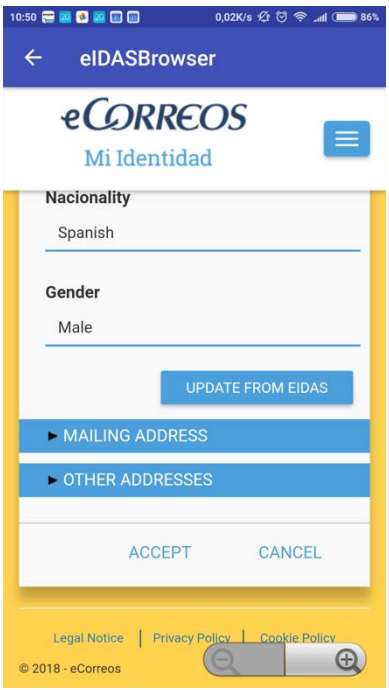


4. Mock-up is launched and simulated data from eIDAS adapter can be seen and/or modified.

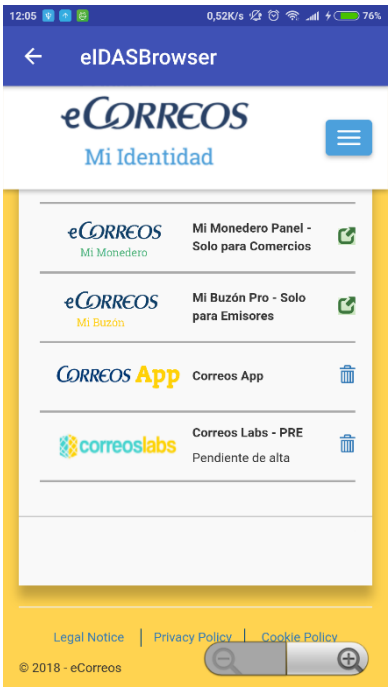


5. Once user clicks on “sign in” in the mock-up, its redirected to profile page of Correos ID. There can also be seen the possibility of “update from eIDAS”, further explained in other use cases.

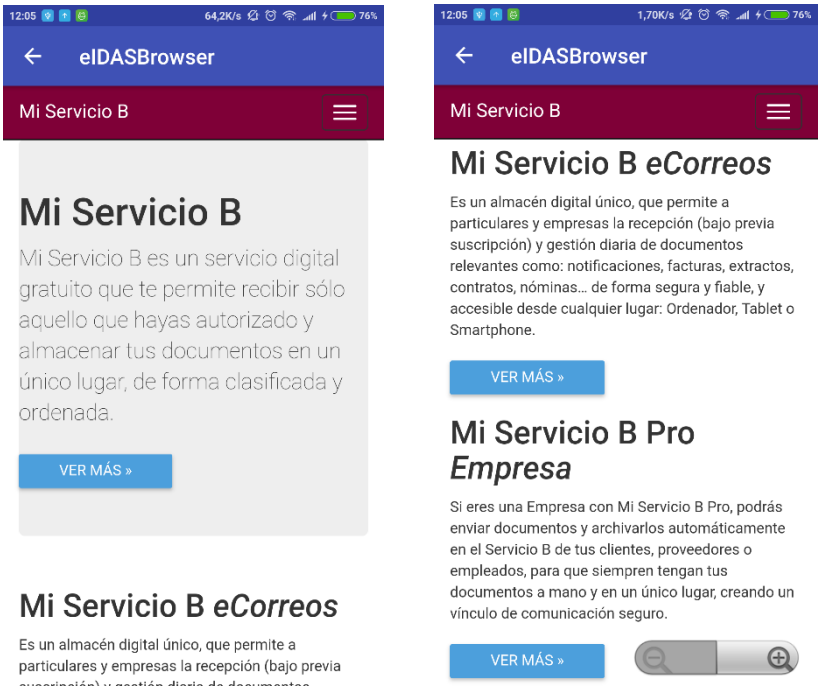




6. User access the “services” tab and then choose “*Servicio B*” service.



7. User is redirected to Service B and now can use it.



9.4 Mobile application development and testing report

The mobile application offers a generic embedded browser extended to give support to Spanish credentials that are official software certificates provided by the FNMT and the Spanish DNIe 3.0 with NFC support.

The initial tests have been very satisfactory, in particular with regard to the tested use cases described in this chapter. The tests have successfully allowed for using both types of authentication credentials for Spanish users and, at the same time, they demonstrated a correct visualization and navigation of the different services tested.

Of course, the application can be improved in several aspect to improve its internal code quality (simplicity, cleanliness, analysis of exceptional cases, ...) and also the user interface. Some of the issues detected during the development and initial integration tests are the following:

- Problems to test due to the immature state of Spanish node. It is still under development/deployment phase, so the node suffers frequent programmed stops and service drops that limit the testing work.
- The connection between the Greek and Spanish nodes is very recent (middle of May 2018), so it has limited the cross-border testing.
- During the development phase, it has been detected some unexpected issues around the Spanish DNIe authentication. It seems to be related with the private key's format expected by the Spanish IdP, but this problem appeared and disappeared without relation to the source code of the application.

- When testing tests on mobile devices with scarce hardware resources, some timeout problems have been detected due to the excessive generation of debug information that will be solved in future versions as it does not need to manage that extra debugging information.
- As seen, the Spanish DNIe cannot be emulated/simulated, and there is not available testing of options. This makes that all the tests done by Greek partners have to be done using the eIDAS testing software credentials.

In general, the issues detected are specific to the testing phase and will be solved as the testing progresses and the production phase is passed.

As seen throughout this section, the integration with the services provided by each member has been satisfactory. The services are shown correctly and the authentication process through the eIDAS infrastructure is possible, providing the authentication information correctly and appropriately to the intermediate eIDAS nodes as well as to the final services.

10 Conclusions

This chapter concludes LEPS activities related to the integration of mobile a application with LEPS services, thus offering a mobile experience for eIDAS authentication. To describe the eIDAS architecture and the mobile application context, Chapter 2 offered an overview of eiDAS architecture, of the Greek and Spanish authentication methods and the services integrated with eIDAS in LEPS by LEPS industrial partners. Chapter 3 presented the description of the eIDAS Mobile Authentication Scenario with the requirements derived from eIDAS architecture and components.

The analysis of the design principles for the mobile application, the effective design of the application operations, the technical decisions made, as well as the application implementation details have been presented in Chapters 4, 5 and 6. Chapter 4 has offered a detailed analysis of possible approaches to solve the “mobile authentication problem” and how we have opted for a single generic application for mobile authentication. Chapter 5 described the technical design details including the use case description, the user interface and internal organization of the application functionality. Chapter 6 extended the content of Chapter 5 the implementation details. Chapter 7 includes the guidelines and the tools to install in order to use and test the mobile application. It is important to highlight that the developed mobile application is SP agnostic and can work any web SP requesting eIDAS authentication for Spanish users. At the same line, other authentication methods (beyond the Spanish DNIe) could be easily integrated in the same code base, therefore extending the implementation to other EU member states.

Chapter 8 is focused on the adaptation requirements for SPs. Because of the design adopted, the requirements for SPs to adopt with the mobile application are practically minimal and limited to those of a mobile environment, i.e. responsive interfaces and the use of standard components such as HTML and JavaScript.

Finally, the process of integration and testing of the mobile application with services of the different partners has been described in Chapter 9, that demonstrates the compatibility and interoperability of the application with the needs of electronic services, the eIDAS Network and the Spanish authentication methods. The integration tests with three typical services provided by LEPS partners have been satisfactory. The services work correctly with the mobile application and the authentication process through the eIDAS infrastructure using username/password, software certificates and the Spanish DNIe 3.0 is performed successfully, returning according to the expectations the authentication information to the intermediate eIDAS nodes and the final services. It is expected that, during the testing phase, both the services and the adapters provided by LEPS as well as the mobile application, will improve further the proposed functionality and user experience.

11 References

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

[2] 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

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

[4] European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+eID, retrieved date 2018/05/23

[5] LEPS, deliverable lead author Pérez Baún, Juan Carlos: D3.2 Operational and Technical Documentation of Correos services customization. Deliverable of the LEPS project, 2018.

[6] European Commission, How does it work: Proxy to Proxy, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/How+does+it+work+-+Proxy+to+proxy, retrieved date 2018/05/23

[7] LEPS, deliverable lead author Pérez Baún, Juan Carlos: D3.3 Operational and Technical Documentation of SP integration. Deliverable of the LEPS project, 2018.

[8] LEPS, deliverable lead author Petros Kavassalis: D4.1/D5.1 Operational and Technical Documentation of SP (ELTA, ATHEX) customization. Deliverable of the LEPS project, 2018

[9] Cuerpo Nacional de Policía, DNI y Pasaporte, Diferencias DNIe y DNI 3.0, https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_038&id_menu=1, retrieved date 2018/06/22

[10] Cuerpo Nacional de Policía, 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

[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