FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Digital Onboarding in the Customer Registration Process for financial services and products

Miguel Rodrigues Pires

Programa Doutoral em Engenharia Informática

Supervisor: Prof. José Manuel de Magalhães Cruz

Second Supervisor: José Amaro da Veiga

Third Supervisor: Telmo Pacheco dos Santos

July 27, 2022

Digital Onboarding in the Customer Registration Process for financial services and products

Miguel Rodrigues Pires

Programa Doutoral em Engenharia Informática

Approved in oral examination by the committee:

Chair: Prof. António Miguel Pontes Pimenta Monteiro
Examiner: Prof. Rolando da Silva Martins

July 27, 2022

Resumo

Os bancos estão a adotar cada vez mais novas tecnologias para melhor identificar novos clientes, autenticar com segurança os clientes atuais, proteger transações de alto valor e combater fraudes. O perfil do utilizador bancário mudou muito e, hoje, é inimaginável pensar no antigo modelo de atendimento em horário comercial. O cliente quer aceder à sua conta e fazer transações 24 horas por dia, sem depender de autorização de terceiros e muito menos deslocar-se às instalações.

Pretende-se que o registo num banco digital seja rápido e fácil, mas não inseguro. Pelo contrário, o processo de validação de documentos e análise de perfis deveria ser realizado sem falhas, de maneira transparente e confiável para as duas partes, o que é possível agora graças aos avanços tecnológicos. O Onboarding Digital torna 100% eletrónico todo o ciclo de registo de consumidores. Não seriam necessários mais papéis, reconhecimento de empresas e recibos para a abertura de uma conta. A interação humana direta apenas ocorre, eventualmente, em fases mais avançadas do registo e quando houvesse pendências ou dúvidas sobre a validação de um novo cliente. Cabe às fintechs o desafio de criar ambientes seguros e com comunicação eficiente para atrair e fidelizar os clientes.

A Agência para a Modernização Administrativa (AMA) é responsável por soluções de autenticação que visam garantir a segurança, física e eletrónica, reduzindo os riscos de fraude e preservando os direitos de confidencialidade e privacidade dos dados pessoais. De maneira a construirmos um sistema capaz de identificar quem uma pessoa realmente diz ser, recorreremos aos serviços desta agência governamental, nomeadamente oo Cartão de Cidadão (CC) e a Chave Móvel Digital (CMD).

Com este projeto pretendemos desenvolver uma plataforma web que automatize o processo de registo de novos clientes através do uso da *application programming interface* (API) da AMA e de outras agências do governo, como o ePortugal ou Portal da Empresa. Estas APIs irão permitir aos consumidores, através da introdução de dados sensíveis como o seu Número de Identificação Fiscal (NIF) ou nº de telemóvel, ou através da leitura do seu CC, a pesquisa rápida e segura de outros dados sensíveis que identificam o seu negócio privado ou a própria pessoa. Desta forma, o cliente sabe que está a dar consentimento para utilizar os seus dados, que depois irão ser guardados e usados para criar o perfil do nosso cliente. Além do registo de contas, estas APIs também poderão ser usadas como uma forma alternativa do utlizador se autenticar no *backoffice*, ou para verificar e validar o conteúdo de documentos.

Com este trabalho esperamos aprimorar o onboarding de futuros clientes no setor financeiro, poupando tempo tanto aos consumidores, na busca e preenchimento da informação, como aos profissionais do sector, na obtenção e validação dessa informação. A prova dessa conquista é a plataforma de Onboarding Digital desenvolvida com sucesso para a empresa Eupago.

Abstract

Banks are increasingly adopting new technologies to better identify new customers, securely authenticate existing customers, protect high-value transactions and fight fraud. The profile of the banking user has changed a lot and, today, it is unimaginable to think of the old customer service model during business hours. The customer wants to access his account and make transactions 24 hours a day, without relying on third-party authorization, let alone travel to the premises.

Registration in a digital bank is intended to be quick and easy, but not unsafe. On the contrary, the process of document validation and profile analysis should be carried out flawlessly, transparently and reliably for both parties, which is now made possible thanks to technological advances. The Digital Onboarding makes the entire consumer registration cycle 100% electronic. No more papers, company recognition and receipts would be needed to open an account. Direct human interaction only occurs, occasionally, in more advanced stages of registration and when there are pending issues or doubts about the validation of a new customer. It is up to fintechs the challenge of creating safe environments with efficient communication to attract and retain customers.

The Agency for Administrative Modernization (AMA) is responsible for authentication solutions that aim to guarantee physical and electronic security, reducing the risk of fraud and preserving the confidentiality and privacy rights of personal data. In order to build a system capable of identifying who a person really claims to be, we will use the services of this government agency, namely the Citizen's Card (CC) and the Digital Mobile Key (CMD).

With this project we intend to develop a web platform that automates the registration process of new customers through the use of the application programming interface (API) of AMA and other government agencies, such as ePortugal or *Portal da Empresa*. These APIs will allow consumers, by entering sensitive data such as their Tax Identification Number (TIN) or mobile phone number, or by reading their CC, to quickly and securely search for other sensitive data that identifies their private business or the person itself. In this way, the customer knows that he is giving consent to use his data, which will then be saved and used to create our customer's profile. In addition to account registration, these APIs can also be used as an alternative way for the user to authenticate in the backoffice, or to verify and validate the content of documents.

With this work, we hope to improve the onboarding of future clients in the financial sector, saving time both for consumers, in searching and filling in information, as well as for professionals in the sector, in obtaining and validating this information. The proof of that achievment is the platform of Digital Onboarding successfully developed for Eupago company.

Acknowledgments

First of all, I would like to express my appreciation to my supervisor, Professor José Magalhães Cruz, for guiding me throughout this journey, correcting my wrongs and helping me learn throughout the writing of this document. I would also like to thank the owners of Eupago for believing in me three and half years ago, giving me the opportunity to learn and grow as a person and professionally, and thank my work colleagues for their companionship, allowing me to learn about their challenges and contribute to them along the way. I would also like to give an "honorable mention" to the Commercial department, for all their support and efforts in helping me validate my project.

Everyone in my family has played a massive part in leading me by example and shaping the basis of what I am today, and for that, I am eternally grateful. A special thanks to my mother, who always believed in me, encouraging every decision I made, besides the bad ones. And to my grandfather, who was my "master" since I was a child, always looking out for me to grant his wish - for me to succeed in life.

Finally, a message of gratitude towards my friends, who extended my knowledge, shaped my character and provided many good memories.

Miguel Pires

"A wizard is never late, nor is he early.
He arrives precisely when he means to."

Gandalf the Grey

Contents

List of Figures

List of Tables

Abbreviations

AMA	Agência para a Modernização Administrativa
AML	Anti-Money Laudering
AP	Attribute Provider
API	Application Programming Interface
BCFT	Branqueamento de Capitais e Financiamento do Terrorismo
CA	Certification Authority
CACP	Código de Acesso Certidão Permanente
CC	Citizen Card
CMD	Chave Móvel Digital
CSS	Cascading Style Sheets
DMK	Digital Mobilte Key
DMKS	Digital Mobile Key Service
FA	Fornecedor de Atributos
GRPD	General Data Protection Regulation
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IBAN	International Bank Account Number
ICT	Information and Communications Technology
JS	Javascript
KYC	Know Your Customer
MVC	Model-View-Controller
NIF	Número de Identificação Fiscal
PEP	Politically Exposed Person
PPE	Pessoa Politicamente Exposta
QR	Quick Response
REST	Representational State Transfer
RGPD	Regulamento Geral sobre a Proteção de Dados
RDBMS	Relational Database Management System
SDK	Software Development Kit
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
VAT	Value Added Tax
UI	User Interface
UX	User Experience

Chapter 1

Introduction

1.1 Context

Banks are increasingly adopting new technologies to better identify new customers, securely authenticate existing customers, protect high-value transactions and fight fraud. The profile of the banking user has changed a lot and, today, it is unimaginable to think of the old customer service model during business hours. The customer wants to access his account and make transactions 24 hours a day, without relying on third-party authorization, let alone travel to the premises [48].

Registration in a digital bank is intended to be quick and easy, but not unsafe. On the contrary, the process of document validation and profile analysis should be carried out flawlessly, transparently and reliably for both parties, which is made possible thanks to technological advances. The Digital Onboarding makes the entire consumer registration cycle 100% electronic. No more papers, company recognition and receipts would be needed to open an account [29].

It is up to fintechs the challenge of creating these safe environments, and euPago, the company that advanced this dissertation proposal, is developing a platform to help with the onboarding of new customers with efficient communication.

1.2 Motivation

The digital onboarding concept is not always the same since each company or service may have different requirements when registering a new customer.

For the company euPago, it is needed accurate, trustworthy data about clients' businesses and their owners. EuPago already fetches some data from governmental Application Programming Interfaces (API) such as Portal da Empresa[1], but other necessary details, such as the person's private data, are still missing and will be collected through the traditional way, which is human interaction involved. In some cases, there is also the need to validate certain legal documents, like the proof of International Bank Account Number (IBAN) or proof of address.

[1]The ePortugal portal aims to facilitate interactions between citizens and companies and the State, making them clearer and simpler. The portal is the responsibility of AMA.

Currently, there are authorized solutions available through the Agency for Administrative Modernization's (in Portuguese Agência para a Modernização Administrativa, or AMA) API that provide this data without the need to contact the customer through an email or a phone call. Also, there is reliable technology to analyze these documents and validate them intelligently [3]. Using these new resources that are available together with those that already exist will allow euPago to automate its process of new customers registration, save time and human resources, improve customer support and respect their privacy.

1.3 Objectives

The goal is to allow any user to register himself as a customer in the companies' system without any potential involvement of a company employee. Direct human interaction only occurs occasionally, in more advanced phases of registration, and when there are pending issues or doubts about the validation of a new customer.

Using AMA's governmental APIs, the user, by simply entering sensitive data such as their fiscal number, mobile phone number, or even by reading their citizen card with a card reader, can quickly and securely fetch his companies' data. The customer will know and consent on how much of the company's data will be allowed to Eupago use, save and register in its customer profile. EuPago would also benefit of easy building and registering of clients database.

Another ambitious feature would be the automated verification of legal documents.

In addition, with the CMD integration, we can have an alternative way for an already registered user to login in Eupago's backoffice.

Besides this, it is aimed to provide the best possible User Experience by creating a friendly and intuitive interface (since the opposite can lead to the user giving up on the process).

Last but certainly not least, it is intended that the developed system to be fully compliant with GDPR (General Data Protection Regulation) and all local KYC (Know Your Customer) and AML (Anti-Money Laundering) directives [24].

1.4 Document Structure

In Chapter 2, a comparison with similar projects is made, as well as a State of the Art exploration on the multiple scopes of this project. Chapter 3 defines the problem as well as the main hypothesis and research questions. Architecture and implementation details are presented in Chapter 4 and the evaluation and analysis of the work is done in Chapter 5. Conclusions are reflected in Chapter 6.

Chapter 2

State of the Art

This chapter will dive deep into existing and similar work related to this project. First, the author clarifies the Definition of Onboarding to better chart the direction of the investigation. Second, a Background is provided for the reader to have context on some relevant work and information that precedes the findings present in the following sections. Then, there will be a comparison between similar technologies and similar existing platforms. To finish, the author will explain and overview the compliance area and the rules that this entire process must comply with.

The author states that, since this dissertation topic is common in other dissertation projects, he will take benefit of some of the research done by Maria Teresa Ferreira, which he thinks fits with his State of the Art investigation [19].

2.1 Definition

There are different onboarding concepts, and to start this section, we need to clarify which one we are going to work around for this project. According to the American dictionary Merriam-Webster, we have three definitions for onboarding [31]:

1. the act or process of orienting and training a new employee
2. the act or process of familiarizing a new customer with one's products or services
3. the act or process of converting data to digital form

The author will take a piece of each of these definitions, as in this project, the company will be orienting and familiarizing a new customer with their service and converting his data to digital form. More specifically, the author will focus on User Onboarding, which is often used for software products, and it can be done in a manual or automated way. In this case, will design new software to automatize the process so that new users are provided and acquire the necessary knowledge, skills, and behaviors in order to become official clients of the company [23].

2.2 Background

Since the company will need to identify their potential clients for their Digital Onboarding platform, the author focused his investigation and literature only on methods for authentication and identification of individuals.

Currently, the Portuguese citizens have at their disposal two significant technologies: the Citizen Card (CC) and the Digital Mobile Key (in Portuguese Chave Móvel Digital, or CMD). Both allow for authentication and digital signature.

In this section, the author will also address some concepts correlated to architecture and implementation to give the reader a context in the following chapters.

2.2.1 Citizen Card

The Citizen Card (CC) is a unique document that stores information relevant to a citizen's identification. The card stores data, both authentication and signature digital certificates, and some applications that are useful for the usage of the card, as is shown in Figure 2.1.

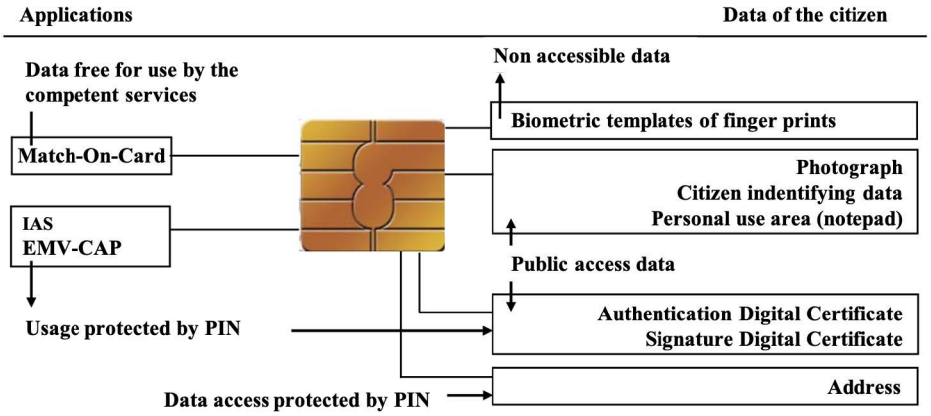

Figure 2.1: Smart card chip components and respective accessibility

The three applications present in the CC are as follows:

- IAS (no specification of this abbreviation was given in the documentation [6]): application responsible for the authentication and digital signature operations; its usage is pin protected;
- EMV-CAP (no specification of this abbreviation was given in the documentation [6]): application responsible for the generation of unique passwords through alternative channels such as by cellphone, for example; its usage is also pin protected; EMV-CAP stands for Europay, Mastercard, and Visa - Chip Authentication Program and it is a solution that banks initially used to mitigate online fraud regarding their operations;
- Match-On-Card: application responsible for the biometric verification of the digital fingerprints this is not pin protected.

The digital certificates present in the chip are the elements that provide the cryptographic guarantees of security promised and private keys. Even though there were no indicators of the presence of the private key in the chip in the documentation, in order for the operations promised to be possible, these keys are mandatory. This reflects a lack of transparency in the documentation.

Users' trust in these certificates stems from Certification Authorities (CA). These authorities are entities that hierarchically guarantee that the information present in the certificates, namely the public key that corresponds to that specific user.

In the past, the chain of trust was also composed of private entities, as the root CA was a private Portuguese company named "Multicert". This constituted a possible vulnerability as it is challenging to guarantee anything once the service was outsourced outside the government's jurisdiction.

This vulnerability has already been addressed, as every certificate emitted since April 2020 is now part of an entirely state-run chain of trust. Both the new and old root certificates are available for installation [42].

2.2.2 Digital Mobile Key

The CMD is a technology implemented in 2015 that allows authentication and digital signatures certified by the Portuguese State, and everything is done with a single login. It associates a cell phone number (SIM card), or an email address, to the civil identification number of each Portuguese citizen and the passport or title or card of residence for foreign citizens [7].

The practical information available revolves around activating the CMD, using its functionalities, and some "Frequently Asked Questions". In addition to this, there is some documentation available regarding operation practices, general conditions of usage, and policies for qualified signing.

The user can activate the CMD with their CC, and for that, they need a card reader and the authentication PIN given with the CC, or they can do it through the Portuguese finances portal if they have the Fiscal Identification Number and access passphrase. If none of these options are suitable, the users can also activate their CMD in person.

The security of the CMD is based upon two codes: the PIN the user introduces upon the activation of the CMD and a code that is received through text message to the associated SIM card. All the activities regarding this technology, such as emission, activation, usage, and revocation, are handled by the Service of the Digital Mobile Key (SCMD).

The SCMD is a Trustworthy System Supporting Server Signing (TW4S), which means the digital signing operations are done on the server and not on an environment controlled by the user. This means the private keys that are needed for the operations are obligatorily handled by a remote entity that provides that service.

The SCMD encompasses the following entities:

- Registration entity;
- Certification entity;

- Key pair generation and safekeeping entity;
- Qualified signature generation entity;
- Key pair holder, also know as signer;
- Trusting part, also know as recipient;

Regarding the technical documentation, many times the clarifications are busy with acronyms that make the reading and interpretation hard, and it is frequent that the processes are only said to be "safe", "trusted", or "secure" and do not disclose anything more about the basis of that said safety.

The documentation available presents the steps of the protocols implemented and these follow standardized procedures that are said to allow a high level of security. In these steps, however, the same lack of depth is present and the more technical aspects do not include deeper specification than for example referring to a "Hardware Security Module".

2.2.3 Applications Interface

For easy access to the functionalities promised, the users have at their disposal, through the Autenticação.gov portal, two different applications, depending on the device they use and/or the features they want [5].

The desktop version allows the user to sign digital documents; change Citizen Card PIN codes, among other features. The application has three main options:

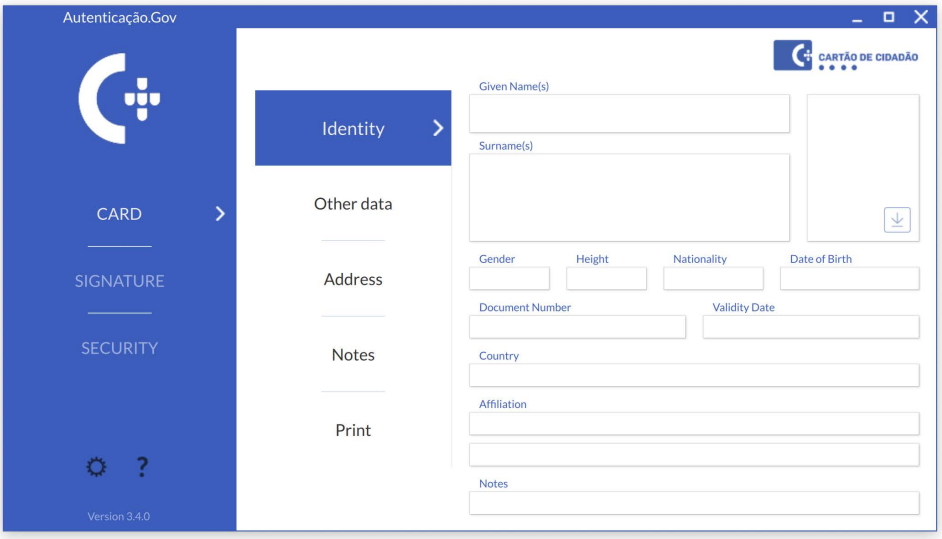

Figure 2.2: Desktop Application User Interface - Citizen Card Option

The Card menu option allows the user to access "all" the personal data stored in the card chip. This includes information like full name, height, document number, date of birth. The address

field is pin protected, allowing for an increased security level if the card is lost and accessed by an unknown party. This section also grants access to a personal notes field that can be edited with a PIN, and an interface for printing is also present. The general interface is as is shown in Figure 2.2.

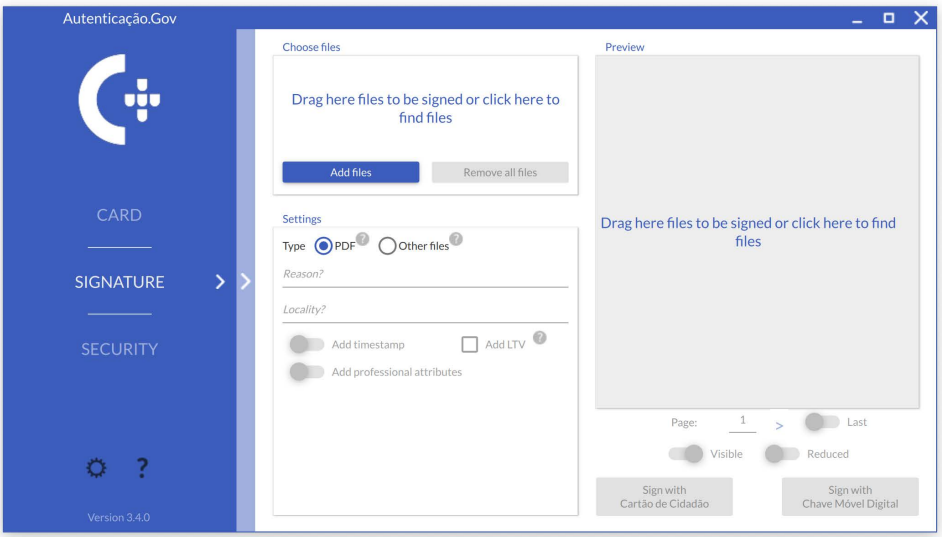

Figure 2.3: Desktop Application User Interface - Digital Signature Option

The Signature menu option features a "drag and drop" area that allows the digital signing of one or more files (PDF or other). The signing can be done through the Citizen Card or the Digital Mobile Key. The interface is as shown in Figure 2.3.

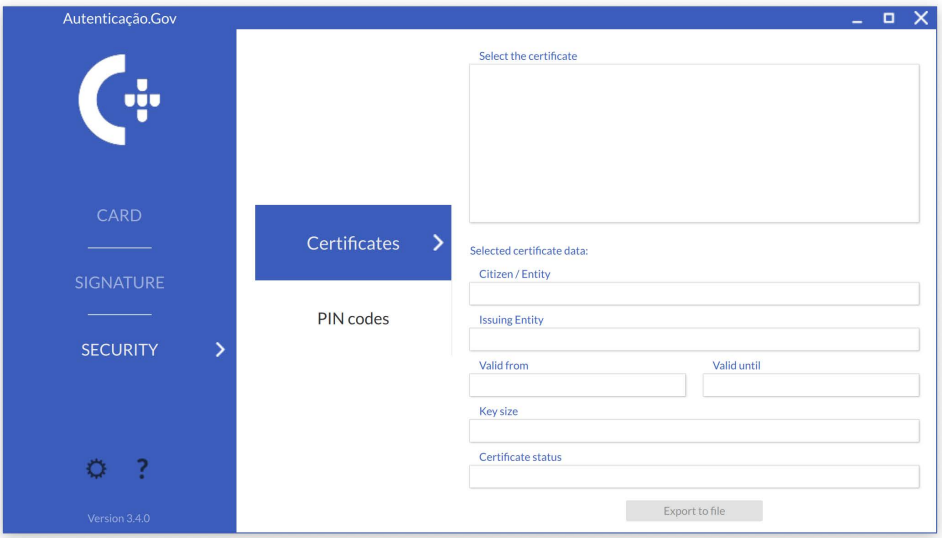

Figure 2.4: Desktop Application User Interface - Security Option

The Security menu option allows the user to access their certificates, check the certificates' information, such as the chain of trust, and download the certificates as files. This option also includes an area where one can test and modify the three personal pin codes: authentication, digital signing, and the pin to access the address information field. The interface is as is shown in Figure 2.4.

In contrast, the mobile application is an app for mobile devices (smartphone and tablet) that allows you to receive the security code of the Mobile Digital Key (CMD) through notification as an alternative to SMS. By installing the Autenticação.gov mobile application, users will immediately receive the security code through the app and no longer receive it by SMS, email, or Twitter 2.5.

It is not enough to uninstall the mobile application to receive the code again via SMS, email, or Twitter. It is necessary to disable the functionality of receiving the code via the app in the reserved area of the authenticacao.gov.pt website.

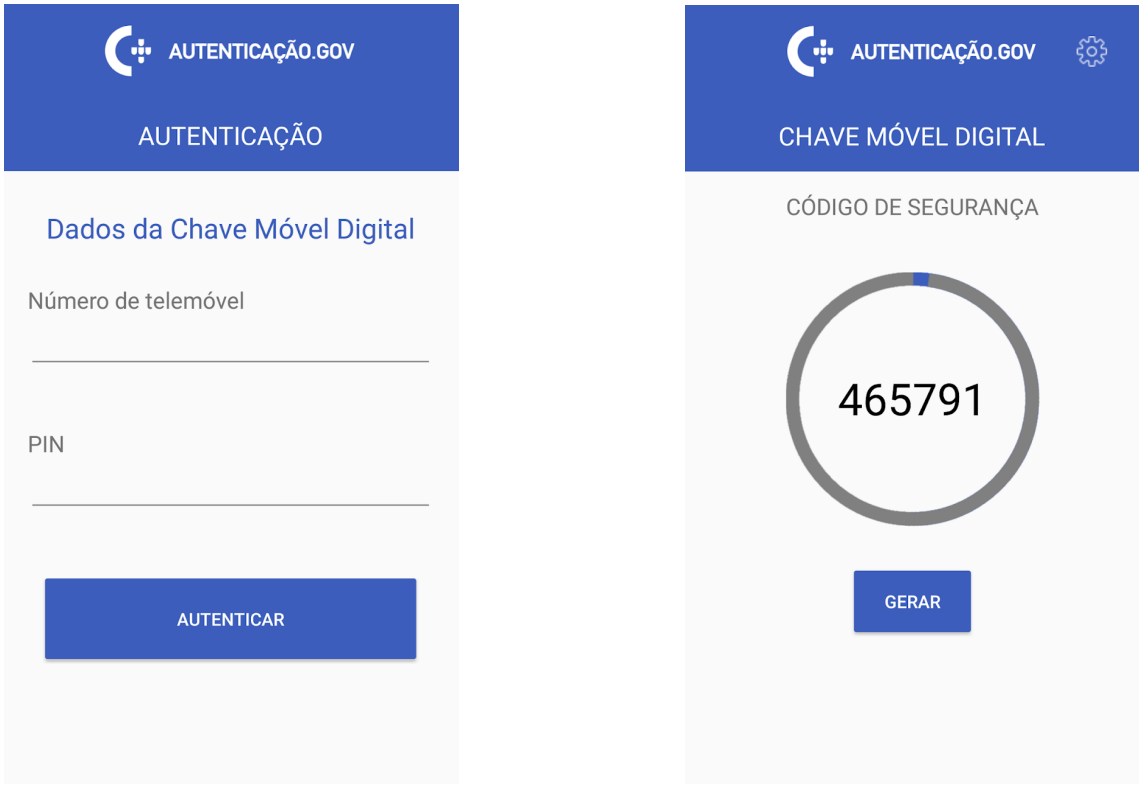

Figure 2.5: Mobile Application User Interface - Authentication form & CMD code

2.2.4 MVC Architecture

The MVC architecture is used for developing user interfaces, and its purpose is to separate business logic and presentation details, i.e., to separate internal representations of information from the ways information is presented to and accepted by the user. The related program logic is commonly divided into three interconnected elements [27], represented in Figure 2.6:

- **Models** - The backend that contains all the data logic, which is known as the lowest level that is responsible for maintaining and handling data logically;
- **Views** - The frontend or graphical user interface (GUI), which generates UI and data representation is done;
- **Controllers** - The brains of the application that controls how data is displayed, which is known as the "main person" because is the component that enables the interconnection between the views and the model, acting as an intermediary.

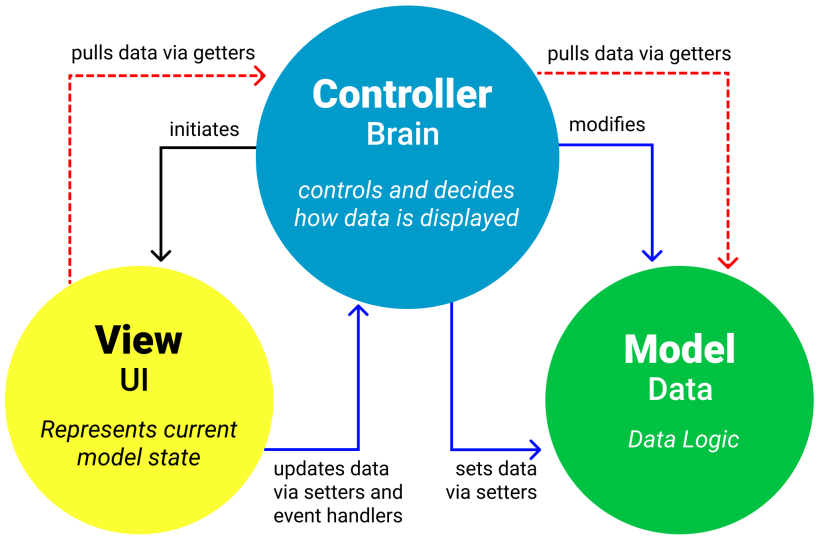

Figure 2.6: MVC Architecture Pattern [22]

2.2.5 MySQL DB

MySQL is a Relational Database Management System (RDBMS) developed by Oracle that is based on Structured Query Language (SQL).

Though often associated with Internet applications or web services, MySQL was designed to be extensively compatible with other technologies and architectures. The RDBMS runs on all major computing platforms, including Unix-based operating systems, such as the various Linux distributions, Mac OS, and Windows. MySQL's client-server architecture means it can support a variety of backends, as well as different programming interfaces. Data can be directly migrated from MySQL to its forks (e.g., MariaDB) and most other RDBMSs, thanks to architectural and language similarities.

The primary factor differentiating relational databases from other digital storage is how data is organized at a high level. These databases contain records in multiple, separate, and highly codified tables instead of a single all-encompassing repository or collections of semi- or unstructured

documents. This allows RDBMSs to optimize actions like data retrieval better, updating information, or more complex actions like aggregations. A logical model is defined over all of the contents of the database, describing, for example, the values allowed in individual columns, characteristics of tables and views, or how indices from two tables are related.

Though MySQL's relational nature and the ensuing rigid storage structures might seem restrictive, the tabular paradigm is perhaps the most intuitive and ultimately allows for superb usability. MySQL makes many concessions to support the broadest possible variety of data structures, from the standard but rich logical, numeric, alphanumeric, date, and time types to more advanced JSON or geospatial data. Beyond mere data types and an expansive built-in feature set, the MySQL ecosystem also includes various tools, easing everything from server management to reporting and data analysis.

Any individual or enterprise may freely use, modify, publish, and expand on Oracle's open-source MySQL code base. The software is released under the GNU General Public License (GPL) [34].

2.2.6 OAuth 2.0

OAuth 2.0, which stands for "Open Authorization", is a standard designed to allow a website or application to access resources hosted by other web apps on behalf of a user. It is an authorization protocol and not an authentication protocol. As such, it is designed primarily to grant access to a set of resources, for example, remote APIs or user's data.

OAuth 2.0 uses Access Tokens. An Access Token is a piece of data representing the authorization to access resources on behalf of the end-user. OAuth 2.0 does not define a specific format for Access Tokens. However, the JSON Web Token (JWT) format is often used in some contexts. This enables token issuers to include data in the token itself. Also, for security reasons, Access Tokens may have an expiration date [8].

Using OAuth 2.0, access requests are initiated by the Client, e.g., a mobile app, website, smart TV app or desktop application. The token request, exchange, and response follow this general flow:

1. The Client requests authorization (authorization request) from the Authorization server, supplying the client id and secret as identification; it also provides the scopes and a redirect URL to send the Access Token or the Authorization Code to;

2. The Authorization Server authenticates the Client and verifies that the requested scopes are permitted;

3. The Resource owner interacts with the Authorization server to grant access;

4. The Authorization server redirects back to the Client with either an Authorization Code or Access Token, depending on the grant type, as explained in the following subsection. A Refresh Token may also be returned;

5. With the Access Token, the Client requests access to the resource from the Resource Server.

In OAuth 2.0, the term "grant type" refers to how an application gets an access token. OAuth 2.0 defines several grant types and each grant type is optimized for a particular use case, whether a web app, a native app or a device without the ability to launch a web browser or server-to-server applications [38]. For this project, and as the reader will see in Chapter 4, Section 4.3, the author will only clarify the Implicit Grant Type.

2.2.6.1 OAuth 2.0 Implicit Grant Type

The Implicit Grant Type is a way for a single-page JavaScript app to get an access token without an intermediate code exchange step. It was created for use by JavaScript apps (which do not have a way to store secrets safely) but is only recommended in specific situations, and some servers prohibit this flow entirely due to the inherent risks of returning access tokens in an HTTP redirect without any confirmation that the client has received it [36]. At a high level, the flow has the following steps (see Figure 2.7):

1. The application opens a browser to send the user to the OAuth server;
2. The user sees the authorization prompt and approves the app's request;
3. The user is redirected to the application with an access token in the URL fragment (e.g., www.example.com#access_token=123).

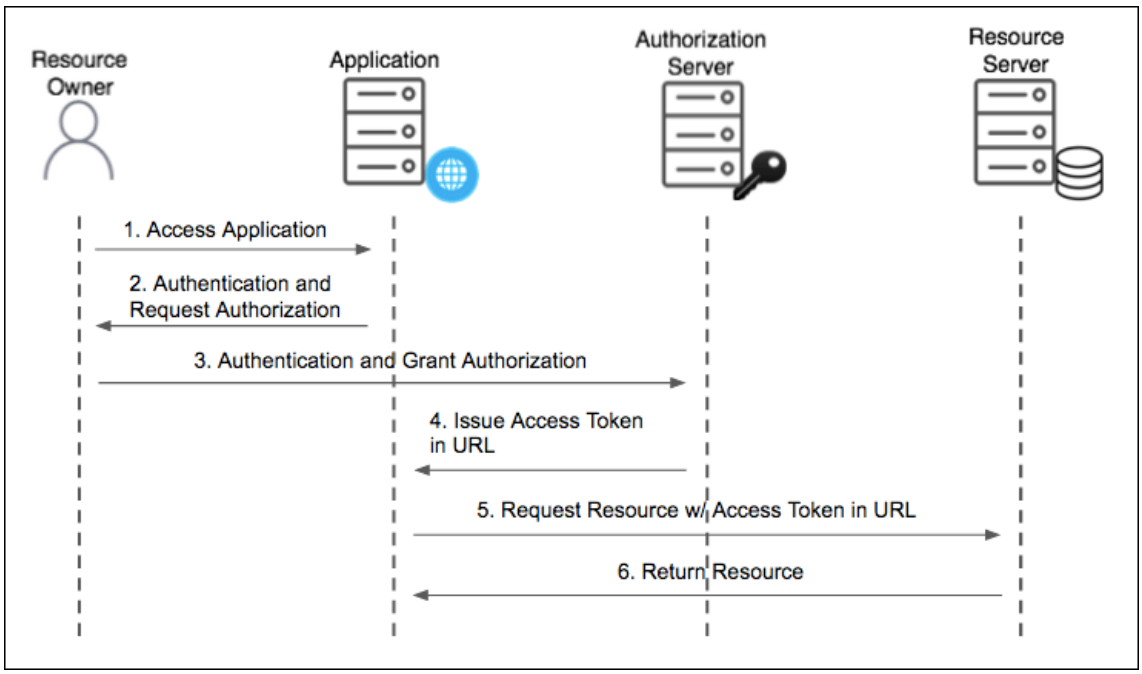

Figure 2.7: Representative flow diagram of the Implicit Grant type [47]

2.3 Similar Technologies

Within the national panorama, there is no other service like that of AMA. Therefore, one way of analyzing the Portuguese approach is comparing and contrasting with the solutions chosen and implemented by other nations. Several countries have been walking towards adopting new and more comprehensive integration of online government.

According to the United Nations' E-Government Survey for 2020, the top performers in e-government development are Denmark, the Republic of Korea, Estonia, Finland, Australia, Sweden, the United Kingdom of Great Britain and Northern Ireland, New Zealand, the United States of America, the Netherlands, Singapore, Iceland, Norway, and Japan [46].

Following is an exposition of the country at the top of the survey.

2.3.1 Estonia

Estonia is sometimes considered the most advanced digital society globally, and, at the moment, it has 99% of its governmental services online. They also have the goal of serving as an example of success, aiming to inspire others to follow their almost full digital integration of services [16].

The Estonian implementation focuses on the *X-Road*, a software solution that interacts with both the public and private sectors and that allows interoperability of services by over 1000 organizations, [25] this structure is depicted in Figure 2.8. The *X-Road* is federated, which means there is the possibility for a direct relationship between each part [16].

There is no fully integrated structure in Portugal, and the Estonian solutions that can be easily paralleled with the Portuguese ones are the ID-card and the Mobile-ID.

The Estonian ID-card is a "smart" identity card, with the digital certificates needed for the features it allows.

The Mobile-ID, similarly to the Digital Mobile Key, allows citizens to authenticate themselves and issue digital signatures through their phone, with a SIM card [26].

These implementations have had vulnerabilities such as issuing the same private key for different users or inclusion of information in the certificates that allowed for the retrieval of the private key [39]. These instances underline even more deeply the need to look with a critical eye even at government-approved technologies.

2.3.2 Denmark

In Denmark, the approach taken relies on the *"NemID"*, translated to English as "Easy-ID". It was implemented in 2007, and it is a single digital key that allows the citizens to access all the integrated features that span both the public and private sectors.

Denmark attributes its outstanding success primarily to two factors: the symbiotic relationship between public and private, and most importantly, the trust the population has in the government [12].

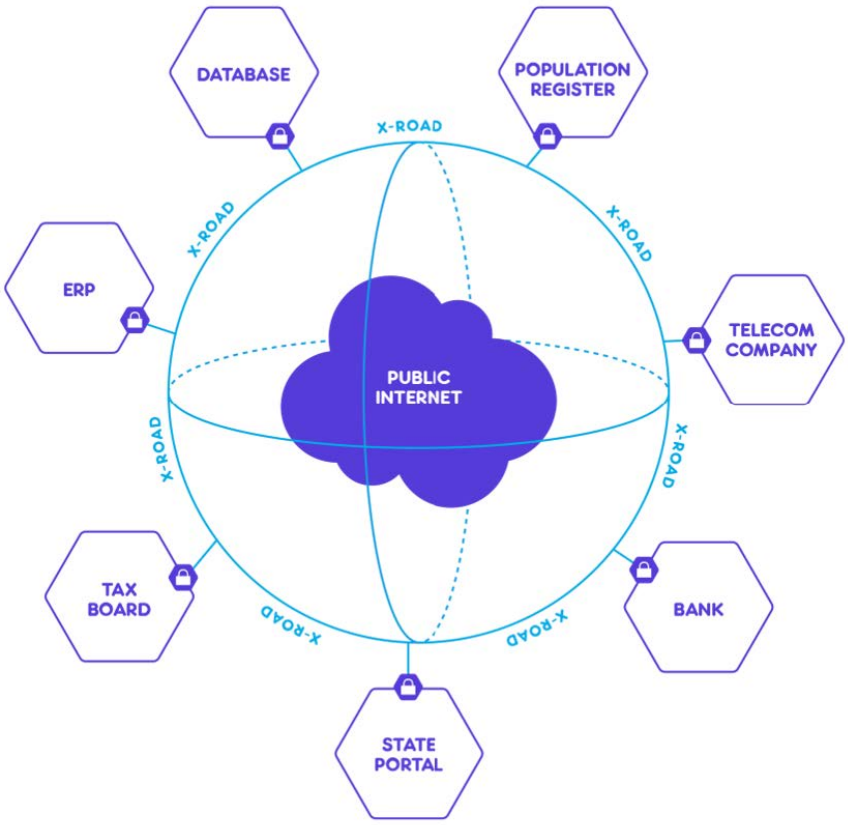

Figure 2.8: X-Road: data exchange layer visualization

The Easy-ID allows authentication in several portals, and this is done through the User ID, password, and a code. This code is taken from a physical user code card that can be seen in Figure 2.9, and it contains user-specific single-use codes. This duality of online paired with the codes is said to provide strong security [20].

Even though Denmark has one of the most deeply integrated digital governments, it is said that users experience several difficulties [43]. Despite this, the number of users is relatively high, which might not mean the system is well implemented and beneficial to the population and might only represent the mandatory use of some actions required [11].

There was no information regarding technologies that would provide the citizens of Denmark with the ability to issue digital signatures neither locally, as is done with the CC, nor remotely, as is done with the CMD.

Figure 2.9: Visualization of the needed information for digital authentication in Denmark

2.3.3 Republic of Korea

Despite ranking high regarding the level of digital governance implementation, South Korea is not part of the European Union, making the information taken from its study more limited. The European Union has legislation covering digital safety measures that Portugal, Estonia, and Denmark must follow to achieve the minimum sectary enforced for the EU members.

Korea has been implementing an extensive Information and Communications Technology (ICT) infrastructure. The components include:

- *On-nara BPS*: a platform that processes the government's work;
- *dBrain*: a platform that handles all governmental financial management activities;
- *GIDC*: which stands for Government Integrated Data Center and is a platform that integrates the management and operation of national IT resources [37].

South Korea has not developed a system similar to the ones mentioned previously regarding digital identification. Its digitization focuses more on the administrative side and not on user interaction. However, there are active plans to implement a digital ID system that makes use of technologies such as blockchain and biometrics [35].

2.4 Similar Platforms

A search was also made for services or platforms similar to AMA, and I found the following:

2.4.1 DigiD

DigiD stands for "DIGItal iDentificatie" or Digital Identification and serves as a virtual identification in the online services we do with government organizations, insurance companies, police, educational institutes, health institutions, and others [15].

The way it works is simple. Just like logging into our E-mail or Skype account, you use a "username" and "password" to connect, and from there, we have access to our data, change them, make orders or cancelations, all directly from our computer, anytime and anywhere [14]. In some organizations, we will also need to have the "SMS" option activated. This option is used to prevent someone from using your "username" and "password", pretending to be you. Thus, you receive a code via message on your mobile phone whenever you request access to specific government organizations. This code will have to be entered to proceed with access, as seen in figure 2.10.

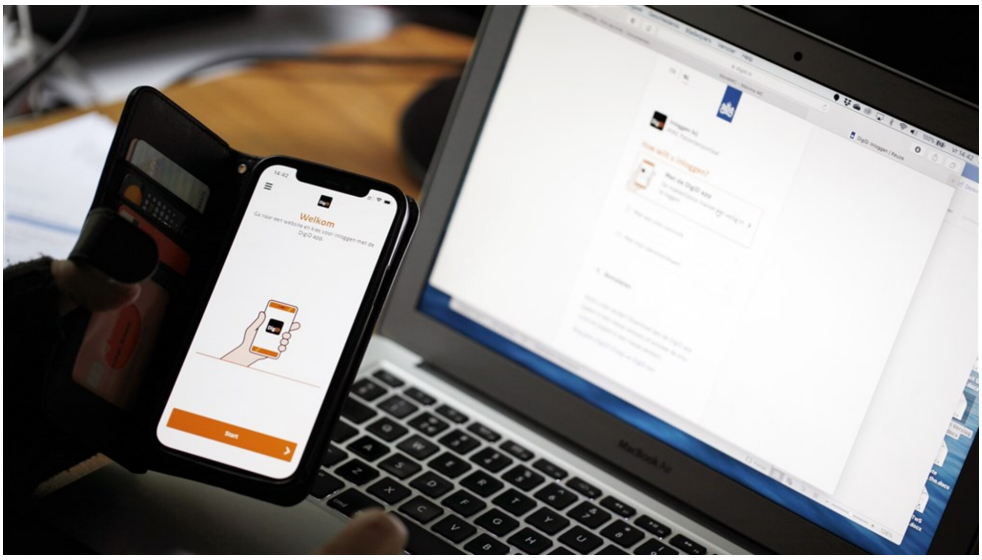

Figure 2.10: Using DigiD App to authenticate on an online service

The problem with this ID system is that it is still only possible to use it in Dutch, and the request to join can only be made by those who have a BSN (Burger Service Nummer) and are registered in a Gemeente, i.e., resides in the Netherlands [13].

2.4.2 Fourthline

Fourthline is one of Europe's fastest-growing fintech companies for digital KYC (know your customer). Trusted by banks, brokerages, insurers, and leading fintech companies, Fourthline verifies millions of identities for their clients with a proven end-to-end solution for bank-grade KYC. They provide best-in-class fraud detection at industry-leading conversion and compliance levels [21].

The Fourthline app (Figure 2.11) lets the user experience the digital KYC flow from the end user's perspective - from ID verification to liveliness check and more. The flow consists of three easy steps to confirm identity:

1. taking a selfie;
2. scanning an ID document;
3. enabling location and submitting the information.

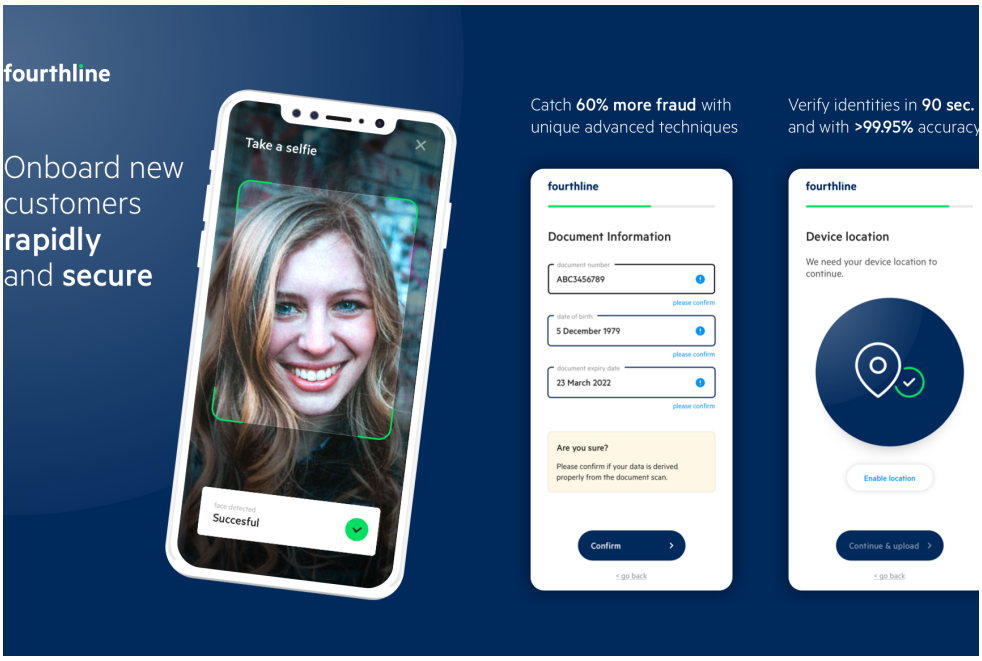

Figure 2.11: Fourthline app flow

2.5 Compliance

Another important detail is that the process of onboarding must be 100% compliant.

The term *compliance* comes from the English verb to comply, which is the act or process of complying with a desire, demand, proposal, regimen, or coercion. In the institutional and business scope, compliance is the set of disciplines in order to comply with and ensure compliance with legal and regulatory standards, policies, and guidelines established for the business and the activities of the institution or company, as well as to avoid, detect and address any deviations or nonconformities that may occur [30].

The idea of compliance programs has its origins in the United States and can be dated back to the turn of the 20th century when regulatory agencies began to emerge. However, it was due to financial institutions that compliance advanced. In 1913, the Federal Reserve System (US Central Bank) was created to design a more stable, secure, and law-abiding financial system. In 1977,

the FCPA (Foreign Corrupt Practices Act), the US transnational anti-corruption law, was enacted, requiring companies to (a) maintain books and records that accurately reflect their transactions and (b) establish an adequate system of controls internal [45].

The Compliance Department or Unit in an institution is responsible for ensuring compliance with all applicable laws, rules, and regulations, having a wide range of functions within the company (activity monitoring, prevention of conflicts of interest). It is the department with importance in maintaining the integrity and reputation of a company. While compliance costs have skyrocketed in recent years, the costs of non-compliance – even if accidental – can be much higher for the institution. Failure to comply with laws and regulations can lead to hefty monetary fines, legal and regulatory sanctions, as well as loss of reputation or even termination [24].

Due to the growing number of regulations, the Compliance Programs of an institution can cover numerous topics, ensuring compliance with rules derived from various areas of law, such as anti-money laundering (AML), export control, Environmental Law, and economic sanctions.

Since this project aims for the automatic registration of new clients, we also have to focus our attention on *Know Your Customer/Client* (KYC) guidelines and *General Data Protection Regulation* (GRPD) issues.

The *KYC* guidelines in financial services require that professionals make an effort to verify the identity, suitability, and risks involved with maintaining a business relationship. The objective is to prevent businesses from using criminal elements for money laundering. Related procedures also enable businesses to understand their customers and their financial dealings better. This helps them manage their risks in a well-judged manner. Today, KYC principles apply to banks as well as different online businesses. They usually frame their KYC policies incorporating the following four key elements [44]:

- Customer acceptance policy;
- Customer identification procedures;
- Monitoring of transactions;
- Risk management.

The *General Data Protection Regulation* (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR is an essential component of EU privacy law and human rights law, particularly Article 8(1) of the Charter of Fundamental Rights of the European Union. It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to enhance individuals' control and rights over their data and to simplify the regulatory environment for international business [18].

Personal data may not be processed unless there is at least one legal basis to do so. Article 6 states the lawful purposes are [18]:

- (a) If the data subject has given consent to the processing of his or her personal data;

- (b) To fulfil contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;
- (c) To comply with a data controller's legal obligations;
- (d) To protect the vital interests of a data subject or another individual;
- (e) To perform a task in the public interest or in official authority;
- (f) For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights (especially in the case of children.

Chapter 3

Problem and proposed solution

This chapter describes the problem tackled in this work, including the planned features and the expected result. Section 3.1 provides some key concepts used throughout the document, Section 3.2 presents the features to be developed in User Story format and section 3.3 shows technical requirements associated. Some developed preliminary work on the topic is presented in Section 3.4. Later, in Section 3.5, this work's proposed solution is presented and in Section 3.6 the factors for validating it. Lastly, in section 3.7, the project's schedule, including the tasks and risks considered, each with a short description.

3.1 Key Domain Concepts

There are some key concepts that will be mentioned throughout this document which are relevant to distinguish:

- **AMA** - the AMA website[1] and online platform, where users need to access to configure their DMK for the first time, and alter their passwords.
- **AMA API** - the API provided by AMA[2], that will power the onboarding platform, enabling users identification by fetching their details and information.
- **Informa D&B API** - the API provided by Informa D&B[3], that will power the onboarding platform, identifying if the users or the user's company belong to a sanctions list or are a PEP.
- **Beneficial Owner (BO)** - the term used to identify the individual who controls/owns a company, association, foundation, business entity, civil society [10].
- **Political Exposed Person (PEP)** - the term used to identify one who has been entrusted with a prominent public function. A PEP generally has a greater risk of potential involvement in bribery and corruption by virtue of his position and the influence he may exert [28].

[1] https://www.ama.gov.pt/
[2] https://github.com/amagovpt/doc-AUTENTICACAO
[3] https://directplus.documentation.dnb.com/

- **Sanctions Lists** - consolidated lists of companies, entities or individuals subject to financial or commercial sanctions by the United Nations Security Council or EU Regulation [17].

3.2 Problem Definition

The registration process in banks and fintechs is still very dependent on human intervention and monitoring. The employee has to make sure the person's identity is authentic, verify that the customer has delivered all the necessary data and is reliable, and validate required legal documents.

The project aims to develop a web platform that automates new customers' registration process through the application programming interface (API) of AMA and other government agencies, such as ePortugal or Portal da Empresa.

The features of the platform are described as follows, in User Story format[4]:

US1 - As a user I want to be able to input specific data required by the system and register it on the system.

US2 - As a user I want to be able to retrieve and edit some of my personal data kept by the system, so that my details are updated.

US3 - As a user I want to be able to leave the onboarding process on standby, so that I have more flexibility, not losing context or information if I resume the process some time later.

US4 - As a user I want to be able to register all the beneficial owners, so that my business complies with all the regulations.

US5 - As a user I want to be able to upload documents, where they are automatically validated, so that I don't need to contact any employee for technical support.

US6 - As a user I want to be able to authenticate in the backoffice using the DMK, so that I have yet another way to login.

3.3 Technical Requirements

Apart from the functional requirements above, the tool should adhere to the following technical requirements:

TR1 - The system should use the authentication API from AMA to authenticate users and provide session functionality.

TR2 - The system should use the API from Informa D&B to identify entities (organizations or individuals) that are PEPs or belong to sanctions lists.

TR3 - The system should send an email to alert the Compliance Department when an organization is identified as belonging to a santions list.

TR4 - The system should send an email to alert the Compliance Department when an individual is identified as a PEP or belonging to a santions list.

[4] In software development and product management, a user story is an informal, natural language description of one or more features of a software system. User stories are often written from the perspective of an end-user or user of a system.

TR5 - The system should send an email to alert the Commercial Department when the user finishes the Onboarding process successfully, in order to validate the information and give the user access credentials to the company's service.

TR6 - Changes and updates to the application should not cause total or partial outages of service.

TR7 - The tool should be available as a web application, able to work on any browser on any form factor (desktop, tablet, or mobile).

TR8 - The application requires an Internet connection.

TR9 - The system should be easy to use/friendly and intuitive.

3.4 Preliminary Work

Some preliminary work was done, namely:

- Downloaded the technical documentation for the integration with the Autenticacao.Gov system, from a provided URL protected by a password;
- Read and analyzed AMA's API documentation, where a template Excel sheet was filled out with necessary data and sent to AMA's technical support;
- Since my real-life/production environment DMK does not work for testing, I needed to set up a DMK on AMA's test/pre-production environment;
- While trying to create a test DMK, I needed to contact AMA's technical support because their test platform was not correctly working during the setup;
- After this issue was overcome, I could finally test their API, making some requests using the Postman[5] software [40].

3.5 Proposed Solution

The proposed solution is to create a web platform where customers can make the registration onboarding, and this workflow will have 4 phases:

1. In the first phase:
    - the user will have to, through his company Value Added Tax (in Portuguese Número de Identificação Fiscal, or NIF) number or Access Code of Permanent Certificate (in Portuguese Código de Acesso à Certidão Permanente, or CACP), provide the data of his business or company;
    - after retrieving his business' data, the user can review it and alter some of the fields before submitting it to create a new account;

[5] https://www.postman.com/

- once the account is created, the app does an entity screening by Organization Name in the Informa D&B API in order to verify it is in a Sanction List;

2. In the second phase:

   - because through the data previously collected, we know the number of managers associated with the company, each one of them must authenticate through the AMA portal in order for us to register as Beneficial Owners;
   - after the user is authenticated, using the full name provided by AMA, the app does an entity screening by Individual Name in the Informa D&B API in order to identify it as a PEP or it is in a Sanction List;

3. In the third phase, the user must upload certain legal documents to formalize the contract. Ideally, the system will somehow intelligently validate these documents appropriately as the case may be;

4. Finally, if all steps are successfully completed, the customer will only have to wait for a contact from the company's Commercial Department to close the contract. In the worst case, there may have to be some human intervention if there are pending issues or doubts about the customer's validation in some aspect.

3.6 Validation

I do not have any statistics or previous work to compare for this project, so I had to think together with my supervisors about how or what factors validate the developed solution. I believe the following points serve to prove that our approach meets the objectives:

- The result obtained is the same as if it were done by the Commercial and Compliance department, that is, the registration made manually by employees;
- Since the Compliance department works as if they were the company's auditors, it is important to highlight their role in the process, and if this department itself says that my software is OK, this is already a validation, since they are autonomous to the company;
- If my software is valid for auditors, it will also be valid for the entity that credits euPago, Banco de Portugal, which is a maximum proof of validation;
- Provide a comparison of the time it takes to complete the automatic onboarding process versus the manual registration process;
- Perform reasonable customer satisfaction inquiries and internal inquiries.

3.7 Schedule

3.7.1 Tasks

Development of the final product will go through several steps that should involve various tasks. The listing goes as follows:

- **Documentation Analysis and Setup** - Analysis of the AMA and Informa D&B documentation will involve a study of the code and testing of environments.
- **Technologies and Libraries Analysis** - Analysis of technologies to be used and solutions for documents validation.
- **Architectural Planning** - Structuring the code taking into account the architecture applied in the company and defining the operating logic.
- **Implementation of Onboarding Platform** - Development of the code for the platform itself.
- **User Interface and User Experience (UI/UX) Design** - Designing of the product's user experience and user interface.

3.7.2 Risk Analysis

The development of this product will face a series of risks that may be unable to deliver what was described before. We will now analyze a series of potential risks:

- **Time Constraints** - The task at hand is not complicated, but it demands much work, and the short amount of time available to complete it may make it impossible to deliver every single feature proposal at the end, especially the documents' validation step.
- **Third-Party Constraints** - The collaborative process of software development may experience delays due to constraints from our third-party service providers, AMA and Informa D&B.
- **Implementation Know-How** - The development of the product may be delayed by the time needed to acquire specific knowledge or abilities.

Chapter 4

Architecture and Implementation

This chapter presents the solutions to the problem presented previously. It explains the rationale behind them and why they were preferred over their alternatives.

First, the general architecture is described with the multiple components of the application. Afterward, each component is described in more detail regarding its functionality and implementation.

4.1 Architecture

This section describes the general architecture of the system, that is represented in Figure 4.2. It comprises multiple microservices, each handling a specific part of the overall work. The primary services are the ones dealing with the frontend application - the web application itself -, the AMA and the Informa D&B web services.

The web application service is managed using Portainer[1], a container management platform, that is built within a Docker[2] Container, allowing the service to be easily deployed and replicated across machines for scalability and fault tolerance. Portainer also ensures that every deployment is identical, regardless of the host machine and environment in which it is deployed. Additional web services are external to the company, and they are integrated into this solution by accessing them using the REST (Representational State Transfer) protocol.

Additionally, an instance of Nginx[3] running defines how the different services should interact with each other, allowing the company to start the application as one entity instead of multiple isolated containers. It conveniently provides internal DNS so services can reach each other by their service name, easily maps all dependencies and stores the connection to the database.

Storage containers are managed using MySQL[4], detailed in Section 2.2.5, which is configured to have data volumes for both staging and production environments, so that when the container is shut down the data is preserved on the host machine and can be recovered later when it restarts.

[1] https://www.portainer.io/
[2] https://www.docker.com/
[3] https://nginx.org/
[4] https://www.mysql.com/

PDO_MYSQL[5] is used to implement the PHP Data Objects (PDO) interface to enable access from PHP to MySQL databases.

The software's architecture the platform was built on one of the company's more recent repositories, which uses a more refined and updated project pattern according to today's standards, the Model-View-Controller (MVC) architecture, previously explained in Section 2.2.4.

Besides the three traditional elements of that architecture, there is also the Service element, responsible for complex logic associated with the external web services, AMA and Informa D&B. This layer returns just DTOs (Data Transfer Objects) [6], which for this case are formatted as JSON.

In this project, the author follows a server-client architecture.

The server-side uses PHP and presents as a REST API, handling some internal logic related to the company's operations, calls to all the external API services, and responds with appropriate JSON data. It is built using a micro framework called Slim[7], and since this framework does not have an ORM (Object–Relational Mapping), the author applies the MVC Repository pattern. By definition, the Repository Design Pattern mediates between the domain and the data mapping layers using a collection-like interface for accessing the domain objects [32]. The Repository Design Pattern separates the data access logic and maps it to the entities in the business logic, as seen in Figure 4.1.

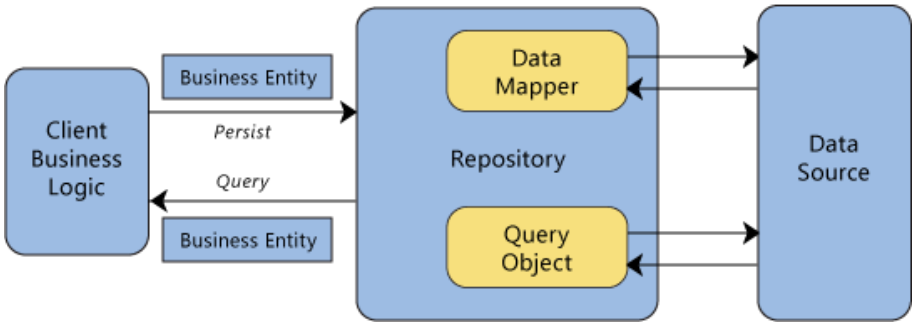

Figure 4.1: Interactions of the repository [32]

Since this platform is intended for the general customer, the easiest and most common client available to users is the web browser. The client-side renders some b̈are-bonesḦTML and CSS documents on the page, and the user makes the interaction with the server through HTML forms. Using Javascript (JS) and JQuery is also critical to do Ajax API calls and make the pages more dynamic [41].

[5] https://www.php.net/manual/en/ref.pdo-mysql.php

[6] A data transfer object (DTO) is an object that carries data between processes. This technique can be used to facilitate communication between two systems (like an API and the server) without potentially exposing sensitive information.

[7] https://www.slimframework.com/

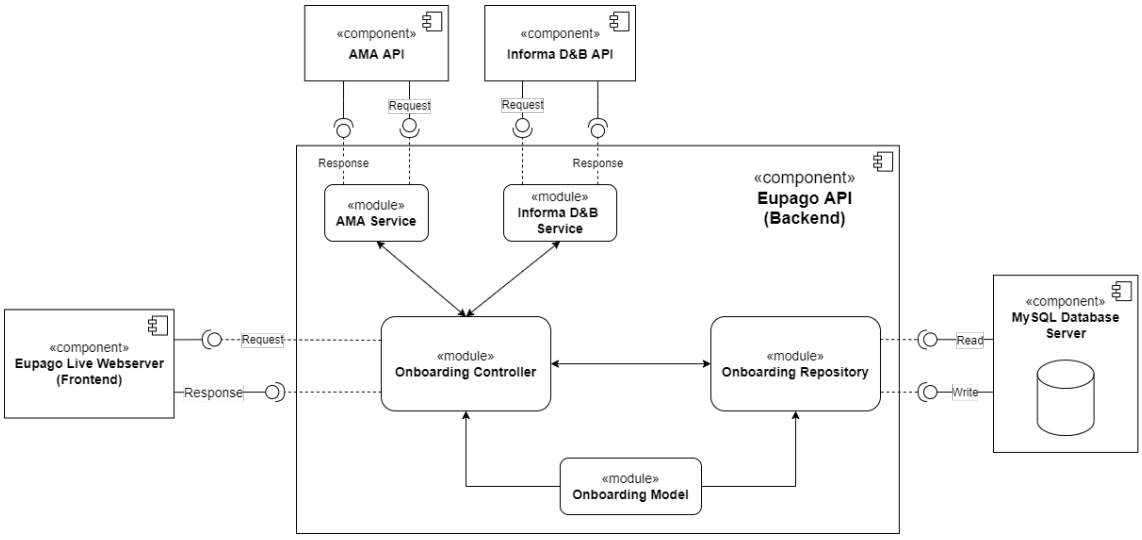

Figure 4.2: Architecture design of Eupago's onboarding system

4.2 MySQL DB

For this project a new table was created using the following query:

```
CREATE TABLE onboardingTokens (
    onboardingID int(9) NOT NULL AUTO_INCREMENT PRIMARY KEY,
    token varchar(255) NOT NULL,
    status enum('certidao', 'ama', 'documentos', 'concluido')
    NOT NULL DEFAULT 'certidao',
    cid int(9) DEFAULT NULL,
    createdAt datetime NOT NULL,
    updatedAt datetime NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
```

Listing 4.1: Query used to create onboarding data table

It is a simple data table, but it holds the primary logic for the onboarding operation. See the columns schema in Table 4.1.

`onboardingID` is the table's primary key, therefore cannot have `null` value and automatically increments with each record. `token` is a randomly generated unique string that will be the entry key for each user onboarding process. `status` represents the phase of onboarding the user is in, being 'certidao' phase 1 and the default value, 'ama' phase 2, 'documentos' phase 3 and 'concluido' phase 4. At the time of development these were the enumeration values that the author decided on, but in the future they may be changed to something more suitable. `cid` stands for customer (account) identifier, starts with `null` value and after phase 1 is done it is updated to the number of the account created. For utility purposes, `createdAt` is a column to store the date and time when the table entry was inserted and this value will not change throughout the

whole process, and `updatedAt` is to store the date and time when each phase of onboarding is completed.

Table 4.1: Onboarding data table schema

Column	Description
onboardingID	onboarding process identifier
token	token generated by Eupago's API to secure access for each onboarding
status	enumeration that identifies in which phase the onboarding process is at
cid	customer account identifier
createdAt	datetime in which the onboarding process is created
updatedAt	datetime in which the onboarding status is updated

4.3 AMA API

AMA created a new authentication system called Autenticação.Gov (AGov), including the CMD. This new method dispenses the physical use of the Citizen's Card, and may constitute a double authentication factor.

AMA's documentation shows that there are several ways to authenticate a citizen, namely through OAuth2, SAML (Security Assertion Markup Language), or QR (Quick Response) Code. AMA's Attribute Provider (in Portuguese Fornecedor de Atributos, or FA) uses these authentication methods to supply the citizen personal data to the requesting system.

During the project planning, the company decided to implement authentication via OAuth2, so we will only focus on this method in this document. The FA uses OAuth2's Implicit Grant Type to authenticate and return the requested attributes in two steps. First, it is necessary to obtain an authentication token (see Subsection 4.3.1), then it is necessary to make a REST request with that token in order to start the data acquisition process, and the FA returns an identifier of the authentication process that the requesting system must then use to make one or more requests to obtain data (see Subsection 4.3.2). This asynchronous flow can be represented in a simplified way by the following scheme:

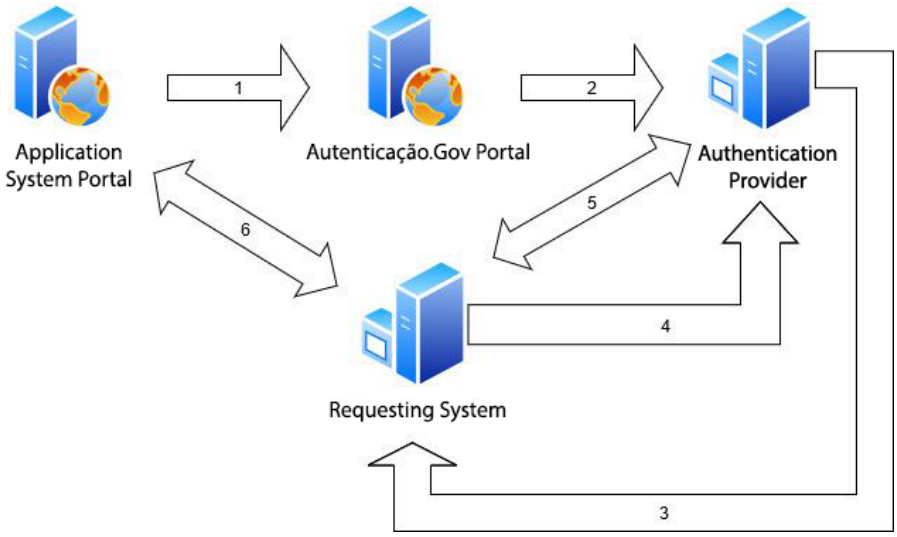

Figure 4.3: AMA asynchronous flow scheme via OAuth2. Adapted from [1]

4.3.1 First Step - Get AMA Token

Figure 4.4: Get AMA token flow. Adapted from [2]

Throughout the whole onboarding cycle, the AMA service is only used in the second phase of the process (see Subsection 4.5.2, which is where, after collecting the user's company information and knowing how many beneficial owners exist, in order to proceed, one of the owners must authenticate using the AMA service. The user can do this by clicking the form button, as seen in Figure B.6 of Appendix B, which makes a GET request to the FA website with the following input parameters in Table 4.2:

Table 4.2: FA Get Token request schema

Input	Description
response_type	query string with the value `"token"`
client_id	identifier of the requesting system, agreed in advance with AMA
redirect_uri	redirect URL, to get back to the requesting system. This parameter is optional and, if not sent, it will be returned to a static FA page. If the host of this URL is used, it must be previously agreed
scope	list of attributes delimited with a space between each one. It is mandatory to include the attribute `http://interop.gov.pt/MDC/Cidadao/NIC` for Portuguese citizens or the attributes `http://interop.gov.pt/MDC/Cidadao/DocNumber`, `http://interop.gov.pt/MDC/Cidadao/DocNationality` and `http://interop.gov.pt/MDC/Cidadao/DocType` for foreign citizens

There are more inputs, but the author only listed the ones necessary for this project, and these inputs should be included as query strings[8].

AMA provides both a staging environment, used by developers to test the service, and a production environment, when the solution is fully integrated. The FA OAuth staging endpoint is `https://preprod.autenticacao.gov.pt/OAuth/AskAuthorization` and the production endpoint is `https://autenticacao.gov.pt/OAuth/AskAuthorization`. An example of the final URL would be:

```
1  https://autenticacao.gov.pt/OAuth/AskAuthorization
2  ?response_type=token
3  &scope=http://interop.gov.pt/MDC/Cidadao/NIC http://interop.gov.pt/MDC/Cidadao/
       NomeCompleto http://interop.gov.pt/MDC/Cidadao/DataNascimento http://
       interop.gov.pt/MDC/Cidadao/NIF http://interop.gov.pt/MDC/Cidadao/NISS
4  &client_id=123456789
5  &redirect_uri=https://autenticacao.gov.pt/OAuth/Authorized
```

Then the user is asked to authorize the reading of the attributes by the requesting system. The user can then use the CC or the CMD to authenticate himself, as seen in Figures B.7, B.8 and B.9 of Appendix B, respectively.

Once the authentication is successfully validated, the client is redirected to the URL entered in the `redirect_uri` parameter previously, and the parameters shown in Table 4.3 are returned to the requesting system in the query string.

[8] A query string commonly includes fields added to a base URL by a Web browser or other client application. Each query string is made up from a parameter and a value that are joined together using an equals sign (=). Multiple Query strings are joined together using an ampersand (&). Query strings allow information to be sent to a webpage in a way that can be easily ingested and used within the webpage.

Table 4.3: FA Get Token response schema

Output	**Description**
token_type	query string with the value `"bearer"`
expires_in	long data type representing the lifetime of the access token
access_token	token generated by the FA to be used in the second step of obtaining the attributes

The requesting system must intercept these parameters, specifically the access_token. An example of the final redirect URL would be:

```
1  https://autenticacao.gov.pt/Oauth/Authorized
2  #access_token=11dd26e4-a1f4-4626-8834-001c00b9158c
3  &token_type=bearer
4  &expires_in=86400
```

Considering this grant type, the author does not think the Implicit Grant is the best practice for this authentication method because returning the Access Token as a parameter in the callback URL has a high potential token leakage. In addition, access tokens grants via the Implicit Flow cannot be refreshed without user interaction.

AMA should use the Authorization Code Flow because the Client can retrieve an Access Token and, optionally, a Refresh Token. It is considered the safest choice since the Access Token is passed directly to the web server hosting the Client without going through the user's web browser and risking exposure [9].

4.3.2 Second Step - Get AMA Attributes

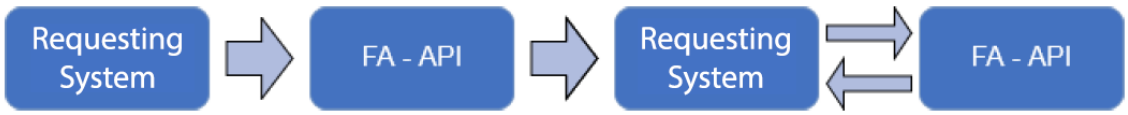

Figure 4.5: Get AMA Attributes flow. Adapted from [2]

After obtaining the access token in the previous flow, the requesting system has to validate it through a POST method to the FA API endpoint `https://autenticacao.gov.pt/OAuthResourceServer/Api/AttributeManager`, passing a JSON object of type (Table 4.4):

Table 4.4: FA Get Attributes request schema

Input	**Description**
token	token value obtained in the previous step
attributesName	string list of attributes to filter. This parameter is optional and if not filled, it will return all attributes related to the token.

In this case, the system just needs to pass the token since the goal is to obtain all the attributes. An example of this POST request can be seen in Listing C.1 of Appendix C.

The FA API returns a JSON object with the following attributes:

Table 4.5: FA Get Attributes response schema

Output	**Description**
token	token value equal to the one sent in the request
authenticationContextId	authentication process identifier

The requesting system must then use the token and authenticationContextId as query string values in a GET request to obtain the values of the requested attributes. The GET request format should be like this (see Listing C.2 of Appendix C):

```
1    https://autenticacao.gov.pt/oauthresourceserver/api/AttributeManager
2    ?token=11dd26e4-a1f4-4626-8834-001c00b9158c
3    &authenticationContextId=b3e98d70-dc69-4e5b-bafa-1849a35c1233
```

After the FA successfully validates the token, a JSON list is returned with the values of the obtained attributes. Attributes not yet obtained are returned with the value `null`, and the system repeats the same request every 2 seconds until it receives all the attributes or 30 seconds have passed, assuming that the requested attribute is unavailable.

```
1  {
2      [
3          {"name": "http://interop.gov.pt/MDC/Cidadao/NIC","value": "14103620"},
4          {"name": "http://interop.gov.pt/MDC/Cidadao/NomeCompleto","value": "Miguel
               Rodrigues Pires"},
5          {"name": "http://interop.gov.pt/MDC/Cidadao/DataNascimento","value": "
               10-05-1992"},
6          {"name": "http://interop.gov.pt/MDC/Cidadao/NIF","value": "210652268"},
7          {"name": "http://interop.gov.pt/MDC/Cidadao/NISS","value": null}
8      ],
9  }
```

Listing 4.2: JSON response with obtained user attributes

If any error occurs, it will come as the JSON in Table 4.6:

Table 4.6: FA Get Attributes JSON error schema

Error	Description
invalid_request	when it is an invalid request for example with empty mandatory fields
unauthorized_client	when client id is invalid
unsupported_grant_type	when the passed grant_type does not equals to token
cancelled	when user cancels login

This is the complete flow of how to authenticate with the CMD, ensuring that we will get the Beneficial Owner (BO) data and will also be helpful for the next part of the process explained in the following section.

4.4 Informa D&B API

Before we register a new beneficial owner based on the user's data, we first need to verify if it is a PEP or belongs to a Sanctions List. For that, we use the external Direct+ API, a service from Informa D&B (Dun&Bradstreet) that allows you to identify, enrich and monitor entities that you consider interesting for your business.

To work with the DIRECT+ API, we need to generate a security token before making any request for information. This is later to use this token in the request of the product to be obtained.

The request for this token is done by making a POST request to the endpoint `https://plus.dnb.com/v2/token`, sending Authorization data in the headers as «Basic <base64encoded Username:Password>», where Username is a consumer key and Password is a consumer secret, both agreed in advance with Informa D&B. The request body sends the grant_type as «client_credentials».

An example of this POST request can be seen in Listing C.3 of Appendix C. The response to this request, when successful, will return the information shown in Table 4.7:

Table 4.7: Informa D&B Get Token response schema

Output	Description
access_token	token to include in each API
expiresIn	token lifetime, displayed in seconds. It is usually 24 hours

Using this access token and the previously obtained AMA attributes, the system will make a POST request to submit an inquiry in Informa D&B Restricted Party Screening API, `https://plus.dnb.com/v1/screening/inquiries`. This operation is for initiating a screening request based on Organization name, Individual name, or DUNS (Data Universal Numbering System) number[9].

This external service is used at two different moments during the onboarding process. One is at the end of the first phase (see Subsection 4.5.1) after we get the company's data and create an account, we use that data to make an entity screening by Organization Name and verify if it

[9] A DUNS number is a unique nine-digit identifier for a business created by credit bureau Dun & Bradstreet. Dun & Bradstreet is one of the three major business credit bureaus. DUNS numbers have become the standard numbering system to identify businesses across the globe.

belongs to a Sanctions List. The other moment is at the end of the second phase (see Subsection 4.5.2) after the user authenticates using the CMD and we collect its attributes, we use that data to make an entity screening by Individual Name and verify if it is a PEP or belongs on a Sanctions List. This subsequent POST request, displayed below in Listing 4.3, is the same for both cases and it only differs on the `subjectType` and some parameters sent in the body. The system knows the `subjectType` based if data["organization"] is set to `true` or not in the body of the request.

```
1   public function createInquiryRequest($settings, $token, $data) {
2       $account_id = $data["account_id"];
3       $full_name = $data["full_name"];
4       $country_code = $data["country_code"];
5       $dob = isset($data["dob"]) ? $data["dob"] : "1970";
6       $address = isset($data["address"]) ? $data["address"] : "123";
7       $locality = isset($data["locality"]) ? $data["locality"] : "Porto";
8       $zip_code = isset($data["zip_code"]) ? $data["zip_code"] : "";
9
10      //  TYPES CAN BE: OrganizationName, IndividualName or DUNS
11      if($data["organization"])
12          $type = "OrganizationName";
13      else
14          $type = "IndividualName";
15
16      // environmental variable stores the Informa D&B Screening endpoint
17      // https://plus.dnb.com/v1/screening/inquiries
18      $url = $settings['Endpoint'] . $settings['Screening']['Inquiry'];
19
20      $headers = array(
21          "Content-Type: application/json",
22          "Authorization: Bearer " . $token
23      );
24
25      $body = array(
26          "customerTransactionID" => "EUPAGO_TRAN_ID_" . $account_id,
27          "inquiries" => [array(
28              "customerInquiryID" => "EUPAGO_CST_INQ_ID_" . $account_id,
29              "customerInquirySecondaryID" => "EUPAGO_CST_INQ_SEC_ID_" .
                    $account_id,
30              "subject" => $full_name,
31              "subjectType" => $type,
32              "birthDate" => $dob,
33              "address" => array(
34                  "addressCountry" => array(
35                      "isoAlpha2Code" => $country_code
36                  ),
37                  "addressLocality" => array(
38                      "name" => $locality
39                  ),
```

```
                    "addressRegion" => array(
                        "name" => $locality
                    ),
                    "streetAddress" => array(
                        "line1" => $address
                    ),
                    "postalCode" => $zip_code
                ),
                "notes" => "euPago screening search",
                "customerReference" => "euPago",
                "isGlobalSearch" => false,
                "screeningMonitoringMode" => "NoMonitoring"
            )]
        );

        $ch = curl_init();
        curl_setopt_array($ch, array(
            CURLOPT_URL => $url,
            CURLOPT_RETURNTRANSFER => true,
            CURLOPT_ENCODING => '',
            CURLOPT_MAXREDIRS => 10,
            CURLOPT_TIMEOUT => 0,
            CURLOPT_FOLLOWLOCATION => true,
            CURLOPT_HTTP_VERSION => CURL_HTTP_VERSION_1_1,
            CURLOPT_CUSTOMREQUEST => 'POST',
            CURLOPT_POSTFIELDS => json_encode($body),
            CURLOPT_HTTPHEADER => $headers
        ));

        $result = curl_exec($ch);
        $info = curl_getinfo($ch);

        if(curl_errno($ch)) {
            // echo 'Error: ' . curl_error($ch);
        }
        curl_close($ch);

        $response = json_decode($result, true);

        if($info['http_code'] === 200) {
            header('Content-Type: ' . $info['content_type']);

            return $response['inquiries'][0]['inquiryID'];
        } else {
            return false;
        }
    }
```

Listing 4.3: POST request snippet to submit inquiry

After much testing and analysis, the author figured that to optimize the retrieving results of entities and events from screening, the essential parameters to send in the body are the `subject`, `subjectType`, and `addressCountry`. If you are searching for a person or an individual, the `birthDate` should also be precise. The `addressLocality`, `addressRegion`, `streetAddress`, and `postalCode` should be specific if you are searching for an organization. Moreover, to keep the search faster and more precise, `isGlobalSearch` should always be set to `false` in order for it to only screen entities in the country sent. Otherwise, the system can get absurd results.

Getting a successful response from this method, we will receive some data in JSON format, but the most important parameter is the `inquiryID` inside the inquiries array, which is the unique identifier assigned by Dun & Bradstreet to track this screening inquiry.

```
{
    "transactionDetail": {
        "customerTransactionID": "EUPAGO_TEST_TRAN_ID_1",
        "transactionID": "rrt-049ab180350b1c6fb-a-eu-19141-984431-21",
        "transactionTimestamp": "2022-06-27T04:11:39.460Z",
        "inLanguage": "en-US",
        "serviceVersion": "1"
    },
    "inquiries": [
        {
            "inquiryID": "a3280733-5524-460d-bba2-2df1de79995c",
            "customerInquiryID": "EUPAGO_INQ_ID_2",
            "customerInquirySecondaryID": "EUPAGO_INQ_SEC_ID_2",
            "subjectType": "IndividualName",
            "birthDate": "1952-11-07",
            "address": {
                "addressCountry": {
                    "isoAlpha2Code": "RU"
                },
                "addressLocality": {
                    "name": "Moscow"
                },
                "addressRegion": {
                    "name": "Moscow"
                },
                "postalCode": "",
                "streetAddress": {
                    "line1": "123"
                }
            },
            "notes": "euPago screening testing",
            "customerReference": "Tester",
            "isGlobalSearch": false,
            "screeningMonitoringMode": "NoMonitoring",
            "subject": "Vladimir Vladimirovitch Putin"
```

```
        }
    ]
}
```

Listing 4.4: POST response snippet to submit inquiry

With this `inquiryID`, the last step of this service can be completed, which is retrieving results of entities and events from screening for a previously submitted Inquiry. A GET request to the endpoint `https://plus.dnb.com/v1/screening/inquiries/{inquiryID}` with `inquiryID` as path parameter must be made, and still sending the access token as «Bearer token» in the authorization header, as exhibited in Listing C.4 of Appendix C.

This last method response usually will return much information inside a JSON if there are matches regarding our inquiry search. It will provide results of entities (the individual or organization that it matched), and for each of these, it will provide different names it is known for, events, roles, news, people associated with, risk information (if its a PEP, belongs on Sanctions Lists) and much more information. Because of this, I decided not to include a snippet or preview of this data, regarding it's too extensive for the document.

If any entities were found, the most viable way to confirm the beneficial owner is or not a PEP or belongs to a Sanctions Lists is to compare the name collected from the AMA service with the personNames array found by Informa D&B service foreach entity. By testing, usually searching the first entity is enough. If there is a match, then the following step is to locate, inside that entity index, if exists a `pep` array, and if thats the case then it means that individual is a PEP. Futhermore, it is necessary to also locate if there is a `events` array, and inside that array to check if any of the events attribute `code` matches the string "SAN" or "WLS", which stands for "Sanctions" and "Watchlist and Sanctions", respectively. You can see this whole logic applied in Listing 4.5.

```
    $pep = 'N';
    $sanctions_list = 'N';

    $informaDB = new InformaDB();
    $informadb_token = $informaDB->generateToken($this->container->get('settings')[
        'InformaDBService']);

    if($informadb_token) {
        $individual_data = array(
            "full_name" => $full_name,
            "dob" => $date_of_birth_formated,
            "country_code" => "PT", //  PT is hard-coded because our customers are
                Portuguese
            "account_id" => $cid,
            "organization" => false
        );

```

```
16          $inquiry_id$informaDB->createInquiryRequest($this->container->get('settings
                ')['IrmaDBService'], $informadb_token, $individual_data
17          if($inquiry_id) {
18              $entities_list$informaDB->getInquiryByID($this->container->get('
                    settings')['InfaDBService'], $informadb_token, $inquiry_id
19              if(!empty($entities_list)) {
20                  $names_list = $entities_list[0]['personNames'
21                  foreach($names_list as $individual) {
22                      if($full_name ucwords(mb_strtolower($individual['fullName'], '
                            UTF-8'))) {
23                          //  Check if individual is PEP
24                          if(isset($entities_list[0]['pep'])) {
25                              $pep = 'Y';
26
27                          //  Check if individual is in Sanction Lists
28                          $events_list = $entities_list[0]['events'];
29                          foreach($events_list as $event) {
30                              for($i = 1; $i <= count($event['categories'][0])/$i++)
                                    {
31                                  if($event['categories'][0]['code'.$i] == "SA||
                                        $event['categories'][0]['code'.$i] == "WLS{
32                                      $sanctions_list = 'Y';
33                                      break 3;
34                                  }
35                              }
36                          }
37                          break;
38                      }
39                  }
40              }
41          } else throw new ApiException("TOKEN_INFORMADB_INVALID");
42      } else throw new ApiException("TOKEN_INFORMADB_MISSING");
```

Listing 4.5: Code logic for the Informa D&B service regarding the user

The code snippet in Listing 4.5 is from phase 2 (see Subsection 4.5.2) of onboarding, where it does an *IndividualName* search, but it works the same way for *OrganizationName* search, just set the `organization` parameter in the body to true, and inside the entities loop try to find a match in the OrganizationNames array instead of personNames. Moreover, If anything fails, exceptions are prepared to give a proper response (e.g., "Informa D&B token was not available in the request", "Informa D&B token is invalid").

If the system finds that the user is a PEP and/or belongs to a Sanction List, it will send an email to alert the Compliance department of Eupago accordingly. Same applies during the company register in phase 1. After that, the system will always save the user as a Beneficial Owner, taking into account the screening search results.

4.5 Web Application (Frontend)

The last component, arguably the most important, is the frontend web application, for it is how the users see the platform. For browsers, it is a set of HTML, CSS, and Javascript files being served by an Nginx web server, but many logic and data manipulation are applied that make this setup more complex than it seems.

The whole frontend application was built from the ground up, as well as the necessary backend logic for this project. The application provides multiple interfaces or pages that are dynamically rendered according to the status of the onboarding token included in the page URL. An example of an onboarding form URL is:

```
https://clientes.eupago.pt/api/extern/onboarding/form/{onboarding_token}
```

In order to have users start the automatic onboarding process, it is necessary to provide them with a link to the form, and for that link to work, an onboarding token needs to be generated. Since Eupago still has not decided how to apply this step, the author created an API internal endpoint specifically for this cause.

POST /api/intern/v1.02/onboarding/email – This endpoint generates a token, saves it by creating a new register in the `onboardingTokens` table of Eupago database and sends an email to the customer with the form link. Internal routes demand that the following headers are sent:

- Authorization header in the format «Bearer client_secret», where client_secret is an internal data secret
- X-Auth-Token header that can be created using JS like this:

```
1  var today_output = today.getFullYear() + (month < 10 ? '0' : '') +
       month + (day < 10 ? '0' : '') + day;
2
3  var admin_token = btoa('Auth-Token-Eupago-' + today_output);
```

The POST request body needs to send a JSON with the intended email value. The onboarding token is generated in PHP, calculating the `SHA-1` hash of a string using the *US Secure Hash Algorithm 1*[10], by the following code line:

```
1  $token = sha1(uniqid(mt_rand(), true));
```

[10]SHA-1 produces a 160-bit output called a message digest. The message digest can then, for example, be input to a signature algorithm that generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.

When the generated token is inserted in the data table, it creates a new `onboardingID`, it sets the `status` value to default, which is *'certidao'*, sets the `createdAt` and `updatedAt` columns to the Date and Time that request was made, and the `cid` column stays as `null`, for now. Figure B.21 represents the email that the user will receive after creating a new onboarding process.

The user can only access the automatic onboarding form if a random onboarding token was generated, stored in Eupago's database, and received a link with that token. By implementing this logic, the process is more secure, controllable and feasible, not being accessed by any third parties.

Having a form link with a generated token, PHP handles the routing and the URLs by rendering different views based on the onboarding token status present in the URL.

GET /api/extern/onboarding/form/:onboarding_token – This endpoint handles the routes rendering. It uses the `onboarding_token` query parameter to fetch from the database the `status` column value associated with that onboarding process and, depending on the status, it will render the appropriated view.

It is essential to point out that all the Eupago API routes containing `"/api/extern/onboarding/form/"` will only work if a valid token is provided, otherwise an error will be thrown. This measure reinforces security because if the token is missing from the URL or a fake token is sent, the API returns a missing or invalid token exception, respectively, and redirects the user to an error page.

Each phase of the onboarding process has its own purpose and logic, where the frontend communicates with the backend by doing Ajax[11] calls to each respective endpoint using JS. This section follows the proposed solution for the onboarding process presented in Section 3.5 and also mentions an extra feature associated with the technology used.

4.5.1 First Phase - Get Company Data

The onboarding process starts here. The first thing to do is get the data of the user's company, display it in the form for the user to analyse (see Figure B.3 of Appendix B) and potentially change some fields. Second, store the data to create an account. These can be achieved through the following endpoints:

1. **POST /api/extern/onboarding/form/:onboarding_token/validatecp** – This endpoint validates the CACP or the NIF input (see Figure B.1 of Appendix B) and fetches data associated with the user's company through external web services, in this case through ePortugal.Gov and Informa D&B. If any of these inputs are invalid, the error message shown in Figure B.2 of Appendix B is thrown.

2. **POST /api/extern/onboarding/form/:onboarding_token/register** – This endpoint uses the fetched company data and runs some internal business logic, thus creating a new account, an

[11] Ajax stands for Asynchronous JavaScript and XML. It is used to make asynchronous communication with the server. Ajax is used to read data from the server, update the page, or send data to the server without affecting the current client page. Ajax is a programming concept.

account channel, associating a commission plan to the account (see Figure B.5 of Appendix B), and runs a company screening, as mentioned in more detail above, in Section 4.4. If the email inserted already exists in Eupago's database, the exception displayed in Figure B.4 of Appendix B is thrown. If this method runs without errors, the last action it does is to update the onboarding token status for the second phase.

4.5.2 Second Phase - Get User Data

JS has a more significant role in this phase because it also has to manipulate data from an external source to the app. By clicking the button shown in Figure B.6 of Appendix B, the system requests the AMA authentication form and follows the workflow described in Section 4.3.1 (for interfaces see Figures B.7, B.8, B.9 and B.10 of Appendix B).

After the user is redirected back to the onboarding form with the AMA access token appended to the URL, when the page JS is fully loaded and the document is ready, it applies data manipulation to the URL address, splitting the output fragment from the endpoint, saving it into a variable and erasing it from the original URL for security issues. This logic is shown in the code snippet in Listing 4.6.

```
1  $(document).ready(function() {
2      var full_url = window.location.href;
3
4      if(full_url.indexOf("#") > -1) {
5          var fragment_url = full_url.split("#");
6
7          history.pushState("", document.title, window.location.pathname + window.
               location.search);
8
9          var fragment_params = fragment_url[1].split("&");
10
11         var access_token = fragment_params[0].split("=");
12     }
13 })
```

Listing 4.6: JS algorithm snippet to manipulate AMA token in the URL

With this manipulated data, the system calls the following endpoints to validate it and register the user as a BO:

1. **POST /api/extern/onboarding/form/:onboarding_token/validate_ama_token** – This endpoint validates the access token given by AMA and gets personal attributes. This is explained in more detail in Section 4.3.1.

2. **POST /api/extern/onboarding/form/:onboarding_token/beneficial_owner** – This endpoint performs an individual screening and registers the user as a BO according to the screening results, as shown by Figure B.11 of Appendix B. Besides this, if the BO was

found to be a PEP or belong to a Sanctions List, an email is sent to alert the Compliance department of that fact. This is explained in more detail in Section 4.3.2. If this method runs without errors, the last action it does is to update the onboarding token status for the third phase.

4.5.3 Third Phase - Get Mandatory Documents

In order to complete the onboarding process, some legal documents are mandatory, namely the proof of address and the proof of IBAN, for internal business issues, as displayed by Figure of B.12 Appendix B. If none of those files is uploaded or one of them is missing, the system will throw an appropriate error message, as shown by Figures B.13 and B.14 of Appendix B.

1. **POST /api/extern/onboarding/form/:onboarding_token/docs_submission** – This endpoint processes the submitted files, validates them by type and size, creates a destination folder, and uploads them (see Figure of B.15 Appendix B). If this method runs without errors, the last action it does is to update the onboarding token status for the last phase.

4.5.4 Fourth Phase - Onboarding Complete and Validation

This is the last phase of the onboarding process, and when the user reaches it does not need to do anymore action. Each Eupago account needs to have at least a user profile associated to it, so when entering this phase the system automatically calls the following endpoint to achieve this:

1. **POST /api/extern/onboarding/form/:onboarding_token/new_user** – This endpoint creates a new user, in terms of internal business logic, immediately after entering the last phase page. Besides this, an email is sent to alert the Commercial department that a new account has been created through the Automatic Onboarding. Figure B.16 of Appendix B displays this interface.

After creating the Eupago user, the onboarding process is complete, and the client has to wait for Eupago's commercial department validation and access credentials for the backoffice, as shown in Figure B.17 of Appendix B.

4.5.5 Extra Task - Autenticação.Gov Backoffice Login

An extra challenge of this project was to implement the possibility for the clients of Eupago to login into their backoffice using the AMA Autenticação.Gov methods, i.e., a user can authenticate in the backoffice using the CC or the CMD. Figure B.19 of Appendix B displays the newly added CMD login button to login page of Eupago's backoffice. Figure B.20 of Appendix B shows the user logged in after authenticating with the CMD.

This feature works the same way as in Section 4.5.2, but with proper routes to handle login operations:

1. **POST /api/auth/login_ama/authenticate** – This endpoint works almost the same as the endpoint of Section 4.3.1. The only difference is that this endpoint, since is not for an onboarding operation, the system does not need to have an onboarding token to access it, and instead of redirecting the user to the onboarding form, will redirect it to the login page of Eupago's backoffice.

2. **POST /api/auth/login_ama/validate** – This endpoint works similarly to Section 4.3.2. The only difference is that instead of creating a new BO, it applies internal logic for the user to login to the backoffice by comparing the obtained attributes data with the stored Eupago user data.

Chapter 5

Evaluation and Analysis

To further understand whether the developed solution met the objectives, it was necessary to find ways of validation. There are two types of target actors on this platform:

- The compliance directors or auditors who certify that all GDPR, KYC and AML directives are met;
- Eupago's potential customers who will use the platform.

5.1 Validation

The best method to validate the platform is to have it used in a real production environment.

For this the Commercial department of Eupago contacted the new customers and ask them if they could participate in an experiment regarding their registration. If they agreed, they would receive by email a link for the onboarding form and go through the process all by themselves. If they completed the process, this by itself would be already a very positive validation factor. If they had trouble, they would always enrole in the c̈lassicalẅay.

Besides this, a survey was elaborated [33] in order to understand how they interacted with the application and collect their opinions and experiences. They would receive this survey by email, and the complete list of questions is present in Appendix A. Metrics relevant for this study are presented next:

1. Age:
    a 18 - 24
    b 25 - 34
    c 35 - 44
    d 45 - 59
    e > 60
2. CMD Adhesion:

   a Yes

   b No

3. Perfomance, asked in the form of a Likert Scale [1]:

   a Very fast

   b Too slow

4. UI/UX, asked in the form of a Likert Scale:

   a Simple and Intuitive

   b Complex and Difficult

5. Convenience, asked in the form of a Likert Scale:

   a Very practical

   b Not practical

6. Feedback and Sugestions:

   a Open answer

5.2 Compliance Director/Auditor Perspective

On July 1st, 2022, the director of Eupago's Compliance department gathered with the author and simulated an onboarding process from beginning to end, giving his feedback on the following statement:

- *"I checked Eupago's new onboarding process. I consider that it encompasses all the areas necessary to contract the payment services that the company makes available to its customers. The process is simple and fast without neglecting the legally required security procedures.*
  On the other hand, it foresees future developments that technological evolution allows. The integration with the various partners (AMA, IRN, InformaD&B, among others) guarantees the veracity and timeliness of the information collected." – Paulo Ramalho

This validates the product on the compliance perspective.

[1] 1A typical item in a Likert scale is a statement to which respondents rate their level of agreement. The statement may be positive (e.g., "The terminology used in this interface is clear") or negative (e.g., "I found the navigation options confusing"). Usually a five-point scale of agreement like the following is used: 1. Strongly disagree 2. Disagree 3. Neither agree nor disagree 4. Agree 5. Strongly agree

5.3 Casual User Use-Case and Feedback

Between 01-06-2022 and 30-06-2022, the Commercial team made 18 contacts with potential customers of collective companies who wanted to join Eupago's payment services and were eligible to carry out tests of the Automatic Onboarding. The vast majority of companies' representatives contacted were between 35 and 59 years old.

One of the author's fears was that customers would not want the hassle of dealing with any process or bureaucracy, but this was not the case. The customers showed availability to participate in the onboarding experience and the supposed main obstacle seemed to be surpassed.

Unfortunately, not everything went as planned. One of the requirements to participate in the onboarding process is that customers need to have the CMD activated or have a card reader to authenticate themselves, as without this it is impossible to complete the process. Although these customers wanted to initiate their onboarding process, almost all did not have the CMD activated or a card reader. Some of them did not even know what was being discussed. This constitutes a significant constraint since they would not be able to test the platform and, consequently, answer the survey.

Other constraints made it impossible for users to test and give their feedback, which will be exposed below through the testimonies given by colleagues in the Commercial department, as they were the ones who made direct (phone) contact with customers:

- *"Of the six calls made, only one had a CMD and no one had a Card Reader.*
  The person who had CMD was not a manager of the company and had no power to bind the company. He was only responsible for the accession process.
  The company manager did not have an active CMD. Of all the people contacted, the vast majority did not know what the CMD was and also that it allowed signing contracts digitally." – Josefa Freixo

- *"I made some contacts with new potential customers who were eligible for testing. I was able to contact two potential customers who were interested in participating in the tests, however, one of them did not have an active CMD. Only one had an active CMD and even opened the link to start the automatic onboarding, however, due to low availability, the information inserted in the form was not corrected.*
  The information that did not allow the potential customer to proceed with the automatic onboarding was due to the fact of entering the IBAN with points. This field must not contain full stops, as this will not be read by the system correctly and will prevent the payment of funds to the merchant's account. The customer was also asked to re-enter the IBAN without points, however he was not willing to continue with the test." – Margarida Mota

- *"There was only one contact who was available to collaborate. He was very attentive and tried several times, but failed in every attempt.*
  Perhaps he did not understand how the access to the CMD was processed or because the card itself had two copies (one almost expired and the other with an updated date), and the

> *error that appeared was in phase 2, within the AMA form, and it was not conclusive what type of error was generated."* – Cátia Mendes

Although the author could not collect feedback from real users to validate the product, these constraints and obstacles taken from the interaction between the Commercial team and the customer can give us insights into how the general public receives these technologies.

AMA has statistical data on their website regarding their CMD [4], such as:

- evolution of the number of activations
- total activations per year, cumulative total and actives
- certificate activations
- activations per channel

Not knowing the degree of confidence observed by this study, analysing Figure 5.1 it seems that over the years, there has been a significant increase in CMD activations. Despite these statistics, almost all the customers the company made available for testing did not have the CMD active or did not even understand anything about it.

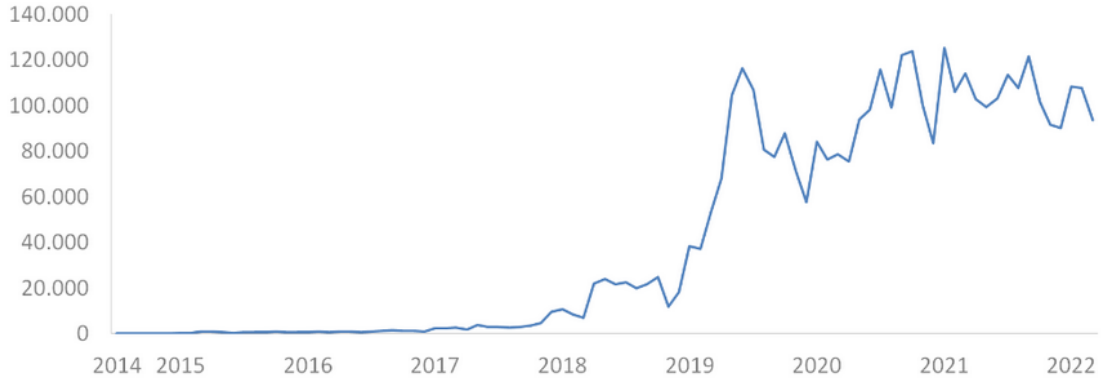

Figure 5.1: Evolution of the number of CMD accessions [4]

Chapter 6

Conclusions

This chapter is divided into various sections. Section 6.1 outlines the contribuitions made during this work. An overview on the achieved results is present in 6.2. Section 6.3 details the difficulties faced during development and realization of this work. Finally, Section 6.4 will delineates future paths for this work, which can bring value to the product and research.

6.1 Contributions

The implementation of a web application to solve the problems identified in Chapter 3 was completed with success, resulting in a minimal production-ready solution, which, at the moment of writing, is starting to be used to register some new clients. All of this was built by using a microservice architecture which was comprised of the following services, that were harmoniously integrated:

- **Eupago API** – Set of endpoints established by Eupago for the use of its functionalities;
- **AMA API** – External webservice with a set of endpoints established by AMA for the use of its functionalities;
- **Informa D&B API** – External webservice with a set of endpoints established by Informa D&B for the use of its functionalities;
- **Web Application (Frontend)** – Frontend for users to interact with the application, allowing them to do their onboarding process by themselves;
- **MySQL DB** – The database to store customer account and onboarding information.

6.2 Results

The goal of this project was to develop software that would automate the customer registration process in the company Eupago.

Traditional registration was a slower process that involved many constant interactions between the company's commercial team and the customer, from phone calls to paperwork and data exchange. This workflow, in some cases, consumed much time and human resources.

Although the author could not get the feedback he wanted, the application was tested and reviewed in a production environment and, at a technical level, meets all the requirements. The system can collect company and manager data in an authorized manner, complying with all usual standard directives, allows the user to submit all mandatory legal documentation, alerts the respective departments when certain conditions are met, and does it all in a simple and fast way.

In terms of usability, although there was a concern for the system to have a simple and intuitive interface and efficient performance, the necessary conditions to prove that the system is feasible and practical for the day-to-day user could not be met.

6.3 Difficulties

During the development of this project, some difficulties appeared and were tackled as best as possible. Some were solved, and others are left as future work in Section 6.4.

The author's first significant difficulty occurred during the preliminary work on this project, which was when testing the AMA API in a quality environment. The CMD we use on a daily basis does not work in the AMA staging environment, so we needed to configure and activate a CMD for this environment. The problem was that the AMA web platform where this was configured was not working correctly, always giving errors regardless of how the author authenticated in their system (by Portal das Finanças, CC). It is expected that when an entity provides a service and its documentation explains how to set it up, it should works. This was not the case, and this forced a constant exchange of emails between the author and the AMA technical support, which proved that the service entity itself was unaware of this failure in its configuration system. This incident makes the author believe that this service (that they provide to companies) is not used much or does not have much support. After our bug reporting and active interaction, AMA has fixed the problem and we were able to proceed with the tests and project development. Of course, other companies are now able to benefit from the correct operation of AMA's services.

Another problem arouse when AMA or Informa DB services were down during the integration period. This congested the project's development in terms of time and was a factor beyond the author's control.

Regarding the project itself, the only functionality that had been planned and was not developed was the automatic validation of documents submitted by the client, which would verify, for example, if the document had not expired. This was because the submitted documents did not all have a standard and uniform structure. There is no proof document, for example of IBAN or address, that is the same for all users, as each user can obtain this document from different entities and each has its own structure. The submitted documents also do not have a specific format defined, so the system has to allow the submission of various formats (pdf, jpeg, png, ...). The author at the beginning of this project had a solution, which would be to apply the PHP's

`file_get_contents` function[1], which reads the entire file and converts it to a string, then search for keywords like "Expiration date", "Expires to" and, through that, try to take the expiry date out of the document and compare it to the current date. However, this was not a viable solution for the reasons described above. The `file_get_contents` function depending on the file format, returns different results. In some cases, like when the document is an image, it is impossible to get the keywords because the result returns strange characters, and in other cases, the function throws an error. It will be necessary to search for another solution, but it was impossible for this project due to time constraints.

The last difficulty or constraint for this project was the luck factor, in the sense that the clients, which the company have managed to convince to perform the validation tests of the platform, could have the CMD active or a reader for the CC. Although customers were willing to participate in the tests, it was impossible to proceed because most of them did not comply with this requirement. Those few who complied, abandoned the process halfway due to reasons that are presented in Section 5.3.

6.4 Future Work

Several ideas come to mind from the reflections made in the previous sections when we think about future work.

First, the company should decide how to share the onboarding link with its clients. The author already developed an API endpoint for that (mentioned at the beginning of Section 4.5), but this is only achievable by making a Postman request for now. A proper interface should be integrated into their existing internal backoffice, so that the Commercial team can start the onboarding process themselves, as it should be.

As was also mentioned in Section 6.3, a solution must be devised that automatically validates customer documents in phase three (check Section 4.5.3) of the onboarding form. This may involve contracting another external entity with a service that does this or developing a standalone solution from scratch. The company must think about what is more convenient.

Other improvements have already been discussed in the company, such as at the end of the onboarding, after the Commercial team validated all the information coming from the process, having an automatic way to send the customer the contract signed by those in charge of Eupago and allowing the customer to perform their digital signature.

[1] https://www.php.net/manual/en/function.file-get-contents.php

References

[1] AMA. (2021). Autenticação.Gov CMD - Manual de Integração [PDF manual]. Available: https://github.com/amagovpt/doc-AUTENTICACAO/blob/main/Autentica%C3%A7%C3%A3o.Gov_CMD%20-%20Manual%20de%20Integra%C3%A7%C3%A3o%20v1.5.7.pdf.

[2] AMA. (2021). Guia rápido de utilização do OAuth2 do FA [PDF manual]. Available: https://github.com/amagovpt/doc-AUTENTICACAO/blob/main/OAuth2/Guia%20r%C3%A1pido%20de%20utiliza%C3%A7%C3%A3o%20do%20OAuth2.pdf.

[3] AMA. "Autenticação - AMA". AMA.gov. https://www.ama.gov.pt/web/agencia-para-a-modernizacao-administrativa/autenticacao.gov.pt (accessed Dec. 13, 2021).

[4] Autenticacao.Gov. "Estatísticas de Chave Móvel Digital". Autenticacao.gov.pt https://www.autenticacao.gov.pt/estatisticas-de-chave-movel-digital (accessed Jun. 30, 2022).

[5] Autenticação.gov. "Aplicação Autenticação.gov". Autenticação.gov. https://www.autenticacao.gov.pt/web/guest/aplicacao/aplicacao-autenticacao-gov (accessed Sep. 21, 2021).

[6] Autenticação.gov. "Guia prático de utilização do cartão de cidadão". Autenticação.gov. https://www.autenticacao.gov.pt/web/guest/documentos (accessed Feb. 11, 2022).

[7] Autenticação.gov. "O que é a Chave Móvel Digital?". Autenticação.gov. https://www.autenticacao.gov.pt/web/guest/a-chave-movel-digital (accessed Sep. 21, 2021).

[8] Auth0. "What is OAuth 2.0?". Auth0.com https://auth0.com/intro-to-iam/what-is-oauth-2/ (accessed Jun. 29, 2022).

[9] Auth0. "Which OAuth 2.0 Flow Should I Use?". Auth0.com https://auth0.com/docs/get-started/authentication-and-authorization-flow/which-oauth-2-0-flow-should-i-use (accessed Jun. 29, 2022).

[10] Black Law's. "Beneficial Owner Definition Legal Meaning - Black Law's Dictionary". TheLawDictionary.org https://thelawdictionary.org/beneficial-owner/ (accessed Jun. 8, 2022).

[11] Digital Denmark. "The most digital country in Europe". DigitalDenmark.dk https://digitaldenmark.dk (accessed Jan. 29, 2022).

[12] Denmark.dk. "The key to Denmark's digital success". Denmark.dk. https://denmark.dk/innovation-and-design/denmarks-digital-success (accessed Jan. 29, 2022).

[13] DigiD. "DigiD - Apply for or activate a DigiD". DigiD.nl https://www.digid.nl/en/apply-or-activate-digid (accessed Feb. 4, 2022).

[14] DigiD. "DigiD - Login Methods". DigiD.nl https://www.digid.nl/en/login-methods (accessed Feb. 4, 2022).

[15] DigiD. "DigiD - What is DigiD?". DigiD.nl https://www.digid.nl/en/what-is-digid (accessed Feb. 4, 2022).

[16] e-Estonia. "Home page - e-Estonia". e-Estonia.com. https://e-estonia.com/ (accessed Jan. 28, 2022).

[17] Shawna R.) Enrico. Rickard-Martin Carisch (Loraine. Meister. *"Evolution of UN Sanctions: From a Tool of Warfare to a Tool of Peace, Security and Human Rights"*. 1st ed. Cham, Switzerland: Springer, 2017.

[18] Europeia, Comissão. "EUR-Lex Access to European Union law". June 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[19] M. Ferreira. "Portuguese Citizen Card and Digital Mobile Key: the trust required of the citizen". M.S. thesis, FEUP, UP, Porto, Portugal, 2021. [Online]. Available: https://repositorio-aberto.up.pt/handle/10216/135946.

[20] Agency for Digitisation Ministry of Finance. "National identity and signing". DIGST.dk https://en.digst.dk/digitisation/eid/ (accessed Jan. 29, 2022).

[21] Fourthline. "Fourthline - Compliance in excellent form". Fourthline.com https://www.fourthline.com/ (accessed Feb. 4, 2022).

[22] FreeCodeCamp. "The Model View Controller Pattern – MVC Architecture and Frameworks Explained". FreeCodeCamp.org https://www.freecodecamp.org/news/the-model-view-controller-pattern-mvc-architecture-and-frameworks-explained/ (accessed Jun. 22, 2022).

[23] HuffPost. "User Onboarding: Not Just for HR and Growth Hackers". Huffpost.com. https://www.huffpost.com/entry/user-onboarding-not-just-_b_5708299 (accessed Feb. 8, 2022).

[24] Investopedia. "Compliance Department", October 2020. Investopedia.com https://www.investopedia.com/terms/c/compliancedepartment.asp (accessed Feb. 15, 2022).

[25] Meelis Kitsing. "Success Without Strategy: E-Government Development in Estonia". *Policy & Internet*, 3(1):1–21, August 2012. doi: 10.2202/1944-2866.1095.

[26] Peeter Laud and Meelis Roos. "Formal analysis estonian mobile-ID protocol". In *Nordic Conference on Secure IT Systems*, pages 271–286. Springer, 2009. doi: 10.1007/978-3-642-04766-4$_1$9.

[27] Avraham Leff and James T Rayfield. "Web-application development using the model/view/-controller design pattern". In *Proceedings fifth ieee international enterprise distributed object computing conference*, pages 118–127. IEEE, 2001. doi: 10.1109/EDOC.2001.950428.

[28] LexisNexis. "What is a Politically Exposed Person (PEP)?". LexisNexis.com https://risk.lexisnexis.com/insights-resources/article/what-is-a-politically-exposed-person (accessed Jun. 8, 2022).

[29] Monica C Meinert. "Digital Onboarding Done Right". *American Bankers Association. ABA Banking Journal*, 111(5):30–32, September 2019. [Online]. Available: https://www.proquest.com/docview/2381627117?pq-origsite=gscholar&fromopenview=true.

[30] Merriam-Webster. "Compliance Definition Meaning - Merriam-Webster". Merriam-Webster.com https://www.merriam-webster.com/dictionary/compliance (accessed Feb. 15, 2022).

[31] Merriam-Webster. "Onboarding Definition Meaning - Merriam-Webster". Merriam-Webster.com. https://www.merriam-webster.com/dictionary/onboarding (accessed Feb. 8, 2022).

[32] Microsoft Docs. "The Repository Pattern". Docs.Microsoft.com https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649690(v=pandp.10)?redirectedfrom=MSDN (accessed Jun. 14, 2022).

[33] Miguel Pires. "Questionário Onboarding Automático". Available at https://forms.gle/c4A3zztp39StpHZ6A.

[34] MySQL. "What is MySQL?". MySQL.com https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html (accessed Jun. 18, 2022).

[35] Pulse News. "S. Korea to outline digital ID system to replace old ID cards by Q3". Pulse-News.co.kr https://pulsenews.co.kr/view.php?year=2020&no=603696 (accessed Jan. 29, 2022).

[36] OAuth 2.0. "OAuth 2.0 Implicit Grant Type". Oauth.net https://oauth.net/2/grant-types/implicit/ (accessed Jun. 16, 2022).

[37] Ministry of the Interior and Safety. "MOIS - Home page". MOIS.go.kr https://www.mois.go.kr/eng/a01/engMain.do (accessed Jan. 29, 2022).

[38] Okta Developer. "What is the OAuth 2.0 Implicit Grant Type?". Developer.Okta.com https://developer.okta.com/blog/2018/05/24/what-is-the-oauth2-implicit-grant-type (accessed Jun. 16, 2022).

[39] Arnis Parsovs. "Estonian Electronic Identity Card: Security Flaws in Key Management". In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1785–1802. USENIX Association, August 2020. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/parsovs.

[40] Postman. "Postman API Platform". Postman.com https://www.postman.com/company/about-postman/ (accessed Nov. 22, 2021).

[41] LSR Rosen and Leon Shklar. *"Web application architecture: Principles, protocol and practices"*. 2nd ed. John Wiley & Sons Ltd.: West Sussex, England, 2009.

[42] SCEE. "Sistema de certificação electrónica do estado - instalação de certificados". SCEE.gov. https://www.scee.gov.pt/rep/certificados/ (accessed Feb. 11, 2022).

[43] StudyCPH. "NemID Digital Denmark". StudyCPH.dk https://studycph.dk/nemid-digital-denmark/ (accessed Jan. 29, 2022).

[44] Thales. "Know Your Customer in banking". ThalesGroup.com https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/issuance/id-verification/know-your-customer (accessed Feb. 16, 2022).

[45] The United States Department of Justice. "Foreign Corrupt Practices Act", February 2017. Justice.gov https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act (accessed Feb. 15, 2022).

[46] United Nations. "UN E-Government Survey 2020". PublicAdministration.un.org. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020 (accessed Jan. 28, 2022).

[47] VMware. "OAuth 2.0 Grant Types". Docs.Vmware.com https://docs.vmware.com/en/Single-Sign-On-for-VMware-Tanzu-Application-Service/1.14/sso/GUID-grant-types.html (accessed Jun. 16, 2022).

[48] Azidah Abu Ziden and Ong Chin Joo. "Exploring Digital Onboarding for Organisations: A Concept Paper". *International Journal of Innovation, Creativity and Change*, 13(9):734–750, 2020. [Online]. Available: https://www.ijicc.net/images/vol_13/Iss_9/13957_Ziden_2020_E_R.pdf.

Appendix A

Onboarding Survey Screenshots

This appendix serves the purpose of registering exactly the online survey developed for this work.

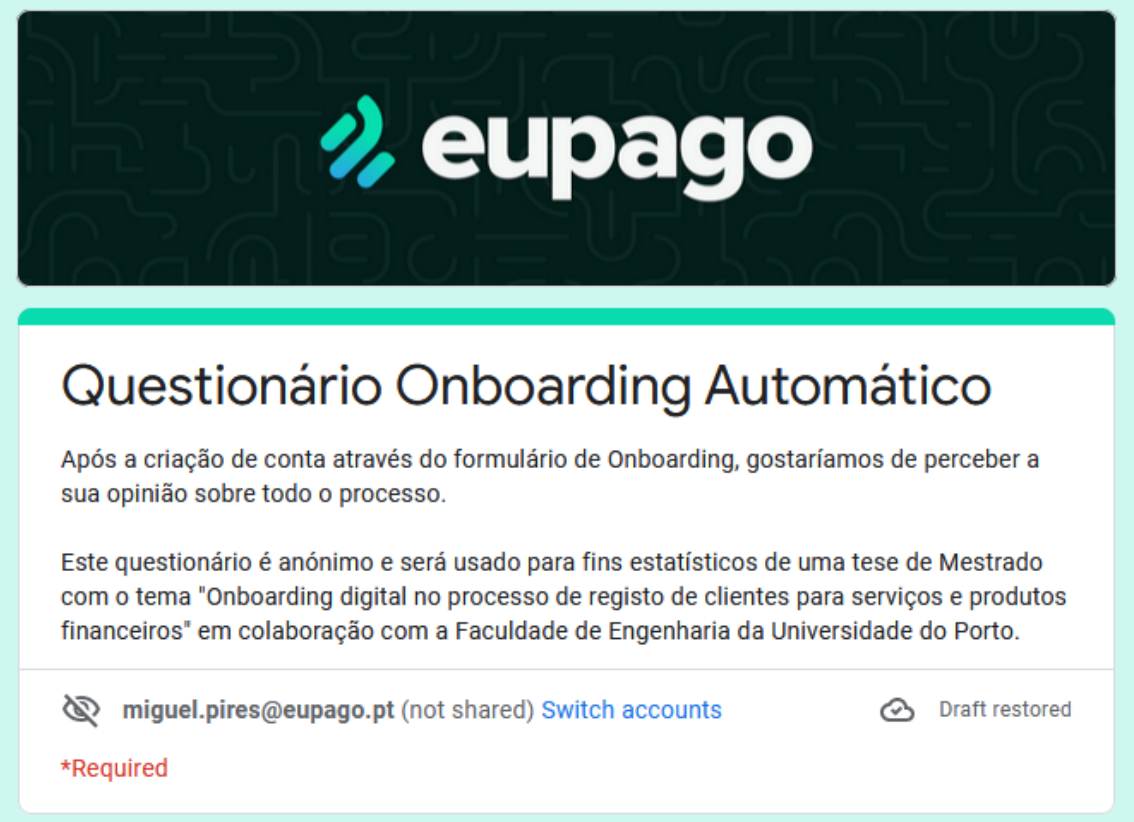

Figure A.1: Online survey introductory text screenshot

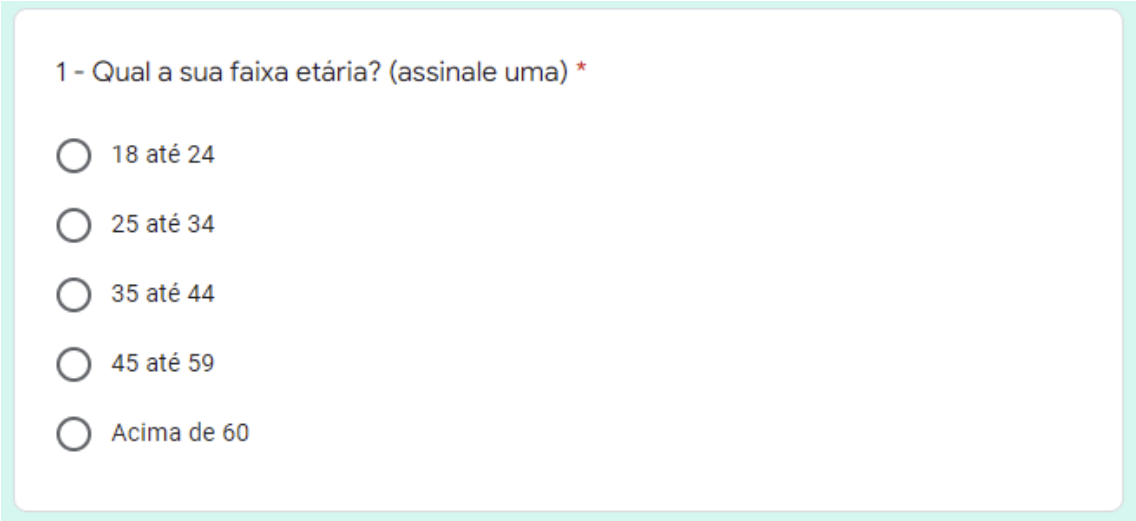

Figure A.2: Online survey age question screenshot

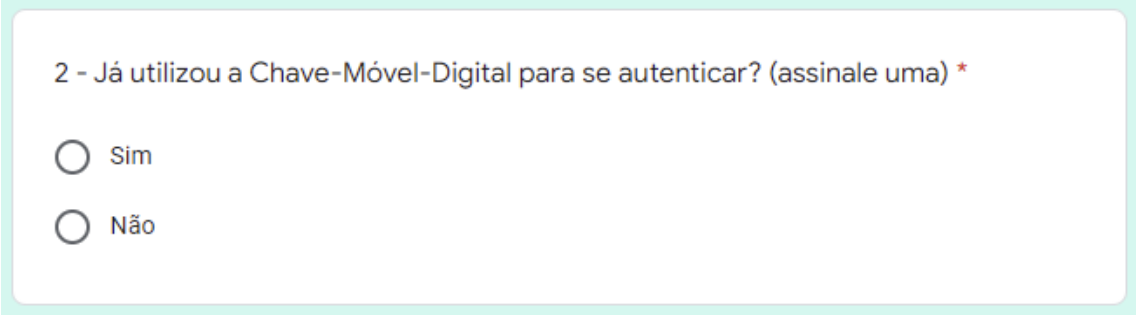

Figure A.3: Online survey DMK question screenshot

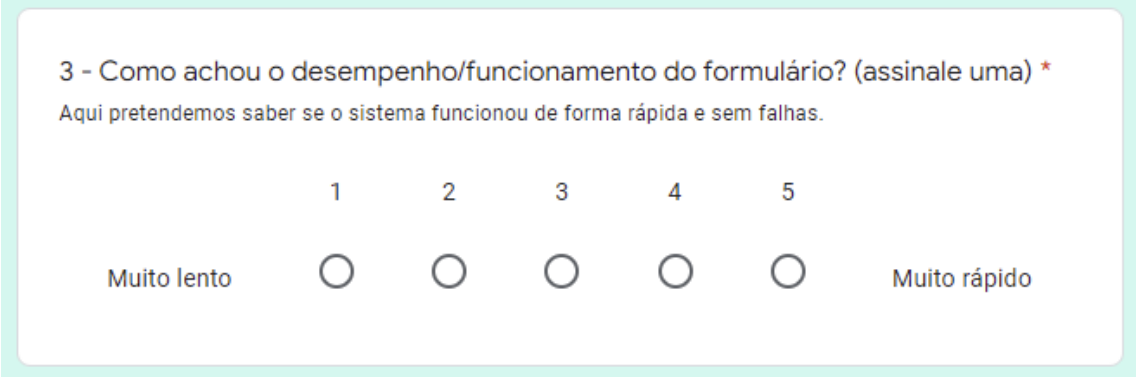

Figure A.4: Online survey perfomance question screenshot

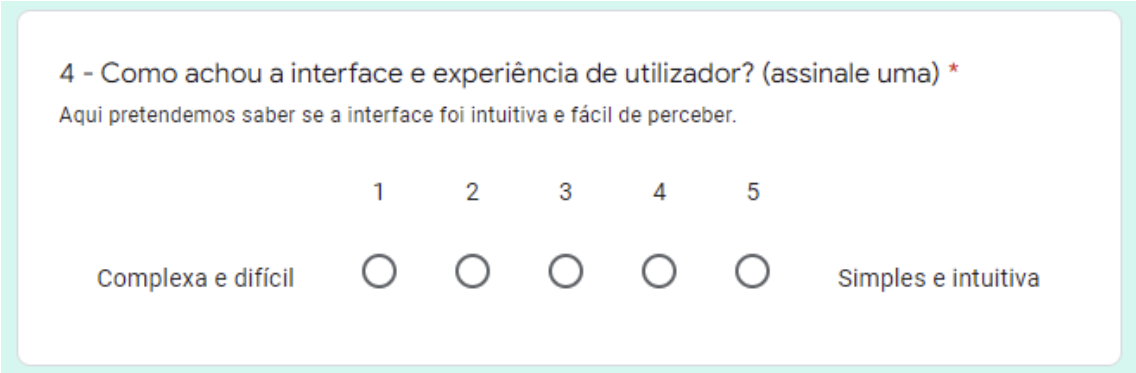

Figure A.5: Online survey interface question screenshot

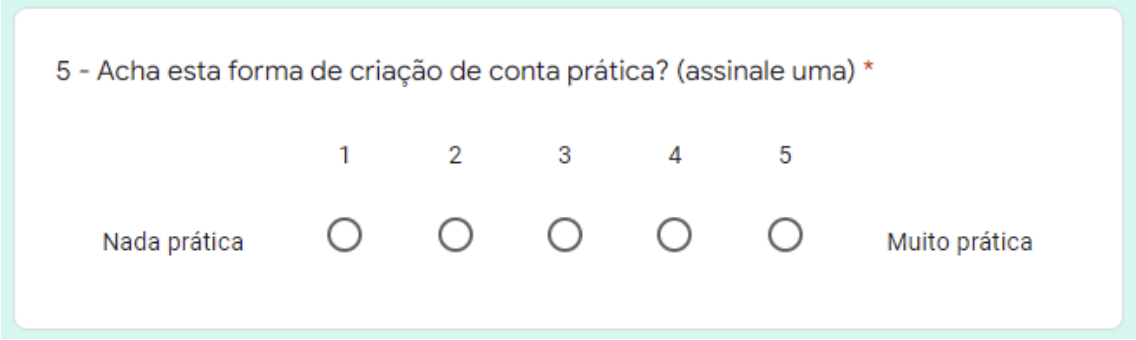

Figure A.6: Online survey viability question screenshot

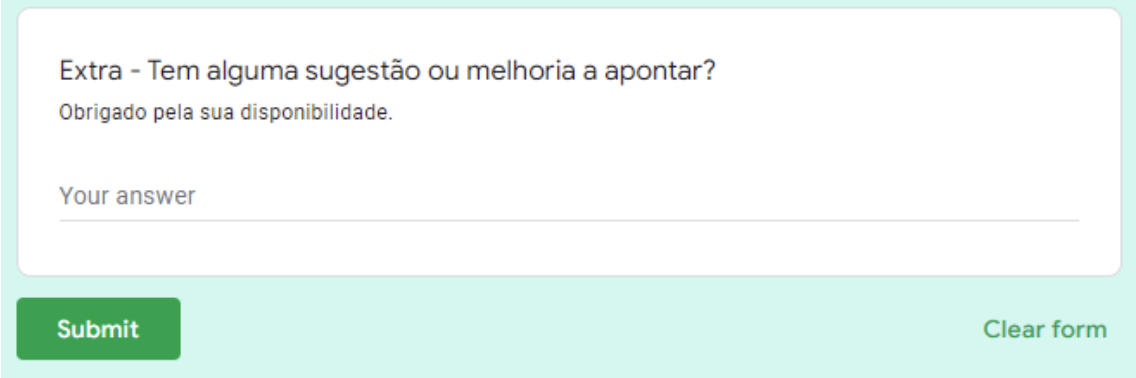

Figure A.7: Online survey extra feedback question screenshot

Appendix B

Eupago Live Frontend Interfaces

The author warns the reader that the prints taken from the automatic onboarding interface are in Portuguese, considering that the audience that will use this platform is Portuguese. It is primarily because CMD authentication only works with Portuguese citizens.

Figure B.1: First phase - Create account page

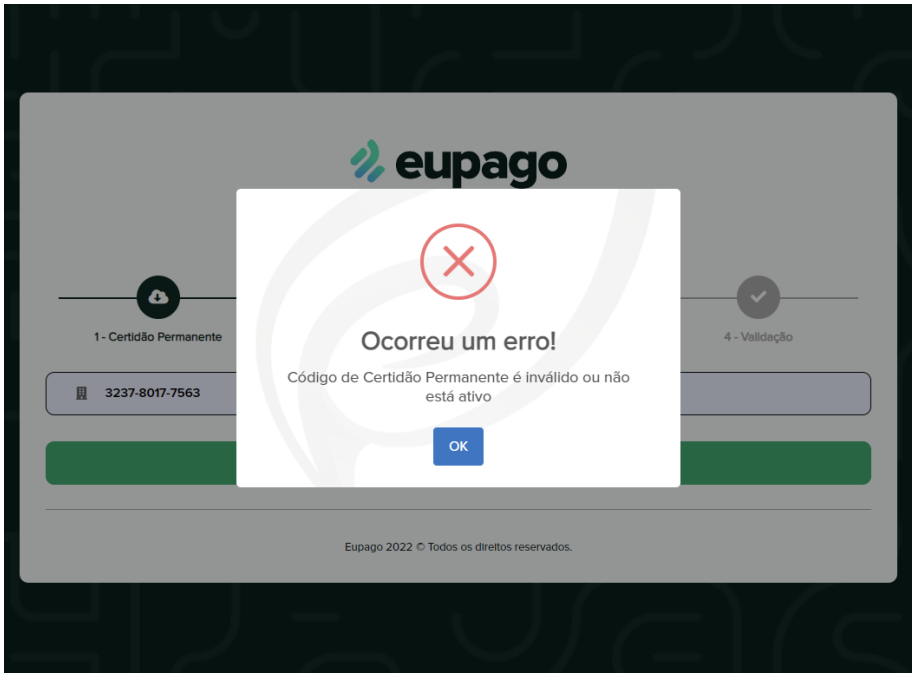

Figure B.2: First phase - Error message validating NIF or Permanent Certificate Code

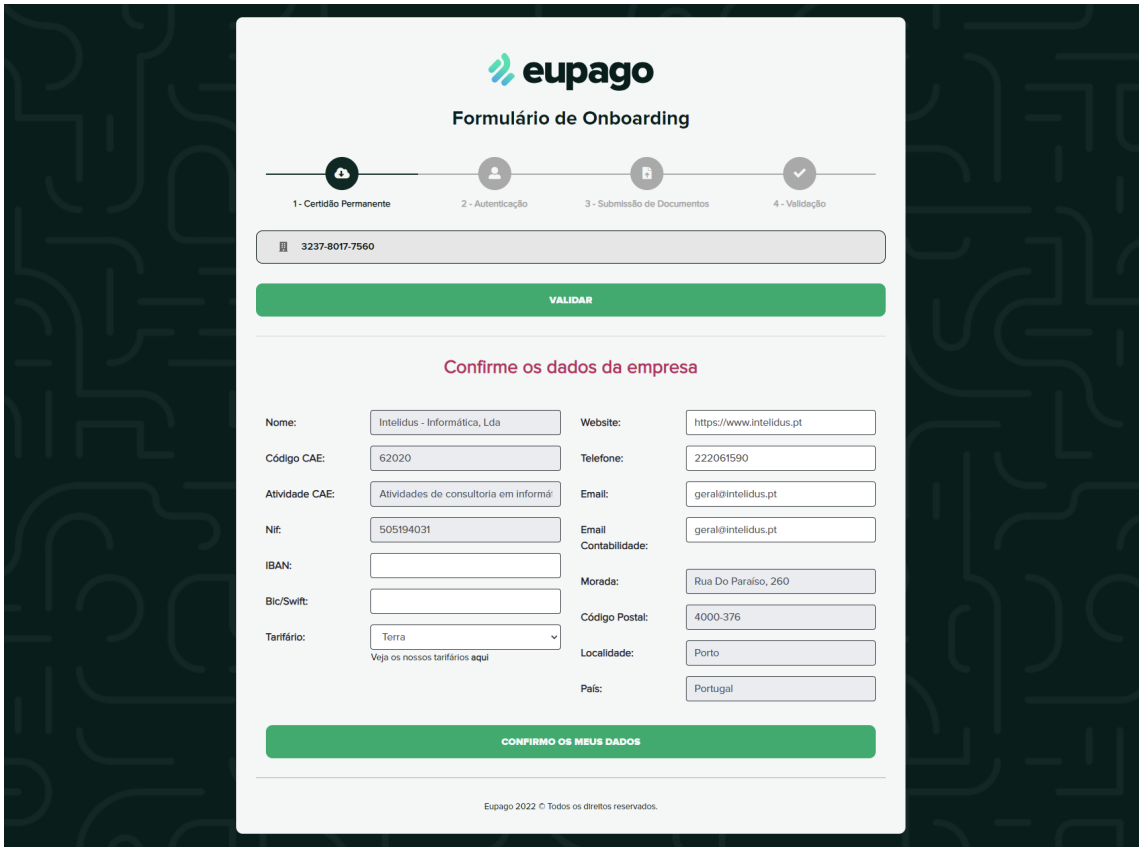

Figure B.3: First phase - Confirm company data form

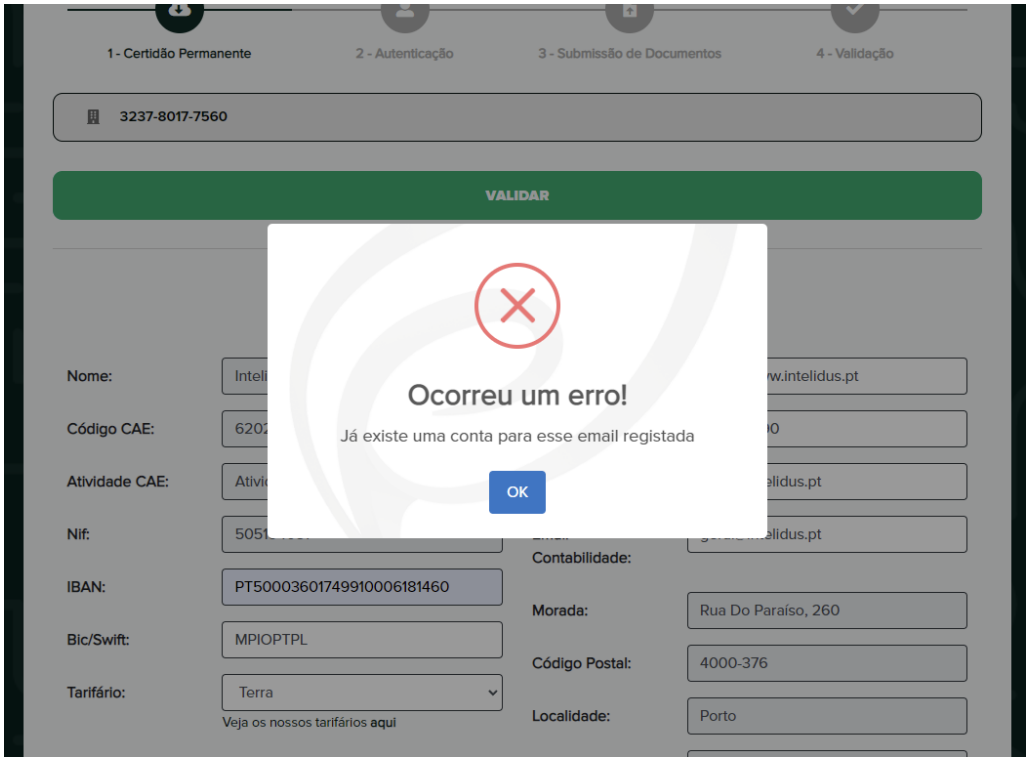

Figure B.4: First phase - Creating account for existing email error

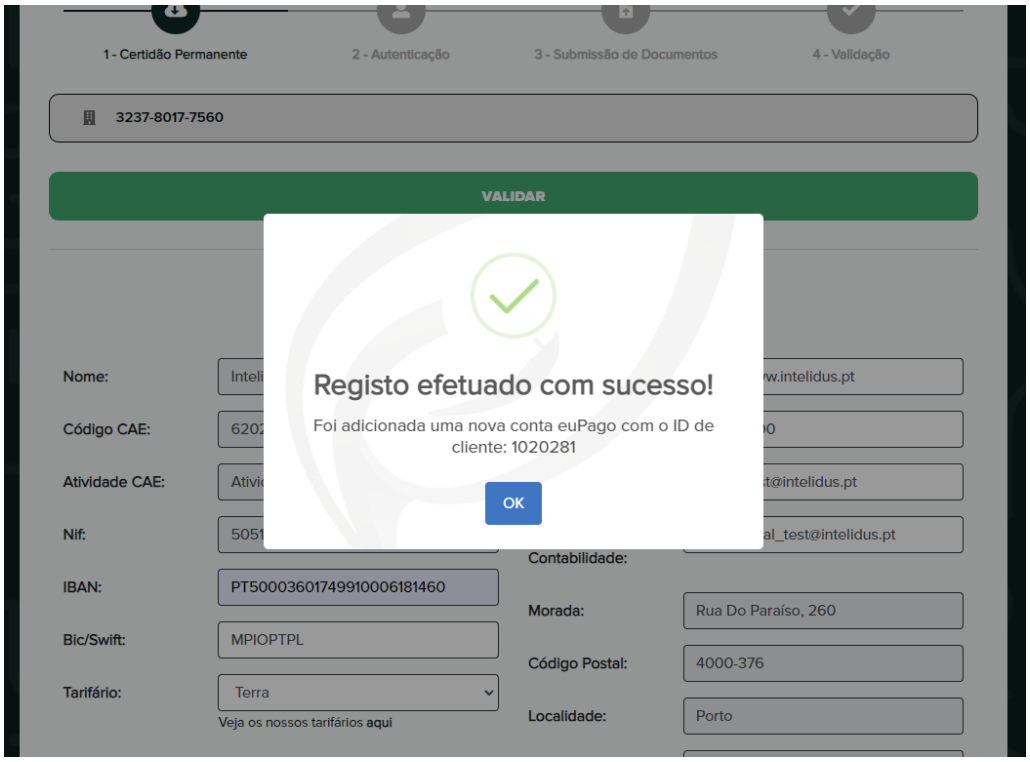

Figure B.5: First phase - Success creating account

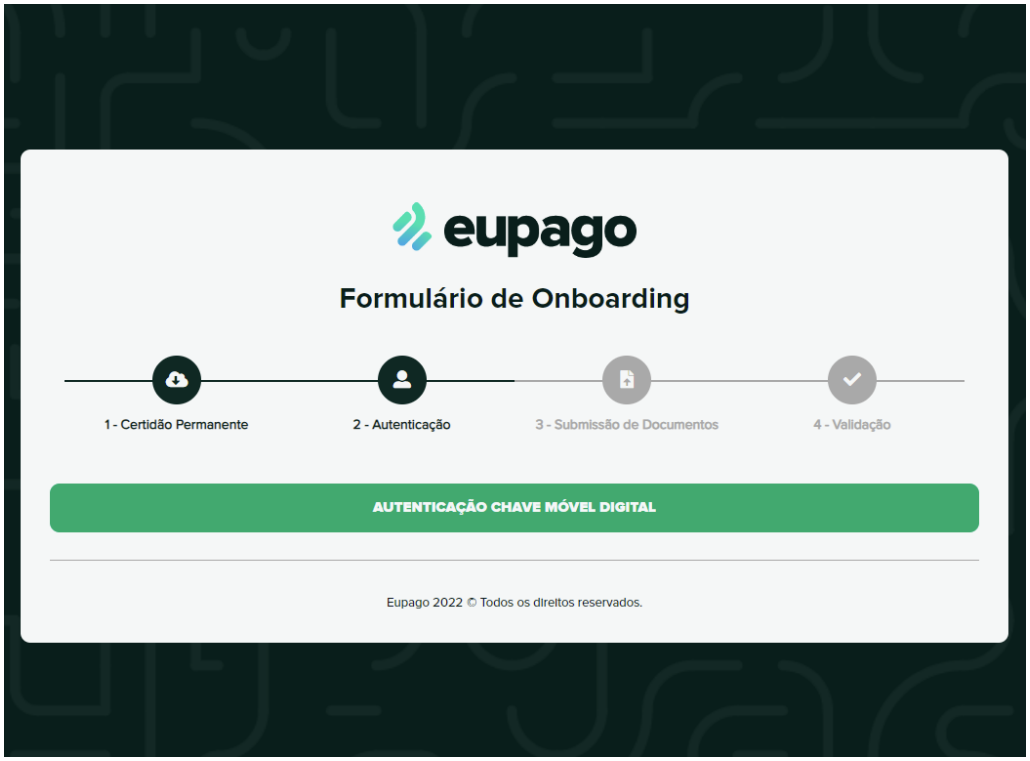

Figure B.6: Second phase - Register Beneficial Owner page

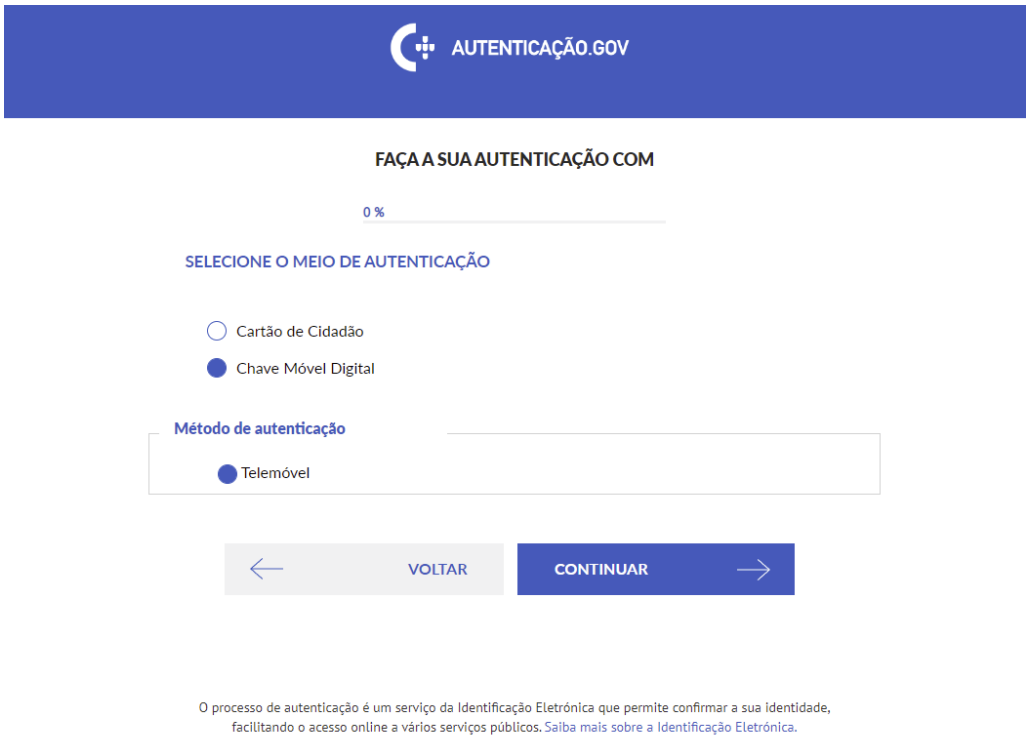

Figure B.7: Second phase - AMA page to choose authentication method

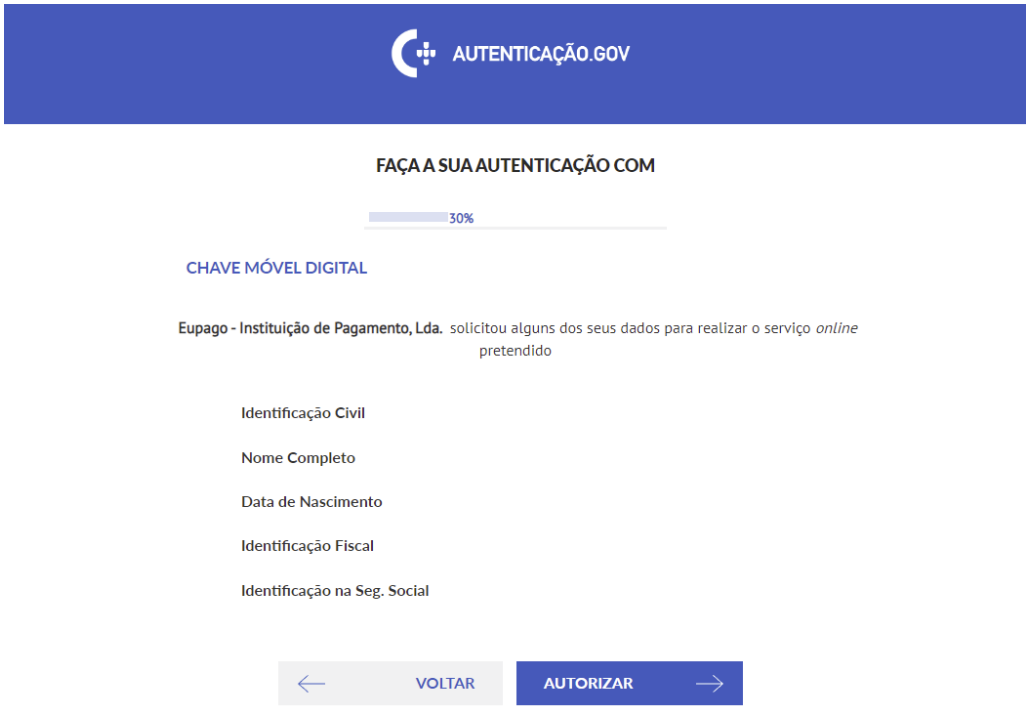

Figure B.8: Second phase - AMA page to authorize requested data

Figure B.9: Second phase - AMA page to insert DMK credentials

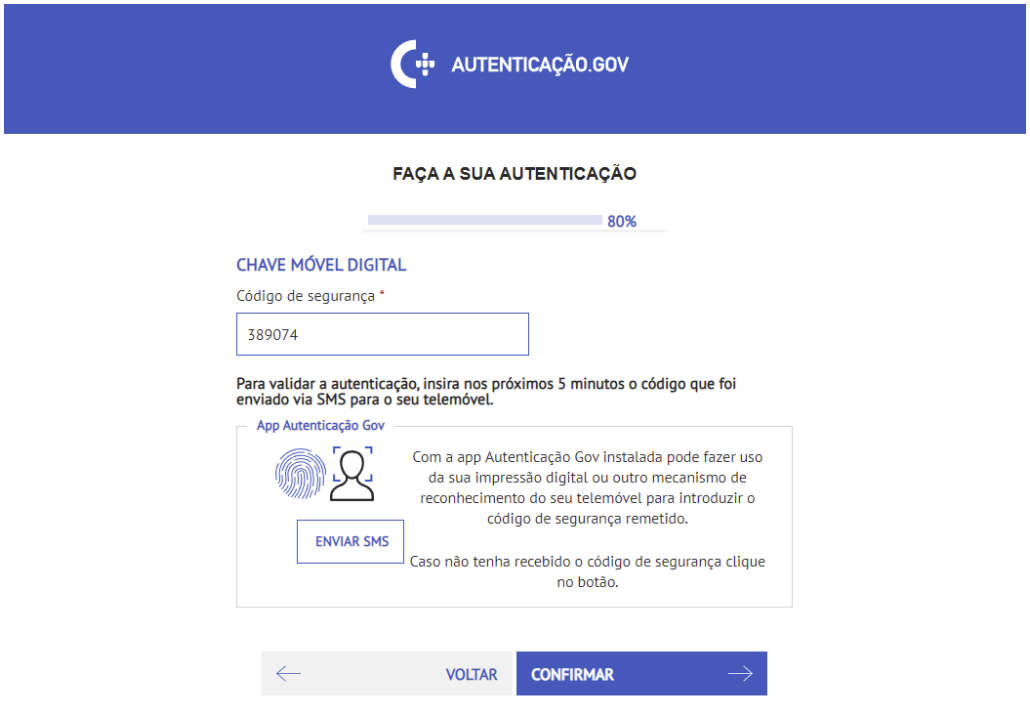

Figure B.10: Second phase - AMA page to insert SMS code key

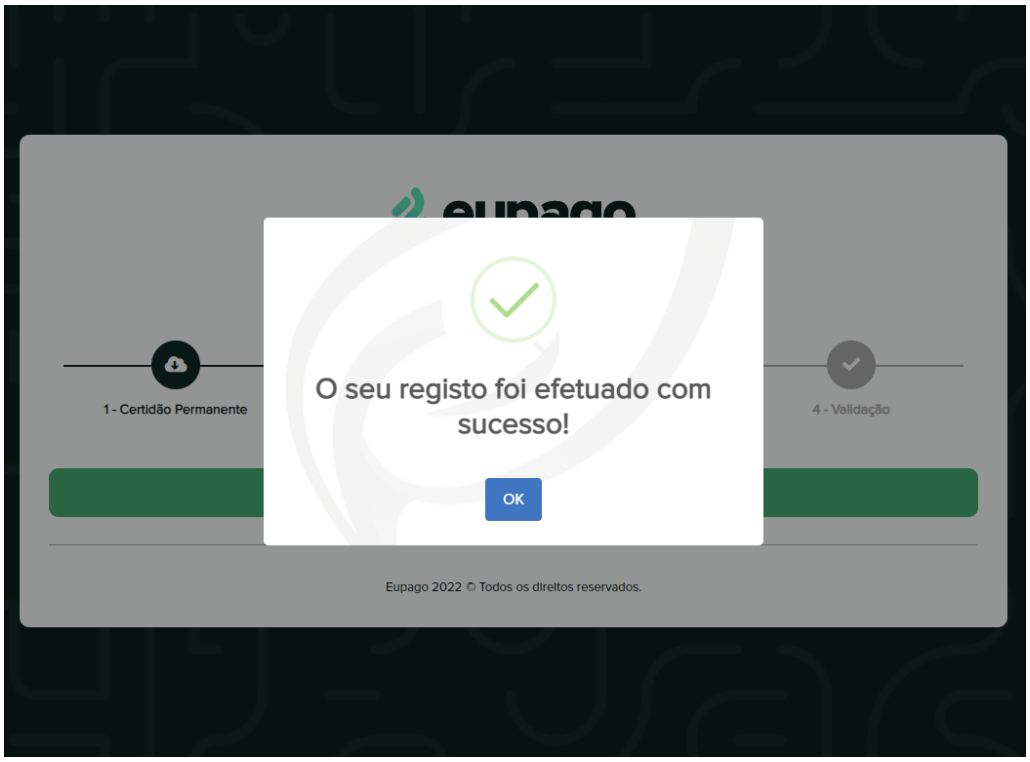

Figure B.11: Second phase - Success registering Beneficial Owner

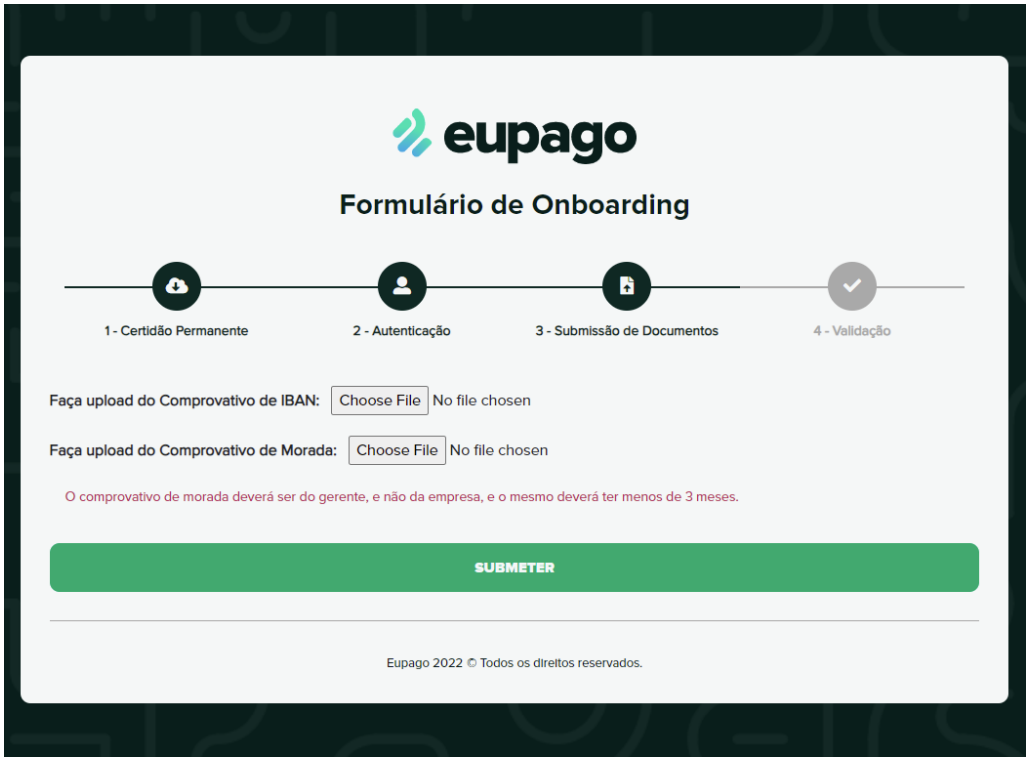

Figure B.12: Third phase - Required documents submission page

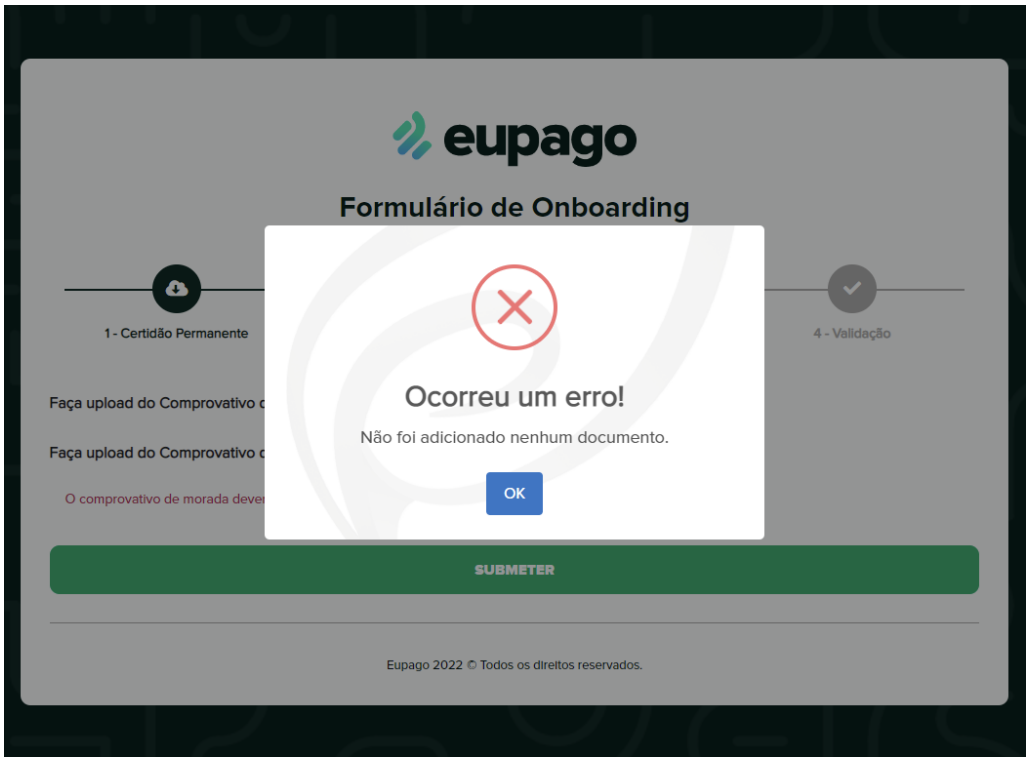

Figure B.13: Third phase - No files submitted error

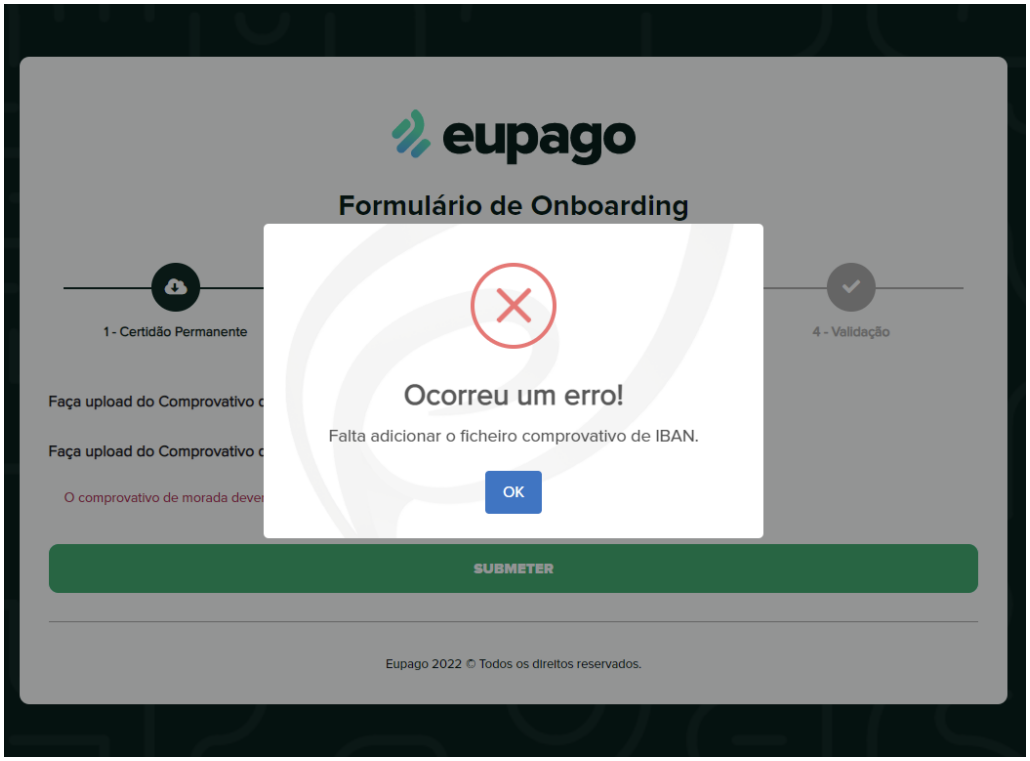

Figure B.14: Third phase - Missing a file error

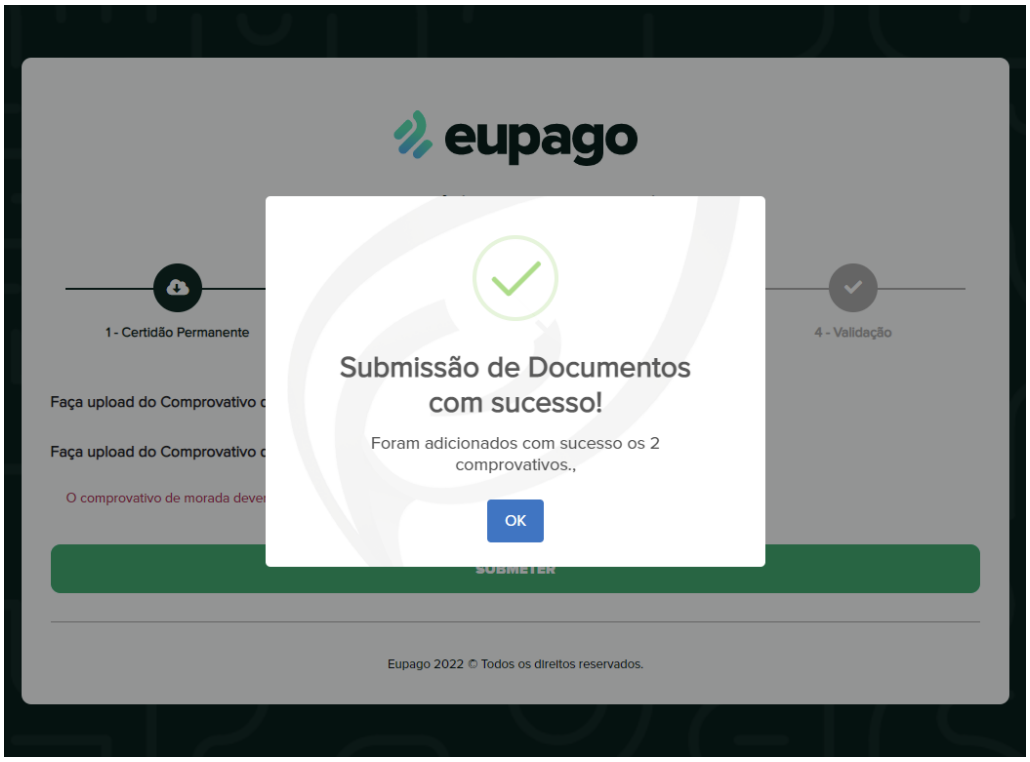

Figure B.15: Third phase - Success submitting all files

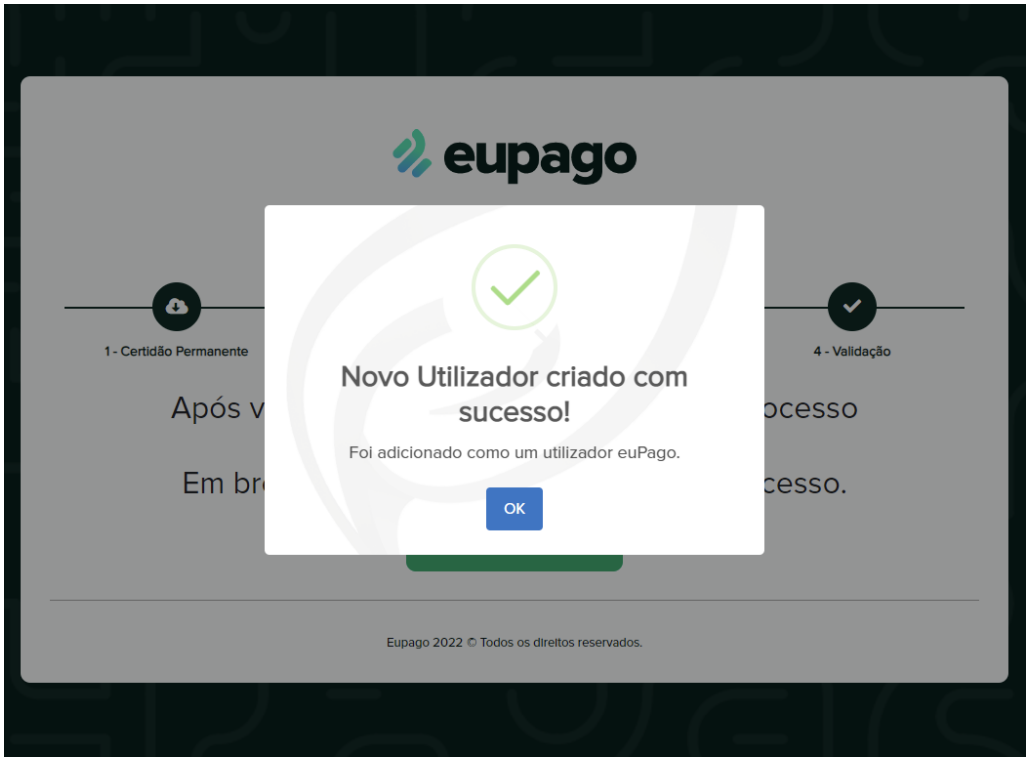

Figure B.16: Fourth phase - Success creating user

Figure B.17: Fourth phase - Onboarding successfully completed page

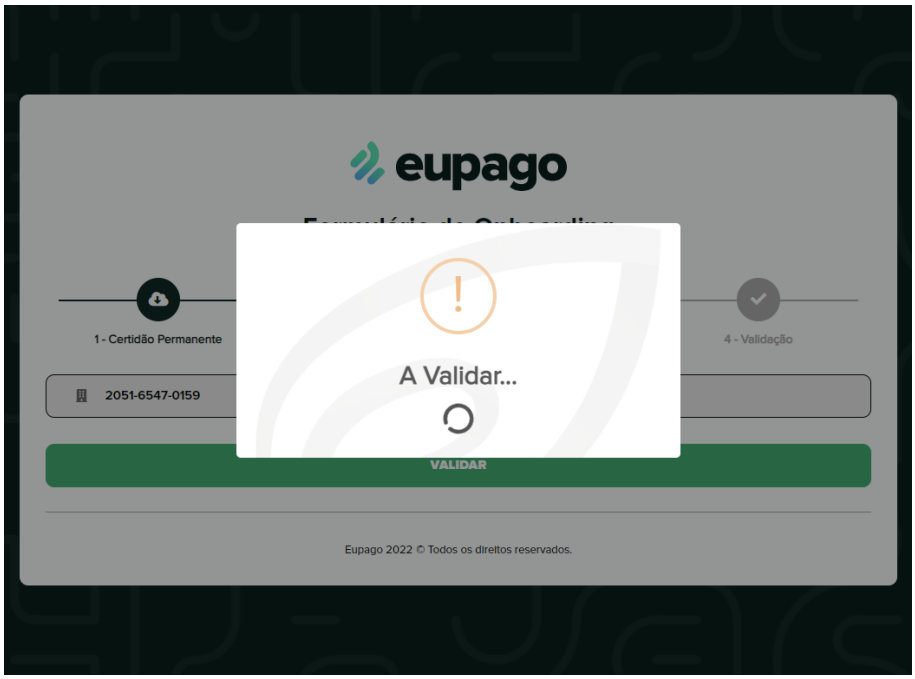

Figure B.18: Onboarding loading animation while validating or saving data

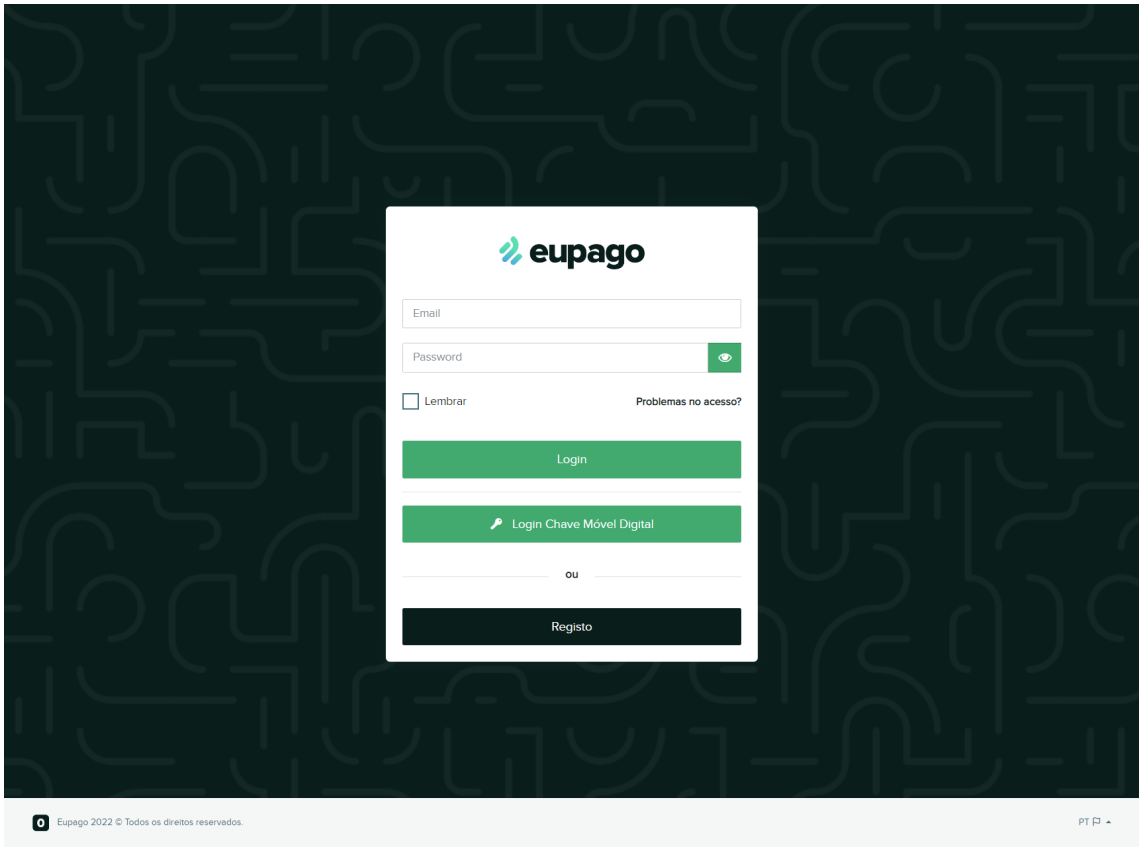

Figure B.19: DMK login option for client's backoffice

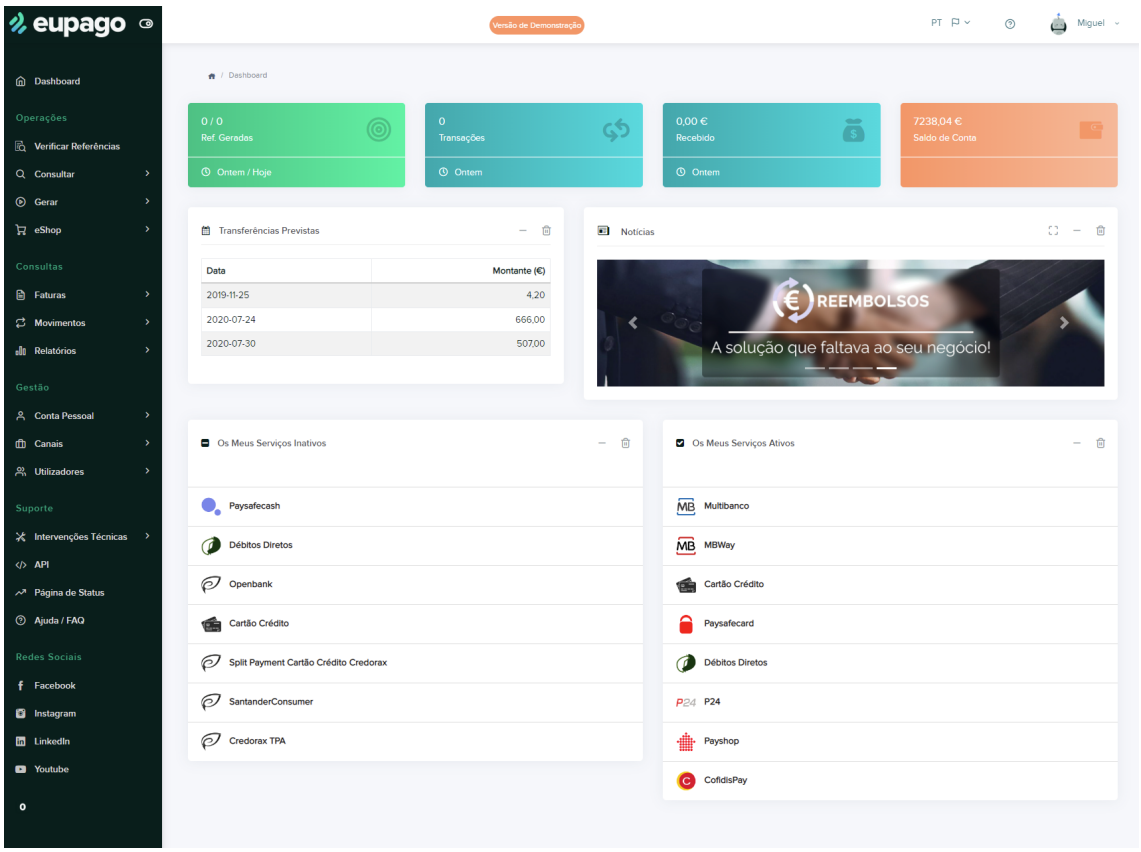

Figure B.20: Backoffice page after successful login using DMK

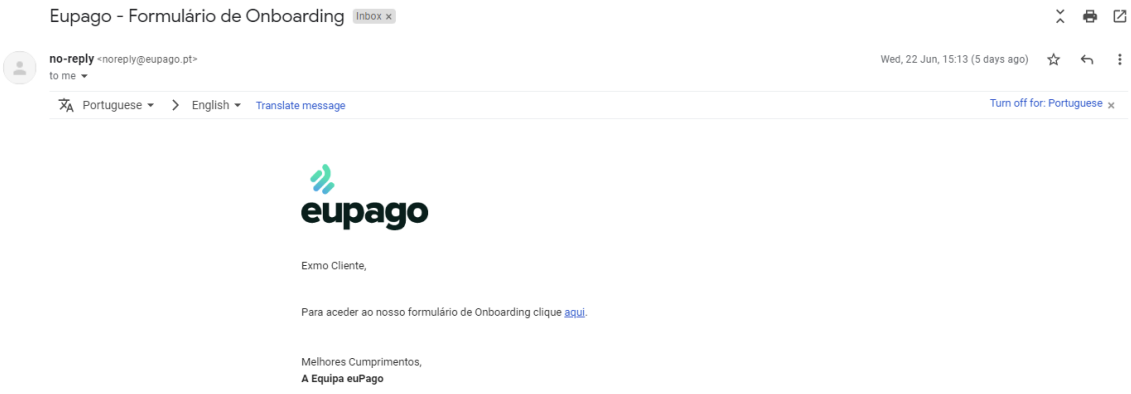

Figure B.21: Email sent to the user when the onboarding process is created

Appendix C

REST API Code Snippets

```
1   public function validateToken($settings, $token) {
2       // environmental variable stores the AMA API endpoint
3       // https://autenticacao.gov.pt/OAuthResourceServer/Api/AttributeManager
4       $url = $settings['endpointAPI'];
5
6       $headers = array(
7           "Content-Type: application/json",
8           "Cache-Control: no-cache",
9           "Accept: */*"
10      );
11
12      $body = array(
13          'token' => $token
14      );
15
16      $ch = curl_init();
17      curl_setopt_array($ch, array(
18          CURLOPT_URL => $url,
19          CURLOPT_RETURNTRANSFER => true,
20          CURLOPT_ENCODING => '',
21          CURLOPT_MAXREDIRS => 10,
22          CURLOPT_TIMEOUT => 0,
23          CURLOPT_FOLLOWLOCATION => true,
24          CURLOPT_HTTP_VERSION => CURL_HTTP_VERSION_1_1,
25          CURLOPT_CUSTOMREQUEST => 'POST',
26          CURLOPT_POSTFIELDS => json_encode($body),
27          CURLOPT_HTTPHEADER => $headers
28      ));
29
30      $result = curl_exec($ch);
31      $info = curl_getinfo($ch);
32
33      if(curl_errno($ch)) {
```

```
34              // echo 'Error: ' . curl_error($ch);
35          }
36          curl_close($ch);
37
38          $response = json_decode($result, true);
39
40          if($info['http_code'] === 200) {
41              header('Content-Type: ' . $info['content_type']);
42
43              return $response;
44          } else {
45              return false;
46          }
47      }
```

Listing C.1: POST request snippet to validate obtained access token

```
1       public function getUserAttributes($settings, $ama_attributes) {
2           $validated_token = $ama_attributes['token'];
3           $auth_context_id = $ama_attributes['authenticationContextId'];
4
5           // environmental variable stores the AMA API endpoint
6           // https://autenticacao.gov.pt/OAuthResourceServer/Api/AttributeManager
7           $url = $settings['endpointAPI'] . "?token=$validated_token&
                authenticationContextId=$auth_context_id";
8
9           $headers = array(
10              "Content-Type: application/json",
11              "Cache-Control: no-cache",
12              "Accept: */*"
13          );
14
15          $ch = curl_init();
16          curl_setopt_array($ch, array(
17              CURLOPT_URL => $url,
18              CURLOPT_RETURNTRANSFER => true,
19              CURLOPT_ENCODING => "",
20              CURLOPT_MAXREDIRS => 10,
21              CURLOPT_TIMEOUT => 0,
22              CURLOPT_FOLLOWLOCATION => true,
23              CURLOPT_HTTP_VERSION => CURL_HTTP_VERSION_1_1,
24              CURLOPT_CUSTOMREQUEST => "GET",
25              CURLOPT_HTTPHEADER => $headers
26          ));
27
28          $result = curl_exec($ch);
29          $info = curl_getinfo($ch);
30
```

```
31          if(curl_errno($ch)) {
32              // echo 'Error: ' . curl_error($ch);
33          }
34          curl_close($ch);
35
36          $response = json_decode($result, true);
37
38          if($info['http_code'] === 200) {
39              header('Content-Type: ' . $info['content_type']);
40
41              return $response;
42          } else {
43              return false;
44          }
45      }
```

Listing C.2: GET request snippet to obtain user attributes

```
1       public function generateToken($settings) {
2           // environmental variable stores the Informa D&B Auth endpoint
3           // https://plus.dnb.com/v2/token
4           $url = $settings['Auth'];
5
6           // environmental variables store the Informa D&B API Key and Secret
7           $headers = array(
8               "Content-Type: application/json",
9               "Cache-Control: no-cache",
10              "Authorization: Basic " . base64_encode($settings['apiKey'] . ":" .
                    $settings['apiSecret'])
11          );
12
13          $body = array(
14              "grant_type" => "client_credentials"
15          );
16
17          $ch = curl_init();
18          curl_setopt_array($ch, array(
19              CURLOPT_URL => $url,
20              CURLOPT_RETURNTRANSFER => true,
21              CURLOPT_ENCODING => '',
22              CURLOPT_MAXREDIRS => 10,
23              CURLOPT_TIMEOUT => 0,
24              CURLOPT_FOLLOWLOCATION => true,
25              CURLOPT_HTTP_VERSION => CURL_HTTP_VERSION_1_1,
26              CURLOPT_CUSTOMREQUEST => 'POST',
27              CURLOPT_POSTFIELDS => json_encode($body),
28              CURLOPT_HTTPHEADER => $headers
29          ));
```

```
30
31          $result = curl_exec($ch);
32          $info = curl_getinfo($ch);
33
34          if(curl_errno($ch)) {
35              // echo 'Error: ' . curl_error($ch);
36          }
37          curl_close($ch);
38
39          $response = json_decode($result, true);
40
41          if($info['http_code'] === 200) {
42              header('Content-Type: ' . $info['content_type']);
43
44              return $response["access_token"];
45          } else {
46              return false;
47          }
48      }
```

Listing C.3: POST request snippet to generate Informa D&B token

```
1       public function getInquiryByID($settings, $token, $inquiry_id) {
2           // environmental variable stores the Informa D&B Screening endpoint
3           // https://plus.dnb.com/v1/screening/inquiries
4           $url = $settings['Endpoint'] . $settings['Screening']['Inquiry'] . "/" .
                $inquiry_id;
5
6           $headers = array(
7               "Content-Type: application/json",
8               "Authorization: Bearer " . $token
9           );
10
11          $ch = curl_init();
12          curl_setopt_array($ch, array(
13              CURLOPT_URL => $url,
14              CURLOPT_RETURNTRANSFER => true,
15              CURLOPT_ENCODING => '',
16              CURLOPT_MAXREDIRS => 10,
17              CURLOPT_TIMEOUT => 0,
18              CURLOPT_FOLLOWLOCATION => true,
19              CURLOPT_HTTP_VERSION => CURL_HTTP_VERSION_1_1,
20              CURLOPT_CUSTOMREQUEST => 'GET',
21              CURLOPT_HTTPHEADER => $headers
22          ));
23
24          $result = curl_exec($ch);
25          $info = curl_getinfo($ch);
```

```
26
27          if(curl_errno($ch)) {
28              // echo 'Error: ' . curl_error($ch);
29          }
30          curl_close($ch);
31
32          $response = json_decode($result, true);
33
34          if($info['http_code'] === 200) {
35              header('Content-Type: ' . $info['content_type']);
36
37              return $response["inquiry"]["entities"];
38          } else {
39              return false;
40          }
41      }
```

Listing C.4: GET request snippet to retrieve results of inquiry