Impulse

Identity Management in PUbLic SErvices

D5.4 IMPULSE wallet - V2

Lead Authors:
Xavier Martínez (GRAD) and Javier Rodríguez (GRAD)
With contributions from:
Jaime Loureiro (GRAD)

Reviewers: [Gianluca Markos (ICERT), Iñaki Gangoiti (ERTZ), Alicia Jimenez (GRAD)]

Deliverable nature:	Demonstrator (D)
Dissemination level: (Confidentiality)	Public (PU)
Delivery date:	28-04-2022
Version:	2.0
Total number of pages:	32
Keywords:	wallet, app, accessibility, identity verifiable credential, onboarding, authentication, service

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004459

Executive summary

This document summarizes the IMPULSE user wallet specifications, gives a hint about the way of using the Android application that acts as an interface to the digital wallet, and describes all the features related to accessibility that are addressed in the development of this component.

The design of this wallet is based on the two main flows described in the architecture section: onboarding and authentication. The onboarding process is performed by the natural persons who want to obtain and store an identity verifiable credential in their devices. The users can initiate this process by selecting their public administration from a list, reading a QR code, or clicking a deep link. At this point, the user will be identified after taking a selfie and identity document photos and uploading all of these to the IMPULSE Enterprise service. The verification of the information uploaded will be done using two AI validation services, one that matches the face in the selfie with the one in the identity document and performs a face presentation attack detection, and the other that verifies that the identity document is real. The face matching service is synchronous, and the document validation service is asynchronous, taking around 1 to 2 minutes to conclude. When everything is correctly verified, onboarding will take place, and the user will end up receiving the identity verifiable credential. The authentication process is even simpler than the onboarding, where the users need to scan a QR or click a deep link to initiate it, and then, the person will select a previously obtained verifiable credential, take a selfie to unlock it, and the digital wallet will present it to the public administration. Once these steps are done, the verification of the credential will be completed, and the person will receive the service in the original app client where the QR or deep link were placed (e.g., a web browser).

Regarding the accessibility section, some features will be discussed like the no need of passwords, the facial recognition to unlock the credentials, the Android Accessibility Scanner, and the icons related to the consent of sharing personal information.

Document information

Grant agreement No.	**101004459**	**Acronym**	**IMPULSE**
Full title	**Identity Management in PUbLic SErvices**		
Call	DT-TRANSFORMATIONS-02-2020		
Project URL	https://www.impulse-h2020.eu/		
EU project officer	Giorgio CONSTANTINO		

Deliverable	**Number**	D5.4	**Title**	IMPULSE wallet - V2
Work package	**Number**	WP5	**Title**	Technology research, evaluation and integration
Task	**Number**	T5.5	**Title**	Continuous integration and deployment for pilots and demonstration"

Date of delivery	**Contractual**	M27	**Actual**	M27
Status	version 2.0		☒Final version	
Nature	☐Report ☒Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☒Public ☐Confidential			

Authors (partners)	GRAD			
Responsible author	**Name**	Xavier Martínez and Javier Rodríguez		
	Partner	GRAD	**E-mail**	xmartinez@gradiant.org

Summary (for dissemination)	Second version of the app to be used by citizens, together with guideline report on how to use it and specifications for accessibility
Keywords	wallet, app, accessibility, identity verifiable credential, onboarding, authentication, service

Version Log

Issue Date	Rev. No.	Author	Change
2022 - January	v0.1.0	Dolores Núñez Taboada (GRAD), Alejandro Cuenca Parra (GRAD)	First draft version of the document.
2022 - February	v0.1.5	Dolores Núñez Taboada (GRAD), Xavier Martínez (GRAD	First review and update of the first draft of the document.
2022 - March	v0.2.0	Dolores Núñez Taboada (GRAD), Xavier Martínez (GRAD	Second review and update of the document.
2022 - April	V1.0	Dolores Núñez Taboada (GRAD), Xavier Martínez (GRAD), Jaime Loureiro (GRAD)	Third review and update of the document.
2023 - March	V1.1	Xavier Martínez (GRAD)	First draft of the wallet specification v2
2023 - April	V1.2	Javier Rodríguez (GRAD)	Sections updated with everything related to the new IMPULSE app design
2023 - April	V1.3	Xavier Martínez (GRAD)	First review of the wallet specification v2.
2023 - April	V1.4	Gianluca Marcos (ICERT), Iñaki Gangoiti(ERTZ), Alicia Jimenez(GRAD)	Deliverable review check
2023 - April	**V2.0**	**Xavier Martínez (GRAD)**	Final adjustments

Table of contents

Executive summary 2
Document information....3
Table of contents 4
List of figures 5
Abbreviations and acronyms 6
1 Introduction 7
2 IMPULSE User Wallet: architecture, features and requirements....8
2.1 User Wallet architecture 8
2.1.1 Wallet Structure....8
2.1.2 Onboarding process 9
2.1.3 Authentication process....11
2.2 User wallet features 13
2.3 User wallet requirements....14
3 Design....15
3.1 Application UX design 15
3.1.1 Main screens 15
3.1.2 Onboarding/register from a QR code....16
3.1.3 Onboarding/register from the + button on the credentials screen....16
3.1.4 Login from a QR code. 16
3.2 Application UI design....16
4 How to use IMPULSE wallet 19
5 Specifications for accessibility 27
6 Conclusions 31
References 32

List of figures

Figure 1. User Wallet Structure 8
Figure 2. High level message flow of the onboarding process from the mobile app perspective 10
Figure 3. High level message flow of the authentication process from the mobile app perspective 12
Figure 4. Wireframes of the IMPULSE User Wallet 15
Figure 5. Examples of windows in the IMPULSE User Wallet 17
Figure 6. Main windows in the IMPULSE User Wallet 19
Figure 7. Option to register using a QR code, selecting the administration implicitly, or manual selection of the administration by creating a new credential 20
Figure 8. Option to register using a QR code, selecting the administration implicitly, or manual selection of the administration by creating a new credential 20
Figure 9. Facial scanning screen 21
Figure 10. Document ID details verification screen 21
Figure 11. Details of document scanning screens (some of the possible interactions are marked with red arrows) 22
Figure 12. Screen for verifying Document ID information and final procedure status 23
Figure 13. Onboarding requests dashboard 23
Figure 14. Credentials screen with a pending onboarding request and an a correctly issued credential 24
Figure 15. Public administration web page 24
Figure 16. QR code shown in the public administration web page 25
Figure 17. Screen for selecting credentials in the login process 25
Figure 18. Result of a successful login in the mobile application 26
Figure 19. Result of a successful login on the public administration website 26
Figure 20. Icons designed by Cyberethics Lab 27
Figure 21. Privacy Policy Screen in the IMPULSE User Wallet 28
Figure 22. Help icon usage in a window of the IMPULSE User Wallet 29
Figure 23. Google Play Store Pre-Launch Accessibility Report of the previous IMPULSE application 29
Figure 24. Google Play Store Pre-Launch Accessibility Report of the new IMPULSE application 30

Abbreviations and acronyms

DID: Decentralized IDentifier
SSI: Self-Sovereign Identity
EBSI: European Blockchain Service Infrastructure
ESSIF: European Self-Sovereign Identity Framework
V.Auth: Verifiable Authorization
ID VC: Identity Verifiable Credential
GDPR: General Data Protection Regulation
APK: Android Application Package
app: application
eID: Electronic IDentification
ID card: Identity card
PA: Public Administration
QR: Quick Response

1 Introduction

This report aims to serve as a guideline for the second version of the app to be used by citizens, which is named *wallet* in this document.

The *wallet* is the tool which the end users will rely on to perform any operation in the IMPULSE eID management solution. It lets them go through a digital onboarding process to obtain an identity verifiable credential and use it to authenticate against a Public Administration, to receive a public online service.

As mentioned, using the app a user can:

- Initiate an **onboarding process**: when users want to start an onboarding, they have to choose between selecting their public administration from a list, reading a QR code, or clicking a deep link. At this point, the user will be identified after taking and uploading a selfie and photos of the id document. When the IMPULSE Enterprise Service verifies that all the information uploaded is valid, the user will receive the identity verifiable credential.
- Initiate an **authentication process**: when a user wants to start an authentication, they only need to scan a QR code or click a deep link to initiate it. Then, the user will select a previously obtained verifiable credential, take a selfie to unlock it, and then, the digital wallet will present it to authenticate the user. Once these steps are done, the verification of the credential will be completed, and the person will receive the service in the web browser where the QR or deep link where placed.

The Section 2 describes the architecture of the IMPULSE solution from the user wallet perspective and the features and requirements of IMPULSE user wallet for instance, supported languages or minimum Android version.

The Section 3 describes how to use the IMPULSE wallet, showing screenshots of the different screens of the app and explaining each required step to perform the onboarding or authentication process.

Finally, the Section 4 explains accessibility specifications, like no need for passwords, facial recognition to unlock the credentials, and the icons related to the consent of sharing personal information.

2 IMPULSE User Wallet: architecture, features and requirements

In this section, the specifications of the user wallet will be described. First, the architecture of IMPULSE solution from a users' wallet perspective will be explained. This implies that the two main flows of the solution will be discussed in this subsection (onboarding and authentication). Then, the general features of the application will be exposed, and finally, the requirements to installation and use will be presented.

2.1 User Wallet architecture

The IMPULSE user wallet is an Android application developed in Kotlin over the Android SDK API 31. This application contains a user interface to perform the registration and login operations, a wallet component that is able to enroll and authenticate a user in a Self-Sovereign Identity way, and a facial recognition module that protects the identity verifiable credentials stored in the device.

2.1.1 Wallet Structure

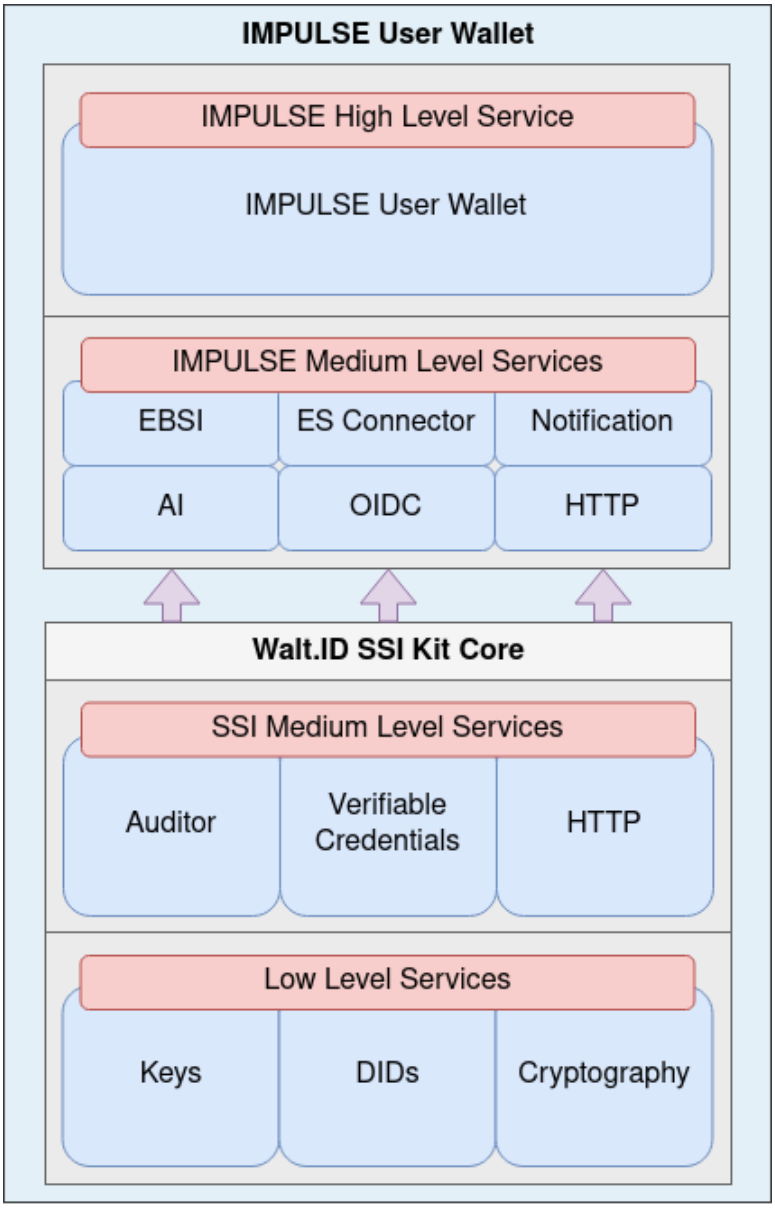

Figure 1. User Wallet Structure

As it can be seen in Figure 1, the IMPULSE user wallet has a structure that builds on top of the Walt.ID SSI Kit library [1]. This open-source solution developed by Walt.ID [2] has some low-level services to handle the private/public keys, the DID Documents and the cryptographic operations. Additionally, it also provides medium level services that internally make use of the low-level services to execute more complex functionalities needed to interact with decentralized identity models. These medium level services provide features to make high level verifications (e.g., verifiable credential presentations, trusted issuers, trusted schemes, etc.), to handle verifiable credentials (e.g., storage, presentation, etc.), and to interact with HTTP APIs (e.g., EBSI APIs).

The IMPULSE digital wallet exposes a high-level service used by the Android application to access all the features of an SSI holder, called IMPULSE User Wallet Service. All the features come from the Walt.ID SSI Kit Core services and some medium-level services developed in the context of the IMPULSE solution. The following gives a brief description of these mentioned IMPULSE medium-level services:

- **EBSI Service**: It handles all the interactions with the EBSI APIs, being these the ones related to the Authorization API, the DID Registry API, the TIR Registry API, and the Trusted Schemes Registry API. It makes use of the IMPULSE HTTP service internally to perform the requests.
- **ES Connector Service**: It handles the interactions with the IMPULSE Enterprise Service related to the digital onboarding process, and the notifications to know the completion of the digital onboarding process. It makes use of the IMPULSE HTTP service internally to perform the requests.
- **Notification**: It handles the Android notifications shown to the user locally in the device.
- **AI**: It exposes all the functionalities of the face recognition module developed by ALICE, being these the camera to take a short video selfie, the creation of the biometric profile, the face presentation attacks detection, and the matching of the selfie with the biometric profile.
- **OIDC**: It provides all the functionalities related to the verifiable credential issuance process based on the OIDC4VCI [3] informal standard, and the verifiable credential presentation process based on the OIDC4VP [4] informal standard. It makes use of the IMPULSE HTTP service internally to perform the requests.
- **HTTP**: It creates a configurable HTTP Client based on the well-known Ktor library [5]. This client is used by the EBSI Service, ES Connector Service and OIDC Service.

Note that the Walt.ID SSI Kit does not natively support Android environments, so we are using an Android ported version of the library developed by GRAD [6].

2.1.2 Onboarding process

In the onboarding process, an end-user asks (through the IMPULSE application) for a Verifiable Credential (VC), or more specifically for an Identity Verifiable Credential (ID VC), but in this document, both terms are used indistinctively. This credential is issued by the Public Administration to which the person belongs, and it will be stored in the device where the application is installed. Other steps are required to follow the ESSIF governance schema [6].

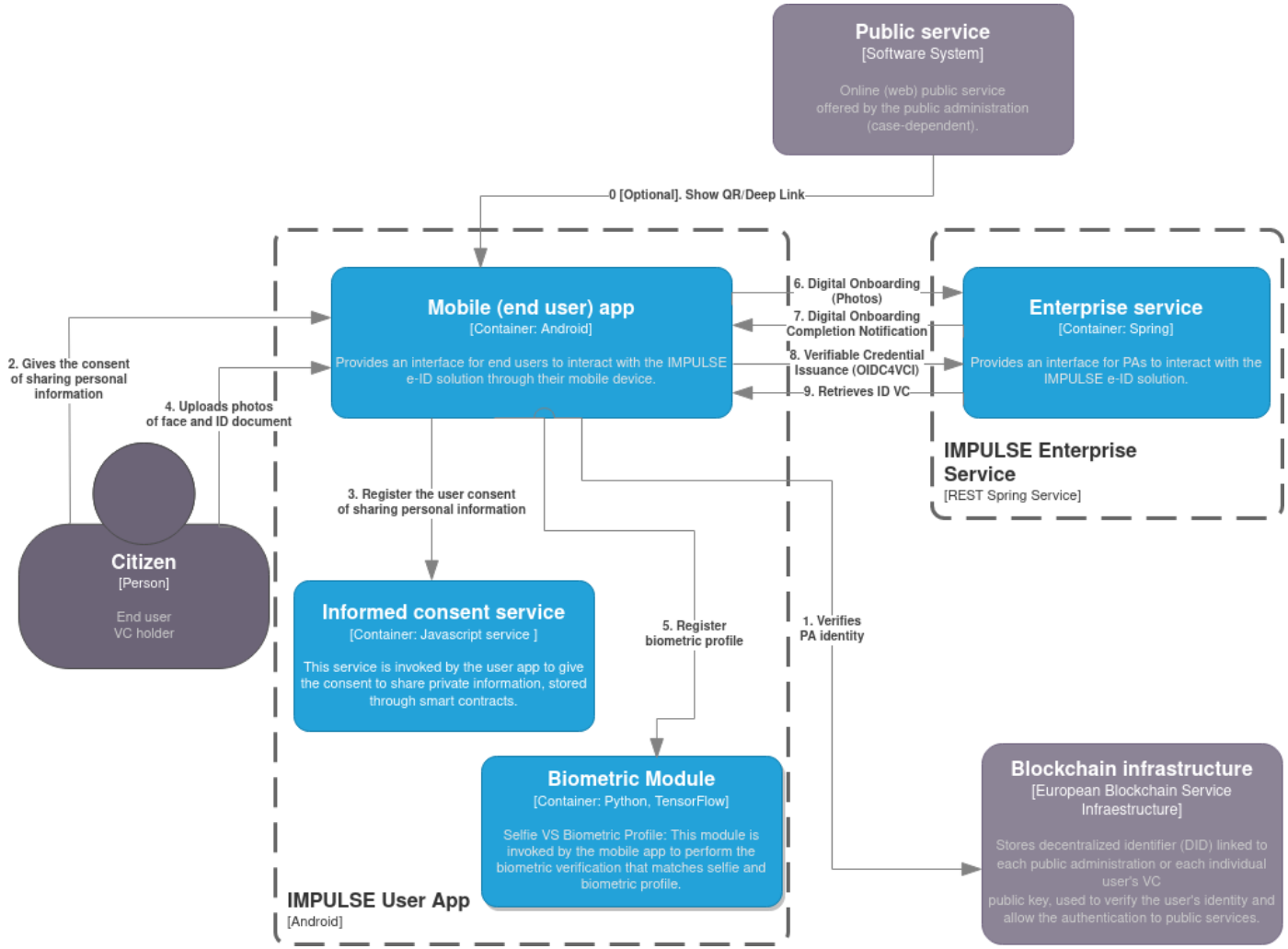

Figure 2. High level message flow of the onboarding process from the mobile app perspective

When a user (citizen) decides to use a particular online public service, they access to it through their web browser. If it is the first time, they will be asked to follow an onboarding process through their IMPULSE mobile app (Step 0). Here there are three possibilities for starting the onboarding: the user can read a QR in the web browser that starts the process, click a deep link in the web browser (within the Android device) that starts the process, or just select the public administration they belong to from a list in the application to start the process. Once the user wallet verifies the identity of the PA checking the EBSI Trusted Issuers Registry (Step 1), the citizen gives the consent to share personal information (Steps 2 and 3) accepting the privacy policy of the legal entity. Then, the IMPULSE app asks the user to upload photos of their face and ID document (Step 4), and prior to sending the photos to the enterprise service (PA), a biometric module integrated into the mobile app will register the biometric profile in the citizen's mobile device (Step 5) for further validations in the authentication process once the user has been already enrolled in IMPULSE.

At this point, all the information required from the person has been uploaded to the Enterprise Service to initiate the digital onboarding process (Step 6). After some verifications inside the Enterprise Service (AI validations and a manual check), the Enterprise Service will notify the IMPULSE app of the completion of the digital onboarding (Step 7). The user wallet can now perform the verifiable credential Issuance process (Step 8), and after some verifications by the Enterprise Service, the user wallet receives the identity verifiable credential (Step 9). At this moment the user is already enrolled in IMPULSE, and they may use their ID VC to get access to the online public service (authentication process).

2.1.3 Authentication process

In the authentication phase, an end user (citizen) who is willing to access an online public service, authenticates to the Public Administration by sharing its ID VC. After the authentication ends, the public administration service is provided into the web browser that started the process.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004459

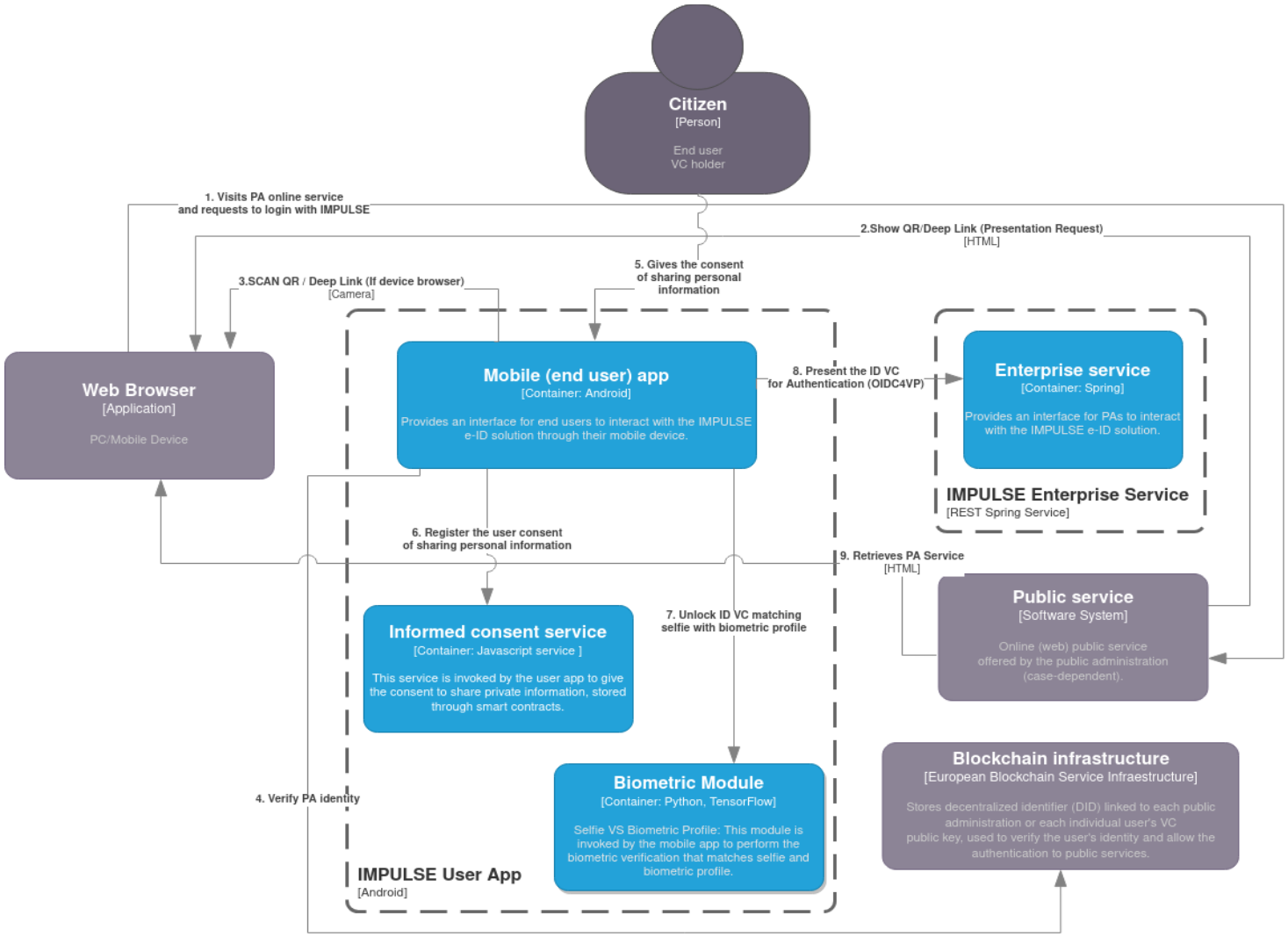

Figure 3. High level message flow of the authentication process from the mobile app perspective

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004459

Once the citizen has been duly enrolled in IMPULSE, they may authenticate themselves with the online public administration service (PAS) by using their ID VC through the IMPULSE mobile application. First, the user accesses the web public service through a web browser and requests to login with IMPULSE (Step 1). At this point, the public service shows a QR code to be scanned with the IMPULSE app or a deep link to be clicked (in case the web browser is in the same Android device) (Steps 2 and 3). Then, the user wallet verifies the identity of the public administration (PA) checking if it belongs to the EBSI Trusted Issuer Registry (Step 4). Next, the user is asked to accept the privacy policy of the legal entity and gives the consent to share personal information (Steps 5 and 6). If the consent given in the onboarding is still valid, these steps can be skipped. Then, the mobile app will prompt the user the available verifiable credentials, so they can select the one they want to present to the PA. To be able to use the select ID VC, the user will need to take a selfie that will be verified against the biometric profile stored during the onboarding process (Step 7), and the user wallet will present this verifiable credential to perform the authentication process (Step 8). If the Enterprise Service correctly verifies the ID VC presented, the user is authenticated, and they can consume the requested online public service in the web browser where the process started (Step 9). At this point the authentication process can be considered complete.

2.2 User wallet features

The app currently supports 7 languages: English, Spanish, Galician, Italian, Bulgarian, Danish and Icelandic. If no language has been configured in the application, the language displayed will be the one configured on the mobile device, and in the case that the device global language is not supported by the application, English will be the default option.

The IMPULSE wallet is able to perform two main operations: onboarding and authentication. The steps in these two processes are handled by the wallet component of this Android application, which is based on an Android ported version (developed by GRAD) of the WaltId SSIKit [2].

Currently, the IMPULSE application allows several ways of interacting with it to make it perform the onboarding and authentication processes. Regarding the onboarding, the citizen can select it's public administration from a pre-configured list, scan a QR Code in the public administration page, or even click a deep link in the device browser that redirects to the application. All of these scenarios will bring the user to the screen that requests the user to accept the privacy policy, and then to the screen that requests the images that have to be taken in order to correctly make the onboarding process. Similarly, a citizen can scan a QR Code from the public administration page, or click a deep link in the device browser, to be able to initiate the authentication process. These two scenarios bring the user to the screen that requests the user to accept the privacy policy, and then to the screen that requests the user to select one identity verifiable credential stored in the device to use in the authentication.

After the uploading of the photos by the user, the IMPULSE user app will show the citizen the content of the ID Document MRZ scanned, so the user can confirm that the information that will be used to create the ID VC is correct.

The ID VC stored in the device is protected with a local biometric profile created from the selfie of the user. This way of locking the verifiable credentials gives a second layer of security in case someone else is able to access the phone, and tries to use the IMPULSE application to login.

When the user gives the consent to share personal information accepting the privacy policy, the user wallet will interact with the informed consent service, and this one will store the consent in a public blockchain invoking a smart contract.

2.3 User wallet requirements

The minimal Android version supported is Android 8.0 (API 26) [7].

The IMPULSE app requires the following permissions:

- Full Network Access.
- Camera Access.

The network access permissions are used to connect with the Enterprise Service, EBSI and Informed Consent Service. The app also needs the front and back camera to take photos from user's face and from the required documents respectively.

The application has a size of approximately 170Mb in disk.

The application consumes around 260Mb RAM in execution.

3 Design

The description and explanation of the application design will be divided into two parts. Firstly, we will discuss the conceptual design of the user experience (UX), explaining for example why a particular screen is located where it is and how it is associated with others to create a satisfying user experience. Secondly, we will briefly discuss the design decisions that have been made at the visual level itself, including colours, typography, illustrations, etc.

3.1 Application UX design

As previously stated, the main functions of the application are the onboarding and authentication calls, for requesting an ID-VC and access a public service using an ID-VC respectively. The application has therefore been oriented towards these two types of use cases, although they do not directly correspond to tabs or sections of the application. Instead, we have these three tabs with well-defined roles: Authenticate, Credentials, and Settings.

3.1.1 Main screens

Below are sketches or wireframes of these three main screens, corresponding to the three sections of the bottom navigation bar available in the application.

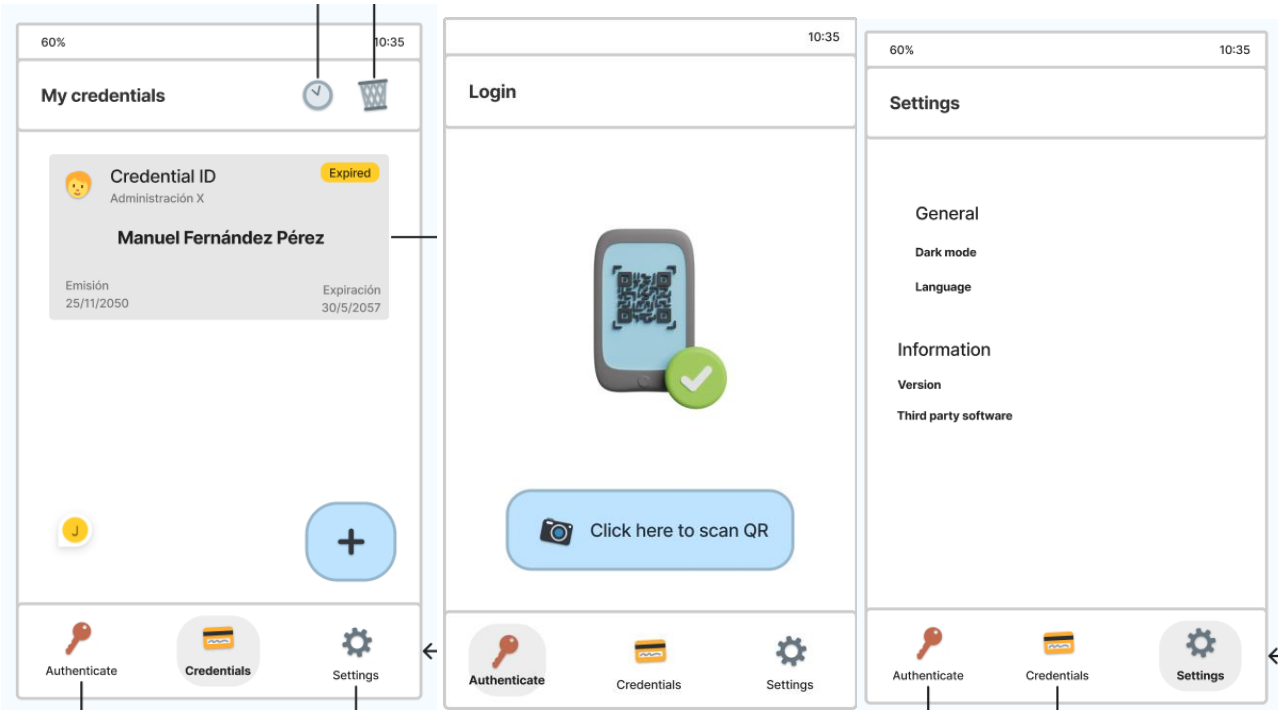

Figure 4. Wireframes of the IMPULSE User Wallet

1. **Authenticate**: A very simple screen where only the possibility to scan a QR code is provided. This way, depending on its content, it will redirect to the onboarding or authentication use case.
2. **Credentials**: A screen where the user's credential is displayed (they will usually have only one, but there could be more) with the possibility to view all its details when tapped. A button is also provided to create a new credential, which would directly redirect to the onboarding use case, but it would be necessary to choose an administration manually instead of having it embedded in the QR code like in the Authenticate screen.
3. **Settings**: Various application settings and information are displayed, such as the option to override the language or system theme, as well as view the version or third-party software used.

3.1.2 Onboarding/register from a QR code.

The process to register from screen 1 or *authenticate* consists of the following steps:

1. Scan a valid QR code that also corresponds to the registration with a specific administration. Note that this step can be perfectly replaced to click on a deep link.
2. Accept the specific privacy policy of the administration if it is the first time interacting with it, or a previous consent is not valid anymore.
3. A selfie from the user is requested. Then, a facial recognition process is performed to extract a biometric profile that will serve as a means to protect the identity verifiable credential.
4. Some preliminary data about the ID document are requested, such as nationality and the type of document itself.
5. Images of the front and back of the ID document are requested. They will be used to extract information from the MRZ, and along the selfie previously taken, to check the validity of the document provided.
6. The user is asked to manually validate the information that has been extracted from the ID document, to detect any errors in the extraction process.

At the end of this process, if everything went well, the user would be presented with a success screen informing them that the request has been submitted successfully and they will be notified when public administration validations are completed.

3.1.3 Onboarding/register from the + button on the credentials screen.

The process will begin once the floating button on screen 2 or *credentials* is tapped. The process is identical to the previous one, with the difference being that instead of scanning a code that implicitly selects the public administration for the user, the administration must now be manually selected from a list. The list of potential administrations to choose from may prioritize those administrations that are geographically closer to you or those from countries that speak the same language as the one used in your application.

3.1.4 Login from a QR code.

This time, the process will be initiated again by tapping the QR scan button on screen 1 or *authenticate*.

1. Scan a QR code that corresponds to the login with a specific administration. Note that this step can be perfectly replaced to click on a deep link.
2. Accept the specific privacy policy of the administration if it is the first time interacting with it, or a previous consent is not valid anymore.
3. Select the identity verifiable credential requested to log in.
4. You are required to scan your face to prevent any type of impersonation.

In this case, facial scanning is performed in the final step, unlike in the onboarding process, as it serves as the final protection before logging in, and it is process executed locally.

3.2 Application UI design

Regarding the visual design section, we have chosen to use the dark blue colour that was part of the impulse website as the accent colour. We have complemented it with other colours, such as a range of yellows for warning states, a range of reds for error states, and a range of greens for success states. Additionally, a range of violet tones was used for information banners, and finally, a range of greys was used as background colours to display different levels of depth. Below is a sample of these colors.

	Pale	*Normal*	*Dark*	*Greyish*	*Saturated*
Information					
Error					
Warning					
Success					

	Normal	*Translucent 75%*	*Translucent 50%*
Blue/Accent			

	Lightest	*Light*	*Dark*	*Darkest*
Grey				

	Normal	*Translucent 10%*
Black		

	Normal	*Translucent 75%*
White		

The purpose of these colour ranges is twofold: on the one hand, to provide different levels of emphasis to each element of the interface while maintaining a level of contrast between the different interface elements, as recommended by standards such as the Web Content Accessibility Guidelines [8]. Below are several screens showing how the colours are used in the interface.

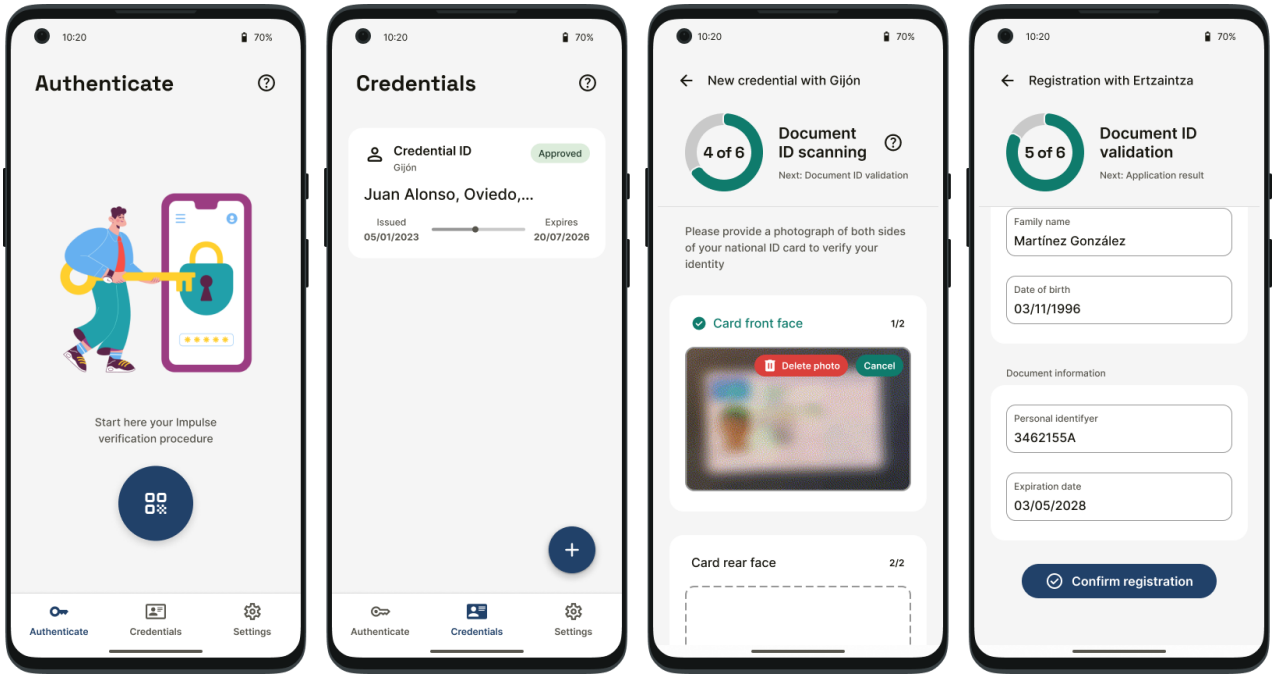

Figure 5. Examples of windows in the IMPULSE User Wallet

As for the text, we have used two typefaces: Space Grotesk [8] and Inter [9]. The former is used in titles and large text in the interface where it is necessary to give extra emphasis, and for the rest of the text, we have used a sans-serif font specifically designed for readability in digital environments such as Inter. The font sizes are those recommended by Google's Material Design [10] guidelines to ensure optimal readability. To give a friendlier touch to the interface, we have incorporated a series of illustrations that accompany different

screens in the application. All of them were obtained from the Icons8 [11] assets service, belong to the "Sammy" illustration package, and are free to use as long as their authorship is credited in the application.

Finally, the style of the application is clearly influenced by Google's Material Design 3, which has been slightly modified to incorporate interface elements from ColorOS [12], used by Oppo, such as the large white areas that denote areas of the screen where interaction with the user occurs (something that Samsung also does with OneUI [13]). This way, we achieve a clean, minimalist, accessible, and modern interface that follows the brand colours of Impulse.

4 How to use IMPULSE wallet

Figure 3 shows the authenticate and credentials screen of the IMPULSE mobile application. The user has a single button to both log in and register by scanning a QR code or a "+" button to directly initiate the registration process.

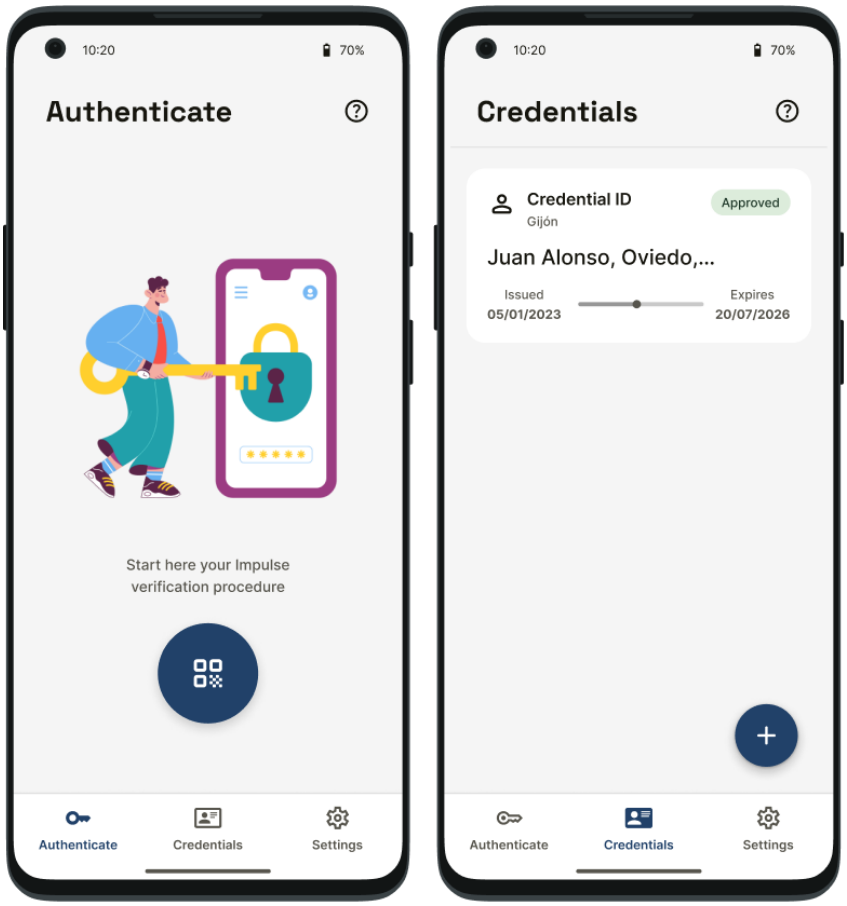

Figure 6. Main windows in the IMPULSE User Wallet

If we wanted to register, this functionality is now divided into two screens. Firstly, if we want to scan a QR code, we simply point the phone towards it. Alternatively, if we want to manually choose the administration, we select 'create a new credential' button and then choose from the available administrations. Figure 4 shows this process. The next step in either case is the same.

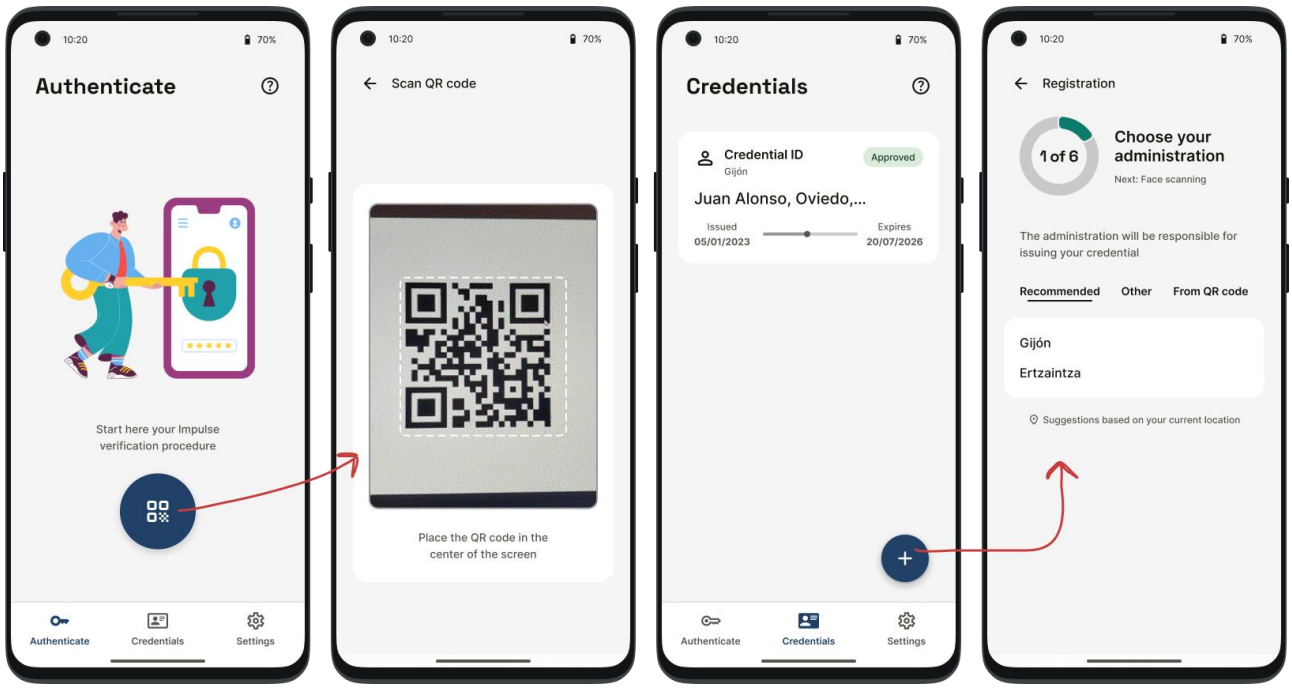

Figure 7. Option to register using a QR code, selecting the administration implicitly, or manual selection of the administration by creating a new credential

The next step is to accept the privacy policy of the public administration, which can be seen in figure 5. Further details about this screen will be detailed in section 5.

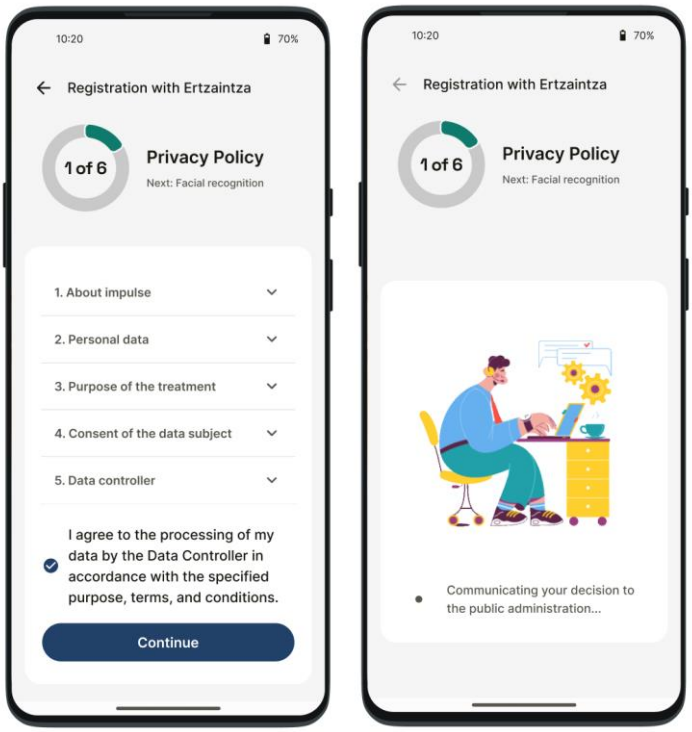

Figure 8. Option to register using a QR code, selecting the administration implicitly, or manual selection of the administration by creating a new credential

Afterwards, the user's face would be scanned as shown in Figure 6, where the first screen acts as a warning about what is going to happen, and the arrows simulate some of the possible interactions.

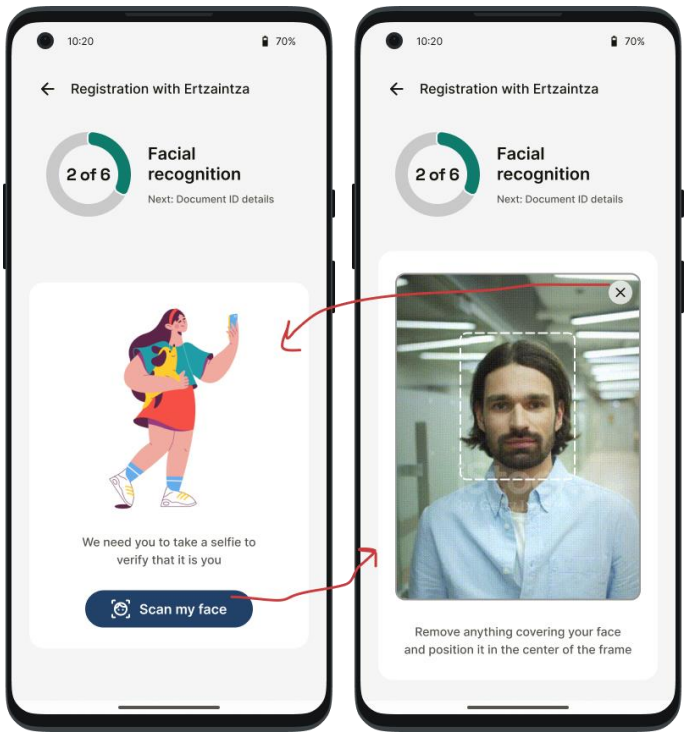

Figure 9. Facial scanning screen

Next, the user is informed of the need for a Document ID to continue with the process, and that details of the document need to be confirmed before proceeding with the actual scanning of the document. This is shown in Figure 7.

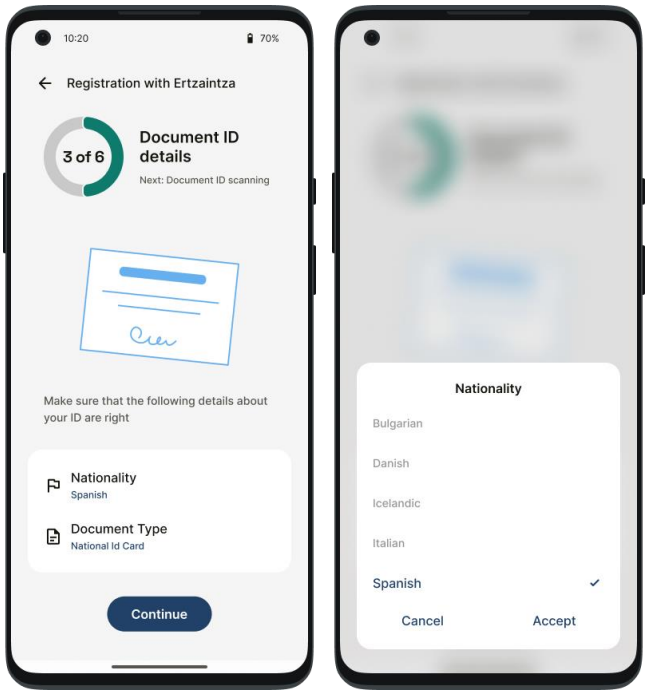

Figure 10. Document ID details verification screen

After the user has specified their document type, the next screen will prompt them to scan photographs of the document's front and back (in the case the document type was a passport, only the front side would be requested). To do this, they will have access to a camera interface specifically designed for this purpose, which shows a cropping guide matching the size of the document being scanned. All the screens regarding the document scanning, including the loading screens, are shown in Figure 8, along with their some of their possible interactions.

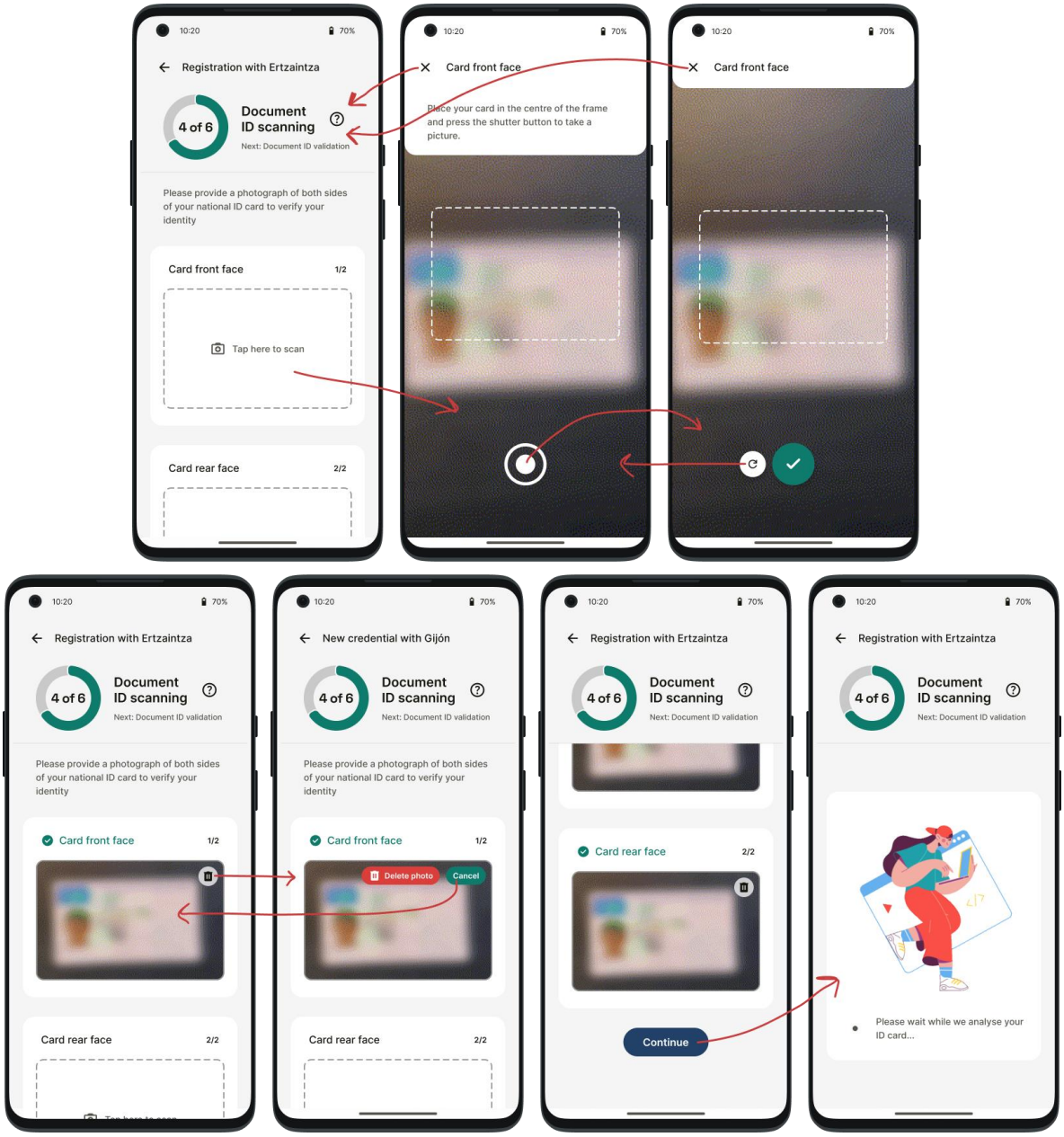

Figure 11. Details of document scanning screens (some of the possible interactions are marked with red arrows)

Finally, after the identity document has been scanned and its most important information extracted, a new screen displays the information in a form, allowing the user to modify any fields in case there were any errors in the MRZ reading task. Once everything is in order, the user moves on to the next screen to be informed about the status of the request.

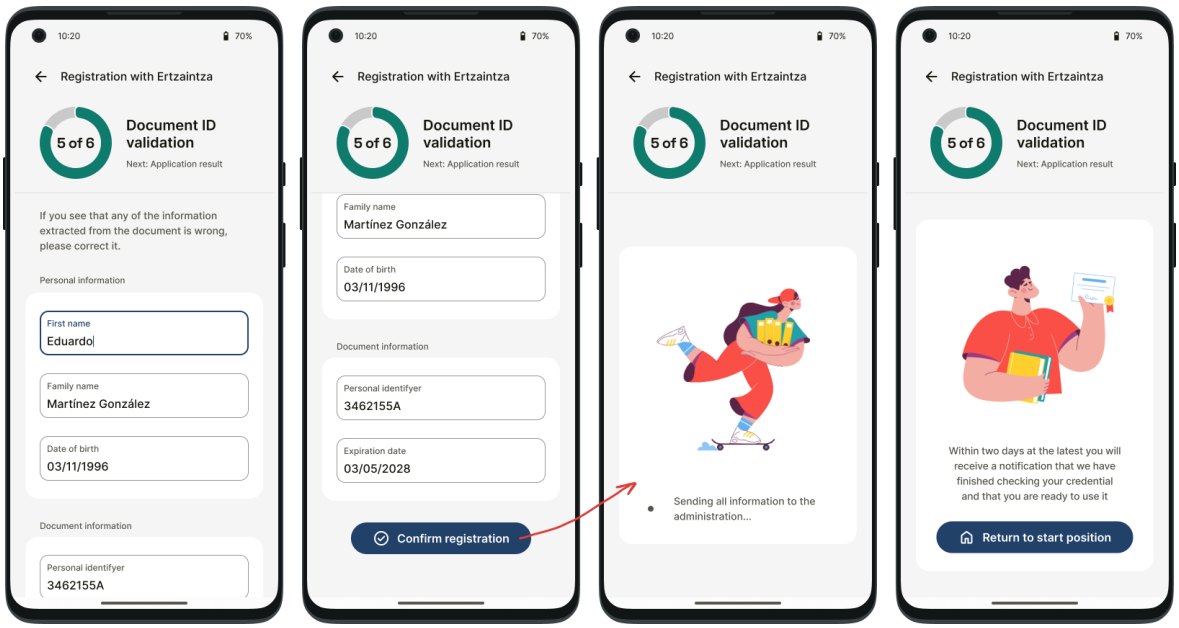

Figure 12. Screen for verifying Document ID information and final procedure status

Once the first part of the process is finished, the user will wait to receive a notification in the smartphone with the final steps. This notification will be received when the public servant operator checks the images in a dashboard. Currently, the dashboard looks like Figure 10.

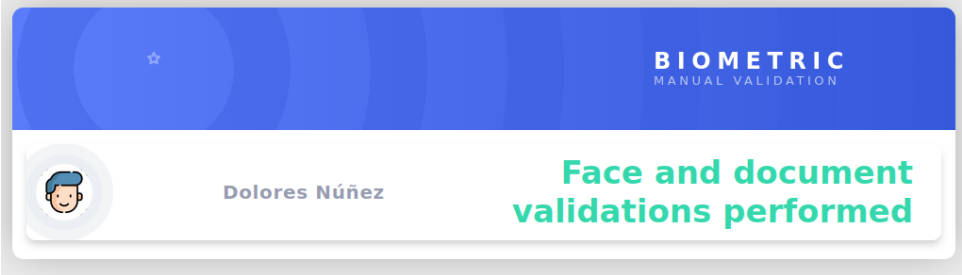

Figure 13. Onboarding requests dashboard

When the successful notification is received, the application will request the identity verifiable credential that was pending approval, so it can be used in login processes. Therefore, the visual appearance of the credential will change now from “Pending” state to “Approved” state, as shown in Figure 11.

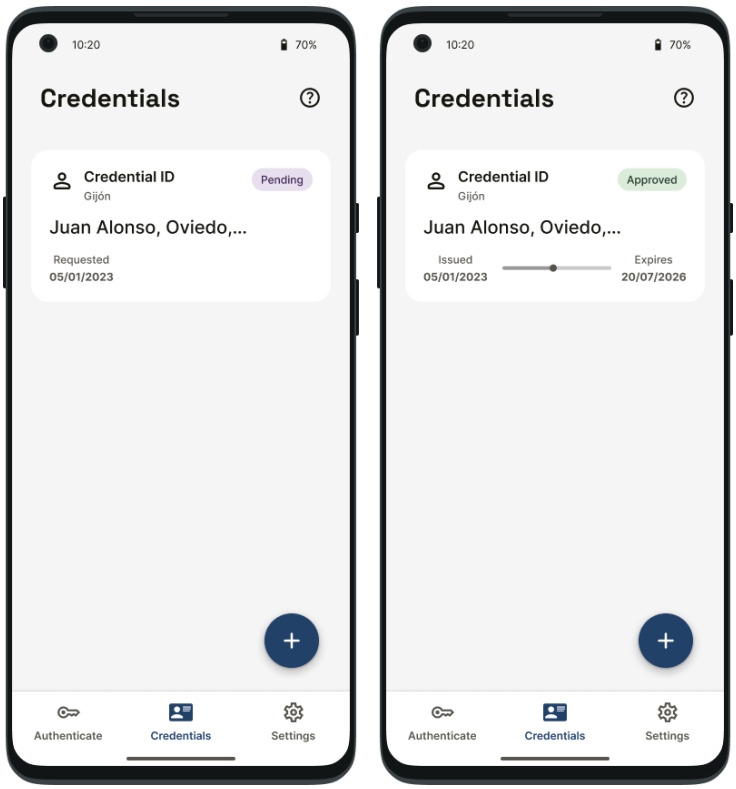

Figure 14. Credentials screen with a pending onboarding request and an a correctly issued credential

Once the identity verifiable credential is stored in the Android device, it can be used to authenticate the citizen. To do so, you must go to the website of a public administration and tap on the 'Log in' option, where a QR code will be presented to you. This can be seen in Figures 12 and 13.

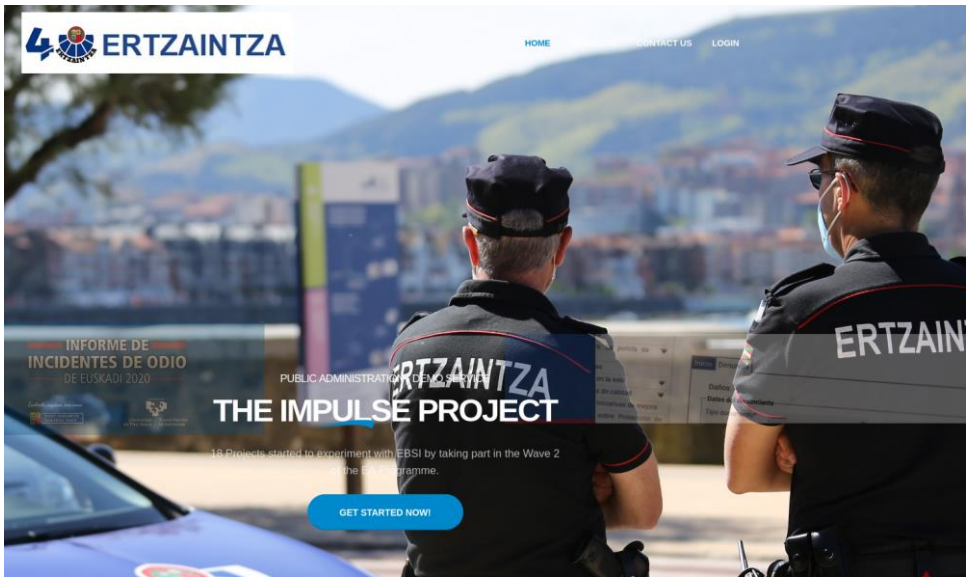

Figure 15. Public administration web page

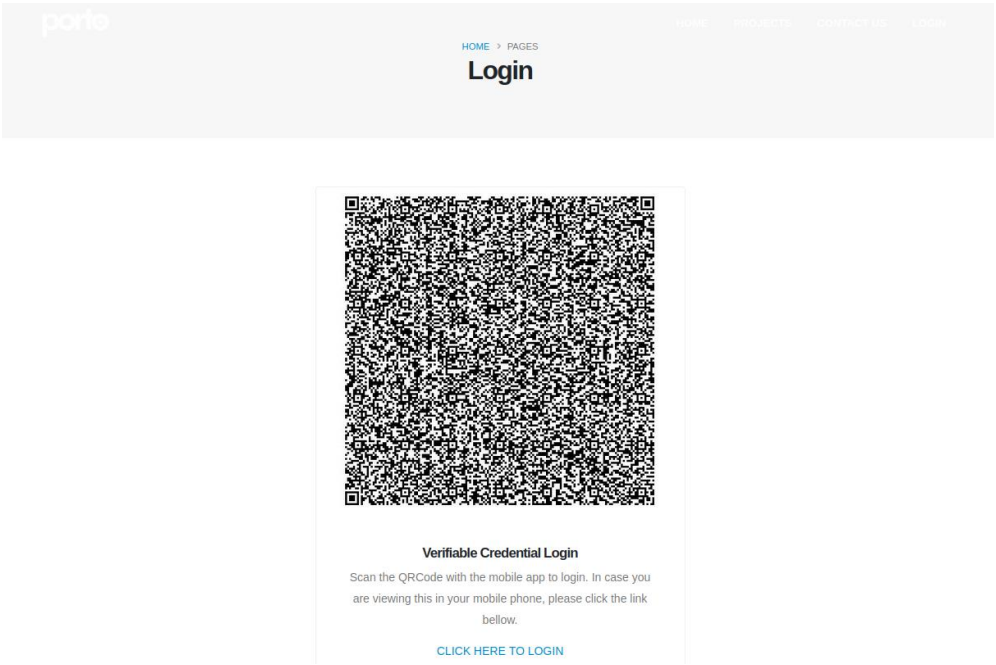

Figure 16. QR code shown in the public administration web page

Again, from the main screen or 'Authenticate' option, we must access the button to scan the QR code, which in this case will be related to a login in the mentioned administration. It is the same process shown in the first two images starting from the left in Figure 4. After scanning the QR code, you will enter the use case of authentication with the chosen administration. To do so, in addition to having to accept the privacy policy if it is the first time you are contacting the administration (or a previous consent is invalid), you will be asked to select the necessary credential. In this case, it will be a credential ID, as shown in Figure 14.

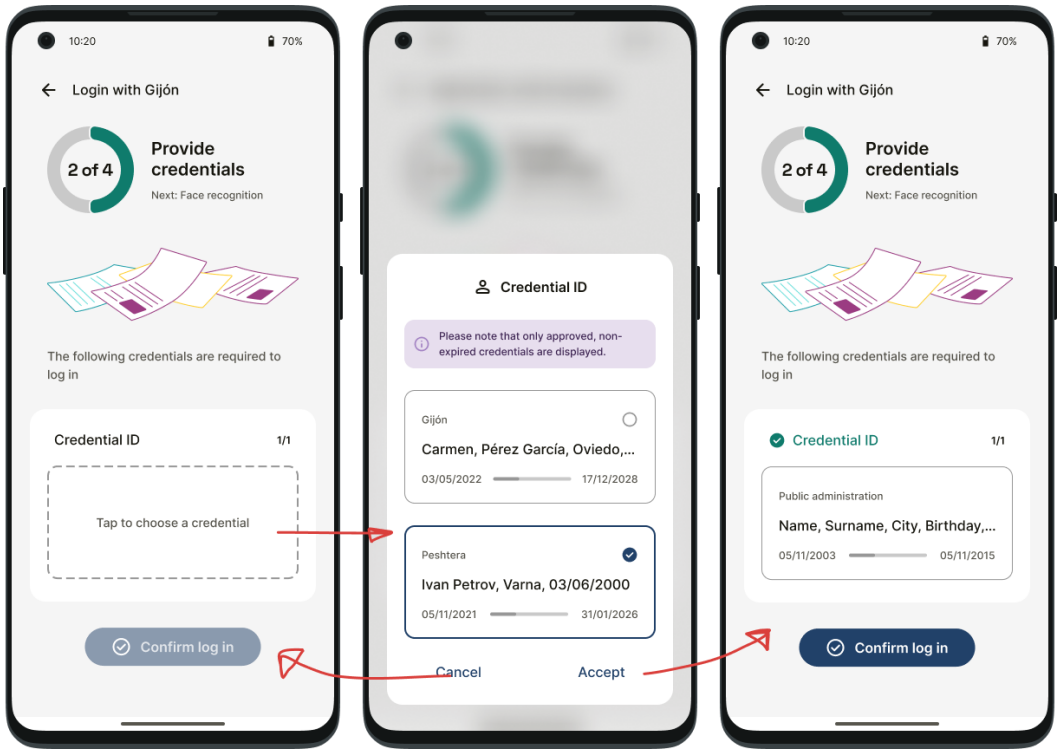

Figure 17. Screen for selecting credentials in the login process

Finally, it is necessary to scan your face to surpass the last local layer of security to the login procedure, just as shown in Figure 6. After scanning and a brief loading screen, a message will be displayed on the mobile device indicating that the login was successful, and the administration's web page will provide you with the requested public online service. This is shown in Figures 15 and 16.

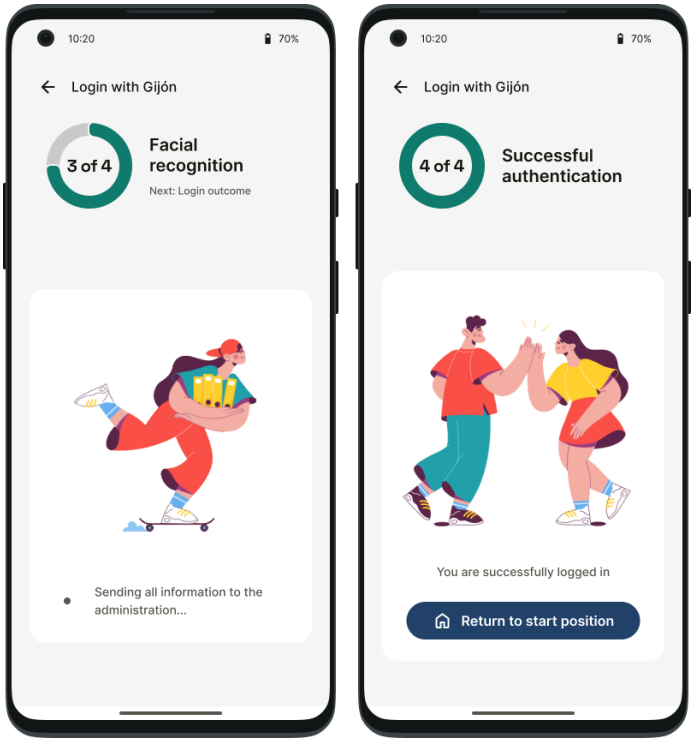

Figure 18. Result of a successful login in the mobile application

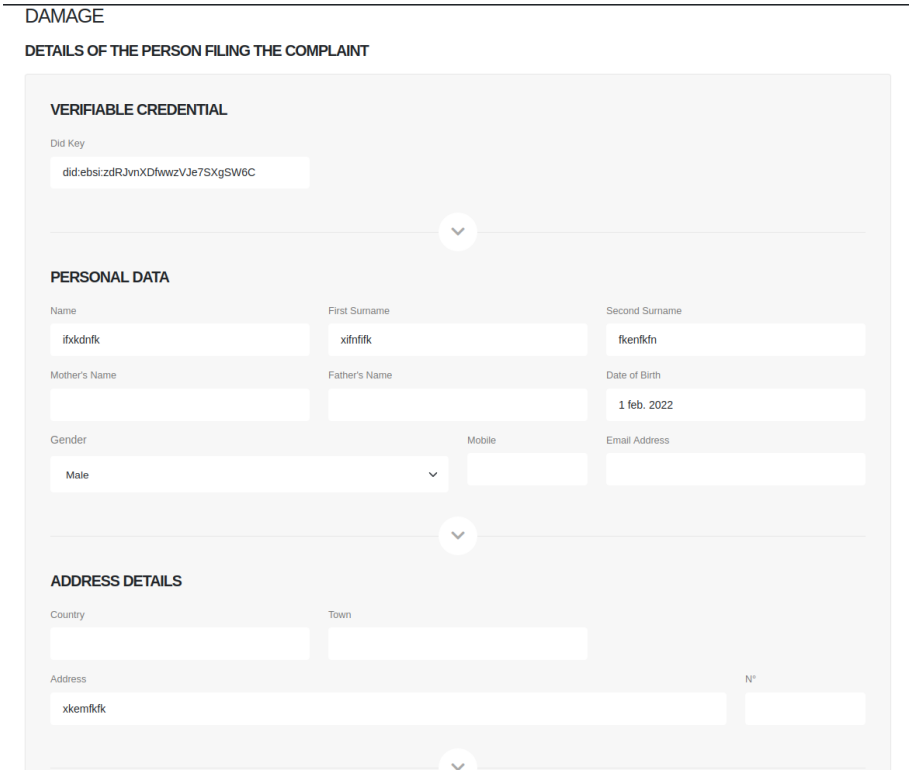

Figure 19. Result of a successful login on the public administration website

5 Specifications for accessibility

One of the purposes of IMPULSE is to facilitate the accessibility to the diverse demographic groups every society constitutes. To accomplish this duty, some considerations have been taken and some tools will be used, or are already implemented:

The two specifications explained below correspond to features already present in the first round of the IMPULSE project.

- An eID management approach like the one implemented in IMPULSE avoids the use of passwords, by means of a combination of biometrics and user-centric Self Sovereign Identity. This facilitates the access to the service by the people ensuring low cognitive loads.
    - Biometrics: Using the biometric profile ensures that only the correct person is allowed to authenticate to the service.
    - Self-Sovereign Identity: The use of Verifiable Credentials and asymmetric cryptography, always under the control of the user, ensures that the authentication to the Relying Party can be done without the use of any password.

- Regarding the capture of the selfie needed for the face recognition: to easily place the face of the user in front of the camera, a crop with the shape of a face is shown to the user. The same approach has been implemented in the case uploading of the ID documents.

- **Informed consent icons**: The Android application has to ask for the user to give the consent of sharing personal information at some specific points of the onboarding and authentication processes. To facilitate the user's understanding of these commonly ignored concepts of the GDPR, some designed icons linked with some short text will be used in the application. The idea behind this is to give the user a reasonable knowledge of what is being consented and what implications that consent might have. Always making it as simple as possible so the person can actually understand the concepts explained and remember them easily through the icons in future consents.

Figure 20. Icons designed by Cyberethics Lab

The GDPR gives a fundamental role to the full, freely given, specific, informed and unambiguous indication of how the consent to personal data's treatment is given. Following a contest held by the Italian Data Protection Authority, in which a set of icons representing the GDPR categories have been produced (under the CC BY license), Cyberethics Lab adapted those icons for the IMPULSE project.

The goal of the presented icons (Figure 21) is to provide a visual-based language with which the citizen can make a complete decision about their data in a fully informed way, solving the long-lasting problem of understanding often hard to grasp consent forms. Thus, those icons try to reshape the consent- giving procedure, allowing for a more open and transparent mechanism in which, thanks to easily readable and accessible information provided by those visual cues, the user/citizen has the opportunity to make significant decisions about their data, such as who will have the permission of process their data, for which purpose, for how much time.

As it can be seen in the next figure, a specific screen has been designed to provide the users the best possible experience when reading the privacy policy of the public administration, with the objective of facilitating the users the understanding of this process. The privacy policy has been divided in sections, and each section has one specific icon accompanied by a brief description that explains the purpose of it.

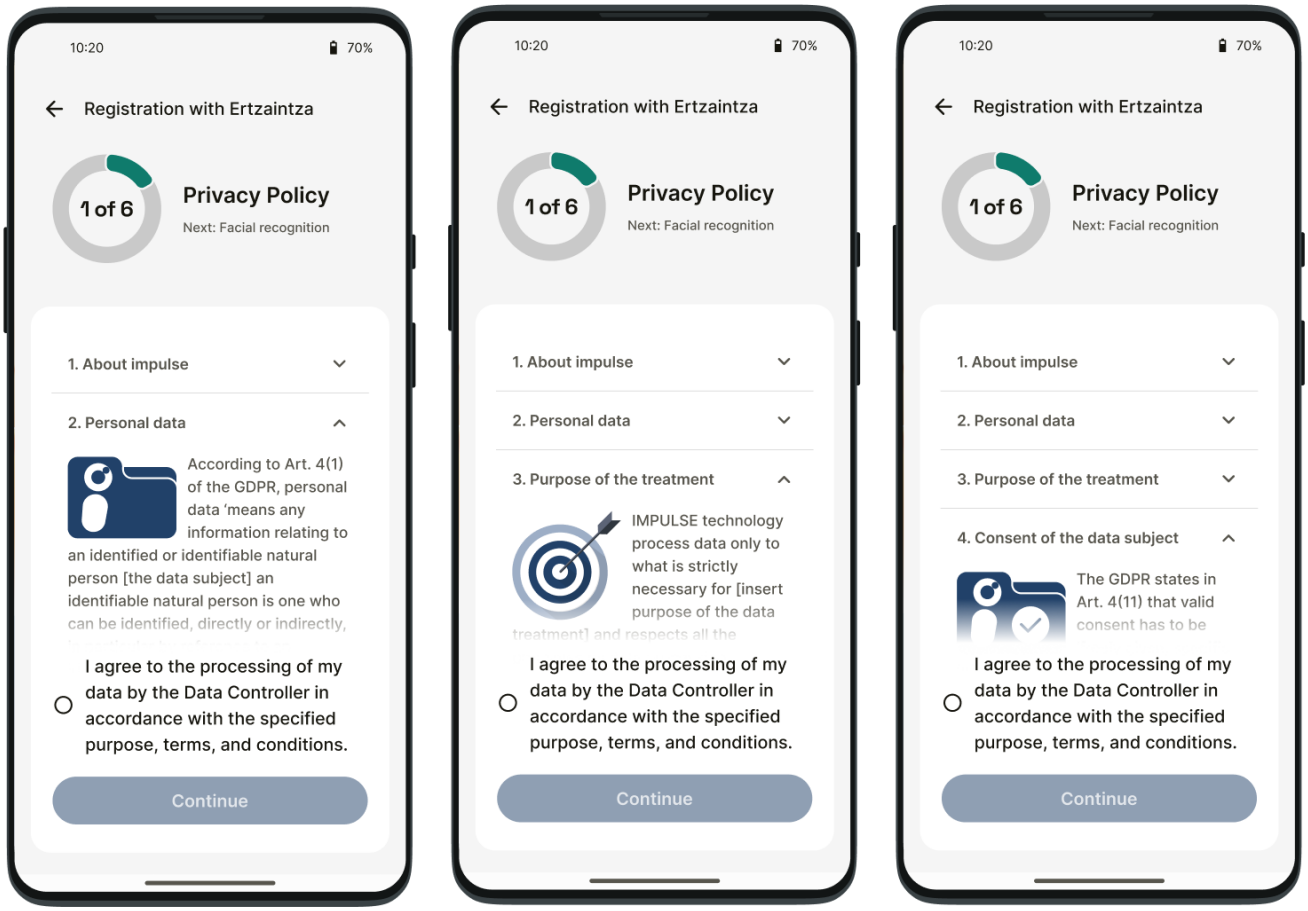

Figure 21. Privacy Policy Screen in the IMPULSE User Wallet

This specification is closely related to section 5.1.1 of the Ethics Protocol (D1.2), where is specified that persons have the right to be provided with clear, transparent and easily understandable information about how the controller use their information and about their rights.

- **Help Buttons**: In order to mitigate the occurrence of situations where the user feels lost using the application, the universal help icon, that can be seen in the next figure, has been placed around all the application. The aim of this button is to provide additional information on what is the purpose of the screen that they are seeing, or what is expected from them in order to continue with the process being carried out. This will reduce the confusion around the usage of the application in a very non-intrusive way.

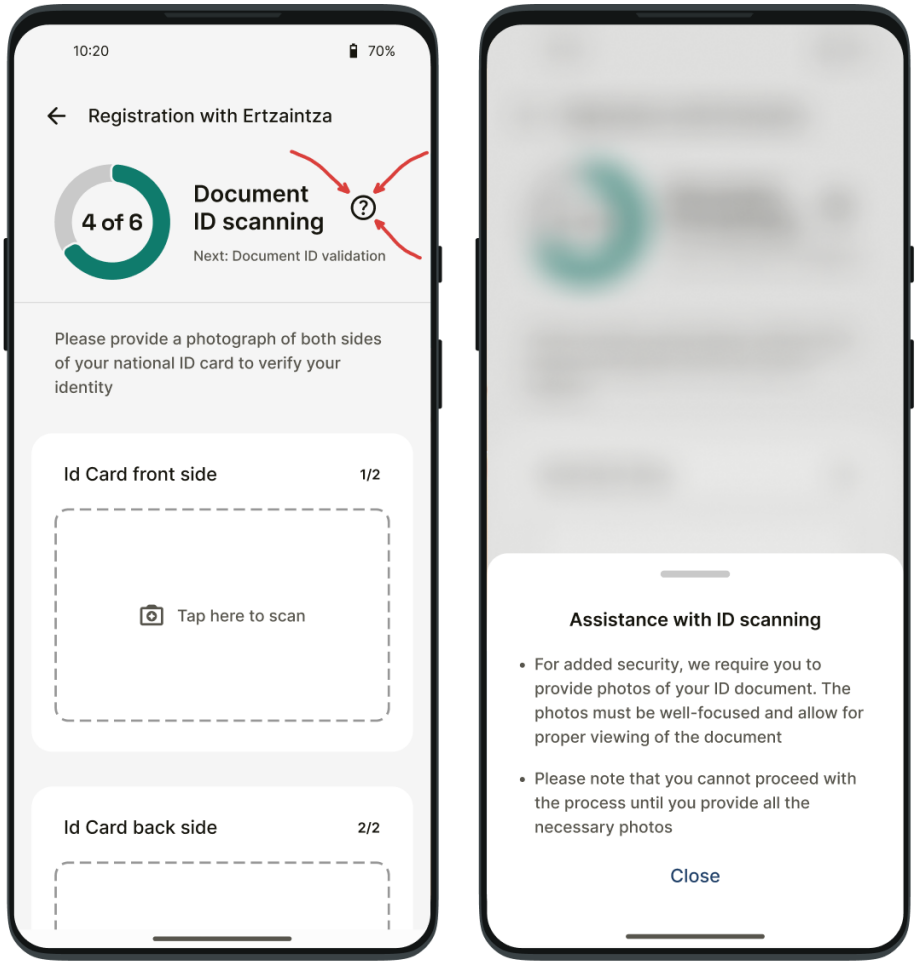

Figure 22. Help icon usage in a window of the IMPULSE User Wallet

- **Google Play Store Pre-Launch Accessibility Report**: The Pre-Launch Report tool of the Google Play Store has been used to compare the previous application design with the new one in terms of accessibility. The results are enlightening as we have improved all of the areas analysed by this tool in the implementation of the new application design.

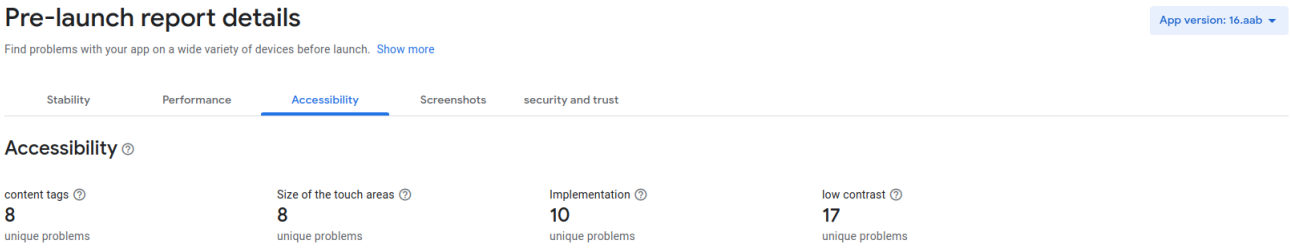

Figure 23. Google Play Store Pre-Launch Accessibility Report of the previous IMPULSE application

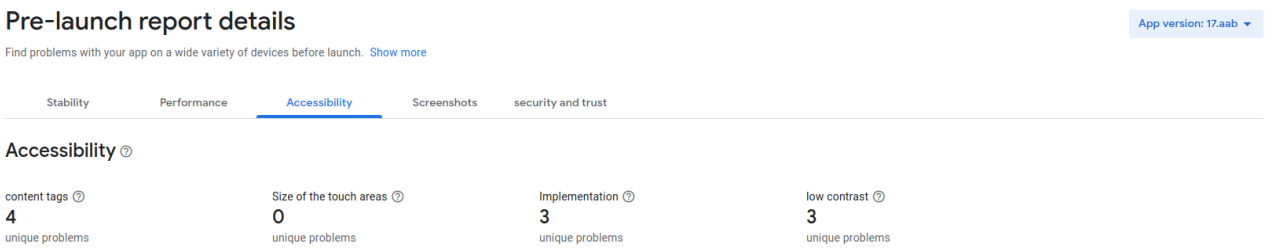

Figure 24. Google Play Store Pre-Launch Accessibility Report of the new IMPULSE application

Finally, it should be noted that certain decisions in the UI design have been made with accessibility in mind, such as the color scheme and font sizes used. These are clearly described in their corresponding section.

6 Conclusions

This deliverable describes the second version of the IMPULSE user app to be used by citizens, together with relevant aspects of the digital wallet, a guide on how to use it, and specifications for accessibility.

The IMPULSE user wallet consists of an Android application developed in Java/Kotlin. It contains a user interface to perform the registration and login operations, a wallet component that can onboard and authenticate a user in a Self-Sovereign Identity way, and a facial recognition module that protects the identity verifiable credentials stored in the device. The minimum Android version supported is Android 8.0 and it requires the following permissions: Full Network Access and Camera Access. The application has a size of approximately 170Mb in disk and it consumes around 260Mb RAM in execution.

There is a section that explains the wallet structure, including the different flows that the application can follow in order to complete the authentication and onboarding processes. The deliverable also describes how to use the IMPULSE wallet, showing screenshots of the different screens of the app and explaining each required step to perform the onboarding or the authentication process.

In terms of accessibility, some features have been implemented in this regard, like the no need for passwords, the facial recognition to unlock the credentials, the design of graphical icons to facilitate the understanding about the consent rules for sharing personal information, the privacy policy screens where these icons are placed within the IMPULSE application, the helping buttons to guide the user through the application, and some design discissions related to the colour scheme and the font sizes used. The application has also been analysed using the Google Play Store Pre-Launch tool to measure the accessibility in comparison with the previous version.

References

[1] **[WaltId, 2023]** Decentralized identity, credentials & wallets, https://walt.id/.

[2] **[WaltId, 2023]** Walt.ID SSI Kit, https://github.com/walt-id/waltid-ssikit.

[3] **[T. Lodderstedt, K. Yasuda and T. Looker, 2023]** OpenID for Verifiable Credential Issuance, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

[4] **[T. Lodderstedt, K. Yasuda and T. Looker, 2023]** OpenID for Verifiable Presentations, https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.

[5] **[Jetbrains, 2023]** Ktor: Build Asynchronous Servers and Clients in Kotlin, https://ktor.io/.

[6] **[Gradiant, 2022]** Android Ported SSI Kit, https://github.com/Gradiant/grad-ssikit-android.

[7] **[Android 8.0, 2017]** Android 8.0 Oreo, https://www.android.com/versions/oreo-8-0/.

[8] **[Florian Karsten, 2016]** Space Grotesk font, https://fonts.google.com/specimen/Space+Grotesk.

[9] **[Dalton Maag, 2007] Inter font**, https://rsms.me/inter/.

[10] **[Google, 2021]** Google Material Design 3, https://m3.material.io/.

[11] **[Icons8, 2023]** Icons8, https://icons8.com/illustrations.

[12] **[Oppo, 2023]** Color OS 13, https://www.oppo.com/es/coloros13/.

[13] **[Samsung, 2021]** OneUI, https://www.samsung.com/es/one-ui/.

[14] **[European Commission, 2019]** European Self-Sovereign Identity Framework, https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=379913698.

[15] **[Accessibility Scanner]** Accessibility Scanner in Android, https://support.google.com/accessibility/android/faq/6376582?hl=en&visit_id=637862245064926873-4111578236&rd=1.

[16] **[European Commission, 2021]** EBSI v2 Architecture, https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Architecture.