



# Identity Management in PUbLic SErvices

---

## D5.3 IMPULSE wallet - V1

---

### Lead Authors:

**Dolores Núñez Taboada (GRAD), Xavier Martínez (GRAD)**

### With contributions from:

**Alicia Jiménez (GRAD), Alejandro Cuenca Parra (GRAD),  
Jaime Loureiro (GRAD)**

**Reviewer: [Bilal Naqvi (LUT), Daniele Levorato (IC)]**

<b>Deliverable nature:</b>	Demonstrator (D)
<b>Dissemination level: (Confidentiality)</b>	Public (PU)
<b>Delivery date:</b>	29-04-2022
<b>Version:</b>	1.0
<b>Total number of pages:</b>	28
<b>Keywords:</b>	wallet, app, accessibility, identity verifiable credential, service, authentication, onboarding



## Executive summary

This document summarizes the IMPULSE user wallet specifications, giving a hint about the way of using the Android application that acts as an interface to the 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 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, or clicking a deep link. At this point, the user will be identified after filling out a form, taking a selfie and identity document photos (one per each side), and uploading all of these to the IMPULSE Enterprise service. The verification of the information uploaded will be done using two biometric validation services, one that matches the face in the selfie with the one in the identity document, 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 verified as authentic, 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. Then, the person will select the previously obtained credential, take a selfie to unlock it, and confirm that it's the one that is going to be presented. 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 were placed.

Regarding the accessibility section, some features are 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.

In the Annex A, there is a link to the video demo of the first version of IMPULSE wallet (V1). It is worth noting that additional features have already been identified to be addressed for the second version of the IMPULSE wallet (V2) during the second implementation and testing round of the IMPULSE eID solution.

## Document information

<b>Grant agreement No.</b>	<b>101004459</b>	<b>Acronym</b>	<b>IMPULSE</b>
<b>Full title</b>	<b>Identity Management in PUBlic SERVICES</b>		
<b>Call</b>	DT-TRANSFORMATIONS-02-2020		
<b>Project URL</b>	<a href="https://www.impulse-h2020.eu/">https://www.impulse-h2020.eu/</a>		
<b>EU project officer</b>	Giorgio CONSTANTINO		

<b>Deliverable</b>	<b>Number</b>	D5.3	<b>Title</b>	IMPULSE wallet - V1
<b>Work package</b>	<b>Number</b>	WP5	<b>Title</b>	Technology research, evaluation and integration
<b>Task</b>	<b>Number</b>	T5.5	<b>Title</b>	Continuous integration and deployment for pilots and demonstration”

<b>Date of delivery</b>	<b>Contractual</b>	M15	<b>Actual</b>	M15
<b>Status</b>	version 1.0		<input checked="" type="checkbox"/> Final version	
<b>Nature</b>	<input type="checkbox"/> Report	<input checked="" type="checkbox"/> Demonstrator	<input type="checkbox"/> Other	<input type="checkbox"/> ORDP (Open Research Data Pilot)
<b>Dissemination level</b>	<input checked="" type="checkbox"/> Public <input type="checkbox"/> Confidential			

<b>Authors (partners)</b>	GRAD		
<b>Responsible author</b>	<b>Name</b>	Dolores Núñez Taboada and Xavier Martínez	
	<b>Partner</b>	GRAD	<b>E-mail</b> dnunez@gradiant.org

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

Version Log			
Issue Date	Rev. No.	Author	Change
January	v0.1.0	Dolores Núñez Taboada (GRAD), Alejandro Cuenca Parra (GRAD)	First draft version of the document.
February	v0.1.5	Dolores Núñez Taboada (GRAD), Xavier Martínez (GRAD)	First review and update of the first draft of the document.
March	v0.2.0	Dolores Núñez Taboada (GRAD), Xavier Martínez (GRAD)	Second review and update of the document.
April 25th	V0.3	Bilal Naqvi (LUT), Daniele Levorato (IC)	Comments from official reviewers assigned
April 29th	V1.0	Dolores Núñez Taboada (GRAD), Xavier Martínez (GRAD), Jaime Loureiro (GRAD), Alicia Jiménez (GRAD)	Third review and update of the document.

## 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 Onboarding/Enrolment process .....	8
2.1.2 Authentication process.....	10
2.2 User wallet features.....	12
2.3 User wallet requirements .....	12
3 How to use IMPULSE wallet.....	13
4 Specifications for accessibility.....	24
5 Conclusions .....	26
References .....	27
Annex A First version of the IMPULSE citizen wallet (v1) .....	28

## List of figures

Figure 1. High level message flow of the onboarding process from the mobile app perspective .....	9
Figure 2. High level message flow of the authentication process from the mobile app perspective .....	11
Figure 3. Main window in the Impulse User Wallet .....	13
Figure 4. Windows with options to register users (option 1) .....	14
Figure 5. Windows with options to register users (option 2) .....	14
Figure 6. Form with personal information.....	15
Figure 7. Photo capture window .....	16
Figure 8. Instructions to take selfie .....	16
Figure 9. Run window .....	17
Figure 10. End of process window .....	18
Figure 11. Dashboard to manual validation.....	18
Figure 12. IMPULSE IMPORTANT INFO message.....	19
Figure 13. Completed user registration .....	19
Figure 14. Public administration web.....	20
Figure 15. QR code.....	20
Figure 16. Login in Impulse User Wallet .....	21
Figure 17. Choose credential for Login.....	21
Figure 18. Take a selfie for Login .....	22
Figure 19. Data of the selected credential .....	22
Figure 20. Public administration form.....	23
Figure 21. Icons designed by Cyberethics Lab.....	25

## 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 first 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 create an onboarding process to obtain an identity verifiable credential and use it to authenticate against a Public Administration and receive an 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 filling out and upload a form and taking a selfie and photos of each side of an id document. After the IMPULSE Enterprise Service verifies that all of 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 or click a deep link to initiate it. Then, the user will select the previously obtained credential, take a selfie to unlock it, and confirm that it is the one that is going to be presented. 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, Android Accessibility Scanner, 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 are described. First, the architecture of IMPULSE solution from a users' wallet perspective is explained. This implies that the two main flows of the solution are discussed in this subsection (onboarding and authentication). Then, the general features of the application are exposed, and finally, the requirements to installation and use are presented.

### 2.1 User Wallet architecture

The IMPULSE user wallet is an Android application developed in Java/Kotlin over the Android SDK API 30. This app 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.

Note that the Figure 1 has a component (Informed Consent Service) in orange. This specific colour implies that this component was not implemented in the first round of IMPULSE, but it will be addressed in the second round version of the IMPULSE solution.

#### 2.1.1 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 [1].

#### Considerations:

1. In this onboarding process, the decentralized identifier (DID) and public key of the natural person is anchored in the EBSI ledger [5]. We are aware of the GDPR compliance issues in this regard and planned to address this issue in the second round of IMPULSE. We will follow the ESSIF updates in this regard to be completely aligned with their identity model.
2. After the initiation of the onboarding process, and before the uploading of the photos, the application requests the user to fill a form. This step will not be required in the second version of IMPULSE, as the information in the form will be directly extracted from the ID document image. After the extraction is completed, the information obtained will be shown to the user, and in case the extraction was not precise enough in all the fields, the user can correct it before they finally confirm it. In this first round of IMPULSE, this feature is not implemented because the OCR module that will extract the information is still under development.

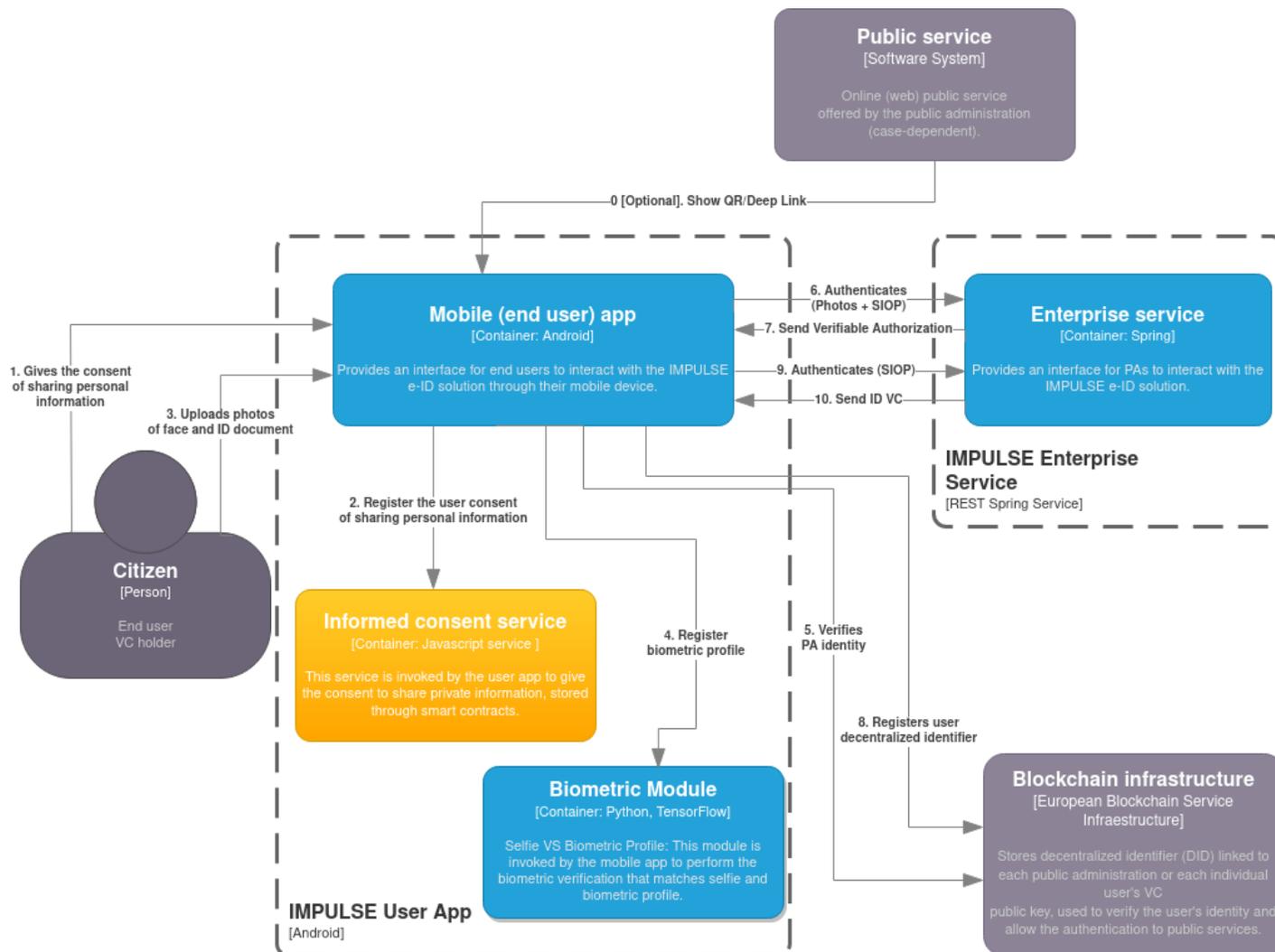


Figure 1. High level message flow of the onboarding process from the mobile app perspective



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 mobile IMPULSE user 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 (inside 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 citizen gives the consent to share personal information (Steps 1 and 2), the mobile app asks the user to upload photos of their face and ID document (Step 3). Previously to send 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 4) for further validations in the authentication process once the user has been already enrolled in IMPULSE. In addition, the mobile user app will verify the PA's identity (PA's DID) in the EBSI blockchain in order to check if PA has been registered and it is in fact a trusted issuer (Step 5). Note that Step 1 and 2 will be implemented in the second version of IMPULSE.

At this point, all of the information is sent to the Enterprise Service alongside a proof of ownership of a specific DID (step 6). After some verification inside the Enterprise Service, an EBSI Verifiable Authorization (V.Auth) will be given to the user wallet (Step 7). The wallet now can use this V.Auth to register the user DID in the EBSI ledger (Step 8). Once the last step is done, the user wallet asks for the ID VC presenting the V.Auth obtained before (Step 9), and after some verifications by the Enterprise Service, the user wallet receives the identity verifiable credential (Step 10). 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).

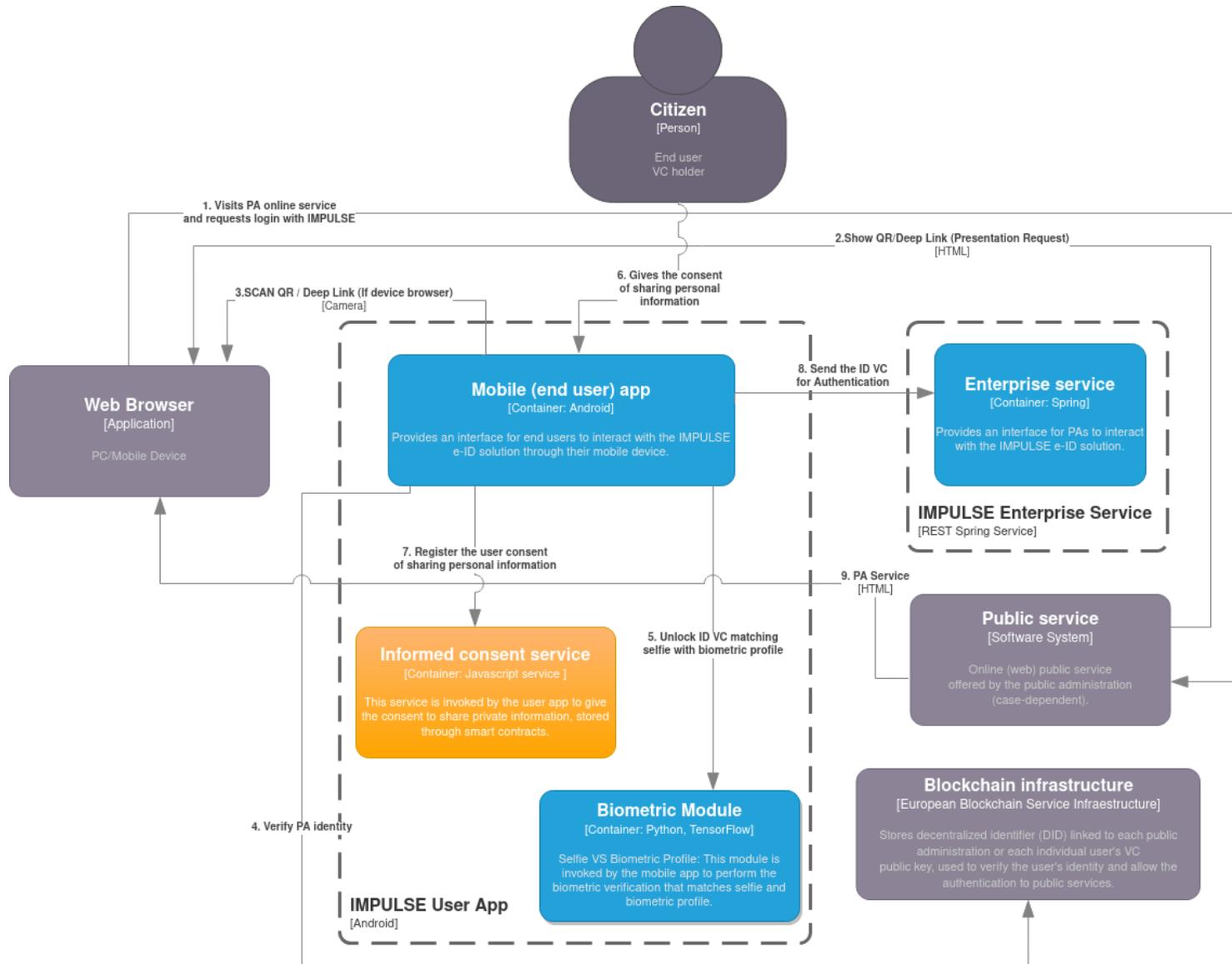
### **2.1.2 Authentication process**

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.

Once the citizen has been duly enrolled in IMPULSE, they may authenticate themselves with the online public administration service (PAS) by using her/his ID VC through the IMPULSE mobile application. First, the user accesses the web public service through a web browser and requests login with IMPULSE (Step 1). At this point, the public service shows a QR code to be scanned with the IMPULSE mobile user app or a deep link to be clicked (in case the web browser is in the same device) (Steps 2 and 3). Then, the user wallet verifies the identity of the public administration (PA) and checks if it belongs to the EBSI Trusted Issuer Registry (Step 4). Next, the user app asks the user for a selfie to match it with the biometric profile previously created, to unlock the ID VC (step 5). If previous steps go right and the citizen gives the consent to share personal information (Steps 6 and 7), the mobile app presents the user ID-VC for authentication (Step 8). Note that the step 6 and 7 will be implemented in the second version of IMPULSE.

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 (Steps 11 and 12). At this point the authentication process can be considered complete.





**Figure 2. 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



## 2.2 User wallet features

The app currently supports 3 languages: English, Spanish and Galician. In the future it will also support the following languages: Italian, Bulgarian, Danish and Icelandic. The language displayed in the app is the one configured on the mobile device. The default language is English, which means that if the mobile configuration language is not supported, English will be the displayed language.

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 IMPULSE) of the Wallet SSKit [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 its 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 form that has to be filled and 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 list of identity verifiable credentials stored in the device, so one can be selected and the process can be performed with it.

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, 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. All of the features regarding the informed consent of the user to share personal information are not implemented in this first round, but it will be available in the second version.

## 2.3 User wallet requirements

The minimal Android version supported is Android 8.0 (API 26) [3].

The IMPULSE app requires the following permissions:

- Full Network Access.
- Camera Access.

The network access permissions are used to connect with the server of IMPULSE project. 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 100Mb in disk.

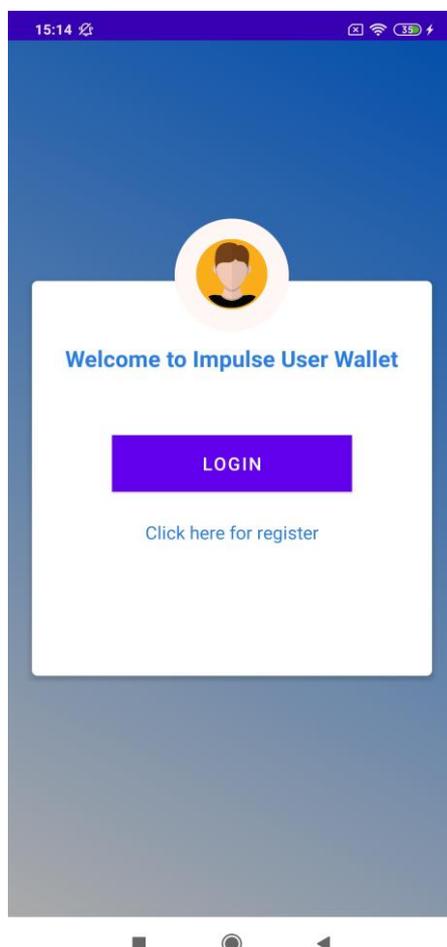
The application consumes around 260Mb RAM in execution.



### 3 How to use IMPULSE wallet

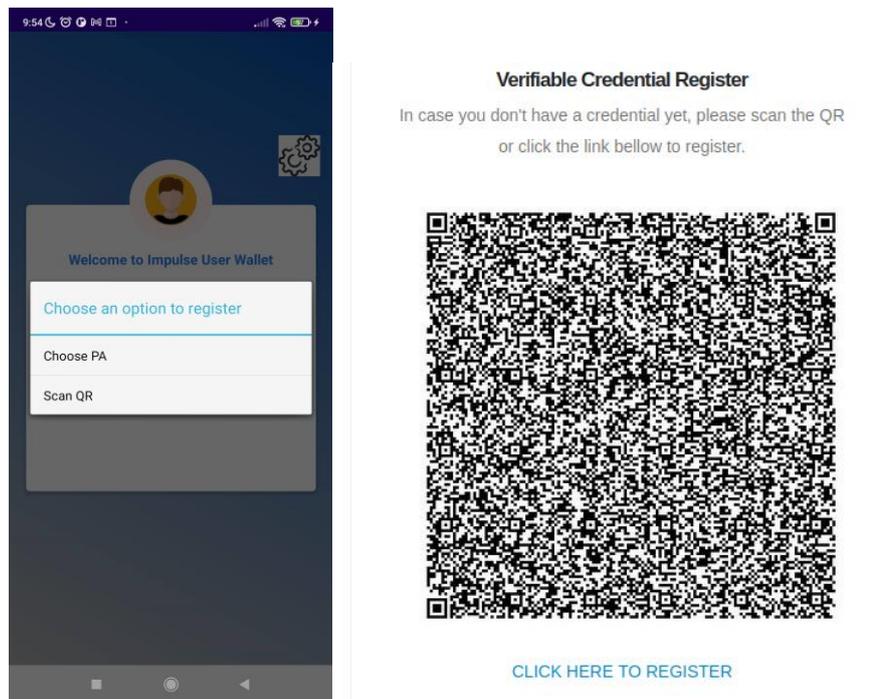
In Figure 3 it is shown the main window of the IMPULSE app. In this screen the user can perform two basic operations:

- Login
- Register



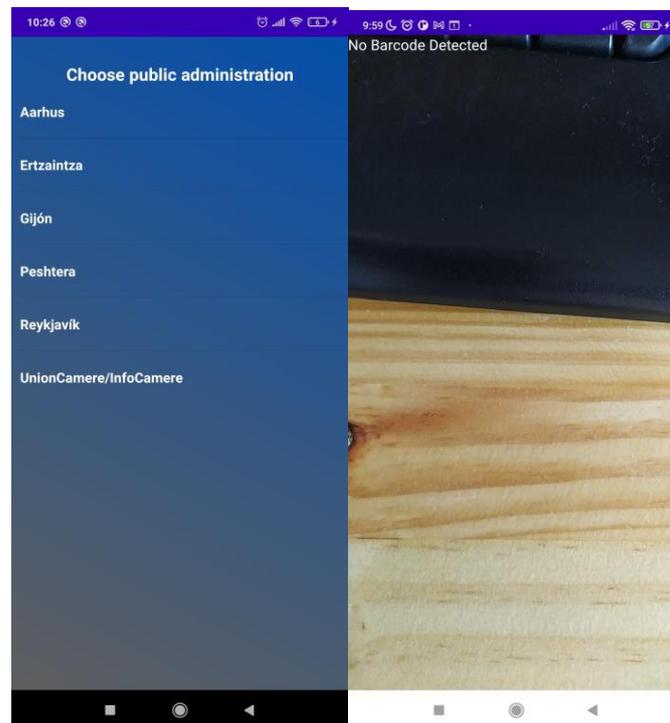
**Figure 3. Main window in the Impulse User Wallet**

When a user wants to register in the IMPULSE app, they can choose between selecting a public administration or scanning a QR, as it appears on the image on the left in Figure 4. It's also possible to click a deep link in the device browser and get redirected to the application, skipping this step, as it appears on the image on the right in Figure 4.



**Figure 4. Windows with options to register users (option 1)**

The Figure 5 presents how to select a public administration among the existing ones (image on the left), and how to scan a QR to dynamically make this selection (image on the right).



**Figure 5. Windows with options to register users (option 2)**

Once the selection of the municipality is done, the user has to fill out a form with personal data and ID card data (Figure 6). The data to fill in is the following:

- First and family name (Required data)
- Name and family name at birth (Optional data)
- Current address (Required data)

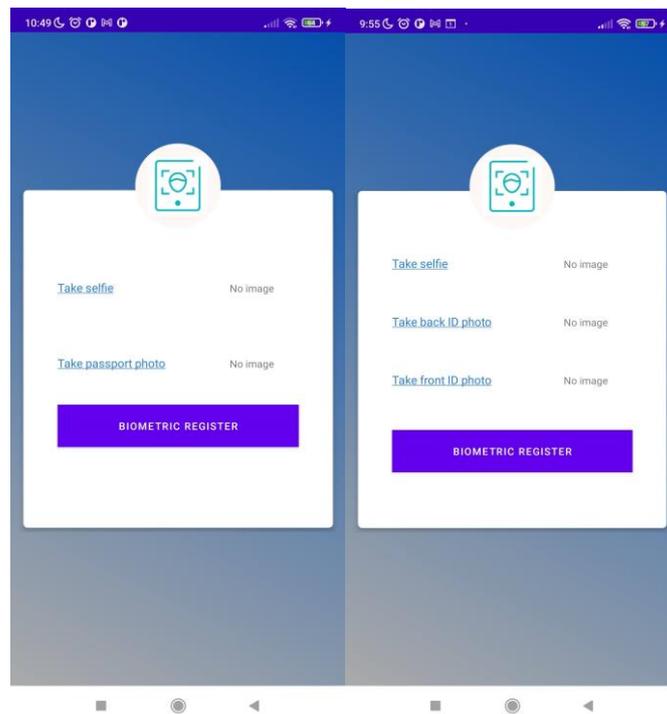
- Gender (Required data)
- Date and place of birth (Required data)
- Nationality (Required data)
- Document type (Required data): the options are ID card and passport.
- Number and expiry date of selected document (Required data)

In the second round, all the information is planned to be extracted directly from the ID Document photos that are taken in the next step.

The image displays two side-by-side screenshots of a mobile application form. The left screenshot, titled "Personal data", contains several input fields: "First Name", "Family Name", "Name and family name at birth (optio...", "Current address", "Gender" (with "Male" selected), "Date of birth" (Not selected), "Place of birth", and "Nationality" (SPANISH). The right screenshot, titled "Info about id card", includes a "Document type" dropdown menu (ID CARD selected), a "Number of ID or passport" field, an "Expiry date" field (Not selected), a checkbox for "You accept the sharing of the data used by this app", and a prominent "SUBMIT" button.

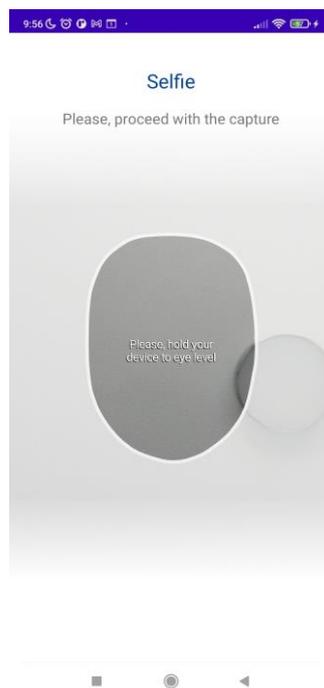
**Figure 6. Form with personal information**

Once the form is filled, it is required for the user to take and upload a selfie and one or more photos of the identity document according to the selected type. Once the ID card is selected (see image on the left in Figure 7), it is necessary to take a photo of the frontside of the ID card as well as the backside . If the passport is selected (see image on the right in Figure 7), it is necessary to take only one photo of the page where the user's photo appears.



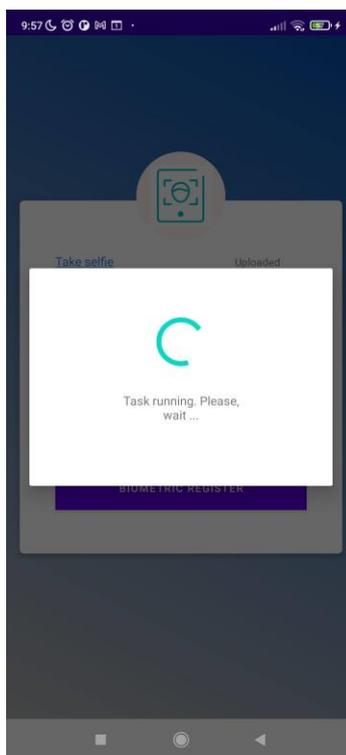
**Figure 7. Photo capture window**

To ease capturing a selfie, the camera displays an oval to place the users' face and some instructions for help, as seen in Figure 8.



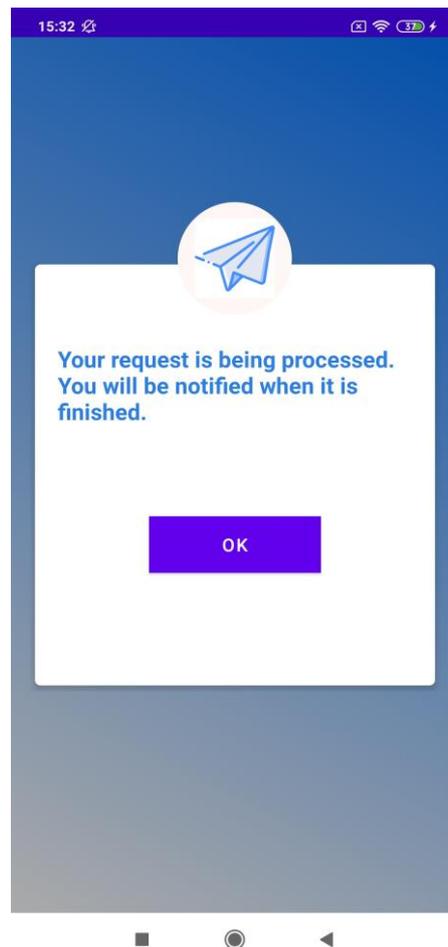
**Figure 8. Instructions to take selfie**

Once the button is pressed, the app executes a series of tasks in the background (e.g. storing the biometric profile, sending personal data to the Enterprise Service, etc.), as seen in Figure 9.



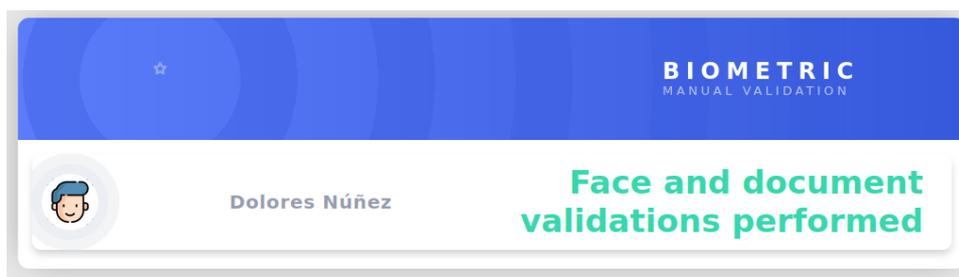
**Figure 9. Run window**

The user app receives an acknowledge from the Enterprise Service when all the personal data has been successfully collected. At this point (Figure 10) the user can consider this part of the process finished and has to wait for a notification regarding the availability of the credential.



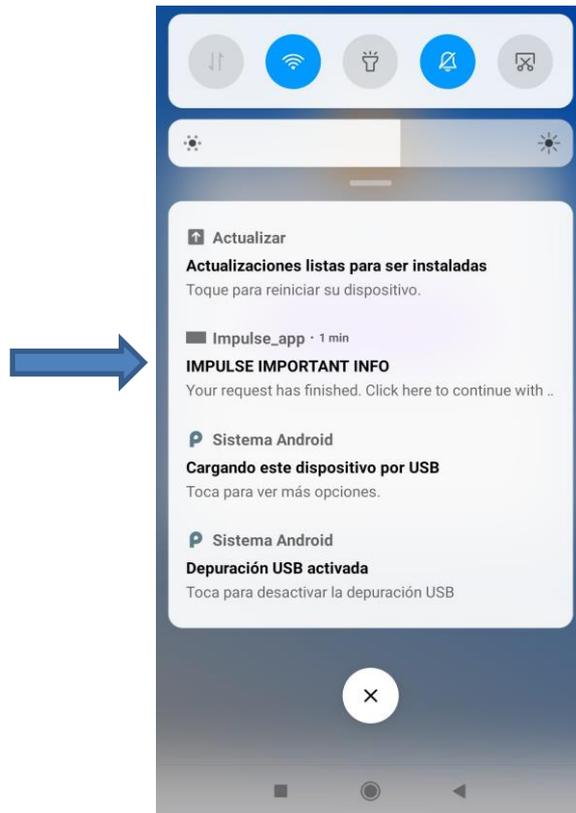
**Figure 10. End of process window**

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, in the scenario where a manual validation is required either by legal issues or by an inconclusive score in the facial recognition or document verification services. Currently, the dashboard looks like Figure 11.



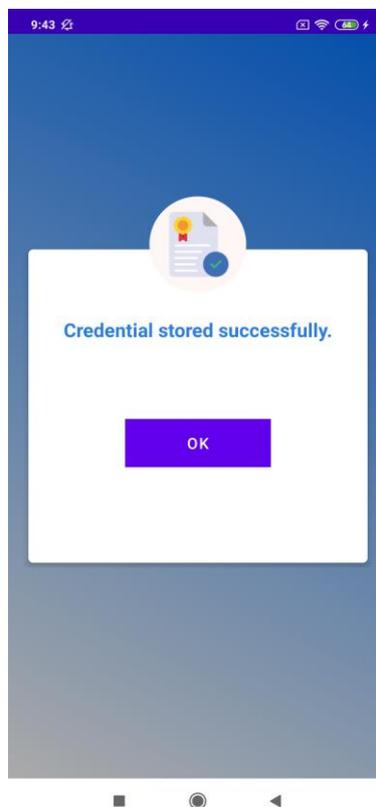
**Figure 11. Dashboard to manual validation**

When the notification arrives to the smartphone, the user must click on it. The title of the notification is "IMPULSE IMPORTANT INFO" and the message is "Your request has finished. Click here to continue with the process.", as seen in Figure 12.



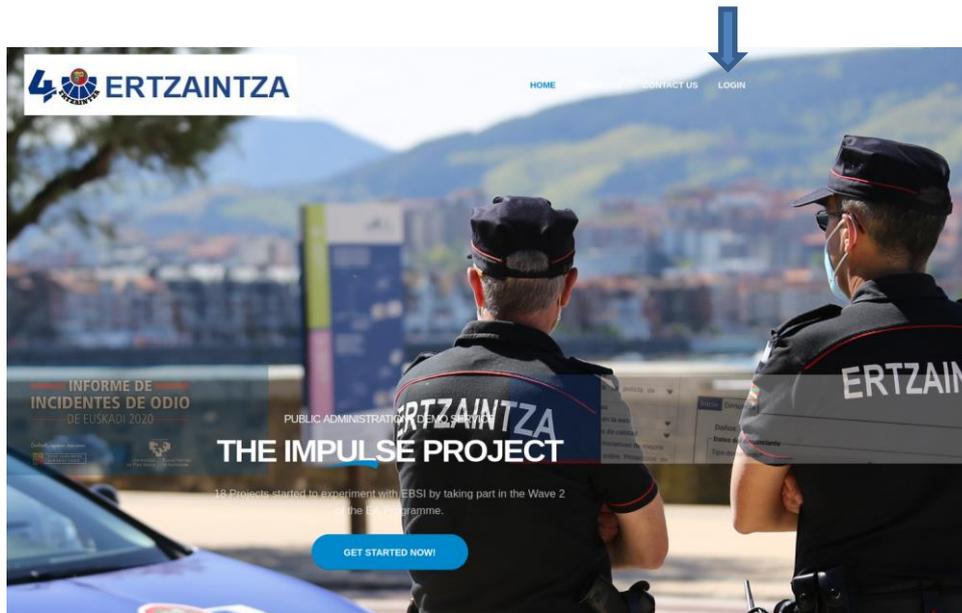
**Figure 12. IMPULSE IMPORTANT INFO message**

When the user clicks on the notification the user app will perform the final onboarding steps. When the steps complete, the user gets registered in the IMPULSE application. By pressing the OK button that appears in Figure 13, the app takes the user to the main screen, where the user can login to the IMPULSE app and start to perform operations.



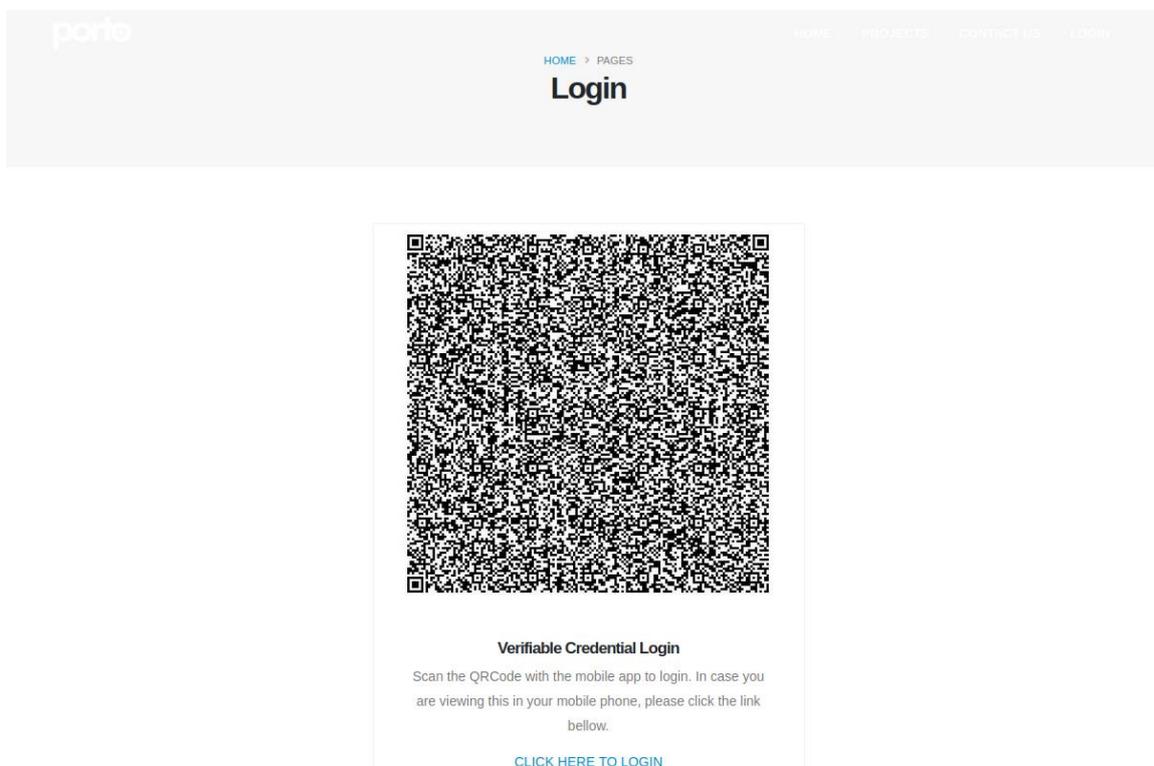
**Figure 13. Completed user registration**

Once the user has registered, they can enter public administration service in their web browsers, and click in the login option, as seen in Figure 14.



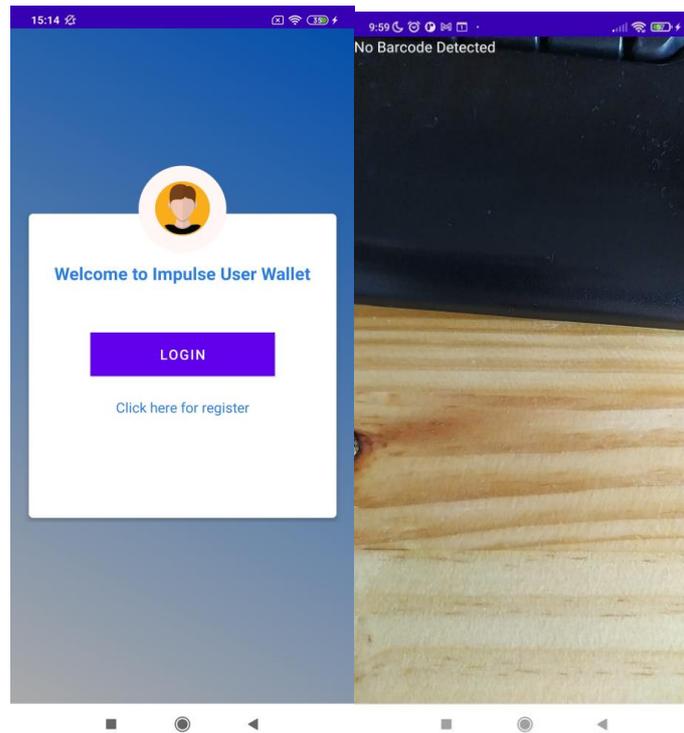
**Figure 14. Public administration web**

After trying to login, the public administration portal will show a QR code or a deep link to the user, as seen in Figure 15.



**Figure 15. QR code**

The user will either click login in the android application (image on the left in Figure 16) and scan the QR (image on the right in Figure 16) showed in the web browser, or click in the displayed deep link if the page is being seen in the device browser.



**Figure 16. Login in Impulse User Wallet**

Once last step is completed, the user chooses a credential from the list of available identity verifiable credentials, as seen in Figure 17.



**Figure 17. Choose credential for Login**

In order to use the identity verifiable credential, the user must unblock it using the biometric module. To do so, the application asks the user to take a selfie, as seen in Figure 18.

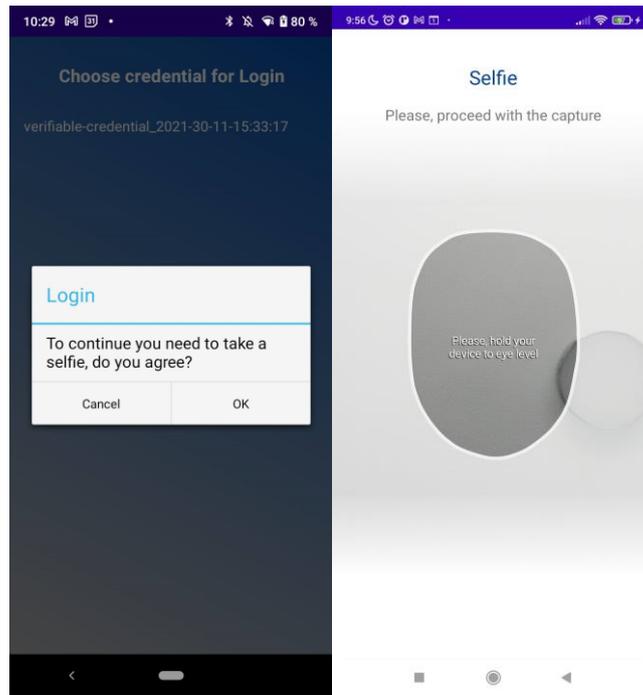


Figure 18. Take a selfie for Login

When unblocked, the application shows the data of the selected credential. After confirming the identity verifiable credential to use when the verification process ends, the application will return to the main screen showing the message: “Verification successfully completed”, as seen in Figure 19.

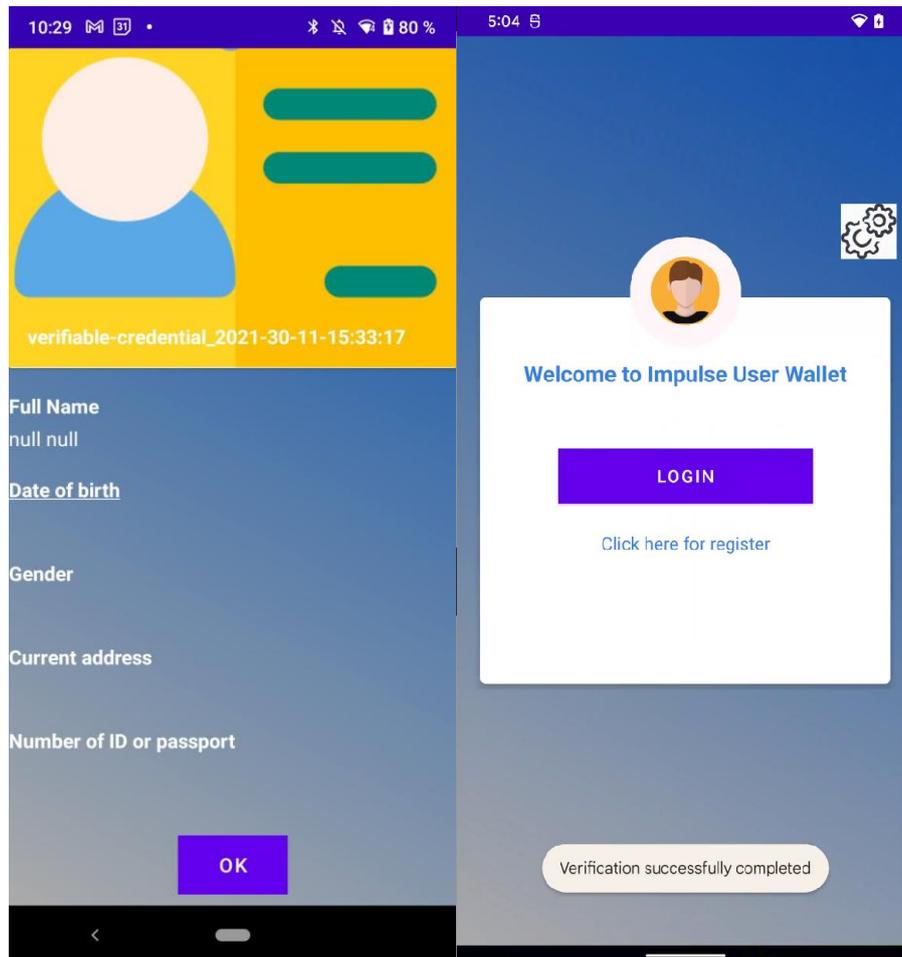


Figure 19. Data of the selected credential

After the end of the verification process, the web browser will get refreshed into the service page (form), filling some fields with the user information presented in the verifiable credential, as seen in Figure 20.

DAMAGE

DETAILS OF THE PERSON FILING THE COMPLAINT

**VERIFIABLE CREDENTIAL**

Did Key

did:ebssi:zdRjvnXDfwzVJe7SXgSW6C

▼

**PERSONAL DATA**

Name	First Surname	Second Surname
ifkdnlk	xifnlfk	fkenlfn
Mother's Name	Father's Name	Date of Birth
		1 feb. 2022
Gender	Mobile	Email Address
Male		

▼

**ADDRESS DETAILS**

Country	Town
Address	N°
xkemlklk	

▼

**Figure 20. Public administration form**

## 4 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.

The Android Accessibility Scanner is a feature that is not present in the first round of the IMPULSE project, but it has been studied to be implemented in the second version.

- **Android Accessibility Scanner** [4] will be used in the application in order to further improve the accessibility of all type of users. This tool offers utilities for accessibility and include the following features divided in 4 sections<sup>1</sup> :
  - Text and image contrast: Accessibility Scanner suggests improvements to colour contrast ratios to make your app more accessible to visually impaired users.
  - Implementation: Accessibility Scanner examines “View” Android hierarchies and identifies instances where users with motor impairments might have difficulty interacting with a layout.
    - Clickable links: Identify uses of Clickable Span that are not Url Spans.
    - Duplicate clickable Views: Identify clickable Views that share the same on-screen location as other clickable Views.
    - Editable item label: Identify Edit Texts and editable Text Views that have a non-empty content Description. Learn more about editable View labels.
    - Unsupported item type: Identify item types that are not supported by accessibility services.
    - Traversal order: Identify possible issues in the traversal ordering of items, which might affect users of screen readers or other accessibility services.
  - Touch target size: Accessibility Scanner looks for small touch targets that could cause difficulty for users with motor impairments.
  - Content Labelling: Many user interface controls depend on visual cues to indicate their meaning and use. A user with impaired vision might have difficulty seeing these cues.

You can make user interface controls more accessible with content labels. Content labels do not appear on the screen, but users with visual impairments can access them through accessibility services like TalkBack or other screen readers.

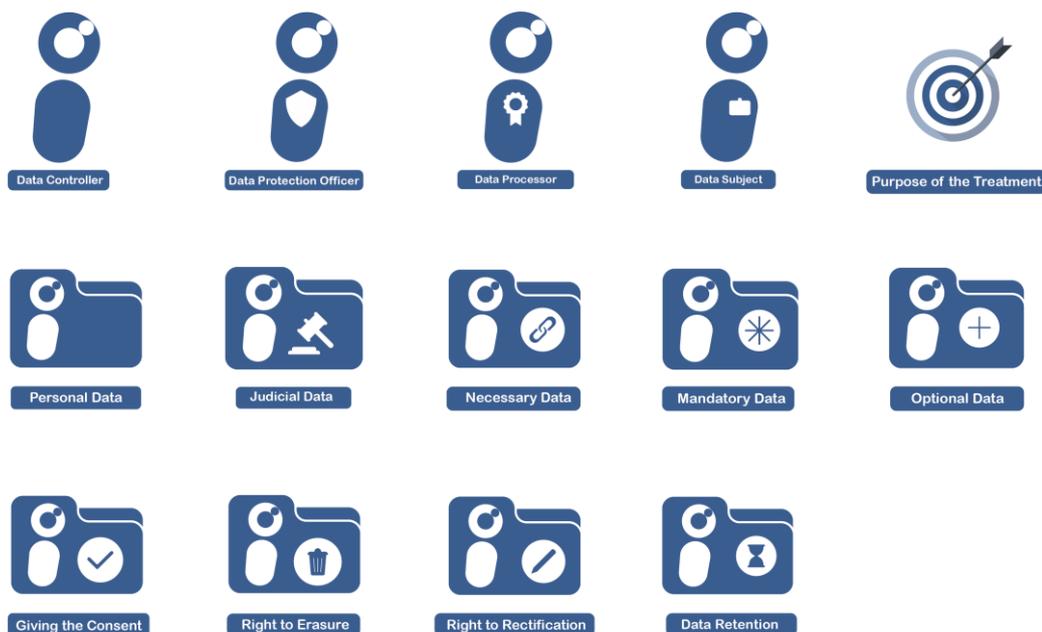
---

<sup>1</sup> Accessibility Scanner:

[https://support.google.com/accessibility/android/answer/6376559?hl=en&ref\\_topic=6376582#zippy=%2Clow-contrast%2ctouch-target-size%2Cimplementation](https://support.google.com/accessibility/android/answer/6376559?hl=en&ref_topic=6376582#zippy=%2Clow-contrast%2ctouch-target-size%2Cimplementation)

The informed consent icons are a feature that is not present in the first round of the IMPULSE project, but it has already been defined for it to be implemented in the second version.

- **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 21. Icons designed by CEL**

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), CEL 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.

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.

## 5 Conclusions

This deliverable describes the first version of the IMPULSE user app to be used by citizens, together with guideline report 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 register 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. 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 100Mb in disk and it consumes around 260Mb RAM in execution

The app currently supports 3 languages: English, Spanish and Galician. In the future it will also support the following languages: Italian, Bulgarian, Danish and Icelandic. The language displayed in the app is the one configured on the mobile device. The default language is English, which means that if the mobile configuration language is not supported, English will be the displayed language.

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 authentication process.

In terms of accessibility some considerations have been taken and some features have been already implemented in this regard, like the no need for passwords, the facial recognition to unlock the credentials, the Android Accessibility Scanner as well as the designing of graphical icons to facilitate the understanding about the consent rules for sharing personal information.

In the Annex A, a link to the video demo of the first version of IMPULSE wallet (V1) is available. It is worth noting that additional features have already been identified to be implemented during the second version of the IMPULSE wallet (V2) during the second round of the IMPULSE project.

## References

- [1] **[European Commission, 2019]** European Self-Sovereign Identity Framework, <https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=379913698>.
- [2] **[WaltId, 2021]** Decentralized identity, credentials & wallets, <https://walt.id/>.
- [3] **[Android 8.0, 2017]** Android 8.0 Oreo, <https://www.android.com/versions/oreo-8-0/>.
- [4] **[Accessibility Scanner]** Accessibility Scanner in Android, [https://support.google.com/accessibility/android/faq/6376582?hl=en&visit\\_id=637862245064926873-4111578236&rd=1](https://support.google.com/accessibility/android/faq/6376582?hl=en&visit_id=637862245064926873-4111578236&rd=1).
- [5] **[European Commission, 2021]** EBSI v2 Architecture, <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Architecture>.

## **Annex A First version of the IMPULSE citizen wallet (v1)**

The video demo for the first version of the IMPULSE eID solution is accessible through the following link:

<https://www.impulse-h2020.eu/2022/03/02/first-demo-of-the-impulse-eid-solution/>