# D4.3
# Development of demonstrators for the scenarios 1

Document Due Date: M15 (30.11.2020)
Document Submission Date: M15 (27.11.2020)

## **Work Package 4:** Platform Setup

Document Dissemination Level:

Public

**D4FLY** - **D**etecting **D**ocument frau**d** and i**D**entity on the fly
This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement No 833704

## Abstract

The D4FLY project will augment the current capabilities and capacities of border authorities in countering emerging threats in document and identity verification at manual and highly automated border control points and in the issuance process of genuine documents.
There were four main scenarios identified in the Grant Agreement, in which the researched technologies shall be integrated, tested and demonstrated. Hence prototype systems and demonstrators are developed for the described scenarios. Prototypes are being developed early in the project to be able to gather feedback from end users at early stages in the research and development. Improvements based on this feedback shall subsequently be incorporated into the prototypes resulting in the final demonstrators of the project.
The described prototypes are based on the platform as developed and defined in work package 4 and integrate the biometric technology components researched and developed in work package 5, the smartphone related technologies from work package 6, as well as the counter spoofing and presentation attack techniques from work package 7 and the document verification technologies from work package 8.
This document is the first deliverable of *Task 4.3- "Development of demonstrators for the scenarios"* of the *D4FLY Work Package 4 - "Platform setup"* and describes the developed prototypes for the scenarios. This deliverable is the first deliverable resulting from Task 4.3, with a due date of M15 (November 2020). Further two deliverables are planned to report the results of this task with due dates in the middle of the project (M21, May 2021) and towards the end of the project (M33, May 2022).

**Project Information**

| | |
|---|---|
| **Project Name** | Detecting Document fraud and iDentity on the fly |
| **Project Acronym** | D4FLY |
| **Project Coordinator** | Veridos GmbH |
| **Project Funded by** | European Commission |
| **Under the Programme** | Horizon 2020 Secure Societies |
| **Call** | H2020-SU-SEC-2018 |
| **Topic** | SU-BES02-2018-2019-2020 Technologies to enhance border and external security |
| **Funding Instrument** | Research and Innovation Action |
| **Grant Agreement No.** | 833704 |

**Document Information**

| | |
|---|---|
| **Document reference** | **D4.3** |
| **Document Title** | **D4.3 - Development of demonstrators for the scenarios 1** |
| **Work Package reference** | WP4 |
| **Delivery due date** | 30.11.2020 [M15] |
| **Actual submission date** | 27.11.2020 [M15] |
| **Dissemination Level** | Public |
| **Lead Partner** | VD |
| **Author(s)** | Armin Reuter, Susanne Kränkl, Jindrich Kodl, Damjan Gicic, Ananya Verma, Adriana Ezpeleta Gonzalez (VD) |
| **Reviewer(s)** | Henri Bouma (TNO)<br>Antonios Danelakis (NTNU)<br>Bartlomiej Markiewicz |

**Document Version History**

| Version | Date created | Beneficiary | Comments |
|---|---|---|---|
| 0.1 | 07.10.2020 | VD | Initial document structure |
| 0.2 | 05.11.2020 | VD | First draft, ready for first (internal) review |
| 0.3 | 11.11.2020 | VD | Second draft, after first review |
| 0.4 | 18.11.2020 | VD | Version after second review |
| 0.5 | 24.11.2020 | VD | Included edits after third review |
| 1.0 | 27.11.2020 | VD | Final edits, version ready for submission |
| | | | |

**List of Acronyms and Abbreviations**

| ACRONYM | EXPLANATION |
|---|---|
| ABC | Automated Border Control |
| BCP | Border Crossing Point |
| BG | Border Guard |
| BGA | Border Guard Application |
| D4FLY | Detecting Document frauD and iDentity on the fly |
| DPIA | Data Protection Impact Assessment |
| EC | European Commission |
| EDI | Enhanced Document Inspector |
| EU | European Union |
| GA | Grant Agreement |
| GDPR | General Data Protection Regulation |
| GUI | Graphical User Interface |
| IDE | Integrated Development Environment |
| IND | Dutch Immigration- and Naturalization Service |
| MRZ | Machine readable zone |
| NTNU | Norwegian University of Science and Technology |
| OS | Operating System |
| PAD | Presentation attack detection |
| RNM | Royal Netherlands Marechaussee |
| TNO | Netherlands Organization for Applied Scientific Research |
| TRI | Trilateral Research (Ethics partner in the project) |
| VD | Veridos GmbH |
| WP | Work package |

# Table of Contents

# 1 INTRODUCTION

## 1.1 Background

Within the D4FLY System new ways of enhanced document verification techniques and traveller verification methods are researched.

In order to test, further improve and finally demonstrate the D4FLY technologies in a relevant environment, prototypes and demonstrators are developed. Those prototypes and demonstrators are being adapted to the five scenarios, which are described in the GA. The six scenarios are summarized in Table 1.

**TABLE 1: SCENARIOS**

| | |
|---|---|
| Scenario 1a | Enhanced document verification focusing on travel documents |
| Scenario 1b | Enhanced document verification focusing on breeder documents |
| Scenario 2 | Highly automated border post with travellers arriving in waves. In the GA, there is a distinction made between a scenario 2a at a cruise ship terminal and a scenario 2b, at a train station. As the prototype that is used for both scenarios is identical, the description of prototypes is also not divided in two parts but summarized under scenario 2. |
| Scenario 3 | A border post at a land border with manual passport controls without automated biometric verification systems |
| Scenario 4 | A coach scenario where border guards must verify documents and identities without a fixed post in a crowded confined space |

Building on the experience of previous EU-funded projects on similar topics (like e.g. [PROTECT]) and taking into account the result of the user needs elicitation, the user stories, as well as the system requirements and the ongoing developments at various partners, in this task the various components are being integrated to functioning prototypes and demonstrators.

For this testing and improvement, an agile like approach has been chosen, where prototypes are developed, even when not all the research contributing to the various components of the prototype is finalized. The goal of this approach is to be able to gather user feedback early in the development process to adjust the forthgoing development, accordingly, thus improving the overall results. A modular approach was taken for the system in order to facilitate parallel development and flexibility.

The initial schedule for these field tests up to the time of writing this deliverable can be seen in Table 2.

**TABLE 2: INITIAL SCHEDULE OF D4FLY FIELD TESTS AND DEMONSTRATIONS**

| Location | Month(s) | |
|---|---|---|
| **Netherlands (Scenario 1a and 1b)** | Field Test 1<br>Field Test 2<br>Demonstration | M13-M14 (Sep./Oct. 2020)<br>M25-M26 (Sep./Oct. 2021)<br>M32-M33 (Apr./May. 2022) |
| **Greece (Scenario 2)** | Field Test 1 | M28-M30 (Dec. 2021-Jan. 2022) |
| **Lithuania (Scenario 3)** | Field Test 1 | M19-M20 (Mar./Apr. 2021) |
| **UK (Scenario 4 and 2)** | Field Test 1<br>Field Test 2<br>Demonstration | M13-M14 (Sep./Oct. 2020)<br>M24-M25 (Aug./Sep. 2021)<br>M35 (May 2022) |

The development of the first prototypes for scenario 1a and scenario 1b has been completed and have been successfully used in the first Field Test in Netherlands. The field test for scenario 2 (corridor scenario) and scenario 3 (land border scenario) are planned to take place only after writing this deliverable, so in section 4 and in section 5 those prototypes for these scenarios are described reflecting the status they had at the time of writing this deliverable. Due to the impact of the Covid-19 pandemic the first field test for the Scenario 4 (coach scenario) could not be executed at the time it was initially planned and it was re-planned to take place after the due date of this deliverable. Up until the decision to shift the field test, the platform and the modules for this scenario have been developed. This prototype is described in section 6 up to the state which the development has reached up to the time when this deliverable was written.

Other work packages have focused on defining the basis and foundation of the prototypes starting with gathering the user needs, converting them into system requirements (Tasks T2.1 and T2.2 in Work Package 2) and defining the technical basis for the prototypes by laying out the Graphical User Interface Guidelines and the System Architecture (T4.1, T4.2 in Work Package 4). Results of other work packages are integrated into the prototypes such as the biometric technologies (from work package 5), the smartphone related technologies (from work package 6), as well as the counter spoofing and presentation attack techniques from work package 8, and the document verification technologies from work package 8. Those results are described in the related deliverables of these tasks in more detail.

## 1.2 Aim of this document

In the GA the deliverable consists of the demonstrators themselves, however, this document aims to describe the demonstrators/prototypes for the scenarios at the time of writing this deliverable, including results or references to results from field tests, where applicable.

This document shall also touch upon how the requirements, mainly those coming from the end users, are implemented in demonstrators.

### 1.3 Input / Output to this document

As a starting point, mainly the results of the H2020 project PROTECT have been studied, the lessons learnt and experiences from this project have been the basis of the first concepts for the prototypes. Further main inputs were derived from the work of the other work packages as described already in section 1.1

Output is this document, describing the status of the prototypes and demonstrators at the time of writing this deliverable.

### 1.4 Outline of the document

In section 2, general aspects and commonalities of the prototypes are being described. The subsequent sections describe the prototypes on a per scenario basis, starting with section 3 on the Enhanced Document Verification until section 6 on the scenario 4. Indications to further development are given in each of the sections relating to the respective prototype for the scenario.

# 2 GENERAL

The general concept for the development of the prototypes and demonstrators in D4FLY follows an approach like an agile methodology. The general idea is to develop first prototypes for each of the scenarios relatively early in the project and execute field tests using these early prototypes. Main goal of these early tests is to collect feedback from end users early in the research and development, which is then used for successive refinement and guidance of the future development. The second field tests aim at showing improvements and implementation of additional features. During the final demonstrations, the prototypes shall be demonstrated in a relevant environment, aiming at TRL6. Further development and testing towards sellable products are not within the scope of this project.

Using this approach, it must be expected that the initial prototypes may have some limitations and may be missing some functionality. These limitations are accepted in favour of the opportunity to gather valuable feedback early in the project.

For the development of demonstrators, the description in the GA has been used as a starting point for the requirements and the design of the prototypes. Refinements have been done during various discussions with the partners and end users. The results of those discussions were analysed and consolidated and put into a structured form in task T2.2, resulting in a set of requirements for the demonstrators (see also [D4FLY-D2.2]). The requirements are structured into

- General requirements
- Requirements on subsystem level and
- Requirements on component level

Within this document the general requirements will be referred to in this section. An indication will be added to each requirement, relating to how the requirement was considered during development. Verification of whether a specific requirement is fulfilled, will be done using the method indicated in the requirement specification and is not reported in this document.

## 2.1 General requirements

The general requirements which have been considered during the prototype design are listed in Table 2. Requirements which are marked as “Post D4FLY” in the requirements document [D4FLY-D2.2] are marked in orange in the table, as they were acknowledged but not turned into specific design decisions or action for the prototypes and demonstrators during the project. These requirements have been considered in a way, that the subsystems can be extended to fulfil these requirements.

The requirements are listed with their ID and short title, as specified in [D4FLY-D2.2]. The full description of the requirements can be found in deliverable D2.2. A column has been added to indicated, whether the requirement could already be implemented or fulfilled, or how the requirement will be evaluated. A conclusion and evaluation of each requirement will be given after their final assessment towards the end of the project in the final deliverable.

To visualize the respective requirement status, a colour code has been used for the comment column. Light orange means “Requirement considered, but not evaluated, yet”, green background means “Requirement fulfilled”, orange background means “Post-D4FLY”-Requirement

**TABLE 3: GENERAL REQUIREMENTS**

| Applicable general requirements from the system requirement (D2.2) | | | |
|---|---|---|---|
| **ID** | **Title** | **Requirement** | **Comment** |
| **Ease of Use requirements** | | | |
| G.11A.001 | Border guard use | Each of the D4FLY subsystems, as described in Section 4.2, shall be capable of being used by an officer that has received basic level training for border guarding (i.e. first-line officer or document expert). | To be evaluated in field test |
| G.11A.002 | Clear UI layout and menu structure | All User Interface (console) screens shall be designed with a simple layout and (menu) structure, making it easy for the user to easily get an overview of the content, view details efficiently (e.g. scroll, detail view, etc), and operate the subsystem intuitively (e.g. intuitive buttons with descriptive text for any action that can be performed). | See also D4.1 (including ease of use and clarity as a basic concept for UI design) |
| G.11A.003 | UI Efficiency | The UI shall be efficient, such that all information can be reached with as little human actions (e.g. mouse clicks) as possible. | See also 4.1. To be evaluated in field tests |
| G.11A.004 | Traveller acceptance | Each D4FLY subsystem shall not reduce traveller acceptance of the control measures involving the subsystem, in comparison to the control measures currently in use (i.e. the equivalent functionality provided by other systems/processes). | Post D4FLY |
| **Personalisation and Internationalisation requirements** | | | |
| G.11B.001 | Language | Each of the D4FLY subsystems, as described in Section 4.2 (in [D4FLY-D2.2] , shall have all user-communication (e.g. user manuals, labelling, audio/visual instructions, console displays) in at least the English language. | English is default, multi-language for traveller apps |
| **Precision or accuracy requirements** | | | |
| G.12C.001 | Biometric performance | The performance of the biometric systems (i.e. sensors and algorithms) used in the D4FLY solution shall exceed the performance of the average biometric systems currently in use at border crossings. | Post D4FLY |
| **Reliability and Availability requirements** | | | |
| G.12D.001 | Reliability | Each of the D4FLY subsystems shall be capable of providing all its functions, as described in Section 4.2, at least at one field test/demonstration, and for the duration of this testing/demonstrations at the BCPs taking part in the D4FLY project. | To be verified in field test |
| **Robustness or Fault Tolerance requirements** | | | |
| G.12E.001 | Human intervention | In each D4FLY subsystem the final decision on lack of authenticity, falsifications and forgeries in documents must always be made/confirmed by a human. | To be evaluated in field tests |
| G12E.002 | Software robustness | All D4FLY components which interact with travellers, border guards or front-office staff shall comply with the software robustness standards Protobuf and ZeroMQ. | Post D4FLY |
| G12E.003 | Hinder or weaken border security | No D4FLY subsystem or component shall weaken or cause hinder to the current border check security measures in any way. | To be evaluated in field tests |
| **Capacity requirements** | | | |
| G.12F.001 | Network load | | To be verified |

| | | |
|---|---|---|
| No network communication between any two components of the D4FLY subsystem, using network infrastructure managed by the border authority, shall require a data transfer rate above 1 Gbit/sec. | | |
| G.12F.002 | Human resources | |
| No subsystem of the D4FLY solution shall require more border authority staff than currently required to fulfil the same amount of work in the current situation (i.e. processing the same number of passengers with the same thoroughness). | | To be verified |
| **Interfacing with Adjacent Systems requirements** | | |
| G.13C.001 | Interfacing with other EU border control systems | Post D4FLY |
| The D4FLY solution shall be capable of accepting, processing and fully integrating information from other EU border control systems into all verification processes within the D4FLY solution.<br><br>The D4FLY solution shall be able to at least provide results of all verification processes within the D4FLY solution for use by other EU border control systems (e.g. by providing a documented API). | | |
| **Privacy requirements (monitored by TRI)** | | |
| G.15C.001 | Privacy during design | To be evaluated (see also DPIA) |
| Each of the D4FLY subsystems shall be built to comply with the regulations regarding privacy as mentioned in [[D4FLY-D3.1]. | | |
| G.15C.002 | Privacy during operation | To be evaluated (see also DPIA) |
| Each of the D4FLY subsystems shall be operated to comply with the regulations regarding privacy as mentioned in Chapter 5 of the Privacy and Data Protection Impact Assessment [D4FLY-D3.2]. This includes all phases of use of the subsystems, from testing to decommissioning the subsystem. | | |
| G.15C.004 | Data storage | To be evaluated (see also DPIA) |
| D4FLY User Interface components shall not retain information regarding a traveller or the traveller's documents longer than the duration of processing of that traveller. | | |
| G.15C.005 | Retention of traveller data | To be evaluated (see also DPIA) |
| All components of the D4FLY solution, including any components not mentioned in this requirements specification, shall ensure that captured traveller data shall only be accessible to the authorized D4FLY end-users (border guards). | | |
| G.15C.006 | Accessibility of traveller data | To be evaluated (see also DPIA) |
| All components of the D4FLY solution, including any components not mentioned in this requirements specification, shall ensure that the captured traveller data shall not be retained longer than needed to process the traveller while the traveller crosses the border, unless anonymized for training purposes. | | |
| G.15C.007 | Data pseudonymisation | To be evaluated (see also DPIA) |
| The captured data of the travellers shall be identified within the component systems using an ID expression which is as unrelated as possible to the identity of the traveller and it should be practically impossible to later restore this relationship by any means. | | |
| **Legal Compliance requirements** | | |
| G.17A.001 | GDPR compliancy | To be evaluated (see also DPIA) |
| The D4FLY solution, subsystems and components shall comply with the EU Regulation (EU) 2016/679 (General Data Protection Regulation). | | |
| G.17A.002 | consent | To be evaluated (see also DPIA) |
| The traveller shall be fully informed on the process and give his/her consent for his/her data to be captured. | | |

Besides the requirements gathered in work package 2, some specific boundary conditions have influenced the design of the system architecture and the prototypes:

- Components and platform had to be developed in parallel and by different partners.
- Partners are developing on different platforms (OS, IDEs, Programming languages)
- Some components are used in only one subsystem, some components are used in multiple subsystems
- Feasibility, results and performance of some components were unknown at the beginning of the project.

Besides choosing a modular approach, it was decided to define a communication protocol, which allows for great flexibility in choosing OS, language and hardware for each component during development and demonstrations. Post-D4FLY, if turned into products, the developer would probably choose to integrate all components on one platform using the same hardware for all modules or even modify the system architecture (or the communication interface) to achieve higher integration and performance levels.

The GUIs have been designed following the principles outlined in deliverable D4.1.

# 3 SCENARIO 1: ENHANCED DOCUMENT VERIFICATION

## 3.1 Overview

Scenario 1 overall is focused on document verification. It has been split into two parts in the GA with a different focus:

**Scenario 1a** relates to travel documents and here mainly passports are considered. The majority of the techniques, which are researched and developed in this scenario are targeted at a first line document inspection process at a border post, where a fast turnaround time to get a first result of the checks of a document is of highest importance. Some of the developed technologies in this scenario can also be used in a second line checking process of passports, where there is usually more time for the checking process, a more detailed investigation can be done and more time can be spent for manual interaction with the tool.

**Scenario 1b** relates to breeder documents, where the documents are largely not standardized and can be anything from a birth certificate on a piece of paper to other official forms, which all may include elements like stamps and signatures. Typically those documents are thoroughly checked in a second or even third line (document expert) check where more time is available, as this type of check is typically not done at a border post but in a document expert centre, e.g. related to the analysis of documents from asylum seekers.

For Scenario 1b the main end user during the project phase is the document expert team of the Immigration and Naturalization Services in the Netherlands (IND). Due to the specific nature of the application and use cases and also due to the specific requirements and boundary conditions around the breeder documents, there was no platform developed for the prototype for this scenario by VD, the development was done by TNO in this case, also using a dedicated user interface.

A more detailed description of the prototype for scenario 1b can be found in the related deliverables of work package 8 (D8.1, D8.3, D8.4, D8.8, D8.10 and D8.11).

The following descriptions therefore mainly relate to the documentation verification platform for scenario 1a.

## 3.1 Relation to other work packages and deliverables

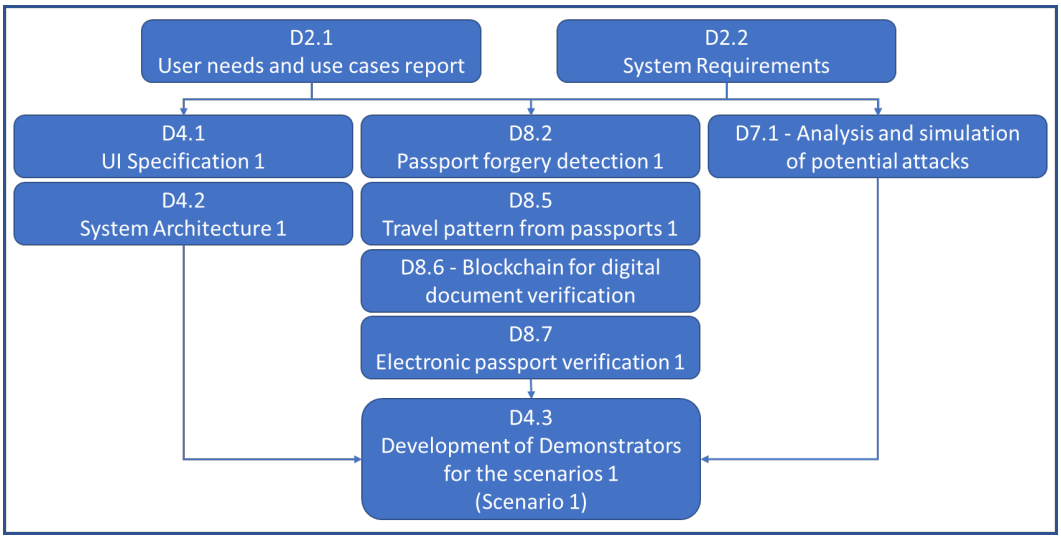


**FIGURE 1: RELATION OF D4.3 (SCENARIO 1B) WITH OTHER DELIVERABLES AND WORK PACKAGES**

In the D4FLY work package 2, the user needs and use cases have been described in Deliverable D2.1 [D4FLY-D2.1], and have been elicited in workshops interviews and discussions. Those have been turned into a set of system requirements in Deliverable D2.2 [D4FLY-D2.2]. A first UI specification and a first system architecture specification have been described in Deliverables D4.1 and D4.2, which served as the basis and specification for the implementation of the prototypes and demonstrators. Most checker components have been developed in work package 8, in the respective tasks with the first results being described in the Deliverables D8.2, D8.5, D8.6 and D8.7 as shown in Figure 1. In work package 7, the research on morphed face detection was done, which led to the checker component for the morphed face detection as described in D7.1 and later D7.2. All software components developed in the tasks relating to the above-mentioned deliverables were used and integrated to the platform, which is described in this deliverable (D4.3).

## 3.2 Prototype implementation (current status)

Following the system architecture as described in deliverable D4.2-“System Architecture 1”, the subsystem is built up as shown in Figure 2 and the components are connected via the communication interfaces using ProtoBuf and ZeroMQ, as also described in the System Architecture.

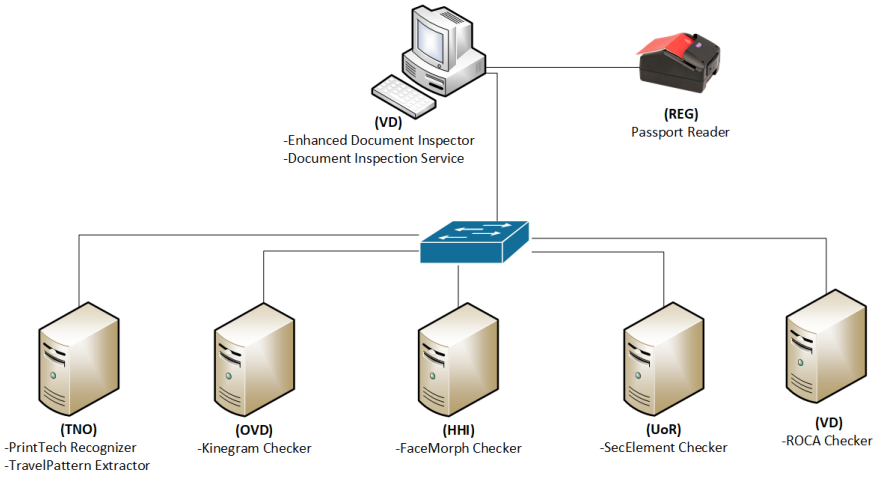


**FIGURE 2: DOCUMENT VERIFICATION SUBSYSTEM HIGH LEVEL OVERVIEW**

### 3.2.1 Hardware

The core module (called "Enhanced Document Inspector" (EDI) in Figure 2) is connected to the Passport Reader. In this case a model 7024M.111 from partner Regula has been used as a passport reader. The central EDI module also controls the GUI, which is displayed on a standard desktop monitor and is connected to the EDI component.

In order to facilitate parallel development of the prototype components, the communication interface has been defined in the system architecture, such that every partner can use his preferred operating system and programming environment during the development. For the prototype the checker software component has been running on a dedicated separate computer, provided by each partner, satisfying the needs of the respective component. For example, the ROCA checker is not very compute intensive and has been optimized for embedded computing, which could be run on a Raspberry Pi computer. Other checker components are more compute intensive, especially if heavy image processing is required. In these cases, a PC with a strong GPU and CPU has been used. The communication in principle can be done either using a local network connection or a dedicated VPN connection over the internet.

Figure 3 shows an image of the prototype setup in use, as it has been installed in the Field Test in the Netherlands (Oct 2020). In that case, the desktop monitor, keyboard and mouse have been set up in the office of the Royal Netherlands Marechaussee (RNM) document experts in Ter Apel, as well as the PCs for the core component and the ROCA checker. All other components have been connected using a VPN internet connection.

**FIGURE 3: DOCUMENT VERIFICATION SETUP PLATFORM IN THE FIELD TEST IN NETHERLANDS (OCT 2020)**

### 3.2.2 Software

The standard high-level flow using this prototype from a user perspective is as follows:

1) The user starts the EDI GUI and connects the passport reader and all checker components.
    - EDI software establishes the connections and a status indication is displayed in the GUI
2) The user puts an opened passport (holder page facing down) on the passport reader.
    - Automatic scanning of the passport data page is started, capturing four images in visual (white light), visual (coaxial white light) illumination, infrared light and ultraviolet illumination respectively.
    - The scanned image (visual light) is displayed in the GUI.
    - Automatic read out of the electronic information of the passport is started in parallel.
    - The captured information is packaged in data structures and is distributed via the communication interface to the checker components using ProtoBuf and ZeroMQ messages.
    - The checker components receive the information and start analysing the data
    - After completion of the processing the checker components send the result back to the EDI core component.
    - As the results become available, they are displayed in a simple results bar in the main GUI.
3) [Optional] If the user requires more detailed information on the result or some manual interaction is required, the user can click on the detail tabs in the main GUI, where additional information and/or additional images are displayed for further review.
4) The user either continues with scanning also the visa pages, which contain entry/exit stamps to perform travel pattern analysis
   or
   continues with scanning the next passport, which he wants to inspect.

The main screen of the GUI is shown in Figure 4.

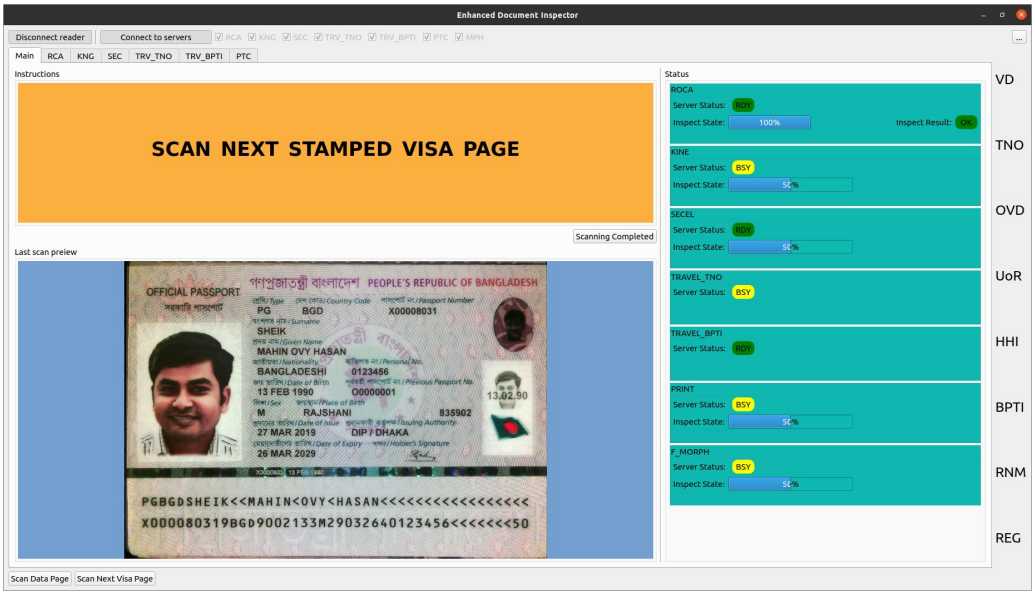


**FIGURE 4: MAIN SCREEN OF EDI GUI (SHOWING SPECIMEN PASSPORT WITH ARTIFICIAL DATA)**

In order to initialize the system, the user must connect the reader, select the available components by clicking on the selector boxes at the top of the screen and click “connect to servers”. In the further development, this mechanism shall be replaced by an automatic setup routine, such that these buttons can be removed from the GUI.

The main screen is split into the instruction field, the scanned image preview pane and the status and results panes at the right of the screen.

On the main screen, there are no further buttons, as the GUI is optimized for a fast checking process requiring no further user interaction in the standard use case. The user is supposed to only put the passport on the reader, the system then does the scans automatically, as well as the checks and the displaying of results.

A block level functional diagram showing the software architecture is shown in Figure 5.

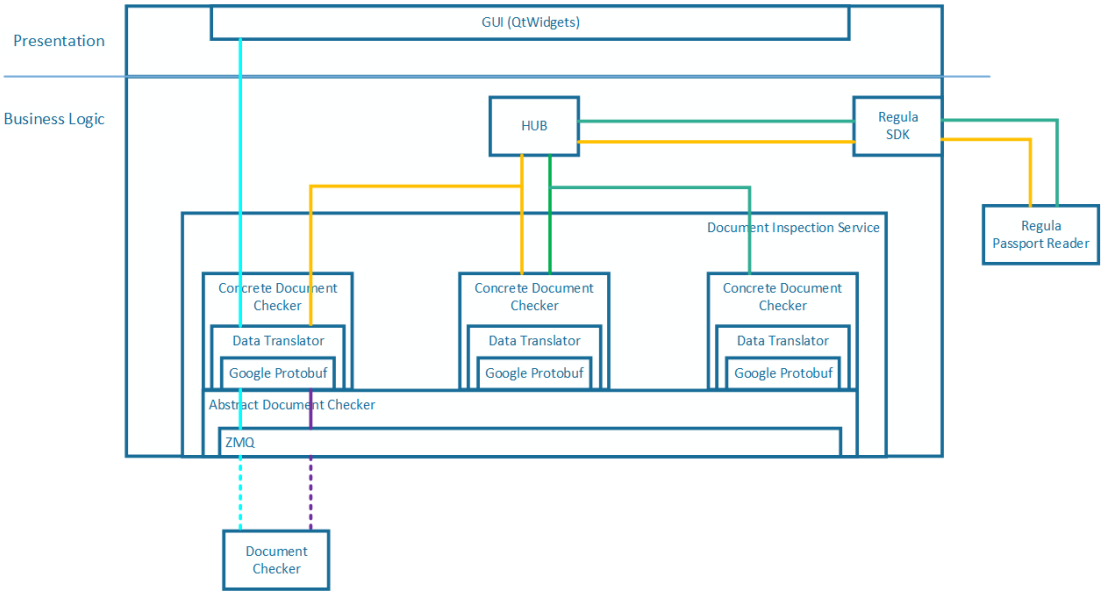


**FIGURE 5: SOFTWARE STRUCTURE OVERVIEW**

Detailed descriptions of each of the checker components can be reviewed in the related deliverables of work package WP08: D8.2, D8.5, D8.6, D8.7 and WP07: D7.1 and following.

## 3.3 Prototype testing the document verification platform

### 3.3.1 Integration testing

Each partner was responsible for unit testing of the respective component during the initial development. For the "EDI" core component, unit testing has also been performed, focussing on the communication and sequencing the interaction with the components, if needed, by developing a dummy version ("mock up") of each checker component, for which mainly only the communication interface had been implemented.

An integration test was planned for this project phase in order to test the full prototype system. As travel has been strictly restricted by governments and companies due to the Covid-19 pandemic, physical meetings for integration testing have not been possible. Instead, remote integration testing has been performed, where all partners who provided components for the system have been connected to the "EDI"core component via a secure VPN connection.

The remote integration test took place from July 20th, 2020 until July 24th, 2020. Starting with the setup and bilateral testing with each single partner, the remote testing concluded with a full integration testing, where all partner checker components were connected. The schedule of the remote testing is shown in Figure 6

| Date | 20.07.2023 | 21.07.2023 | | 22.07.2023 | | 23.07.2020 | | 24.07.2020 |
|---|---|---|---|---|---|---|---|---|
| Component (partner) | SecElement Checker (UoR) | TravelPattern Extractor (TNO) | TravelPattern Extractor (BPTI) | Kinegram Checker (OVD) | PrintTech Recognizer (TNO) | ROCA Checker (VD) | FaceMorph Checker (HHI) | all components |
| 09:00 | | | | | | | | |
| 10:00 | 9AM UK time | | | | | | | |
| 11:00 | | | | | | | | |
| 12:00 | | | | | | | | |
| 13:00 | | | | | | | | |
| 14:00 | | | | | | | | |
| 15:00 | | | | | | | | |
| 16:00 | | | | | | | | |
| 17:00 | | | | | | | | |
| 18:00 | | | | | | | | |
| 19:00 | | | | | | | | |
| 20:00 | | | | | | | | |

Legend:
testing
bug fixing
reserved
lunch
free

**FIGURE 6: SCHEDULE OF REMOTE INTEGRATION TEST**

After the remote integration testing and a phase of bug fixing and improvements, the system has been used in the field test in the Netherlands.

### 3.3.2 Field testing

There are in total six events planned in the Netherlands, four field test events and two final demonstrations, where two field tests and one demonstration are foreseen for each of the scenarios 1a (Travel documents) and 1b (Breeder documents) respectively.

The first field test for scenario 1a, focusing on travel documents, has been executed in the week starting September 29th, 2020, the first field test for scenario 1b, focusing on breeder documents, was performed on 14th and 15th September, 2020, so these field tests have been

completed before finalizing this document. A functional prototype system, integrating contributions from WP5-WP8, and configured ready for the field test have been provided.

Further field tests are planned for September 2021 and final demonstrations in April 2022.

Field testing of the document verification platform was executed using a remote connection for most of the components, as most partners could not attend physically due to the travel restrictions imposed by the Covid-19 pandemic. The platform was working very stable and without crashing. The overall prototype, the platform and the GUI received overall positive feedback with important recommendations on desired improvements for the further development.

The field test for scenario 1a used a prototype of a platform system integrating one module from WP7 and six modules from WP8. The field test for scenario 1b used four modules from WP8. Details of how the testing was set up for the first Field Test in Netherlands and the resulting feedback of the end users can be reviewed in the deliverable D9.3 – "Field Test Netherlands 1" (which is classified as EU Restricted).

### 3.4 Further development

The following main improvements and extensions shall be done to the platform and the platform GUI during the further development up until the second Field Test in Netherlands planned for September 2021:

- Integration improved versions of the different checker components and the respective extension of the GUI
- Integration of the blockchain component, which has been developed and tested as a standalone application up to the field test in Netherlands.
- Improvements to the GUI to further optimize the presented information, as well as the manual interaction procedures, which are required while performing some of the more detailed analysis steps.

More improvements may be discussed in further meetings and workshops during the project.

# 4 SCENARIO 2: HIGHLY AUTOMATED BORDER

## 4.1 Overview

In Scenario 2 the focus is on border crossing situations with a high number of travellers arriving in waves. To avoid delays and long queues at the border posts for border controls at the actual border crossing, the traveller data is enrolled before his/her arrival at the border. This enrolment could also be performed before the actual travel starts. The approach for this scenario is to develop a prototype, which supports a pre-enrolment for travellers at an enrolment kiosk. The travel document of the traveller is captured and checked, as well as biometric information that is captured using various biometric sensors. The captured data is stored in the system, partially in a database, partially on the traveller's smartphone. Located at the travel destination, a biometric verification area (a biometric corridor) is set up. When the traveller approaches this corridor, his pre-enrolled reference data is loaded in the corridor system, triggered by the traveller, who presents his smartphone at the corridor entrance by tapping it to an NFC reader. As the traveller walks through the biometric corridor, various biometric sensors will capture biometric data from the traveller, verify each biometric modality against the pre-enrolled reference data, fuse the single results into an overall score value and finally present the verification result to the border guard for her/him to decide, whether the traveller can continue or needs to be taken to additional investigations. The

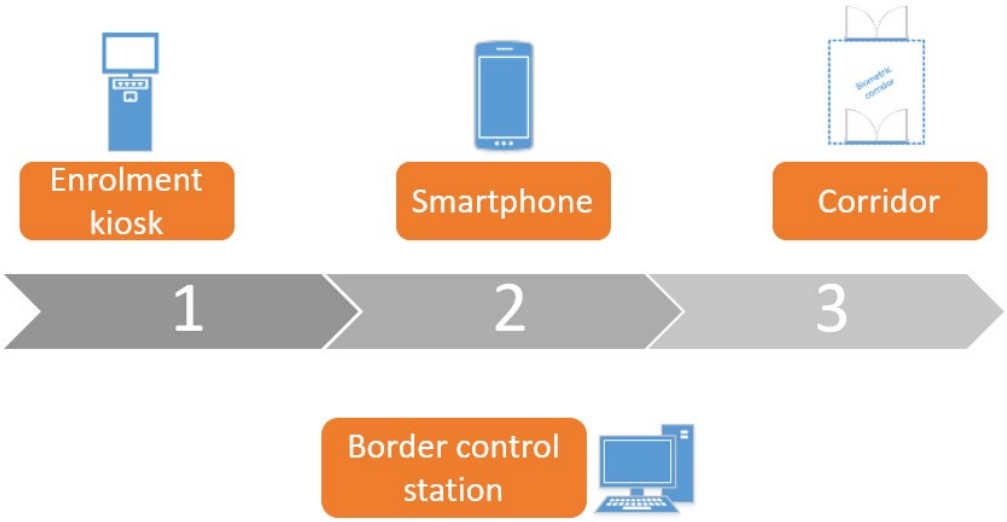


**FIGURE 7: HIGH LEVEL PROCESS OF PROTOTYPE FOR SCENARIO 2**

biometric corridor allows for a border crossing process without the traveller having to touch anything during the whole process. An overview of the process is visualized in Figure 7.

As the initial schedule and planning as described in the GA had foreseen a first field test only after the due date for this deliverable and thus the development and implementation of the prototype is still ongoing, this deliverable describes the current intermediate stage, with mostly the concepts and plans and intermediate results, as they were available at the time of writing this deliverable.

## 4.2 Relation to other work packages and deliverables

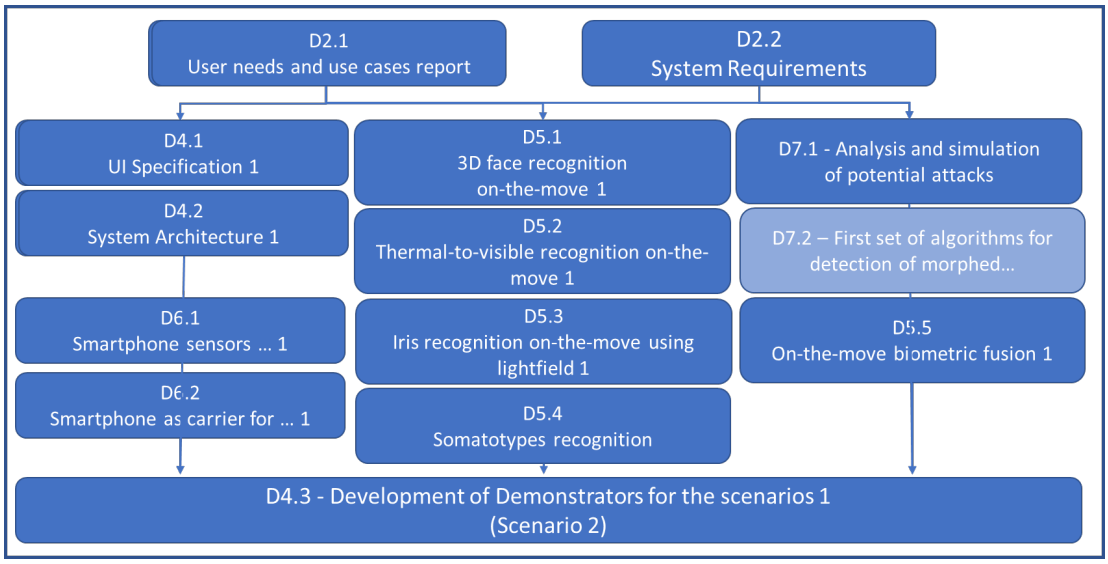


**FIGURE 8: RELATION OF D4.3 (SCENARIO 2) WITH OTHER DELIVERABLES AND WORK PACKAGES**

Similar to scenario 1, the foundation of the research and development has been laid out in the D4FLY work package 2, where the user needs and use cases have been described in deliverable D2.1 [D4FLY-D2.1], and the system requirements in deliverable D2.2 [D4FLY-D2.2]. A first UI specification for all software including the smartphone apps and a first system architecture specification have been described in Deliverables D4.1 and D4.2. The biometric modalities that have been used were researched in work package 5 and described in the deliverables shown in Figure 8. Contributions came also from work package 6 related to the smartphones used as additional sensors and as carrier for the identity data. Also included in the enrolment kiosk as well as the biometric corridor are presentation attack technologies that have been researched in work package 7 and are described in the related deliverables.

## 4.3 Prototype implementation (current status)

An enrolment kiosk is relevant not only in scenario 2, as described in this section, but also in scenario 4 (“coach scenario”, described in section 6). As the enrolment steps and the sensors needed for scenario 2 are a superset of what is needed in scenario 4, only one prototype kiosk will be developed during the project. The kiosk is designed such that it can be used for both scenarios. Although optimizations could be made for the design of the kiosk for scenario 4, making it smaller and lighter, as less sensors are required, the option of saving effort and cost and the possibility to do more experimentation with a ‘universal’ kiosk was seen as advantageous in the project.

Therefore, the kiosk is described in more detail in this section for scenario 2 and only the differences in usage will be highlighted in section 6.

### 4.3.1 Enrolment Kiosk

The first major stage of the process that the traveller encounters is the enrolment kiosk. The kiosk’s purpose is to carry all the sensors and equipment needed for traveller’s enrolment within one compact space and to act as an instrument for capturing all data needed for a seamless border crossing in a later phase. There are three major functions imparted on the first kiosk prototype when the traveller interacts with it. These are:

- verification of traveller's identity,
- enrolment of the selected biometric modalities of each traveller, and
- detection of traveller's liveness.

The first prototype of the enrolment kiosk was developed to accommodate for size and operational needs by each of the instruments required for biometric enrolment and Presentation Attack Detection (PAD) as specified by every contributing partner.

#### *4.3.1.1 Hardware*

The hardware configuration incorporates requirements imposed on it from the perspective of the user needs, operational specifications of the utilised sensors as well as aspects stemming from general safety considerations during operation.

A drawing of the very first kiosk prototype and the initial planned placement of the sensors and other kiosk elements can be reviewed in Figure 9.

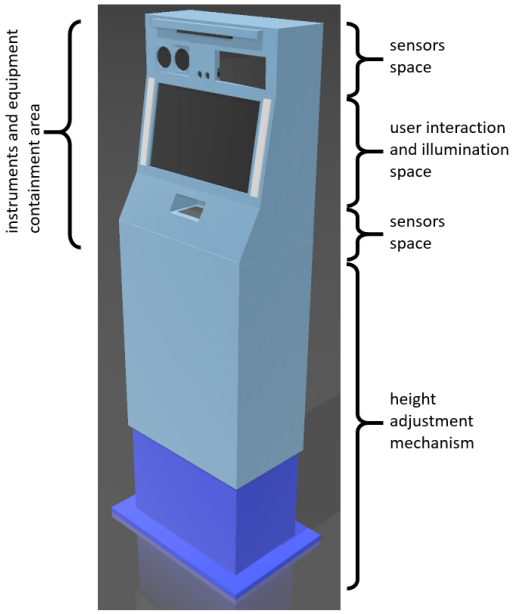


**FIGURE 9: INITIAL KIOSK CONCEPT**

The concept structures the kiosk into an upper part and a lower part of the kiosk, where the lower part of the kiosk contains the height adjustment and is designed to ensure no injuries to happen, by using a closed design, where nothing can be squeezed under the movable part of the kiosk (even if the height adjustment mechanism features an emergency stop). The upper part is structured into three main areas: The upper sensor space predominantly for image capturing sensors, the middle space with the touch screen and the illumination and the lower sensor space with openings as required for laying the passport or the smartphone onto a horizonal surface, as provided for the passport reader and the NFC reader, respectively.

Based on this initial design, as shown in Figure 9, the first prototype of the kiosk has been manufactured, after some modifications and adjustments. Images of the first manufactured prototype are shown in Figure 10. The images show the kiosk prototype on the manufacturing floor with no sensors or computers installed.

**FIGURE 10: KIOSK PROTOTYPE FRONT AND BACKSIDE VIEW**

Some of the notable features are listed in the following paragraphs:

*The kiosk is height adjustable.* The height adjustment serves to aid usability, where height is adjusted for comfortable manipulation according to the traveller's height. More importantly though, the height adjustment allows for correct positioning of all sensors to ensure reliable and accurate enrolment of biometric modalities. Currently, the height adjustment is done manually using up and down buttons at the kiosk. It is planned to automate the height adjustment at a later stage of the project.

*Equipment placement.* The placement of sensors and all required equipment for the first prototype was selected according to the enrolment sequence, the optimal distances required for capturing clear images and biometric data, and usability aspects. As this is the first prototype of the enrolment kiosk, it is expected that minor configuration adjustments are required related to the sensors and PAD systems (e.g. placement, model). To enable easy modifications, openings for sensors placements were cut out in the main kiosk panel, three above the monitor and three below the monitor (see Figure 10). Depending on the sensors used and their placement, the openings can be adapted to the specific needs using covering plates. Should an adjustment be needed, a new covering plate can be manufactured adapted to new requirements (placement, different sensor model needed, etc). Hence no complete overhaul of the kiosk is needed, only a modification of a cover plate. Compromises in the aesthetics of this prototype had to be accepted to realize the easy adaptability.

The area above the monitor houses the sensors required for verification and enrolment of biometric modalities in the head region, i.e. 2D, 3D and thermal face image capture, and iris enrolment. The sensor placement is such that it is as close as possible to the upper rim of the monitor. Also, the off-centre sensor areas are slightly horizontally tilted inwards, allowing the sensors to directly point towards the traveller's face. Both features shall improve usability and comfort as the traveller does not have to move his/her head extensively during enrolment. Additionally, the overall design of the kiosk promotes positioning of traveller's head within the 40-60 cm range, which is optimal for the accurate enrolment and verification of traveller's biometrics.

The vertical placement in separate cut-outs for passport and NFC readers in the lower part of the kiosk prevents passport or smartphone from falling to the ground during the enrolment process.

*Operational safety.* Occurrences of functional hazards and foreseeable operational disturbances were also considered during the prototype development. For example, the kiosk

was built from non-flammable material. It contains vents to prevent overheating. The height adjustment mechanism stops automatically if an obstacle is introduced in its movement.

Not all the biometric sensors could be placed within the confines of the kiosk. Due to the nature of traveller's somatotype enrolment, the necessary equipment for recording this modality must be placed outside of the kiosk, allowing for side capture of enrolling traveller from a longer distance since the somatotype biometric requires a full-body lateral image.

#### *4.3.1.2 Software*

The enrolment process is conducted through an application, which guides the traveller through all the phases, manages the interaction of the core kiosk with the attached sensors, and communicates the enrolment results to the off-site database. As such, the implemented software can be split into two areas; UI and frontend utilised for traveller-kiosk interaction, and backend managing the functionality and dataflow of sensor controllers as well as communication with the enrolment database. The system runs on Debian Linux distribution and is implemented in C/C++.

The current implementation of the UI reflects the fact that this is the first prototype of the enrolment kiosk. The UI offers only essential features with an elementary screen design realised using Qt Widgets. Additionally, the traveller is given greater control over the background processes when interacting with individual biometric sensors than necessary. For example, the traveller is required to initiate certain enrolment processes by pressing a "start" button, something that will be automatized in the future prototypes.

The background processes are designed in a modular way, with every module having a unique, standalone function. At the centre of the design stand two main core components, kiosk and Biometric Acquisition Service, which manage the remaining modules. Figure 11 highlights their roles and how they are used to tie all internal enrolment processes together. In a nutshell, the Biometric Acquisition Service component controls the communication with all the sensor controllers and PADs, and the kiosk component manages all the remaining processes. The detailed description of the architecture can be found in Deliverable D4.2 – System Architecture.

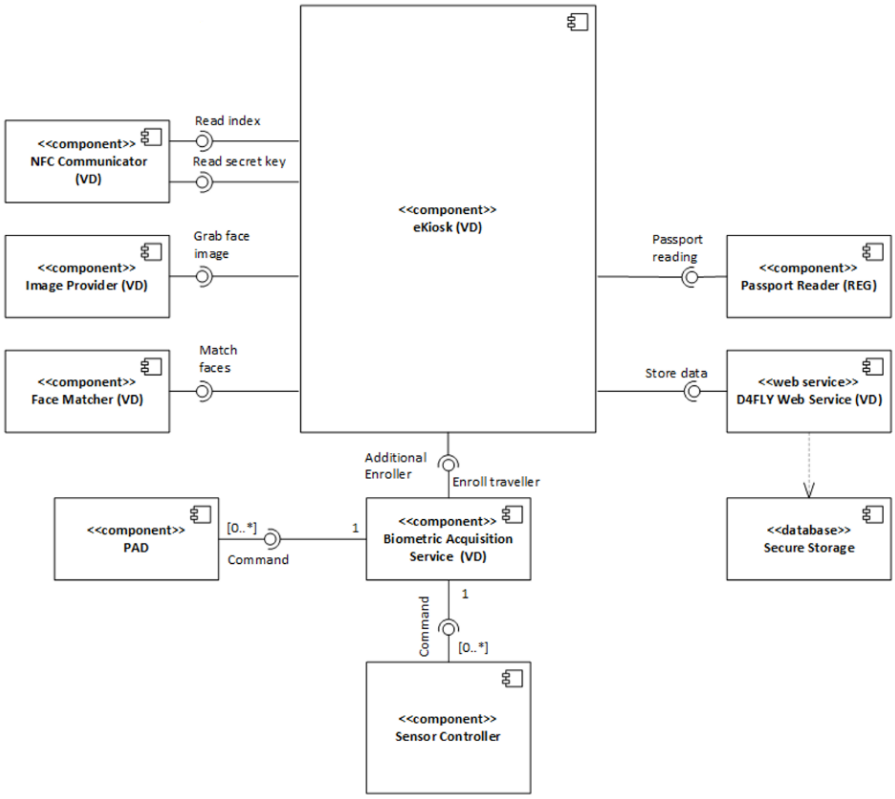


**FIGURE 11: STRUCTURE OF THE SOFTWARE COMPONENTS FOR THE ENROLMENT KIOSK**

### 4.3.2 Biometric Verification Corridor

The biometric verification corridor prototype is developed to allow the verification of the traveller´s identity using a combination of several biometric modalities, aiming at verifying the travellers as they walk through the corridor.

In Table 5 the used biometric modalities and the respective sensors, which will be used in the biometric corridor are listed:

| Biometric modality | Used sensor in the corridor |
|---|---|
| Thermal-to-visible | RGB camera: Basler ace acA2040-90uc |
| 3D Face | Raytrix camera |
| Iris | Raytrix camera |
| Somatotype | RGB camera: Amcrest IP2M-852EW ProHD Outdoor 1080P |

**TABLE 4: BIOMETRIC MODALITIES AND SENSORS USED IN THE BIOMETRIC CORRIDOR**

There are also some PAD technologies planned to be tested in the verification corridor (e.g. Iris PAD), however, as of the time of writing this deliverable, no additional sensor hardware is required for the PAD, the planned PAD functionality, can be realized in software only.

#### *4.3.2.1 Hardware*

In addition to the requirements collected within work package 2 (see also Figure 8), the technical requirements stemming from the usage of the various biometric sensors have been collected and discussed with all involved partners. These technical requirements like the width, length and height of the corridor, the required distances between the travellers and the capturing sensor, the placement and required orientation of the sensors and the type and placement of illumination have been considered.

Considering those requirements, an initial design of the biometric corridor with an initial placement of all the sensors (as listed in Table 5) has been done. Based on the specific requirements for the somatotype verification, which is to capture a full body image, the camera required for the somatotype capture was placed outside the corridor. Additionally, the first part of the corridor must be designed to be transparent, to enable to capture a good quality full body image. This specific arrangement will have to be considered for the space required for the prototype in the planned integration and field tests.

In addition to the partner specific requirements resulting from the used biometric sensor, the corridor itself shall also meet some general requirements:

1) The biometric corridor shall be stable.
   This means, the walls should have enough stability to not bend or fall easily.
2) All the components shall be fireproof, to be allowed to be set up inside buildings with standard requirements on the fire resistance of installed equipment (even if installations of the prototype would be only temporary).
3) The biometric corridor shall not have sharp edges,
   to avoid any injuries during operation.
4) The biometric corridor shall also be light and easy to mount and dismount and should be reasonably easy to transport.
5) None of the components used to construct the corridor, which shall be used in the field tests and demonstrations, shall fall under any export restrictions.

With these considerations a first design for the corridor was created, resulting in the following main features:

- The width of the corridor is 1m
  (to allow travellers with trolleys or other luggage to walk through)
- Have (automatic) a single gate at the entrance and a double gate at the exit, allowing to guide travellers to second line control if needed.
- The biometric corridor has a bend to ensure, travellers can investigate sensors in a straight line (where frontal biometrics must be captured)
  - In the bend there is space for all biometric sensors, illuminators and additional hardware needed to be placed.
- Provides good illumination zones at the distances required by the various sensors:
  - At 1.2m from the sensors for the thermal to visible capture
  - At 1.8m from the sensors for the 3D face capture

- At 1-1.8m for the iris capture

- 1m wide wall left transparent for the capturing of the image for somatotype

A 3D model image and a drawing of the prototype 1 corridor design with the sensor positions indicated can be seen in Figure 12.

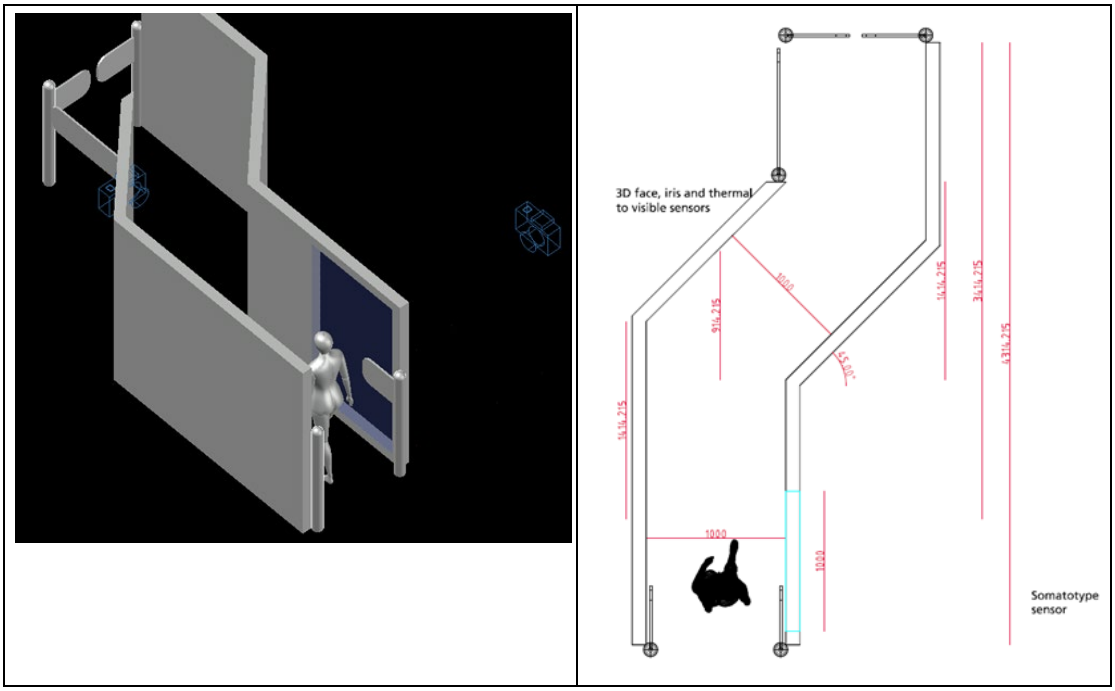


**FIGURE 12: 3D MODEL AND DRAWING OF THE CORRIDOR WITH SENSOR LOCATIONS INDICATED**

The main goal of this first prototype is to serve as a basis for further experimentation. The construction of this first prototype is currently ongoing at the time of writing this deliverable. The prototype will be constructed in a straightforward and modular way, such that required changes can be done easily and components can be modified, replaced or rearranged easily for optimizations. The current design foresees to construct this corridor using several "unit wall elements" of 1 or 2 metres high and 0.5 or 1 metre wide. These wall elements are made of a ground of white wood and two profiles at each side which would have a joining flat profile on top of them to join them.

#### *4.3.2.2 Software*

The software for the biometric corridor verification system follows the principles as described in the system architecture [D4FLY-D4.2]. A central component is developed, which controls the overall system and the sequence of events. It also communicates with the various sensor controllers using a component, which is called biometric acquisition service, where results are being received from the sensors via the sensor controllers. Each sensor controller is developed by the respective partner leading the research on the specific biometric modality. Interfaces are being implemented, which connect to a variety of supporting components, like the Person Tracker component, which tracks the traveller as he walks through the corridor to adjust sensors optimally (to be implemented for the second field test) or the Gate Controller Component, which controls the gate that is planned at the end of the corridor to guide the traveller to move on or to go to second line control. Interfaces to a web service where the encrypted reference data for each traveller is stored, is also implemented, as well as interfaces

to NFC reader and the Border Guard Monitoring App, which is planned to be implemented on a tablet, which is then carried by the border guard overlooking the process.

The high-level diagram of the components and their interfaces is shown in Figure 13.

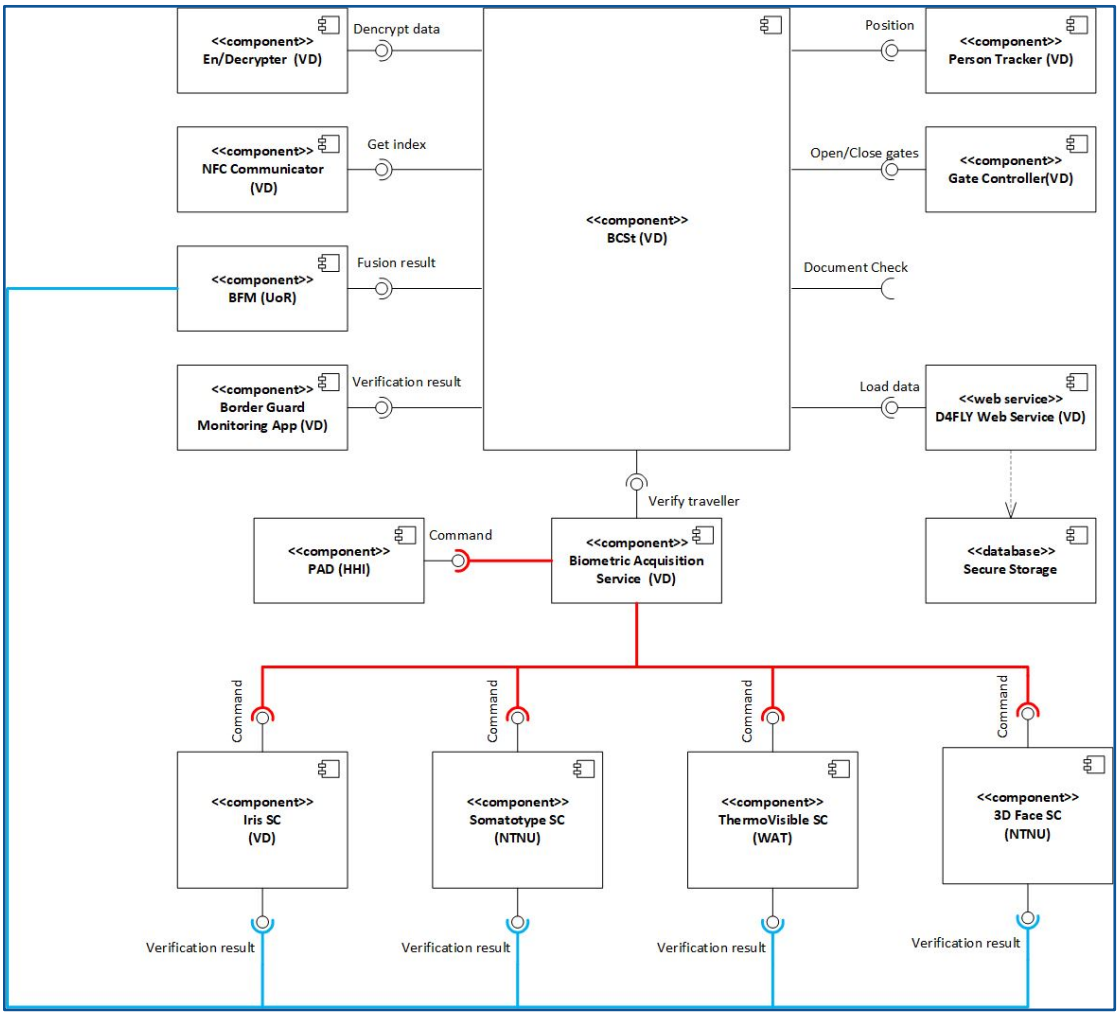


**FIGURE 13: COMPONENT LEVEL DIAGRAM OF BIOMETRIC CORRIDOR VERIFICATION SYSTEM SOFTWARE**

At the time of writing this deliverable, the software was in the final stages of the definition of the details of all connected components as well as the communication between the components and the BCSt. Implementation has started, aiming at being ready for the first integration test, which is scheduled for the end of January 2021.

### 4.3.3 Smartphone Application

A smartphone-based application shall be used by the traveller in this scenario mainly to store certain information as a result of the enrolment process, as well as to initiate the verification processes at a later point in time before entering the biometric corridor. The smartphone will store a specific cryptographic key which is used to encrypt all the traveller's enrolled data. This key is stored securely on the smartphone and available to be used only after valid authentication and approval of the traveller. Using this concept, the traveller is in full control of his enrolled data, as without his consent (and provision of the stored key) the enrolled encrypted data is not usable for the verification or for any unauthorized access.

At the time of writing this deliverable a first working prototype has been developed. Parts of the unit testing has also been completed, however, full testing, in connection with the kiosk and the corridor is planned in the next phase of the project.

#### *4.3.3.1 App main features*

The features of the application are:

- Secure data handling, transparent and easy to use for the traveller.
- Secure storage of the received cryptographic encryption key and secure extraction and transmission to the biometric verification corridor system for the traveller verification.
- Secure data communication via NFC interface with additional encryption of the transmitted data to add an additional layer of security.
- Re-using the smartphone authentication (fingerprint, pin, etc.) as authentication for the app.

#### *4.3.3.2 App structure*

Figure 14 shows a brief overview of the interfaces and components involved for the smartphone application.

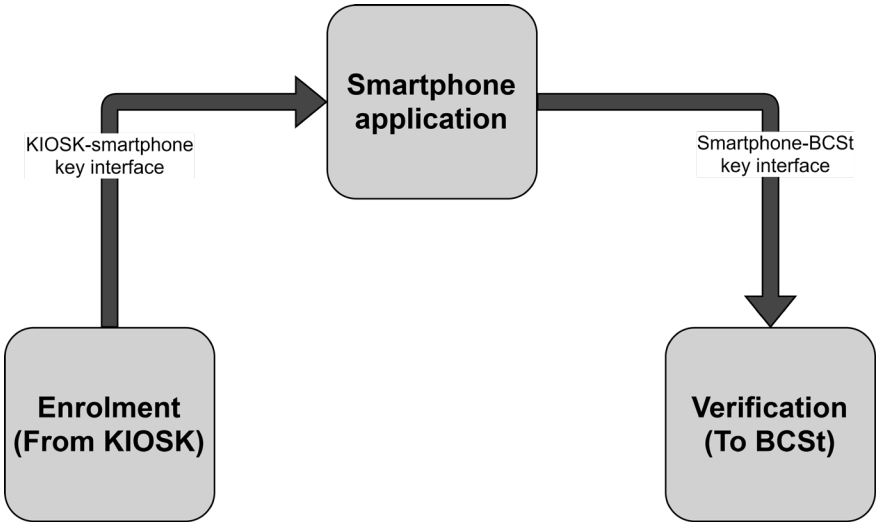


**FIGURE 14: SMARTPHONE APPLICATION INTERFACES TO OTHER COMPONENTS**

Further details on the interfaced and the implementation of the smartphone application can be found in deliverable D6.2 in sections 3.3.1, 3.3.2 and 3.4.1 [D4FLY-6.2].

#### *4.3.3.3 Prototype*

The steps and graphics below show various exemplary screens of the GUI of the current prototype smartphone application.

##### 4.3.3.3.1 Enrolment process steps and app screens

*Step 1.* The traveller clicks on “Enrol” button to begin the enrolment process (screen shown in Figure 15).

*Step 2.* The traveller then approaches the kiosk and taps the "Reached" button (screen shown in Figure 16).

*Step 3.* After the traveller completed the enrolment, the instruction screen on the kiosk will ask the traveller to tap his smartphone to the kiosks NFC reader. This instruction is also reflected on the smartphone (screen shown in Figure 17).

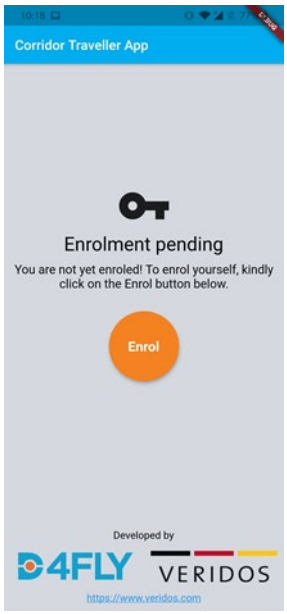


**FIGURE 15: APP SCREEN 01**


**FIGURE 16: APP SCREEN 02**


**FIGURE 17: APP-SCREEN 03**

*Step 4.* The smartphone receives data from the kiosk via NFC the interface (screen shown in Figure 18).

*Step 5.* Once the data transfer is finished, the process on the smartphone ends (screen shown in Figure 19).

*Step 6.* When the enrolment is completed, the application prompts asking if the enrolment was successfully completed. If the traveller confirms successful completion the transmission and storage process is completed, otherwise the data process is considered as incomplete or interrupted and all data is deleted. (screen shown in Figure 20)

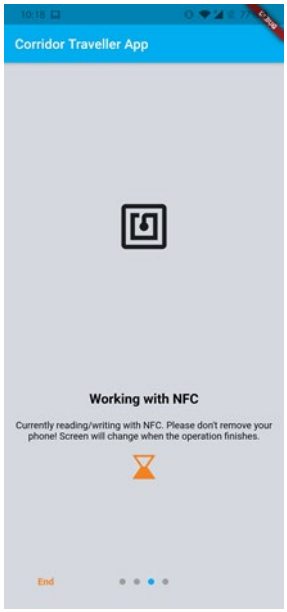


**FIGURE 18: APP SCREEN 04**

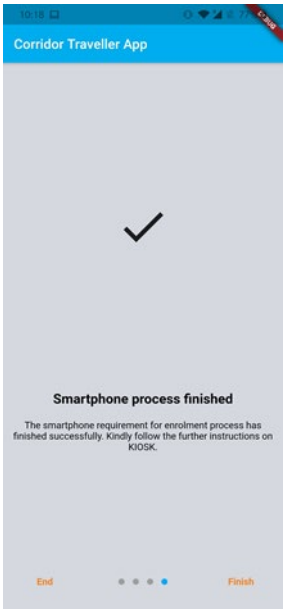


**FIGURE 19: APP SCREEN 05**

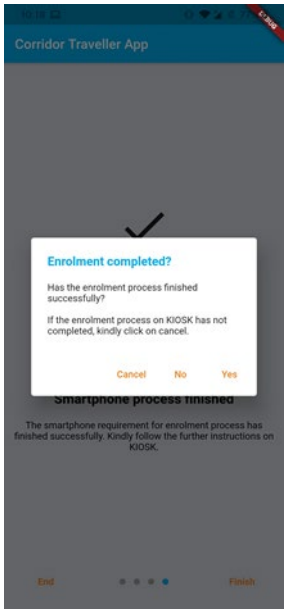


**FIGURE 20: APP SCREEN 06**

#### 4.3.3.3.2 Verification process steps and app screens

*Step 1.* Approaching the biometric corridor at the respective travel destination the traveller starts the smartphone app. Selecting "Verify" on the initial screen starts the verification process. There is also an option foreseen for a new enrolment, which would delete all previously enrolled and stored data and re-enter the enrolment part (screen shown in Figure 21).

*Step 2.* Approaching the biometric corridor, the traveller taps the "Reached" button (as shown in Figure 22).

*Step 3.* At this point, the traveller's authentication is verified using the standard authentication means of the used smartphone. If the authentication succeeds, the process continues otherwise the process ends with authentication error.

*Step 4.* The traveller is now asked to tap the smartphone at the NFC reader available at entrance of the biometric corridor (as shown in Figure 22).

*Step 5.* The smartphone now starts sending the traveller's data to the corridor system (as shown in Figure 23).

*Step 6.* Once the transfer is finished, the process on smartphone ends (as shown in Figure 24). The traveller can now walk through the corridor to complete the verification process (see also Figure 25).

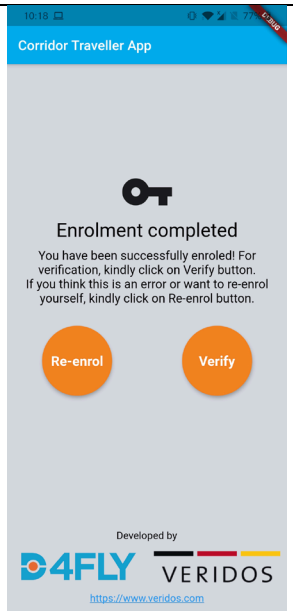


**FIGURE 21: APP SCREEN 07**

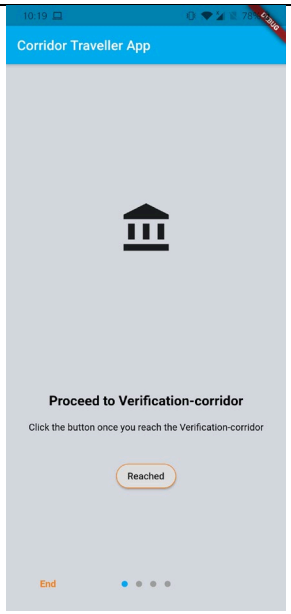


**FIGURE 22: APP SCREEN 08**

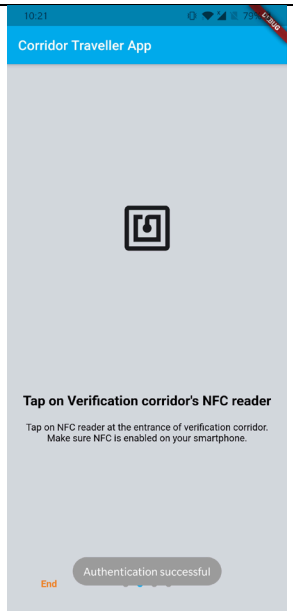


**FIGURE 23: APP SCREEN 09**

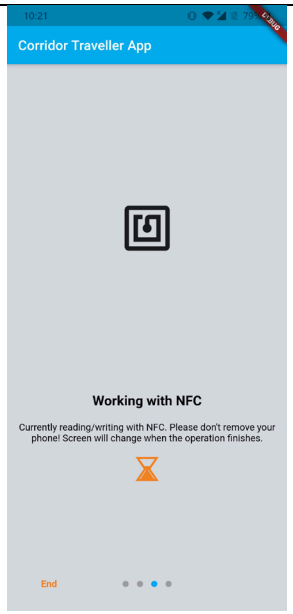


**FIGURE 24: APP SCREEN 10**

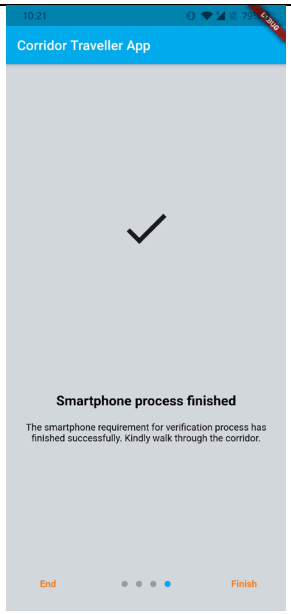


**FIGURE 25: APP SCREEN 11**

## 4.4 Border Guard Application (BGA)

A border guard application planned to be implemented on a mobile device like a tablet is another part of the overall subsystem for scenario 2. It will be used to display the verification status of travellers moving out of the biometric corridor at the end of the verification process. Using this information, the border guard can determine which travellers have been successfully verified and which travellers failed verification and need further investigation. A tablet was selected to enable mobility, freedom of movement and removing the need for a fixed booth using up more space. This approach was used also in previous projects like PROTECT with good results.

The BGA will communicate directly with the Border Control Station (BCSt, see Figure 13). The main functionality of the BGA is:

1. Controlling the BCSt (starting, stopping the system)
2. Communication with the BCSt
3. Visualization of ongoing verification procedures in the corridor, e.g. when a traveller taps on the NFC reader at the entrance of corridor, the application will display a new entry (in form of a card) depicting which traveller is about to enter the biometric corridor.
4. Visualization of verification results, e.g. when the traveller leaves the biometric corridor, the card is updated with the traveller's verification result.

The BGA shall also display the traveller's crossing the biometric corridor in a list. Each entry in the list (called a card) will correspond to one traveller. The card shall contain the following basic information:

1. *Enrolled face image:*
   The face image that was captured at enrolment kiosk during the enrolment process.
2. *Live face image:*
   The live face image captured in the biometric corridor.
3. *Verification status:*
   The final verification result will be shown based on colour of the card (E.g.: green means success and red means failure).
4. *Final verification score:*
   The final verification score obtained in the verification process.

If the border-guard needs to know more details of the result, this can be displayed, as well, like the traveller's name, the passport details and verification scores from every single sensor controller.

### 4.5 Next steps and further development

*Next steps*

This first prototype is planned to be tested in a first full integration test hosted in Veridos premises, currently planned for early 2021, with all the partners and their sensors and software present. The aim of this integration test is to test the communication amongst all the sensors and components, as well as a run through the complete process using the kiosk for enrolment, the smartphone app to store the data and the biometric verification corridor.

This first prototype, possibly with some improvements, is also planned to be used in a first field test in the UK currently planned for mid 2021 (described as scenario 2b in the GA, see also Table 1: Scenarios). Based on the feedback collected in these two events a second improved prototype corridor will be designed and manufactured with an improved composition, materials and optimized placement of the sensors. Also, the enrolment kiosk and the smartphone application will be improved base on the feedback of the test users.

The second scenario 2 prototype (kiosk, smartphone application and biometric corridor) is foreseen to be used in the second field test planned at Piraeus Port in Athens, Greece (described as scenario 2a in the GA, see also Table 1: Scenarios). Ideally it can also be used for the final demonstration, planned for UK towards the end of the project with only minor further optimizations.

*Further development*

Using the agile like approach for the development, the aim of the field tests is, to get feedback and use the feedback to guide the further development. The feedback and evaluation from the tests will be collected and compiled into a list. A prioritization will be done, and a list of features or improvements are defined, which shall be implemented until the second field test.

# 5 SCENARIO 3: LAND BORDER SCENARIO

## 5.1 Overview

Scenario 3 aims at supporting border guards at land border posts where no automated equipment is available. The scenario description in the GA focuses on two main challenges:

1) Document verification and
2) Impostor fraud detection.

The requirements for challenge 1) are overlapping with those in scenario 1b. The prototype configuration for scenario 3 mostly consists of the same platform, GUI and checker components as used in scenario 1b, as described in section 3.

Addressing the challenge 2) the research and development aims at supporting the border guard in the visual verification where the border guard compares the images in the document against the person standing in front of him. Based on this comparison, the border guard decides, if the person is the rightful holder of the passport and the person which is identified in the passport. For this purpose, additional components will be added to the already existing platform and the platform GUI.

One of the additional components will provide automatically manipulated images, which are based on the images read out of the passport. Those images shall show potential changes in the appearance of the depicted person to give the border guard a better basis to compare the images. More details about this technology can be reviewed in [D4FLY-D7.1].

## 5.2 Prototype implementation (current status)

The field test in Lithuania is currently scheduled for M19-M20, the due date for this deliverable is M15. Some details of the configuration of the prototype are currently being finally discussed at the time of writing this deliverable. The implementation of the platform is available and has already been used in a first field test, as described in section 3. The additional components for impostor fraud detection are currently being developed.

Further details on the implementation will be reported in the next deliverable of this work package, which is D4.7 – “Development of Demonstrators for the Scenarios 2” due in M21.

There is one field test foreseen for scenario 3 in the GA, with no final demonstration, so those components which are specific to this scenario and are not re-used in prototype configurations for other scenarios will not be improved and enhanced further after the field test. The suggestions and feedback from the field test will be reported in the deliverable D9.5 – “Field Testing Lithuania”, due in M20 (classified as “Restreint UE/EU Restricted”)

# 6 SCENARIO 4: COACH SCENARIO

This section contains a high-level description of the coach scenario in which an enrolment kiosk shall be used to enrol a traveller's data before they embark a coach (or train). Specifically, the traveller's passport data and a facial image is being captured during the enrolment. A smartphone application will be used for the verification process at the time the coach arrives at the border for the border checking process. The focus in this scenario is to develop technologies that help the border guards with their risk assessment by providing pre-information on the travellers arriving at the border. Another main aspect is to use mobile technologies for passenger verification, thus improving the flexibility and effectiveness of the border control process.

The following sections describe the prototype that has been developed for this scenario.

## 6.1 Overview

The scenario consists of three main parts: the pre-boarding enrolment, the backend system and the smartphone application for verification. The enrolment will take place before the traveller boards the coach and the verification will take place inside the coach by a border guard using a smartphone application. The data enrolled during this process is stored in the backend [D4FLY-D6.3]. The graphic in Figure 26 describes the scenario in a brief overview.

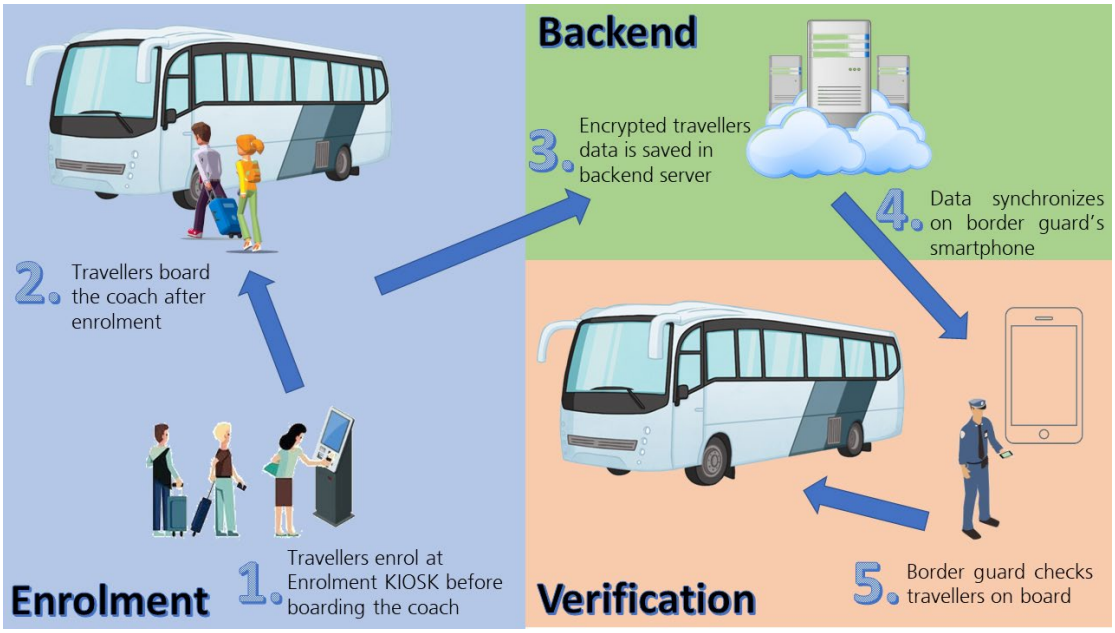


**FIGURE 26: SCENARIO 4 HIGH LEVEL OVERVIEW (SEE ALSO [D4FLY-6.3])**

## 6.2 Relation to other work packages and deliverables

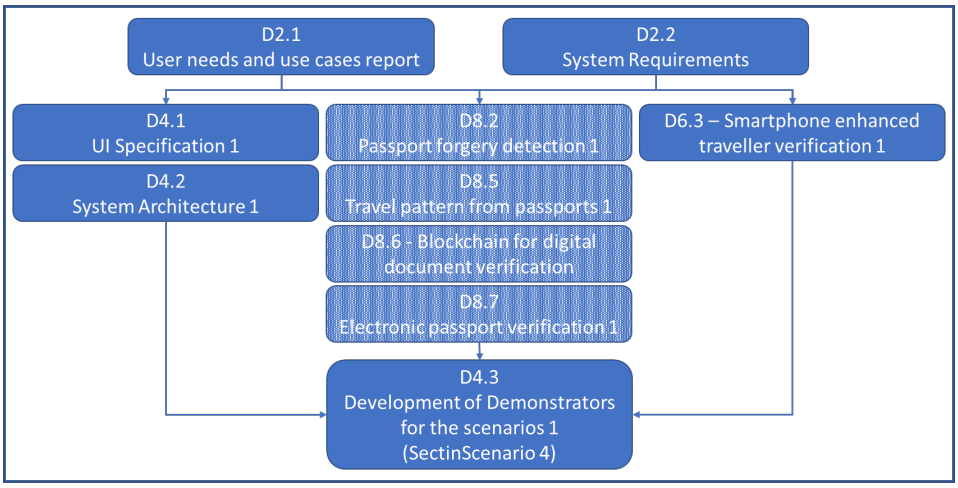


**FIGURE 27: SCENARIO 4: RELATION TO OTHER WORK PACKAGES AND DELIVERABLES**

As in the other scenarios, user needs, use cases and system requirements are described in the deliverables resulting from work package 2 ([D4FLY-D2.1],[D4FLY-D2.2]). The platform related deliverables D4.1 and D4.2 describe the specification of the underlying system architecture and UI design guidelines [D4FLY-D4.1, D4FLY-D4.2]. The kiosk uses a passport reader, hence the advanced document verification components resulting from work package 8 could be used here as well., as also described in the GA for this scenario. As the advanced document verification components are extensively tested in the prototype configuration for scenario 1b those components are not included in the prototype and demonstrator for this scenario (hence shown in different texture in the image). Deliverable 6.3 from work package 6 task 6.3 describes the smartphone application as well as the backend system in detail [D4FLY-D6.3]. The deliverables and their relationship are depicted in Figure 27

## 6.3 Prototype implementation (current status)

As already described, the scenario consists of three main parts: the pre-boarding enrolment, the backend system and the smartphone application for verification. Figure 28 shows the top-level architecture. In this section each part will be described in detail based on the current prototype implementation.

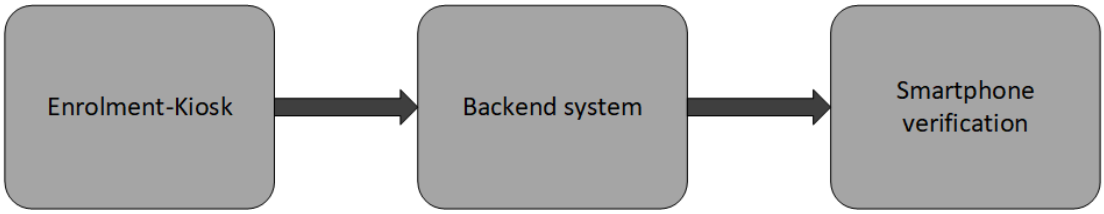


**FIGURE 28: SCENARIO 4 SUBSYSTEM TOP LEVEL BLOCK DIAGRAM**

### 6.3.1 Enrolment kiosk

As explained in section 4.4.1 the same enrolment kiosk prototype is used in both scenarios, scenario 2 and this scenario 4. The kiosk is designed in a modular way, such that parts can be configured to support different enrolment sequences for the scenarios.

For this scenario 4, no biometric modality must be enrolled, except for a 2D facial image in visible light. Hence no other biometric sensor will be mounted in the kiosk, only the camera

capturing this 2D facial image will be present during the enrolment. The other openings in the kiosk body will be covered with blanking plates.

The reduced functional requirements on the kiosk in Scenario 4 are also reflected in shorter GUI screen sequence and smaller number of modules used to make up the overall controlling software (see Figure 29). Since none of the biometric sensor controllers connected via Biometric Acquisition Service are required, the underlying software now contains only one core component, kiosk. All helper modules connected to kiosk remain the same, except for Ticket Service Agent, which replaces NFC communicator used in Scenario 2. The Ticket Service Agent supports the selection of a specific bus travel, which is identified by its departure time, the destination and a unique coach number. This unique coach trip number is used to reference the correct data set at the border post at which the coach crosses the border.

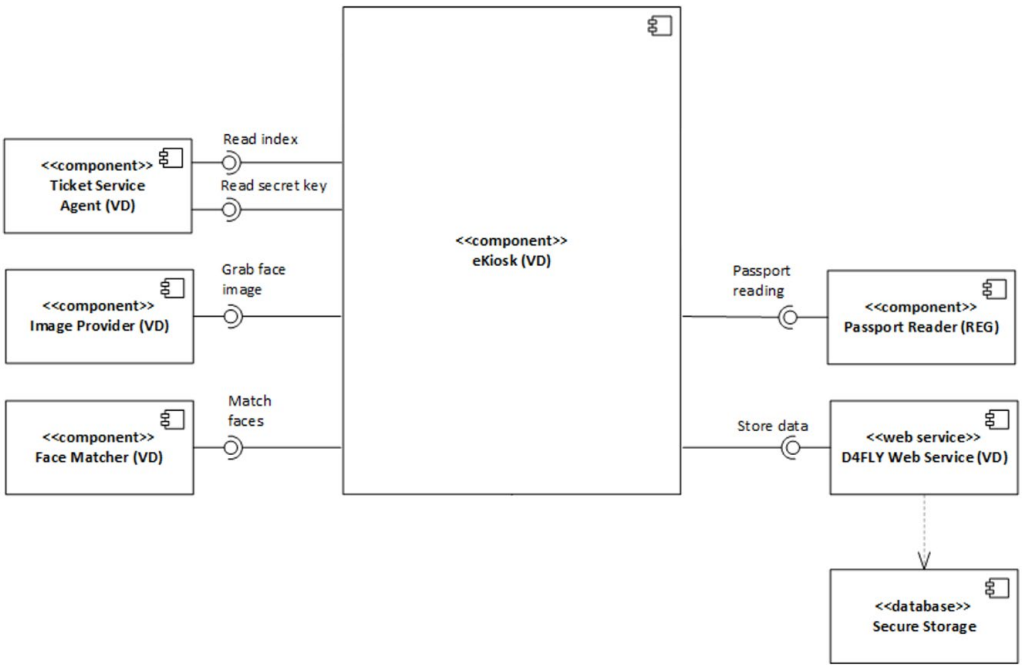


**FIGURE 29: SOFTWARE COMPONENT OVERVIEW OF THE KIOSK, CONFIGURED FOR SCENARIO 4**

### 6.3.2 Backend system

The backend has three main functions:

- Storage and authentication of border guard's login details
- Storage of traveller's pre-enrolled data
- Data protection and encryption services

The backend system is implemented to bridge and connect the enrolment process to the verification process. A first prototype for this backend system has been designed and implemented. Figure 30 shows the high-level block diagram of the backend system.

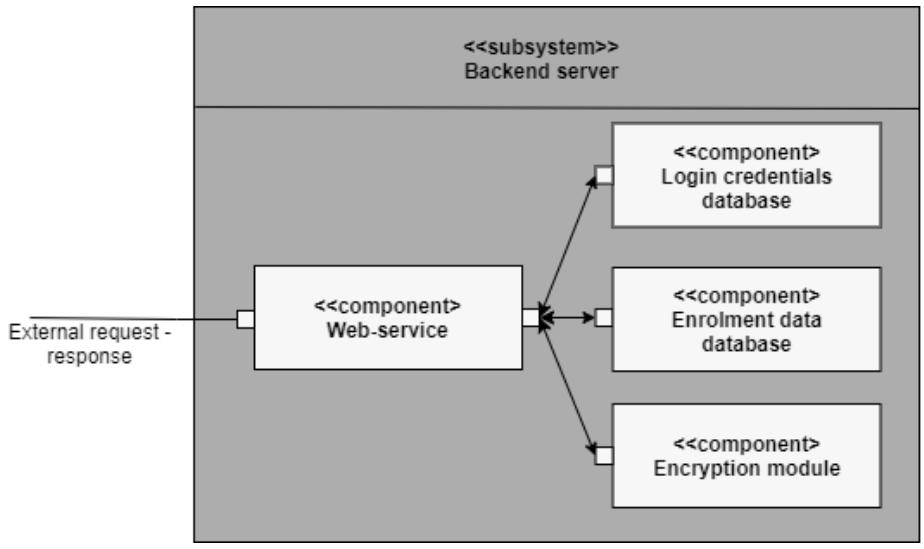


**FIGURE 30: BACKEND TOP LEVEL DIAGRAM**

The backend system communicates using a webservice through which the enrolment kiosk and the smartphone verification app can connect to. The web-service internally connects to databases and the encryption module to provide the intended functionalities. The internal components are as explained below:

- **Login credentials database**
  The user (border guard) must authenticate to the smartphone application using a login name and a password. This function provides an additional layer of security and protection against unauthorized use. To securely store the login credentials for reference, a database on a backend server is used. An account is created for a border guard in this database by an administrator. The authentication from smartphone to backend system is implemented using a secure channel. The credentials are also hashed before being sent over the channel for additional security. D6.3 section 3.3.1.1 explains this database implementation in detail [D4FLY-D6.3]

- **Enrolment data database**
  This database stores the enrolled traveller's data sorted by the respective coach number. The enrolled data is transmitted to the database using a webservice. The smartphone application also connects to this database via the webservice to download the stored data set for a coach. The request and response in this communication is implemented using a secured channel. All exchanged data encrypted. The deliverable D6.3 section 3.3.1.2 explains this database implementation in [D4FLY-D6.3].

- **Encryption module**
  All data in the backend enrolment database will be encrypted. The encryption module on the backend system will be generating and providing keys for the encryption of the data. For each coach trip number, this module will generate a dedicated public and private key pair using asymmetric encryption. The public key will be used by the enrolment-kiosk to encrypt the traveller's data before storing it in the enrolment data database. The private key will be used by the smartphone application to decrypt the downloaded data during the verification process.

### *6.3.2.1 Smartphone Verification*

A smartphone-based application is used by a border guard to perform the traveller identity verification in the confined space of the coach. It will be installed and setup on a smartphone which is used by the border guard.

The main functions of this smartphone application are:

- Additional authentication with dedicated credentials for additional security and protection against unauthorized usage of the application (in addition to the standard authentication means of the smartphone).
- Download for temporary storage of travellers encrypted enrolled data (data set) from the backend.
- Secure decryption and handling of the downloaded data set.
- Verification of the passengers in the coach against the pre-enrolled reference data using the smartphone built-in camera.
- Provision of statistics like for example a count of traveller's having been successfully verified, traveller's registered but not boarded the coach, and traveller's that failed verification.
- In case the verification should fail, a secondary method is provided to access the pre-enrolled data, where the app provides a manual MRZ reading feature through which the traveller's travel document MRZ can be read and the corresponding data can be fetched from database for manual verification.

### *6.3.2.2 App structure*

Figure 28 shows a brief overview of the interfaces and components involved for the smartphone application.

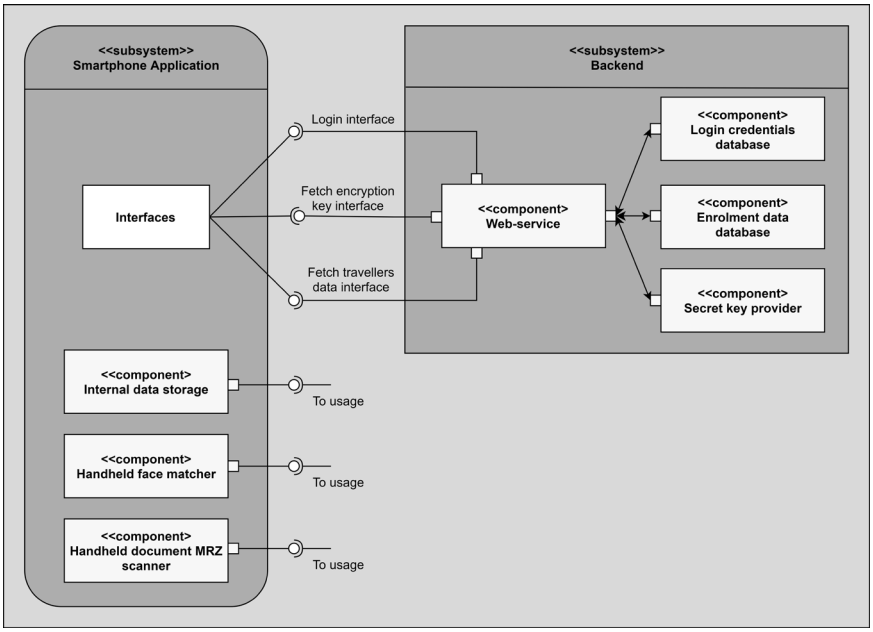


**FIGURE 31: SMARTPHONE APP COMPONENTS AND INTERFACES**

Detailed descriptions of the components shown in Figure 31 can be found in deliverable D6.3 [D4FLY-6.3]

### *6.3.2.3 Current prototype*

The steps and graphics below show the implementation of some main screens in the process of verification as per the current status of the prototype implementation. The images are depicted following the sequence of their appearance in the process.

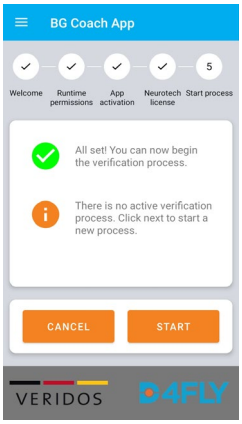


**FIGURE 32: BG COACH APP 01**

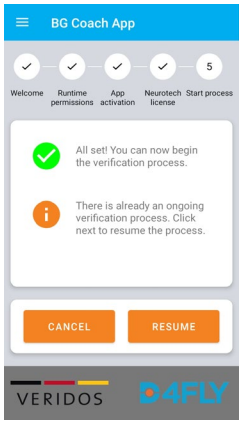


**FIGURE 33: BG COACH APP 02**

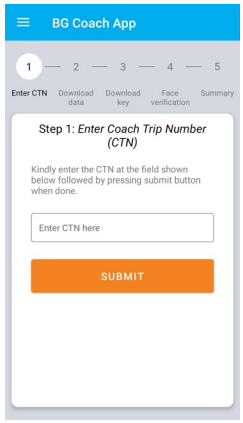


**FIGURE 34: BG COACH APP 03**

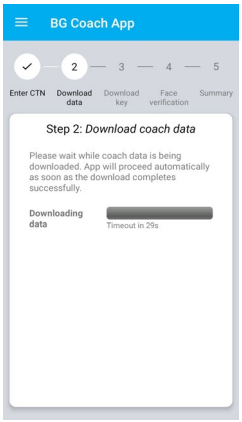


**FIGURE 35: BG COACH APP 04**

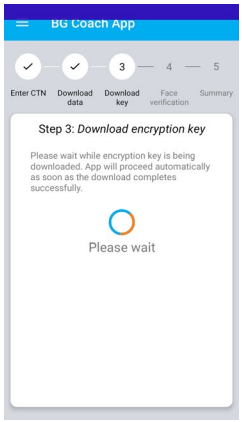


**FIGURE 36: BG COACH APP 05**

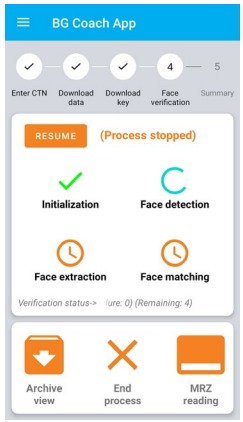


**FIGURE 37: BG COACH APP 06**

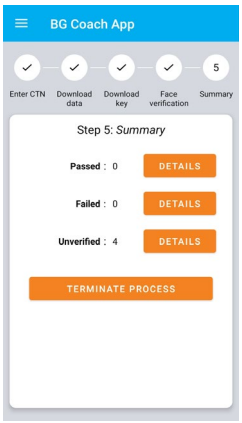


**FIGURE 38: BG COACH APP 07**

### 6.4 Prototype testing

A manual testing approach has been taken for the unit test of the database and the smartphone application.

*Database testing*

The database functionality in the coach scenario is limited to the CREATE functionality. There is no further action performed on the data after it was entered into the database.

The following main attributes have been tested on the database in the backend:

1. The data of the passengers is not lost or corrupted during the process.
2. Mapping of the fields according to the UI and backend
3. A partially enrolled/aborted passengers' data should not be stored in the database
4. The passenger's data should not be made available to unauthorized persons.
5. There is no data duplication of the passengers in the database during the process.
6. NULL values checked for required fields
7. Database integrity in case of disconnection

*Smartphone Application Testing:*

Two main areas have been tested for the smartphone application

1. Hardware Compatibility Testing: As this application is not available to the general public, the application was tested on a single model running Android OS for any compatibility issues.

2. Application Testing: Execution of testcases targeting the functionality of the application using a manual test approach.

The application software was tested using a manual test approach. Functional testcases have been defined and executed to validate

- whether all the required permissions are granted to the application as required.
- that the device can perform required multitasking requirements whenever it is necessary to do so.
- that the navigation between relevant modules in the application are as per the requirement.
- that there are no truncation errors in the passenger's information.
- that the border guard receives an appropriate error message whenever there is any network error during the download of the passenger's data.
- that the border guard application resumes at the last operation in case of a crash.
- that the border guard can access the keypad to enter the Coach trip number.
- the count of the passengers, after every successful verification.

Additional tests have been performed to ensure the usability and ease of use of the application. Aspects that have been tested include:

- Validation that the buttons have the required size for the easy use.

- Validate that the buttons are placed synchronously in every screen, to avoid the confusion.
- Validating the text on buttons for visibility and simplicity
- Validation that the application provides proper user feedback, whenever needed.
- Validation that the closing of the application is performed from different states and verify if its re-opens in the same state.

### 6.4.1 Integration testing

Integration test was initially planned to be performed in Veridos premises, as all main components are developed by Veridos. The first field test for the coach scenario, which was planned in the UK for M13-M14 could not be executed due to the Corona virus pandemic, it has been planned to be shifted to mid-2021. Therefore, at the time of writing this deliverable no further integration testing nor field test has been completed using the prototype for this scenario. Any future test activities are planned to be reported in the next deliverable D4.7.

## 6.5 Further development

The current prototype has a version where the coach scenario in general can be tested and evaluated. Certain features and improvements are being looked as potential possibilities for the next version of the prototype depending on the feedback from the first field test. Some of these possible features are as described below:

1. **Data in backend system database will be deleted after verification process ends.**
   Once the verification process for a coach is completed, the data from the border guard's smartphone is going to be deleted. Correspondingly, the data in the backend system will also get deleted.

2. **Add multiple border guards based parallel verification process.**
   Multiple border guards can perform verification process inside the coach (with their own smartphones), thereby parallelizing and speeding up the verification process.

3. **Include traveller's ticket information to prevent the traveller from enrolling twice for the same journey.**
   The journey will be combined with the traveller's purchased ticket to make sure the traveller enrols only once.

4. **Add QR code-based traveller's ticket scanning.**
   The traveller can simply scan the QR code available on their purchased ticket from Enrolment-kiosk to automatically select the coach trip number and associate their ticket with their enrolment.

# 7 SUMMARY AND NEXT STEPS

The prototypes described in this deliverable relate to the four main scenarios as described in the GA.

The prototypes for scenario 1 (1a and 1b) have been developed, containing all planned functionality for this first prototype. The document verification prototype has been field tested successfully in the field test in Netherlands. Feedback has been provided by the end users, which will be considered in the next phase of the development with the next version of the prototype planned to be tested at the second Netherlands field test in September/October timeframe in 2021.

The design for the initial prototype for scenarios 2, with its main parts the kiosk, the smartphone application and the biometric corridor, is completed, the implementation is ongoing at the time of writing this deliverable. A first (internal) integration tests with all components from all participating partners is planned for January 2021, however, at the time of writing this deliverable, there is a high risk, that integration testing might have to be re-planned depending on the further development of the Corona pandemic. The first field test of this prototype is currently planned in UK in the second half of 2021.

The design for the initial prototype for scenario 3 is also completed, the implementation is ongoing at the time of writing this deliverable. A field test of this prototype is currently planned in Lithuania in the first half of 2021.

The implementation of the prototype for scenario 4 has been completed for the smartphone application and the backend system. The implementation of the enrolment kiosk is ongoing at the time of writing this deliverable. The field test for this prototype was initially planned for September/October 2020, but it had to be postponed to mid'2021 due to the Covid-19 pandemic and its implications.

These prototypes mainly consist of the platform as a result from this work package 04 and components resulting from work packages 05, 06, 07 and 08, hence the parallel development and the integration of all components into working systems pose a specific challenge. An agile like approach was selected with early field tests to gather feedback early in the project allowing for adjustments in the further project phase. The further development of the prototypes will be described in the subsequent deliverables D4.7 – "Development of demonstrators for the scenarios 2" and D4.8 – "Development of demonstrators for the scenarios 3".

# 8 REFERENCES


| | |
|---|---|
| [D4FLY-D2.1] | D4FLY Deliverable D2.1 – User needs and use cases report |
| [D4FLY-D2.2] | D4FLY Deliverable D2.2 – Requirements Analysis Report |
| [D4FLY-D3.2] | D4FLY Deliverable D3.2 – Privacy and Data Protection Impact Assessment |
| [D4FLY-D4.1] | D4FLY Deliverable D4.1 – UI Specification 1 |
| [D4FLY-D4.2] | D4FLY Deliverable D 4.2 – System Architecture 1 |
| [D4FLY-D6.2] | D4FLY Deliverable D6.2 - Smartphones as carrier for identity data 1 |
| [D4FLY-D6.3] | D4FLY Deliverable D6.3 – Smartphone enhanced traveller verification 1 |
| [D4FLY-D7.1] | D4FLY Deliverable D7.1 – Analysis and simulation of potential attacks |
| [D4FLY-D8.2] | D4FLY Deliverable D8.2 – Passport forgery detection 1 |
| [D4FLY-D8.5] | D4FLY Deliverable D8.5 – Travel pattern from passports 1 |
| [D4FLY-D8.6] | D4FLY Deliverable D8.6 – Blockchain for digital document verification |
| [D4FLY-D8.7] | D4FLY Deliverable D8.7 – Electronic passport verification 1 |
| [PCW-01] | https://www.pcworld.com/article/2938520/nfc-security-3-ways-to-avoid-being-hacked.html |
| [PROTECT] | http://projectprotect.eu/v |
| [IEEE-01] | https://ieeexplore.ieee.org/document/7345265 |