D6.2

Smartphones as carrier for identity data 1

Document Due Date: 31.05.2020 (M09)
Document Submission Date: 29.05.2020 (M09)

Work Package 6:

Alternative technologies to identifying people

Document Dissemination Level: Public

Abstract

The main objective within the work package WP6 of the D4FLY research project is to explore alternative technologies to people identification. Within this work package task 6.2 focusses on research and development of a smartphone application based solution which can be used as an alternative data carrier to a travel document such as an ePassport. The smartphone application will be used in the D4FLY automated border post scenario and the objective is to speed up the inspection procedure at a border in particular airport, port or train station in due consideration of privacy and security requirements.

The solution will be based on ICAO's Digital Travel Credential (DTC) concept. In D4FLY the DTC data will be derived from a traveller's ePassport and supplemented by additional biometrics, i.e. biometrics in addition to the face portrait image stored on the ePassport. This DTC data is stored encrypted in a central repository and the traveller grants a Border Control Station access to this data by means of their smartphone application. While this solution reduces the amount of data that needs to be transferred from the smartphone application to the Border Control Station and therefore minimises the transmission time, it allows the traveller to control access to their data. The minimised transmission time and the usage of additional biometrics enables an on-the-move biometric verification of the traveller and a seamless inspection procedure at border control.

This deliverable describes the initial implementation concept including the enrolment and the usage of the smartphone application in the seamless inspection procedure. Field testing of the initial version of the application is planned after the submission of this deliverable in order to collect user feedback. Further improvements are anticipated based on the user feedback and further refinements. The final version will be described in the subsequent deliverable “D6.7 – Smartphone as data carrier for identity data 2”, which is due in M24.

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	**D6.2**
Document Title	**Smartphones as carrier for identity data 1**
Work Package reference	WP6 Alternative technologies to identifying people
Delivery due date	31.05.2020 [M09]
Actual submission date	29.05.2020
Dissemination Level	Public
Lead Partner	Veridos GmbH
Author(s)	Ananya Verma, Jens Urmann (VD)
Reviewer(s)	Armin Reuter (VD)

Document Version History

Version	Date created	Beneficiary	Comments
0.1	31.03.2020	Veridos	Draft document structure
0.2	27.04.2020	Veridos	Integrated Sections 3 and 4
0.3	28.04.2020	Veridos	Integrated Sections 1, 2
0.4	30.04.2020	Veridos	Added Section 5
0.5	11.05.2020	Veridos	Veridos internal reviews
0.6	19.05.2020	UREAD	UREAD internal review
0.7	20.05.2020	Veridos	Resolved comments from UREAD review
.0	27.05.2020	Veridos	Final edits

List of Acronyms and Abbreviations

ACRONYM	EXPLANATION
AA	Active Authentication
AES	Advanced Encryption Standard
BAC	Basic Access Control
BCSt	Border Control Station
CA	Chip Authentication
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
D4FLY	Detecting Document frauD and iDentity on the fly
DG	Data Group
DTC	Digital Travel Credential
DTC-PC	DTC Physical Component
DTC-VC	DTC Virtual Component
eID	electronic ID
EAC	Extended Access Control
EC	European Commission
eMRP	electronic Machine Readable Passport (also known as ePassport)
eMRTD	electronic MRTD
EU	European Union
ICAO	International Civil Aviation Organization
IMEI	International Mobile Equipment Identity
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
NFC	Near Field Communication
NTWG	New Technology Working Group
OS	Operating System
PACE	Password Authenticated Connection Establishment
PROTECT	Pervasive and UseR Focused BiomeTrics BordEr ProjeCT
TEE	Trusted Execution Environment

Table of Contents

1 INTRODUCTION

1.1 Background

This section summarises the status of ongoing relevant standardisation activities in the field of identity management using mobile devices, in particular the standardisation of so called Digital Travel Credentials (DTCs). In addition the relevant results from the PROTECT project are presented that has used a smartphone as a data carrier for identity data. This summary serves as input for the specification of the requirements and the solution in the following sections.

1.1.1 Digital Travel Credential Standardisation

The ICAO New Technology Working Group (NTWG) is working on a policy paper for Digital Travel Credentials (DTC) [3]. Based on this concept and its requirements the standardisation group ISO/IEC JTC 1 / SC 17 / WG3 is preparing a specification [4] on behalf of ICAO which incorporates Veridos / D4FLY comments [7]. This clause outlines ICAO's DTC concept which is based on the ICAO Doc 9303 [2] specification for ePassports (eMRP) – or electronic Machine Readable Travel Documents (eMRTD) in general – in order to minimise the effort for the DTC implementation. In particular it is intended to re-use the eMRTD storage format, i.e. the Logical Data Structure (LDS) that contains the holder's biographical and biometric data as well as other data, and the eMRTD's security protocols, see Table 1-1.

TABLE 1-1: EMRTD PROTOCOLS FOR SECURING ELECTRONIC DATA

Protocol	Description
Passive Authentication	The issuing State or organization cryptographically signs the Logical Data Structure (LDS) stored on the eMRTD. This allows to verify that this data is authentic and has not been changed after issuance.
Active Authentication (AA)	The eMRTD stores a private key which is used to prove that the eMRTD is authentic, i.e. LDS has not been copied to another chip.
Chip Authentication (CA)	
Basic Access Control (BAC)	These protocols are designed to prevent skimming (reading the LDS via the contactless interface without the consent of the eMRTD holder) and eavesdropping on the communication between the eMRTD and the inspection system via this contactless interface. Therefore the inspection system needs to optically retrieve data printed on the eMRTD in order to set up and encrypt the communication via the contactless interface. This optical access is interpreted as deliberate use of the eMRTD by its holder.
Password Authenticated Connection Establishment (PACE)	
Extended Access Control	Access control to additional biometrics may require specific

Protocol	Description
(EAC)	keys. ICAO Doc 9303 does not specify the protocol, but leaves the details to the implementing States or organizations.
Encryption of Additional Biometrics	In order to restrict the access to additional biometrics, the data may be encrypted. ICAO Doc 9303 does not specify the protocol, but leaves the details to the implementing States or organizations.

ICAO's DTC concept follows a hybrid approach, i.e. the DTC is made up of two components:

- The **DTC virtual component DTC-VC**: A data structure containing biographical and biometric data of the DTC holder as well as other data based on the Logical Data Structure (LDS) stored on an eMRTD chip. Passive Authentication, see Table 1-1, is applied.
- The **DTC physical component DTC-PC** which implements the Active Authentication (AA) or Chip Authentication (CA) protocol, see Table 1-1, known from the eMRTD. For these protocols the DTC-PC securely stores a private key.

If the DTC supports a DTC-PC, the DTC-PC public key is stored in the DTC-VC and subject to passive authentication, i.e. the DTC-PC and the DTC-VC are cryptographically linked. The DTC-PC aims to prevent copying of the DTC. The issuing State or organization will indicate in the DTC-VC a security level of the DTC-PC using the ISO/IEC 23220 specification that is under development, see clause 1.1.2.2. This security level may express e.g. whether the DTC-PC is a software based or hardware based solution, whether a security certification applies, details about the user identification in the enrolment process etc. It can be used by a verifying State or organization in the inspection procedure to assess its risk.

The ICAO NTWG policy paper defines three types of Digital Travel Credentials:

- **eMRTD bound DTC**, see Table 1-2
- **eMRTD-PC bound DTC**, see Table 1-3
- **PC bound DTC**, see Table 1-4

TABLE 1-2: EMRTD BOUND DTC TYPE

Topic	Description
DTC-VC	The DTC-VC contains a copy of (a part of) the eMRTD's Logical Data Structure (LDS). If the eMRTD supports Active Authentication and / or Chip Authentication, the corresponding public keys are stored in the eMRTD's LDS and therefore the DTC-VC; in this case there is a cryptographic link between the DTC-VC and the eMRTD.
DTC-PC	There is no DTC-PC, but the eMRTD itself serves as physical authenticator. Either AA and / or CA is used or the eMRTD booklet itself with its physical security features serves as physical authenticator.
Issuance	The eMRTD holder can create the DTC-VC on his own; an involvement of the eMRTD issuing State or organization is not required as no additional cryptographic signature is created.
Validity	The DTC-VC inherits the validity period of the eMRTD that was used to

Topic	Description
	derive the DTC-VC.
Revocation	The DTC-VC and the eMRTD share the same document number. For this reason a separate revocation of the DTC-VC is not possible, but a revocation by the document number revokes the DTC as well as the eMRTD.
Fallback	A traveller is required to carry her eMRTD with her while travelling.

TABLE 1-3: EMRTD-PC BOUND DTC TYPE

Topic	Description
DTC-VC	The DTC-VC contains a copy of (a part of) the eMRTD's LDS, its own document number that is different from the eMRTD's document number, its own validity date, the public key of the DTC-PC and possibly further data. The DTC-VC is cryptographically signed by the issuing State's or organization's DTC signer.
DTC-PC	The DTC-PC supports the Active Authentication and / or Chip Authentication protocol. It may be hosted on a device issued by the issuing State or organization or a device of the citizen. The eMRTD serves as fallback for the DTC-PC.
Issuance	The DTC-VC is derived from an existing eMRTD and the issuing State or organization is involved in the DTC issuance process. It cryptographically signs the DTC-VC and creates the DTC-PC application.
Validity	The DTC has its own validity date that must be within the validity of the eMRTD that was used to derive the DTC-VC.
Revocation	As the DTC has its own document number, it can be revoked independently of the eMRTD. A revocation of the eMRTD also revokes the DTC.
Fallback	A traveller should carry his eMRTD with him while travelling.

TABLE 1-4: PC BOUND DTC TYPE

Topic	Description
DTC-VC	The DTC-VC is not derived from an eMRTD. It contains the LDS populated at least with the biographical data and the portrait image, a document number, the public key of the DTC-PC, and optionally further data. The DTC-VC is cryptographically signed by the issuing State's or organization's DTC signer.
DTC-PC	The DTC-PC supports the Active Authentication and / or Chip Authentication protocol. It may be hosted on a device issued by the issuing State or organization or a device of the citizen. There is no fallback for the DTC-PC.
Issuance	The issuing State or organization creates and cryptographically signs

Topic	Description
	the DTC-VC. In addition it creates the DTC-PC application.
Validity	The DTC has its own validity date.
Revocation	As the DTC is not derived from an eMRTD, it is revoked on its own.
Fallback	-

The following topics are out of the scope of ICAO's DTC concept and specification:

- The storage of the DTC-VC will be implementation specific. Possible solutions include (but are not limited to) storage in a cloud, a database, or on the device implementing the DTC physical component.
- The physical device which implements the DTC-PC.
- The protocols to transmit the DTC-VC, in particular any protocols to send the data in advance of travelling e.g. in the context of a visa application. The following exception applies: If the DTC-PC stores the DTC-VC, the ICAO specification will probably specify the transmission protocols that can be used at border control.

The following topics are out of the scope of the first version of the ICAO’ DTC, but may be in the scope of a second version:

- Biometrics other than the face portrait image is in principle out of scope.
- LDS version 2 which allows to store visa, travel stamps, and additional biometrics in the LDS and write this data after issuance. Additional biometrics denotes biometrics in addition to the biometrics stored in LDS version 1.

1.1.2 Related standardisation activities

1.1.2.1 Mobile driving licence

The draft for the ISO/IEC 18013-5 "Mobile driving licence (mDL) application" standard [5] deals with a driving licence on a mobile device or requiring the usage of a mobile device such as a smartphone or tablet. The first revision of ISO/IEC 18013-5 will standardise the so called attended use case involving a physically present verifier who binds the mDL holder to the mDL data read from the mDL, for example, by means of the face portrait image. Later on the unattended use case will be standardised which makes use of either the mobile device itself to bind the mDL holder to the mDL data (for example, via a biometric verification performed by the mobile device) or a remote verifier.

The current mDL draft standard supports an offline usage where the verifier retrieves the mDL data directly from the mobile device and an online usage where the verifier retrieves an access token from the mobile device to request the data online from the issuing authority.

1.1.2.2 Building blocks for identity management via mobile devices

The drafting of the ISO/IEC 23220 series "Building blocks for identity management via mobile devices" [6] is at an early stage. The objective is to standardise interfaces and protocols that can be re-used for mobile eID systems such as an mDL. Therefore the standard is supposed to generalise and enhance the mechanisms of the draft mDL standard. While the draft mDL standard covers only the operational phase, other life cycle phases such as the installation phase and issuing phase are in the scope of the ISO/IEC 23220 series.

1.1.3 PROTECT project

In the PROTECT (Pervasive and UseR Focused BiomeTrics BordEr ProjeCT) project [8] a smartphone application has been developed which acts as virtual travel document. This smartphone application stores encrypted biographical and biometric data of the traveller and the key material to decrypt this data is maintained by a central service. At a Border Control Station the encrypted data is read from the smartphone application via a contactless transmission protocol and the corresponding decryption key requested from the central service.

One of the PROTECT results was that the time required to retrieve the encrypted data from the smartphone application via the contactless transmission protocol was rather long. Therefore the overall performance of the border control process is in need of further improvement to allow for a seamless inspection procedure.

1.2 Aim of this document

This document describes the design of the smartphone application based solution that can be used as a data carrier for biographic and biometric data instead of an ePassport (or an eMRTD in general). In addition the document describes the enrolment process for this smartphone application, the border control inspection procedure, as it is planned for D4FLY and explains the relationship with ICAO's Digital Travel Credential (DTC) concept that is in the process of standardisation.

1.3 Input / Output to this document

1.3.1 Requirements

A preliminary set of requirements for the border control scenario with a smartphone application based solution as DTC has been collected and defined based on an analysis of the D4FLY Grant Agreement [1], the ICAO DTC policy paper [3] and draft specification [4], initial discussions with partners and end users in the consortium, as well as an analysis of requirements from other projects in the same area, including PROTECT. The collection and consolidation of the requirements based on user needs and other inputs is ongoing at the time of writing this deliverable. These will be considered int the further development and related to in the final deliverable of this task, which is D6.7 – “Smartphone as carrier for identity data 2”.

This preliminary set of requirements is noted here.

Before these requirements are listed some underlying design decisions are discussed.

Which DTC type to use for the D4FLY DTC app?

The eMRTD-PC bound DTC is chosen for the D4FLY DTC solution for the following reasons:

- The quality of the portrait image stored in the eMRTD is not sufficient to support an "on-the-fly" processing for a seamless border control as envisaged in the D4FLY project. Such an "on-the-fly" verification processing can be optimized for short processing time, if a (1:1) biometric matching, i.e. a comparison of the biometric data captured “on-the-move” from 1 traveller against one set of data for this traveller that was retrieved e.g. from his/her DTCs. As the eMRTD bound DTC re-uses the face portrait image stored on the eMRTD and does not allow to add further data in the DTC-VC, it is not suitable for "on-the-fly" processing. The eMRTD-PC and PC bound DTC allow to add data that is not present in an eMRTD's LDS.

- The eMRTD bound DTC makes use of the ePassport as physical authenticator. While the ePassport is suitable for usage in eGates, it is not suitable for "on-the-fly" processing.
- The PC-bound DTC does not make use of an eMRTD as fallback solution. In order to ensure that travellers are able to pass border control in case of any failure, a fallback solution is required. The eMRTD-PC bound DTC is derived from an eMRTD which serves as a fallback solution.

Where and how to store the biographical and biometric data of the traveller?

The biographical and biometric data needs to be stored encrypted for security and privacy reasons. In the PROTECT project (see Section 1.1.3) the encrypted biographical and biometric data was stored in the smartphone application under the control of the traveller and the key material to decrypt the data managed by a central service. As a PROTECT outcome the reading time needs to be improved.

The Mobile driving licence (mDL) application (see Section 1.1.2.1), requires a significantly smaller amount of data as no biometric reference data for an on-the-move biometric verification is needed, but only a portrait image of approximately (10 to 20kBytes). Therefore the offline solution that stores the data on the mobile device is not re-usable for performance reasons. An online connection is in a border control scenario often not available and therefore the online solution is also not re-usable.

For performance reasons, in the D4FLY project the encrypted biographical and biometric data is stored encrypted in a central repository and the traveller's smartphone application stores the key material to decrypt the traveller's biographical and biometric data.

Which biometric modality to use for "on-the-fly" processing in this scenario?

The face portrait image is the primary biometric used in eMRTD systems for global interoperability and ICAO recommends to apply the security mechanisms PACE or BAC, see Table 1-1. ICAO has also specified the use of fingerprint images and iris images, however as these are considered to be more sensitive data than the face portrait image, it is recommended to restrict the access to stored fingerprint and iris images further. For this reason additional access control mechanisms such as Extended Access Control or further encryption, see Table 1-1, should be applied.

For the on-the-move biometric verification in a biometric corridor the face portrait image of the ePassport is not suitable and therefore the following biometrics are used:

- 2D-face image,
- 3D-face image,
- a template of an iris,
- an image or a template for somatotype

The biometric reference data is stored encrypted in conformance with the ICAO recommendations for additional access control for biometric data, see Table 1-1 and [2].

Table 1-5 lists the high level requirements that apply to the scenario and its components, in particular the smartphone application.

TABLE 1-5: HIGH-LEVEL REQUIREMENTS FOR THE SCENARIO AND ITS COMPONENTS

Req.Nr.	Description
R1	The scenario shall implement a DTC-VC for an eMRTD-PC bound DTC based on the draft ICAO Technical Report on DTC [4] (or a later version) – taking into account required technical clarifications and corrections. Note: The ICAO Technical Report on DTC is still under preparation and addition additional biometrics is out of the scope of the first version of this Technical Report.
R2	The scenario shall support an on-the-fly border control procedure with an on-the-move biometric verification of the traveller, see the D4FLY Grant Agreement [1], and therefore additionally store a 2D face image, a 3D-face image, a template of an iris, and an image or a template for somatotype.
R3	The DTC system should allow the traveller to delete their DTC. Note: According to [3] this requires also a revocation of the DTC.
R4	The smartphone application may implement a DTC-PC and support the Active Authentication protocol according to ICAO Doc 9303 [2]. Note: This is an optional requirement as the D4FLY DTC focus is on the biometric on-the-move verification. This verification should prevent the usage of the smartphone application and therefore the DTC-VC of another person thanks to the additional biometrics. Therefore a DTC-PC (as required in [4]) is not necessarily needed in the D4FLY context.
R5	The smartphone application shall enable the traveller to control access to their DTC-VC data.
R6	The smartphone application shall be executable on a smartphone with an Android OS version , which has NFC capabilities and a touch screen.
R7	The smartphone application shall be installable using standard Android mechanisms. Note: The ISO/IEC 23220 installation and issuing mechanisms are still in an early drafting stage and the standardisation need for these mechanisms at all is under discussion. Therefore these mechanisms are not taken into consideration yet.
R8	The smartphone application shall have a User Interface, which is easy to use and can be interacted with using the touch screen of the smartphone.
R9	The KIOSK shall derive the DTC-VC in conformance with [4] from the traveller's ePassport.
R10	The KIOSK shall encrypt the DTC-VC in a way that allows to decrypt the DTC-VC only in collaboration with the traveller's smartphone application.
R11	The KIOSK shall have a User Interface, which is easy to use.
R12	The backend - triggered by the KIOSK - shall cryptographically sign the DTC-VC in conformance with [4].

In addition to these requirements, the concept for the smartphone application has been designed considering data protection, data privacy, IT security as well as ethical aspects. In the course of the project, all these aspects are continuously monitored and will be reviewed in a privacy, data protection, social and ethical impact assessment, which will be reported in separate public deliverables.

1.3.2 Output

This document serves as specification and description of processes, components and interfaces related to the smartphone application that is to be used in the prototype D4FLY system configuration for the automated border post scenario. As such it serves as input to the design and implementation of the smartphone application, the implementation of the system prototype for the automated border post scenario and as input for the planning and execution of the related field tests and demonstrations.

2 Scenario and User Perspective

This section provides a high level overview of the scenario and its procedures and components from the user point of view. It describes how the process in general will look like and what a user can expect when going through the scenario.

2.1 Scenario description

The scenario is made up of the following parts:

- The enrolment of the user and their DTC including the smartphone application prior to travelling. For this enrolment procedure the KIOSK is used.
- The backend which stores the encrypted DTC-VC and provides other services such as a signature service for the DTC-VC enrolment.
- The verification procedure of the user and their DTC while travelling, e.g. at the destination border. The smartphone application allows the traveller to control the access to his personal data, i.e. the DTC-VC. For this verification procedure a Border Control Station (BCSt) is used and for the on-the-move biometric verification a biometric corridor. While the traveller walks through this corridor biometric data is captured and compared with the additional biometric reference data stored in the DTC-VC.

2.2 User perspective

2.2.1 Data acquisition and enrolment procedure

Figure 2-1 illustrates the steps of the enrolment procedure for the D4FLY DTC solution from the user perspective. In the interest of readability the smartphone (application) and the backend are not shown and only the successful procedure is displayed. Please note that the order of the steps does not prescribe an order for the implementation, e.g. steps may be performed in parallel, but the figure only provides a schematic overview. The KIOSK leads the traveller through the process and requests certain actions from the traveller. The KIOSK will be equipped with

- an ePassport reader to retrieve the data required for the DTC-VC from the traveller's ePassport;
- a camera to take a high quality live face image to be matched with the traveller’s portrait image data stored on the ePassport chip;
- an NFC reader to personalize the smartphone application,
- the biometric capture devices to collect the additional biometric reference data which is stored in the DTC-VC.

The following preconditions must be fulfilled for the enrolment procedure:

- The traveller is in possession of a valid ePassport.
- The traveller has installed the smartphone application on their smartphone.
- The traveller has unlocked their smartphone and the smartphone application by means of a user authentication via fingerprint, pattern, PIN, or password.

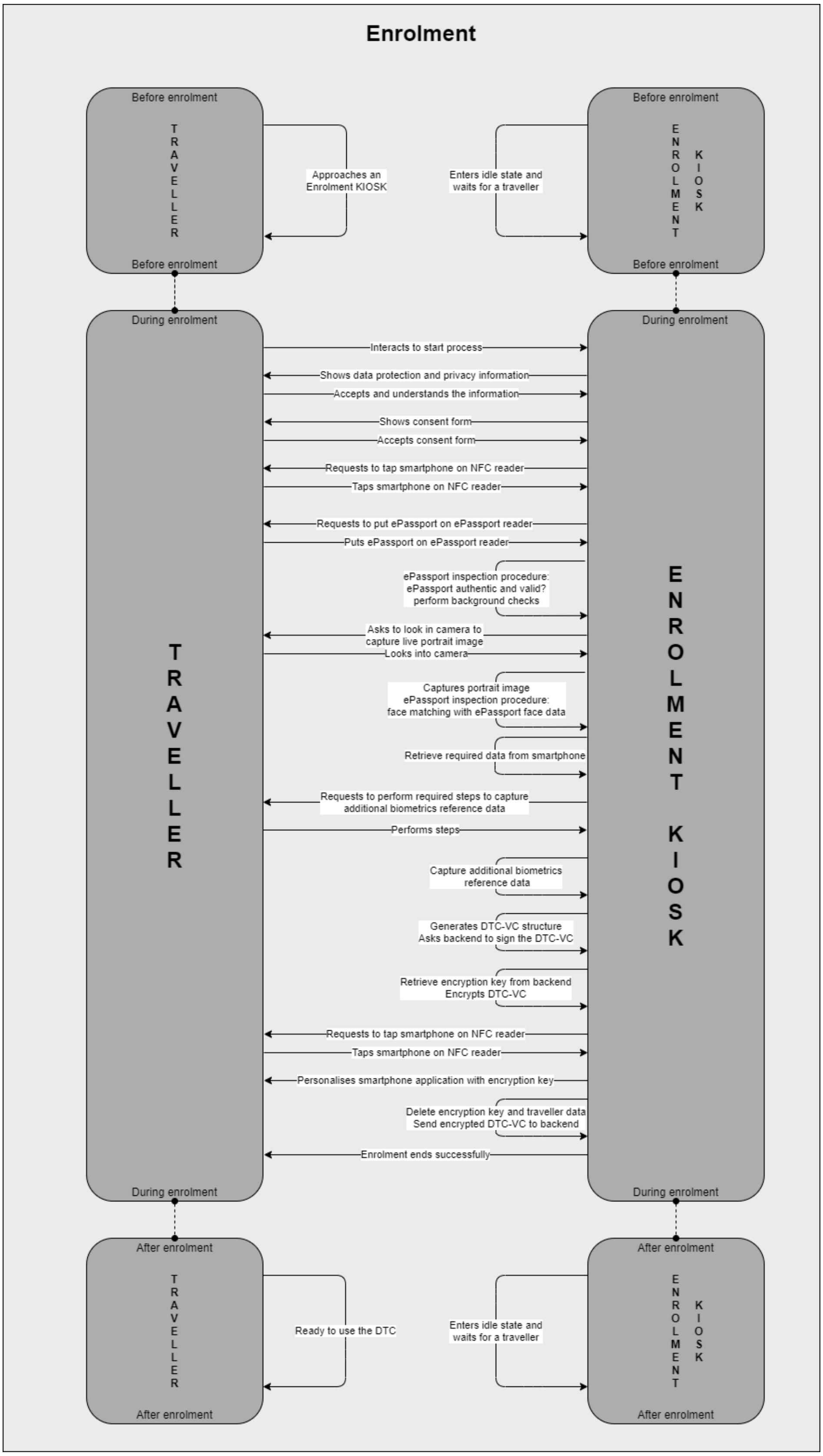

Enrolment
Before enrolment
TRAVELLER
Before enrolment
Approaches an Enrolment KIOSK
Enters idle state and waits for a traveller
Before enrolment
ENROLMENT KIOSK
Before enrolment
During enrolment
TRAVELLER
During enrolment
ENROLMENT KIOSK
Interacts to start process
Shows data protection and privacy information
Accepts and understands the information
Shows consent form
Accepts consent form
Requests to tap smartphone on NFC reader
Taps smartphone on NFC reader
Requests to put ePassport on ePassport reader
Puts ePassport on ePassport reader
ePassport inspection procedure: ePassport authentic and valid? perform background checks
Asks to look in camera to capture live portrait image
Looks into camera
Captures portrait image ePassport inspection procedure: face matching with ePassport face data
Retrieve required data from smartphone
Requests to perform required steps to capture additional biometrics reference data
Performs steps
Capture additional biometrics reference data
Generates DTC-VC structure Asks backend to sign the DTC-VC
Retrieve encryption key from backend Encrypts DTC-VC
Requests to tap smartphone on NFC reader
Taps smartphone on NFC reader
Personalises smartphone application with encryption key
Delete encryption key and traveller data Send encrypted DTC-VC to backend
Enrolment ends successfully
During enrolment
During enrolment
After enrolment
TRAVELLER
After enrolment
Ready to use the DTC
Enters idle state and waits for a traveller
After enrolment
ENROLMENT KIOSK
After enrolment

FIGURE 2-1: ENROLMENT PROCEDURE - OVERVIEW

2.2.2 Backend

The backend is responsible for two main tasks: cryptographically signing the DTC-VC data structure and storage of the traveller's enrolled data.

- **Signature service**
  The signature service implements a DTC Signer according to [4]. The DTC Signer makes use of its private key to sign the DTC-VC data structure. For its public key the Country Signing Certification Authority (CSCA), see [2], issues the DTC Signer certificate which is specified in [4]. The revocation status of the DTC Signer certificate can be checked by means of the CSCA's Certificate Revocation List (CRL).
- **Database**
  The database stores the traveller's enrolled data, i.e. the encrypted DTC-VC and an identifier generated in the enrolment process. In the verification process it will return the encrypted DTC-VC to the Border Control Station.

2.2.3 Inspection procedure

Figure 2-2 describes the interaction between the Border Control Station (BCSt) and the traveller in the verification procedure from the user perspective. In the interest of readability the smartphone (application) and the backend are not shown and only the successful procedure is displayed. Please note that the order of the steps does not prescribe an order for the implementation, e.g. steps may be performed in parallel, but only provides a schematic overview. The BCSt leads the traveller through the process using the smartphone application as interface to the traveller.

The following preconditions must be fulfilled for the verification procedure:

- The traveller has been enrolled for the DTC (D4FLY) solution.
- The traveller has unlocked their smartphone and the smartphone application by means of a user authentication via fingerprint, pattern, PIN, or password.

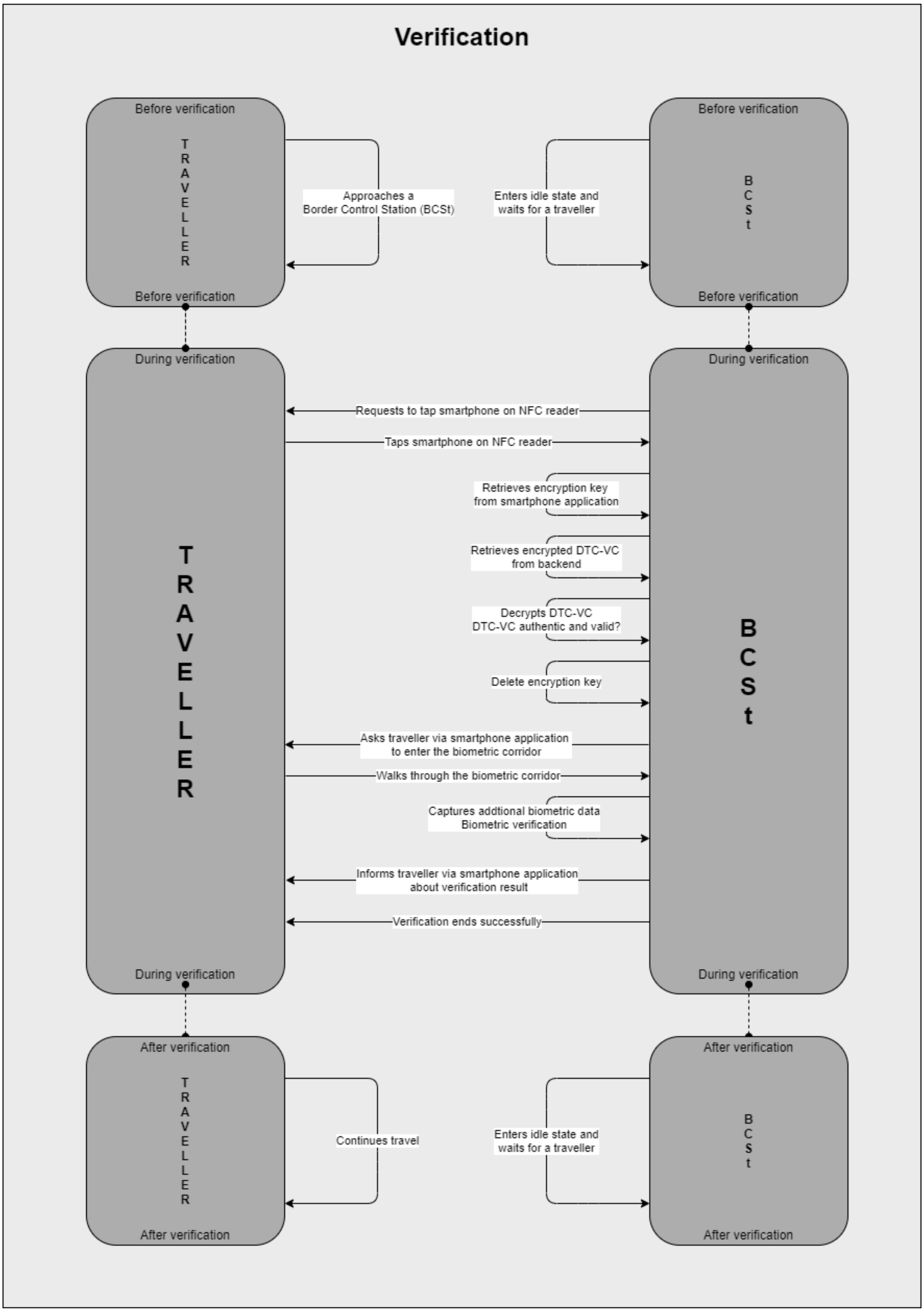

Verification
Before verification
TRAVELLER
Before verification
Approaches a Border Control Station (BCSt)
Enters idle state and waits for a traveller
Before verification
BCSt
Before verification
During verification
During verification
Requests to tap smartphone on NFC reader
Taps smartphone on NFC reader
Retrieves encryption key from smartphone application
Retrieves encrypted DTC-VC from backend
Decrypts DTC-VC
DTC-VC authentic and valid?
Delete encryption key
Asks traveller via smartphone application to enter the biometric corridor
Walks through the biometric corridor
Captures addtional biometric data
Biometric verification
Informs traveller via smartphone application about verification result
Verification ends successfully
TRAVELLER
BCSt
During verification
During verification
After verification
TRAVELLER
After verification
Continues travel
Enters idle state and waits for a traveller
After verification
BCSt
After verification

FIGURE 2-2: VERIFICATION PROCEDURE - OVERVIEW

3 Architecture, Components and Interfaces

This section describes the top-level architecture followed by the interfaces and the storage components for the smartphone application.

3.1 Top-level architecture

Figure 3-1 shows the top-level architecture. As already explained, the smartphone app acts as the physical carrier of a cryptographic key which is created and sent by the Enrolment-KIOSK (enrolment module) during the enrolment process. This key is then given to the Border Control Station (verification module) during the verification process. In this section the smartphone module will be described.

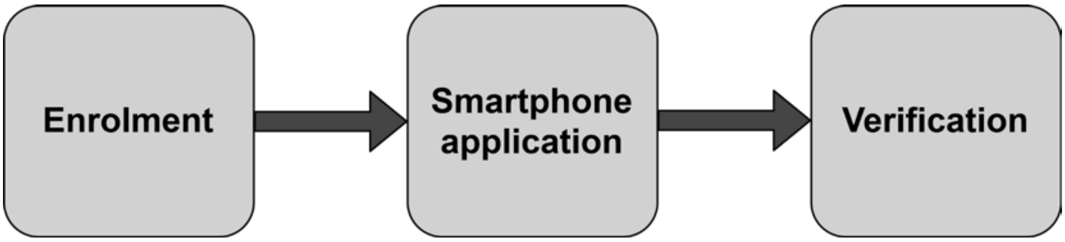


Figure 3-1: Top level architecture

3.2 Smartphone application

The following are the key points that the smartphone application can handle:

- The app stores the required cryptographic key securely and can extract and transmit it when the traveller needs to.
- It communicates (receiving and sending) the key only via NFC, thus reducing the opportunities for an attacker to eavesdrop on communications and adding security and privacy [9].
- The communication via NFC will also be encrypted to add further security to the key communication.
- The app utilizes TEE (Trusted Execution Environment) [10] of a smartphone for secure storage of the secret cryptographic key. This is described in Section 3.4.1.
- The app also provides option to securely store the required cryptographic key on smartphones that do not have a TEE. This is described in Section 3.4.2.
- The app does not store any other traveller sensitive data during the processes.

3.3 Interfaces to smartphone

The smartphone application handles two interfaces. The first interface interacts with the KIOSK to receive the cryptographic key after the enrolment by which the traveller’s data has been encrypted. This key is then stored securely by the smartphone. The second interface interacts with Border Control Station (BCSt) to provide this key for the data decryption and verification process.

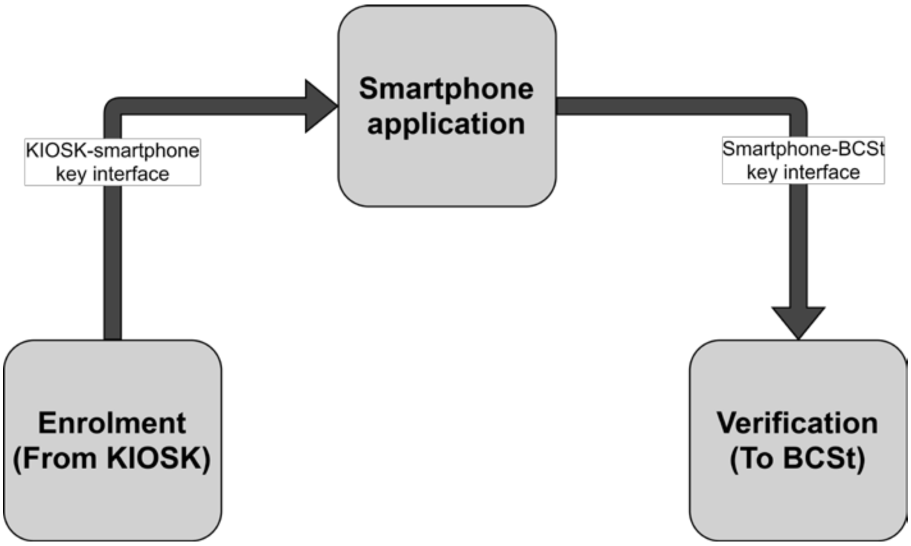


FIGURE 3-2: INTERFACES OF THE SMARTPHONE APPLICATION

Figure 3-2 shows the interfaces in the top-level architecture diagram (Figure 3-1). These interfaces will be discussed next.

3.3.1 KIOSK-Smartphone key interface

The smartphone connects to the KIOSK using NFC. The smartphone has to be tapped onto the NFC reader (present in the KIOSK) two times during the entire enrolment process per traveller. The graphic below (Figure 3-3) describes the interface process how the communication with the KIOSK works (only success case shown).

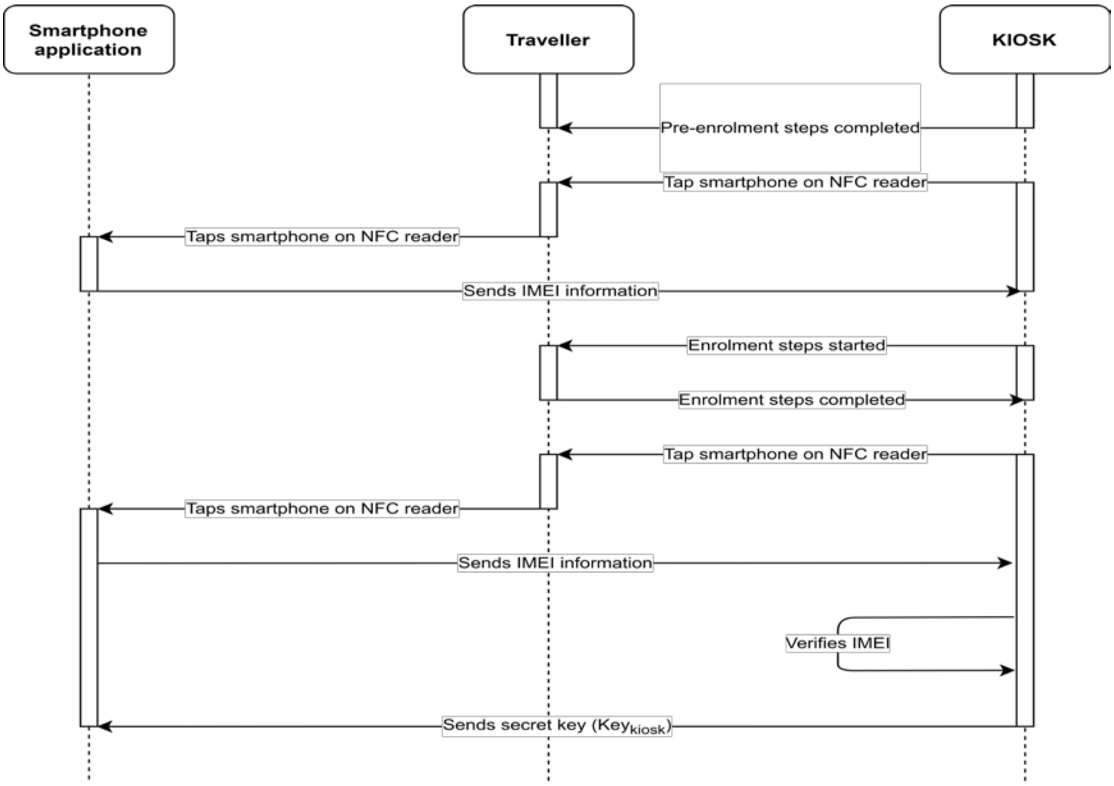

Smartphone application
Traveller
KIOSK
Pre-enrolment steps completed
Tap smartphone on NFC reader
Taps smartphone on NFC reader
Sends IMEI information
Enrolment steps started
Enrolment steps completed
Tap smartphone on NFC reader
Taps smartphone on NFC reader
Sends IMEI information
Verifies IMEI
Sends secret key (Key$_{kiosk}$)

FIGURE 3-3: INTERFACE SMARTPHONE APPLICATION - KIOSK

The description is as follows:

1. **Pre-enrolment steps completed:** The initial steps on the KIOSK like reading the information screen about data protection and privacy information, giving consent using the consent form, etc., have been completed.
2. **Tap smartphone on the NFC reader:** This is the first time the traveller is asked to tap the smartphone on the NFC reader. This is required to get the IMEI information from the traveller's smartphone in order to identify which smartphone is actually performing the enrolment.
3. **Taps smartphone on NFC reader:** The traveller taps the smartphone on NFC reader present at the KIOSK.
4. **Sends IMEI information:** The smartphone sends the IMEI number through NFC to the KIOSK. At the end of this step, the smartphone can be removed from the NFC reader, as it will be indicated on the kiosk screen.
5. **Enrolment steps started:** The core enrolment process starts.
6. **Enrolment steps completed:** The core enrolment process completes and data is ready and has been encrypted.
7. **Tap smartphone on NFC reader:** This is the second time the traveller is asked to tap the smartphone on the NFC reader. This is needed to again get the IMEI information from the traveller's smartphone. This IMEI information is compared to the IMEI information from the first tapping step to ensure the same smartphone is being used to complete the enrolment process as the one that was used to initiate the enrolment process.
8. **Taps smartphone on NFC reader:** The traveller taps the smartphone on the NFC reader present at the KIOSK.
9. **Sends IMEI information:** The smartphone again sends the IMEI number through NFC to the KIOSK.
10. **Verifies IMEI:** The KIOSK verified this IMEI against the IMEI from step 4.
11. **Sends cryptographic key (Key_{kiosk}):** The key is sent via a secure channel to the smartphone for storage.

3.3.2 Smartphone-BCSt key interface

The smartphone connects to the Border Control Station (BCSt) using the NFC interface. Here the smartphone only connects once to transmit the stored key to the BCSt. The graphic below (Figure 3-4) describes the interface process for communication with the BCSt (only success case shown).

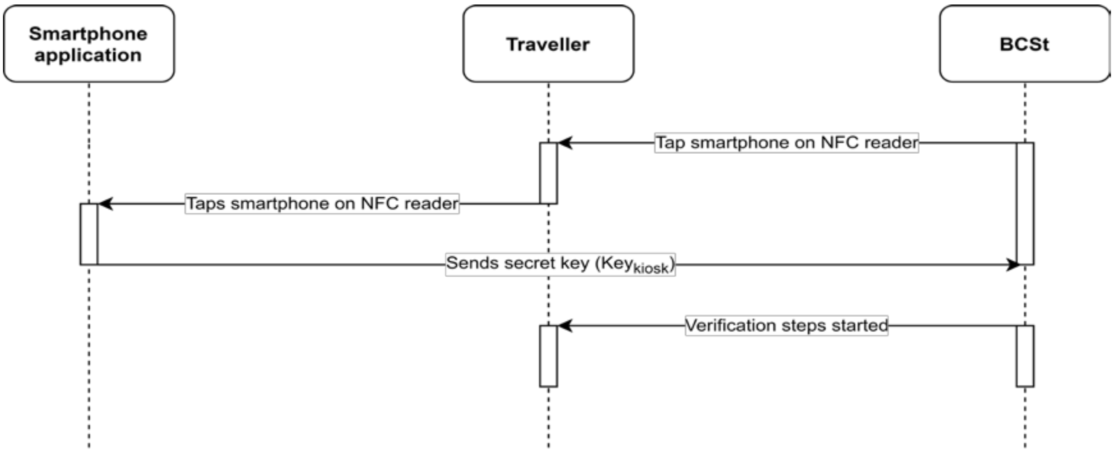

Smartphone application
Traveller
BCSt
Tap smartphone on NFC reader
Taps smartphone on NFC reader
Sends secret key (Key$_{kiosk}$)
Verification steps started

FIGURE 3-4: INTERFACE SMARTPHONE APPLICATION – BORDER CONTROL STATION

The description is as follows:

1. **Tap smartphone on NFC reader:** The instruction near the BCSt will direct the traveller to tap the smartphone on the NFC reader when the traveller approaches the entrance of the biometric corridor.
2. **Taps smartphone on NFC reader:** The traveller taps the smartphone on NFC reader present near the BCSt entry point.
3. **Sends key (Key$_{kiosk}$):** The smartphone sends the stored encryption/decryption key through NFC.
4. **Verification steps started:** The further verification steps start for the traveller.

3.4 Key storage on smartphone

The key storage on the smartphone depends upon whether the smartphone has a TEE (Trusted Execution Environment) or not. Hence, the smartphone application module in Figure 3-1 could be divided up further, in smartphones with TEE and smartphones without TEE. These two categories will be described next.

3.4.1 Smartphones with TEE

A trusted execution environment (TEE) is a secure, integrity protected processing environment, consisting of processor, memory and storage capabilities. It is isolated from the standard processing environment, where the device operating system and applications run [11]. This environment is well suited to securely store information, which shall be accessible only by the user.

The steps being performed are as follows:

1. **For the enrolment steps**
   a. The key that is generated in the KIOSK (called Key$_{kiosk}$) will be received by the smartphone through the KIOSK-Smartphone key interface at the end of the enrolment process.
   b. The smartphone application will generate encryption/decryption key inside the TEE (Key$_{tee}$) which will be used to encrypt the received Key$_{kiosk,}$.The result is the encrypted KIOSK key called Key$_{kiosk.enc}$.
   c. The Key$_{kiosk.enc}$ will then be stored in the smartphone application in a secure area, which can only be accessed by this smartphone app.

The encryption/decryption key$_{tee}$ will always remain inside TEE and will never leave it. The Key$_{kiosk.enc}$ will always be stored in secure area and cannot be accessed from outside.

2. **For verification steps**
    a. The smartphone application will use TEE for decryption of Key$_{kiosk.enc}$ with the stored Key$_{tee}$ by TEE.
    b. TEE will decrypt and give Key$_{kiosk}$.
    c. The smartphone application will then send this Key$_{kiosk}$ to BCSt through Smartphone-BCSt key interface.

    The key Key$_{kiosk}$ can be sent through Smartphone-BCSt key interface only after a positive verification of traveller using fingerprint authentication or authentication with pattern/pin/password on their smartphone.

3.4.2 Smartphones without TEE

The devices that do not have a TEE can still be used to securely store the key from KIOSK (Key$_{kiosk}$). This can be done by generating an internal key (called HW$_{hash}$) based on a number of specific hardware information, which is unique for one specific smartphone. By this internal key, the Key$_{kiosk}$ can be further encrypted and stored in private memory of the application. The mechanism of binding the hardware information cryptographically to the encryption key provides additional security, as this key cannot be used on another smartphone, in the unlikely case, that it could be copied by someone to another smartphone.

The steps being performed are as follows:

1. **Enrolment steps**
    a. The key from KIOSK (called Key$_{kiosk}$) will be received by the smartphone through the KIOSK-Smartphone key interface towards the end of the enrolment process (same as in the case using a smartphone with a TEE).
    b. The smartphone application will collect smartphone hardware information and execute a hash function on it (HW$_{hash}$).
    c. The smartphone application will then encrypt the Key$_{kiosk}$ with HW$_{hash}$. The result will be encrypted KIOSK key called Key$_{kiosk.enc}$.
    d. The Key$_{kiosk.enc}$ will then be securely stored in the smartphone application's private memory.

    The Key$_{kiosk.enc}$ will always be stored inside the private memory of the smartphone application which can only be accessed by the application and nowhere from outside.

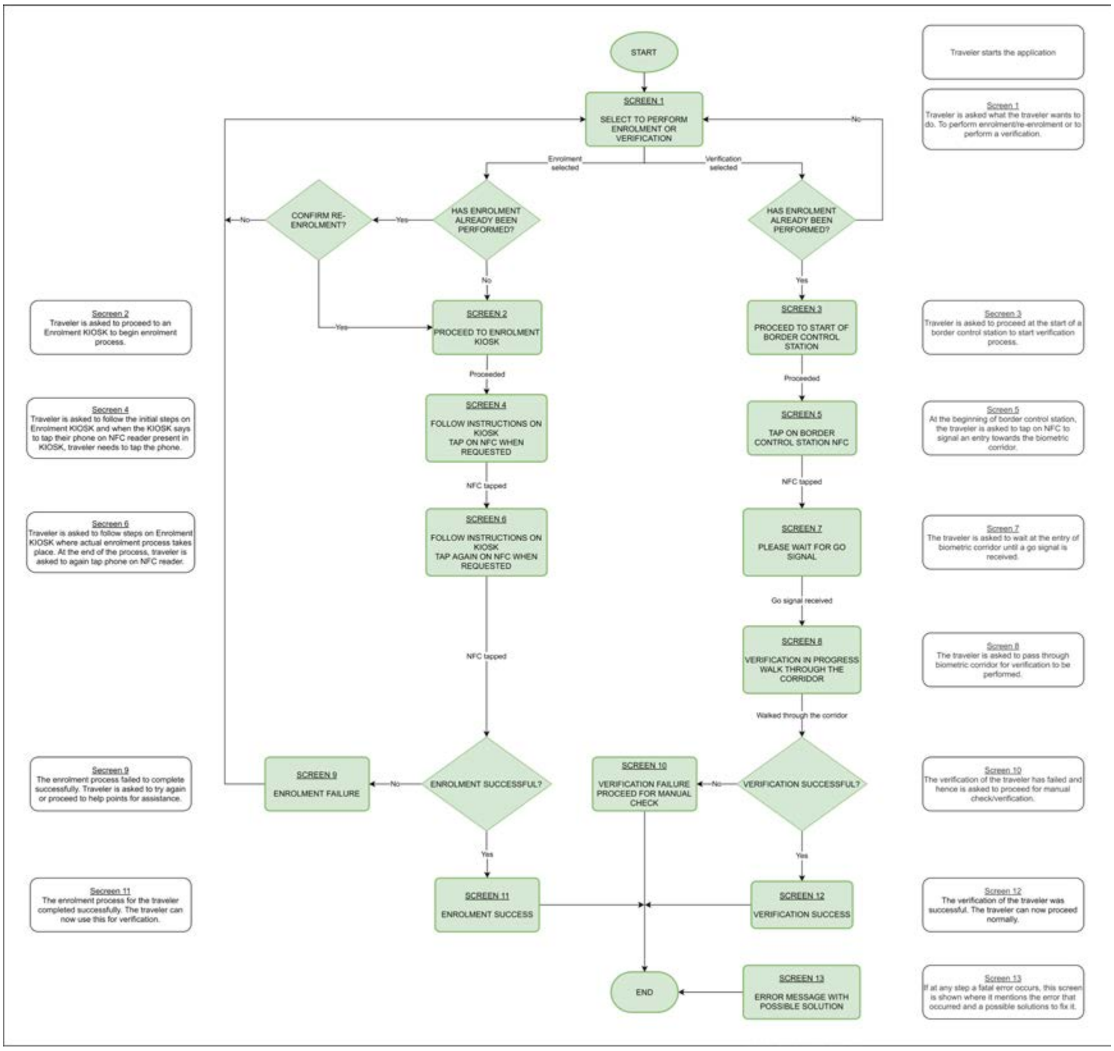
2. **Verification steps**
    a. The smartphone application will collect smartphone hardware information and generate HW$_{hash}$ again.
    b. The smartphone application will then fetch Key$_{kiosk.enc}$ from application's private memory and decrypt it with HW$_{hash}$. This will result in the Key$_{kiosk,}$ which then is sent to BCSt.

    The key Key$_{kiosk}$ can be sent through Smartphone-BCSt key interface only after a positive verification of traveller using fingerprint authentication or authentication with pattern/pin/password on their smartphone.

The HW_{hash} will not be stored anywhere but only created and used during encryption of Key_{kiosk} and decryption of $Key_{kiosk.enc}$.

4 USER INTERFACE

The smart phone application is the client application that the traveller interacts with. Below (Figure 4-1) is a graphical description of all the screens that take input or give output to the traveller.


START
SCREEN 1
SELECT TO PERFORM ENROLMENT OR VERIFICATION
Enrolment selected
Verification selected
HAS ENROLMENT ALREADY BEEN PERFORMED?
CONFIRM RE-ENROLMENT?
Yes
No
No
Yes
SCREEN 2
PROCEED TO ENROLMENT KIOSK
Proceeded
SCREEN 4
FOLLOW INSTRUCTIONS ON KIOSK
TAP ON NFC WHEN REQUESTED
NFC tapped
SCREEN 6
FOLLOW INSTRUCTIONS ON KIOSK
TAP AGAIN ON NFC WHEN REQUESTED
NFC tapped
ENROLMENT SUCCESSFUL?
No
SCREEN 9
ENROLMENT FAILURE
Yes
SCREEN 11
ENROLMENT SUCCESS
HAS ENROLMENT ALREADY BEEN PERFORMED?
No
Yes
SCREEN 3
PROCEED TO START OF BORDER CONTROL STATION
Proceeded
SCREEN 5
TAP ON BORDER CONTROL STATION NFC
NFC tapped
SCREEN 7
PLEASE WAIT FOR GO SIGNAL
Go signal received
SCREEN 8
VERIFICATION IN PROGRESS
WALK THROUGH THE CORRIDOR
Walked through the corridor
VERIFICATION SUCCESSFUL?
No
SCREEN 10
VERIFICATION FAILURE
PROCEED FOR MANUAL CHECK
Yes
SCREEN 12
VERIFICATION SUCCESS
END
SCREEN 13
ERROR MESSAGE WITH POSSIBLE SOLUTION

Traveler starts the application

Screen 1
Traveler is asked what the traveler wants to do. To perform enrolment/re-enrolment or to perform a verification.

Secreen 2
Traveler is asked to proceed to an Enrolment KIOSK to begin enrolment process.

Secreen 3
Traveler is asked to proceed at the start of a border control station to start verification process.

Secreen 4
Traveler is asked to follow the initial steps on Enrolment KIOSK and when the KIOSK says to tap their phone on NFC reader present in KIOSK, traveler needs to tap the phone.

Screen 5
At the beginning of border control station, the traveler is asked to tap on NFC to signal an entry towards the biometric corridor.

Secreen 6
Traveler is asked to follow steps on Enrolment KIOSK where actual enrolment process takes place. At the end of the process, traveler is asked to again tap phone on NFC reader.

Screen 7
The traveler is asked to wait at the entry of biometric corridor until a go signal is received.

Screen 8
The traveler is asked to pass through biometric corridor for verification to be performed.

Secreen 9
The enrolment process failed to complete successfully. Traveler is asked to try again or proceed to help points for assistance.

Screen 10
The verification of the traveler has failed and hence is asked to proceed for manual check/verification.

Secreen 11
The enrolment process for the traveler completed successfully. The traveler can now use this for verification.

Screen 12
The verification of the traveler was successful. The traveler can now proceed normally.

Screen 13
If at any step a fatal error occurs, this screen is shown where it mentions the error that occurred and a possible solutions to fix it.

FIGURE 4-1: SMARTPHONE APPLICATION SCREEN FLOW

The screens are interactive and assist in giving and taking information from the traveller. The interactive user procedure consists of the following steps (in regards to the screens):

1. **Enrolment**
   i. **Start screen (Screen 1):** The first screen (after app start-up) asks the traveller to choose whether the traveller wants to enrol/re-enrol or verify. Here, the traveller selects enrol/re-enrol option. If traveller had already performed enrolment, then a re-enrolment takes place. Before re-enrolment, traveller is asked to confirm whether they want to proceed or not since this will delete the last enrolment.

ii. **Proceed to Enrolment KIOSK (Screen 2):** Traveller is asked to find and proceed to an Enrolment KIOSK to perform enrolment.

iii. **Initial instructions on KIOSK and tap NFC (Screen 4):** After traveller proceeds to an Enrolment KIOSK, app instructs the traveller to interact with the KIOSK and follow the initial steps. The user interface of the KIOSK will ask the traveller to tap the smartphone onto the NFC reader present in the KIOSK. At this point, the traveller taps the smartphone on the NFC reader to initiate a connection between smartphone application and Enrolment KIOSK.

iv. **Further instructions on KIOSK and tap NFC (Screen 6):** After the connection has been established between the smartphone application and the Enrolment KIOSK, the app instructs the traveller to follow further instructions on the KIOSK. Towards the end of the enrolment process the KIOSK UI directs the traveller to tap the smartphone onto the NFC reader a second time. At this point, the traveller taps the smartphone on the NFC reader to receive the encryption key on smartphone and complete the enrolment process.

v. **Enrolment success (Screen 11):** If the entire process completes successfully and the key gets successfully transferred to the smartphone, this screen is shown denoting the enrolment process as being completed successfully.

vi. **Enrolment failure (Screen 9):** If a problem occurs in the process or the key transfer, this screen is shown denoting the enrolment process failed to complete successfully.

2. **Verification**

i. **Start screen (Screen 1):** The first screen (after app start-up) asks the traveller to choose whether the traveller wants to enrol/re-enrol or verify. Here, the traveller selects the verify option. This option will only work if a successful enrolment has already been performed.

ii. **Proceed to Border Control Station (BCSt) (Screen 3):** The app asks the traveller to proceed towards the entry of a Border Control Station where the verification process will take place.

iii. **Tap on BCSt NFC (Screen 5):** At the start of the BCSt area, the traveller is asked by the app to tap on the NFC reader. This activity is also used by the system as a start signal for the further verification process with the traveller being ready to enter the biometric corridor.

iv. **Wait for GO signal (Screen 7):** The traveller now has to wait until a GO signal is displayed on the app. As soon as it is displayed, the traveller can start walking through the biometric corridor.

v. **Verification in progress (Screen 8):** The app tells the traveller to keep walking through the biometric corridor where the verification will take place.

vi. **Verification success (Screen 12):** If the verification succeeded, this screen is shown and the traveller can proceed normally.

vii. **Verification failure (Screen 10):** If the verification failed, this screen is shown and the traveller is asked to follow the border guard's instruction and move to a manual verification check point.

5 EVALUATION

5.1 Security and privacy

For security and privacy of the traveller's data, standard ICAO security mechanisms [2], [4] and additional mechanisms are applied:

- The DTC Virtual Component (DTC-VC) is cryptographically signed in order to preserve the integrity of the data and as proof its origin.
- The DTC Virtual Component (DTC-VC) is stored encrypted with a key under the control of the traveller in his smartphone application.
- The encryption key is stored on the traveller's smartphone in an encrypted way using a TEE. Only if no TEE is available on the smartphone, alternative software solutions are used.
- The encryption key is transferred from the smartphone application to the Border Control Station via a secure encrypted channel.
- The encryption keys are deleted if not used any longer.
- A Border Control Station could verify that the smartphone application is authentic by means of the optional Active Authentication protocol.
- A smartphone application in contrast to an ePassport has a user interface which allows to implement user consent before releasing any data.

5.2 Performance

The evaluation with respect to the transaction time at border control will be performed in the context of the D4FLY field tests and is subject to Deliverable D6.7.

5.3 Usability

The evaluation with respect to the usability will be performed in the context of the D4FLY field tests and is subject to Deliverable D6.7.

5.4 Conformance to standards

The DTC Virtual Component (DTC-VC) data structure is in principle in conformance with the ICAO draft specification [4] which may need further clarifications and corrections. This conformance statement includes the security mechanisms for the DTC-VC, i.e. the cryptographic signature for passive authentication. The additional biometrics is not yet in the scope of the ICAO DTC draft specification, but the ICAO recommendation to use an encryption for additional access control to this data [2] is followed. The transmission protocols for the DTC-VC are out of the scope of the ICAO draft specification.

For the DTC Physical Component (DTC-PC) no draft standard is available yet, but according to the optional D4FLY requirement the ICAO Doc 9303 [2] Active Authentication protocol as suggested in [4] is applied.

For the installation and issuance of the smartphone application standard Android mechanisms are preferred over the mechanisms specified in the ISO/IEC 23220 drafts [6] for the following reasons. The ISO/IEC 23220 drafts are still in an early stage and not yet stable, but major changes are expected. In addition the need for standardisation of these mechanisms itself is still under discussion.

5.5 Future Work

In the first version of the solution only data required at every border control is stored in the DTC-VC and for this reason there is no need for a selective disclosure mechanism. If further data are linked to the DTC-VC such as visa or other country specific data a selective disclosure mechanism is required.

Implementing the DTC-PC is an optional D4FLY requirement as the biometric on-the-move verification is supposed to be good enough to prevent any look alike fraud and re-using the smartphone application of another person. For this reason the DTC-PC may be implemented in the future.

Future work may include additional enrolment steps such as requesting the deletion of the DTC by the traveller – including its revocation according to [4].

REFERENCES

[1] European Commission Research Executive Agency, Grant Agreement Number 833704 — D4FLY

[2] International Civil Aviation Organization (ICAO), Doc 9303 *Machine Readable Travel Documents* Seventh Edition, 2015 [viewed 2020-04-27]. Available at https://www.icao.int/publications/pages/publication.aspx?docnum=9303

[3] International Civil Aviation Organization (ICAO), *NTWG Subgroup Policy Paper Digital Travel Credentials (DTC)*, Version 4.4, May 8 2020

[4] International Civil Aviation Organization (ICAO), *Technical Report Digital Travel Credentials (DTC)*, Version 1.0, May 12, 2020

[5] ISO/IEC DIS 18013-5:2020, *Personal identification ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application*, Draft International Standard, 2020

[6] ISO/IEC 23220, *Cards and security devices for personal identification — Building blocks for identity management via mobile devices*, work in progress

[7] ISO/IEC JTC 1 / SC 17 / WG3 TF5 N0285, Veridos comments on ICAO Technical Report Digital Travel Credentials (DTC), Version 0.08, May 2020

[8] PROTECT Pervasive and UseR Focused BiomeTrics BordEr ProjeCT project, see http://projectprotect.eu/

[9] https://www.pcworld.com/article/2938520/nfc-security-3-ways-to-avoid-being-hacked.html

[10] https://www.trustonic.com/news/technology/what-is-a-trusted-execution-environment-tee/

[11] https://www.embedded.com/trusted-execution-environments-on-mobile-devices/

LIST OF FIGURES

LIST OF TABLES