

## Security Sensitivity Statement

This form is related to the Security Sensitivity Assessment procedure which will assure that no sensitive information will be included in the publications and deliverables of the MobilePass project.

Security sensitive information means here all information in whatever form or mode of transmission that is classified by Council Decision on the security rules for protecting EU classified information (2011/292/EU) and all relevant national laws and regulations. The information can be already classified, or such that it should be classified.

In practice the following criteria is used:

- Information is already classified
- Information may describe shortcomings of existing safety, security or operating systems
- Information is such, that it might be misused.
- Information that can cause harm to
  - o European Union
  - o a Member State
  - o society
  - o industry and companies
  - o third country
  - o citizen or an individual person of a country.

### Publication identification

*Title of the Publication:* **Deliverable D 1.3 Vision and Requirements of the Future**

*Authors (Name / Affiliation):*

Christoph Weiß AIT

*Contributors authors:*

Markus Hofstätter	AIT
Martin Fletzer	AIT
Bernhard Strobl	AIT
Subashini Aleti	AIT
Beatrice Ganster	AIT
Mircea Radan	RBP
Eduardo Monari	PhG
Kai Nickel	Videmo

*Type of the publication:*

This is a deliverable

- WP1/T1.3
- Dissemination level: PU

**Please fill in below:**

*This is:* *pre-assessment*  *final assessment*



List the input material used in the publication/deliverable:

1. See Annexes, pg. 83

List the results developed and presented in the publication/deliverable:

1. The output of this task will be a functional design supported by preliminary interface definitions using:
  - a. a "vision" of a future mobile border control device
  - b. a technical architecture (hardware and software)
  - c. a description of an "ideal mobile device" and more detailed requirements

The draft publication

is attached to this statement

can be found in link:

[https://portal.ait.ac.at/sites/MobilePass/WP%201%20User%20Requirements%20System%20Design/Forms/AllItems.aspx?RootFolder=%2fsites%2fMobilePass%2fWP%201%20User%20Requirements%20System%20Design%2fd%201\\_3&FolderCTID=&View={3D538D59-D8C6-489C-9370-8FFFD1CF2F09}](https://portal.ait.ac.at/sites/MobilePass/WP%201%20User%20Requirements%20System%20Design/Forms/AllItems.aspx?RootFolder=%2fsites%2fMobilePass%2fWP%201%20User%20Requirements%20System%20Design%2fd%201_3&FolderCTID=&View={3D538D59-D8C6-489C-9370-8FFFD1CF2F09})


**This publication does not include any data or information that could be interpreted as security sensitive.**

True

Not sure

*If not sure, please specify what are the material / results that you are not sure if they are security sensitive? Why?*

Date 29.12.2014

Signature of the Responsible Author: 

**Comments of the SSA Group**

The publication can be published as it is.

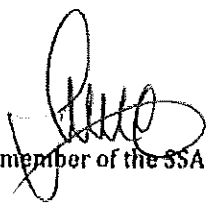
Before publication the following modifications are needed:

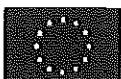
-  
-

Date: 29.12.2014

On behalf of the SSA Group:

George ION

Signature of a member of the SSA Group 



## Vision and Requirements of the Future

Version 0.9, 30.12.2014

### Project

### MobilePass

Project Reference: Grant agreement no. 608016  
 Project Short Name: MobilePass  
 Call: FP7-SEC-2013-3-2-3  
 Funding Scheme: Capacity Project  
 Project web-site: [www.mobilepass-project.eu](http://www.mobilepass-project.eu)



## Deliverable D 1.3

## Vision and Requirements of the Future

### Document

Deliverable No.:	1.3	Due Date:	2014-31-12
Issued by Partner:	AIT	Actual Date:	2014-30-12
WP/Task:	WP1/T1.3	Pages:	89
Confidentiality Status:	PU		

### Authors

	Name	Organization/Unit
Main Author	Christoph Weiß	AIT
Contributing Author(s)	Markus Hofstätter	AIT
	Martin Fletzer	AIT
	Bernhard Strobl	AIT
	Beatrice Ganster	AIT
	Mircea Radan	RBP
	Eduardo Monari	FhG
	Philipp Mayr	G&D
	Kai Nickel	Videmo
	Irma van de Ploeg	UNU-MERIT
	Sanneke Kloppenburg	
	José Miguel Diestre Casaus	INDRA

### Approval

	Name	Organization/Unit
Technical Reviewer	Vuk Krivec	Freelancer/CEN
Language Reviewer	Subashini Aleti	AIT
Security Assessment	George Ion	RBG

### Authorization

	Name	Organization/Unit
Project Officer	Andrei Lintú	European Commission

### File

MobilePass Deliverable D 1 3\_Final.docx

## Document History

Document Information		Chapters affected	Description of change	Author	Document Status
Date	Version				
19.10.2014	0.1	all	Initial Version	Bernhard Strobl	In progress
05.11.2014	0.2	4	Added system architecture chapter	Markus Hofstätter	In progress
26.11.2014	0.3	(new) 3,4	Added chapters Overview and Requirements	Bernhard Strobl	In progress
10.12.2014	0.3	3	Improved Chapter requirements	Bernhard Strobl	In progress
11.12.2014	0.3	5	Added Chapter Architecture	Christoph Weiß	In progress
12.12.2014	0.4	4	Comments on Face Verification	Kai Nickel	In progress
12.12.2014	0.5	all	Overall comments and description of vision on face and fingerprint capturing process and image enhancement	Eduardo Monari	In progress
19.12.2014	0.5	3	Added Potential data protection issues and Potential social/ethical issues in requirements list	Irma van de Ploeg, Sanneke Kloppenburg	In progress
21.12.2014	0.6	4, Backend Interface	Added Backend interface content	José Miguel Diestre Casaus	In progress
22.12.2014	0.7	4	Consolidated and reworked Chapter 4 (shifted detailed specifications to Deliverable D 1.4)	Christoph Weiß	In progress
28.12.2014	0.8	1,4.2, 4.3, 4.4, Annex 5.1, 5.2	Final amendments, clarifications, illustrations	Bernhard Strobl	Pre-final
30.12.2014	0.9	all	Included Language Review, Included Technical Review Comments	Bernhard Strobl	Final

## Document Reviews

The following table gives an overview of all document reviews.

Date	Version reviewed	Remarks, Corrections	Reviewer	New Status
28.12.2014	0.8	Technical Review; see document "Comments D1.3_V0.8-Krivec"	Vuk Krivec	Pre-Final-technical reviewed
29.12.2014	0.8	Language Review	Subashini Aleti	Pre-final-proof-read
29.12.2014	0.8	Security Sensitive Assessment	George Ion	Final

## Table of content

Table of content .....	4
1 Introduction.....	6
1.1 Purpose of the document.....	6
1.2 Document scope.....	6
1.3 Description of work for this deliverable.....	6
2 Distributed Architecture Overview .....	7
2.1 Introduction.....	7
2.2 Constitutive elements .....	7
2.3 Device compositions.....	8
2.3.1 One Appliance Concept .....	8
2.3.2 Distributed Appliance Concept (two elements).....	9
2.3.3 Distributed Appliance Concept.....	10
2.4 Data Processing Architecture .....	10
2.4.1 Appliance Concept.....	10
2.4.2 MobilePass Appliances .....	11
2.4.3 Distributed MobilePass Appliance Concept (several elements) .....	13
2.4.4 Embedding in national environments .....	14
3 Requirements .....	16
3.1 Requirements capturing process and structure.....	16
3.2 ICAO Requirements (ABC Guidelines similarities).....	17
3.3 Requirements List (defined by MobilePass).....	18
4 Device Vision and Architecture .....	42
4.1 Overview.....	43
4.2 Device Components and functions.....	43
4.2.1 Camera system .....	44
4.2.2 Finder Display .....	46
4.2.3 Illumination .....	46
4.2.4 Central Processing Unit (CPU) .....	47

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

4.2.5	Trusted Platform Module for platform integrity.....	50
4.2.6	Ideal Algorithm Integration .....	51
4.3	Ergonomic concept.....	52
4.3.1	Handling comfort.....	52
4.3.2	MRZ capture .....	54
4.3.3	Fingerprint capture.....	57
4.3.4	Face capture .....	63
4.4	MobilePass Full-Page Passport Scanner Components and Functions.....	67
4.4.1	Device Components.....	68
4.4.2	Device Functions.....	68
4.5	Device Operating Modes.....	70
4.5.1	Stand Alone Operation .....	72
4.5.2	Scanner Function.....	72
4.5.3	External Interfaces.....	73
4.6	Backend Interface.....	74
4.6.1	Central System.....	75
4.6.2	Operational record .....	78
4.7	Security Concept.....	83
4.7.1	Trusted Boot .....	83
4.7.2	Device Authentication .....	84
5	Annex.....	85
5.1	References.....	85
5.2	Databases .....	86
5.2.1	Schengen Information System (SIS) .....	86
5.2.2	Visa Information System (VIS) .....	86
5.2.3	INTERPOL.....	87
5.2.4	Entry Exit Database (EES) .....	88
5.2.5	Registered Traveller Programme (RTP) .....	88

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

**1 Introduction****1.1 Purpose of the document**

This document serves three purposes. Firstly, it should give an overview about the system architecture using distributed appliances. Secondly, the document further exploits on the “ideal mobile device” and more detailed requirements, which will be presented in a structured list. Based on the previous work in Deliverable 1.1, a “vision” of a future mobile border control device will be formulated, taking into account that the envisioned device should work in a network environment and exchange information with other devices and databases. This device is embedded in a heterogeneous set of different devices with different functionalities. Thirdly, a technical architecture (hardware and software) will complement the vision.

It is intended to be read by technical people and border guards working in the field of border control. However, some preliminary high level specifications on technical interfaces and an overall architecture are also included.

**1.2 Document scope**

The document starts with an architectural overview for a set of distributed devices and defines constitutive elements and appliances. Further, the document formulates a “vision” for the MobilePass device and the passport verification process applied at borders as well as concepts for future identity check procedures. The process of gathering data (MRZ, fingerprints, facial images, RFID readings, UV/IR passport images), database checks and necessary user interfaces are described. Also, the concept of merging the integrated device with all the required components is presented. The architecture as well as the design is based on the idea that maximum flexibility is given for future application development.

More detailed interface definitions will be included in deliverable 1.4

**1.3 Description of work for this deliverable**

The Vision and requirements for future devices as described in this document formulates a vision of mobile device for passport control needed in the future. This deliverable also includes a list of all requirements for a mobile device and describes a system architecture taking as many end-user requirements into account as possible.



## 2 Distributed Architecture Overview

### 2.1 Introduction

This chapter should give an overview about the complete mobile passport verification/control scenario. It focuses on different solutions in such scenarios, describing monolithic and distributed solutions with one or several appliances. For better understanding in the following sections each element is introduced. The overview will further describe future device compositions and the overall architecture.

### 2.2 Constitutive elements

The MobilePass system is designed as a composition of several distributed devices. Therefore, it is necessary to describe on which physical and logical element (appliance) the functionalities are provided.



Figure 1: Constitutive elements.

#### Appliance:

An appliance is a combined system of hardware and software elements performing one or several functionalities. For handheld systems the device's overall geometry, shape, size, weight, stability, grip, etc. are crucial for law enforcement officers operating in the field in various environmental conditions.

#### Process:

An action carried out on one appliance using hardware and data elements with the use of an algorithm leading to more aggregated or transformed data. It could be an example of capturing of biometric samples, a 1:1 verification or 1:N identification process.

#### Data:

Data is a set of qualitative or quantitative variables in digital representation. In case of data elements higher structures are formed (e.g. a biometric sample); the integrity of data is important and should be assured. If the data is related to identities, special data protection rules should be applied. If data leaves one appliance, encryption of data is necessary.

#### Database:

A database is an organized collection of data for verification and identification purposes. It should have (at least) one access point and should be located on (at least) one appliance.

#### Data Transmission:

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

It might be necessary that the data is transmitted via network (wireless or cable) between appliances. Protocols should be introduced that ensures integrity, delivery, security and access of data from the right appliance.

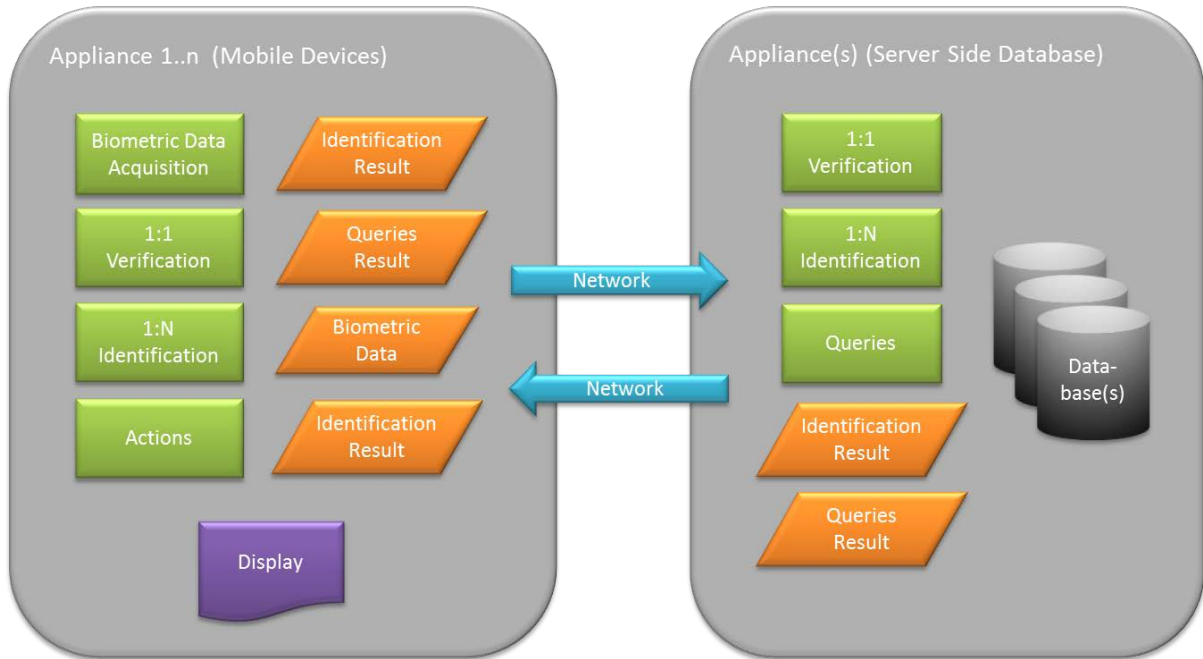


Figure 2: Different appliances for mobile devices communicating with a server side data base

The intention of the proposed semantics should ease the work and mutual understanding between project partners, particularly, for better communication between border guards, technicians and legal people. Also, it should be used to describe the demonstrator designed in later project phases.

**2.3 Device compositions**

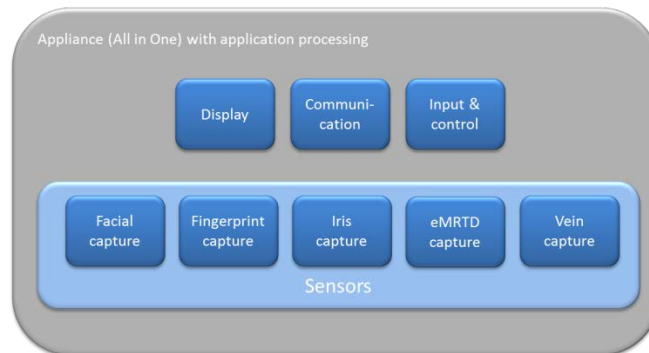
Since, more and more wearable computing devices are being launched (intelligent glasses, intelligent watches, smart phones) the need of a physically single integrated device is eliminating. It has to be taken into account that all device compositions have to operate in an interoperable way with several remote databases containing international and national information about travellers. There are scenarios where offline databases and other identification applications for law enforcement agencies are also required. However, MobilePass will focus on distributed border control situations and data exchange between central and local databases which are of high importance that has access to most recent passenger/traveller information. It is also planned to design the MobilePass data handling concept in a way to fit for local (stand-alone) applications.

**2.3.1 One Appliance Concept**

The classical approach consists of a device with a single physical body which contains all the processing unit/elements such as display, communication, input, control, and the sensors (all-in-one mobile solution) see Figure 3.

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

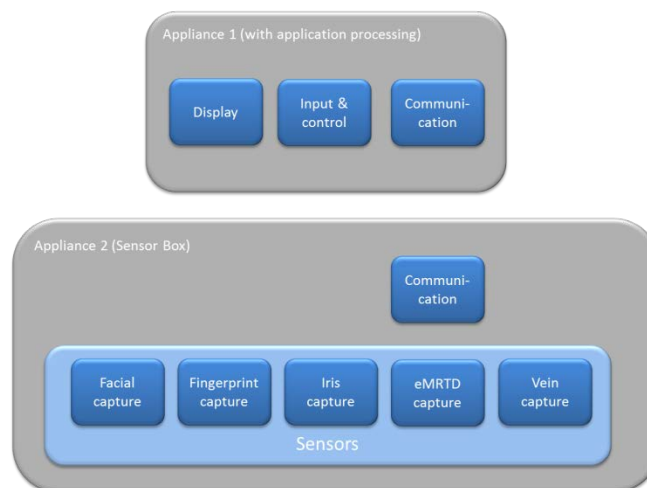


*Figure 3: All-in-one mobile system, containing different elements and biometric sensors*

The above figure shows a (hypothetical) All-in-One system which encompasses all sensors on-board including face capturing, fingerprint capturing, eMRTD (and more which are not in the Scope of MobilePass). Due to technical constraints (battery life, size, ergonomics, etc.) such a device is not available in the market today. Based on current state of the art on related technologies, such products might not be available in near future. However, there are already existing devices including facial capture, fingerprint capture and eMRTD capture functionalities.

**2.3.2 Distributed Appliance Concept (two elements)**

Considering ergonomic aspects (handling in combination with the cooperating traveller) it is feasible that functionality is split among different (e.g. two) appliances. This concept includes physical bodies that only contain sensors and displays, however a separate device is required as processing/communication unit (“dedicated” peripheral). See Figure 4.



*Figure 4: Distributed system, two-device approach: one display & command unit, and the second one for capturing of biometric data)*

The above figure shows a distributed concept (two appliances) with a sensor box containing 5 different sensors for capturing.

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

**2.3.3 Distributed Appliance Concept**

When we assume an application scenario where face and fingerprint capturing is necessary, a three-device approach is feasible. Hence, a wrist worn display and control element is capable of capturing the eMRTD, the camera appliance captures the face and the third element (e.g. which can be given away) takes the fingerprint of the traveller. (For now, available eye glasses are not capable of transmitting a video stream with enough quality for facial recognition. Quality lacks in terms of video compression, motion blur and unavailable artificial illumination.)

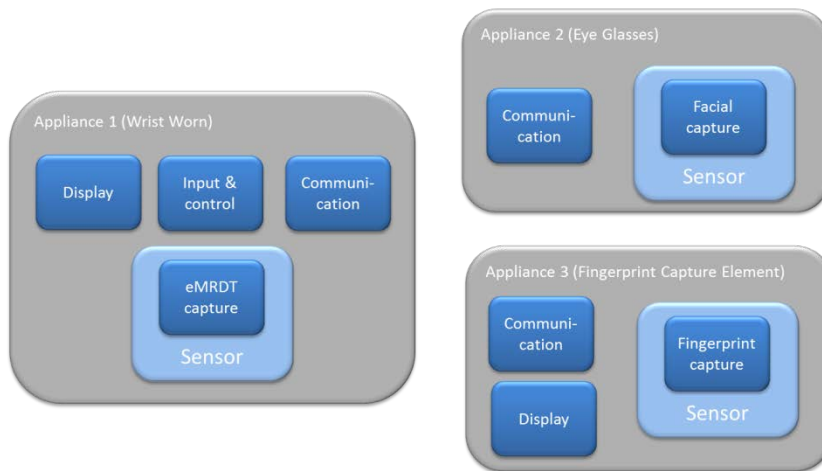


Figure 5: Distributed system, three-device approach: one display & command unit, a second one for capturing facial images and a third for capturing fingerprints

**2.4 Data Processing Architecture**

**2.4.1 Appliance Concept**

Using the elements in 2.2 we can formulate the architecture of an application doing a 1:1 verification of (e.g.) eMRTD facial data and live facial data. In this case biometric data never leaves the system. There is also no database involved.

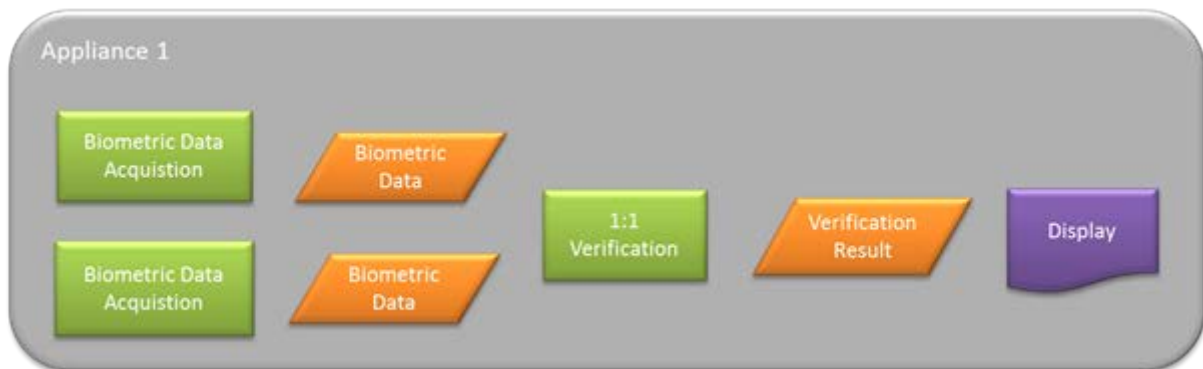


Figure 6: Example for a 1:1 verification in one appliance, biometric data and result do not leave appliance

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

In typical land border scenarios there is also the need to make queries in remote databases. This will introduce the necessity of radio communication and an additional appliance where the database server resides.

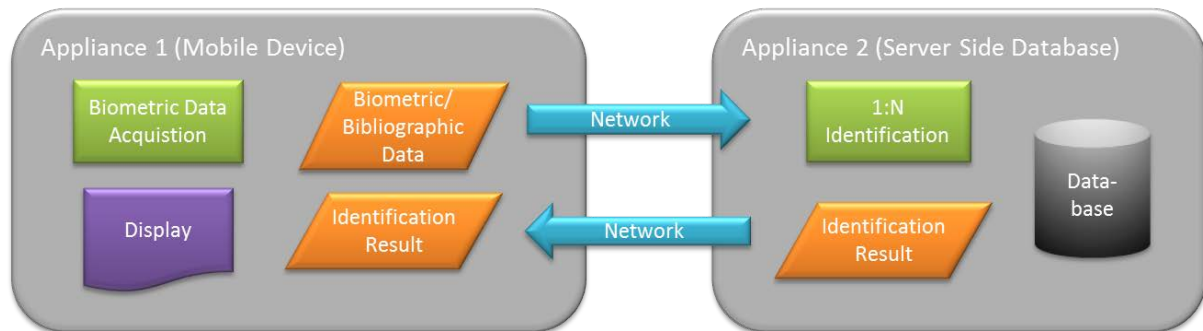


Figure 7: Example of 1:N identification with one device and a server

### 2.4.2 MobilePass Appliances

MobilePass will improve fingerprint, face and travel document capturing using mobile equipment. There are several devices available in the market with different capabilities and unique features. MobilePass provided a list in deliverable D 1.1. However, MobilePass will focus on three appliances.

1. **COTS ruggedized device:** Fast and ongoing developments in the smart phone market reveal that the new devices (COTS) are gradually increasing in performance. However, functionalities and ergonomics of such devices are always designed for general purpose.
2. **MobilePass Face/Fingerprint Camera Module:** Consumer products encompass built in cameras which are directed perpendicularly to the screen, programming interfaces are not designed for burst capturing and fast focus control. It turns out that a dedicated additional device for capturing biometrics (face and finger) would be of enormous advantage used in combination with a standard phone. Further improvements of this additional device (not in the MobilePass Scope) will substitute functions of the COTS devices over time, removing them completely so that only one device is left.
3. **MobilePass Full-Page Passport Scanner:** The third element will be a novel mobile reader for full page passport scanning. After technical discussions with the project partners it turned out that a separate device is necessary due to technical requirements and for showing the distributed character of developments.

For MobilePass a combination of the three devices will be used for WP7 (Demonstration).

- A1 - COTS Device (commercial of the shelf device) for Display, Control & Input (Figure 8)
- A2 - FullPage Passport scanner (Figure 9)
- A3 - MobilePass scanner (Figure 10)



Figure 8: A1 - COTS ruggedized Devices with missing functionality, works in combination with additional elements



Figure 9: A2 - Full Page Passport reader without a display and long range communication functionality

Vision and Requirements of the Future

Version 0.9, 30.12.2014

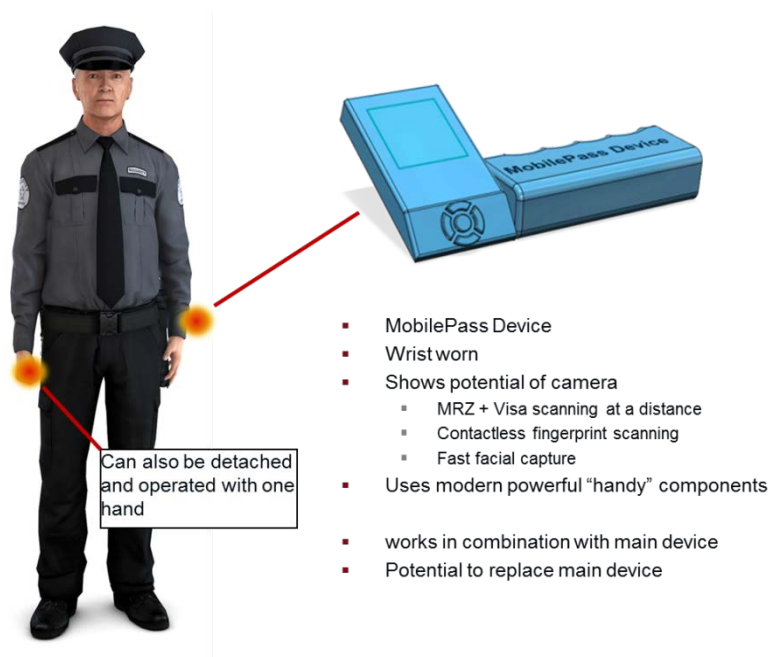


Figure 10: A3 - Vision of MobilePass Face/Finger Camera Device

2.4.3 Distributed MobilePass Appliance Concept (several elements)

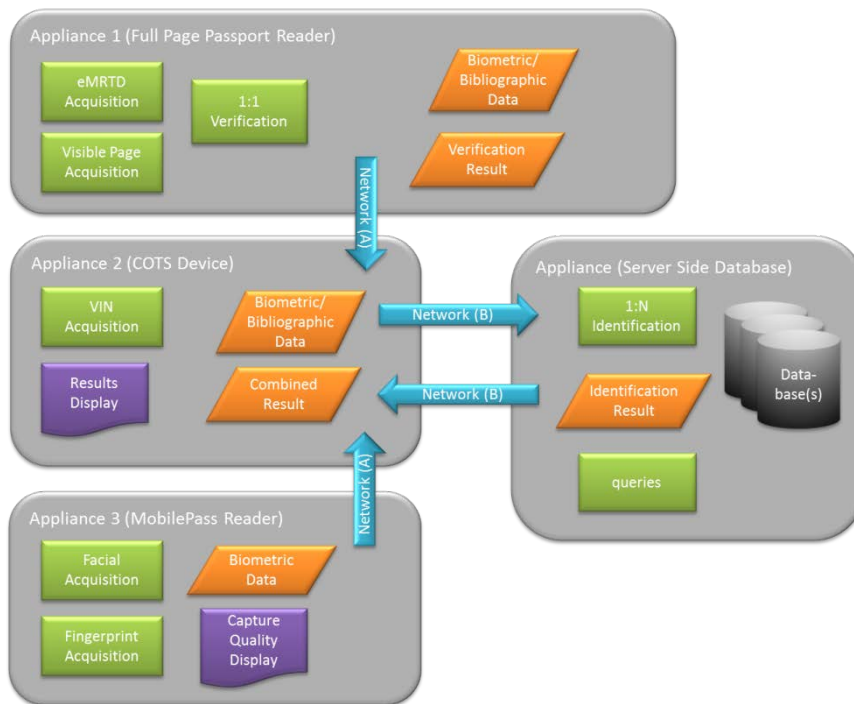


Figure 11: MobilePass appliances; Example of distributed functionality

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

For demonstration purpose of a distributed system a combination of all MobilePass appliances (A1, A2 and A3) will be chosen. An example of a combination is shown in *Figure 11*. However, the distribution of functionalities among them might be different to those in the draft above. The following example shows the flexibility of the proposed distributed architecture.

1. The e-passport of the traveller is applied to the **A1**
  - a. On A1 the eMRTD acquisition is performed, as well as the scan of visible data page in UV, IR and visual light
  - b. The A1 performs a 1:1 verification if data on the visible page and chip data is the same (except face image)
2. Chip data, and UV scanned images are transferred to **A2** (it can be more data, e.g. IR, etc.)
  - a. Verification results of step 3 are shown on A2
  - b. A2 starts data queries via long range communication services
  - c. Border Guard is able to inspect and investigate the UV image on the display of A2
3. **A3** is used as module for capturing of fingerprints and face images
  - a. A3 consists of a single- or dual-camera device (depending on technical requirements for short-distance fingerprint capturing and longer distance face capturing) with integrated active lighting.
  - b. image quality during capturing process is monitored using build-in display of A3
  - c. Fingerprints and Face images are sent to A2
4. **A2** starts data queries (face, finger) via long range communication services
  - a. Border guard enters eventually VIN number into A2
  - b. A2 gathers results from databases and display it to border guard for final decision

### Notes:

- In this combination two different networks are used. Network A for short range communication and Network B for long range communication.
- There are several activities which can be done in parallel, however it is not considered here.
- The example is based on the assumption that for the envisaged EES [11] a facial image is captured at the moment of border crossing.

#### 2.4.4 Embedding in national environments

As mentioned in the introduction of Section 2.3 the MobilePass appliances have to work in a complex IT environment. In Figure 12 an exemplary “complete” environment is illustrated. It shows that it might be possible to take more than one logical networks into account which leads to further requirements for secure network authentication. Detailed description of these issues can be found in Chapter 85 (architecture).

- For usability reasons a single access point to the end-users data centre is necessary
- In the end-users data centre a database of all mobile appliances with authentication codes is necessary



Vision and Requirements of the Future

Version 0.9, 30.12.2014

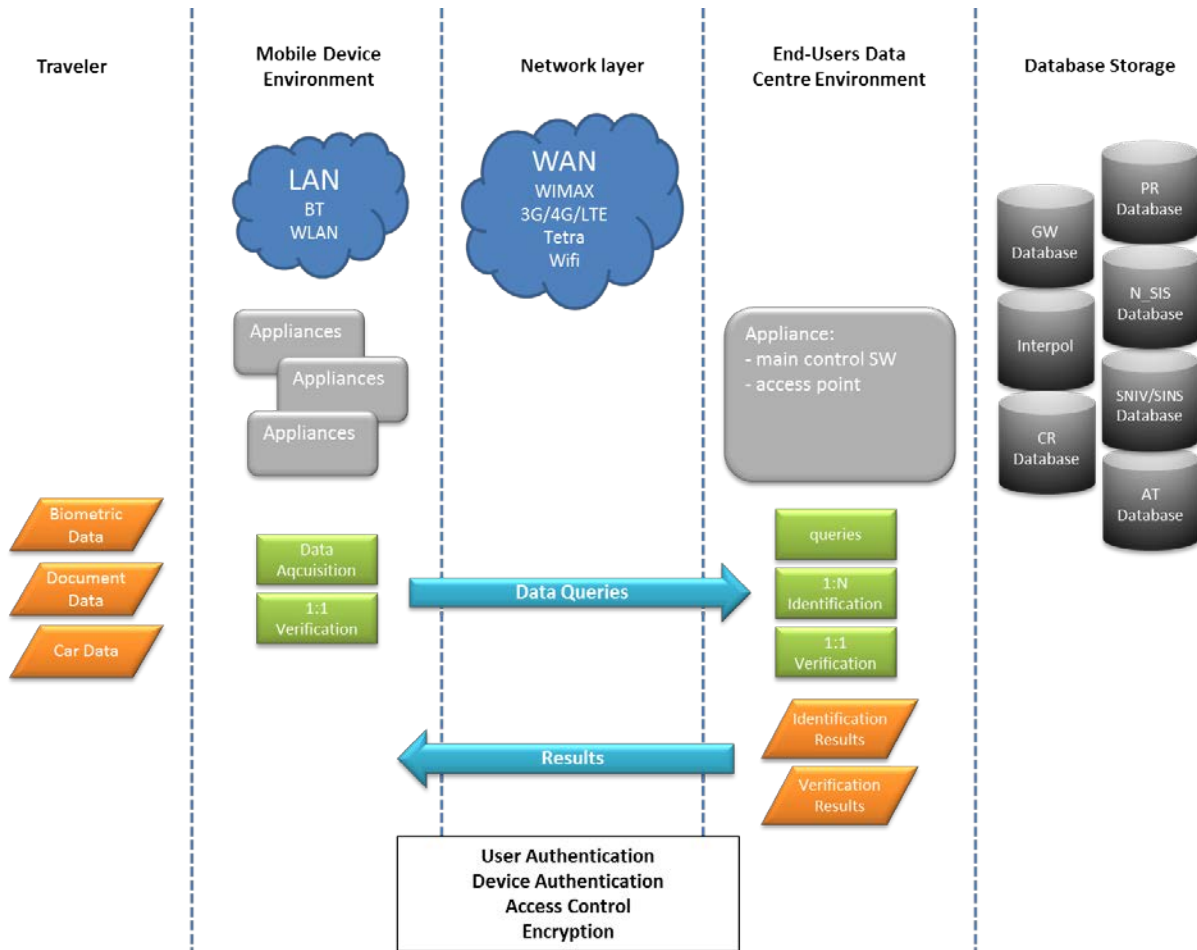


Figure 12: Logical view on MobilePass appliances in national environment

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

### 3 Requirements

#### 3.1 Requirements capturing process and structure

The MobilePass requirements have been determined based on stakeholders needs. The stakeholders (Rumanian and Spanish Boarder Guards) expressed their needs during two workshops – one in Galati (Rumania) on 22.-23.July 2014 and another in Madrid (Spain) on 15.-16.September 2014. The consortium partners gathered the expressed needs and transformed them into scenario descriptions. Deliverable D 1.1 [5] describes the scenarios for different travellers and necessary identity checks. It describes the workflow at the border guards and lists disadvantages/advantages of used devices. Furthermore, it describes handling problems and possible improvements. Based on this, sketches of high level requirements have been produced.

The requirements have been expressed as a hierarchical structure where high-level requirements have been further divided into more detailed low-level requirements. High-level requirements only contain general statements and group the low-level requirements. Furthermore requirements are split into main categories and sub-categories.

##### Main categories are

- Mobile Device and Software
- Communication Requirements
- Application and IT Database

##### Sub categories are

- Functionality
- Usability
- Reliability
- Performance
- Supportability
- Design
- Physical
- Safety

##### Tags

As two countries are involved in MobilePass activities, we added a separate column in the requirements list to have a tag, describing for which country/nationality this specific requirement applies.

- RBG (Rumanian Border Guards)
- SBG (Spanish Border Guards)
- Both

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

A separate column was introduced for the category (priority) of the specific requirement. The possible entries for this are:

- M - Mandatory requirement. This feature must be built into the final system
- D - Desirable requirement. This feature should be built into the final system unless the cost is too high
- O - Optional requirement
- E - Possible future enhancement

Two separate columns have been introduced to capture potential data protection issues and potential social/ethical issues.

- yes - Potential issues
- no - no Potential issues

It is planned to further enhance the requirements list, which exists also as an EXCEL File with the following entries:

- For each requirement or requirement group a reference of standardisation should be given.
- Acceptance criteria should be described. This will be done to some extent in the work packages 3, 4 and 5 later in the project development phases

### 3.2 ICAO Requirements (ABC Guidelines similarities)

For a mobile architecture high level requirements for the design of an ABC system are also very important for many aspects, if the implementation proves successful and sustainable over time. Some of the fundamental requirements are outlined below (as listed in GUIDELINES: electronic – Machine Readable Travel Documents & Passenger Facilitation)[3]:

- The overall design must be technically compatible with associated standards of operation and communication while allowing ongoing flexibility to accommodate developments in this area.
- The architectural design should be modular using COTS components allowing easy re-configuration or expansion in a vendor agnostic manner if possible.
- The design should support systems redundancy and fall-back in order to maintain operation in the event of host component failure.
- The physical configuration including signage should confirm accepted best practice in order to present consistent user interfaces.
- The design should accommodate scalability and should not be limited.
- The design should meet the requirements and obligations of the hosting administration with standard components and should not be bespoke.
- The architectural design should be easily supported by third party support organisations and should not be vendor specific.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

### 3.3 Requirements List (defined by MobilePass)

Level A code	Level A Basic Requirements	Level B codes	Level B Detailed Requirements	Category	Country Specific	Potential data protection issues	Potential social/ethical issues
<b>Device/s and Dedicated Software Requirements</b>							
<b>Functionality (DF)</b>							
ADF-001	The device must read the data of eMRTD travel documents					yes	
		BDF-001-1	The device must read RFID data from 1st, 2nd and 3rd generation passports	M	both	no	yes
		BDF-001-2	The device must extract the following data from the DG1 data group: Document type, Issuing State, Name of Holder, Document Number, Nationality, Date of Birth, Sex, Expiration Date, Check Digits	M	both	yes	no
		BDF-001-3	The device must check data integrity with check digits of DG1	M	both	no	no
		BDF-001-4	The device must extract the data from the DG 2 data group: Facial Image Data	M	both	yes	no
		BDF-001-5	The device must extract the data from the DG 3 data group: Finger Image Data	D	both	yes	no
		BDF-001-6	The device must extract the data from the DG 4 data group: Iris Image Data	O	both	yes	no

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

		BDF-001-7	The device must extract the data from the DG 15 data group: (AA) active authentication public key info	M	both	no	no
		BDF-001-8	The device must read the data from the EF.SOD data group the document security object	M	both	no	no
		BDF-001-9	The device must read the data from the EF.COM data group the common directory file	M	both	no	no
		BDF-001-10	The device must do a EF.SOD verification and a comparison between EF.SOD and EF.COM	M	both	no	no
		BDF-001-11	The device must do a DS certificate signature verification, a certificate validity period check and check the DS certificate revocation status	M	both	no	no
ADF-002	The device must capture a biometric sample of the travellers face					yes	yes
		BDF-002-1	The facial capture process should be able to capture faces for all kind of users with different demographic and physical characteristics (Age over 18)	M	both	yes	yes
		BDF-002-2	The device should be able to capture facial images with the appropriate quality	D	both	yes	yes
		BDF-002-3	The device should be able to reduce noisy images by the means of active light sources with dedicated light control mechanism that focus on	E	both	yes	yes

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

			the face area rather than on the whole image				
		BDF-002-4	The device should give immediate feedback to the operator about the quality of the observed face, even while the capturing is in progress	E	both	yes	yes
		BDF-002-5	The device should have a automatic image quality assessment functionality, to select viable images from a captured set and to give feedback to the operator if suitable images where found. This includes feedback about problem sources (motion blur, low light, shadows and non-frontal poses	E	both	yes	yes
		BDF-002-6	The device sensor should have a high dynamic range of grayscales to avoid saturated pure-white/black regions	E	both	yes	yes
		BDF-002-7	The device should capture facial images with lowest drop shadows (especially in eyes- and nose regions)	E	both	yes	yes
		BDF-002-8	The device sensor should have appropriate resolution (min. 60 pixel eye distance)	D	both	yes	yes
		BDF-002-9	The technology used to capture a facial images must not affect the travellers physiology	M	both	no	yes
ADF-003	The device must capture a biometric samples of the travellers					Yes	Yes

Vision and Requirements of the Future

Version 0.9, 30.12.2014

	fingerprints						
		BDF-003-1	The device should capture fingerprint images without the need for the traveller to touch a sensor surface to reduce hygienic inconveniences	M	both	no	yes
		BDF-003-2	The fingerprint scanner should be able to capture fingerprints with the appropriate quality. If it is not possible, inform the operator	M	both	yes	yes
		BDF-003-3	The fingerprint scanner should allow repeated capture process, at certain number of attempts if the quality of the capture image is not enough	M	both	yes	yes
		BDF-003-4	The fingerprint capture process should be able to capture fingerprints for all kind of users with different demographic and physical characteristics (Age over 18 years old)	M	both	yes	yes
		BDF-003-5	The fingerprint scanner shall be able to capture fingerprints considering different environmental conditions (i.e. indoors and outdoors)	M	both	yes	yes
		BDF-003-6	The fingerprint scanner shall be able to detect artefacts that users might use to spoof the system	D	both	yes	yes

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

		BDF-003-7	The fingerprint system shall be able to compare the capture fingerprint to the fingerprint reference. Depending on the type of comparison, the system should be able to read the biometric reference from the passport or to send the capture fingerprint to the eID or the centralised server or to do both processes	M	both	yes	yes
		BDF-003-8	The fingerprint scanner shall be able to compare the capture fingerprint to the fingerprint template	M	both	yes	yes
		BDF-003-9	The fingerprint system shall be able to compare as accurate as possible fingerprints captured using different kinds of fingerprint scanners	M	both	yes	yes
		BDF-003-10	If many fingers are captured the system should be able to compare all of them against the fingerprints stored in the passport, one positive match gives a positive match of whole fingerprint verification process	M	both	yes	no
		BDF-003-11	The system shall be able to provide a comparison decision to the operator (pass or fail) at least. Other details such as quality score should be given	D	both	yes	yes
ADF-004	The device must capture a biometric samples of the travellers iris		Iris capturing is not in the scope of MobilePass	E	-	-	



**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

ADF-005	The device must be able to capture data about the travellers transportation means					YES	
		BDF-005-1	The device must be able to take a photo of the transportation means	D	RBG	yes	yes
		BDF-005-2	The device must be able to capture the number plate of the vehicle (car, bus, motor cycle)	D	RBG	yes	yes
		BDF-005-3	The device must be able to capture the vehicle identification number (VIN)	D	RBG	yes	yes
ADF-006	The device user interface should ease the work of the operator						
		BDF-006-1	The device's user interface shall be uniform (look and feel) for all features	M	both	no	no
		BDF-006-2	The user interface must give the operator full control about the biometric capturing processes. The operator must have the option to select or decline biometric samples	M	both	yes	yes
		BDF-006-3	The user interface must give all information about the scanned document security status	M	both	no	no
		BDF-006-4	The user interface must have options to override (input manually) data already captured	M	both	yes	yes

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

ADF-007	The software of the device should have a functionality for the management of sessions						
		BDF-007-1	A session should be a complete check for a travellers group or a individual traveller	D	RBG	yes	yes
		BDF-007-2	The software should be able to handle at least two sessions in parallel, allowing switching between sessions.	D	RBG	no	no
ADF-008	The software of the device should enable the notification of the operator about the comparison results in the remote databases or eMRTD verification status						
		BDF-008-1	The warnings sent to the device operator should be discrete as possible, configurable in a way only known by the advised operator	M	both	yes	yes
		BDF-008-2	The warnings sent to the device operator on database hits of other border control operational elements should be only visual	M	both	yes	yes
		BDF-008-3	The warnings about device integrity and operational status should be visual and/or acoustical	D	both	yes	yes

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

		BDF-008-4	How warnings and database hits are notified to the device operator should be configurable (optical, acoustical, vibration, blinking LED's) for each comparison, verification and integrity check	D	both	yes	yes
ADF-009	There should not be any possibility to harm the device data integrity by not authorized persons						
		BDF-009-1	It should not be possible to do changes in the operating system of the involved mobile systems without authorisation	M	both	yes	yes
		BDF-009-2	It should not be possible to do changes in the applications software of the involved mobile systems without authorisation	M	both	yes	yes
		BDF-009-3	Access keys and signatures should be stored in a trusted module	M	both	yes	yes
		BDF-009-4	Before the device is operated, there should be a 2 factor authorisation allowing only authorised persons to operate the system	M	both	yes	yes
		BDF-009-5	The authorisation process should repeat automatically in a configurable interval	D	both	yes	yes
		BDF-009-6	If the authorisation process is not done correctly the system should stop operation	D	both	yes	yes

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

		BDF-009-7	The software of the device must have the possibility to be wiped per remote access.	D	both	yes	yes
		BDF-009-8	The boot image should be signed from manufacturer	D	both	yes	yes
		BDF-009-9	If boot image signature does not correspond to the one stored in the trusted module, device should stop operation	D	both	yes	yes
ADF-010	The software should give the operator the possibility to link travellers to groups and transportation means						
		BDF-010-1	The operator should have the possibility to open and close groups of travellers	D	RBG	yes	yes
		BDF-010-2	When the check process begins the device should offer two options (single traveller or group)	D	RBG	yes	yes
		BDF-010-3	Upon closing a group a means of transportation can be assigned to this group	D	RBG	yes	yes
		BDF-010-4	The device should have the possibility send travellers data to the database for checks either by complete group or individual traveller	D	RBG	yes	yes
		BDF-010-5	Default configuration for BDF-10-4 should be configurable	D	RBG	no	no
		BDF-010-6	Data captured during the check are to be deleted immediately after the process is completed	M	RBG	yes	yes

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

ADD-011	The device should have the capability to perform the database checks manually					yes	
		BAF-011-1	The device must have the possibility to enter data for different database checks for manual inspection	M	both	yes	yes
		BAF-011-2	The device should have the possibility to enter a announce message for persons on the discrete watch lists	O	RBG	yes	yes
ADD-012	The user interface of the device should make the user's interaction as simple and efficient as possible						
		BDD-012-1	The user interface can be a mixture of text and graphical symbols	M	both	no	no
		BDD-012-2	The user interface of the system should be in English	M	both	no	no
		BDD-012-3	Other user Interface languages should be configurable	D	both	no	no
		BDD-012-4	The dialog on the device's display should be self-descriptive	D	both	no	no
		BDD-012-5	The dialog should be error tolerant despite of evident errors in input, the intended result may be achieved with either no or minimal action by the user	D	both	no	no
		BDD-012-6	User initiated actions should be interruptible at any time	M	both	no	no

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

		BDD-012-7	If the device software is in an atomic state of operation (non-interruptible state) it should be notified(no input possible)	M	both	no	no
		BDD-012-8	Identification and verification matches should be displayed	M	both	yes	yes
		BDD-012-9	The acceptance levels for identification and verification should be configurable	M	both	yes	yes
		BDD-012-10	The result of identification and verification process should be displayed in a form of a bar graph and a percentage of the perfect match score	D	both	yes	yes
ADD-013	The device functions must be documented						
		BDD-013-1	All user interface functions should be described	M	both	legal req.	no
		BDD-013-2	The device's interfaces and access points must be described in a list	M	both	legal req.	no
		BDD-013-3	If 3rd party software is used, each software component should be named (manufacturer and version)	M	both	legal req.	no
		BDD-013-4	For each selectable function of the device the flow of biometric data must be described in document	M	both	legal req.	no
		BDD-013-5	The system should not store any private data, except that one's which are necessary to fulfil the actual schengen border code or other laws allowing this	M	both	legal req.	no

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

ADD-014	The device should provide an verification of biometric features between the passport holder and the data given by the eMRTD					yes	
		BDD-014-1	The system should provide a verification result between captured fingerprints and eMRTD fingerprints	M		yes	no
		BDD-014-2	The system should provide a verification result between captured face and eMRTD face	M		yes	no
ADD-015	The device must check the security attributes of the document						
		BDD-015-1	The system must check the falsification attributes of the document (visible light, UV, IR)	M	both	no	no
ADD-016	The device must check if data captured from the eMRTD is equal to the data captured via the visible data page of the document						
		BDD-016-1	The system should check if the issue date of the travel document is plausible	M	both	no	no
		BDD-016-2	The system must check the expiration date of the travel document is plausible	M	both	no	no

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

<b>Usability (DU)</b>							
ADU-001	The ergonomic design of the device should give the operator the option to perform a manual inspection of documents.						yes
		BDU-001-1	The system must be handheld device, always leaving a free hand to the operator	D	both	no	no
		BDU-001-2	There should be a possibility to attach the device to the operator's body harness, leaving both hands free for the operator	D	both	no	no
		BDU-001-3	For observing and selecting data from the device it should not be necessary to use two hands	D	both	no	no
		BDU-001-4	For selecting different information from the system's screen or other hardware, no input device should be required by another hand	D	both	no	no
		BDU-001-5	It should be possible to operate the system wearing gloves	D	both	no	no
<b>Reliability (DR)</b>							
ADR-001	The MTBF of the system should be 4000 hours of operation (minimum)						
		BDR-001-1	The software of the system should provide a run-time counter of the	D	both	no	no



**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

			total device operating hours				
		BDR-001-2	It should not be possible to edit or reset the run-time counter	D	both	no	no
<b>Performance (DP)</b>							
ADP-001	The overall time span to capture all data from a traveller and transportation means should be as fast as possible					yes	
		BDP-001-1	The overall capture process should not exceed 20 seconds on average	D	both	yes	no
		BDP-001-2	Capturing actions can be done in parallel	D	both	yes	no
		BDP-001-3	Capturing of the MRZ by camera should not exceed 2 seconds on average	D	both	yes	no
		BDP-001-4	Capturing of the Passport visible page (UV,IR, visible light) should not exceed 5 seconds on average	D	both	no	no
		BDP-001-5	Capturing of the RFID chip of the eMRTD should not exceed 7 seconds on average	D	both	yes	no
		BDP-001-6	Capturing of all biometric data of a traveller shall not exceed 10 seconds on average	D	both	yes	yes
		BDP-001-7	If a fingerprint is not captured during this time, a new attempt should be conducted. If maximum number of attempts is achieved, the system should inform to	D	both	yes	yes

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

			the operator				
		BDP-001-8	Duration takeover of all the data from the registration of motor vehicles shall not exceed 5 seconds	O	RBG	no	no
		BDP-001-9	Capturing of the VIN (Vehicle identification number) should not exceed 5 seconds	O	RBG	no	no
		BDP-001-10	Capturing of the vehicle number plate should not exceed 2 seconds	O	RBG	no	no
		BDP-001-11	Capturing of the vehicle data (photo) should not exceed 2 seconds	O	RBG	no	no
ADP-002	The device operation by battery should be as long as possible						
		BDP-002-1	The operation time should be given in minimum figures	M	both	no	no
		BDP-002-2	The device should be supplied with electricity through batteries	M	both	no	no
		BDP-002-4	The battery should be removable/exchangeable	M	both	no	no
		BDP-002-5	It should be possible to charge the removed battery by a dedicated charger	M	both	no	no
		BDP-002-6	The minimum duration of operation of the system should be 12 hours minimum between two charges (all device components)	M	both	no	no
		BDP-002-7	The minimum number of battery cycles should not be less than 1000 cycles	D	both	no	no

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

		BDP-002-8	It should be possible to recharge the device by means of solar energy	O	both	no	yes
		BDP-002-9	The minimum duration of operation, between two power supply using and electricity recharge devices, based on transformation to the sunlight, will be for 15 hours	O	RBG	no	no
<b>Supportability (DS)</b>							
ADS-003	The battery should be exchanged very quickly with minimum effect to the ongoing operation					no	
		BDS-003-1	The battery charging status should be displayed anytime (percentage of full charge, estimated time to go)	D	both	no	no
		BDS-003-2	When changing the battery, all configured data (operating mode, actual status) should remain stored in the device	D	both	no	no
		BDS-003-3	There should not be the need to re-enter operator's authentication after battery change	D	both	no	no
<b>Design (DD)</b>							
ADD-001	The visualisation system should not display any secret information to the traveller					yes	yes

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

		BDD-001-1	The position and arrangement of the device's display should limit the possibility to see data for other persons than the operator	D	RBG	yes	yes
		BDD-001-2	It is allowed to use a privacy filter foil	D	both	yes	yes
		BDD-001-3	For capturing a person's face with the device camera there should be a possibility to detach the device from the (body) mount and move it with one hand	D	both	no	no
ADD-002	There should be the possibility to charge batteries for the devices with photovoltaic equipment			O	RBG	no	no
<b>Physical (DPR)</b>							
ADPR-001	The device must be lightweight						
		BDPR-001-1	The devices should have a weight less than three kilo (including all device parts)	M	both	no	no
		BDPR-001-2	The device held by operator's hand should have less than one kilo	M	both	no	no
		BDPR-001-3	It should be possible to operate the device with only one hand	D	both	no	no
ADPR-002	All the device functionalities and features will be shown for operator through a display						

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

		BDPR-002-1	Operator interface will be provided through a color display with, minimum, 5.5 inch wide (high).	M	both	no	no
		BDPR-002-2	The display should have the capability to display a picture of a traveller in colour with enough resolution to identify a person	M	both	yes	no
		BDPR-002-3	The system display should be readable in the night and also in direct sunlight	D	both	no	no
ADPR-003	Rainy conditions should not make any harm to the system						
		BDPR-0031	Rainy conditions should not degrade the performance of the device, as long as sensors (glasses) are not affected	D		no	no

**Communications Requirements**
**Functionality (DF)**

ADF-001	There should be no possibility to change data inside the device from other networks						
		BDF-001-1	A communication link to the device should only be established with valid authentication	M	both	no	no
		BDF-001-2	A port-scan should not reveal relevant and responding ports with connected services	M	both	no	no
		BDF-001-3	The device should not respond in any form to network requests from	M	both	no	no

Vision and Requirements of the Future

Version 0.9, 30.12.2014

			outside the device				
		BDF-001-4	Unusual and frequent network requests from outside should lead to a user's notification	M	both	no	no
ADF-002	The communication system should inhibit the possibility of eavesdropping or interception of data						
		BDF-002-1	The communication to the central databases should be established via VPN	M	both	yes	no
		BDF-002-2	The communication should be encrypted	M	both	yes	no
		BDF-002-3	The encryption method should be AES 128 Bit or higher	M	both	yes	no
<b>Usability (DU)</b>							
ADU-001	The device should automatically search for network connections						
		BDU-001-1	There should be a possibility to parameterize the device or network connectivity including cooperating devices	M	both	no	no
		BDU-001-2	The device should not communicate to other services or devices than those parameterized (in a list)	M	both	no	no
		BDU-001-3	The actual network connectivity status for all connected devices should be displayed	M	both	no	no

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

		BDU-001-4	The device should be capable to connect to a WIMAX network	M	RPB	no	no
		BDU-001-5	The device should be capable to connect to a 3G/4G network	M	both	no	no
		BDU-001-6	The device should be capable to connect to a WiFi network	D	both	no	no
		BDU-001-7	The device should be capable to connect to a TETRA network	D	both	no	no
		BDU-001-8	The device should be capable to connect to a Bluetooth network	M	both	no	no
		BDU-001-9	The device should be capable to connect to a Bluetooth BTLE network	D	both	no	no
		BDU-001-10	In case of communication loss, the device should automatically re-establish a secure communication	D	both	no	no
<b>Reliability (DR)</b>							
ADR-001	The device should scan available networks						
		BDR-001-01	The status of all available networks should allow to select a network to set up the transmission connection of the best performance	D	both	no	no
		BDR-001-02	The selection of the best connections should be based on some QoS parameters measured on the transmission link	D	both	no	no
		BDR-001-03	If link disturbances occur, the data will try to re-send a few times	D	both	no	no
ADR-002	The receiving site should send an						

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

	acknowledge to the device about received data						
<b>Performance (DP)</b>							
ADP-001	The device should send data for verification in central databases as fast as possible						
		BDP-001-1	The typical turnaround time (send, verify, receive, display) of passenger data should not exceed 5 seconds	D	both	no	no
<b>Supportability (DS)</b>							
ADD-001	The device should log data about communication issues						
		BDD-001-1	The device should log points in time for establishing a communication link	D	both	yes	no
		BDD-001-2	The device should log actual data rates for communication	D	both	no	no
		BDD-001-3	The device should log reasons for communication failures, timeouts, authentication failures	D	both	yes	no
		BDD-001-4	The device should log response times from central database services	D	both	no	no
<b>Design (DD)</b>							
ACD-001	The design of the device's software should allow central database checks via						



Vision and Requirements of the Future

Version 0.9, 30.12.2014

	anyone of the chosen communication links						
		BCD-001-1	If parametrized the device should be able to switch over the next best/available communication link if available	E	?	no	no
		BCD-001-2	Active communication should be displayed on the device's screen	D	both	no	no
<b>Physical (DPR)</b>							
ADPR-001	The emitted radiation by radio communication should not exceed the allowed limits given by national and international regulations			M	both	no	no
<b>Application IT Database Requirements</b>							
<b>Functionality (DF)</b>							
ADF-001	Only registered devices should be able to connect to the central database						
		BDF-001-1	There should be a device list at the server containing the device identifiers	D	both	yes	no
		BDF-001-2	The device itself should authenticate at a central server to make sure that only devices which are registered are allowed to connect to the databases	D	both	yes	no

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

		BDF-001-3	Every attempt to connect to the central database service should be logged	D	both	yes	no
		BDF-001-4	Authorisation codes for changing the device list should be different from normal authorisation for operation	D	both	yes	no
ADF-002	The device must be able to send data to perform checks in central databases						
		BDF-002-1	The system must check the passenger data via the eSIF system	D	RBG	-	no
		BDF-002-2	The system must check the passengers in the N.SIS database	D	both	yes	yes
		BDF-002-3	The system must check the passengers in the General Wanted database	D	both	yes	yes
		BDF-002-4	The system must check the passengers in the SNIV/SINS database	D	both	yes	yes
		BDF-002-5	The system must check the passengers in the Interpol database	D	both	yes	yes
		BDF-002-6	The system must check the passengers in the Rumanian Populations Record database	D	RBG	yes	yes
		BDF-002-7	The system must check the passengers in the car registration database	D	both	yes	yes
ADF-005	The system should provide the result of the identification process to the device						

Vision and Requirements of the Future

Version 0.9, 30.12.2014

			After results transmission no residual biometric information should be kept by the system. Data regarding the last specific check should be deleted.	M		yes	no
<b>Usability (DU)</b>							
<b>Reliability (DR)</b>							
<b>Performance (DP)</b>							
ADP-001	The system should be able to perform a search in all databases within 2 seconds						
		BDP-001-1	The time measurements start at arrival of data at the common Database entry point at the servers location and stops when the results leave the servers appliance	D	both	no	no
		BDP-001-2	Only statistical data and no personalised data should be kept. The purpose is to improve IT-processes	D	both	yes	no
<b>Supportability (DS)</b>							
ADS-001	The fingerprint image shall be stored according to an specific data format			M	both	yes	no
<b>Design (DD)</b>							
<b>Physical (DPR)</b>							

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

### 4 Device Vision and Architecture

The "Smart Borders" Package was proposed by the Commission in February 2013. It follows the European Commission (EC) Communication of February 2008 suggesting the establishment of an Entry/Exit System (EES) and a Registered Traveller Programme (RTP).

It aims to improve the management of the external borders of the Schengen Member States. The fight against irregular immigration, information on over stay of foreigners as well as facilitate border crossings for pre-vetted frequent third country national (TCN) travellers.

The future MobilePass device architecture shall support and speed up border processes like the RTP and EES.

The vision of future device is based on the requirements list and the future needs of upcoming smart border packages. For now, it is not clear how these two systems (RTP, EES) will be implemented exactly. However, it is very likely that taking fingerprints and facial images will play an important role.

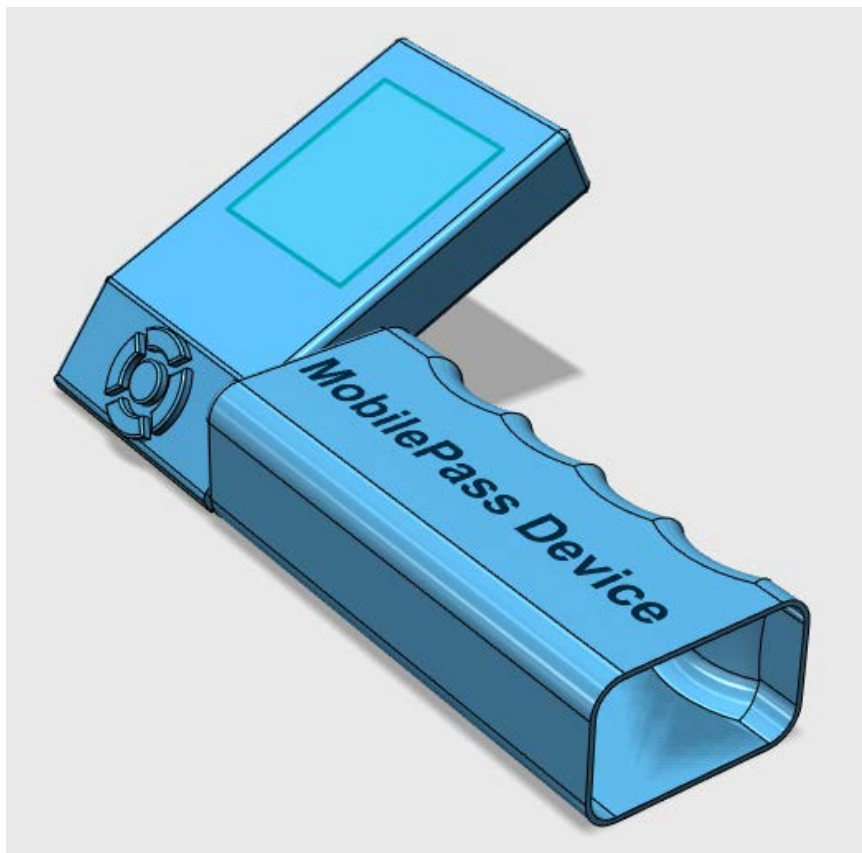


Figure 13: Design study of a future border control device.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

### 4.1 Overview

The work in chapter 4 (Vision and Architecture) is the result of workshops and discussions with border guards, manufacturers and researchers. The device can be used in combination with existing devices and it enlarges the field of operation for border guards with face and finger scanning technologies. It is not the final form but it is a well thought-out design study. There is a 3D model available and after finishing this document the MobilePass consortium will have a 3D printout of this device as a mock-up. This will ease discussions about usability and ergonomics.

In the next chapters each element of the device is described.

### 4.2 Device Components and functions

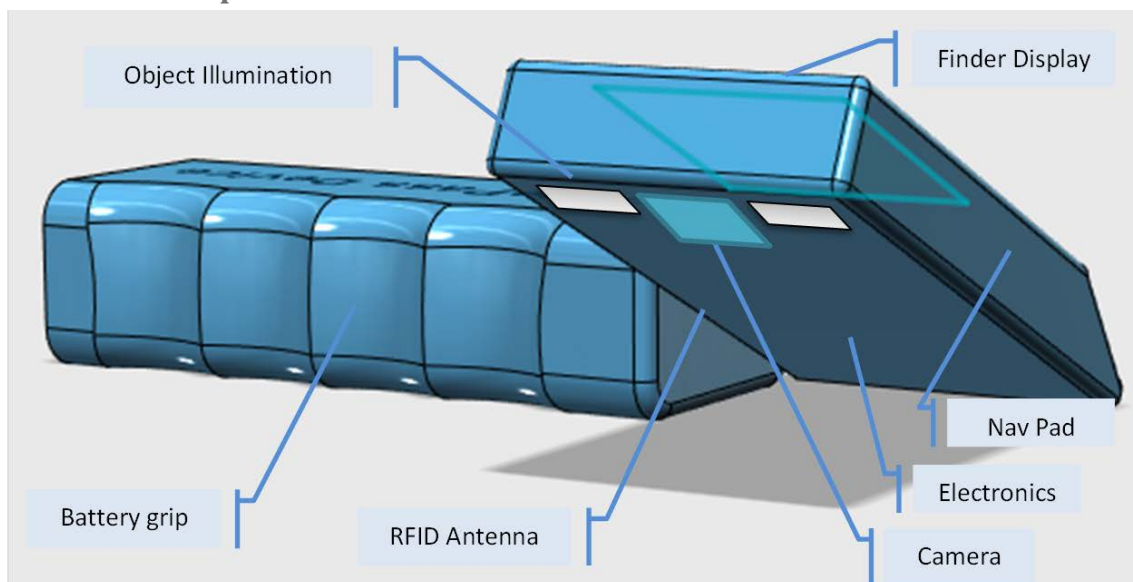


Figure 14: Elements of a design study of a future border control device.

As sketched graphically in the Figure 14 the following (main) components are required to be included in the MobilePass Face/Finger scanner.

- Camera
- Display
- Illumination
- CPU
- RFID chip Reader
- Modem I (BT,WAN)
- Modem II (3G,4G,LTE,WIMAX)
- Keypad
- Trusted Platform Module
- Battery system

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

### 4.2.1 Camera system

One of the critical system elements is the camera system. For a mobile device weight and size is very important. The function of the envisioned camera (system) is to capture

- visual information of the travel document, specially the MRZ zones which are designed to be read by machines as they are printed in OCR-B font in three different formats
- images of fingerprints with enough resolution to extract quality minutia's
- images of the face of the traveller with high enough resolution and quality.

The following constraints are to be considered:

As there is no fixed connection between the scanned object and the imaging device there is a lot of motion between both. The camera should use fast exposure modes for sharp images and low motion blur. It is essential for the camera system to be operated in a mode where the fast shutter is given priority over the gain control. In dark scenes the noise in the image will increase due to higher gain values and this is the reason to integrate artificial illumination on the device.

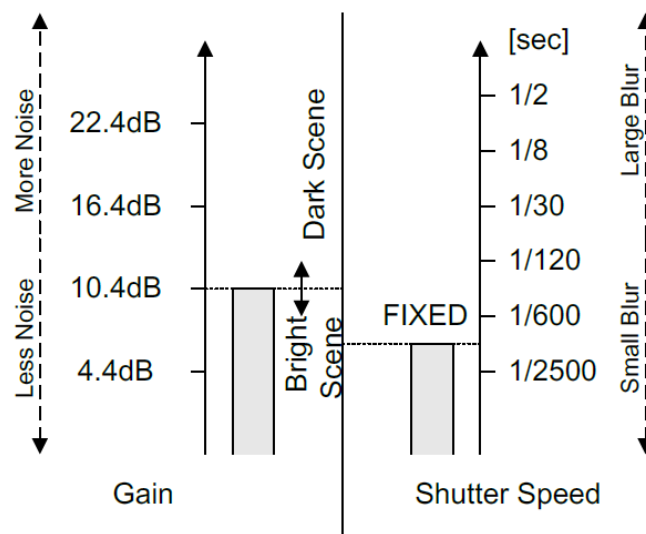


Figure 15: Shutter speed priority mode

(Source: Sony Functional Camera Block FCB MA-130 Application note, Version 1.0 5th Mar, 2013)

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014



*Figure 16: Example of motion blur (left without, right with) (Source AIT Laboratory)*

The camera system might be used indoors (trains, busses, buildings) as well as in outdoor scenarios. It is very likely that very high contrast variations will occur during the capturing process. The camera should have a built-in compensation for backlight illumination. Due to challenging illumination conditions standard Automatic Exposure (AE) mechanism should be improved by more advanced camera control approaches specifically designed for this scenarios and applications.



*Figure 17: Example of backlight compensation (left without, right with)  
(Source Sony Functional Camera Block FCB MA-130 Application note, Version 1.0 5th Mar, 2013))*

Furthermore, one of the most known problems in imaging is the focusing issue. For the perception of the human eye it is necessary to control focus and exposure in a way that the best harmonic image for the photographer or to fulfil his artistic conception. For border control scenarios, control of the focus and exposure is also necessary but not to satisfy the need for a nice-looking harmonic image. It is the performance of the algorithms which is to be maximized. A picture of a face may be perfect for the human eye but not for the algorithm which extracts features. It is not necessary to find the best white balance configuration or colour fidelity.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

The camera system interface itself should consist of a direct digital connection to transmit images as raw data. In particular for fingerprint images it is crucial to transmit images in any lossy compression format like JPG, or YUV etc. Therefore, a direct digital connection is of advantage to access full quality data. Of course Wavelet Scalar Quantization algorithms (WSQ) are allowed for compression of fingerprint images.

Furthermore, resolution of the camera system should be approx. 500 DPI for fingerprint images (minimum resolution of enhanced images).

The operation type of the camera system should not be “steady shot” type only. The envisioned system should produce video streams (e.g. 25 frames per second) which are constantly feeding into the CPU system and constantly processed by the algorithms to have an immediate response about the quality of the image (calculated by dedicated algorithms). By taking quality assessment algorithms into the loop recognition, performance should be improved as well as capturing time should be optimized. In addition, the immediate feedback to the operator improves interaction and usability of the device and as a consequence, the overall result.

In addition, the camera system should have the possibility to provide interrupts to the system when a frame is exposed. This signal can be used to control the illumination system via a central processing unit.

### 4.2.2 Finder Display

Our vision of an easy-to use capturing device includes a camera module with integrated digital finder (display). The function of the Display serves three purposes:

- provide user feedback information about the actual quality of the scanning process
- provide finder overlay to allow the user to see where to point at with the camera
- provide the user interface for capturing control

In sunlight conditions a high readability (display contrast) is necessary and on the other hand low power consumption extends the battery lifetime. Currently, the idea to fulfil these requirements is to use OLED displays which are able to display deep black levels and can be thinner and lighter than a liquid crystal display (LCD). In low ambient light conditions (such as a dark room), an OLED screen can achieve a higher contrast ratio than an LCD, regardless of whether the LCD uses cold cathode fluorescent lamps or an LED backlight.

While a OLED consumes around 40% of the power when an LCD is displaying an image that is primarily black, for the majority of images it will consume 60–80% of the power of an LCD. White backgrounds should be avoided as they reduce battery life in mobile devices.

### 4.2.3 Illumination

Due to the fact that the camera system has to be in a shutter priority mode (to avoid motion blur), additional illumination is necessary. For low maintenance a durable illumination system is of advantage. This could be provided by a customized LED illumination. Highlights should be avoided for



## Vision and Requirements of the Future

Version 0.9, 30.12.2014

a maximum ambient light distribution high power LED with a wide dissemination angel should be chosen.

Controlled illumination intensity and PWM (Pulse Width Modulated) mechanisms are suitable. The main advantage of PWM is power loss in the switching devices is very low. In addition it allows a wide operating range by varying power on and off duty cycles.

The light control mechanism should have the possibility to synchronize with the camera system and the reaction time should be faster than the frame rate to allow an illumination change immediately after the calculations (e.g. histograms) from the last captured frame are done.

The arrangement of light emitting elements should provide maximum ambient light conditions for uniform illumination.

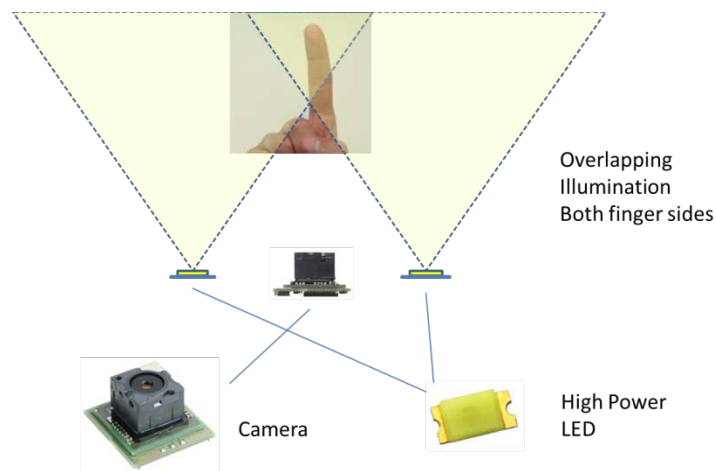


Figure 18: Example arrangement of 2 high power LED's and a camera illuminating both sides of a finger

### 4.2.4 Central Processing Unit (CPU)

When we think about the best CPU for a mobile device fulfilling the tasks of mobile border control, it might be easy considering the available CPU's for globally handy and table market. These CPU's are produced in high volumes and interface peripherals are tailored for the demands of consumer products. However, detailed analysis revealed several shortcomings.

The following chapters will give an overview on how the features of a central processing unit should be composed by taking special consideration for border control purposes into account.

#### 4.2.4.1 Video processing capabilities:

Typical mobile hardware is well suited to produce high quality still images for nice-looking harmonic images. Also, well-developed capabilities are streaming (encoding/decoding) videos for recording and display which is done in special dedicated CPU module. Image processing capabilities in mobile phones are typically under-developed as it is not required. If local processing power is not sufficient, images are transferred to a cloud processing system that shifts the problem to the cloud service

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

provider. Nevertheless, comparing and capturing the biometric data from local image processing and video processing are the most complex and desired tasks of future mobile device for border control. The interaction and connection between the camera and the CPU is also of high importance.

Typically there are several ways to provide image processing power:

- i. Brute force CPU speed (desktop and mainframe power)
- ii. Special dedicated hardware (FPGA, ASIC)
- iii. Parallel computing platforms
- iv. A mixture of all above

On mobile devices power is limited. Therefore, option “i” is not the best idea. Production quantities of mobile control devices for border control will remain far below the production rate of consumer products from a manufacturer point of view. Hence, option “ii” is very expensive because of high development costs if not combined and tightly coupled with embedded CPUs. Parallel computing (iii.) would be an option if dedicated image processing capabilities are provided. Raising the numbers of CPU’s would not solve the problem.

### 4.2.4.2 Power consumption

Taking the intermittent way of processing into account (checking of travellers biometric data - needing all processing capabilities - is not the only task) a flexible CPU architecture is essential where processing elements can be used when required, however energy is not consumed when not in use.

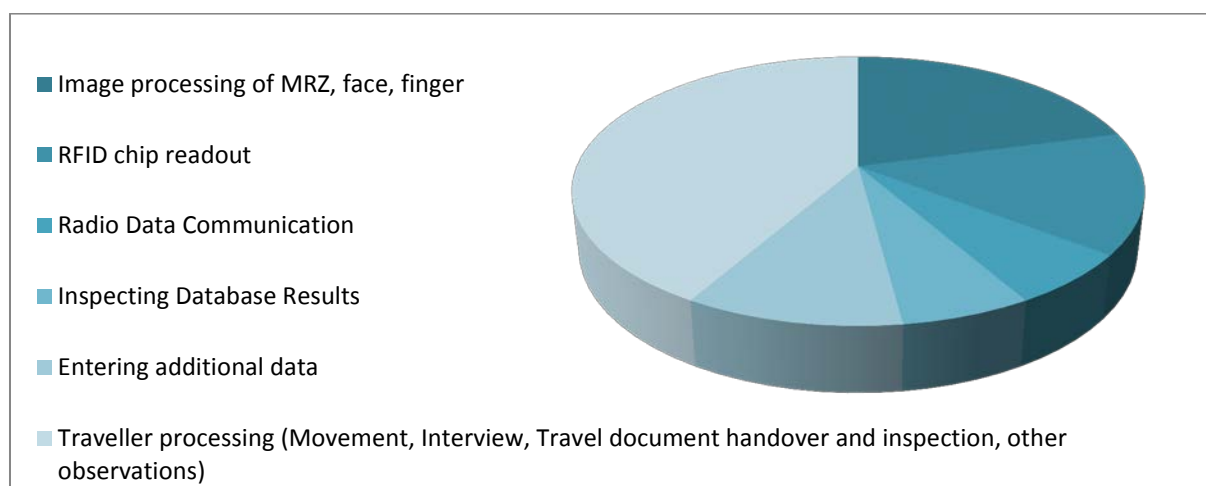


Figure 19: Estimated distribution of processing times for a mobile border scenario (land border checking travellers in cars)

Figure 19 shows the estimated distribution of processing time for different tasks in a land border scenario checking travellers in cars. Roughly only 20 % of the time is used for image processing which is the most CPU demanding task. The other tasks only need relatively low CPU resources. CPU architecture capable of handling impulse utilisation is needed.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

Among all the challenges the mobile device industry faces, keeping components cool is most important since, overheating causes significant reductions in the operating life of a device and leads to device failure. Devices such as cell phones are becoming increasingly complex with larger screens and more functional capabilities which make heat dissipation even harder.

The CPU chip should be designed for portable computers typically housed in a smaller chip package, but more importantly in order to run cooler it should lower voltages than its desktop counterpart and has more "sleep mode" capability. The mobile processor should have the capability to be throttled down to different power levels or sections where the chip can be turned off completely when not in use. Further, the clock frequency may be stepped down under low processor loads. This stepping down conserves power and prolongs battery life.

The requirements for a visionary MobilePass device CPU are:

- Capability to provide desktop performance like image processing power for 20% of total operating time
- Capability to lower power consumption (power down unused components and lower clock frequency) compared to modern smartphones in sleep mode
- High interconnectivity for additional components (e.g. extra illumination)
- Operating temperature between -20 and +40 degrees

### 4.2.4.3 *Operating system and software interoperability*

The software design of future device for border control is a very complex task. As several processing elements are working together simultaneously as a multitasking operating system is essential. In addition, real-time capabilities are necessary to control several hardware extensions (cameras, RFID reader, Illumination). There must be possibilities to sign a boot image to ensure that only certified and authorised software is operating.

For the application software it is advantageous that (accelerating) libraries such as OpenCV exists for image processing. Additional libraries should be available for encryption (EAC, BAC, SAC, SSL and HTTPS). Also additional libraries for image compression (wavelet), RFID reading, communication, live display, overlay display, keypad inputs, touch input methods, trusted platform modules are necessary.

Many of the mentioned libraries are available under LINUX. Linux distributions like ubuntu have the possibilities to adapt special needs because the source is available.

The requirements for a visionary MobilePass operating system are:

- Multitasking
- Expandable (signed boot image, real time capabilities)
- Available libraries (communication, encryption)
- Image processing libraries
- Available on modern embedded chipsets (ARM)

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

- Application programmable in C/C++

### 4.2.4.4 CPU conclusions

Taking all previous considerations into account two different novel CPU architectures are of interest for a future mobile border control device.

#### **Zynq 7000 (SoC) by XILINX**

The Zynq™-7000 family of devices combines the software programmability of a Processor with the hardware programmability of an FPGA resulting in high levels of system performance, flexibility, scalability while providing system benefits in terms of power reduction, lower cost with fast time to market. Unlike traditional SoC (System on Chip) processing solutions, the flexible programmable logic of the Zynq-7000 devices enables optimization and differentiation, allowing designers to add peripherals and accelerators to adapt to a broad base of applications.

#### **Tegra K1 by NVIDIA**

Tegra K1 is the world's first chip to have the same advanced features & architecture as a modern desktop GPU while still using the low power draw of a mobile chip. Therefore it allows embedded devices to use the exact same CUDA code that would also run on a desktop GPU with similar levels of GPU-accelerated performance as a desktop.

### 4.2.5 Trusted Platform Module for platform integrity

The need for a TPM (in combination with other implementations) is to assure the integrity of a secure platform. In this context "integrity" means "behave as intended" and a "platform" is generically any computer platform which is also an embedded system and not limited to a particular operating system. Start the power-on boot process from a trusted condition and extend this trust until the operating system has fully booted and applications are running.

Together with the special boot image a TPM should form a root of trust which should contain several registers that allow a secure storage and reporting of security relevant metrics. These metrics can be used to detect changes to previous configurations and derive decisions on how to proceed.

Trusted Platform Module (TPM) is an international standard for a secure crypto processor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices. TPM's technical specification was written by a computer industry consortium called Trusted Computing Group (TCG). International Organization for Standardization (ISO) and International Electro technical Commission (IEC) standardized the specification as ISO/IEC 11889 in 2009.[18]

For securing sensitive information a Trusted Platform Module (TPM) offers facilities for the secure generation of cryptographic keys and limitation of their use in addition to a random number generator. [19] It also should include capabilities such as remote attestation and sealed storage as follows:

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

- Remote attestation – creates a nearly unforgettable hash key summary of the hardware and software configuration. The program hashing the configuration data determines the extent of the summary of the software. This allows a third party to verify that the software has not been changed.
- Binding – encrypts data using TPM bind key, a unique RSA key descended from a storage key.[20]
- Sealing – encrypts data in a similar manner to binding, but in addition specifies a state in which TPM must be in order for the data to be decrypted (unsealed).[21]

Application software should use a Trusted Platform Module to authenticate hardware devices. Since, each TPM chip has a unique and secret RSA key burned in as it is produced, it is capable of performing platform authentication.

Generally, pushing the security down to the hardware level in conjunction with software provides more protection than a software-only solution.

### 4.2.6 Ideal Algorithm Integration

Typically an ABC-gate (Automated Border Control Gate) is composed of various parts and elements from different vendors like camera systems, illumination systems, face capturing systems, fingerprint capture systems, integrators software and many more. As a consequence, the algorithm developer is not able to design an optimal capturing system because this would require control over (e.g.) the illumination system provided by another vendor for robust feature extraction and over the camera system setup which is also provided by another vendor and to have full control illumination, camera focus, exposure, gain, and other camera settings. It is the role of the integrator to make things work together. However, the integrator is typically not the specialist for biometric capturing or comparison.

MobilePass tries to include biometric specialists, integrators and end-users at the very beginning in the design process. MobilePass targets a mobile Scenario where border guards are using a device as a means of the travellers identity check. For that scenario it is not necessary to design an algorithm for best automatism, it is necessary to design the algorithm interface in a way that it is of help for the border guard. While operating the device the algorithm should give him feedback at the capturing process.

Figure 20 shows a possible ideal implementation of the fingerprint capture process as an example. It should be noted that this process should work with several frames per second as it is essential that the algorithm feedback is given immediately to the operator. This ensures that the operator can respond quickly to the algorithm's improvement suggestions. For example, if finger three is not captured with enough quality, angle of image not correct. The operator immediately reacts to this by aiming at finger three with a different angle. It would not be necessary for the operator to start the capture process from the beginning, only capturing of finger three is revamped. It would also be possible for the algorithm to give feedback about illumination, focus and distance to the object.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

Distance measures can also be displayed at the finders display so that the operator can check for additional corrections.

The process shown in Figure 20 repeats until the operator has a sufficient quality capture or when the process is aborted.

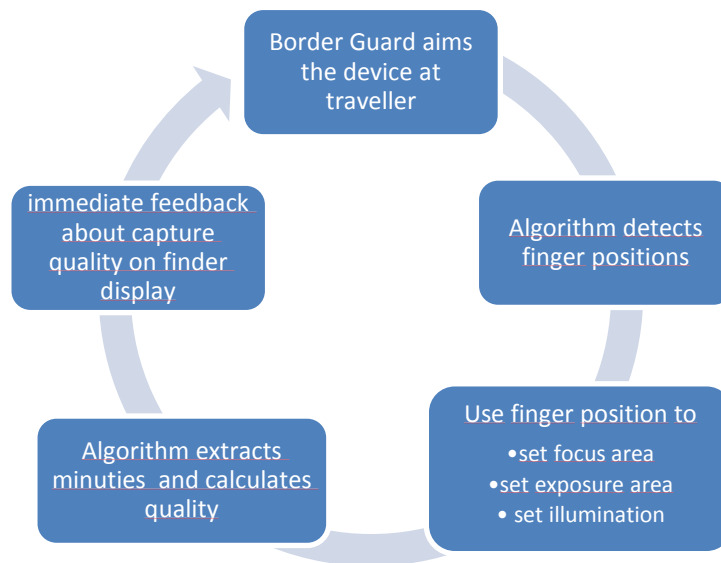


Figure 20: Example of algorithm interaction with operator

## 4.3 Ergonomic concept

### 4.3.1 Handling comfort

The main idea of the device shape and handling concept is based on workshops and discussions with the project end-users. The border guard stated that they want to have their hands free for handling the passport itself or additional elements like driver's license, residence permissions, vehicle identification documents and more. It would be ideal to have a device which is not held by the hand with the use of fingers.

After internet investigation work we found that people and workers in the logistics field already use devices which are mounted on the forearm. The device is equipped with a battery, a CPU, a display, a keyboard for additional inputs and an extension for bar code reading mounted on the finger (See Figure 21). MobilePass adopted the concept and added additional elements (See Figure 14).



*Figure 21: Wrist mounted device used in the logistics sector (Source Motorola).*

However, the border guards skipped the idea of the finger scanner as it disturbs the process of scrolling through the passport and is cumbersome since it reduces the sensitivity of the fingers checking the travel document. Also, the cable shown in the figure is a potential handicap. But the single idea of mounting the device on the forearm seems to be a good idea and it has several advantages compared to existing devices (see [5]):

- Hands free
- Operation with one finger
- Automatic power sleep mode when hand is dangling
- No cables, easy detachment for operation by one hand (just in case of)
- It allows the positioning of cameras (face and finger capturing) in an optimal way
- At the capturing process no display information is shown to the traveller

The MobilePass consortium wants to implement a prototype of this device. It may not be the final solution but it will show future ways of operations:

- The device has not to be equipped with a display, future eye glasses have built-in head-up displays
- The device display can be a normal smart phone or smart watch
- When further miniaturized, it can be integrated in some other appliances
- A moveable camera system would ease the aiming process

The following chapters (MRZ capture, face capture and fingerprint capture) are based on the idea of an intelligent device, mounted on the forearm of the border guard. For operation, the border guard has a choice to:

- a) Positioning the arm in a way that face and fingerprint capture from the traveller is possible
- b) Detach the device for better aiming, operate it with only one hand by pressing the “capture” button

#### 4.3.2 MRZ capture

To speed up the process for capturing the MRZ on the passports visible data page, MobilePass proposes the following procedure which will be implemented in an embedded system in later project phases. Figure 22 shows the draft concept of the MRZ capturing procedure. It is assumed that during passport verification the passport is handed over to the border guard by the traveller. After handover, the passport will be positioned correctly by the border guard.

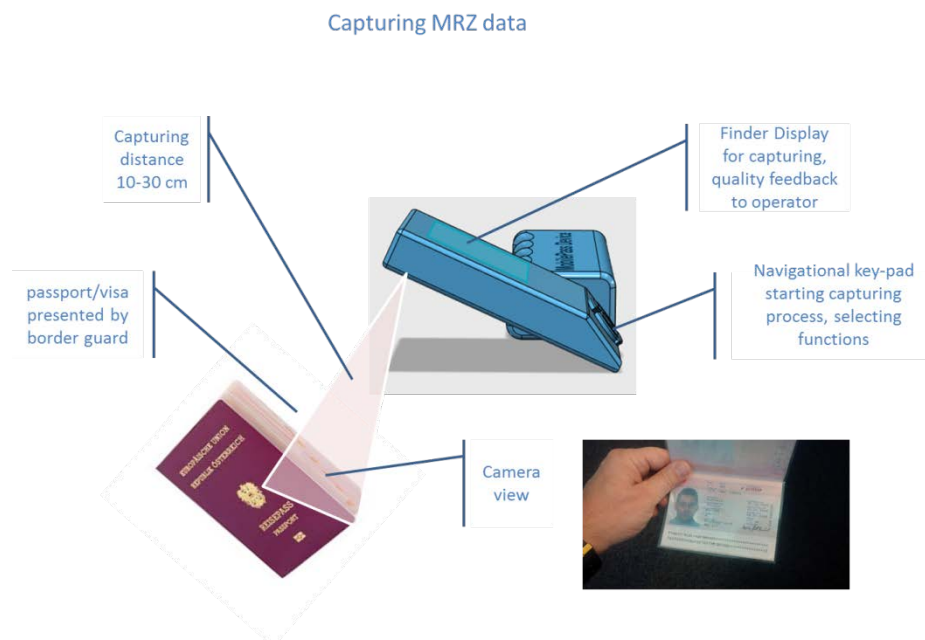


Figure 22: Ergonomic concept for capturing MRZ data

1. As the user selects the mode for reading of MRZ, the camera switches into the initial MRZ capture mode:
  - a. A continuous capturing process will be initiated at roughly HD resolution (1920x1080). This data stream is fed into the video processing system.
  - b. The camera optics will be set to a fixed-focus at a distance of ~20cm
  - c. The finder display will display a live-image
  - d. The finder display should provide the operator with an indication of the distance to the passport. The capture distance should be changed for the passport to be completely in focus.
  - e. The image exposure time is controlled by a standard algorithm which considers the whole image, but places an emphasis on the central region. Small overexposed regions will be ignored as specular reflections on the passport should not trigger an underexposure of the whole image.



**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

- f. For white-balance, a simple histogram-based approach working on the whole image will be used.



Figure 23: Red markers on the finder display show the calculated MRZ position

2. As the user aligns the passport with the reader, the captured images are continuously evaluated with an MRZ-detection algorithm. If a possible candidate for a MRZ region is detected:
  - a. Markers in the finder display (Figure 23) are shown around the candidate MRZ region in red to indicate the detected region to the user
  - b. The exposure algorithm switches to a region based approach that considers the region of the MRZ only.
  - c. The candidate region is evaluated for possible lighting problems such as peculiar highlights. If problematic areas are detected, the user gets visual feedback on the finder image indicating the problematic regions and capturing continues.
  - d. If the candidate region is determined to be sharp (contrast), in focus, correctly exposed and without lighting problems, the candidate region is passed to the next step, the MRZ recognition.
3. As soon as the MRZ recognition starts:
  - a. The markers in the finder display indicating the position of the MRZ turn green
  - b. The candidate region is analysed with an OCR algorithm
  - c. If all checksums of the MRZ are determined to be correct, the acquired information is handed back to the main program, and the user receives the information that the MRZ has been correctly read.
  - d. If the checksums are not correct, the markers in the finder display turn red again, and processing continues again with the detection of the MRZ.

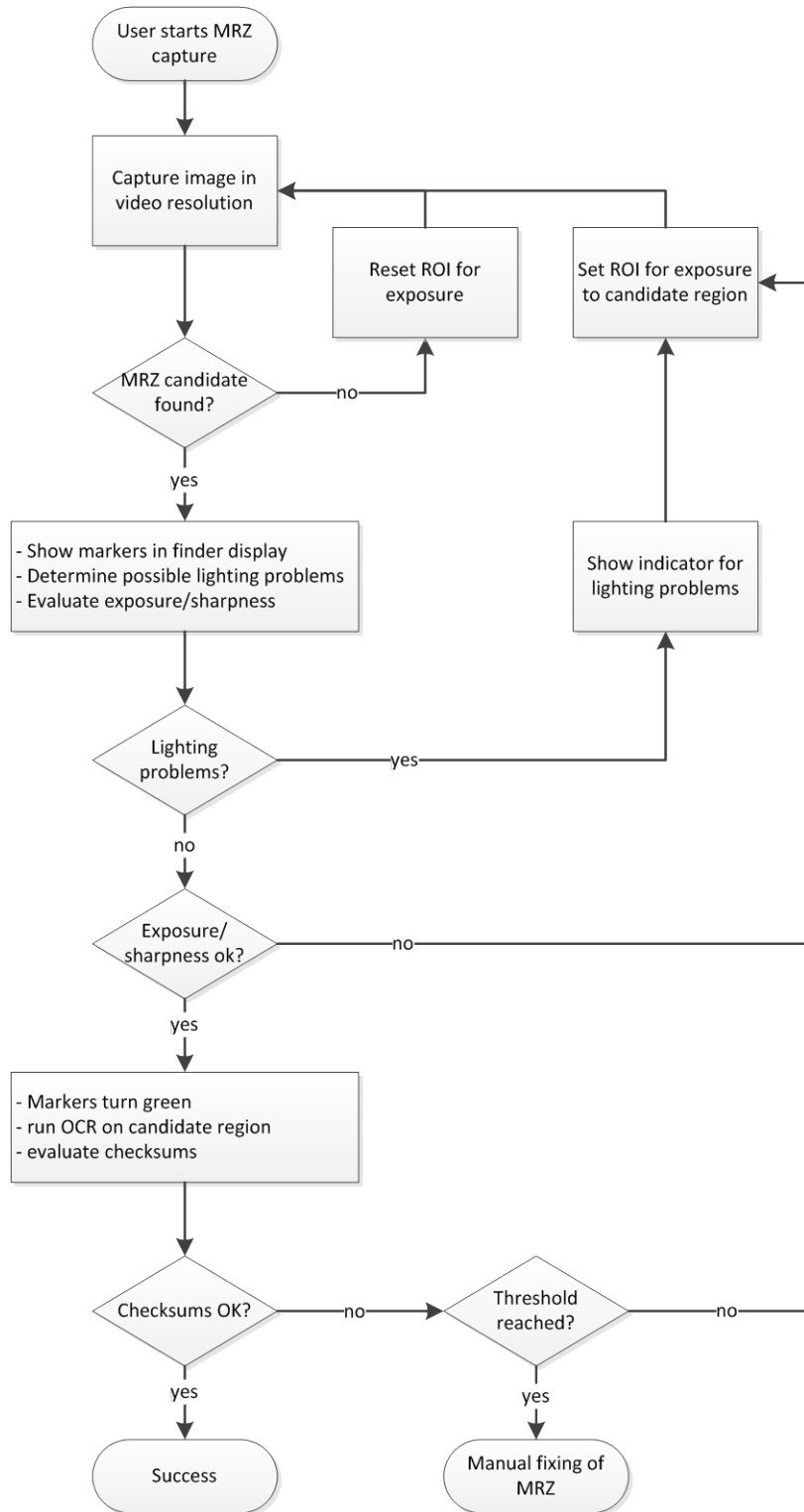


Figure 24: Process flow for capturing MRZ data

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

### 4.3.2.1 *Optional features*

There are additional optional features which can be taken into account, improving the MRZ capture quality and speeding up the OCR recognition and eventually removing the need of user interaction.

#### Automatic character replacement by second best match

To avoid unnecessary delays in the capture process, additional information from the OCR-algorithm can be exploited in the case that the checksums do not validate. The OCR algorithm should return a quality indicator for each character about how good the character could be recognized. If there are one or two characters with bad recognition values, it can be assumed that those characters were not recognized correctly. Those characters can be replaced by the second-best character matches and if the checksums can now be validated correctly, it can be assumed that the correct characters have been found.

#### Manual change for individual characters

If the validation of the checksum fails and the error cannot be recovered, this might have several reasons. One reason might be that the passport has been degraded by wear & tear or by dirt and subsequently the MRZ cannot be recognized correctly. In this case the recognized strings should be presented on the main display to the user and the user should have the ability to change parts of the MRZ to the correct values.

#### Counterfeit detection

Another reason might be that the passport is actually a counterfeit and the forger of the passport failed to correctly calculate the checksum values. This case could be detected by the software if the OCR algorithm reports a very high detection quality of the MRZ characters; however the checksums still can't be validated. The OCR algorithm could try to validate if the used font is actually the correct one (OCR-B). If the wrong font is used this is an indication for a counterfeit passport.

### 4.3.3 **Fingerprint capture**

The process of fingerprint capturing needs to be designed in a way to allow the operator to capture a person's fingerprint in a quick and easy way by achieving minimum quality standards regarding image acquisition. The capturing system should be designed in a way that a quality assessment in the loop is performed in real-time during data gathering to provide a real-time visual feedback to the user and assist him or her during capturing.

Therefore, it is important to design the capturing process very intuitively. One key point here is to visualize status and procedure of the process to the operator to allow for user interaction and feedback. Furthermore it is mandatory that he or she is able to validate the capturing results and to provide the possibility to give consent on data transmission to other devices or sub-systems.

Vision and Requirements of the Future

Version 0.9, 30.12.2014

Capturing fingerprints

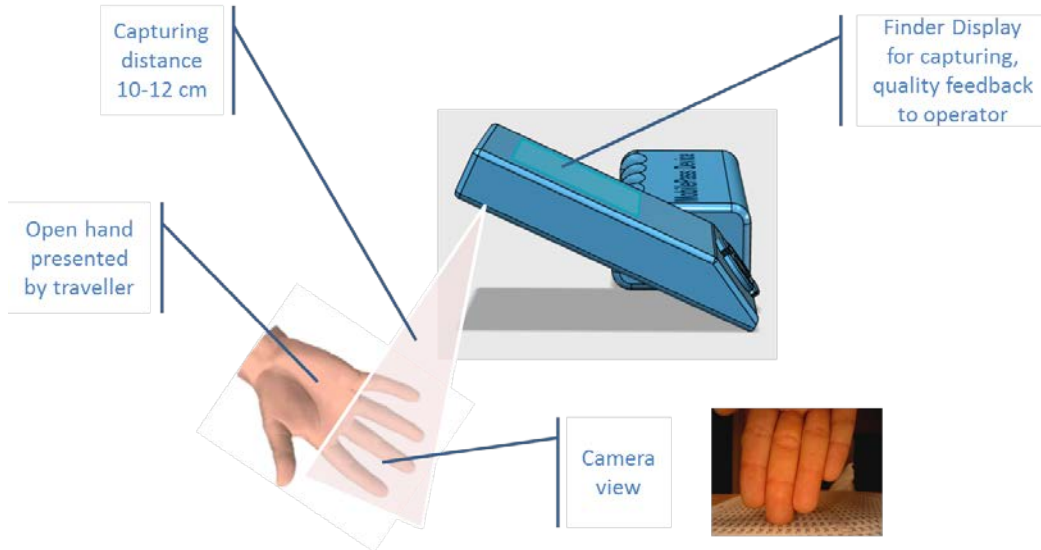


Figure 25: Ergonomic concept for capturing fingerprints.

The above Figure 25 shows the draft concept of the fingerprint capturing device. It is assumed that during passport verification the traveller is sitting or standing in front of the border guard. After the passport is handed over to the border guard, the traveller will be asked to reach out the hand. Currently three different concepts for hand finger capturing are under investigation. Fingers presented to the border guard with a) palm towards sky (camera from top), b) palm towards ground (camera looking to the sky), and c) palm towards border guard (camera hold towards traveller). All these concepts have advantages and disadvantages. For example backlight issues, application of artificial light, image dynamic range, usability and ergonomics etc. So, for concept design all options will be further discussed and investigated, and only aspects which are relevant for all options will be presented in this document.



Figure 26: Capturing Concepts – Scanning fingers from the top, front, or bottom.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

Based on one of the three described capturing concepts an image sequence of one or more fingers is captured by the fingerprint camera device while the camera finder display and the user interface are only visible from the operator's perspective. It is assumed that the traveller's fingers are captured at a distance of approx. 10-20cm from the capturing device and that the hand plane (fingerprints) are captured approximately perpendicular to the optical axis of the camera. It should be considered to integrate a colour LED (e.g. red) at the side of the device so that the image is visible to the traveller to indicate that the capture process is currently running.

The vision for the fingerprint capturing process is going beyond state of the art approaches.

Firstly, a challenge in MobilePass is to perform fingerprint capturing and verification up to four fingers simultaneously. The idea is to capture between two and four fingers (except the thumb) in a single step and to detect the fingers in the whole image first and then segment them (crop fingerprint areas in the image) and perform fingerprint analysis to each sub-image. This concept would allow a quick capturing process, and at the same time increases verification performance by using redundancies. Hence, the idea could be to set thresholds for successful fingerprint verification for different security level. Example for low security level traveller it might be sufficient if two out of four fingers have been verified successfully in a single image while in case of higher security levels four out of four successful verification is mandatory and even this process needs more time or more trials to completion.

Secondly, in MobilePass touchless fingerprint capturing under challenging illumination condition is in scope. Due to these conditions, there is a need for robust and advanced capturing approaches as well as image analytics. At the same time, capturing procedure (interaction) also becomes very important. Since, correct usage of the device facilitates to handle difficult conditions in a better way. As an example, image and video analytics will be integrated to perform quality assessment in real-time and to provide user feedback on current light conditions and image quality. Therefore, the border guard should receive assistance about how to proceed with capturing or what should be done in case of failure of the automated capturing. However, several algorithms will be integrated to perform image enhancement as automated as possible and to keep need for user interaction minimal.

In the next sections these two aspects which are in scope of research in MobilePass will be described in more detail and the idea of a suitable user interaction (interface) is presented.

### 4.3.3.1 *User interface for fingerprint capturing*

The proposed user interaction for fingerprint capturing consists of three steps that correspond to the three user-interface sketches depicted below:

1. The operator initiates fingerprint capturing by clicking a button named "Fingerprint capture" in the main menu or by pressing a dedicated button on the device to enable fingerprint capturing mode. Fingerprint-Camera and illumination are activated and the start-screen displays live video. The operator will now point the device at the person's fingers such that

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

the fingertips (or e.g. the relevant subset of the hand) are roughly located in a target area highlighted on the screen by a four-corner-overlay (bounding box).

2. The operator starts the actual capturing process by clicking “Start”. Now the system automatically collects a sequence of images. While capturing the image the operator should try not to move the device to avoid motion blur. In the currently shown “Capture screen” the following feedback is provided to the operator:
  - a. A set of rectangles around the (automatically) detected fingerprints. The colour of the rectangle can be green (finger with good image quality) or yellow (quality insufficient).
  - b. One of a set of warning icons can appear - Bad illumination, motion blur, missing fingers, insufficient finger size.
  - c. A progress indicator for the number of good-quality images that were captured (Capturing process bar, with 0 to 100%).

Capturing should end automatically as soon as the required number of good quality fingerprint images has been captured (e.g. 5 images).. As long as the required number of images is not reached, the video analysis continues until a timeout occurs (e.g. 10s). Then capturing is stopped and the user interface shows an error message before returning to the start-screen The operator should be allowed to abort capturing any time by clicking “Abort” or pressing a dedicated button on the device.

3. If capturing succeeds in collecting the required number of good quality finger images, then the “Confirmation screen” is shown. In this screen, all captured fingers are shown in a grid-view with a quality map overlay (showing the quality of the fingerprints at different areas of each image). In this way, the user will be able to check if the captured fingerprint images are of overall sufficient quality. To end the confirmation screen (and therewith the entire capture process) he either confirms positively by clicking “Confirm” or negatively by clicking “Abort”. In case of positive confirmation, the fingerprint images are transmitted to the fingerprint verification module.

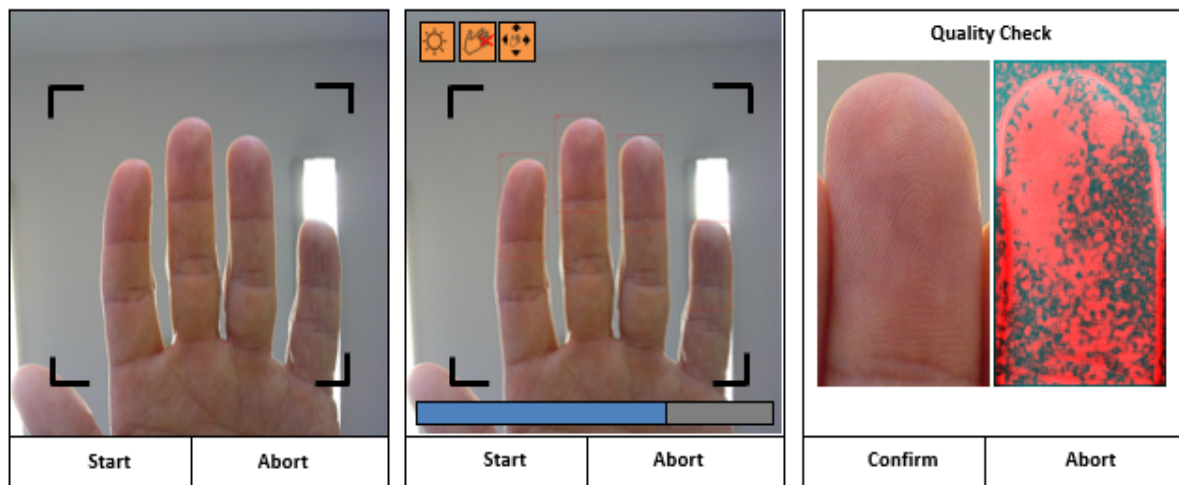


Figure 27: Sketch of the user interface for fingerprint capture.  
From left to right: "Start screen", "Capture screen" and "Confirmation screen".

#### 4.3.3.2 Automatic fingerprint image quality assessment

During the capturing phase, the system collects fingerprint images and checks if they basic parameters fulfil basic requirements, in particular focus and exposure settings of the camera. These are crucial to obtain sharp fingerprint images from a distance. To be able to perform this in sufficient performant way, and as a consequence to allow to apply user feedback (e.g. adaptation for the distance to the fingers), this phase might work in a lower image resolution than sufficient for fingerprint verification (e.g. Full-HD, with 30fps, instead of 15MP with 5fps).

However, based on the available resolution the following attributes should be checked automatically by integrated quality assessment algorithms (It should be noted that listed attributes strongly depend from fingerprint comparison algorithm and could be loosed or tightened according to comparison algorithm's needs):

- Size - The minimum resolution of ~500 dpi must be met. Larger sizes are to be preferred.
- Perpendicularity - The out-of-plane rotation of the hand must be less than 5° to left, right, top or bottom. As this is a minimum requirement, smaller rotations are to be preferred.
- Illumination - No areas in the fingerprint region should be over or underexposed.
- Position of the fingers - A natural position of the fingers to each other is important for ergonomics. However, due to illumination conditions and complexity, we define to capture the (opened) hand with fingers close to each other (basically in parallel to each other) or only a little bit apart.
- Sharpness - Motion blur and de-focussing of the face should be avoided. To determine if finger image is sharp enough, distance between object and camera will be determined as well as camera ego-motion (for motion blurs estimation). Additionally, texture analysis will be performed on fingerprint areas. In case of too large or too fast camera/object movements

image quality is assumed to be of lower quality and image enhancement approaches are applied to algorithmic improvements.

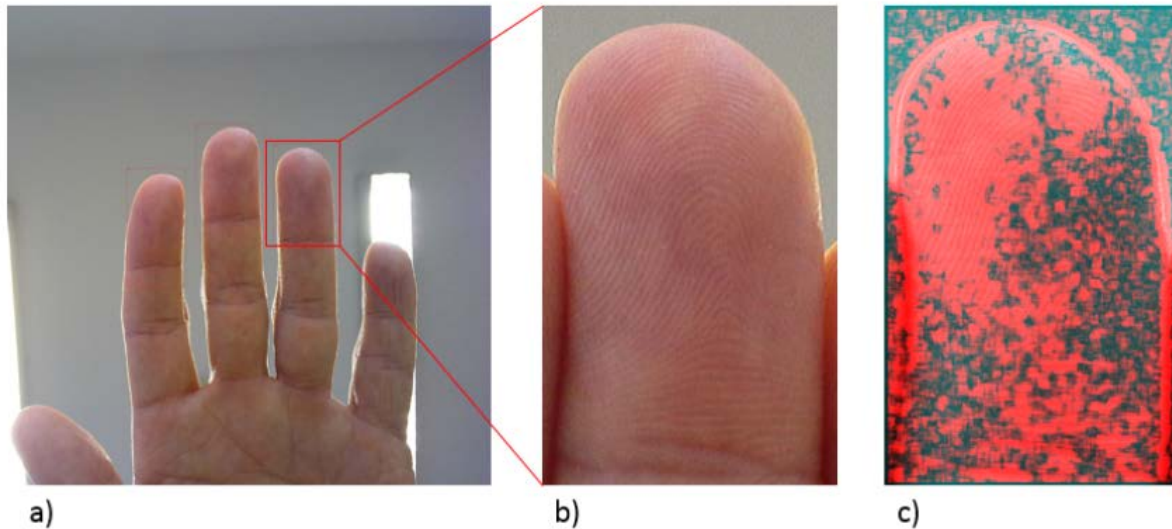


Figure 28: Automated Fingerprint Quality Assessment and Visual Feedback.

#### 4.3.3.3 Fingerprint image enhancement

As mentioned in Section 4.3.3.2 quality assessment techniques are of high importance, on one hand for usability of the device and on the other hand as the basis for post-processing of the captured data. Depending on image quality, images can be post-processed by algorithms for enhancement.

The focus of MobilePass will be on

- Fingerprint image de-noising (in case of low light behaviour)
- Fingerprint Image de-convolution for de-focus compensation (in case of faces slightly out of focus). This is currently assumed to be one of the major issues for touchless fingerprint capturing!
- Illumination compensation and contrast enhancement (e.g. local band pass filters and texture enhancement)
- Multi-Frame analysis (best shot or image fusion) for handling of focus variation of non-planar fingerprint surface.

At present it is assumed that such image enhancement algorithms will be integrated in the capturing device (embedded processing). However, depending on the challenges which will be identified after first camera prototype a selection of relevant algorithms will take place. In particular, based on details related to capturing approach and camera parametrisation, (e.g. shutter speed, optics, etc.) further algorithms might be of higher relevance and will be taken into consideration during research phase.



## Vision and Requirements of the Future

Version 0.9, 30.12.2014

However, from the “vision/system design” perspective it is expected that in many cases which are in practise the camera system will be able to capture fingerprint images even in a non-optimal quality. Subsequently, the system design takes into account an embedded image enhancement process to improve quality of images before forwarding them to validation/verification processes.

It is important to mention here that even improved/enhanced images might be forwarded to other modules (visualisation or fingerprint verification modules). It should be possible for the user to always access the original data in case of manual data validation. This is an important feature to allow data consistency validation (access to raw image data).

### 4.3.4 Face capture

The process of face capture needs to be designed in a way to allow the operator to capture a person’s face quickly and as easy as possible. At the same time, the system needs to ensure that the minimum quality standards for face images are met. It should inform the operator about quality issues and guide him to achieve his goal.

The operator needs to be fully informed about the process that he is in charge of. It is therefore mandatory that he should see the results of the face capture process in a way that no images are transmitted without his or her explicit consent.

The following Figure 29 shows a concept of the device being used for face capture. The device is directed at the person to be captured while the camera finder display and the user interface are only visible from the operator’s perspective. It is assumed that the traveller is located within a certain distance range (e.g. 80-200cm) from the capturing device and that he or she looks (approximately) straight into the camera. It should be considered to integrate a colour LED (e.g. red) at the back of the device to indicate the traveller that the capture process is currently running.

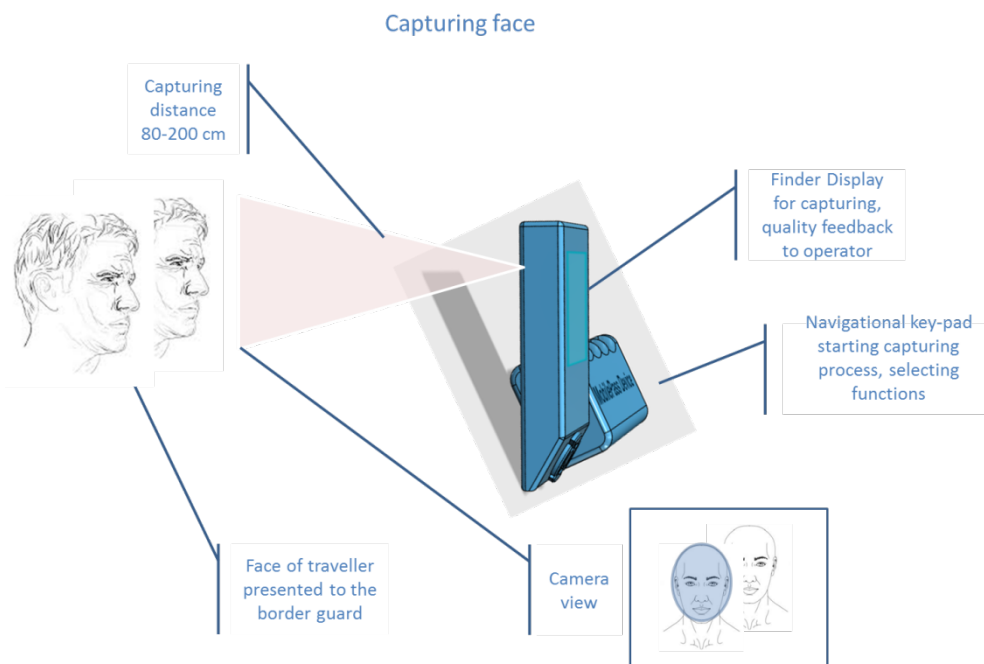


Figure 29: Ergonomic concept for capturing faces.

#### 4.3.4.1 User interface for face capture

The proposed user interaction for face capturing consists of three steps that correspond to the three user-interface sketches depicted below:

1. The operator initiates face capturing by clicking a button named "Face capture" in the main menu or by pressing a dedicated button for enabling face capturing on the device. Camera and illumination are activated and the start-screen displays live video. The operator will now point the device at the person such that the face is roughly located in the target area (depicted by a 4-corner-overlay).
2. The operator starts the actual capturing process by clicking "Start". Now the system automatically collects face images. While capturing the image the operator should try not to move the device to avoid motion blur. In the "Capture screen" the operator gets the following kinds of feedback from the system:
  - a. A rectangle around the (automatically) selected face. The colour of the rectangle can be green (face quality good) or yellow (face quality insufficient).
  - b. One of a set of warning icons can appear - Bad illumination, motion blur, person confusion, insufficient face size.
  - c. A progress indicator for the number of good-quality images that were captured (Capturing process bar, with 0 to 100%).

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

Capturing should end automatically as soon as the required number of face images has been captured (e.g. 5 images). As long as the required number of images is not reached, the video analysis continues until a maximum time is reached (e.g. 10s). Then capturing is aborted and the user interface shows an error message before returning to the “Start screen”. The operator should be allowed to abort capturing any time by clicking “Abort”, or pressing a dedicated button on the device.

3. If capturing succeeds in collecting the required number of face images, in a sufficient quality then the “Confirmation screen” is shown. In this screen, all captured faces are shown in a grid-view. The operator makes sure that all images show the correct person. To end the confirmation screen (and therewith the entire face-capture process) he either confirms positively by clicking “Confirm” or negatively by clicking “Abort”. In case of positive confirmation, the face images are transmitted to the face verification module.

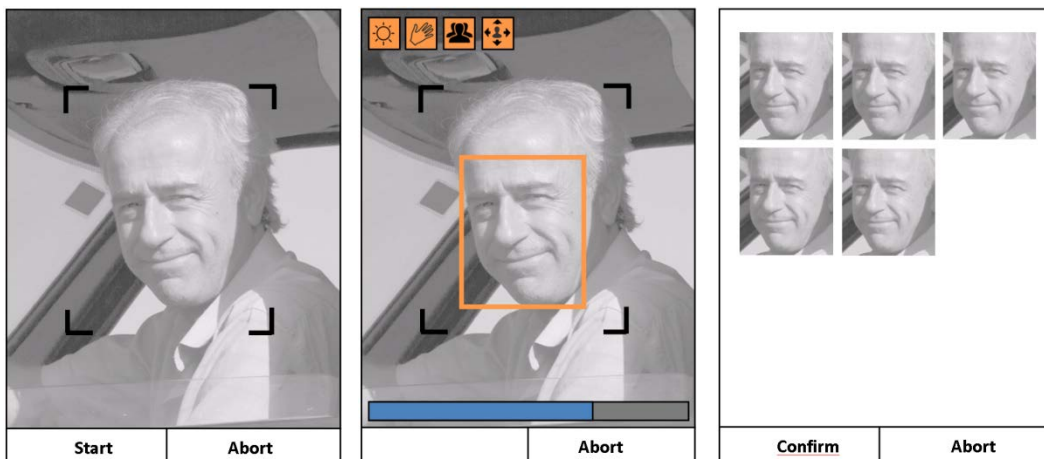


Figure 30: Sketch of the user interface for face capture.  
From left to right: “Start screen”, “Capture screen” and “Confirmation screen”.

### 4.3.4.2 Automatic face image quality assessment

During the capturing phase, the system collects face images and checks if they qualify for automatic face verification. The following aspects should be checked automatically (It should be noted that listed attributes strongly depend from facial comparison algorithm and could be loosed or tightened according to comparison algorithm’s needs):

- Size - The minimum inter-ocular distance of 60 pixels must be met. Larger sizes are to be preferred.
- Frontality - The out-of-plane rotation of the face must be less than 30° to either left, right, top or bottom. As this is a minimum requirement, smaller rotations are to be preferred.
- Illumination - No areas in the face region should be over- or underexposed.
- Expression - A neutral facial expression (i.e. no smiling or talking) is required.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

- Sharpness - Motion blur and de-focussing of the face should be avoided. To determine if face image is sharp enough, distance between object and camera will be determined as well as camera ego-motion (for motion blur estimation). In case of too large or too fast camera/object movements image quality is assumed to be of lower quality, and image enhancement approaches are applied to algorithmic improvements.

Both inter-ocular distance and out-of-plane rotation can be estimated robustly by means of facial landmarks localization. The landmark localization confidence can further be used as quality metric for the face in general, as the following figure illustrates.

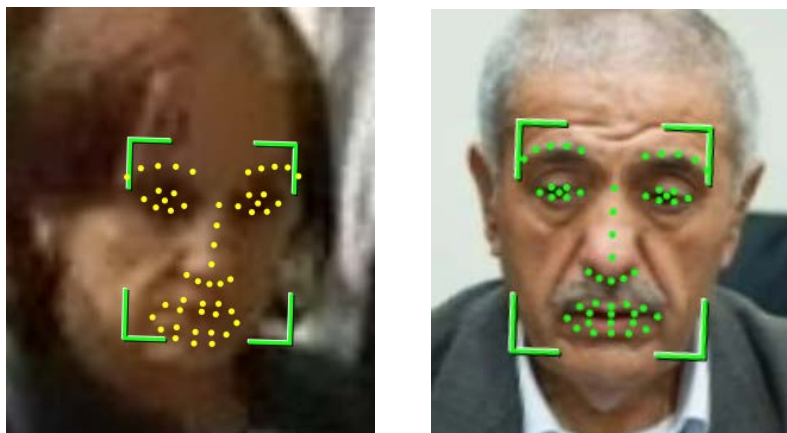


Figure 31: Facial landmarks localization with low confidence (left) versus high confidence (right).

### 4.3.4.3 Face image enhancement

As mentioned in Section 4.3.4.2 quality assessment techniques are of high importance, on one hand for usability of the device and robust capturing of face images and on the other hand as the basis for post processing of the captured data. Based on image quality, images can be post-processed by algorithms for enhancement.

The focus of MobilePass will be on

- face pose normalization (e.g. 3D perspective warping, to compensate view angle of the traveller into the camera)
- face image de-noising (in case of low light behaviour)
- face Image de-convolution for de-focus compensation (in case of faces slightly out of focus)
- face image super-resolution (for face images with slightly to low resolution)

At present it is assumed that such image enhancement algorithms will be integrated in the capturing device (embedded processing) but not all of them. Selection of relevant algorithms will highly depend on the details of capturing approach and camera parametrisation (e.g. shutter speed, optics, etc.) as well as the illumination conditions in real application.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

However, from the “vision/system design” perspective, it is expected that in many cases which are in practise the camera system will be able to capture images of lower quality than required for face verification algorithms. So, the system design takes into account an embedded image enhancement process to improve quality of images before validation/verification and user feedback.

As described in 4.3.3.3, for face capturing, even improved/enhanced images might be usually forwarded to other modules (visualisation or face verification modules). It should be possible for the user to always access the original data to double check inconsistencies on original data. This is an important feature to allow data consistency validation.

### 4.4 MobilePass Full-Page Passport Scanner Components and Functions

In addition to the MobilePass device it may be necessary to scan documents and check their authenticity. This additional device used in MobilePass will be an advanced and mobile Passport Reader/Scanner, without display but with an interface/SDK (software development kit) that allows integration into other systems. It is not intended to work standalone.

At the project start of MobilePass project partner Regula had a prototype of this device, but integration into a larger system was not done so far. Further development of the functions and testing of the interfaces are needed.



*Figure 32: Mobile Full-pagePassport Scanner*

The device should be equipped with a shoulder strap and should have a light weight body which contains full data processing on-board with a built-in PC. The reader can be connected to an external PC or any other visualization device (see **Fehler! Verweisquelle konnte nicht gefunden werden.**) via

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

wireless network. The power supply should be formed by rechargeable batteries with hot change possibility. It should include no moving parts.

The device should allow capturing images in white, infrared, ultraviolet and coaxial lights. In addition a module for reading RFID chips is necessary. A module for reading smart cards would be optional. The device should be supplied with a software development kit (SDK) for easy integration into existing end-user systems.

### 4.4.1 Device Components

The device should include the following components

- Optical Reader with different light sources:
  - white
  - infrared, 870nm
  - ultraviolet, 365 nm
  - white coaxial (optional)
  - Scanning area, 90×130mm: full passport page
- Video sensor
  - type — CMOS
  - colour depth — RGB
  - imaging, 24 bit
  - number of megapixels — 3,1:
  - resolution, 375ppi
  - frame size, pixels — 2048×1536, 1024×768
- Reader of radio frequency identification devices (RFID)
  - Supported standards — ISO 14443: type A and B
  - Data exchange rate, Kbaud — 106, 212, 424, 848
  - Reading an RFID tag regardless of its position in the document
  - Anti-collision: reading an RFID tag according to the MRZ
- Processing Element:
  - Low power consuming CPU
  - Volatile RAM
- Housing and interfaces
  - Protection rating — minimum IP54
  - external USB 2.0 ports for connection of peripherals
  - Connection interface with result visualization device – wireless network
  - Power supply — rechargeable batteries

### 4.4.2 Device Functions

For MobilePass the following enhancements of the device are planned for connectivity and interaction with other devices:

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

- Additional Bluetooth connectivity
- Remote display of document authentication results and images (not only device website display)
- Seamless integration into border control application
- Secure communication

For MobilePass the following enhancements of the device are planned after scanning process and document type recognition is done:

- Checking image patterns in white, IR and UV light
- Checking luminescence of UV protection fibres
- Detection of false luminescence
- Checking photo embedding type: printing or attachment
- Checking IR Visibility of:
  - elements of the form,
  - text data,
  - the photograph (main and additional)
- Detection of holograms/kinegrams (OVD), OVI
- Reading a luminescent text and comparing it with the data obtained from the MRZ and VIZ (OCR Security Text)
- Visualization of IPI (Invisible Personal Information)
- Checking retro reflective protection

The following integrity checks should be made between the MRZ zone data, the RFID data and the visible information page

<b><i>Element Name</i></b>	<b><i>MRZ &lt;-&gt; visual</i></b>	<b><i>MRZ &lt;-&gt; RFID</i></b>	<b><i>RFID &lt;-&gt; Visual</i></b>
Document Class Code	Check	Check	Check
Issuing State Code	Check	Check	Check
Surname and given Names	-	Check	-
Given Names	Check	Check	Check
Nationality Code	-	Check	-
Sex	Check	Check	Check
Date of Birth	Check	Check	Check
Date of Birth Checkdigit	-	Check	-

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

Date of Expiry	Check	Check	Check
Date of Expiry Checkdigit	-	Check	-
Document Number	Check	Check	Check
Document Number Checkdigit	-	Check	-
Final Checkdigit	Check	Check	Check

### 4.5 Device Operating Modes

This section describes the two possible operating modes that are foreseen for the MobilePass device. On one hand it is desired to be able to reuse existing solutions whose sensor portfolio can be augmented or replaced by the MobilePass device. On the other hand it is driven by the possibility to provide a one stop solution that can operate on its own.

These two modes of the MobilePass device are:

- The device is operating in a remotely controlled mode. An external application controls the device and the device is working as a scanner or reader
- The device is operating as a standalone device. All checks and database communication is done on the MobilePass device

In both operating modes the device should perform its operation in the steps described in Figure 33. The diagram shows the planned process of what is required and which steps are optional. It covers the complete workflow from placing the passport on the reader until the final decision, if the passenger is allowed to entry or exit the country. A background check versus background systems like Interpol will be performed after the document is completely read. Afterwards, it is also possible for the details to differ if the traveller is citizen or foreigner with or without visa for special treatment. Additional information like the handling of embarkation cards can be entered on the "Additional info screen". Further, it is possible for group passengers, for example if the traveller is under age and is not allowed to travel without company.

Every component can be easily added or removed. Therefore, it is possible to cover various combinations for different scenarios.



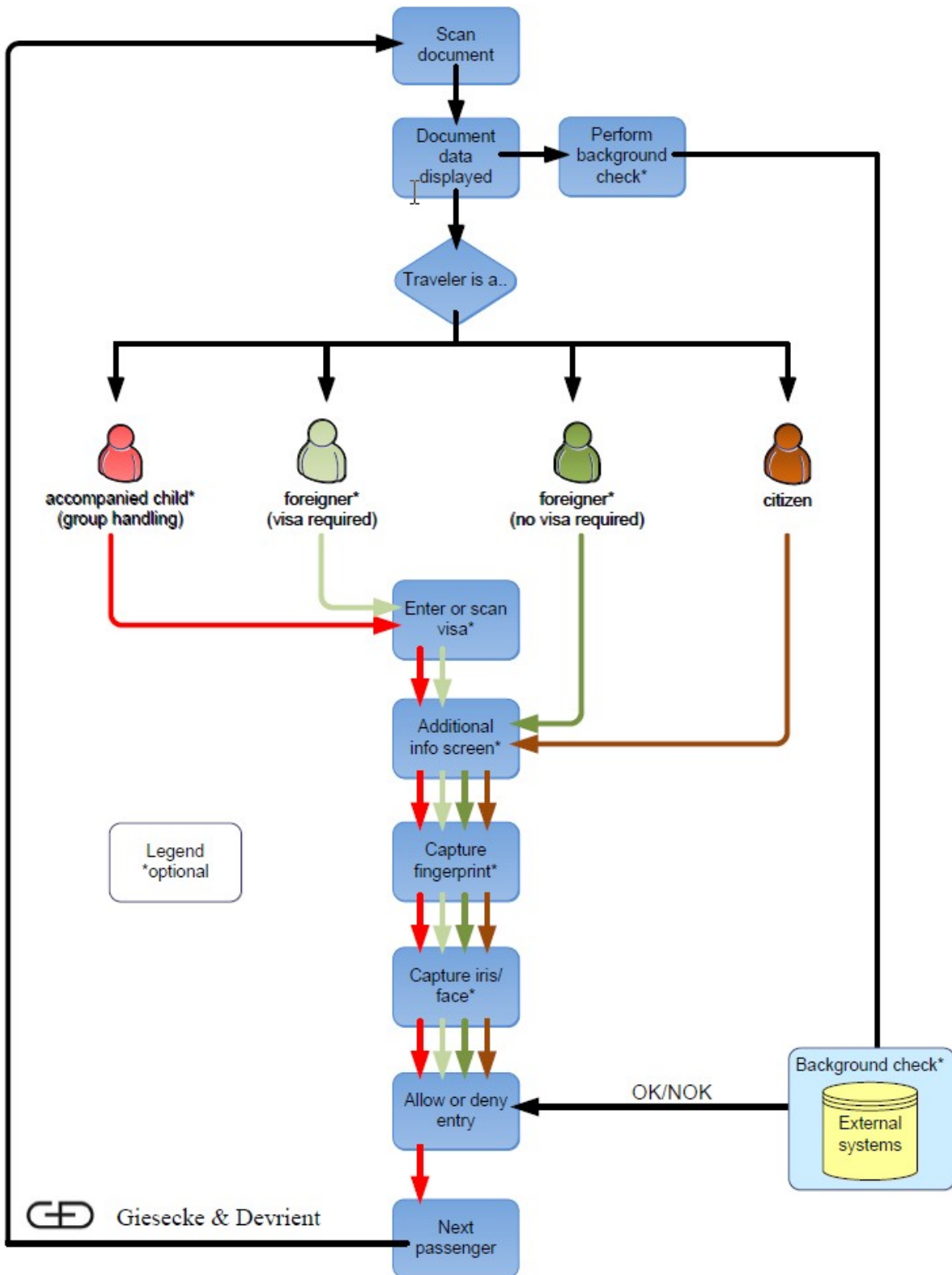


Figure 33: Workflow diagram

Vision and Requirements of the Future

Version 0.9, 30.12.2014

4.5.1 Stand Alone Operation

In the stand alone operation mode (see Figure 34) there is obviously no third party device controlling the MobilePass device. The border guard application is running on the device and there are no other sensors available than those built into the device. The communication with the back-end’s is done using the device’s internal network interfaces (WiFi, 3G/4G/LTE, ...).

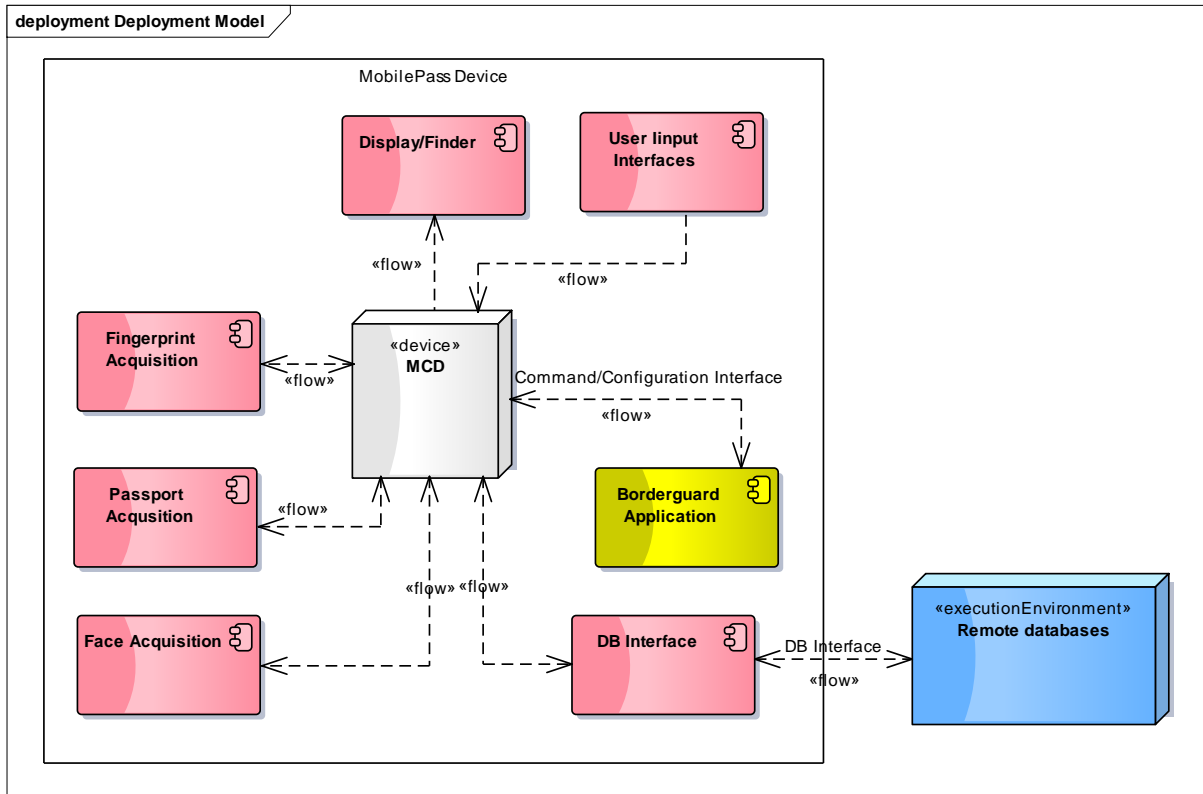


Figure 34: Use case of standalone mode of MobilePass device

4.5.2 Scanner Function

As a scanner the devices simply acquires data from a traveller and his documents. Evaluation of the data and database communication is done by the external application and pre-processing is done on the device (see Figure 35).

In this externally controlled user case the third party device controls the MobilePass device that will be running the application that controls the workflow. This could be a mobile phone, a tablet or a custom built device capable of communicating with other devices. The MobilePass device provides its set of sensors to acquire data. If necessary, the third party handheld device can also be connected to other sensor devices so that it is possible to take fingerprints with one device and scan a traveller’s document with another.

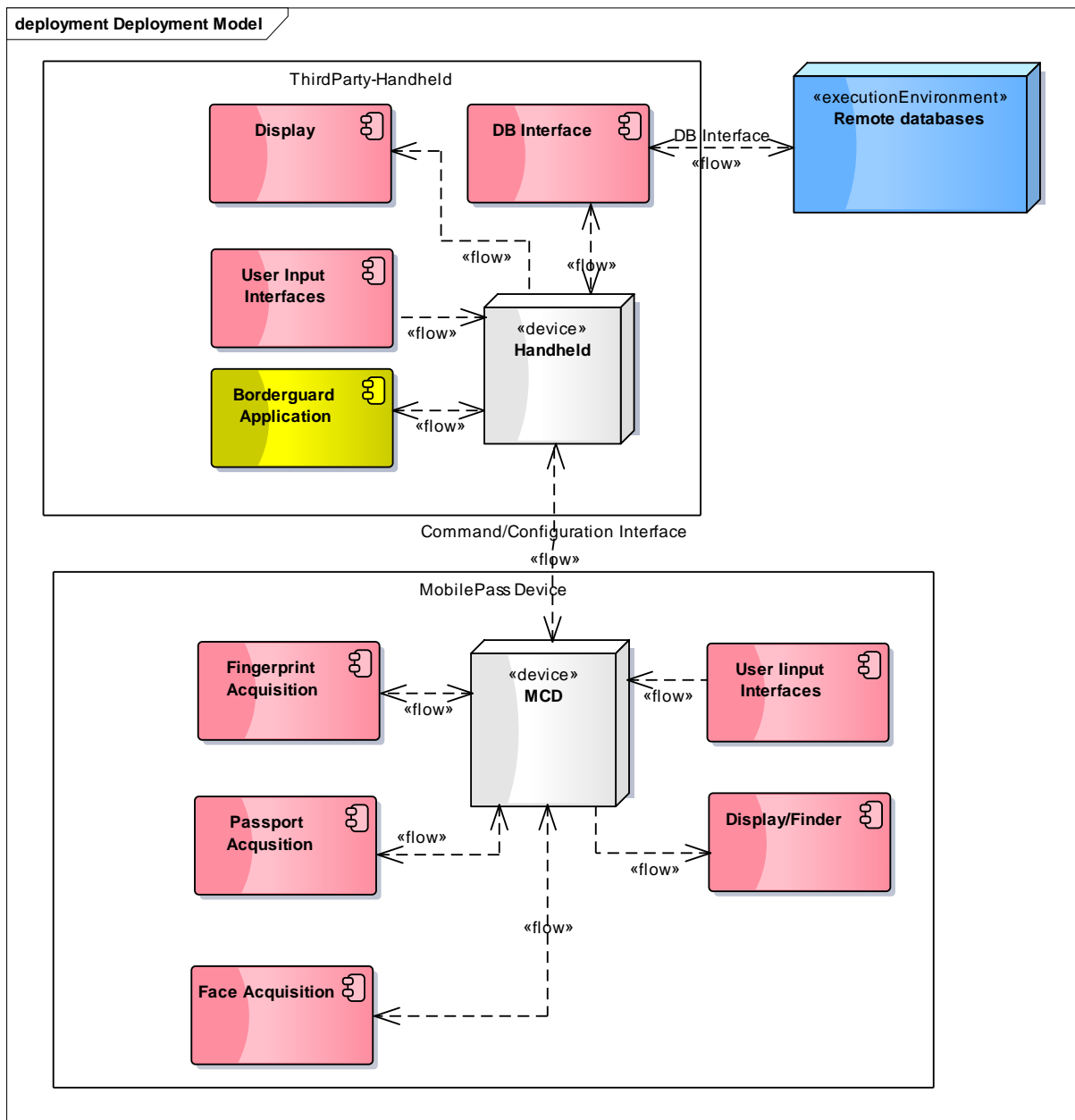


Figure 35: Use case of remotely controlled MobilePass device

### 4.5.3 External Interfaces

For these two user cases two interfaces between the MobilePass device and external parts of the framework can be identified:

- The command and configuration interface between application and device. This interface should be same for both the user cases to be able to easily change between internal and external applications.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

- The interface to the database back-end's. In the remotely controlled mode this interface is operated by the application. In the standalone mode, the MobilePass device has to be able to access this interface.

These interfaces will be described in the Deliverable D1.4 Embedded Systems and Communication Architecture.

### 4.6 Backend Interface

The generic term backend represents the methods of accessing remote databases (national and international databases, EES[11], RTP[12]). These databases are partly specific to each country and are partly accessed through a centralized service which is specific to each country as it is operation by national authorities. These centralized services handle the different login schemes for the different databases. The MobilePass framework strives to be interoperable within any country located in the EU.

The required databases that need to be accessed are:

- Schengen Information System (SIS)[17]
- Visa Information System (VIS)[16]
- Interpol databases
- Entry/Exit database (EES) [11]
- Registered Travellers programme (RTP) [12]
- National tracing, vehicle information and watch list databases

A basic check would require transmitting the gathered personal data (traveller's document data, biometric features) to a verification system and waiting for the check results. This would result in the traveller either being allowed to enter the country or being rejected in the first level check and being forwarded to the second level border checks.

The database interface which is exposed in the system management subsystem of the MobilePass device (see Figure 36) provides a unified interface for accessing all databases. In general, the interface to the back-end depends on the national implementation. In the future, unification may facilitate the adaption to new databases or national implementations. If necessary the database interface can be implemented as a remote service or can be implemented in the national database access points as a service.

Authentication will use a separate subsystem to store the necessary information received during authentication from the database interface. This information will be used to sign messages or be passed as session tokens for further communication with the national access points.

To manage certificates for distributed readers a Terminal Control Center (TCC) can be used. It is specified in the Technical Guideline 3129 of the German BSI [10]. Using a TCC, a hardware reader does not have to store certificates locally in order to authenticate itself to an electronic travel

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

document. The TCC can either be directly integrated to a terminal with multiple readers or it can be used remotely with a permanent online connection.

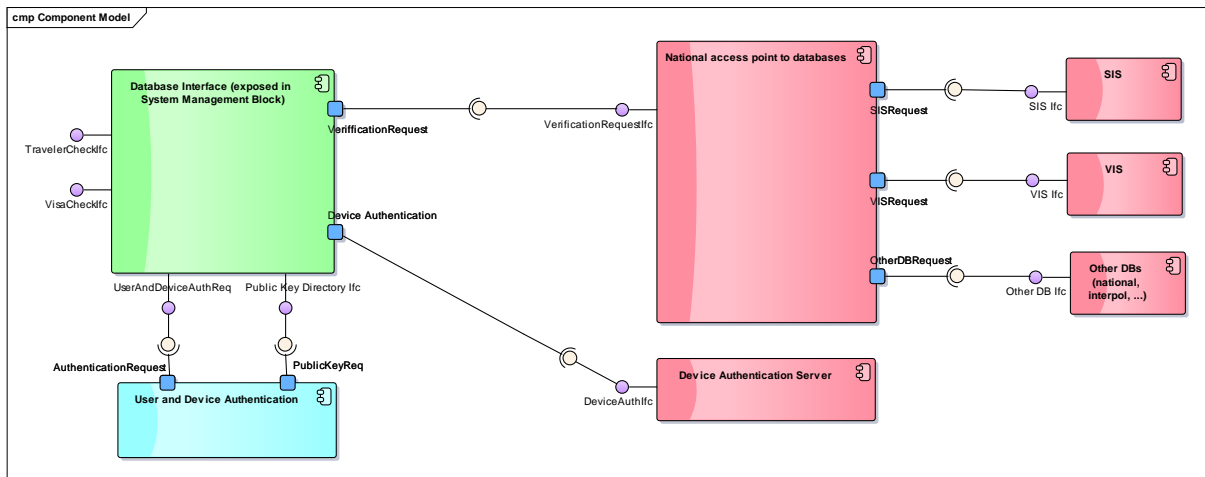


Figure 36: Interface to back-end's

In addition to the interface with the above said external systems, a web service communication with central systems must be addressed in order to collect information about the border crossing process:

- Web service in charge of feeding the Operational record (see section 4.6.2), it means collecting information about the border crossing for statistical purposes
- Web service in charge of distributing the configuration parameters set remotely to every mobile device
- Web service in charge of distributing the validations taken into account in the decision matrix (see section 4.6.1.3)

**4.6.1 Central System**

Central systems should provide all the functionalities involved in the border crossing process, allowing an easy and customizable deployment in a central servers.

Central services can be separated into three centralized modules:

1. Admin & Monitoring - Aimed at user management (including users, profiles, roles, etc.), remote system monitoring for all mobile devices and their components
2. QA & Accounting - This module is designed for statistics and reports, including both predefined and customized reports in real time. It involves also the patterns management database as well as the remote database distribution process to each mobile installation. Finally, Border Crossing decision matrix is also included in this module, allowing the configuration of the predefined parameters to be considered during the border crossing process.
3. Supervisor - It allows to check the operation of every MobilePass device in real time

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

These modules should be deployed on an application server. The SOA[14][15] software architecture of Central modules should be designed to be independent of the implementation technology.

### 4.6.1.1 *User Management*

This module allows creating, updating and deleting users, groups and roles in central system. Every user will access the central system with credentials (login/password) stored in central database. The integration with a LDAP[13] will be possible, if needed. The system will check the existence of this user and will obtain the permissions related to this user group. The user management module permits:

- Creation/edition of groups - it involves the permissions which a group of users is granted
- Creation/edition of statistics groups - it allows selecting the mobile devices for which each group has access for statistical data exploitation.

### 4.6.1.2 *Mobile Devices Configuration*

The configuration of every mobile device operating in different border crossing points allows registering new devices, modifying the existing ones and removing them if required. It also involves the configuration of the device components, previously registered in the system. The parameters included in this module are fully customizable.

### 4.6.1.3 *Decision Matrix*

The decision matrix allows choosing which of the verifications carried out by the MobilePass device will be taken into account in the border crossing point and which ones can be ignored. Changes performed in the decision matrix will affect the identification modules directly in one mobile device.

Each configuration parameter related to a particular verification can be selected or unselected:

- Active Authentication
- Passive Authentication
- Chip Authentication
- Terminal Authentication
- MRZ comparison
- Black/Watch list search
- IR patterns
- UV patterns

### 4.6.1.4 *Monitoring*

The monitoring functionality provides an interface showing the operating state of every mobile device registered and deployed in the border crossing points. The system shows the detail of every device and the alarms that may arise in case of malfunctions etc.

This interface will show the detail of each device and the alarms which may arise in case of malfunction. Different possibilities can be handled, such as “Properly operating device” and “Partial

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

operation” if any of the components of the device presents a defect (e.g. identification system is out of service) or the communication of any component of the mobile device with an external system is lost. “Incorrect operation” is displayed in case the incident prevents the device to fulfil its functionality (e.g. all the identification systems are out service, passport reader doesn’t work, etc.). “No connection” is displayed in case the device is not accessible from central server and thus it cannot be monitored.

In case the monitoring system detects changes in hardware or software, an alarm will alert the central system and the mobile device will be blocked in order to prevent it to access the back-end. The same applies in case the device has been reported stolen or the user credentials entered into the system are repeatedly wrong after a maximum number of attempts. In this case a memory wipe will be triggered and the certificate for the online connection will be revoked.

### 4.6.1.5 *Statistics*

This module allows the access to any statistical data stored in the system by filtering:

- Dates
- Mobile device, document issuing country and type of document
- Range of processing times, facial biometrics, fingerprint biometrics, etc.

### 4.6.1.6 *Patterns Database*

A pattern database containing most of the eMRTDs should be provided. In order to guarantee the authenticity of the document this database can be configured to make it possible to search the security measures or patterns required. The different versions of the pattern database are accessible and downloadable.

### 4.6.1.7 *Supervisor*

Central system should include a Supervisor module of the overall performance of the mobile devices deployed. It implies that the supervision of every border crossing process in real time is shown on screen for the identification process of every traveller. The supervisor module provides information about:

1. Summary of border crossing was performed and the result of the border crossing is checked in real time showing on screen:
  - a. Mobile device Id, the device where the identification process is being performed, must be identified
  - b. Facial image extracted from the chip
  - c. Live facial image captured by the mobile device
  - d. Type of document
  - e. Flag of the issuing country
  - f. ICAO code of the issuing country
  - g. Results comprising of validation and physical logical verification of the document.
  - h. Result of watch lists check. In order to identify criminal records and stolen documents

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

- i. Result of biometric verification shows the result of the comparison between the live photo with the facial image stored in the travel document and the photo printed on the data page surface
  - j. Global result of border crossing process shows different states as a result of the checks performed. It can be:
    - Pending - in case the crossing has not been completed yet
    - Correct - all the checks were successful
    - Incorrect - in case the result of any of the checks is incorrect, the global result will be failed and an alarm will be generated
2. The result of the verification of the travel document will be displayed:
- a. Summarize of the traveller's personal data
  - b. Logical verification - it comprises the verification of the information stored in the chip as well as the inspection ICAO/BSI EAC involving:
    - BAC - needed to access the chip
    - PA - certifies that the document was issued and signed by the origin country
    - EAC - it implies Chip Authentication and Terminal Authentication, needed to access the fingerprints, if needed
    - Comparison between the visual MRZ and the chip MRZ (DG1)
  - c. Physical verification:
    - Visualization and recognition of the security measures, comparing the pattern obtained with the one expected
    - Checking of optical whiteners under Ultraviolet
    - Checking of inks transparent to Infrared
    - Scanned picture viewer
  - d. Biometric verification compares the live photo with the one in the chip, and the printed one on the data page

### 4.6.2 Operational record

It corresponds to the Quality control and Business Statistics Databases referred in Frontex Best Practices Guidelines. It is the most relevant database in central services and stores all the data related to the crossing border processes. The only operations allowed on the operational record are insertions (insert) and queries (select). No deletions or updates are permitted.

It contains the following information:

<b>Name</b>	<b>Type</b>	<b>Description</b>
DATE	DATE	Date of the identification process
MOBILE DEVICE	STRING	Name/ Identifier of the mobile device
IDENTIFICATION COMPONENT	STRING	Mobile device identification component



**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

TYPE OF DOCUMENT	STRING	Type of document (Passport, VISA, etc)
ISSUING COUNTRY	STRING	Travel document issuing country (ICAO code 3 characters)
SEX	STRING	Sex of the document holder (ICAO code 1 character)
AGE	LONG	Age of the document holder
VIN	STRING	Vehicle identification number (VIN)
IDENTIFICATION TOTAL TIME	LONG	Total duration of the identification process
ACCESS TIME INSPECTION SYSTEM	LONG	Time spent in the access to inspection system (Passport=EDIS)
ACCESS TIME TO ATLAS	LONG	Time spent in the access to the watch list external system
DOCUMENT VERIFICATION TIME	LONG	Total time spent in the physical verification of the document (scanning, optical recognition, MRZ extraction, pattern comparison, etc.)
FINGERPRINT RECOGNITION TIME	LONG	Total time spent in fingerprint capture/recognition
TOTAL TIME ACCES BORDER	LONG	Total time spent in border crossing
TIME FACIAL TEMPLATE	LONG	Time from the facial capture until the detection of the first template with enough quality
TIME FINGERPRINT_TEMPLATE	LONG	Time from the fingerprint capture until the detection of the first template with enough quality
FINAL RESULT	BOOLEAN	Final result of the identification process
RESULT OF THE BIOMETRIC VERIFICATION	BOOLEAN	Result of the biometric verification
RESULT OF THE FACIAL VERIFICATION	BOOLEAN	Result of the facial recognition

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

RESULT OF THE FINGERPRINT VERIFICATION	BOOLEAN (ALLOW NULL)	Result of the fingerprint recognition
RESULT OF THE PHYSICAL VERIFICATION	BOOLEAN	Result of the document physical verification (only for passport)
RESULT OF THE CHIP VERIFICATION	BOOLEAN	Result of the document logical verification (only for passport)
RESULT OF MRZ VERIFICATION	BOOLEAN	Result of comparison between MRZ printed and MRZ in the chip (only for passport)
RESULT OF DOCUMENT VERIFICATION	BOOLEAN (ALLOW NULL)	Result of document verification
RESULT VERIFICATION ATLAS CRIMINAL RECORDS	BOOLEAN (ALLOW NULL)	Result of criminal records checks in external system.
RESULT OF DOCUMENT VERIFICATION ATLAS	BOOLEAN (ALLOW NULL)	Result of document checks in external system.
RESULT OF CHIP PA VERIFICATION	BOOLEAN (ALLOW NULL)	Result of Passive Authentication (only for passport).
RESULT OF CHIP AA VERIFICATION	BOOLEAN (ALLOW NULL)	Result of Active Authentication (only for passport).
RESULT OF CHIP CA VERIFICATION	BOOLEAN (ALLOW NULL)	Result of chip authentication (only for 2nd generation passport).
RESULT OF CHIP TA VERIFICATION	BOOLEAN (ALLOW NULL)	Result of terminal authentication (only for 2nd generation passport)
RESULT OF CHIP BAC VERIFICATION	BOOLEAN (ALLOW NULL)	Result of basic access control (BAC) (only for passport).
RESULT OF _VERIFICACION CHIP_RD	BOOLEAN (ALLOW NULL)	Result of reading DGs (only for passport)

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

ERROR MESSAGE CHIP VERIFICATION	STRING	Error message (in case of error when reading or electronic verification of the document).
ERRORS IR AREAS	BYTE (ALLOW NULL)	Number of errors in IR areas (only for passport)
ERRORS UV AREAS	BYTE (ALLOW NULL)	Number of errors in UV areas (only for passport).
ERRORS_IR PATTERNS	BYTE (ALLOW NULL)	Number of errors in IR light patterns (only for passport)
ERRORS UV PATTERNS	BYTE (ALLOW NULL)	Number of errors in UV light patterns (only for passport)
ERRORS VISIBLE PATTERN	BYTE (ALLOW NULL)	Number of errors in visible light patterns (only for passport)
FACIAL_SCORE	DOUBLE	Score reached in facial recognition
FACIAL_ACEPTANCE TRESHOLD	DOUBLE	Acceptance threshold in facial recognition
FACIAL_REJECTION TRESHOLD	DOUBLE	Rejection threshold in facial recognition
FACIAL_RANGE	STRING	Value range score/threshold in facial recognition
FACIAL_RELIABILITY PHOTO CAPTURED	DOUBLE	Reliability of the best photogram live capture (0-100)
FACIAL_QUALITY_PHOTO_CAPTURED	DOUBLE	Quality of the best photogram live capture (0-255)
FACIAL_RELIABILITY CHIP PHOTO	DOUBLE	Reliability of the photo stored in the chip (0-100)
FACIAL_QUALITY CHIP PHOTO	DOUBLE	Quality of the photo stored in the chip (0-255)
FACIAL_RELIABILITY_PHOTO	DOUBLE	Reliability of the printed photo image (0-100)

**Vision and Requirements of the Future**

Version 0.9, 30.12.2014

PRINTED		
FACIAL_QUALITY PHOTO PRINTED	DOUBLE	Quality of the photo printed (0-255)
FINGERPRINT_COMPLETED	BOOLEAN	Fingerprint recognition completed
FINGERPRINT_SCORE	DOUBLE	Score reached in fingerprint recognition
FINGERPRINT TRESHOLD	DOUBLE	Fingerprint recognition threshold
FINGERPRINT RANGE	STRING	Range of score/threshold in fingerprint recognition
CAPTURED FINGERPRINT QUALITY	DOUBLE	Quality of the fingerprint captured (0-255).
CHIP FINGERPRINT QUALITY_	DOUBLE	Quality of the fingerprint stored in the chip (0-255)
FINGERPRINT QUALITY DEVICE	DOUBLE	Quality of the fingerprint captured in the mobile device identification (0-255)
MULTIBIOMETRIC_SCORE	DOUBLE	Score reached in multi biometry
MULTIBIOMETRY_TRESHOLD	DOUBLE	Multibiometry threshold
MULTIBIOMETRY_RANGE	STRING	Range of score/threshold in multibiometry
BIOMETRIC FUNCTION NAME	STRING	Biometric algorithm name
FALSE BIOMETRY REJECTION	STRING	In case of error during the biometric recognition, it is due to the operation of the system.
FALSE REJECTION ATLAS	STRING	In case of error during the ATLAS external system verification, it is due to the operation of the system

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

FALSE REJECTION DOCUMENT	STRING	In case of error during the document verification due to the operation of the system.
--------------------------	--------	---

### 4.7 Security Concept

This section will address the security issues of a mobile handheld device. As the access to the national and international databases as well as to the MobilePass framework is security critical, the device has to prevent efforts to compromise the operating system and to be able to discontinue access to the databases if a device is stolen.

#### 4.7.1 Trusted Boot

In a security critical environment it is of great importance to be able to prevent changes to the operating system of the device. During the boot process of a device, the processor will execute its first level boot loader which in turn loads and executes a second stage boot loader. This boot loader will then load the operating system image and then jump to the entry point of the OS.

The first step to securing the device against compromised images is the use of a verified boot system. In this case the OS image is signed with a generated private key of an asymmetric encryption method. The second stage boot loader knows the public key portion of the key pair and checks the signature of the image when loading the image. After loading the image, the boot loader has the possibility to deny execution of an image that fails signature verification. Thus, images from a certified manufacturer or developer are allowed.

However, this method does not prevent a malicious party from exchanging the second stage boot loader with a boot loader that does not use verification. To overcome this problem the second stage boot loader has to be placed in read only memory enlarging the root of trust and making it immutable. Another possibility would be the use of a verifying first stage boot loader. However, as this boot loader is processor manufacturer dependent, it requires a high volume of devices to justify the costs of this.

With these mechanisms it is possible to disallow the execution of malicious code on the MobilePass devices. Nevertheless, one could still extract the image from the flash memory of the device and execute it on a hardware platform without a verifying boot loader. Two approaches are possible to circumvent this problem:

- Encrypt the operating system image
- Use a measured boot mechanism to scan the used hardware and check the hardware configuration during operating system start

The problem with encrypting the image is the storage of the private key needed to decrypt the image. It has to be accessible by the boot loader but must not be readable by other parties. Thus, storing keys in external memory blocks is not applicable solution. One possibility would be the use of

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

on-chip read only memory within the system-on-chip. This makes it virtually impossible to read the keys. However, this option is only available in certain microprocessors with built-in security features (hardware encryption engines, tamper detection) which might not provide other features that are needed within the device.

A second option is the use of a cryptographic coprocessor such as the Trusted Platform Module (TPM) [6]. This chip provides security features such as:

- Platform configuration registers (PCR) useable to perform a measured boot ensuring the integrity of the system
- Hardware encryption/decryption engine, its private keys never leave the chip
- Data encryption for secure storage
- Message signing for secure communication

In case of using a measured boot method the boot process will create hashes of all relevant software parts during the boot sequence. The TPM provides the PCR mechanism to store and process these hashes and to create boot log holding the results. This can then be compared to a history file or sent to a remote attestation service.

As discussed it may not be feasible to store all necessary keys to fully encrypt and secure an image such that it cannot be read by other parties. Instead, two-level authentication mechanisms using the users' security token or credentials may be used. These tokens or credentials could be used during the boot process to authenticate with a TPM or decrypt the necessary keys directly. Although, this does not guarantee that a thief may acquire both the device and a user's secrets. Furthermore, the user could be presented with a fake device, which has a built-in memory extracted from a stolen device. Using this method a man-in-the-middle-attack can be performed to extract the necessary keys to decrypt the boot image which in turn breaks the chain-of-trust.

### 4.7.2 Device Authentication

All devices should be able to authenticate themselves within the wide area network that the MobilePass framework will work in. An ideal device would provide means to certify that it is running an official and uncompromised operating system on the exact hardware that the developers are expecting. The remote endpoints the device should communicate with use remote attestation methods to verify the device's authenticity and only process the requests of the device if it passes attestation.

A mobile device that has been reported stolen or has failed remote attestation (due to changed hardware or software) might still contain valuable information for the intruder. To circumvent this, a mechanism to perform a memory wipe triggered from a remote end point would be useful. This should erase the operating system and root file system, if an illegal attempt to access from the back-end occurs or if a device that has been reported stolen tries to log on to the network. In combination with requesting the repeated input of a user's credentials at a certain frequency, this would reduce the window of opportunity to exploit the device's connection drastically.

## 5 Annex

### 5.1 References

- [1] S P Gupta, S Keates and P J Clarkson, Usability considerations in the design of handheld electronic devices, International conference on Engineering design, ICED 03 Stockholm, August, 19-21, 2003
- [2] Mital, A., & Kilbom, A. (1992) Design, selection and use of hand tools to alleviate trauma of the upper extremities: Part I – Guidelines for the practitioner. Int. J. of Ind. Erg. 10, pp 1-5.
- [3] ICAO GUIDELINES: electronic – Machine Readable Travel Documents & Passenger Facilitation; Version – 1.0; Date – April 17, 2008; Architectural Design Considerations; pg. 40
- [4] COM(2011)680 - Smart borders - options and the way ahead
- [5] Axel Weissenfeld, et al, "Scenario list: Deficiencies, Handling problems Deliverable 1.1", MobilePass - A secure, modular and distributed mobile border control solution for European land border crossing points, FP7-SEC-2013-3-2-3
- [6] Trusted Computing Group, TPM Main Specification, [http://www.trustedcomputinggroup.org/resources/tpm\\_main\\_specification](http://www.trustedcomputinggroup.org/resources/tpm_main_specification)
- [7] Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems v.1.1
- [8] Best Practice Operational Guidelines for Automated Border Control (ABC) Systems v2.0
- [9] Best Practice Technical Guidelines for Automated Border Control (ABC) Systems v2.0
- [10] [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03129/BSI\\_TG\\_03129.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03129/BSI_TG_03129.pdf)
- [11] [http://ec.europa.eu/dgs/home-affairs/doc\\_centre/borders/docs/1\\_en\\_act\\_part1\\_v12.pdf](http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v12.pdf)
- [12] [http://ec.europa.eu/dgs/home-affairs/doc\\_centre/borders/docs/1\\_en\\_act\\_part1\\_v14.pdf](http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v14.pdf)
- [13] Dieter Klünter / Jochen Laser: LDAP verstehen, OpenLDAP einsetzen. Grundlagen und Praxiseinsatz. dpunkt.verlag, Heidelberg 2007, ISBN 978-3-89864-263-7.
- [14] Jump up "Service Oriented Architecture : What Is SOA?". opengroup.
- [15] Jump up "SOA Reference Architecture Technical Standard : Basic Concepts". opengroup. Retrieved 2014-10-10.
- [16] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008R0767:EN:NOT>
- [17] <http://www.statewatch.org/news/2013/mar/eu-council-sis-stats-7389-13.pdf>
- [18] ISO/IEC 11889-1:2009. ISO.org. International Organization for Standardization. Retrieved 29. November 2013
- [19] TPM Main Specification Level 2 Version 1.2, Revision 116 Part 1 - Design Principles. Retrieved 2012-06-14.
- [20] `tspi_data_bind(3)` - Encrypts data blob. Trusted Computing Group. Retrieved 2009-10-27.
- [21] TPM Main Specification Level 2 Version 1.2, Revision 116 Part 3 - Commands. Trusted Computing Group. Retrieved 2011-06-22.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

### 5.2 Databases

#### 5.2.1 Schengen Information System (SIS)

The SIS is a shared database of information on individuals and objects of interest to EU countries. Its purpose is to support police and judicial co-operation, manage external border controls and maintain public security. All EU countries can create entries on the database called "alerts" which provides information on missing people, people wanted for extradition or arrest, and people who are needed in relation to criminal cases or public security threats. They can also create alerts on property for seizure or use in criminal proceedings. Schengen Information System is not applicable in UK and Ireland according to their exemption from SIS, but some other non-EU countries use SIS. Norway, Iceland, Switzerland and Liechtenstein are members of SIS and use it.

When you cross an external border into an EU country (excluding Ireland and the United Kingdom), the immigration authorities will automatically check to see if you are the subject of a SIS alert.

Personal relevant information stored in the SIS covers the following points:

- Surname, given name and middle initial
- Aliases used by an subject
- Any specific objective physical characteristics not subject to change
- Date and place of birth
- Nationality
- Sex
- Reason for an alert
- Action to be taken if the subject has been discovered
- Information, if the subject was armed, violent or escaped

The following alerts are kept:

- Alerts pertaining to persons wanted for arrest for extradition purposes
- Alerts pertaining to foreign nationals who were refused the right of entry
- Alerts pertaining to missing persons or persons who disappear for their own protection or in order to prevent threats, need to be temporarily placed under police protection
- Alerts pertaining to witnesses, persons summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted, persons who are to be served with a criminal judgement or a summons to report in order to serve a penalty involving deprivation of liberty
- Alerts pertaining to discreet surveillance of persons and vehicles

#### 5.2.2 Visa Information System (VIS)

The VIS is a shared database with information of people who have applied for short-stay visas to visit or pass through Europe's border-free travel zone, the Schengen area. The VIS allows EU countries to



## Vision and Requirements of the Future

Version 0.9, 30.12.2014

exchange data on short-stay visa requests and decisions on refusal, extension, annulment or withdrawal of visas. When you present your short-stay visa to the border authorities of the first Schengen area country you enter, your details will automatically be cross-checked in this shared database.

There are two types of search request, verification and identification. Identification requests search the whole database for matches, verification requests only match the fingerprints scanned at the border crossing point with those associated with the biometric data of the visa. If fingerprints cannot be taken, one can perform a request with the following data stored in the VIS:

- surname, surname at birth, first names
- sex
- date, place and country of birth
- current nationality and nationality at birth of the visa applicant
- type and number of the travel document, the authority that issued it and the date of issue and expiry
- main destination and duration of the intended stay
- purpose of travel, and intended date of arrival and departure
- intended border of first entry or transit route
- residence
- fingerprints
- type of visa and number of the visa sticker
- details of the person that has either issued an invitation for the visa applicant or is liable for the applicant's subsistence costs during his/her stay

### 5.2.3 INTERPOL

INTERPOL's secured global police communications system, I-24/7, connects law enforcement officials in its member countries to each other and to INTERPOL's criminal databases. Those related to border security are hosted in the INTERPOL Travel and ID Document Reference Centre. Border points are critical locations for preserving national security. Therefore, INTERPOL assists countries in allowing instant access to its databases by both first-line and second-line inspection officials at airports, sea ports and border crossings. Technical solutions called MIND/FIND allow for interoperability with existing national border security infrastructure.

As for border controls, the Interpol databases are queried with information extracted from the MRZ of a passenger. In case of a hit, the system does not return any information about the subject so that the responsible authorities can be contacted.

Operational databases available for first-line checks:

- Stolen and Lost Travel Document database (SLTD)  
Helps identify the illegal use of passports reported as lost, stolen, stolen in blank or revoked.
- Nominal databases  
Records of known international criminals and missing persons.

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

- **Travel Documents Associated with Notices (TDAWN)**  
Helps to identify criminals subject to INTERPOL notices when checking their travel documents.
- **Stolen Motor Vehicles database (SMV)**  
Records of vehicles reported stolen around the world.
- **Stolen Vessels Database (SV)**  
Provides identification information on stolen vessels, to assist investigations.

### 5.2.4 Entry Exit Database (EES)

There is no EU wide entry/exit database at the moment. The proposal in [11] lists the following data fields (MRZ data and additional fields regarding the border crossing of the traveller)

- Passport type
- Issuer
- Surname
- Given Names
- Passport number
- Nationality
- Date of birth
- Sex
- Expiration date
- Personal number
- Chip Image
- Border Crossing Point
- Date
- Time
- Visa Number
- Visa Validity
- (Authority)
- (Member State)
- (Fingerprint)

### 5.2.5 Registered Traveller Programme (RTP)

There is no EU wide RTP database at the moment. The proposal in [12] lists the following data fields. A request to the RTP will contain a unique identifier number and the fingerprints of the traveller.

- A unique application number
- Fingerprints of the passenger
- Status information, indicating that access to the RTP has been requested
- The authority with which the application has been lodged, including its location
- The surname, surname at birth and first names of the passenger
- The date, place and country of birth of the passenger.
- The nationality(ies) of the passenger
- The type and number of the travel document(s), as well as the authority, which issued it and the date of issue and of expiry
- The place and date of the application

## Vision and Requirements of the Future

Version 0.9, 30.12.2014

- If applicable, the details of the person liable to pay the applicant's subsistence costs during the stay, being:
  - (i) In the case of a individual person, the surname and first name, address of the person and telephone number
  - (ii) In the case of a company or other organisation, the name and address of the company/other organisation, surname and first name of the contact person in that company/organisation and telephone number
- The main purposes of the journey
- The applicant's home address and telephone number
- If applicable, the visa sticker number
- If applicable, the residence permit or residence card number
- The current occupation and employer; for students: name of educational establishment.
- In the case of minors, surname and first name(s) of the applicant's parental authority or legal guardian
- Information regarding refused, revoking or extending access to the RTP