

**H2020 – BES – 5 – 2015**

**Research Innovation Action**



**Intelligent Portable ContROl SyStem**



*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700626*

## **D2.2 Reference Architecture and components specifications**

Report Identifier:	D2.2		
Work-package, Task:	WP2	Status – Version:	1.0
Distribution Security:	CO	Deliverable Type:	R
Editors:	EVR, ICCS		
Contributors:	ALL PARTNERS		
Reviewers:	ED, STR		
Quality Reviewer:	ED		
Keywords:	Definition of the Reference Architecture of the iBorderCtrl framework, high level system design, technical specifications and interfaces, system hardware and firmware.		
Project website: <a href="http://iborderctrl.eu/">http://iborderctrl.eu/</a>			

### **Copyright notice**

© Copyright 2016-2019 by the iBorderCtrl Consortium

This document contains information that is protected by copyright. All Rights Reserved. No part of this work covered by copyright hereon may be reproduced or used in any form or by any means without the permission of the copyright holders.

## Table of Contents

<b>ABBREVIATIONS.....</b>	<b>9</b>
<b>EXECUTIVE SUMMARY.....</b>	<b>11</b>
<b>1 INTRODUCTION.....</b>	<b>12</b>
1.1 PURPOSE OF THIS DOCUMENT.....	12
1.2 STRUCTURE OF THE DOCUMENT.....	12
<b>2 REQUIREMENTS .....</b>	<b>14</b>
2.1 TECHNICAL REQUIREMENTS DERIVED FROM THE ANALYSIS OF FUNCTIONAL (END USERS) AND GENERAL REQUIREMENTS FROM D2.1.....	14
<b>3 DESCRIPTION OF THE IBORDERCTRL INTERDISCIPLINARY TECHNOLOGIES .....</b>	<b>38</b>
3.1 AUTOMATIC DECEPTION DETECTION SYSTEM (ADDS) DESCRIPTION.....	40
3.1.1 Technical Requirements derived from the SOTA analysis from D2.1 .....	41
3.1.2 Functional description .....	42
3.1.3 Additional Technical Requirements derived from Architecture Components .....	48
3.2 DOCUMENT AUTHENTICITY ANALYSIS TOOL (DAAT) DESCRIPTION .....	49
3.2.1 Technical Requirements derived from the SOTA analysis from D2.1 .....	49
3.2.2 Functional description .....	50
3.2.3 Additional Technical Requirements derived from Architecture Components .....	51
3.3 BIOMETRIC MODULE (BIO) DESCRIPTION.....	52
3.3.1 Technical Requirements derived from the SOTA analysis from D2.1 .....	53
3.3.2 Functional description .....	54
3.3.3 Additional Technical Requirements derived from Architecture Components .....	55
3.4 FACE MATCHING TOOL (FMT) DESCRIPTION .....	56
3.4.1 Technical Requirements derived from the SOTA analysis from D2.1 .....	57
3.4.2 Functional description .....	57
3.4.3 Additional Technical Requirements derived from Architecture Components .....	59
3.5 HIDDEN HUMAN DETECTION TECHNOLOGY (HHD) DESCRIPTION .....	60
3.5.1 Technical Requirements derived from the SOTA analysis from D2.1 .....	61
3.5.2 Functional description .....	62
3.5.3 Additional Technical Requirements derived from Architecture Components .....	64
3.6 RISK BASED ASSESSMENT TOOL (RBAT) DESCRIPTION.....	65
3.6.1 RBAT Functional Description.....	65
3.6.1.1 Rule Authoring.....	65
3.6.1.2 Risk Evaluation .....	66
3.6.1.3 Risk Assessment.....	67

---

3.6.1.4	Automatic Suggestion and Optimization .....	67
3.6.2	Additional Technical Requirements derived from Architecture Components .....	67
3.7	INTEGRATED BORDER CONTROL ANALYTICS TOOL (BCAT) DESCRIPTION .....	68
3.7.1	Technical Requirements derived from the SOTA analysis from D2.1 .....	68
3.7.2	Functional description .....	69
3.7.3	Additional Technical Requirements derived from Architecture Components .....	71
3.8	EXTERNAL LEGACY AND SOCIAL INTERFACES (ELSI) DESCRIPTION .....	73
3.8.1	Technical Requirements derived from the SOTA analysis from D2.1 .....	73
3.8.2	Functional description .....	73
3.8.3	Additional Technical Requirements derived from Architecture Components .....	79
<b>4</b>	<b>GENERAL CONSTRAINTS .....</b>	<b>80</b>
4.1	LEGAL CONSTRAINTS .....	80
4.1.1	Data Subject's Rights .....	80
4.1.2	Privacy and Security by Design .....	80
4.1.3	Data Protection Impact Assessment .....	81
4.1.4	Data Protection Requirements .....	81
4.1.5	IT Security Requirements .....	84
4.2	MAINTAINABILITY AND EXTENSIBILITY/ SCALABILITY .....	88
4.3	GENERAL (HARDWARE AND ADDITIONAL) SYSTEM CONSTRAINTS .....	90
4.4	RISK MITIGATION PLAN D1.2 .....	91
<b>5</b>	<b>USE CASES .....</b>	<b>95</b>
5.1	PRE-REGISTRATION GENERAL SCENARIO .....	95
5.2	"ON BORDER" CROSSING POINT CHECK GENERAL SCENARIO .....	98
5.3	"ON BORDER" CROSSING POINT CHECK WITH NO PRE-REGISTRATION SCENARIO .....	101
5.4	TRAVELLER CROSSING THE BORDER IN THEIR OWN PRIVATE VEHICLE SCENARIO .....	103
5.5	TRAVELLER CROSSING THE BORDER IN A VEHICLE USED FOR THE TRANSPORT OF GOODS SCENARIO ....	103
5.6	TRAVELLER CROSSING THE BORDER "ON BOARD" A COACH BUS OR TRAIN SCENARIO .....	103
5.7	FREIGHT TRAIN CROSSING THE BORDER SCENARIO .....	105
5.8	WORKFLOWS .....	106
5.8.1	Pre-registration phase .....	106
5.8.2	Crossing border phase .....	108
<b>6</b>	<b>THE OVERALL IBORDERCTRL FUNCTIONAL ARCHITECTURE .....</b>	<b>109</b>
6.1	USER INTERACTION WITH THE SYSTEM .....	111

6.2	IBORDERCTRL SYSTEM – DATA HANDLING (INPUTS / OUTPUTS) .....	112
6.3	IBORDERCTRL SYSTEM – INTEGRATION OF COMPONENTS AND RELATED INTERCONNECTIONS .....	113
6.4	SOFTWARE STACK .....	115
6.5	DATA BASE DESCRIPTION AND ARCHITECTURE .....	118
6.6	PORTABLE UNIT ARCHITECTURE DESIGN .....	120
6.6.1	Portable Unit description .....	121
6.6.2	Wireless Radio Network connection of the portable units.....	126
6.6.2.1	Functional Description of the Radio Network .....	126
6.6.2.2	Break Down of the basic network connections.....	127
6.6.2.3	Practical Aspects of Network Dimensioning .....	129
<b>7</b>	<b>USERS MANAGEMENT AND USERS INTERFACES.....</b>	<b>132</b>
7.1	TRAVELLERS’ USER INTERFACE DESCRIPTION .....	133
7.2	BORDER GUARDS AGENT USER INTERFACE (AUI) .....	140
7.3	BORDER MANAGERS AGENT USER INTERFACE (AUI).....	146
<b>8</b>	<b>FINAL CONCLUSIONS - TRACEABILITY MATRIX .....</b>	<b>149</b>

## List of Tables

TABLE 1 LIST OF IBORDERCTRL TECHNICAL REQUIREMENTS FROM FUNCTIONAL REQUIREMENTS FOR THE PRE-ARRIVAL PHASE .....	15
TABLE 2 LIST OF IBORDERCTRL TECHNICAL REQUIREMENTS FROM FUNCTIONAL REQUIREMENTS FOR THE BACKGROUND CHECK PHASE .....	21
TABLE 3 LIST OF IBORDERCTRL TECHNICAL REQUIREMENTS FROM FUNCTIONAL REQUIREMENTS FOR THE BORDER CHECK PHASE .....	23
TABLE 4 LIST OF IBORDERCTRL TECHNICAL REQUIREMENTS FROM GENERAL FUNCTIONAL REQUIREMENTS .....	29
TABLE 5 LIST OF IBORDERCTRL COMPONENTS .....	38
TABLE 6 LIST OF ADDS TECHNICAL REQUIREMENTS BASED ON SOTA ANALYSIS .....	41
TABLE 7 LIST OF ADDS ADDITIONAL TECHNICAL REQUIREMENTS .....	48
TABLE 8 LIST OF DAAT TECHNICAL REQUIREMENTS BASED ON SOTA ANALYSIS .....	49
TABLE 9 LIST OF DAAT ADDITIONAL TECHNICAL REQUIREMENTS .....	51
TABLE 10 LIST OF BIO TECHNICAL REQUIREMENTS BASED ON SOTA ANALYSIS .....	53

---

TABLE 11 LIST OF BIO ADDITIONAL TECHNICAL REQUIREMENTS .....	55
TABLE 12 LIST OF FMT TECHNICAL REQUIREMENTS BASED ON SOTA ANALYSIS.....	57
TABLE 13 LIST OF FMT ADDITIONAL TECHNICAL REQUIREMENTS.....	59
TABLE 14 LIST OF HHD TECHNICAL REQUIREMENTS BASED ON SOTA ANALYSIS.....	61
TABLE 15 LIST OF HHD ADDITIONAL TECHNICAL REQUIREMENTS .....	64
TABLE 16 LIST OF RBAT ADDITIONAL TECHNICAL REQUIREMENTS .....	67
TABLE 17 LIST OF BCAT TECHNICAL REQUIREMENTS BASED ON SOTA ANALYSIS .....	69
TABLE 18 LIST OF BCAT ADDITIONAL TECHNICAL REQUIREMENTS .....	71
TABLE 19 LIST OF EXTERNAL INTERFACES TECHNICAL REQUIREMENTS BASED ON SOTA ANALYSIS .....	73
TABLE 20 EXAMPLE OF TWITTER’S API REQUESTS AND THEIR RESPONSE .....	74
TABLE 21 LIST OF ELSI ADDITIONAL TECHNICAL REQUIREMENTS .....	79
TABLE 22 LIST OF IBORDERCTRL DATA PROTECTION REQUIREMENTS.....	82
TABLE 23 LIST OF IBORDERCTRL IT SECURITY REQUIREMENTS .....	84
TABLE 24 LIST OF IBORDERCTRL MAINTAINABILITY REQUIREMENTS .....	89
TABLE 25 LIST OF IBORDERCTRL EXTENSIBILITY REQUIREMENTS .....	89
TABLE 26 LIST OF IBORDERCTRL SCALABILITY REQUIREMENTS.....	90
TABLE 27 LIST OF IBORDERCTRL GENERAL SYSTEM CONSTRAINTS / REQUIREMENTS.....	91
TABLE 28 LIST OF IBORDERCTRL ADDITIONAL ARCHITECTURAL COMPONENTS.....	110
TABLE 29 IBORDERCTRL DATA HANDLING .....	112
TABLE 30 PORTABLE UNIT MODULES AND REQUIREMENTS.....	124
TABLE 31 PORTABLE UNIT COMPLIANCE WITH EU STANDARDS.....	126
TABLE 32 802.11X STANDARDS .....	129
TABLE 33 TECHNICAL DETAILS OF DVB-S-STANDARDS .....	129
TABLE 34 IBORDERCTRL TRACEABILITY MATRIX .....	150

## List of Figures

FIGURE 1 RELATIONSHIP BETWEEN D2.1 AND D2.2 .....	14
FIGURE 2 DRAFT ARCHITECTURE DIAGRAM FOR ADDS .....	42

---

FIGURE 3 ADDS WORKFLOW .....	45
FIGURE 4 COMPONENTS OF ADDS .....	47
FIGURE 5 WORKFLOW AND ARCHITECTURE OF DAAT SYSTEM .....	50
FIGURE 6 BIO ARCHITECTURE AND WORKFLOW .....	55
FIGURE 7 FMT SYSTEM WORKFLOW.....	57
FIGURE 8 ARCHITECTURE OF THE HHD TOOL .....	62
FIGURE 9 RBAT ARCHITECTURE AND WORKFLOW .....	66
FIGURE 10 BCAT SYSTEM WORKFLOW .....	69
FIGURE 11 ELSI WORKFLOW SCHEMA .....	74
FIGURE 12 SIS II DATABASE DIAGRAM .....	77
FIGURE 13 VIS DATABASE DIAGRAM.....	78
FIGURE 14 PRE-REGISTRATION SCENARIO – DATA TREATMENT CONSENT .....	95
FIGURE 15 PRE-REGISTRATION SCENARIO – REGISTRATION IN THE SYSTEM.....	96
FIGURE 16 PRE-REGISTRATION SCENARIO – LOGIN IN THE SYSTEM.....	96
FIGURE 17 PRE-REGISTRATION SCENARIO – TRAVEL INFORMATION.....	97
FIGURE 18 CROSSING BORDER GENERAL SCENARIO FOR TCNs .....	98
FIGURE 19 CROSSING BORDER GENERAL SCENARIO FOR EC.....	100
FIGURE 20 CROSSING BORDER GENERAL SCENARIO WITHOUT PRE-REGISTRATION FOR TCNs.....	101
FIGURE 21 CROSSING BORDER GENERAL SCENARIO WITHOUT PRE-REGISTRATION FOR ECs .....	102
FIGURE 22 CROSSING BORDER “ON BOARD” TRAIN OR COACH BUS SCENARIO .....	104
FIGURE 23 CROSSING BORDER FREIGHT TRAIN SCENARIO.....	105
FIGURE 24 IBORDERCTRL NEW USER WORKFLOW .....	106
FIGURE 25 IBORDERCTRL PRE-ARRIVAL PHASE WORKFLOW .....	107
FIGURE 26 IBORDERCTRL BORDER CROSSING PHASE WORKFLOW .....	108
FIGURE 27 THE IBORDERCTRL FUNCTIONAL ARCHITECTURE .....	109
FIGURE 28 INTERCONNECTIONS AND COMMUNICATION .....	114
FIGURE 29 OVERALL ARCHITECTURE.....	115
FIGURE 30 ‘PURE’ IAAS .....	117
FIGURE 31 IAAS + PAAS + BACKING SERVICES .....	117
FIGURE 32 SELECTING YOUR DATABASE PLATFORM (UC BERKELEY’S IST DATABASE SERVICES DIVISION) .....	118

---

FIGURE 33 THE iBORDERCTRL DATABASE .....	119
FIGURE 34 HARDWARE ARCHITECTURE OF THE PORTABLE UNIT .....	120
FIGURE 35 SOFTWARE ARCHITECTURE OF THE PORTABLE UNIT .....	121
FIGURE 36 FORWARD/REVERSE RADIO CONNECTIONS .....	126
FIGURE 37 NETWORK DEPLOYMENT USING THE CELLULAR SYSTEM AS BACKHAUL LINK.....	128
FIGURE 38 NETWORK DEPLOYMENT USING THE SATELLITE LINK AS BACKHAUL LINK .....	128



## Abbreviations

4G	4 <sup>th</sup> generation of mobile telecommunications technology
ADDS	Automatic Deception Detection System
API	Application Programming Interface
APP	Application
BCAT	Border Control Analytics Tool
BCP	Border Crossing Point
BIO	Biometric Module
BMI	Border Manager Interface
CIRAM	Common Integrated Risk Analysis Model
CPU	Central Processing Unit
DAAT	Document Authenticity Analysis Tool
DoW	Description Of Work
DSP	Digital Signal Processing
EC	European Citizens
ELSI	External Legacy and Social Interfaces
EP	European Parliament
EU	European Union
FMT	Face Matching Tool
FPS	Frames Per Second
GUI	Graphical User Interface
HHD	Hidden Human Detection
HTTPS	Hypertext Transfer Protocol Secure
iBorderCtrl	Intelligent Portable Control System
ID	Identification
iFADO	Intranet False and Authentic Documents Online

MP	Mega Pixels
MRZ	Machine Readable Zone
NVB	Non-Verbal Behaviour
OS	Operative System
PC	Personal Computer
QR	Quick Response code
RBAT	Risk Based Assessment Tool
REST	Representational State Transfer
SIS	Schengen Information System
SOTA	State Of The Art
SQL	Structured Query Language
ST	Silent Talker
TCNs	Third Country Nationals
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VIS	Visa Information System
WI-FI	Wireless Fidelity - Wireless Internet
WP	Work Package

---

## Executive Summary

The purpose of this Deliverable is to create and define the general iBorderCtrl architecture, to provide the architectural framework for all the different modules that consist the iBorderCtrl system and to describe the different use cases, applications and interfaces.

Within this Deliverable two main Sections will be described. The first Section will undertake the analysis of the user requirements extracted in Deliverable D2.1 and their translation into functional and technical requirements. This part will also provide a functional description of each one of the modules in iBorderCtrl together with specific technical requirements related to the State of the Art (SOTA) analysis performed in Deliverable D2.1 and some additional technical requirements derived from the architecture of each module. Finally this analysis will be completed with a description of the general constraints related to the security and privacy of the data that will be stored in the system and the system itself, together with a summary of the legal issues and constraints that are thoroughly analysed in deliverable D2.3.

The second Section will contain the analysis of the different use cases for the system, both in the preregistration phase and during the actual crossing of the border and the definition of the functional architecture of iBorderCtrl. It will also provide the description of the different user interfaces of the system (for travellers, Border Guards and Border Guard Managers). This section will conclude with a traceability matrix between the technical requirements and each respective iBorderCtrl module responsible to realise each requirement in order to ensure that every requirement is covered and that the final functionality of the iBorderCtrl system meets the needs described by the end-users in Deliverable D2.1.

# 1 Introduction

## 1.1 Purpose of this Document

This report corresponds to the Task 2.2, the development of a reference architecture together with the technical and functional specifications for all the modules that are included within the iBorderCtrl system. Besides the Reference Architecture, this task will describe and specify the high-level design, including dependencies, interactions and applications as well as early interfaces between the iBorderCtrl various components.

The overall objectives of WP2 are to:

- Analyse the end-user requirements and to assess user functional and technical needs.
- Identify the processes, technologies, challenges and their shortcomings through participatory research.
- Develop the iBorderCtrl reference architecture and component / module specifications.
- Conduct a thorough legislation review, both in EU and national level, to ensure iBorderCtrl's legal compliance and to address privacy issues related to border control pilot scenarios i.e. agreements and informed consent.

The main goal of Task 2.2 is to fulfil the third objective of WP2. The Reference Architecture encompasses the determination of the iBorderCtrl software platform specification requirements covering four application areas: scenarios, use cases, end-user functionalities and technical requirements.

Furthermore, the iBorderCtrl legal framework of Task 2.3 provides a valuable guidance in this effort since both the reference Architecture and the system's requirements depend greatly on the relevant legal, ethical and security aspects. At this point it should be mentioned that both Deliverables D2.2 and D2.3 were obliged to adapt themselves to the latest regulation changes; it should be highlighted herein that according to the newly inserted Regulation (EU) 2017/458 imposed by 7th of April 2017, the procedure of travel documents' authenticity check became mandatory for the EU citizens as well, apart from the Third Country Nationals (TCNs). As a result, the role and importance of certain modules within iBorderCtrl is further enhanced or altered.

To this respect and based on the analysis and outcomes of Task 2.1 and in direct interaction with Task 2.3 that evolves in parallel, the user requirements are translated in the following into technical requirements for the overall system, the platform and its modules. Furthermore, Task 2.2 provides specifications on the components' implementation while focusing on the technical specifications of each specific module and its interfaces that adhere to the requirements.

## 1.2 Structure of the Document

The structure of this document is as follows:

- Chapter 2 comprises a description and analysis of the functional (user) requirements extracted in the framework of the previous Deliverable D2.1. These requirements are divided in pre-arrival phase requirements (pre-registration), back-end requirements, border crossing requirements and general requirements described in the DoW. For each one of them, several respective technical requirements are derived from the functional requirements and are described within Chapter 2 along with the involved systems and implementation priority.

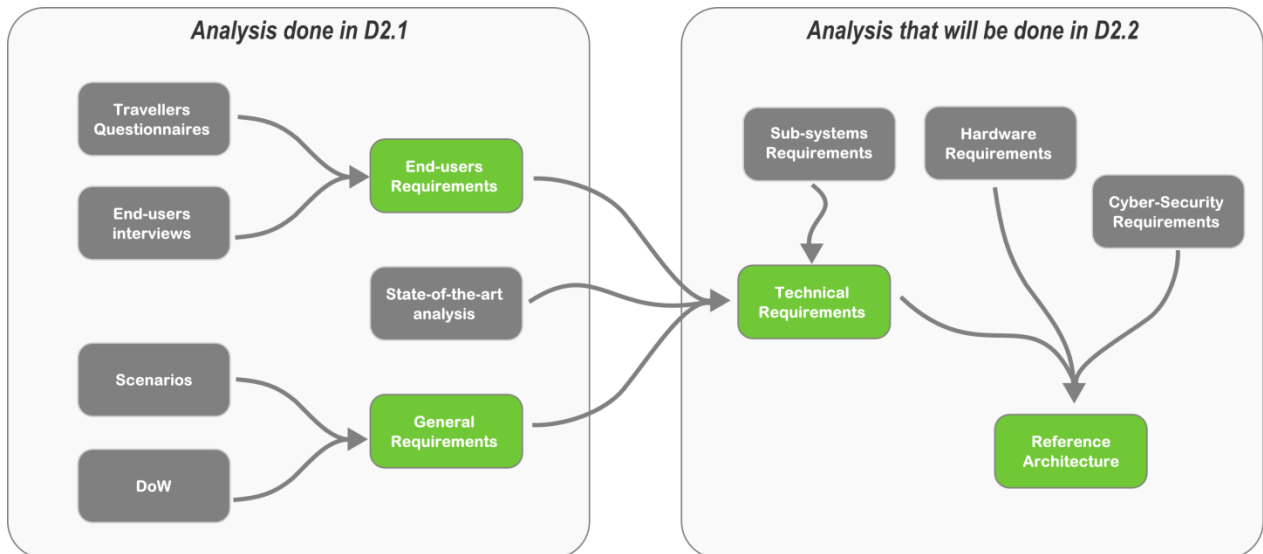
- Chapter 3 provides the functional description of all the basic interdisciplinary modules and tools of the iBorderCtrl system. Together with this functional description, for each of these sub-systems a set of technical requirements originated from the SOTA analysis, performed in D2.1, is described. Also additional technical requirements associated to each of the systems is added to complete the technical functionalities and requirements.
- Chapter 4 describes the general constraints that iBorderCtrl must take into account with regards to Privacy and Security by Design, data protection and general security measures, other general (hardware and software) constraints and requirements along with the relevant legal issues guiding this effort.
- Chapter 5 illustrates the different use cases for the iBorderCtrl system and describes how the different systems interact in the various scenarios especially for border control checks.
- Chapter 6 delineates the overall iBorderCtrl functional architecture together with the software stack needed for the iBorderCtrl solution deployment and the description of the iBorderCtrl Portable Unit. This section also describes the first approach to the database schema definition and architecture.
- Chapter 7 describes the three different user interfaces that the iBorderCtrl project will implement for each type of user. The first interface is the one that will be available for the travellers that want to preregister in the system. The second interface is the one that the Border Guards will use in the Portable Unit in order to guide them during the check procedure and the use of the different readers, scanners and sensors. Finally, a third interface will be available for the Border Managers that will provide further analysis of the system performance facilitating their administrative role and resources allocation.
- Chapter 8 provides the overall Conclusions along with a traceability matrix linking the technical requirements with the iBorderCtrl modules. This section is a summary of all the information gathered in this Deliverable and intends to be a reference for all the partners during the iBorderCtrl project's development phase.

**Important Note:** It should be noted herein that according to the iBorderCtrl legal and ethical advisors, children under 18, minors with or not guardian's supervision, and disabled people travelling should not be under the scope of the iBorderCtrl system especially during the research, development and piloting phases. These issues are very important and in certain cases (i.e. guardian status including the right to travel abroad with a given minor) are crucial i.e. in fighting back cross-border trafficking of minors.

However, this would imply certain special conditions in respect to the legal framework and ethical basis, which could not be dealt within the iBorderCtrl project but lie more within the potential future exploitation of the iBorderCtrl system after the successful end of the project. Thus, these issues will be subject of the WP7 and will be addressed within the project's Exploitation Plan relevant Deliverables to provide the roadmap for the successful inclusions of these issues in the future exploitation of the iBorderCtrl system.

## 2 Requirements

The general user requirements for the iBorderCtrl system, as these were one of the main outputs of Deliverable D2.1, act as the input for the present Deliverable D2.2 – “*Reference Architecture and Components specifications*” as depicted in Figure 1 below. In this section, the technical needs and requirements of each subsystem together with the hardware and cyber-security requirements will be analysed and linked to each of the user functional requirements.



**Figure 1 Relationship between D2.1 and D2.2**

### 2.1 Technical Requirements derived from the Analysis of Functional (End Users) and General Requirements from D2.1

The functional and general user requirements which were based on:

- Traveller’s survey results,
- Border Guard’s survey results,
- Border Guard Officers and Managers interview results,
- Experience of experts of the participating end-users and
- The Description of Work,

were described in D2.1 and grouped per stages.

This chapter aims at describing the technical requirements derived from these functional requirements described in the previous deliverable D2.1. The description will follow the grouping per stage used in D2.1 incorporating four sections: pre-arrival phase, background check phase, border crossing phase and general requirements described in the DoW.

*Table 1 List of iBorderCtrl technical requirements from functional requirements for the pre-arrival phase*

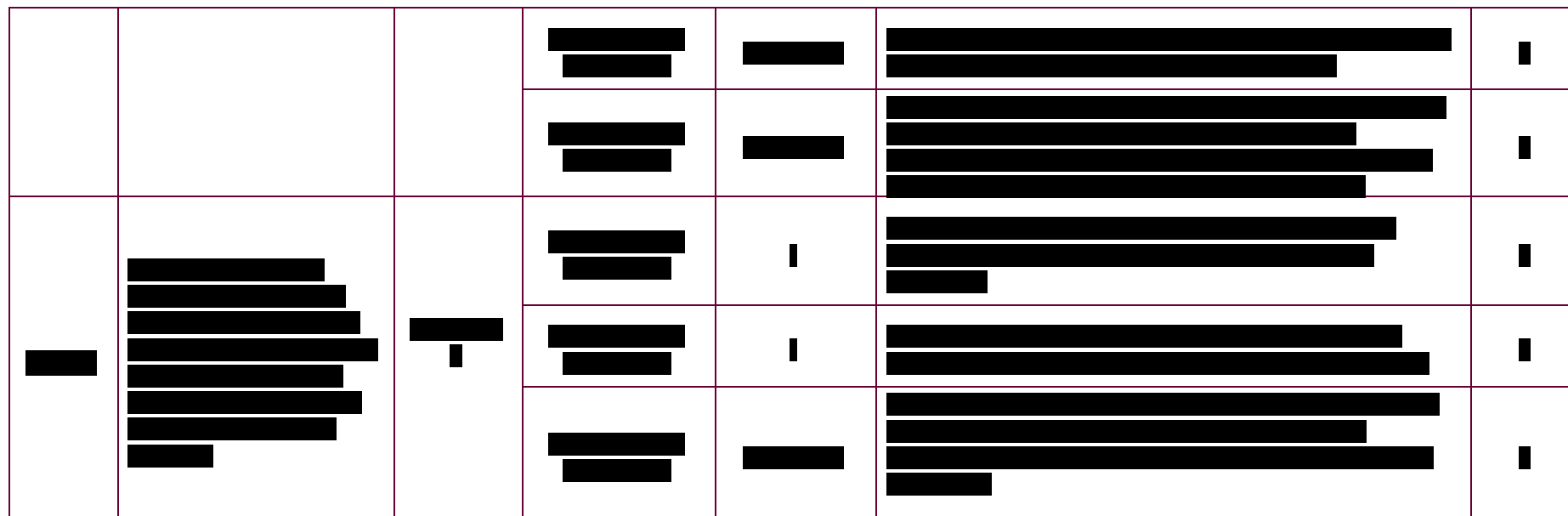
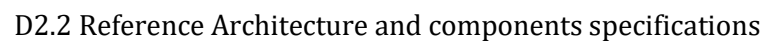
■	■	■	■	■	■	■
■	■ ■ ■ ■ ■ ■ ■	■ ■	■ ■	■	■ ■ ■ ■ ■	■
			■ ■ ■	■	■ ■ ■ ■	■
			■ ■	■	■ ■ ■ ■ ■ ■	■
■	■ ■ ■ ■ ■ ■	■ ■	■ ■ ■ ■	■	■ ■ ■ ■ ■	■
			■ ■ ■	■	■ ■ ■ ■	■

■  
■  
■  
■  
■






■	■ ■ ■ ■ ■ ■	■ ■ ■	■ ■	■	■ ■ ■ ■ ■ ■ ■	■
			■	■	■ ■	■
■	■ ■ ■ ■ ■ ■	■ ■ ■	■ ■	■	■	■
			■	■	■ ■	■
■	■ ■ ■ ■ ■	■ ■ ■	■ ■ ■	■	■ ■ ■ ■	■
			■	■		
■	■ ■ ■ ■ ■	■ ■ ■	■ ■	■	■ ■ ■ ■	■
			■ ■	■	■ ■ ■	■
			■ ■	■	■ ■ ■ ■	■

[illegible]

№	Наименование	Содержание	Ссылка	Статус	Комментарий	Действие
1	1.1	1.1.1	1.1.1.1	1.1.1.1	1.1.1.1	1.1.1.1
	1.2	1.2.1	1.2.1.1	1.2.1.1	1.2.1.1	1.2.1.1
	1.3	1.3.1	1.3.1.1	1.3.1.1	1.3.1.1	1.3.1.1
	1.4	1.4.1	1.4.1.1	1.4.1.1	1.4.1.1	1.4.1.1
	1.5	1.5.1	1.5.1.1	1.5.1.1	1.5.1.1	1.5.1.1
	1.6	1.6.1	1.6.1.1	1.6.1.1	1.6.1.1	1.6.1.1
	1.7	1.7.1	1.7.1.1	1.7.1.1	1.7.1.1	1.7.1.1
	1.8	1.8.1	1.8.1.1	1.8.1.1	1.8.1.1	1.8.1.1
	1.9	1.9.1	1.9.1.1	1.9.1.1	1.9.1.1	1.9.1.1
2	2.1	2.1.1	2.1.1.1	2.1.1.1	2.1.1.1	2.1.1.1
	2.2	2.2.1	2.2.1.1	2.2.1.1	2.2.1.1	2.2.1.1
	2.3	2.3.1	2.3.1.1	2.3.1.1	2.3.1.1	2.3.1.1
	2.4	2.4.1	2.4.1.1	2.4.1.1	2.4.1.1	2.4.1.1
	2.5	2.5.1	2.5.1.1	2.5.1.1	2.5.1.1	2.5.1.1
	2.6	2.6.1	2.6.1.1	2.6.1.1	2.6.1.1	2.6.1.1
	2.7	2.7.1	2.7.1.1	2.7.1.1	2.7.1.1	2.7.1.1
	2.8	2.8.1	2.8.1.1	2.8.1.1	2.8.1.1	2.8.1.1
	2.9	2.9.1	2.9.1.1	2.9.1.1	2.9.1.1	2.9.1.1

*Table 3 List of iBorderCtrl technical requirements from functional requirements for the border check phase*

	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	.
			[REDACTED]	[REDACTED]	[REDACTED]	.
			[REDACTED]	[REDACTED]	[REDACTED]	.
			[REDACTED]	[REDACTED]	[REDACTED]	.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	.
			[REDACTED]	[REDACTED]	[REDACTED]	.
			[REDACTED]	[REDACTED]	[REDACTED]	.



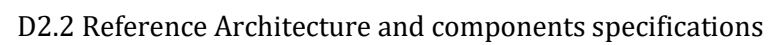
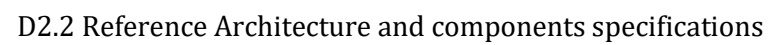
			<div></div> <div></div> <div></div>	<div></div>	<div></div> <div></div> <div></div> <div></div> <div></div>	<div></div>
<div></div>	<div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div>	<div></div>	<div></div>	<div></div> <div></div> <div></div>	<div></div>
			<div></div>	<div></div>	<div></div> <div></div> <div></div> <div></div>	<div></div>
			<div></div>	<div></div>	<div></div> <div></div> <div></div> <div></div>	<div></div>
			<div></div>	<div></div>	<div></div> <div></div> <div></div>	<div></div>
			<div></div>	<div></div>	<div></div> <div></div> <div></div> <div></div>	<div></div>
			<div></div>	<div></div>	<div></div> <div></div> <div></div> <div></div>	<div></div>
			<div></div>	<div></div>	<div></div> <div></div> <div></div> <div></div>	<div></div>
			<div></div>	<div></div>	<div></div> <div></div> <div></div> <div></div>	<div></div>

Page 26 of 165

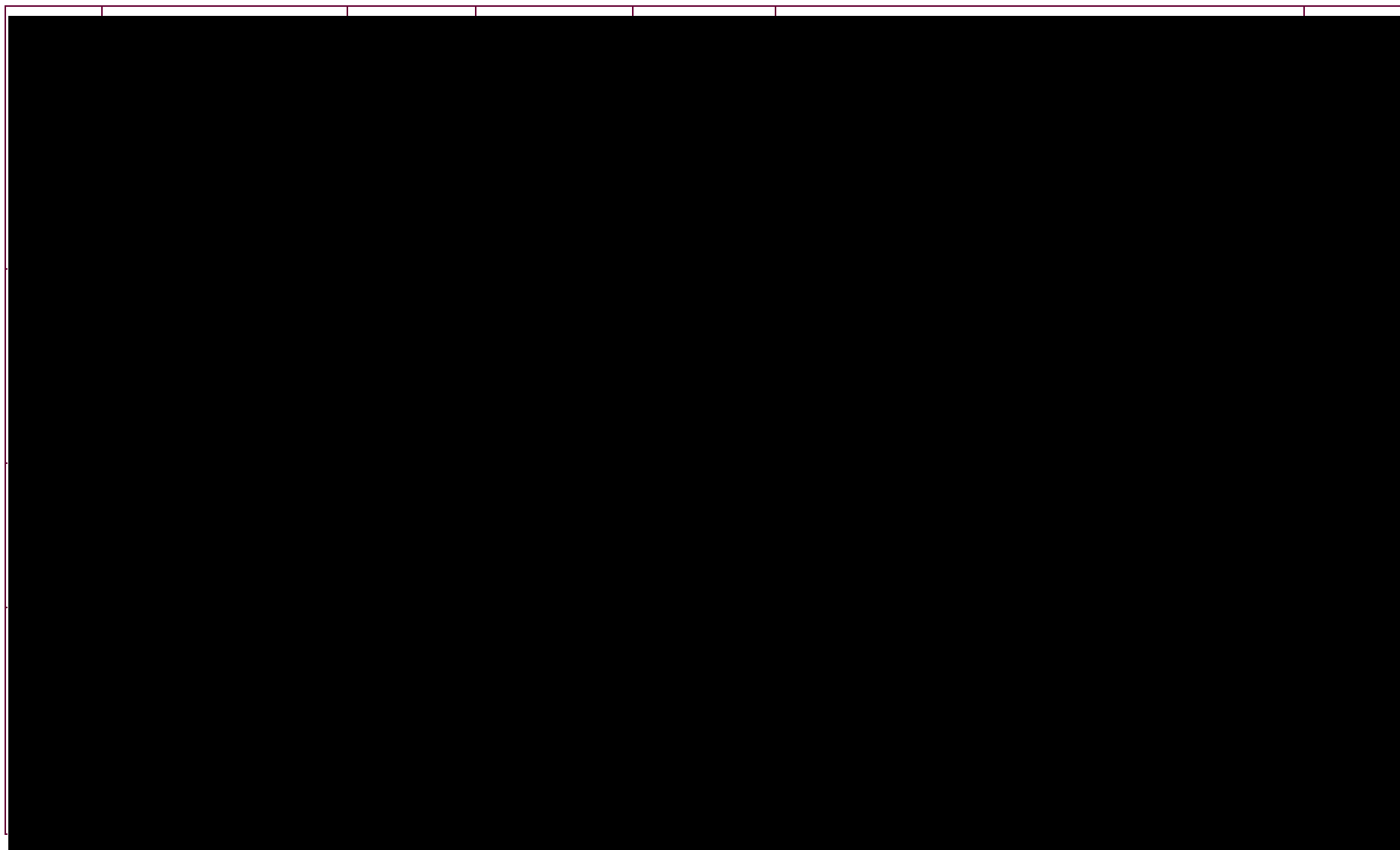

[illegible]

№	Наименование	Единица измерения	Количество	Единица измерения	Стоимость	Единица измерения
1	Автомобиль	шт.	1	шт.	1000000	шт.
			1	шт.	1000000	шт.
2	Автомобиль	шт.	1	шт.	1000000	шт.
			1	шт.	1000000	шт.
3	Автомобиль	шт.	1	шт.	1000000	шт.
			1	шт.	1000000	шт.
4	Автомобиль	шт.	1	шт.	1000000	шт.
			1	шт.	1000000	шт.
5	Автомобиль	шт.	1	шт.	1000000	шт.
			1	шт.	1000000	шт.
6	Автомобиль	шт.	1	шт.	1000000	шт.
			1	шт.	1000000	шт.
7	Автомобиль	шт.	1	шт.	1000000	шт.
			1	шт.	1000000	шт.
8	Автомобиль	шт.	1	шт.	1000000	шт.
			1	шт.	1000000	шт.
9	Автомобиль	шт.	1	шт.	1000000	шт.
			1	шт.	1000000	шт.
10	Автомобиль	шт.	1	шт.	1000000	шт.
			1	шт.	1000000	шт.

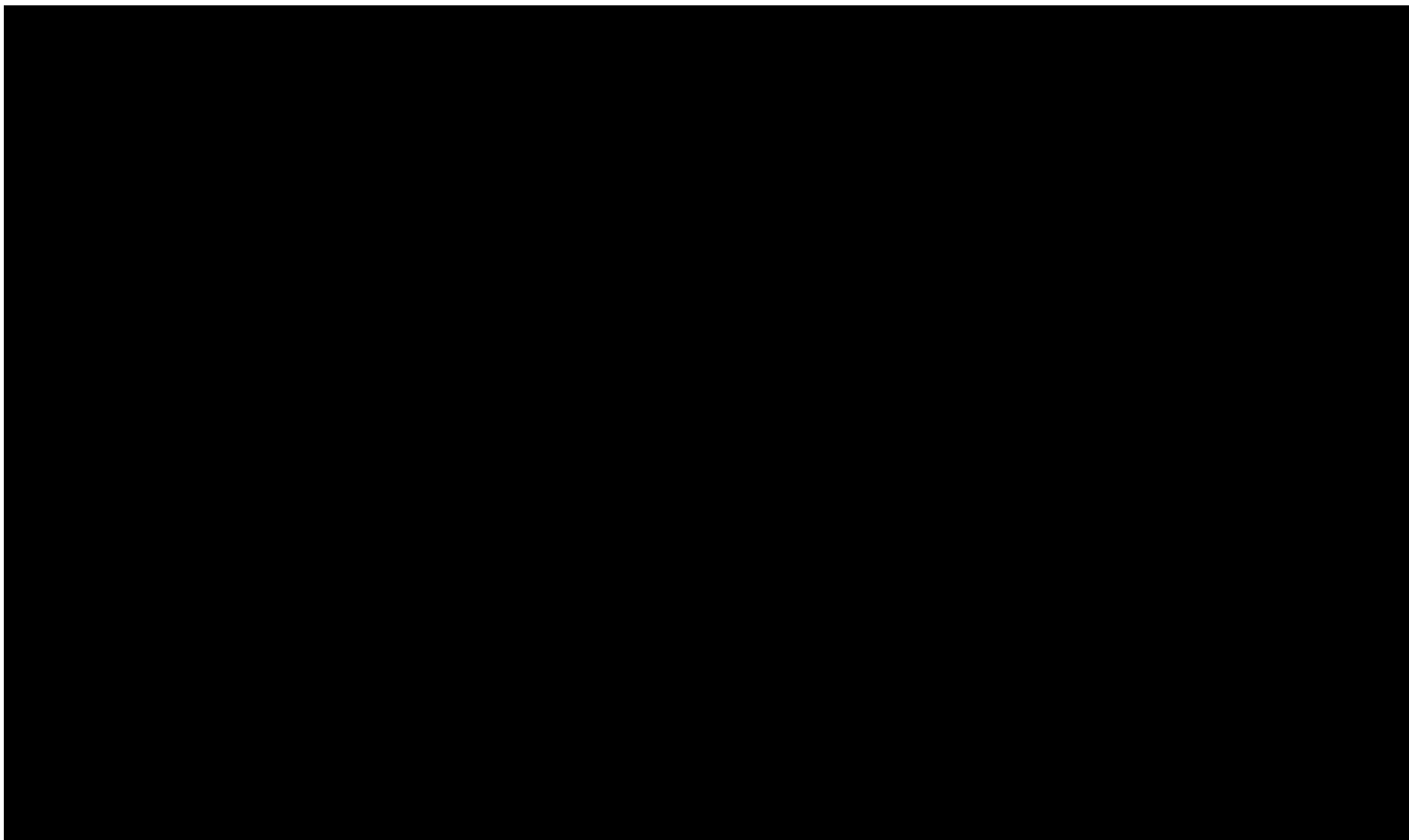
[illegible]

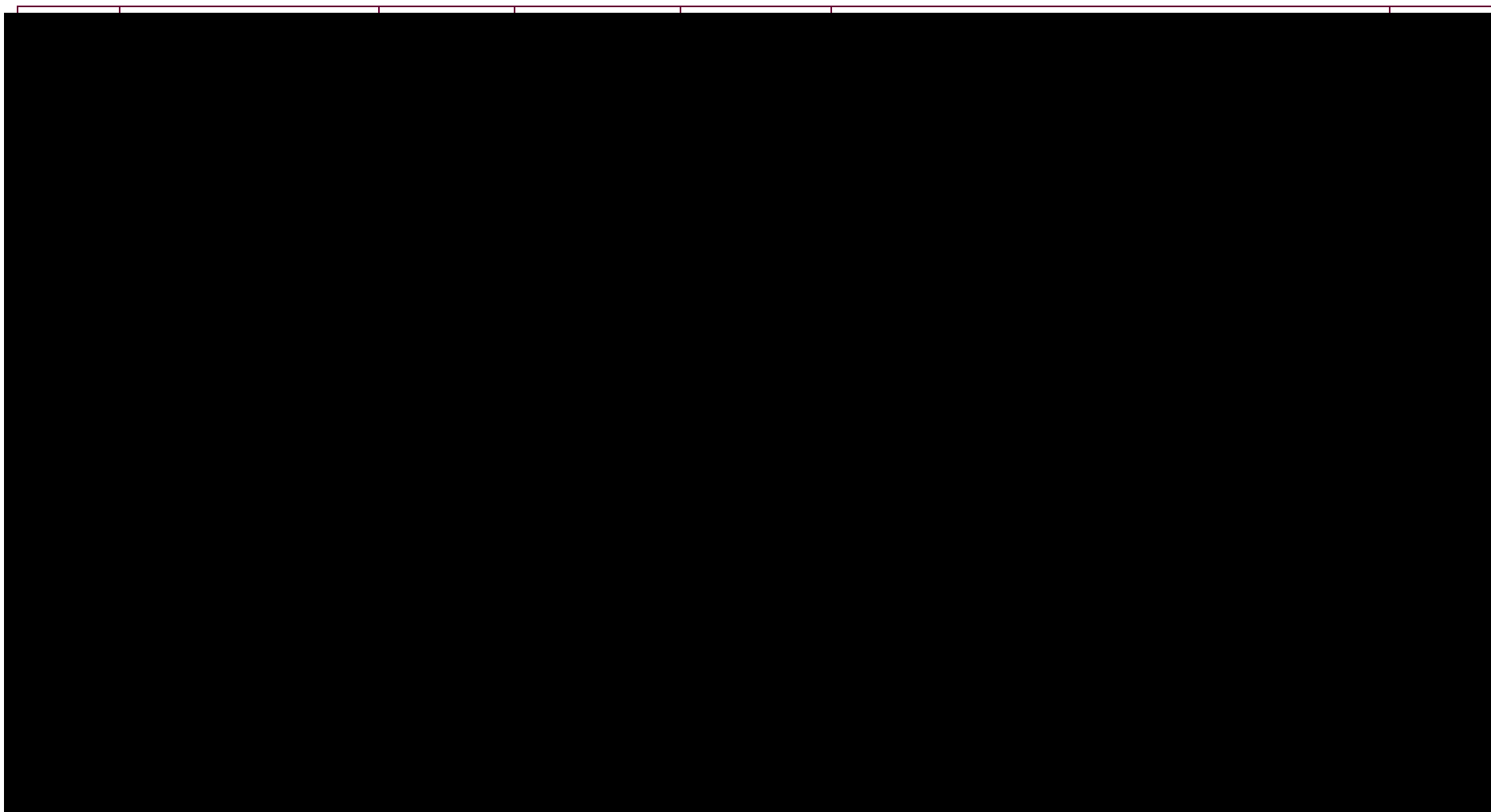


Year	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Population (millions)	7.5	7.6	7.7	7.8	7.9	8.0	8.1	8.2	8.3	8.4	8.5	8.6	8.7	8.8	8.9	9.0	9.1	9.2	9.3	9.4	9.5
GDP (trillion USD)	45.0	48.0	51.0	54.0	57.0	60.0	63.0	66.0	69.0	72.0	75.0	78.0	81.0	84.0	87.0	90.0	93.0	96.0	99.0	102.0	105.0
Urban population (millions)	4.5	4.6	4.7	4.8	4.9	5.0	5.1	5.2	5.3	5.4	5.5	5.6	5.7	5.8	5.9	6.0	6.1	6.2	6.3	6.4	6.5
Life expectancy (years)	72.5	73.5	74.5	75.5	76.5	77.5	78.5	79.5	80.5	81.5	82.5	83.5	84.5	85.5	86.5	87.5	88.5	89.5	90.5	91.5	92.5
Renewable energy share (%)	15.0	16.0	17.0	18.0	19.0	20.0	21.0	22.0	23.0	24.0	25.0	26.0	27.0	28.0	29.0	30.0	31.0	32.0	33.0	34.0	35.0
CO2 emissions (Gt)	15.0	15.5	16.0	16.5	17.0	17.5	18.0	18.5	19.0	19.5	20.0	20.5	21.0	21.5	22.0	22.5	23.0	23.5	24.0	24.5	25.0
Forest cover (%)	22.0	22.5	23.0	23.5	24.0	24.5	25.0	25.5	26.0	26.5	27.0	27.5	28.0	28.5	29.0	29.5	30.0	30.5	31.0	31.5	32.0
Healthcare expenditure (GDP %)	5.0	5.2	5.4	5.6	5.8	6.0	6.2	6.4	6.6	6.8	7.0	7.2	7.4	7.6	7.8	8.0	8.2	8.4	8.6	8.8	9.0
Internet usage (%)	40.0	45.0	50.0	55.0	60.0	65.0	70.0	75.0	80.0	85.0	90.0	95.0	98.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
Gender inequality index	0.65	0.64	0.63	0.62	0.61	0.60	0.59	0.58	0.57	0.56	0.55	0.54	0.53	0.52	0.51	0.50	0.49	0.48	0.47	0.46	0.45
Urbanization rate (%)	60.0	60.5	61.0	61.5	62.0	62.5	63.0	63.5	64.0	64.5	65.0	65.5	66.0	66.5	67.0	67.5	68.0	68.5	69.0	69.5	70.0
Renewable energy investment (Bn USD)	10.0	11.0	12.0	13.0	14.0	15.0	16.0	17.0	18.0	19.0	20.0	21.0	22.0	23.0	24.0	25.0	26.0	27.0	28.0	29.0	30.0
CO2 emissions per capita (t)	2.0	2.05	2.1	2.15	2.2	2.25	2.3	2.35	2.4	2.45	2.5	2.55	2.6	2.65	2.7	2.75	2.8	2.85	2.9	2.95	3.0
Forest cover loss (ha)	1000000	1050000	1100000	1150000	1200000	1250000	1300000	1350000	1400000	1450000	1500000	1550000	1600000	1650000	1700000	1750000	1800000	1850000	1900000	1950000	2000000
Healthcare expenditure (Bn USD)	225.0	252.0	275.5	297.0	316.5	334.5	351.0	366.0	380.5	394.5	408.0	421.0	433.5	445.5	457.0	468.0	478.5	488.5	498.0	507.0	515.5
Internet usage (millions)	30.0	36.0	42.0	48.0	54.0	60.0	66.0	72.0	78.0	84.0	90.0	96.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
Gender inequality index	0.65	0.64	0.63	0.62	0.61	0.60	0.59	0.58	0.57	0.56	0.55	0.54	0.53	0.52	0.51	0.50	0.49	0.48	0.47	0.46	0.45
Urbanization rate (%)	60.0	60.5	61.0	61.5	62.0	62.5	63.0	63.5	64.0	64.5	65.0	65.5	66.0	66.5	67.0	67.5	68.0	68.5	69.0	69.5	70.0
Renewable energy investment (Bn USD)	10.0	11.0	12.0	13.0	14.0	15.0	16.0	17.0	18.0	19.0	20.0	21.0	22.0	23.0	24.0	25.0	26.0	27.0	28.0	29.0	30.0</



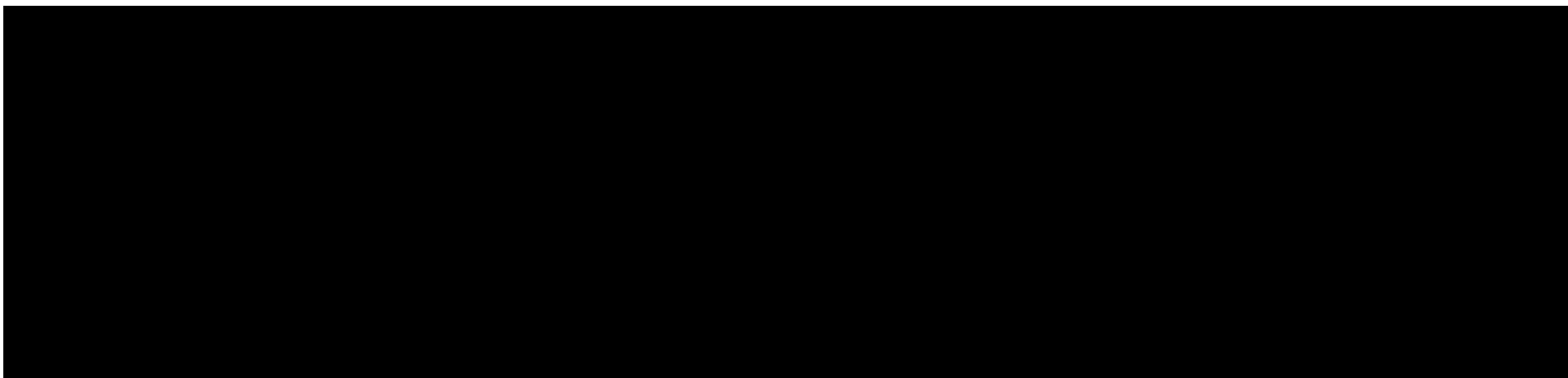










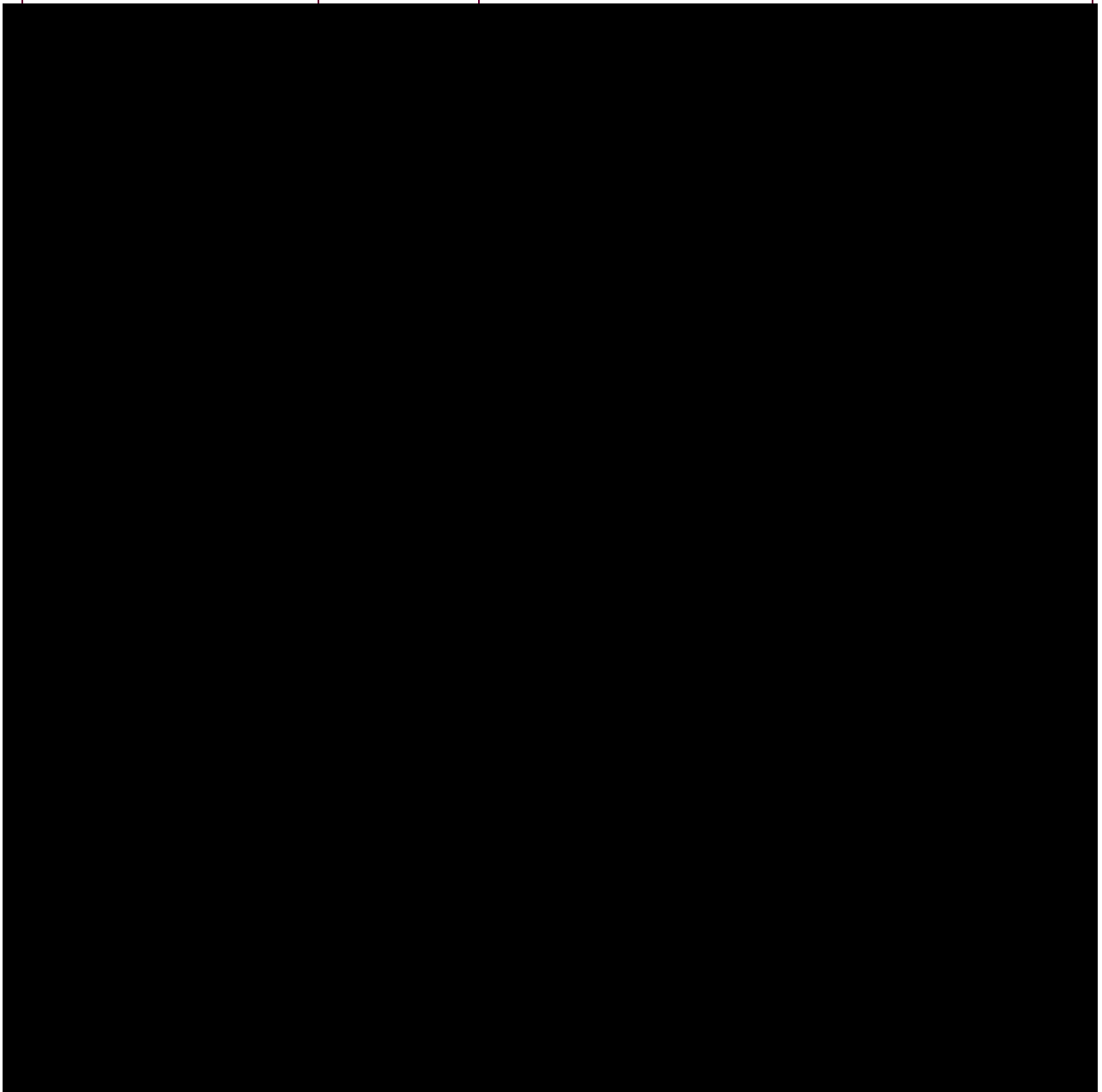


### 3 Description of the iBorderCtrl interdisciplinary Technologies

Following the interpretation of the general User requirements to Functional and Technical ones presented in the previous Chapter, the description of all iBorderCtrl involved technologies will take place herein. The iBorderCtrl project brings together various interdisciplinary technology sectors in order to result in an innovative overall platform to enable a more effective and reliable border crossing. The overall iBorderCtrl platform is formulated by various modules, each one representing the above mentioned interdisciplinary components which will be detailed in the following paragraphs. The following table provides a functionality overview of these separate technology modules of the iBorderCtrl system along with the respective partner in charge of each component.

### Table 5 List of iBorderCtrl components

[illegible]



Within the following sections each one of the modules and subsystems that encompass the iBorderCtrl system will be described in detail.

### 3.1 Automatic Deception Detection System (ADDS) description

The Automatic Deception Detection System (ADDS) consists of three main components:

- The Avatar which conducts the interview with the traveller and poses the questions,
- Silent Talker (ST) which processes the Image Feature Vectors and classifies the deception level
- The main ADDS application unit which performs the overall analysis and assessment.

In this section, the term “traveller’s device” refers to a piece of hardware used by the traveller to complete a pre-travel interview. Therefore it could refer to (but not limited to): a smartphone, a tablet computer, a laptop computer or even a desktop computer. The prototype system will use Windows based devices (laptop or PC) and be extended later.

[illegible]



\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**Table 6 List of ADDS technical requirements based on SOTA analysis**

Country	Country	Country	Country
Country	Country	Country	Country
Country	Country	Country	Country
Country	Country	Country	Country

### 3.1.2 Functional description

\_\_\_\_\_

- [REDACTED]
- [REDACTED]
- [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [illegible]

\_\_\_\_\_

\_\_\_\_\_

- 
- | Row | Bar Length (approx. % of total width) |
|-----|---------------------------------------|
| 1   | 95                                    |
| 2   | 95                                    |
| 3   | 95                                    |
| 4   | 65                                    |
| 5   | 95                                    |
| 6   | 10                                    |
| 7   | 95                                    |
| 8   | 95                                    |
| 9   | 85                                    |
| 10  | 95                                    |
| 11  | 65                                    |
| 12  | 95                                    |
| 13  | 95                                    |
| 14  | 95                                    |
| 15  | 95                                    |
| 16  | 95                                    |
| 17  | 95                                    |
| 18  | 95                                    |
| 19  | 95                                    |
| 20  | 95                                    |
| 21  | 95                                    |
| 22  | 95                                    |
| 23  | 95                                    |
| 24  | 95                                    |
| 25  | 95                                    |
| 26  | 95                                    |
| 27  | 95                                    |
| 28  | 95                                    |
| 29  | 95                                    |
| 30  | 95                                    |
| 31  | 95                                    |
| 32  | 95                                    |
| 33  | 95                                    |
| 34  | 95                                    |
| 35  | 95                                    |
| 36  | 95                                    |
| 37  | 95                                    |
| 38  | 95                                    |
| 39  | 95                                    |
| 40  | 95                                    |
| 41  | 95                                    |
| 42  | 95                                    |
| 43  | 95                                    |
| 44  | 95                                    |
| 45  | 95                                    |
| 46  | 95                                    |
| 47  | 95                                    |
| 48  | 95                                    |
| 49  | 95                                    |
| 50  | 95                                    |

[REDACTED]

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[illegible]

### 3.1.3 Additional Technical Requirements derived from Architecture Components

\_\_\_\_\_

**Table 7 List of ADDS additional technical requirements**



### 3.2 Document Authenticity Analysis Tool (DAAT) description

The main functional and technical features of the DAAT module are given in the following Table:

<i>Name:</i>	<i>Document Authenticity Analytics Tool (DAAT)</i>
<i>Technologies:</i>	<i>Java, JavaScript, HTML, CSS, REST, SSO, HTTPS, Optical Character Recognition, Image Pattern Recognition, Cross-Device User Interface.</i>
<i>Installation:</i>	<i>Linux server, Tomcat, MySQL, and Scanner.</i>
<i>Conditions:</i>	<i>The scanner will be compliant with the portable unit equipment requirements.</i>
<i>Power:</i>	<i>N/A</i>
<i>Connectivity:</i>	<i>Internet/Intranet.</i>
<i>Internal Information:</i>	<i>Information retrieved from iFADO.</i>
<i>Data at Rest:</i>	<i>MySQL iBorderCtrl Database.</i>
<i>User Management:</i>	<i>Traveller, Border Guard, Administrator.</i>
<i>System States:</i>	<i>Waiting, Processed.</i>
<i>Security Needs:</i>	<i>End-To-End HTTPS, Firewall.</i>

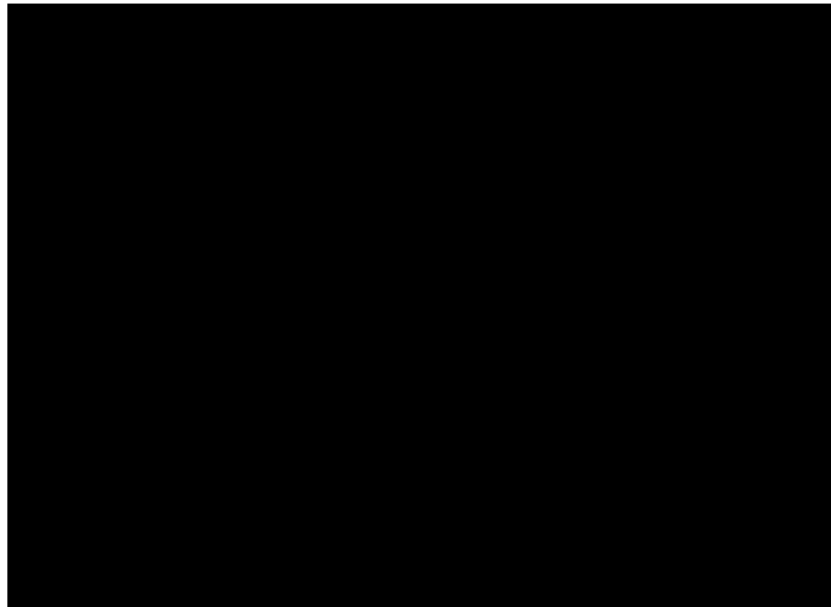
#### 3.2.1 Technical Requirements derived from the SOTA analysis from D2.1



*Table 8 List of DAAT technical requirements based on SOTA analysis*

<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>

### 3.2.2 Functional description



[REDACTED]

[REDACTED]

### 3.2.3 Additional Technical Requirements derived from Architecture Components

[REDACTED]

*Table 9 List of DAAT additional technical requirements*

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

### 3.3 Biometric Module (BIO) description

The BIO module is composed by two different biometric modules: fingerprints and palm vein.

<b>Name:</b>	<b>BIO: BioSec LifePass</b>
<b>Technologies:</b>	<b>Palm vein based biometric personal authentication</b>
<b>Installation:</b>	<b>The system consists of biometric sensor via USB and connected software</b>
<b>Conditions:</b>	<b>0 to +60 degrees Celsius, -20 to +60 with special enclosure, Microsoft based operation system</b>
<b>Power:</b>	<b>Via USB no additional power required, only for the connected computing device (micro PC, laptop, PC)</b>
<b>Connectivity:</b>	<b>USB, communication from client to server via LAN</b>
<b>Internal Information:</b>	<b>Palm vein system will store basic information from the traveller (such as iBorderCtrl ID and name) together with the biometric hash code generated during biometric enrolment from left and right hand (if both are available). The system will check, if during enrolment, the biometric templates have the highest possible security rating, if not, the procedure has to be repeated. During authentication, the BRT (biometric registration template) will be compared with the BCT (biometric capture template) and the result will be signalled to the officer.</b>
<b>Data at Rest:</b>	<b>User ID and biometric hash code will be stored in BioSec database, depending on end user in MySQL, MsSQL, Oracle, PostgreSQL</b>
<b>User Management:</b>	<b>The system will have two different type of users: the administrative one (only used for the developers of the system for maintenance) and the iBorderCtrl user (Border Guard). The iBorderCtrl system user will have a limited access to the system only for those functionalities allowed.</b>
<b>System States:</b>	<b>Waiting, Processing, Processed.</b>
<b>Security Needs:</b>	<b>Firewall, Secure access and storage</b>

<b>Name:</b>	<b>BIO: Fingerprint</b>
<b>Technologies:</b>	<b>Fingerprint based biometric identity validation</b>
<b>Installation:</b>	<b>The system consists of biometric sensor via serial or TCP/IP and connected software</b>
<b>Conditions:</b>	<b>0 to +60 degrees Celsius, Microsoft based operation system</b>
<b>Power:</b>	<b>Via USB no additional power required, only for the connected computing device (micro PC, laptop, PC)</b>

Connectivity:	<i>serial or LAN communication from client to server via LAN</i>
Internal Information:	<i>Fingerprint system will store basic information from the traveller (such as iBorderCtrl ID and name) together with the biometric hash code/image generated during biometric enrolment. The system will check, if during enrolment the biometric templates have the highest possible security rating, if not, the procedure has to be repeated. During authentication, the BRT (biometric registration template) will be compared with the BCT (biometric capture template) and the result will be signalled to the officer.</i>
Data at Rest:	<i>User ID and biometric hash code will be stored in database, depending on end user in MySQL, MsSQL, Oracle, PostgreSQL</i>
User Management:	<i>The system will have two different type of users: the administrative one (only used for the developers of the system for maintenance) and the iBorderCtrl user (Border Guard). The iBorderCtrl system user will have a limited access to the system only for those functionalities allowed.</i>
System States:	<i>Waiting, Processing, Processed.</i>
Security Needs:	<i>Firewall, Secure access and storage</i>

### 3.3.1 Technical Requirements derived from the SOTA analysis from D2.1

[REDACTED]

**Table 10 List of BIO technical requirements based on SOTA analysis**

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

### 3.3.2 Functional description

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

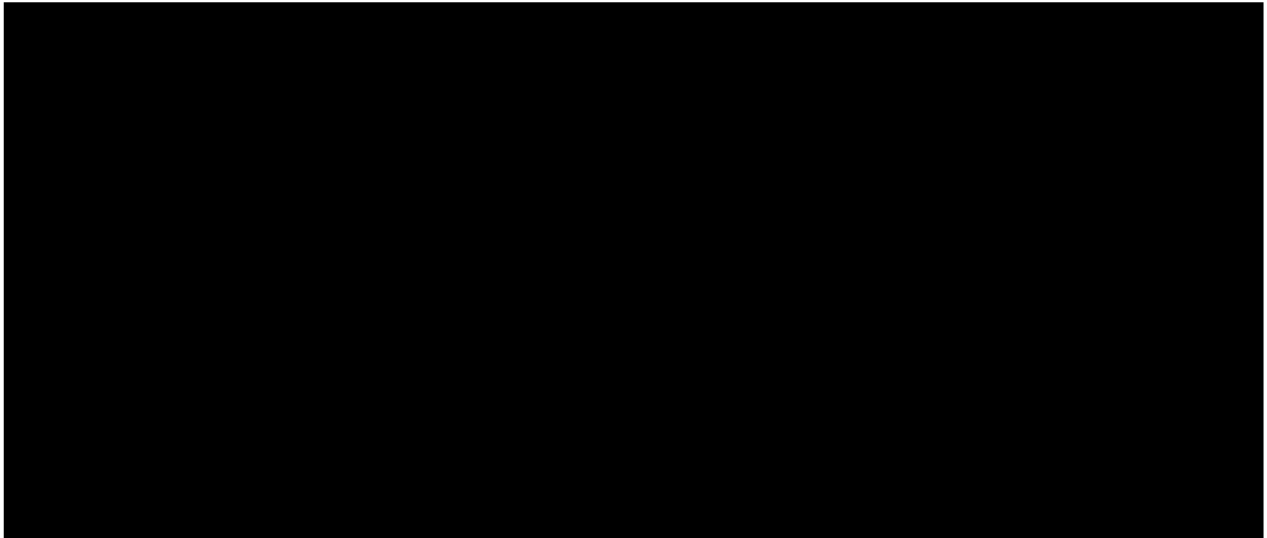
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

### 3.3.3 Additional Technical Requirements derived from Architecture Components

[REDACTED]

*Table 11 List of BIO additional technical requirements*

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]

### 3.4 Face Matching Tool (FMT) description

The main function of the Face Matching Tool (FMT) module will be to provide a scoring in matching a reference image (normally the HD photo stored in the passport, VISA or ID card) with the subject appearing in the video (taken during the pre-registration phase or in the border crossing point). The FMT provides also a second and optional functionality that will allow to the BCP officers (Border Guards) to have a “black list” of known suspects and receive an alert whenever a possible match is detected.

The main functional and technical features of the FMT module are given in the following Table:

<b>Name:</b>	<b>Face Matching Tool (FMT)</b>
<b>Technologies:</b>	<b>Facial biometrics algorithms; Postgres database; C#; Java Spring</b>
<b>Installation:</b>	<b>Application and database installed in the cloud server</b>
<b>Conditions:</b>	<b><i>In order to provide an accurate result is important that the image used to create the biometric signature of the traveller is a High Quality image acquired by a respective camera. The same is true with the videos (i.e. 720p video). However as part of this project the algorithm is going to be adjusted in order to work with less quality videos and images.</i></b>
<b>Power:</b>	<b>N/A</b>
<b>Connectivity:</b>	<b><i>The FMT module will connect with the rest of the iBorderCtrl system through Web services.</i></b>
<b>Internal Information:</b>	<b><i>FMT will store basic information from the traveller (such as iBorderCtrl ID and name) together with the biometric model generated using the traveller's HD photo stored within his/her passport RFID chip or by capturing the passport's photo from the scanned document sent to the DAAT module. This biometric model can be updated with new images or videos both during the pre-registration phase (using the images provided by the ADDS module) and during the border crossing with the video provided by the mounted camera in the portable unit. It will provide to the rest of the systems a score when comparing the biometric models with other images.</i></b>
<b>Data at Rest:</b>	<b><i>The system will store basic information of the traveller (iBorderCtrl ID and full name) together with internal information generated by the FMT system.</i></b>
<b>User Management:</b>	<b><i>The system will have two different type of users:  The administrative one (only used for the developers of the system for maintenance) and the iBorderCtrl system internal user. The iBorderCtrl system internal user will have a limited access to the system only for those functionalities allowed.</i></b>
<b>System States:</b>	<b><i>Waiting, processing, Processed</i></b>
<b>Security Needs:</b>	<b><i>Secure access and storage</i></b>



### 3.4.1 Technical Requirements derived from the SOTA analysis from D2.1

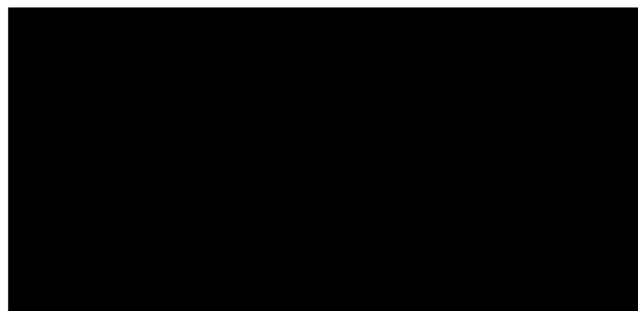
[REDACTED]

*Table 12 List of FMT technical requirements based on SOTA analysis*

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

### 3.4.2 Functional description

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 3.4.3 Additional Technical Requirements derived from Architecture Components

[REDACTED]

[REDACTED]

*Table 13 List of FMT additional technical requirements*

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]

### 3.5 Hidden Human Detection Technology (HHD) description

The Hidden Human Detection (HHD) module is an additional iBorderCtrl tool to support the Border Guards in searching and detecting hidden people in various kinds of vehicles. Thus its main target will be to support the Border Guards to better confront illegal human trafficking, illegal migration or passengers trying to illegally cross the land borders. The main function of the HHD tool will be to detect the presence and thus to provide a score of whether an alive being ("subject") is detected to be hidden inside the vehicles or not. Herein, by the term "vehicles" we mean either ordinary cars or closed compartments (such as containers carried on trucks or freight train wagons).

As it was extensively analysed in the previous Deliverable D2.1 concerning the relevant State of the Art, the technologies to be used for such a purpose greatly depend on the vehicle's type and use, along with the implementation parameters each time. To this respect, this type of checking incorporates various technologies whereas not all of them are suitable for all kinds of vehicles (when considering ordinary cars, containers and also trucks or train wagons).

Furthermore, since the HHD tool is used at the BCPs, the relevant technologies should: enable connectivity to the iBorderCtrl portable unit, enable the inclusion and adaptation of those technologies already used at the Borders and of new ones or combinations, assist the existing visual or other methods improving vehicle inspection's efficiency and should be implemented through small size, harmless and easy-to-use equipment. To this respect, the HHD tool within the framework of iBorderCtrl will attempt to include already used methods and new ones, through different sensors, up to the level that this is feasible in implementation terms and depending on the Use Case scenarios under consideration each time. The main features of the HHD tool are given in the following table:

Name:	<b><i>Hidden Human Detection (HHD) Tool</i></b>
<i>Technologies to be examined:</i>	<p><b><i>The following technologies will be examined and assessed:</i></b></p> <ul style="list-style-type: none"> <li>• <b><i>For general purpose, mainly for ordinary cars:</i></b> <ul style="list-style-type: none"> <li>× <b><i>EM (electromagnetic / microwave) radiation using radar sensor</i></b></li> </ul> </li> <li>• <b><i>For close compartments (containers on trucks or on freight train wagons):</i></b> <ul style="list-style-type: none"> <li>× <b><i>Acoustic signals using (passive / active) acoustic sensors</i></b></li> <li>× <b><i>Gas sensors and / or Geophones (heartbeat) sensors</i></b></li> </ul> </li> </ul> <p><b><i>(* The Gas sensors and Geophones sensors are already in use at the BCPs so a roadmap for their inclusion will be provided.)</i></b></p> <p><b><i>Each sensor technology module will consist of 2 main units: a) the sensing and analogue processing and b) the digital signal processing.</i></b></p>
<i>Installation:</i>	<p><b><i>The HHD tool will be connected with the portable computer (laptop / tablet) of the portable unit. Operation on Microsoft Windows. Due to the sensors foreseen, the HHD tool cannot be mounted to a wearable device (the sensors cannot be mounted). As a sub-system the HHD tool could also act as an independent unit (optional, if needed).</i></b></p>
<i>Conditions:</i>	<p><b><i>The sensors to be used should be harmless for human beings.</i></b></p> <p><b><i>In certain cases close proximity or direct contact with the subject is needed (gas and geophones sensors). For the EM and acoustic sensors the range of operation is a trade-off with the emitted / required received power so, depending on the implementation and the performance required, close proximity may be needed as well. These reflect each technology's limitations and thus affect the HHD tool itself in order to ensure adequate performance. There are no specific limitations or conditions that affect the iBorderCtrl system or the interaction of the HHD tool with other modules of the iBorderCtrl system.</i></b></p> <p><b><i>Resistance against dust, water, weather and temperature / humidity conditions:</i></b></p>

	<ul style="list-style-type: none"> <li>× <i>The HHD tool equipment (apart from the sensors) will be compliant with the Portable Unit equipment requirements</i></li> <li>× <i>Concerning each sensor itself, the compliance to the above should be further examined per sensor depending on what is available commercially. However, all sensors will be operating at least to ambient environmental conditions.</i></li> </ul>
Power:	<i>Battery pack to ensure energy for devices. All electronics involved need DC power.</i>
Connectivity:	<i>The HHD tool will be connected to the portable unit via USB or Bluetooth.</i>
Internal Information:	<i>The HHD tool will provide to the Border Guard User Application, an Event including a score on the detected presence (or not) of a hidden alive being inside the vehicle. The score is ideally a "go / no go" action. However, a probability index of presence detection will be included as well. The Event will be given in a suitable defined form (i.e. Json-format). An alert signal in case of presence hit could be made available directly from the HHD tool, if required (optional). This alert can either be derived from the HHD tool itself (optional) or be incorporated within the Border Guard User Application.</i>
Data at Rest:	<i>The HHD tool's Event record will be attributed to the rest of the relevant data by the Border Guard Application according to the specific defined configuration (i.e. vehicle's and driver's data obtained during the Border check, date, time stamp, GPS etc.). No specific data is stored permanently on-board the HHD tool. There is no need to send any other information concerning i.e. the signal processing, to the iBorderCtrl database.</i>
User Management:	<i>The HHD tool will be used only by the Border Guards and related Border staff (end users). It will also be handled by the tool developers for maintenance.</i>
System States:	<ul style="list-style-type: none"> <li>a) <i>Standby (waiting)</i></li> <li>b) <i>data acquisition/processing</i></li> </ul>
Security Needs:	<i>Tamper protection (hardware security; nobody is allowed to tamper the sensor).</i>

### 3.5.1 Technical Requirements derived from the SOTA analysis from D2.1



**Table 14 List of HHD technical requirements based on SOTA analysis**

### 3.5.2 Functional description

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[illegible]

### 3.5.3 Additional Technical Requirements derived from Architecture Components

[REDACTED]

**Table 15 List of HHD additional technical requirements**



### 3.6 Risk Based Assessment Tool (RBAT) description

<i>Name:</i>	<i>Risk Based Assessment Tool (RBAT)</i>
<i>Technologies:</i>	<i>N-tier Java Enterprise SOA, JPA 2.1 compliant Data Access Layer, JEE6 software infrastructure, Unified cross-platform software stack, AJAX</i>
<i>Installation:</i>	<i>N/A</i>
<i>Conditions:</i>	<i>DAAT, FMT, ADDS, BIO, HHD modules should provide feedback to RBAT. Criteria and specific rules for each subsystem's input will be defined in the framework of WP3 and WP4.</i>
<i>Power:</i>	<i>N/A</i>
<i>Connectivity:</i>	<i>Internet connection</i>
<i>Internal Information:</i>	<i>Get input data from DAAT, FMT, ADDS, BIO, HHD through exposed web services created by RBAT.</i>
<i>Data at Rest:</i>	<i>Risk scores stored in the iBorderCtrl database</i>
<i>User Management:</i>	<i>Roles: Administrator User User authentication needed</i>
<i>System States:</i>	<i>N/A</i>
<i>Security Needs:</i>	<i>Secure access and storage to the iBorderCtrl database and other databases/legacy systems, firewall, encryption etc.</i>

#### 3.6.1 RBAT Functional Description

[REDACTED]

##### 3.6.1.1 Rule Authoring

[REDACTED]

[REDACTED]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

### 3.6.1.2 Risk Evaluation

[Redacted text block]

[Redacted text block]

[REDACTED]

### 3.6.1.3 Risk Assessment

[REDACTED]

### 3.6.1.4 Automatic Suggestion and Optimization

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

## 3.6.2 Additional Technical Requirements derived from Architecture Components

[REDACTED]

*Table 16 List of RBAT additional technical requirements*

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

### 3.7 Integrated Border Control Analytics Tool (BCAT) description

The Border Control Analytics Tool (BCAT) will help the Border Guards to quickly identify false acceptance or false rejection of travellers. This will be initially based on the data collected in the Pilot implementation period. The specific functionality offered by BCAT will enable achieving the following goals:

- To evaluate the performance of each iBorderCtrl module and its effectiveness to the Border Control agent (Border Guard) both independently and when used in collaboration with other iBorderCtrl modules and sub-systems.
- To discover key patterns in the data, associated with either false accept or false rejects of travellers, which can be used for better decision making during border control.

The BCAT will also perform analysis on traffic data at the borders, in order to provide the traffic history and the expected traffic for certain dates.

The main functional and technical features of the BCAT Tool are given in the following Table:

<i>Name:</i>	<b><i>Border Control Analytics Tool</i></b>
<i>Technologies:</i>	<b><i>Scientific Workflow Management System</i></b>
<i>Installation:</i>	<b><i>Installed on a server</i></b>
<i>Connectivity:</i>	<b><i>Connected to the internet</i></b>
<i>Internal Information:</i>	<b><i>Get data from the iBorderCtrl database</i></b>
<i>Data at Rest:</i>	<b><i>Results of the analyses</i></b>
<i>User Management:</i>	<b><i>User authentication needed (only authorised users access the BCAT)</i></b>
<i>System States:</i>	<b><i>N/A</i></b>
<i>Security Needs:</i>	<b><i>Secure access to the iBorderCtrl database</i></b>

#### 3.7.1 Technical Requirements derived from the SOTA analysis from D2.1

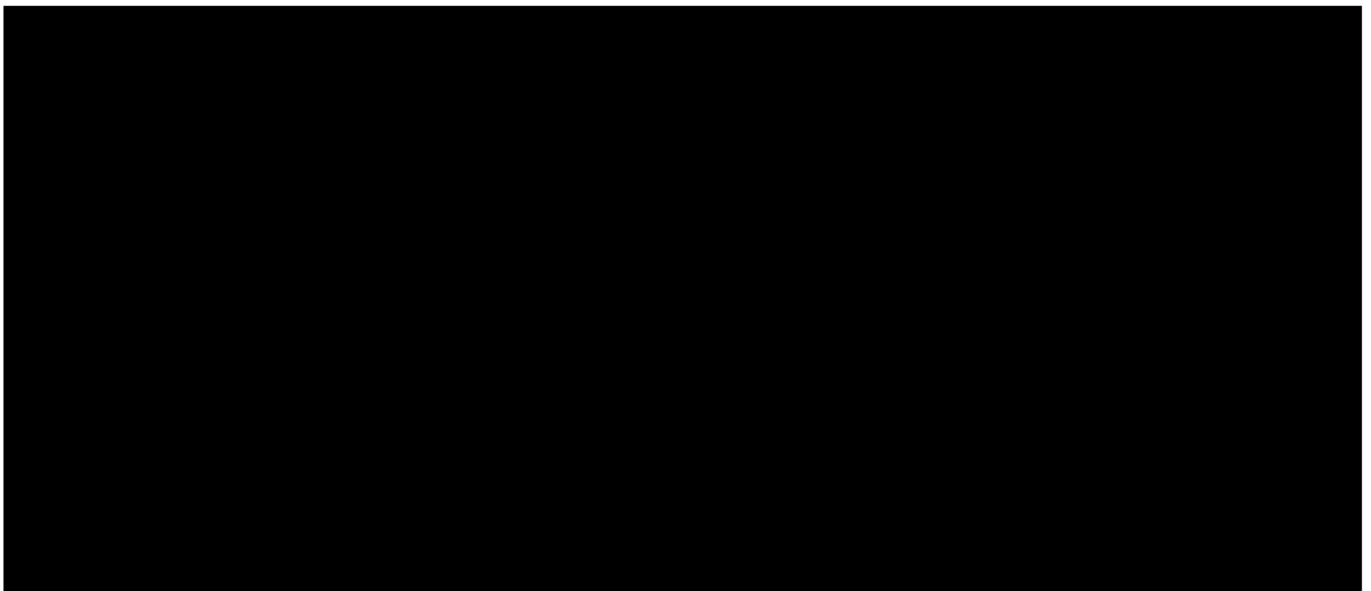


**Table 17 List of BCAT technical requirements based on SOTA analysis**





### 3.7.2 Functional description

**Figure 10 BCAT system workflow**

#### Data Collection

## [REDACTED]

- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

## [REDACTED]

### [REDACTED]

- [REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

## [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]  
[REDACTED]

## [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

### 3.7.3 Additional Technical Requirements derived from Architecture Components

[REDACTED]

[REDACTED]

**Table 18 List of BCAT additional technical requirements**

[illegible]



### 3.8 External Legacy and Social interfaces (ELSI) description

<i>Name:</i>	<i>External Legacy and Social Interfaces</i>
<i>Technologies:</i>	<i>REST API</i>
<i>Installation:</i>	<i>N/A</i>
<i>Connectivity:</i>	<i>Connected to the internet</i>
<i>Internal Information:</i>	<i>Get data from social media and legacy systems</i>
<i>Data at Rest:</i>	<i>The retrieved data stored in iBorderCtrl database</i>
<i>User Management:</i>	<i>User authentication needed</i>
<i>System States:</i>	<i>N/A</i>
<i>Security Needs:</i>	<i>Secure access to the iBorderCtrl database, and to the social media and legacy systems</i>

#### 3.8.1 Technical Requirements derived from the SOTA analysis from D2.1

[REDACTED]

*Table 19 List of External Interfaces technical requirements based on SOTA analysis*

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

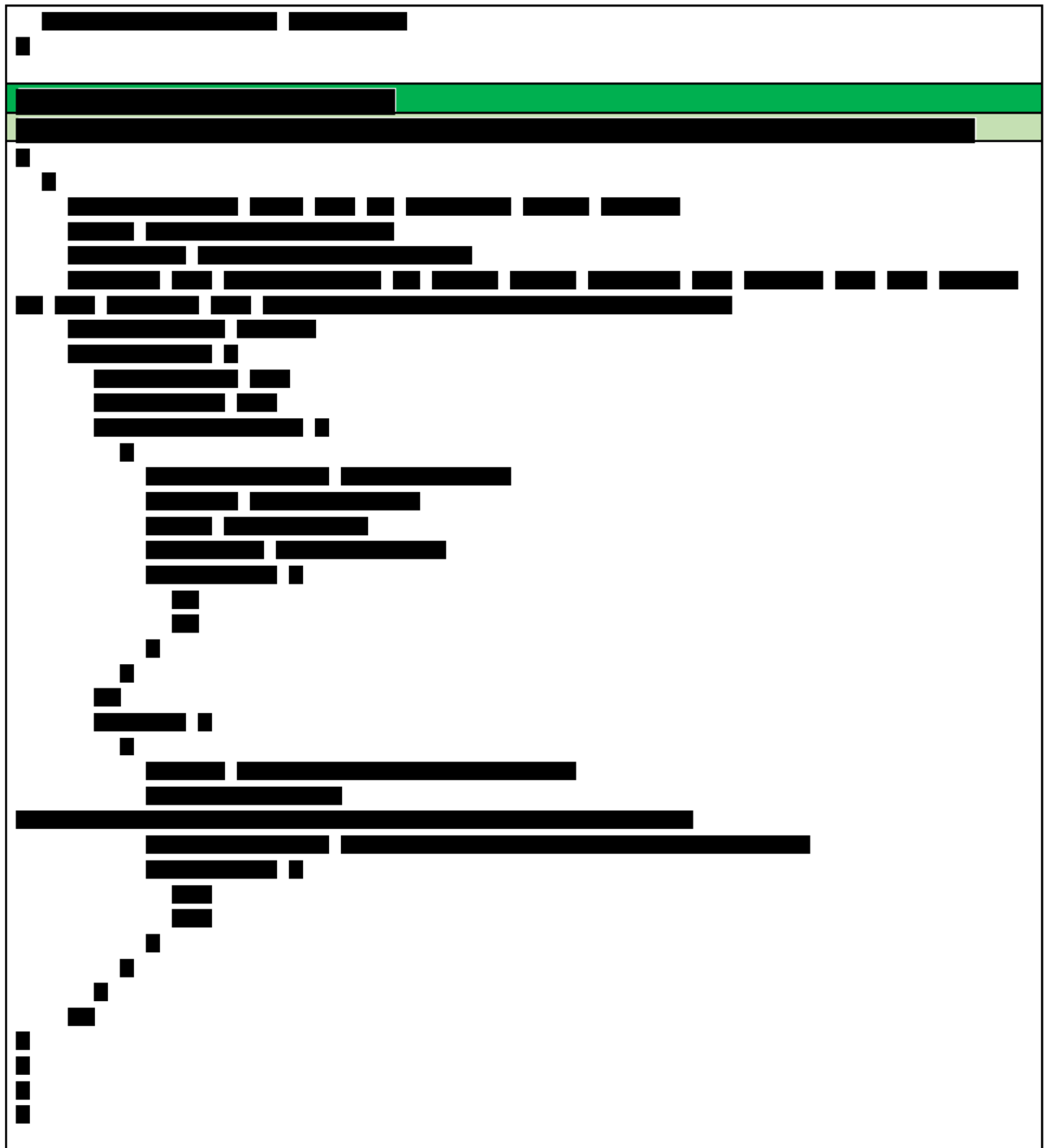
#### 3.8.2 Functional description

[REDACTED]

**Table 20 Example of Twitter's API requests and their response**

Page 74 of 165

[illegible]



[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 3.8.3 Additional Technical Requirements derived from Architecture Components

[REDACTED]

*Table 21 List of ELSI additional technical requirements*

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

## 4 General Constraints

### 4.1 Legal Constraints

As the reference architecture will be developed in parallel to the legal analysis conducted in D2.3, a direct interaction of both deliverables is required. To this extent, D2.3 contains the legal requirements that have to be implemented to the different functionalities and the overall system. As far as the reference architecture is concerned, the following principles and requirements are particularly important, as they can be directly transposed into technical specifications for the system. On the contrary, the lawfulness of and/or limitations to certain measures are described in D2.3.

#### 4.1.1 Data Subject's Rights

A fundamental aspect of data protection law is that data subjects are granted certain rights which they are free to exercise, unless restricted by law.<sup>4</sup> These include the right to information, right of access and the right to rectification or erasure of personal data and restriction of processing. Additionally, an iBorderCtrl volunteer participating in the piloting test run might revoke his or her consent, meaning that personal data of the data subject might not be processed anymore.

Since end users data is managed by the iBorderCtrl platform, this responsibility falls within the platform.

Moreover, regarding data replication within the iBorderCtrl platform the following are observed:

- ephemeral data are not replicated, and we can assume that zeroing the data can be enough;
- block storage is replicated using RAID technology, and hence same argument of ephemeral data applies;
- when an object deletion request is received, all the copies are synchronously deleted

#### 4.1.2 Privacy and Security by Design

**Privacy by Design** (PbD) is a principle for projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.<sup>5</sup> The approach to implementing privacy by design is reflected in the data protection reform package, consisting of the GDPR and Directive 680/2016/EU.<sup>6</sup> As already stated in Article 19, of the EU General Data Protection Regulation (GDPR 679/2016/EU), data controllers and processors are obliged to apply technical and organizational measures to protect data against accidental or unlawful destruction, loss disclosure, and other forms of unlawful processing.

The definition of such a principle should be as technologically neutral as possible, in order to last for a long period in a fast changing technological and social environment. Also it should be flexible enough so that data controllers and Data Protection Authorities are able, on a case by case basis, to translate it into concrete measures for guaranteeing data protection<sup>7</sup>.

---

<sup>4</sup> For further information, see chapter 5 of D2.3

<sup>5</sup> Privacy by design, [ico.org.uk](http://ico.org.uk)

<sup>6</sup> For further information on the legal aspects see chapter 6.2.3 of Deliverable 2.3.

<sup>7</sup> ARTICLE 29 Data Protection Working Party, Working Party on Police and Justice, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Adopted on 01 December 2009



The objectives of PbD may be accomplished by practicing the 7 Foundational Principles<sup>8</sup>.

Another fundamental aspect of the GDPR and Directive 680/2016 is the requirement to implement technical and organisational measures for the security of the data processed.<sup>9</sup> To this extent, the approach of **Security by Design** (SbD) has to be implanted in iBorderCtrl as well. Security by Design is also an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards and adherence to best programming practices.<sup>10</sup>

The objectives of SbD may be accomplished by practicing the 10 principles proposed by OWASP (see here: [https://www.owasp.org/index.php/Security by Design Principles](https://www.owasp.org/index.php/Security_by_Design_Principles)) that are related to the three pillars of information security namely: Confidentiality, Integrity and Availability.

### 4.1.3 Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA) is a process that can help identify and reduce the privacy risks of a project. A DPIA enables organisations to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.<sup>11</sup> A DPIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help design more efficient and effective processes for handling personal data. To be effective, it should be used throughout the development and implementation, using existing project management processes, thus reducing the resources needed to conduct the assessment.

The outcome of a DPIA should be a minimisation of privacy risk. More on the process, the consultation, the need for a DPIA, the information flows involved in a project, how we should identify any privacy and related risks, how we should identify possible privacy solutions (actions) to address the risks that have been identified can be found in<sup>12</sup>.

### 4.1.4 Data Protection Requirements

Most of the following data protection actions refer to IT-Security, which indeed is an integral part of data protection. Despite the question whether IT-security is to be seen in terms of data protection laws or from a technical perspective, both views lead on the same target: Securing the data (protecting data from being accessed by unauthorized users) and for ensuring the availability of data accessed by authorized users (backups, data recovery, archiving, replication, etc.).

To this respect, the requirements tables of the present 4.1.4 and the following 4.1.5 paragraph could be given in a merged version as well, since from a legal point of view, the requirement to ensure an adequate level of IT-security are stipulated both in the GDPR and directive 680/2016. However, in order to provide a more comprehensive presentation from a technical point of view, two separate tables (and thus corresponding paragraphs) are used so that:

- The requirements that are more related to the external users data protection are grouped together herein (paragraph 4.1.4) and
- Those that fall more in a wider IT and communication security approach are presented in 4.1.5.

---

<sup>8</sup> <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>

<sup>9</sup> For further information on the legal aspects see chapter 6.2.3 of Deliverable 2.3.

<sup>10</sup> “security by design”, Margaret Rouse, WhatIs.com

<sup>11</sup> “Conducting privacy impact assessments code of practice”, UK Information Commissioner’s Office, February 2014

<sup>12</sup> “Conducting privacy impact assessments code of practice”, UK Information Commissioner’s Office, February 2014

However, since the boundaries between are not clearly defined, the reader (as well as the IT developers involved) is strongly encouraged to view both tables as aspects of the same iBorderCtrl security dimension.

In order to add the requirement to implement technical and organisational measures to ensure a high level of IT-Security<sup>13</sup>, the following general recommendations are foreseen:

**Table 22 List of iBorderCtrl data protection requirements**

ID	Description
DPT-001	Establish procedures to sanitise tenant data when a program or project ends.
DPT-002	Track the destruction of both the tenant data and metadata through ticketing in a CMDB
DPT-003	Ensure that unauthorised users cannot access data either intentionally or accidentally ( <i>Restrict access to sensitive information</i> )
DPT-004	Only use supported software, i.e. software for which updates are still being provided
DPT-005	For data in transit end-to-end encryption should be applied. It must be ensured that personal data in transit is protected against active (e.g. replays, traffic injection) and passive attacks (e.g. eavesdropping), thus ensuring data integrity
DPT-006	Data must also be encrypted when stored. The data can be brought back through an encryption gateway for processing on secure servers. This makes encrypted data stored in the cloud a secure solution.
DPT-007	The encryption keys should not be used by, or be accessible to anyone others than the appointed consortium member(s)
DPT-008	Data should not be available in unencrypted form longer and more extensively than is absolutely necessary for the data processing process at hand.
DPT-009	Store sensitive data that we need. Never store unnecessary data. The first thing we have to determine is which data is sensitive enough to require encryption. For example, passwords, credit cards, health records, and personal information should be encrypted.
DPT-010	Use algorithms such as AES, RSA public key cryptography, and SHA-256 or better. Do not use weak algorithms, such as MD5 or SHA1
DPT-011	Ensure that all random numbers, random file names, random GUIDs, and random strings are generated in a cryptographically strong fashion. Also ensure that random algorithms are seeded with sufficient entropy
DPT-012	Use widely accepted algorithms and widely accepted implementations. Ensure that the implementation has (at minimum) had some cryptography experts involved in its creation. If possible, use an implementation that is FIPS 140-2 certified
DPT-013	Ensure data integrity and authenticity. Encryption must be always combined with message integrity protection. Otherwise the ciphertext will be vulnerable to padding oracle attack and data manipulation, especially if it's being passed over untrusted channel (e.g. in an URL or cookie).
DPT-014	Store the hashed value of passwords. The implemented services should not restrict the types of special characters (character set, or encoding) and the length (short or no length) of credentials.

<sup>13</sup> For further information on the legal aspects see chapter 6.2.3 of Deliverable 2.3.

	<p><u>MD5 and SHA-1 should not be used for hashing passwords.</u></p> <p>The European Union Agency for Network and Information Security Agency (ENISA) has published a detailed assessment of cryptographic measures. The report is entitled Algorithms, Key Sizes and Parameters Report - 2013 Recommendations. In section 3.3 it supports that:</p> <ul style="list-style-type: none"> <li>• MD5 is not appropriate; and</li> <li>• SHA-1 is acceptable for legacy systems but should not be designed into new systems.</li> </ul>
DPT-015	Periodically review the strength of the hash function and keep up to date with advances in computing power. The best way of achieving this is to use a password hashing scheme with a configurable work factor. Examples include: PBKDF2, bcrypt and scrypt <sup>14</sup> .
DPT-016	Use salting to make offline brute-force attacks less effective. A typical salt-length would be 128-bits, and this length is given as a minimum in NIST's "Recommendation for Password-Based Key Derivation".
DPT-017	Have a plan of action in case of a password breach. This should include how to reset users' passwords in bulk and how to notify them of what has happened and what they need to do about it <sup>14</sup> .
DPT-018	<p>Encourage users to strengthen their passwords by: <sup>14</sup></p> <ol style="list-style-type: none"> <li>a) creating long password or passphrase;</li> <li>b) using wide range of characters such as uppercase/lowercase letters, numbers, punctuation, special symbols;</li> <li>c) avoiding dictionary words and use of patterns derived from the physical keyboard layout such as "qwerty" or "!@2#3qaz".</li> </ol>
DPT-019	Provide a well-designed password "strength meter", to visually assist users, and give them an immediate feedback
DPT-020	The maximum length or permissible character set of passwords should not be limited as this simply reduces the time needed to mount a successful brute force attack
DPT-021	Document concrete procedures for managing encryption keys through the lifecycle and train the key custodians
DPT-022	Change encryption keys periodically. Key rotation is a must as all good keys do come to an end either through expiration or revocation
DPT-023	Generate encryption keys offline and store private keys with extreme care. Never transmit private keys over insecure channels
DPT-024	Use tools that employ open-source or public-domain encryption methods, such as: Truecrypt, GNU Privacy Guard, Off-the-record messaging or OTR
DPT-025	All uses of personal data should be automatically logged
DPT-026	Ensure that deletion of personal data from disks and other storage media can be executed in an effective way
DPT-027	Ensure that data deletion also affects backups
DPT-028	Use next-generation firewalls to facilitate understanding of what kind of data is leaving the perimeter. if it does not have the right security attributes or is going to an unfriendly destination, encryption should be enforced making sure that data is protected
DPT-029	Data should be unintelligible except when an authorized individual performs authorized operations on that data
DPT-030	<p>Put in place an effective data breach management policy covering:</p> <ul style="list-style-type: none"> <li>• Containment and recovery</li> <li>• Assessment of ongoing risk</li> <li>• Notification of breach</li> </ul>

#### 4.1.5 IT Security Requirements

### Table 23 List of iBorderCtrl IT Security requirements

[illegible]

<sup>14</sup> “Top five issues in VM backup”, Antony Adshead, January 2015

<sup>17</sup> “Protecting Personal Data in Online Services: Learning from the mistakes of others”, UK Information Commissioner’s Office, May 2014

	<div><div></div><div></div><div></div><div></div></div>
	<div><div></div><div></div><div></div></div>
	<div><div></div><div></div><div></div><div></div></div>
	<div><div></div><div></div><div></div><div></div><div></div><div></div></div>
	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>
	<div><div></div></div>
	<div><div></div><div></div></div>
	<div><div></div></div>
	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>
	<div><div></div><div></div><div></div><div></div><div></div></div>
	<div><div></div><div></div></div>
	<div><div></div><div></div><div></div><div></div></div>
	<div><div></div><div></div><div></div></div>
	<div><div></div><div></div><div></div><div></div><div></div></div>

<sup>18</sup> “Before you move to the cloud”, InfoSec Institute, April 2013

<sup>19</sup> “Five Simple Strategies for Securing APIs”, Scott Morrison, CA Technologies

<sup>20</sup> “Cloud Computing – Managing Security”, Harpreet Singh Sidana, 2012

<sup>21</sup> Cyber resilience is the ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions (according to <https://www.dhs.gov/what-security-and-resilience>)

<sup>22</sup> “Security Think Tank: For cyber resilience, assume the worst”, Tim Holman, July 2014

<sup>23</sup> “Security Think Tank: Cyber security resilience: Prepare, Share, Test”, Vladimir Jirasek, July 2014

<sup>24</sup> “Security Think Tank: Key elements of an incident response plan”, Peter Wenham, July 2014





performance or other attributes, or adapt to a changed environment." To this respect the following iBorderCtrl relevant requirements are set:

**Table 24 List of iBorderCtrl maintainability requirements**

■	■
■	■
■	■
■	■
■	■
■	■
■	■
■	■
■	■
■	■
■	■
■	■
■	■
■	■

■

■

■

■

■

■

■

**Table 25 List of iBorderCtrl extensibility requirements**

■	■
■	■ ■ ■ ■
■	■

■

■

Scalability is an overloaded term. Scalability exists in several dimensions<sup>29</sup>:

- Scalability of Performance
- Scalability of Availability
- Scalability of Maintenance
- Scalability of Expenditures

Following the established Scalability Design Principles<sup>29</sup> the following table lists the iBorderCtrl relevant requirements:

### Table 26 List of `iBorderCtrl` scalability requirements

[illegible]

### 4.3 General (hardware and additional) System Constraints

In this section the basic and most significant constraints at general system level will be presented in the following Table. Relevant requirements, where applicable, on a module / tool level have already been presented in the functional description and the tables per tool in the previous Chapter 3. It is noted that within this Deliverable the requirements contain the relevant information that will affect

<sup>29</sup> <https://elastisys.com/2015/09/10/scalability-design-principles/>

the design of the overall iBorderCtrl architectural aspects while the corresponding technical specs will be subject of WP3 and WP4 where they will be further examined and elaborated.

### Table 27 List of iBorderCtrl general system constraints / requirements

[illegible]

#### 4.4 Risk Mitigation Plan D1.2

Given that the project involves complex and significant ethics issues, i.e. the risk of stigmatization of individuals and groups and the risk of false positives, appropriate mitigation measures have to be

implemented. To this extent, measures that can be included in the reference architecture are listed below. As the legal framework to be applied during the research phase, for instance for the test pilots, differs from the legal framework to be applied for a (commercial) exploitation and a usage in real border-check scenarios after the project end, the mitigation measures are listed according to every phase.<sup>30</sup> A detailed description on the different ethical implications and arising risks will be provided in D1.2.

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

■ [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]



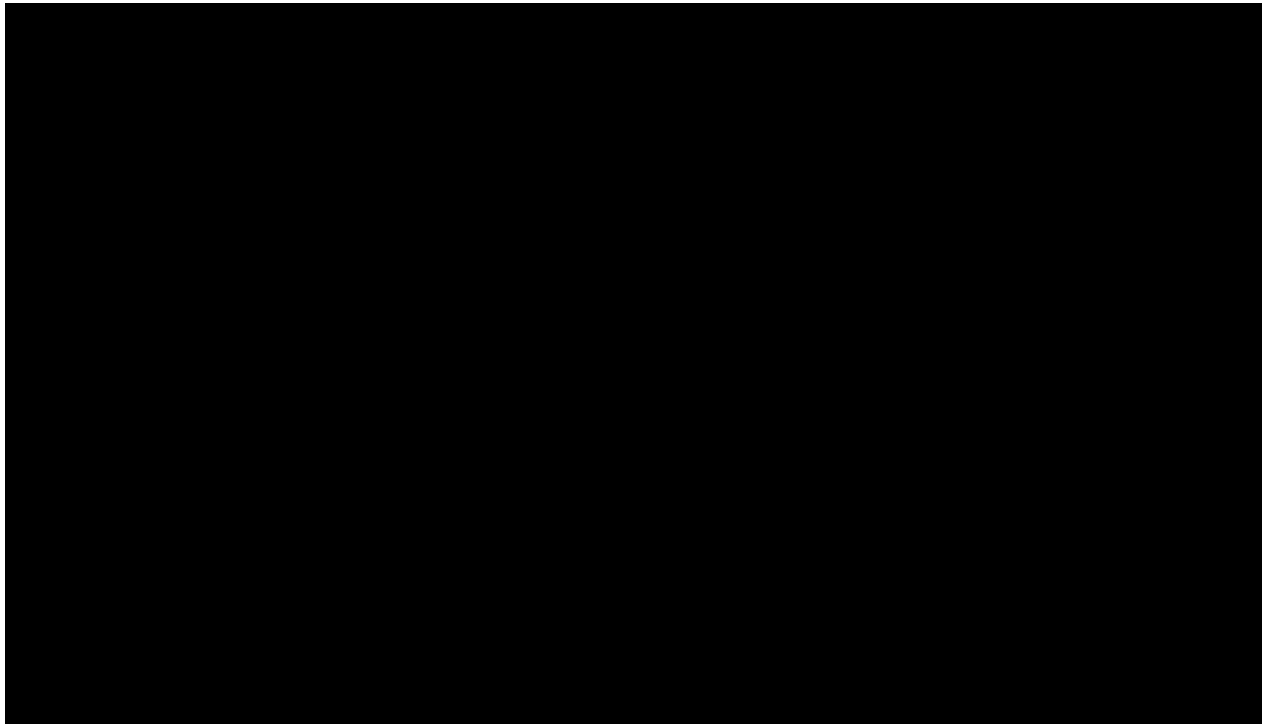
## 5 Use cases

The iBorderCtrl system unifies different modules and technologies and provides to both the travellers and the Border Guards a friendly and useful tool to speed up the procedure of crossing the border for bona fide travellers. The first step in defining the system's architecture would be to describe the Use Cases for each process.

Use Cases are basically stories that describe how discrete processes work. The stories include people (actors) and describe how the solution works from a user perspective. Use cases may be easier for the users to articulate, although the use cases may need to be distilled later into more specific detailed requirements (in particular through the evolution of the WP3 and WP4). The following section will describe the general Use Cases for the iBorderCtrl system.

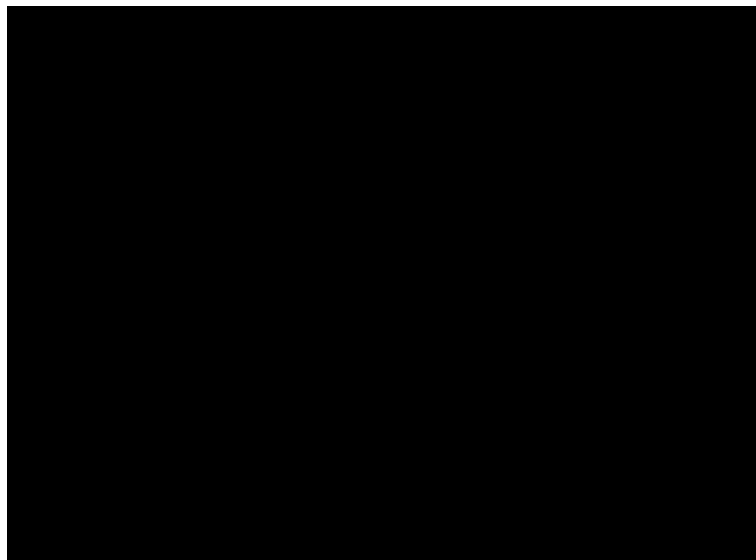
### 5.1 Pre-registration general scenario





[Redacted text line]

[Redacted text block consisting of five lines]



[Redacted text line]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

## 5.2 “On border” crossing point check general scenario

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 5.3 “On border” crossing point check with no pre-registration scenario

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

#### **5.4 Traveller crossing the border in their own private vehicle scenario**

[REDACTED]

[REDACTED]

#### **5.5 Traveller crossing the border in a vehicle used for the transport of goods scenario**

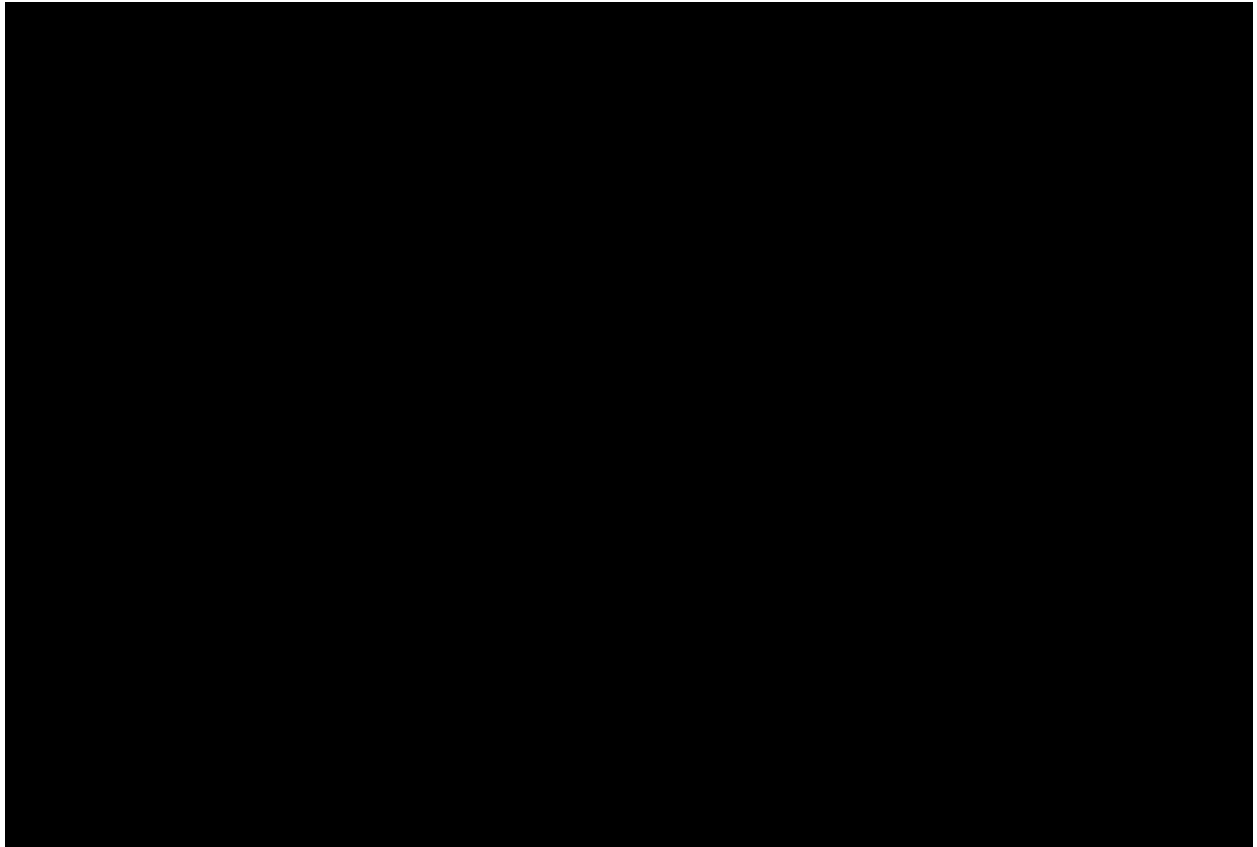
[REDACTED]

[REDACTED]

#### **5.6 Traveller crossing the border “on board” a coach bus or train scenario**

[REDACTED]

[REDACTED]



[Redacted text line]

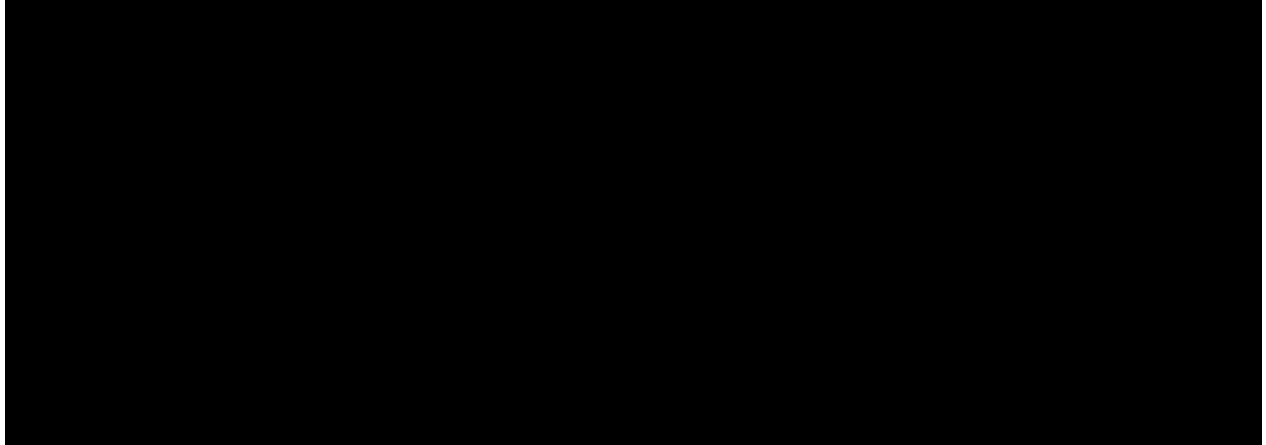
[Redacted text block]

[Redacted text block]

[Redacted text block]



## 5.7 Freight train crossing the border scenario



---

<sup>33</sup> CIM: Convention Internationale concernant le transport des Marchandises par chemin de fer (An internationally standardized freight document issued in rail transport)

## 5.8 Workflows

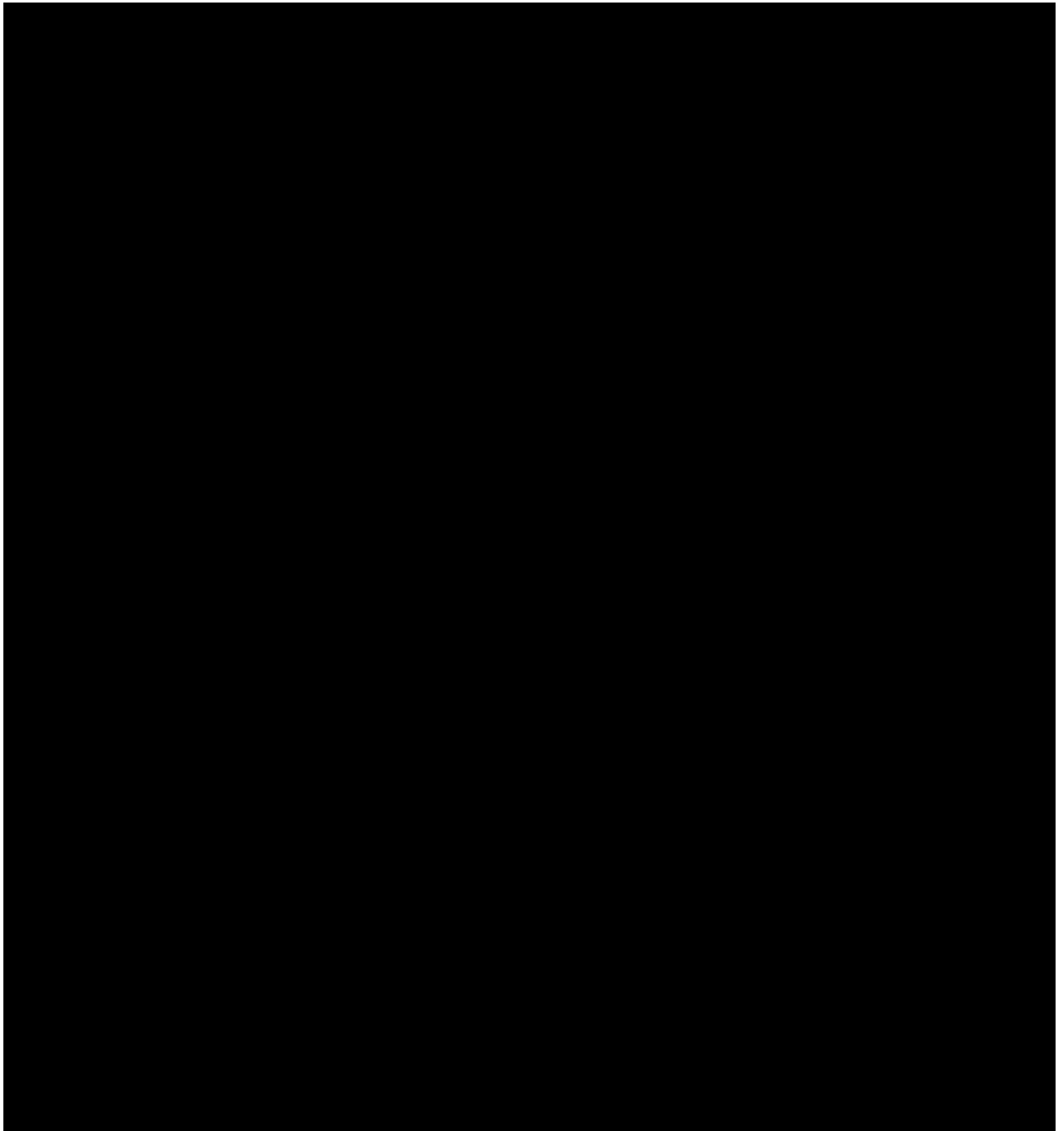
[REDACTED]

### 5.8.1 Pre-registration phase

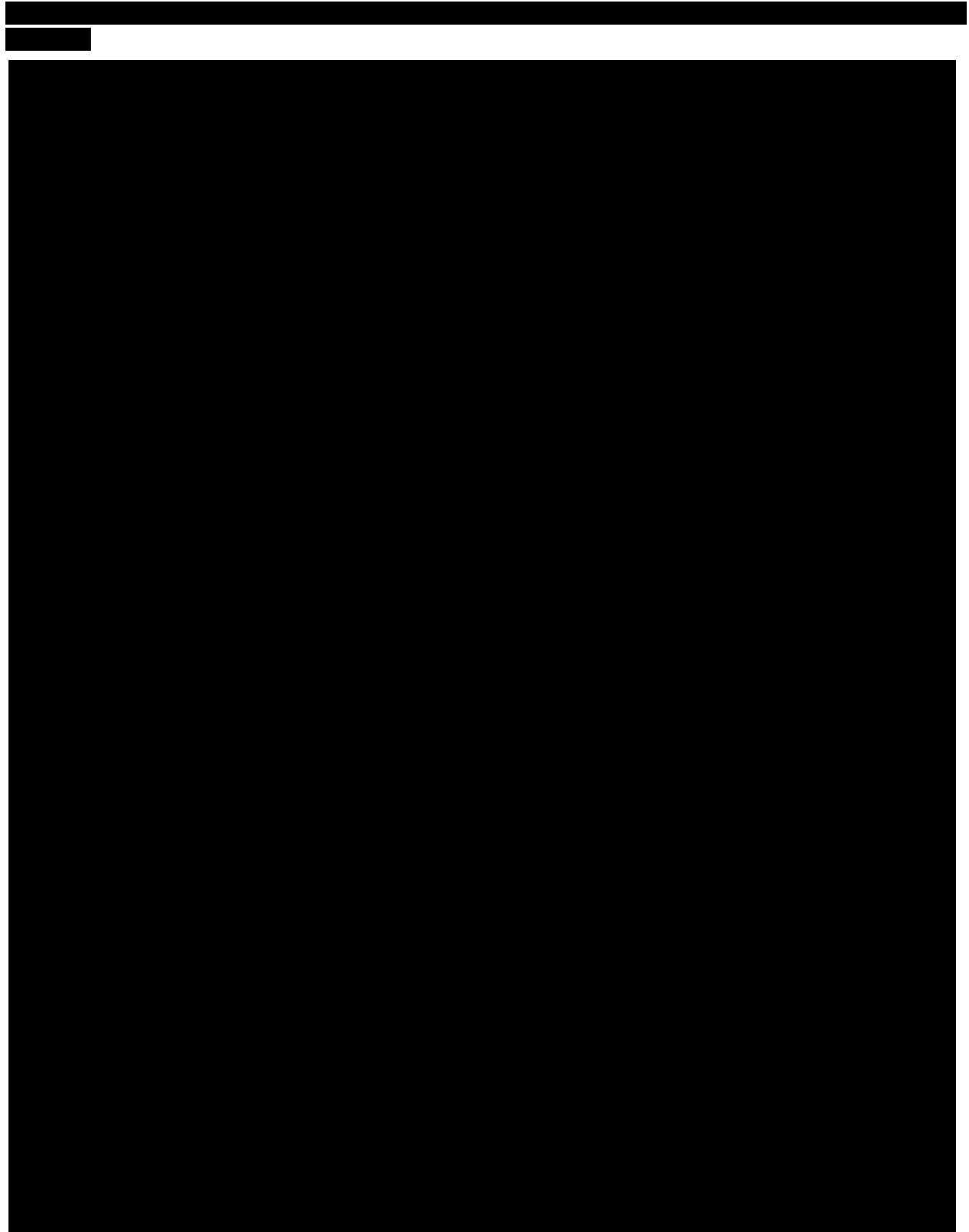
[REDACTED]

[REDACTED]

[REDACTED]



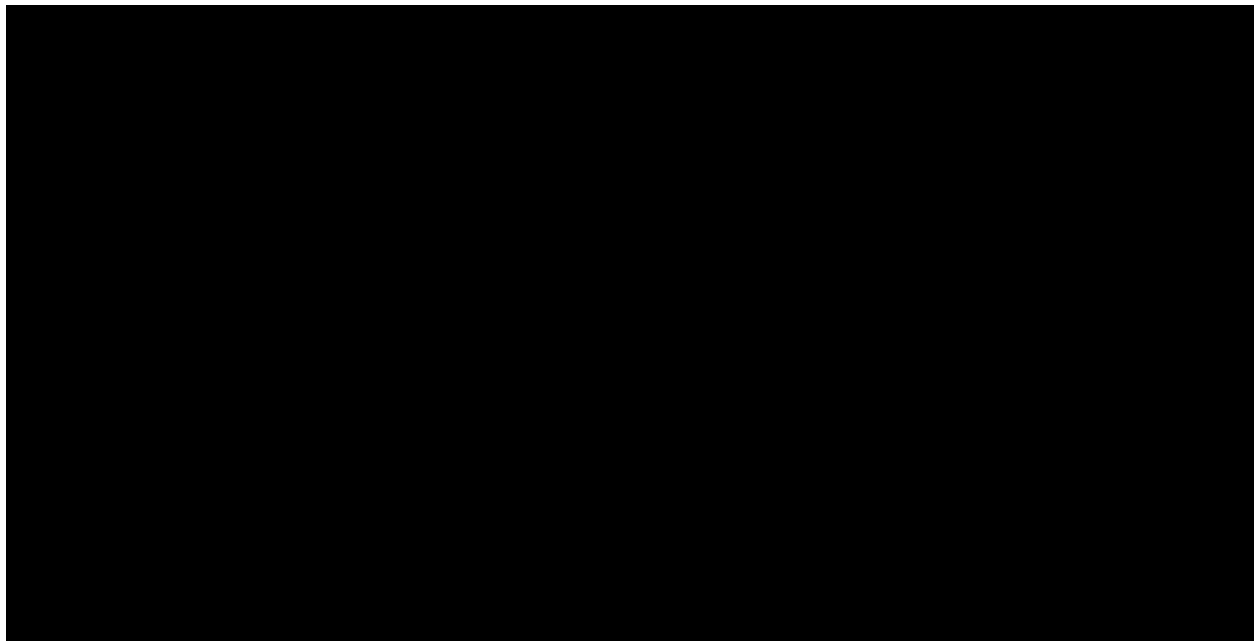
## 5.8.2 Crossing border phase



## 6 The overall iBorderCtrl Functional Architecture

The iBorderCtrl system unifies the different interdisciplinary modules presented in Chapter 3 and by taking into consideration the user, functional & technical requirements of Chapter 2 and the overall constraints analysed in Chapter 4 converges into an overall system that provides to both the travellers and the border guards a friendly and useful tool to speed up the procedure of crossing the border for bona fide travellers.

In a high level architecture the iBorderCtrl system can be described in three main parts: the traveller's side representing the pre-registration phase, the border crossing point side at the BCPs and the iBorderCtrl platform being the heart of the overall iBorderCtrl system. [REDACTED]



[REDACTED]

[REDACTED]

[illegible]

## 6.1 User Interaction with the system

[REDACTED]

- [REDACTED]  
[REDACTED]
- [REDACTED]

[REDACTED]  
[REDACTED]

- [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

## 6.2 iBorderCtrl system – Data handling (inputs / outputs)


*Table 29 iBorderCtrl data handling*




### 6.3 iBorderCtrl system – Integration of components and related interconnections

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

## 6.4 Software Stack

A large black rectangular redaction box covers the majority of the page content, obscuring all text and graphics in this section.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 6.5 Data Base description and architecture

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 6.6 Portable Unit architecture design

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

### 6.6.1 Portable Unit description

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]



[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

1. [REDACTED]

### Table 30 Portable Unit modules and requirements

[illegible]

Page 125 of 165

**Table 31 Portable Unit compliance with EU standards**





## 6.6.2 Wireless Radio Network connection of the portable units

### 6.6.2.1 Functional Description of the Radio Network

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

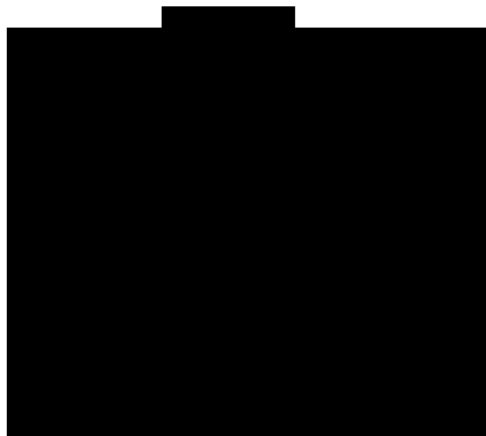
#### 6.6.2.2 Break Down of the basic network connections

[REDACTED]

[REDACTED]



[REDACTED]



[REDACTED]



[illegible][illegible]

\_\_\_\_\_

\_\_\_\_\_

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]

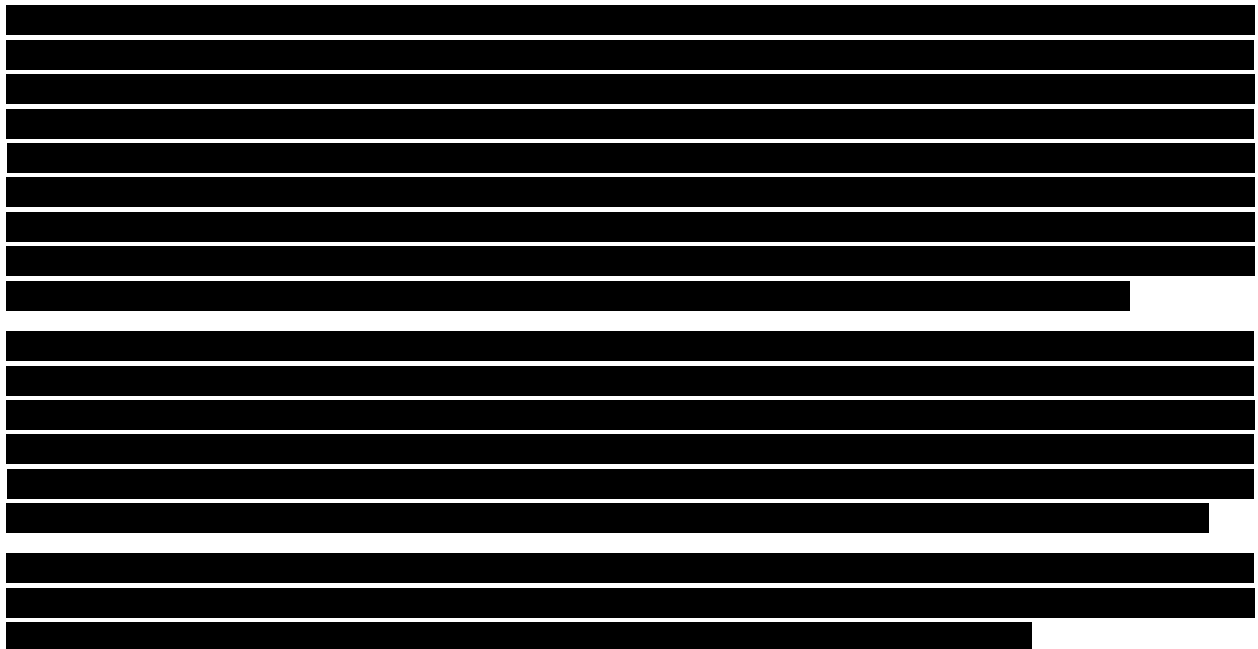
	<div></div> <div></div> <div></div> <div></div>
<div></div>	<div></div> <div></div> <div></div> <div></div>

## 7 Users management and users interfaces

Regarding the iBorderCtrl user interfaces (traveller, border guard, border manager) a common cross-platform client (both mobile and web) will be used.

Some examples of the technologies to be engaged could be Electron and Ionic, along with a web application (on a Tomcat servlet container) featuring a number of REST services. This technology (as well as most of the advanced cross-platform technologies/frameworks, enabling operation independently of the Operating System) allows the creation of a web-application as well as a client application for Windows, Linux, Mac, mobile phones, etc. at the same time.

More specifically, Electron is a framework for creating native applications with web technologies like JavaScript, HTML, and CSS. Electron is combining **Chromium** and **Node.js** into a single runtime and its applications can be packaged for Mac, Windows, and Linux. **Hence**, Electron is compatible and its applications are build and run on three platforms<sup>35</sup>.



---

<sup>35</sup> <https://electron.atom.io/>

<sup>36</sup> [https://mobidev.biz/blog/cross-platform\\_development\\_for\\_desktops\\_choosing\\_the\\_right\\_technology](https://mobidev.biz/blog/cross-platform_development_for_desktops_choosing_the_right_technology)

<sup>37</sup> [https://en.wikipedia.org/wiki/Electron\\_\(software\\_framework\)](https://en.wikipedia.org/wiki/Electron_(software_framework))

<sup>38</sup> <https://stackoverflow.com/tags/electron/info>

## 7.1 Travellers' User interface description

[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]


■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
	[REDACTED]

■	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]



[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
[REDACTED]	
[REDACTED]	
	[REDACTED]
	[REDACTED]
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]

[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
[REDACTED]	
	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]

## 7.2 Border Guards Agent User Interface (AUI)

[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]

[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[illegible]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]

[REDACTED]	
[REDACTED]	
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]

<div></div>	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
<div></div>	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
<div></div>	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
<div></div>	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	

[REDACTED]		
[REDACTED]		
<div></div>	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
<div></div>	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
<div></div>	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
<div></div>	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
<div></div>	[REDACTED]	
	[REDACTED]	
	[REDACTED]	



[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]

[illegible]

[illegible]

■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]

	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
	[REDACTED]
■	[REDACTED]

	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
■	[REDACTED]

[REDACTED]	
[REDACTED]	
■	[REDACTED]
	■ [REDACTED]
	■ [REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
[REDACTED]	

## 8 Final conclusions - Traceability Matrix

The present Deliverable D2.2 presents the general Reference Architecture of the iBorderCtrl system along with an extended set of functional and technical requirements derived from the user requirements set within the previous Deliverable D2.1.

Throughout this document, the overall architectural framework of the project is described both as an overall system and through its individual interdisciplinary components as well. The interaction with the various types of users (Border Guards and Border Managers at the BCPs and the general group of travellers) have been analysed both in terms of required functionalities and in technical architectural terms through the respective Applications and Interfaces. The various scenarios of the Use Cases, involving mainly the preregistration phase and the Border Crossing have been described in detail and are taken into serious consideration in the conceptual architecture definition so that to facilitate the forthcoming project development and implementation stages.

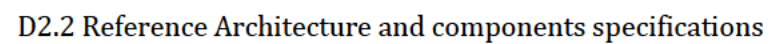
The overall iBorderCtrl software platform implementation will be based on a distributed computing architecture whose resources will be hosted on a cloud based infrastructure; the iBorderCtrl consortium is already after the accomplishment of this goal which will be further defined in the framework of WP4. Additionally, a mapping of the various iBorderCtrl modules and tools functionalities was carried out along with a set of respective technical requirements which will be further elaborated in the framework of WP3.

The iBorderCtrl consortium pays a great deal of attention to the Legal, Privacy and Security requirements that affect these kind of projects. Privacy by Design and Security by Design are the two pillars that the iBorderCtrl software platform builds upon. To this respect, this Deliverable D2.2 was in close connection and interaction with the legal framework provided through the Deliverable D2.3, evolving in parallel, while recent Regulations were also incorporated in the overall architecture. The result was a set of additional constraints (given in Chapter 4) which provide the main bases for data protection and IT security actions that will drive the subsequent development.

As denoted, the immediate benefit of D2.2 will be to stimulate the work and activities of the iBorderCtrl technical development framework in respect to WP3, WP4 and WP5 and to pave the way for an appropriate piloting implementation (WP6). This is accomplished by taking into account the existing procedures of border control and by adapting them through the Reference Architecture in order to facilitate more reliable, faster and more effective border checks and above all, to facilitate both the travellers and the BCP end users in that context.

Apart serving the abovementioned project goals, the present Deliverable will act as a reference point for the internal communication among the iBorderCtrl technical partners in all stages of research and development. To this respect, this document indicates how the work should evolve within the Work Packages 3 and 4, by showing and specifying the development paths, and the functional and technical parameters to be followed in order to finally meet the user needs.

For this reason, the Deliverable D2.2 concludes with a traceability matrix so that to facilitate the link between the technical requirements and the respective modules within the iBorderCtrl system and to place a common ground for ensuring that the overall final functionality of the iBorderCtrl system meets the all technical and user requirements. This traceability matrix, summarising all technical requirements per module is given in the following section. Constraints, such as the Privacy and Security by Design approached described in Chapter 4 will not be part of the traceability matrix and will followed during the development of each component separately but also by the integrated system implementation as a whole.

[illegible]

