H2020 – BES – 5 – 2015

Research Innovation Action

Intelligent Portable Control System

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

D3.2 First version of all technological tools and subsystems

Report Identifier:	D3.2		
Work-package, Task:	WP3	**Status – Version:**	1.00
Distribution Security:	PU	**Deliverable Type:**	R
Editor:	EVR		
Contributors:	ED, STR, MMU, JAS, BIO, ICCS		
Reviewers:	ED, ICCS		
Quality Reviewer:	ED		
Keywords:	Technical description, Prototypes, Development		
Project website: www.iborderctrl.eu			

Table of Contents

List of Tables

[redacted]

List of Figures

[redacted]

[redacted]

[redacted]

Abbreviations

ADDS	Automatic Deception Detection System
ANN	Artificial Neural Network
AP	Access Points
API	Application Programming Interface
BCP	Border Check Point
BS	Base Station (mobile network)
COTS	Commercial off-the-shelf
DAAT	Document Authenticity Analytics Tool
DB	Data Base
DPI	Dots Per Inch
ED	European Dynamics
ELSI	External and Legacy Systems Interface
EU	European Union
FAR	False Acceptance Rate
FMT	Face Matching Tool
FRR	False Rejection Rate
GUI	Graphical User Interface
HD	High Definition
HHD	Hidden Humans Detection
HNP	Hungarian National Police
HTTPS	Hypertext Transfer Protocol Secure
iBorderCtrl	Intelligent Portable Control System
ICAO	International Civil Aviation Organization
iFADO	Intranet False and Authentic Documents Online
IFrame	Inline Frame

IIS	Internet Information Services
JSON	JavaScript Object Notation
MMU	Manchester Metropolitan University
MRZ	Machine Readable Zone
NB	Non verbal
NVB	Non-Verbal Behaviour
OCR	Optical Character Recognition
PC	Personal Computer
PoE	Power over Ethernet
PU	Portable Unit
RBAT	Risk Based Analytics Tool
REST	Representational state transfer
RFID	Radio-Frequency Identification
SBC	Single Board Computer
SDK	Software Development Kit
SIS	Schengen Information System
ST	Silent Talker
TCN	Third Country National
URL	Uniform Resource Locator
UWB	Ultra-Wide Band
VIS	Visa Information System
WP	Work Package
XML	Extensible Mark-up Language

Executive Summary

This document describes the different subsystems and their applications that -combined with the physical sensors and hardware as identified and analysed in D3.1- provide the iBorderCtrl system with the appropriate routines to fulfil the expected checks and related processing of collected data.

Within this report, a thorough analysis of the developments and operation of all subsystems (ADDS, DAAT, BIO, FMT and HHD) is presented. For each system, a general overview followed by its technical description is given; the different interfaces with the rest of the modules in iBorderCtrl are listed followed by a description of the dataflow for the system and the data structures used. To ensure that the different systems comply with the technical requirements described in deliverable D2.2 a coverage matrix for each of the systems is compiled.

In the present Deliverable, a hardware components' description and their technical characteristics – to introduce the hardware integration of the iBorderCtrl portable unit to be described in-depth within the following WP5 Deliverables - is presented, to provide the technical approach of how the different components connects within the portable unit and a first approach to the harness design.

The appropriate performance of the above modules along with the iBorderCtrl Portable Unit is enabled by a robust iBorderCtrl radio network which is described in the last section of this report. The target is to implement a professional private radio network that guarantees increased performance throughput and sustainability without compromising in security features and quality of service. Thus, different requirements are imposed than a trivial commercial/consumer relevant application.

To sum up and link the work implemented within this deliverable in relation to the workplan of the Contract, this document provides an extensive description of the work linked to Work Package 3 and present the first version of the different technological tools used in iBorderCtrl project. This deliverable describes the results achieved till the first development milestone defined for the project (Milestone 2 – First version of all tools). The design and implementation of the different technologies described within this document started in month 3 with the selection of data collection devices (described in deliverable D3.1).

Deliverable D3.2 describes the work done - for the realisation of individual early prototypes of subsystems to finally constitute the iBorderCtrl system- till month 18 in all the different systems and will be updated in the following deliverable "D3.3 - Second version of all technological tools and subsystems for integration" that will be submitted during month 24 of the project.

1 Introduction

The present Deliverable D3.2 describes the different subsystems and their applications that are directly connected to the hardware components of the overall holistic iBorderCtrl system and correspond to the various scanners / sensors / readers that are implemented as technological modules. The physical sensors and scanners, as these were presented in Deliverable D3.1, are mainly connected with the iBorderCtrl Portable Unit in order to provide the border guards with an efficient and reliable portable tool to facilitate effective border checks during border crossing.

Based on that, the present Deliverable provides a general overview of the modules' technical description and describes in detail the appropriate routines to fulfil the expected checks and related processing of collected data, the different interfaces with the rest of the iBorderCtrl software tools and the main database along with the dataflow for each subsystem and the data structures used.

The Deliverable D3.2 is the first version of the WP3 development phase; thus, comprising a presentation of the specifications, technical features and the first, early versions of the related subsystems. The deliverable D3.2 refers to all technological development Tasks 3.2 – 3.8, directly addressing the general WP3 objectives which are:

- to adopt the physical sensors and hardware to be used for data collection,
- to develop and technically test all the hardware components and modules: the automated real time deception detection system (ADDS) along with the associated avatars, the biometrics tools (fingerprints and palm vein – BIO tools), the travel document authenticity analytics tool (DAAT), the face matching tool (FMT), to provide hidden human and vehicle detection functionalities
- and finally, to orchestrate and integrate all the above tools into a wearable iBorderCtrl Portable Unit, worn by the border guards, that will communicate with the rest of the system through a wireless radio network which guarantees performance and QoS.

As it will be seen in the following text, the present report highlights the multi-disciplinary manner of the involved modules. The involved disciplines range from purely biometrics applications (such as the fingerprints checks already carried out at the BCPs) to the use of acting and mimic methods (for the development of the avatars as border guards replicas) and the gesture and non-verbal behavior aspects of ADDS; also from purely algorithmic biometrics models (such as the face recognition module) along with document and OCR authentication (such as the DAAT tool with the iFADO functionalities) to basically hardware and signal processing aspects (as those related to the HHD tool).

And all these will be integrated and orchestrated together both through their hardware dimension through the iBorderCtrl Portable Unit, and through their software part as components of the overall holistic iBorderCtrl platform. Based on that, the current document should be read in parallel and in combination to the other respective deliverable of WP4, the Deliverable D4.1 which in turn represents the first version of the iBorderCtrl software platform and its main software components (the iBorderCtrl Database, the RBAT and the BCAT and ELSI tools). Thus, the delivery of these two reports fulfils the respective Milestone MS2 concerning the completion of the first iteration of all tools in M18.

At this point, in the present document, the main aspects of the corresponding design and development phase of the above tools is presented. The various tools will be checked for their proper communication and connectivity to the iBorderCtrl main Database and the RBAT and BCAT software tools to ensure that the foreseen performance in terms of the calculation of the matching and risk scores is achieved and that the various modules presents adequate level of reliability when combined together. Furthermore, these modules are currently being integrated as hardware parts to result in certain iterations of the iBorderCtrl Portable Unit to be tested and implemented during the project's implementation phase (in the framework of WP5 and WP6). To this respect, the results of all developments tests along with the software integration with the overall iBorderCtrl platform and together with their early integration and implementation outcomes for their debugging and improvements will lead to the second final version of the development that will be described in the following deliverable D3.3.

1.1 Structure of the document

The structure of the document is as follows:

In section 2 each of the subsystems (ADDS, DAAT, BIO, FMT and HHD) is described. For each system a general overview is provided followed by a technical description of the system. Then the different interfaces with the rest of the iBorderCtrl platform software modules are listed followed by a description of the dataflow for the system and the data structures used. To ensure that the different systems comply with the technical requirements described in deliverable D2.2 a coverage matrix for each of the systems is compiled. The last subsection for each system technical description is the definition of the Unit tests that are going to be performed for each system.

Section 3 describes the different hardware components that form the Portable Unit, together with their technical characteristics. This section also provides a first description of how the different components connects within the portable unit along with a first approach to the harness design, while a more detailed description of the Portable Unit will be held within the related WP5 Deliverables.

Finally, section 4 describes the iBorderCtrl radio network. This description includes the list of technical requirements for the Radio network, both from the user point of view and the equipment minimum requirements. The technical features of the different radio network options will be described together with the implementation design, including equipment description, internet service provision and the radio equipment selection. Finally, this section describes the different performance testing that will be done including the metrics that will be used and the testing scenarios.

2 iBorderCtrl sub-systems technical description

This section provides a technical overview of each of the different modules that are being developed in the framework of WP3 as part of the iBorderCtrl system. Each module is described in its own subsection providing a technical description together with the module's interfaces and the data flow and structure. Finally for each module a list of the technical requirements described in deliverable D2.2 is provided along with the way that these are fulfilled.

2.1 ADDS and AVATAR overview

Overview

This section provides an overview of the ADDS module. An overview of the workflow in relation to the other modules can be seen in Figure 1.

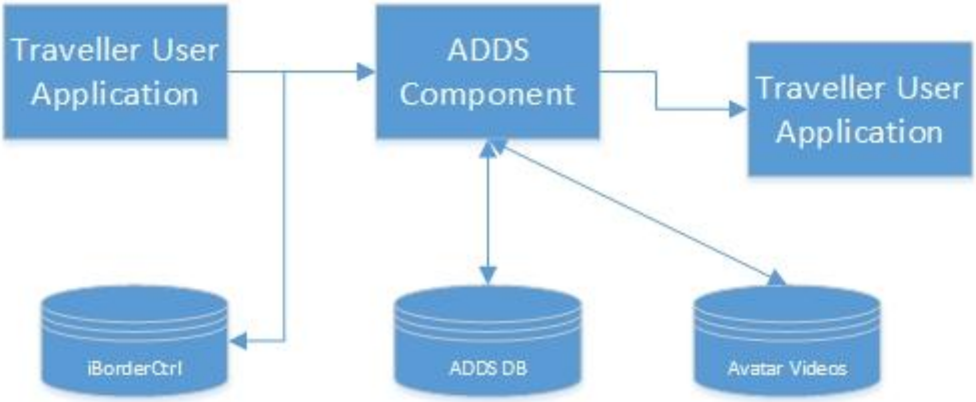

Figure 1 High Level ADDS Module Workflow

Each traveller will have been assigned an iBorderCtrl_ID (through a QR code) that will be used throughout the interview. Control will be passed from the Traveller User Application to ADDS using an iframe, at which point ADDS will request sufficient information about the traveller and the trip to be able to ask 16 interview questions (see 0). ADDS will be responsible for conducting the interview where the Avatar asks questions, utilising three attitudes (puzzled, neutral and positive) and two avatars, one male and one female. The type of attitude used by the Avatar will depend upon the deception score of the last question answered by the traveller. Such adaptation of attitude will be determined empirically through internal experiments at MMU and during the pilot study. During the interview, ADDS will make requests to the avatar database to receive the requested corresponding Avatar video and will also update the local ADDS database respectively. At the conclusion of the interview: 1) questions and interview scores and classification and 2) 1 second of video frames will be uploaded to the iBorderCtrl database to be used by the RBAT, FMT and BCAT modules.

The ADDS module consists of five components:

- The ADDS API
- The Avatar
- The Silent Talker
- The ADDS Control Module
- The ADDS Interview interface

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

2.2 DAAT overview

This application concerns the verification of travel documents in short time durations. The implementation will take place in two stages, both in the pre-arrival/registration phase (1st phase), as well as in the check phase (2nd phase). Document scanners/readers/IP cameras will be used, for travellers' documents (passports, IDs, car licence, etc.), so that the level/quality of information will be checked, to offer unparalleled scrutiny of travel documents for signs of falsification or counterfeiting.

Summarising, the DAAT system functionality comprises of the following:

- Informing the border guard about passport security features that he should focus on.
- Assessing the validation performed by the Regula scanner and creating a risk score.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

2.3 BIO overview

The BIO module is composed of two sub-modules related but independent from each other: the palm vein module and the fingerprint module.

2.3.1 Fingerprint module

This module is used to validate the identity of a traveller using the fingerprints stored in different national or European databases (SIS, VIS, EURODAC, National Databases, etc.) or in their travel document (biometric passport – RFID chip) to compare them with the sample that the fingerprint reader in the portable unit will capture.

The fingerprint module will be integrated in the Portable Unit, and will run in the central processor of the tablet that hosts the Border Guard interface. The Border Guard interface will provide a specific functionality that will allow the border guard to capture the fingerprints from the traveller and will send these images to the fingerprint module for validation.

The validation module will receive the captured image from the traveller fingerprints and the sample with which the module has to compare the fingerprints. This sample could be retrieved from different sources such as external system (VIS, SIS, National Databases etc.) or the biometric information stored in the traveller passport. The module will compare both images and provide a match / not match result. This result corresponds to a risk score (according to the match percentage) that will be send to the iBorderCtrl database and will be made known to the border guard through the RBAT overall risk score calculation and assessment (fingerprint analysis information).

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

2.3.2 Palm Vein module

This module is used to validate the identity of a traveller using the palm vein sensor as a secondary identification method. Currently, there is no palm vein database on different national or European level, therefore the palm vein database will grow based on the usage of the system but will be able to support the identification of the traveller regardless of personal information. The palm vein system compares the biometric captured template with the biometric enrolment template previously stored. The module consists of the following software and hardware components:

Hardware components:

- Palm vein sensor for the enrolment procedure with the associated handguide
- Palm vein sensor for the capture procedure either in a handguide or without handguide integrated into the portable device.

Software components:

- Client software, responsible for carrying out security features, compressing the data package, establishing a secure communication channel with the server.
- Client GUI for the portable device or fat client, where the end users can use all user related features.
- Server software, responsible for the management of the central palm vein database, carrying out matching procedures, communicating with third party systems (multiple server software can be connected to each other). The updating can be carried out via real time synchronization.

- System management module for the administrators of the end user.

The palm vein reader will be integrated into the portable unit but will be also used as a desk device in connection with fat clients. The border guard can start the authentication or enrolment procedure via the client GUI. The captured or enrolled templates will be forwarded to the central server software for matching and the result of the matching will be sent back to the client GUI to inform the border guard about the result (match /no match) and will be forwarded also including log files to the central iBorderCtrl database in order the risk score to be included within the RBAT.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

2.4 FMT overview

The Face Marching Tool (FMT) system provides to the iBorderCtrl solution facial recognition biometric capabilities. These capabilities are used in different ways in both the pre-registration and the crossing phases. The main purpose of this module is to detect deception in the process and provide a risk related with this possibility. In section 3.4 of deliverable D2.2 a first approach to the functionality of this module was provided, together with the technical requirements related to both the FMT module and system as a whole.

Pre-registration validation:

During the pre-registration phase the iBorderCtrl user logs into the application and during the process of entering the travel information the user undertakes an interview with iBorderCtrl avatar. The FMT will estimate the risk that the person that is answering the interview is not the iBorderCtrl application user. In order to calculate this risk, the module will match the user's biometric reference stored in the system with the images taken during the interview.

If is the first time the user makes use of the application, the images taken during the interview will be employed to create the biometric model of the user. This biometric reference is the one that will be used later to check the risk of deception.

The risk provided by the FMT in the pre-registration phase will be defined by a three-value scale. If the matching score is above certain threshold the risk will be low, if it's between two defined values it will be medium and if it's below certain threshold it will be high.

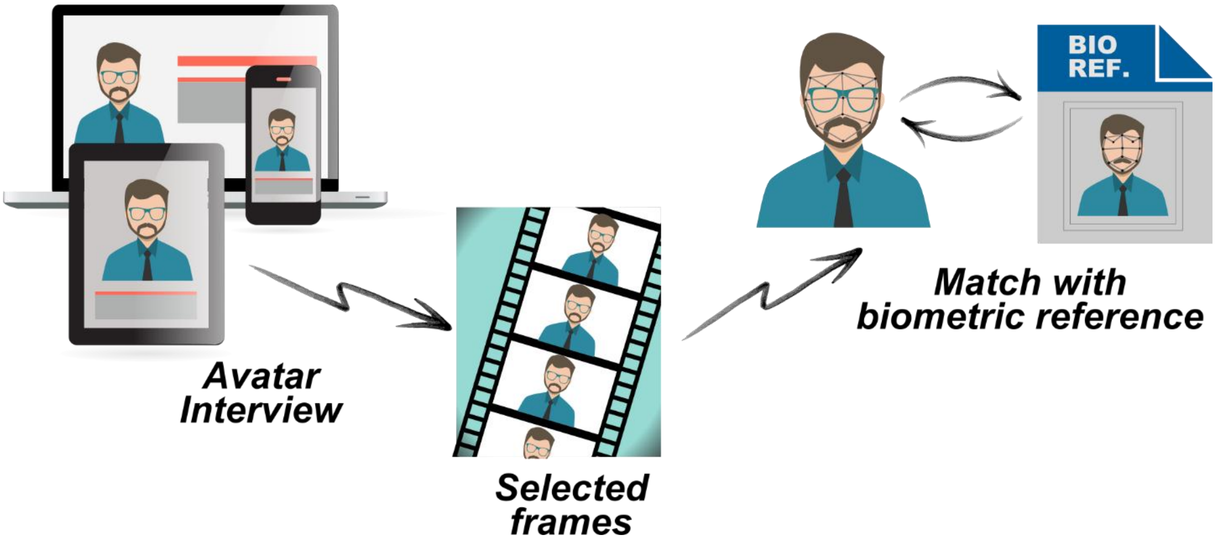

Figure 30 FMT pre-registration matching

BCP crossing validation:

In the BCP the border guard will follow the defined procedure using the application that the Portable Unit provides. This Border Guard User Application will indicate all the steps the check must undertake (read iBorderCtrl QR code, check documents, etc.). Within this process, one of the steps will be the validation of the identity of the traveller using facial recognition.

To assign the risk of deception during the BCP control process, three different checks will take place: the first one will match the images taken by the portable unit's camera and the High definition (HD) image obtained from the passport (embedded RFID chip) or from any external system (such as VIS). This will provide the risk that the person at the border crossing point is not the same one than the one shown in the documents.

If the person at the BCP has passed through the pre-registration phase, then the second check will measure the risk that the person appearing in the documents (i.e. passport) is the same one that performed the avatar interview during the pre-registration process. The third check that will be held is the risk that the person at the BCP (images taken by the camera of the portable unit) is the same one that undertook the interview during the pre-registration.

Like in the pre-registration phase the risk will be calculated as follows: If the matching score is above certain threshold the risk will be low, if it's between two defined values it will be medium and if it's below certain threshold it will be high.

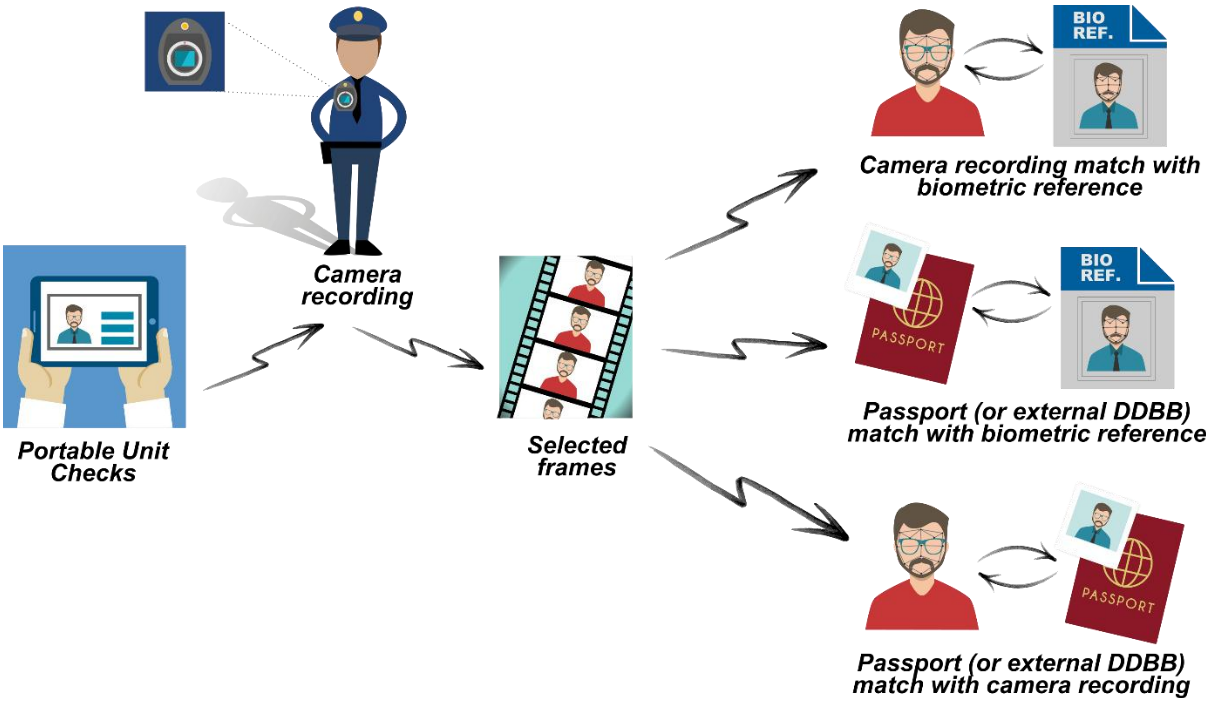
Camera recording
Portable Unit Checks
Selected frames
BIO REF.
Camera recording match with biometric reference
PASSPORT
BIO REF.
Passport (or external DDBB) match with biometric reference
PASSPORT
Passport (or external DDBB) match with camera recording

Figure 31 FMT BCP matching

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

2.5 [redacted]

The Hidden Humans Detection tool (HHD) addresses the issue of illegal migration and trafficking, often confronted at the border control points; passengers trying to illegally cross the borders, often hide themselves inside ordinary vehicles or closed compartments (i.e. in cargo containers). Detailed aspects of the problem and the up-to-date knowledge of confronting mechanisms and technologies have already been described in D2.1 and in D3.1; covering both the scientific and commercial state of the art and the commercially available solutions in a wider perspective of relevant applications.

In section 3.5 of Deliverable D2.2 a first approach towards the functionalities and initial architecture of this module has been described, together with its general technical requirements. Furthermore, in D2.3 concerning the relevant legal framework, it was seen that no specific technology is mandatory or recommended by the regulations for the relevant checks at the BCPs and that the checks for hidden humans are being made when the Border Guards feel that is necessary (i.e. when the subject – driver or vehicle – is under suspicion or a warrant or directive has been imposed prior to the border check).

The main purpose of the HHD module is to detect the presence of an alive being inside vehicles or closed compartments and provide a risk related with this possibility. The detection of presence is based on the detection (capture, tracking) of the micro-movements or vital signs of the alive being such as: breathing, slight movements or slight vibrations derived when leaning upon the surface in between. The detection greatly depends on the medium between the subject (hidden alive being) and the detection device; the medium may be air, plastic, wood or metallic (as in cargo containers). Thus, different technologies and sensors are used depending on the medium in between.

The most penetrating detection technology through all mediums is the x-rays. However, the relevant devices are large and expensive facilities, not complying with portable or handheld devices and low size apparatus. Furthermore, in the x-rays case, the border guard's visual inspection of the received images, representing the whole interior of the closed compartment, is absolutely needed to determine the presence of alive beings inside; to this respect, the detection signals and images in this case do not facilitate their integration within the scope and means of the iBorderCtrl system and platform. Moreover, the use of x-rays imaging systems often requires separate lanes where long queues of truck containers are the usual routine in BCPs every-day activities.

On the other hand, a more thorough search in all kinds of vehicles is usually being made at the second line, often dictated by specific warrants and inside information or even sample checks at regular periods or, usually, caused by suspicions raised during the first line border checks; the latter is based on the border guard's own experience and perspicacity, often with the help of K9 units. However, all the above, are not a standard everyday routine at all border control checks in all countries; they do present an occasional manner requiring specific facilities and equipment, while the relevant control checks are being transferred to the second line, to avoid further delays in the first one.

To this respect, **the attempt of implementing a kind of hidden human detection (HHD) tool within the iBorderCtrl, apart from its integration aspects to an overall holistic platform, addresses the issue of transferring the relevant control checks from the second line to the first one**; thus, the target is the border guard to be given the ability to perform at least preliminary checks of this kind on a routine basis and check if this approach leads to reducing the inherent delays. For that, other technologies than the static, large x-rays facilities need to be tested and exploited, while the second line related checks should still be integrated within the iBorderCtrl system.

In this context, the use of other technologies that conditionally can be made portable and lower in size is being examined herein for the aims and purpose of the iBorderCtrl project. The main aspects of these technologies have been extensively described both in D2.1 for the relevant state-of-the-art and in D3.1 in relation to the commercially available systems. From the scientifically point of the view**, the large degree of difficulty when implementing such technologies cannot be ignored;** the issue still remains an active problem for which no completely suitable solutions exist. To this respect, there is no single sensor or device that can accommodate all technologies or be used in all mediums. As already argued in the previous deliverables, the whole aspect is in the edge of current research for a variety of applications starting from bio-signals acquisition for medical purposes up to locating and detecting alive beings trapped or buried under buildings or their remains after earthquakes.

For that reasons the sensors that will constitute the HHD tool, different in size and technology, are not possible to be integrated, as a hardware, to the wearable set of the iBorderCtrl Portable Unit. However, the sensors to be implemented are selected in such a way so that to be as small in size as possible and even handheld, in order to create the least possible inconvenience to the Border Guard when implementing and carrying them.

HHD tool functionalities: contribution to the iBorderCtrl and differences from other tools

From all the above it is clear that the HHD tool is different from the other biometric modules of the iBorderCtrl system in the sense that it is mostly a sensing (detector) and data acquisition device. **Both functionalities are made on-board: upon the sensor device.**

A risk score representing the degree of certainty that an alive being has been detected will be provided directly from the HHD tool to the iBorderCtrl portable unit; and through that to the iBorderCtrl database and the rule based RBAT tool, contributing to the overall risk score and facilitating the Border Guard's final decision.

The risk score – representing the presence of hidden humans inside a vehicle and thus representing the degree of the driver's / traveller's reliability – along with other information provided by the HHD tool i.e. the level of detection confidence, will be stored and recorded. To this end, either in first or second line, **the HHD tool is mostly useful to the BCAT tool; by contributing to the determination of bona fide (or not) travellers**. As seen in the use scenarios of D2.2 (Chapter 5), the detection for illegal immigrants hidden inside vehicles or closed compartments takes place in the end of the process, ideally representing a "go - no go" situation. Thus, by this way, the result of this tool may just instantly alter and invert the potentially "good / low risk" result of the previous biometrics checks.

A driver that hides illegal passengers in his vehicle may himself be absolutely legal and a low risk, frequent traveler; however, this cannot be verified unless his vehicle is searched and thus all his bona fide image is tumbled. The main tool for analyzing, processing and recording this overturn, caused by the implementation of HHD tool, is the BCAT tool which will provide the final profile of bona fide (or not) travelers over time. Also, through the BCAT tool and the Border Manager Application the determination of the rules defining the RBAT's risk score can be adjusted in case that a sequence of similar hidden humans detected events occurs on a constant basis.

Given the specific operational dimensions discussed in the previous paragraph, the HHD tool is meant only for the actual BCP crossing at the borders. Due to the different nature of the tool and its purpose, it is evident that no comparison or matching takes place with prior stored database elements (i.e. images like in fingerprints or in face matching).

Since, in principle due to the current border control legal framework, it lies upon the decision of the Border Guard whether or not to perform detection for hidden humans, the Border Guard User Application and related User Interface (within the iBorderCtrl portable unit's tablet) have accordingly specified and adjusted as this is described in Deliverable D4.1; following the provisions of D2.2 (Chapter 7) and the border crossing case studies and relevant scenarios (D2.2 Chapter 5).

As it seems, the focus of the HHD tool is on the sensor (sensing and data acquisition device). To this respect, the system data structure and data flow is rather simpler than the rest of the iBorderCtrl modules, as it will be presented in the following.

As mentioned above, the HHD tool mainly addresses the issue of illegal migration and trafficking; it is evident though, that this is not a biometric tool like the rest of the main iBorderCtrl modules. However, since the iBorderCtrl project addresses a holistic system for more efficient and reliable border crossing to facilitate also the Border Guards in their everyday activities and final decisions, a tool like the HHD could not be disregarded. Especially, when nowadays, attempts for illegal border crossing have been dramatically increased due to conflicts in the vicinity of EU area and due to the wide extend of terrorism both in the interior and the exterior of EU. As a consequence, this was also confirmed and verified by the Border Guards end users through their interviews responses and end users requirements in D2.1 and their interpretation into technical and functional requirements in D2.2.

Of course, the relevant approach of research and development concerning the HHD tool in the framework of the iBorderCtrl project will be made up to the level that is feasible in implementation terms, given the limitations in the technical and scientific approach as these were described in D2.1, D2.2 and D3.1 and briefly presented in the previous paragraph. To this respect, the main purpose of implementing the HHD tool within the iBorderCtrl framework is to present, up to the technical permitted level, **a proof of concept** of how similar tools or subsystems can be integrated, as software response, to the overall holistic iBorderCtrl platform and respectively to provide a roadmap on how this can be rendered feasible for current and future commercial similar modules.

This is also, evident due to the procedures that are being currently followed within the BCPs, where the use of similar tools (as for example gas sensors) is left to be conducted mainly at the second line checks. To this respect, the attempt herein, in the framework of the iBorderCtrl project, is to provide the ability to the Border Guards to make at least a preliminary such check during the first line and if suspicions of fraud in this matter are conceived or the overall RBAT risk score is high enough, to guide and transfer the whole control check to the second line and to more thorough checks.

Based on all the above, the HHD technical description will be presented in the following sections. Due to the inherent nature of the HHD tool, as discussed above, the presentation will follow in general terms the given structure so far, while differences will be indicated.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3 iBorderCtrl Portable Unit description

The main purpose of the Portable Unit (PU) development is to achieve greater comfort, security and to reduce time spent at the border by travellers.

It should be noted herein, that since the iBorderCtrl Portable Unit is the outcome of the hardware integration process, a more detailed and thorough description of its related aspects will be presented in the relevant deliverables of WP5. However, for the sake of providing a complete presentation within the current document, the main components and development parameters of the iBorderCtrl PU are given briefly herein as an introduction to the relevant integration that will follow.

The PU will be used as a tool to detect and prevent illicit crossings of people and goods. Although such means were mainly available at airports and harbours, the implementation of iBorderCtrl PU makes them available also along the border.

The complete solution of PU will comprise of six devices (plus the HHD tool which is a separate not mounted device) communicating with the central processing unit through wireless and wired connection interfaces, such as WiFi, Bluetooth and USB. The devices selected and connected to the PU provide all the necessary technologies to carry out the Border Crossing Procedures (BCP) according to European standards and the iBorderCtrl project concept.

The management of the system will be provided by the central module – the tablet application responsible for integrating all hardware modules, wireless communication with the remaining parts of the iBorderCtrl platform, intelligent control of the power consumption and providing the interface with the Border Officer (the end-user).

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4 iBorderCtrl Radio Network description

In this section a detailed overview of the radio network solutions is provided, namely the required features to be implemented within the framework of WP6, the design/dimensioning considerations and the planned architecture of the several subsystems.

4.1 Radio Network Requirements and Technical description

As already mentioned in previous deliverables and in the project's description itself, the iBorderCtrl platform will provide the border guards with portable devices to enhance the travellers screening process at the border control points (BCPs); such devices will have to communicate with the various iBorderCtrl subsystems to exchange data (retrieve information and provide feedback) through a cloud-based database/application servers. As the border guards will have to move freely around the BCP control areas while performing the various checks/screening procedures, their equipment must be able to maintain a stable, high throughput connection with the application servers.

In the following a more detailed description of the various requirements that the network setup needs to meet is given.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4.3 Radio Network Planning and Dimensioning

Radio network planning and dimensioning is generally a non-trivial procedure as it involves many different and sometimes dependent or conflicting aspects.

The deployed network should ensure that the following **performance criteria** are met:

Coverage

The **whole area of the BCP** locations where the travellers' checks take place have to be **fully covered** by the radio network. This should happen in an efficient manner, i.e. with as few Access Points (APs) as possible for practical and economic reasons. Coverage if affected by the environment, in this case a rural location. The terrain at BCPs is expected to be **flat with no clutter** at the area of interest. The buildings/booths are not expected to particularly hinder coverage as they are small, of low height and usually built using light materials. Should it be required, **in-building coverage** can be maintained using indoor APs. To ensure best network performance, **line-of-sight links** must be maintained as possible; the **presence of cars** can introduce **multipath effects** to the signal and their impact on coverage and performance must be properly addressed.

Throughput

Taking into consideration the type of data that is exchanged in the iBorderCtrl platform (mainly text data with a few images/video), **an estimated minimum throughput to ensure trouble-free operation shall be in the order of 10 Mbps**. Assuming that typically no more than 10 border agents will use the iBorderCtrl Portable Unit simultaneously and considering the worst-case scenario, this corresponds to 1Mbps or better for each of them (at 100% usage duty cycle). The aforementioned values can be reassessed following tests under real conditions and can be guaranteed in terms of the radio network by employing good design practices as described below; the bottleneck in this case would be the backhaul connection (e.g. xDSL, LTE, satellite etc).

Latency

As iBorderCtrl is not a very strictly time-sensitive application, latencies in the order of **a few hundred millisecond shall be tolerated** without affecting the Quality of Experience (QoE) of the end user (i.e. the border agent). The radio network itself shall not be a bottleneck regarding latency, rather than again the backhaul connection.

Availability

The system shall ideally meet a **99,99% availability**. To achieve this, fail-over features have to be built-into the radio network, such as back-up APs to be enabled in case of failure. The exact number of APs to be used (active + redundant) is to be determined while deployment.

Security

As **sensitive data** are going to be exchanged over the air, **security features** must be implemented as described in the previous section. Also, the physical security of the equipment must be ensured.

4.3.1 Overall planning considerations

In order to meet the radio network performance criteria as defined above, the following **physical factors** come into play:

- The **network topology** (single- or multi-hop/mesh topologies) to achieve the required coverage
- The **location of the network's nodes**, i.e. APs
- The **antenna types** to use for each node
- The **height** at which each node is mounted
- The **channel selection** for each link
- The **transmit power** for each node

The above **physical factors cannot always be controlled**; the type of environment, in this case a **governmental site can** impose many **limitations on the actual deployment**. The existing infrastructure along with the demand for not placing equipment at designated areas can influence the network design significantly. As an example, there might be areas that no equipment shall be installed, areas where no power is available, physical security cannot be guaranteed etc.; also cosmetic implications might arise (i.e. the equipment must not be visible). Such limitations cannot usually be foreseen and shall be discussed and assessed in-situ during deployment. Finally, the network topology and location of APs can significantly affect cost; the installation of high towers for the APs can be very expensive, as well as the materials used. Preferably lower node heights should be selected (less than 5m from the ground) as they involve the use of lighter, less expensive mounting masts.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4.5 Performance Testing

In order to ensure maximum performance and availability of the network, thorough testing and benchmarking both before and after the deployment at the actual border sites is required. The key metrics of interest as well as the tools used to evaluate the performance are described in detail below.

[redacted]

4.5.1 Description of metrics and evaluation tools

Any actually deployed network will eventually be a compromise between cost and performance; access to network performance metrics is therefore a prerequisite in order to allow for further optimization and/or error troubleshooting.

When evaluating the performance of a network, two different approaches are to be considered; the first one is a qualitative approach, where the end-users assess their experience and satisfaction based merely on intuitive factors, i.e. how responsive their connection is, how fast the data exchanged seem to be etc. Obviously, this kind of assessment is subjective to the users' perception and cannot be considered as an accurate metric as it can often lead to misunderstandings or false judgement. To circumvent this, a more systematic approach, involving quantitative metrics is the preferred method for the performance evaluation.

The most important metrics used to evaluate any network are the following:

- Latency / Delay / Jitter
  - Processing delay
  - Queueing delay
  - Transmission delay
  - Propagation delay
- Bandwidth and throughput
- Coverage
- Capacity
- Utilization
- Packet Losses / Errors

The tools used to evaluate the performance of the network shall be open-source whenever possible to minimize costs as well as be well proven. Some of the tools to be used (to be amended):

- **Unix tools:** Iperf, Iptraf, Tcpdump, Wireshark, Netstat
- **Router/proprietary tools:** Mikrotik/WinBox tools
- **Radio Coverage Planning & Surveying tools**

[redacted]

[redacted]

[redacted]

[redacted]

5 Conclusions

Following the thorough technical descriptions of the different implementations, in regard to the separate modules to be integrated and form the final iBorderCtrl system, it should be noted that at the current stage, the iBorderCtrl consortium holds the early prototypes of each module -with limited functionalities as expected- and is in the position to start the integration process. The assessment conducted within this report, related to the fulfilment of initial requirements (as these have been handed over by D2.1 and D2.2) assures the successful realisation of the project and the acceptance by the end-users. The complete definition of the data flows and work flows, in a technical manner, enables the integration process to be initiated and run smoothly; the main milestone of this phase is this report to be used towards the creation of a minimum viable product, both in terms of hardware integration but also of software integration that will allow to identify technical interoperability problems and bugs early.