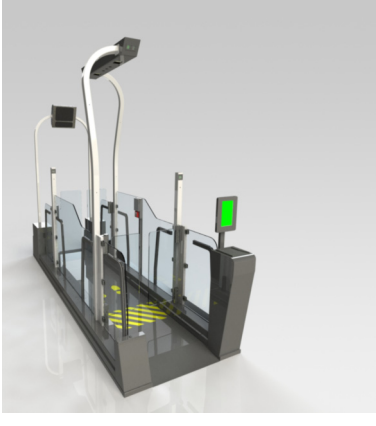
TECHNOLOGY • RESEARCH HIGHLIGHTS • VISIONS • SCIENCE

303

Recommendations for future ABC installations

Best practices

Sirra Toivonen & Heta Kojo (Editors)



VTT TECHNOLOGY 303

Recommendations for future ABC installations

Best practices

Sirra Toivonen & Heta Kojo (Editors)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312583.

ISBN 978-951-38-8559-5 (URL: http://www.vttresearch.com/impact/publications)

VTT Technology 303

ISSN-L 2242-1211
ISSN 2242-122X (Online)
http://urn.fi/URN:ISBN:978-951-38-8559-5

JULKAISIJA – UTGIVARE – PUBLISHER

Teknologian tutkimuskeskus VTT Oy
PL 1000 (Tekniikantie 4 A, Espoo)
02044 VTT
Puh. 020 722 111, faksi 020 722 7001

Teknologiska forskningscentralen VTT Ab
PB 1000 (Teknikvägen 4 A, Esbo)
FI-02044 VTT
Tfn +358 20 722 111, telefax +358 20 722 7001

VTT Technical Research Centre of Finland Ltd
P.O. Box 1000 (Tekniikantie 4 A, Espoo)
FI-02044 VTT, Finland
Tel. +358 20 722 111, fax +358 20 722 7001

Cover image: MAGNETIC Autocontrol and Gunnebo

Preface

Sirra Toivonen, VTT

Future border checks will rely on the availability of secure, smooth and fair processes. To reach these goals the border check concepts that are based on automation and traveller self-services have been promoted by EU, member states and Frontex. These automated border control systems (ABC) are based on traveller self-service, authentication of standardised machine readable travel documents and advanced biometric verification. European member states have already deployed several variants of ABC systems, and they have become something of a success story in recent years especially at airports, where they support the overall promotion of advanced automated processes in the service of businesses. However, many European member states are still reluctant to implement these systems for various reasons, which include security concerns, usability or human factors reasons or unsure business cases. Additionally, the successful transfer of these systems from airports to other types of borders has not been demonstrated in a large scale.

During recent years, the environment around international borders has evolved. The operational changes include the increasing passenger flows through border control points, tightened border security within the EU, new terrorist attacks that have influenced the security landscape and the increasing implementation of technology at border checks.

Despite the technological advances which the automated systems represent, the key challenge has been their ability to reach the efficiency goals. For smaller checkpoints, many of the solutions have been ineffective. Harmonisation of the travellers' user experience at various checkpoints has also been a key challenge, because it undoubtedly has affected the overall efficiency of ABC systems. This is important when considering that the travellers play a key role in defining the acceptability of the systems and determining the efficiency and the smoothness of the travel flows. Given the current challenges faced by automated border control system implementations outside the airport environment, it is not realistic to consider building them without serious consideration of harmonisation. Furthermore, it is necessary to derive approaches, develop technologies and handle the development comprehensively.

This report summarizes the results of the FastPass project, an EU research project aimed at providing solutions the rising challenges by developing a next generation reference system for Automated Border Control (ABC). FastPass started with the ambition to research and innovate the ABC concept from a new perspective. Putting the user in the centre of the developments, considering all aspects of social and legal implications and integrating the views of all involved stakeholders, FastPass settled the requirements of a next generation ABC system. New developments in the technology areas of passport scanning, biometrics, video surveillance and sensors enabled the designing of a reference architecture that can implement current and novel processes. This all includes new 2-step approaches for ABCs at airports, new solutions for cruise ships and a solution for land borders, where passengers can remain seated in their vehicle. All this was shown in demonstrations at Vienna International Airport, Piraeus Port, and the land border crossing point in Moravita. The results obtained were evaluated, and provided insights into the advantages and remedies of the targeted technologies and also some process solutions. This resulted in best practice guidelines as well as in blueprints for harmonised security assessment of ABC systems.

This document aims to provide a view to these FastPass project outcomes: its experiences, knowledge and research results obtained during the project. The aim is to provide recommendations from the experience gained in the project and to describe how the project achieved its goals. This document will look at the automated border control development and implementation with an interdisciplinary approach, taking into account the underlying factors as well as operational, technical, conceptual and organisational aspects to be addressed when developing automated systems for different borders**.** The aim is that this document will guide future development and implementation of ABC systems, and will initiate a European initiative for a global standard in ABC technology.

Furthermore, the possible upcoming introduction of the Smarter and Stronger Borders framework ([COM/2016/0194 final – 2016/0106 (COD)], including the proposals for an Entry/Exit system (EES) is aimed at promoting automated solutions while increasing security. Meanwhile, the biometric verification of third country nationals according to the Visa Information System (VIS) has become obligatory, introducing another additional technology aided task to the border checks. At the time of writing this report, the Smarter and Stronger Borders programme is still in under negotiations. This means that in this report exact recommendations that could be followed in the implementation of future EES compliant systems cannot be given. On the other hand, as FastPass has tested systems that go beyond the current e-Gate systems with kiosks, additional biometrics, pre-registration and registered traveller programs, it has provided a broad-minded view of the development and implementation of different future systems including options of registered traveller programs.

The purpose of this best practice report is to support the development of harmonised, secure and smooth automated border checks by addressing both current and future needs. Apart from the technical, operational and implementation guidelines it

includes valuable information on legal, political and social aspects of the development and implementation of automated border control.

The report approaches the issue pragmatically. We have tried to consider the relevant target readers by organising the document to follow the development process, and to start from mainly supporting information at the beginning of the document to detailed technical development information towards the end. In addition, each section has three main parts. First, some background information of the subject at hand is given. It is followed by scientific or project results. Finally, we provide recommendations concerning the definitive best practices, recommendations or guidelines based on the project results. The recommendations are presented in text boxes to simplify the reading process. Some of the recommendations provided in this report may seem apparent for the more experienced readers; however, it was decided to take a comprehensive perspective and to let the recommendations cover broadly the areas of design and implementation of automated control systems. The more profound scientific results are outlined on the projects web pages, https://www.fastpass-project.eu/dissemination.

As a whole, this report is organized as follows:

Section 1 **Introduction** with the sub-**sections FastPass – a pacemaker for innovative harmonised ABC solutions and FastPass ABC demonstrations for different border types provides an overview of the FastPass** project and its achievements in developing the novel border control technology and innovative ABC concepts.

Section 2 **Development of highly accepted ABCs solutions** examines the role of social, legal and political aspects that must be considered when implementing new technologies. It summarises the broad understanding of different drivers, which was gained as a part of requirements building.

Section 3 **Towards operational harmonisation of future automated border checks** examines the operational aspects of the ABC development process. It introduces the concepts of the different border types, the process of requirements management, and addresses privacy impact aspects, cost-benefit considerations and usability issues.

Section 4 **Technical aspects when implementing ABC** introduces the technical features necessary for automated e-Gate development. It presents several approaches for the development of future ABCs, such as built-in security, system modularity, biometric identification approaches, document authentication, and e-Gate hardware considerations for different border types.

Section 5 **ABC implementation project** presents the recommendations for an ABC running-in process, including training and acceptance testing. It presents the experiences gained during the different demonstration implementations and suggests recommendation based on the project's observations.

Finally, the Section **Conclusions** discusses the main attributes that a future ABC system is expected to have and provides some potential viewpoints of the future landscape considering the predictable development of the EU legislation and its possible impacts on ABC deployments.

With FastPass, this has been a 4-year journey of a 27-partner consortium to accomplish a tremendous amount of work. Without the ambition, enthusiasm, and diligence of so many people this result would not have been possible. Let us guide you through this journey of ABC research and present the world of FastPass. We hope that the following sections will provide insights, transfer knowledge and inspire the reader to envisage how border checks could be more efficient and effective with automated systems of the future.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312583.

Contents

Preface **3**

Acronyms and abbreviations **9**

1. Introduction **11**

1.1 FastPass – a pacemaker for innovative harmonised ABC solutions 11
1.2 FastPass ABC demonstrations for different border types 13
1.3 Best practices 18

2. Development of highly accepted ABCs solutions **20**

2.1 Success of ABC solutions 20
2.2 Engaging policy makers 23
2.3 Assessing the impact of a technology implementation 29
2.4 Legal requirements 31
2.5 Data protection impact assessment for ABC systems 37

3. Towards operational harmonisation of future automated border checks **41**

3.1 Stakeholder needs 41
3.2 Harmonised future border control processes 45
3.3 Harmonised ABC requirements engineering and management 50
3.4 Cost – benefit considerations for the development 54
3.5 Usability as a key success factor for ABC implementation 57
3.5.1 ABC usability – the traveller's point of view 58
3.5.2 ABC usability challenges from the border guard's point of view 63

4. Technical aspects when implementing ABC **67**

4.1 Modular architecture of an automated border control 67
4.2 High security solution 72
4.3 Technical considerations for ABC gate and housing hardware at different border types 76
4.4 Document authentication 84
4.5 Innovations in the biometric area 88
4.5.1 Fingerprint 88
4.5.2 Face 90

4.5.3 Iris 92
4.6 Innovations in the video surveillance area 94
4.7 Data fusion and alarming 95

5. ABC implementation project 97

5.1 ABC implementation recommendation 97
5.2 Training as a part of the implementation project 99
5.3 End user acceptance testing 101

6. Conclusions 105

Acknowledgements 109

References 110

Appendices

Appendix A: Legal Instruments
Appendix B: Partners of the FastPass -project

Abstract

Acronyms and abbreviations

ABC	Automated Border Control
BA	Basic authentication
BAC	Basic access control
BDF	Biometric data fusion
BG	Border Guard
CBA	Cost Benefit Assessment/Analysis
CSCA	Country signing certification authority
DG	data group of the RFID chip
DPIA	Data Protection Impact Assessment
DS	Document signer
EAC	Extended access control
EAN	European Article Number
EES	Entry-Exit system
EU	European Union
EU/EEA/CH	European Union/European Economic Area/Switzerland
eID	Electronic identity document
eMRTD	Electronic machine readable travel document
ETIAS	European Travel Information and Authorisation System
EU	European Union
FPA	FastPass Architecture
GDPR	General Data Protection Regulation
GUI	Graphical User Interface

IATA	The International Air Transport Association
ICAO	International Civil Aviation Organisation
ID	Identity document
IPI	Invisible personal information
IR	Infrared
ISPS	International Ship and Port Facility Security
ITF	Interleaved Two of Five
MRZ	Machine readable zone
nPKD	National public key directory
OCR	Optical character recognition
PA	Passive authentication
PACE	Password Authenticated Connection Establishment
BCP	Border Crossing Point
PIA	Privacy Impact Assessment
PKD	Public key directory
RFID	Radio-frequency identification
RTP	Registered Traveller Programme
SAC	Supplemental access control
SBC	Schengen Borders Code
SST	Self-service technology
TCN	Third Country National
TR	Technical Guideline
UV	Ultraviolet
UX	User Experience
VIZ	Visual inspection zone

1. Introduction

1.1 FastPass – a pacemaker for innovative harmonised ABC solutions

Sirra Toivonen, VTT

This Best Practice report summarises the practical findings related to ABC implementation of the FastPass-project (run between 2013 and 2017). The project accumulated 27 partners with different expertise to develop and demonstrate novel harmonised automated border control systems. More specifically, FastPass designed a system which facilitates border crossing of travellers by automating the process, while respecting the laws concerning Schengen external border control, as well as the fundamental rights of the travellers. The main objectives of FastPass are presented in Figure 1.

The main approaches in the effort were user-centric design, an innovative approach to technical and conceptual challenges and contextual awareness with demonstration the ideas with pilots in different border types. Harmonisation of the ABC designs between various border type implementations is a key solution to this problem.

From the beginning of the project, it was clear that many challenges must be considered and met in full:

- The border control process must comply with European values and policies, despite increasing passenger flows.
- User-centred design must be followed in order to ensure a smooth, fast and secure border crossing.
- Different user characteristics should be carefully considered in order to guarantee the acceptability and availability of as many user groups as possible.
- The existing processes and infrastructures must be reflected and supported.
- The solutions should consider the current security challenges of border checks and ensure that the technology implementation and new solutions enhance security.

- The growing importance of the ethical and social aspects must be recognized in the development.
- The solution should be European, contributing to standardizing and harmonizing attempts and providing commercial opportunities for manufacturers and integrators.

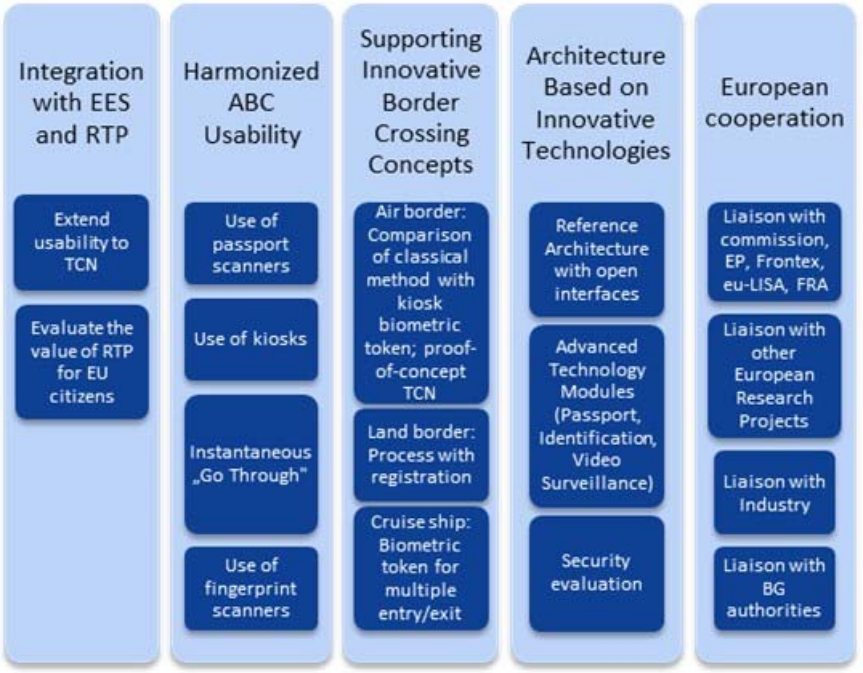


Figure 1. Summary of the FastPass Objectives [Clabian 2016].

The automated border control (ABC) system is usually an upgrade or a complement to an existing border control arrangement. Therefore, the ABC system must adapt and integrate to the different infrastructures and models. It must be possible to integrate it into the physical environments, as well as to different control procedures and modes of operation: from the controlled air border environment to the outside environment of the land border. As each border type has its own specific requirements, one system does not fit all the different border types. FastPass has made the effort to design and to adapt the solutions to the operational and environmental differences in all borders in order to enhance harmonisation efforts.

The FastPass solution is based on innovative modules that can be standardized across Europe using the experiences of the test installations. The demonstrated solution provides opportunities to enhance travellers' seamless and fast border transit through a harmonized user-experience for different (land, sea and air) border control points across Europe and enables border guards to maintain strict control

that is both unobtrusive and convenient to navigate. One of the aims of this report is to discuss the technical design and standards and open them in order to allow manufacturers to promote an open standard. The design will provide border control authorities with a standard, proven design with module options, thus providing possibilities for reducing design, specification and procurement time. This will likewise present manufacturers and integrators with a design which is simple, fast and cheaper to build and adjust into different border types and which is easy for customers to understand.

As a summary, the following general objectives guided the FastPass work towards the innovative approach to provide new features for customers (border police forces) and users (travellers):

- "Efficient border management": assisting border guards with instant availability of information, risk assessment, intuitive interfaces, and efficient control – maximizing the time a border guard can assess border crossing eligibility. Additionally, the system should be easy to use.
- "Privacy preserving solution": a European solution emphasizing the user's interest of control over data.
- "Faster border crossing": reduced transaction times in an on-the-move solution, trying to minimize waiting times for the passenger.
- "Next generation biometric identification": towards the integration of multiple biometrics, modular/open design, higher quality, increased identification accuracy, less rejections at the e-Gate.
- "Extensible approach towards a paperless process": modularity throughout the entire system design, extensibility and open architecture supporting our vision of a paperless air travel process at check in/security/boarding in the future.
- "Security evaluated approach": a thorough risk analysis of the proposed approach, careful selection of interfaces, protected and secure infrastructure.

1.2 FastPass ABC demonstrations for different border types

FastPass demonstrated the research results in operational demonstrations at three different border types (Figure 2). The automated border check solutions were adapted to each border type and end user requirements and were in operational use for a defined period. The demonstrations served for validating the FastPass objectives for ABC solutions, i.e. maintaining border security at the highest possible level while increasing the speed and comfort for all legitimate travellers at border control points. This was accomplished by the establishment and demonstration of a harmonized, modular approach for Automated Border Control system and by working out an ABC reference architecture. The work contained several air border scenarios, a cruise-ship scenario, and a land border scenario with travellers remaining

in their vehicles. In order to reach the set objectives for the system performance, next-generation sensors and novel frameworks, software and algorithms were developed. In the following, the demonstrations are introduced on a general level.

Figure 2. FastPass was operationally demonstrated at three border crossing points. Snapshots of the demonstration installations in their real environments.

The different environments cause challenges to the harmonized implementation because the border types have versatile different requirements to be solved. For inside solutions, the environmental factors are easier to handle than for the road e-Gate

outside. As the solutions greatly rely on the functionalities of the facial recognition it poses extra high requirement to the functioning and reliability of that system.

The FastPass e-Gates were integrated to the three different port/facility infrastructures, so that they enable easy installation with as little as possible assembly work. The traveller profiles were studied and the demonstrated solutions were planned in order to allow the majority of the travellers to use the systems.

The automated border check systems and self-service lines should be located so that they are attractive, visible and easy to find, and all demos tried to fulfil the requirement despite the existing permanent infrastructure.

AIR BORDER

In Vienna, the demonstration included three different operational stages where a normal all in one installation integrated e-Gate and an e-Gate with a kiosk process were operational for a prolonged period and RTP-tested in operational mode. The tests were performed for entry checks next to the manual gates. It should be noted that all demonstrations were executed with two e-Gates from two different manufacturers. The aim of using two different gates and switching between configuration stages was to develop harmonisation principles, test new technologies and processes and to compare the outcomes of different stages against project objectives.

In the demonstration installations, the consent procedures were needed for data protection purposes. In practice, after selecting the language and accepting the declaration of consent concerning data storage and the terms and conditions, required document checks and face recognition take place. Thereafter the person search and document search are initiated. In some predefined cases, e.g. if the traveller is not eligible to use the ABC, the traveller is sent to the manual border control.

In the first stage of the demonstration, the 1-step process, the enrolment process by passport reader takes place directly at the entry side of the gate. This process resembles a process that is often seen at installed ABC installations. Different workflows were already tested in this stage. In addition, the novel facial recognition system with the on the move identification concept was implemented.

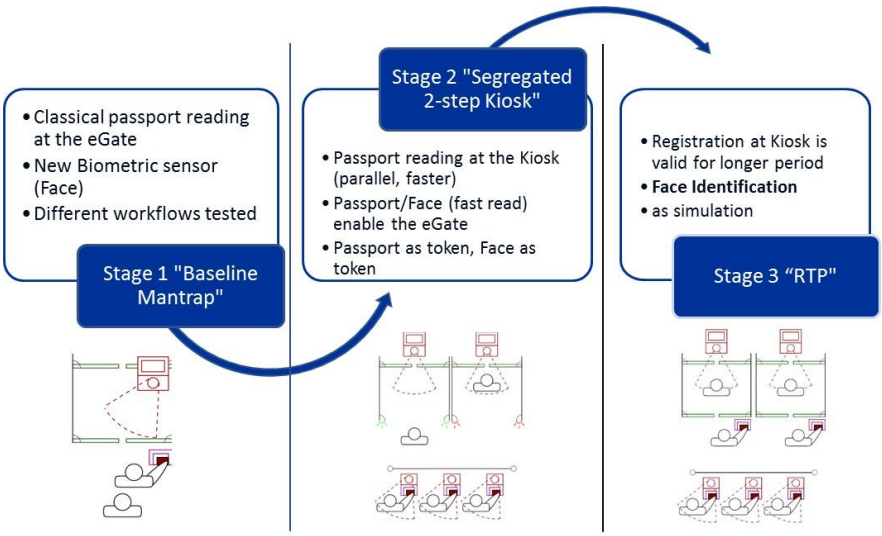


Figure 3. Air border operational modes at different stages of FastPass demonstration, along with the key operational and technical principles.

The second stage used a 2-step process in which the enrolment process takes place in separate kiosks. The demonstration was performed with four kiosks. After the language selection and consent processes, the kiosk enrolment includes document authentication and facial verification. If these are accepted, the traveller is guided to the e-Gate. For entering the e-Gate a traveller needs his/her passport as a token. After entering the e-Gate, face recognition and single person detection are carried out. In case of any abnormality, e.g. a person search hit, the border guard is requested to open the e-Gate via the border guard interface and a manual border control can subsequently be carried out. Additionally, the border guard can request manual inspection of any traveller at any time according to his/her judgement.

The third stage was performed as a simulation, which meant that it did not serve as a real border crossing. This stage simulated an RTP (NFP) program and a situation in which the registration would be valid for a longer time. It also included an option for a face as a token, which simulated a paperless process.

LAND BORDER

As the first of its kind, the FastPass land border ABC provided the opportunity for travellers to remain seated in their vehicles while passing the self-service border check. For the land border, the e-Gate was installed beside the normal border check lines for exit checks. In addition to person identity verification, this also included checking of the vehicle-related documentation. The check also allowed for multiple

persons in the vehicle to be checked simultaneously. For registered frequent travellers, the land border ABC has proved to be relatively smooth, convenient and time-saving.

The land border solutions also included the enrolment process at a separate kiosk. In addition to travel document authentication and facial verification, the vehicle documents are also enrolled. The enrolment data is also saved for future use, which enables direct use of the e-Gate for returning vehicles and travellers. The e-Gate solution is explained in more detail in Section 4.3 Technical considerations for ABC gate and housing hardware at different border types.

SEA BORDER

The FastPass sea border objective was to provide an approach to enhance the border security at seaports by maintaining almost the same level of convenience and smooth processes for cruise passengers. In addition, in the case of the sea border ABC, the FastPass solution led the way with a prototype for cruise ships. The test included operation at the exit check. The solutions were modified and customised from the air border solutions. The registration phase took place in kiosks inside the cruise ship and the border check was performed with on-the-move facial recognition at the e-Gate process in the terminal.

Thanks to FastPass, the port operators and border authorities are expecting to improve border control processes with limited resources, without causing any delay to cruise ship passengers. Further, one expected impact is the implementation of a unique One Stop Point Control (OSPC) for security and border control (SBC), without any delay but still satisfying the International Ship and Port Facility Security (ISPS) Code.

E-GATE MONITORING

In all of the three demonstration sites, the border guard interface allows supervision of the traveller enrolment at the Kiosks and e-Gates passage. The border guard has a user interface with which the passenger data can be followed, in a booth behind the air border gate, mobile for the sea border, and a monitoring room for the land border. At the air border, the system was also compatible with the existing information systems, so that the border guard could perform the background checks through the ABC system. In general, all the demonstrated e-Gate solutions could be adjusted to allow both entry and exit operation. The border guard is supported in his decision concerning a manual border control by a variety of data offered by the border guard interface, e.g. personal data, document data, results of face recognition, document checks, person search, document search, single person detection, as well as video surveillance. Via the border guard interface the Kiosks and e-Gates may also be administered, e.g. doors can be opened and closed.

Although the main purpose of ABC gates is to facilitate border crossings for legitimate travellers, there is also a clear need to prevent illegal border crossing.

Moreover, should such an unauthorised act occur despite all counter measures, it should at least be monitored and properly followed-up. The handling of unclear travellers during the different steps of the process varies according to the process defined by the border guard authority. Based on the analysis of vulnerabilities that could be exploited for illegal border crossing, design of the systems for the individual border types has taken into account appropriate protective measures. On the other hand, there are certain FastPass innovations that already significantly reduce the likelihood of certain vulnerabilities. The 2-step approach is an example of this, as it allows for a better early warning about certain risk profiles.

Biometric data quality (face, fingerprints, and iris) is the most crucial aspect for authentication based on biometrics. This emphasizes the importance of successful management of all quality decreasing factors. The project has made a particular effort to improve the quality of biometric recognition, including biometric sample quality. The system should provide acceptable availability performance over its entire life cycle and be future-proofed by the possibility of integration with the Smart Borders initiative.

1.3 Best practices

Sirra Toivonen, VTT

This report provides recommendations to design, deliver and implement automated border control systems based on the four years of research and months of practical demonstrations at air, land and sea border checkpoints. As all the demonstrations handled real passengers and furthermore the air border demonstration was operational, the project provided much new information and many experiences of different aspects of ABC implementation and development.

As a guideline for the reader it must be stated that the analyses, assessments, proposals and recommendations should to be seen in the context with which they are connected, but they are formulated in a way that they may well be applicable to other BCPs and other solutions in the border area, and beyond.

In this report, we mainly provide recommendations. The definitions for recommendations and best practices adopted by the Schengen Evaluation Committee's report/Working Party on Schengen Evaluation [Commission Recommendations of 06/XI/2006] are also followed in this report:

- Recommendation: a non-exhaustive series of measures, which should make it possible to establish a basis for the correct application and monitoring of the Schengen acquis.
- Best practice: a non-exhaustive set of working methods or model measures, which must be considered as the optimal application of the Schengen acquis, it being understood that several best practices are possible for each specific part of Schengen cooperation.

The aim is not to repeat the already given and updated recommendations or to evaluate their validity, but to share the experience obtained during the project from versatile viewpoints ranging from political viewpoints and binding legal requirements to actual experiences in the field in the three demonstrations that were carried out.

The automated border control has already been promoted for some years, and in order to reinforce its usage quite a few guidelines are available for the design and implementation. The legal regulation provides the framework under which the self-service concepts operate (e.g. Schengen border code [EU 2016/399 2016], more references in Appendix A), and guidance in its implementation has been given (e.g. Handbook [Commission Recommendations of 06/XI/2006]). Especially Frontex has had an influence on the increasing number of ABC implementations in the EU. Already in 2012, Frontex published guidelines for ABC implementation, and in 2015 the Best Practice Operational Guidelines for Automated Border Control (ABC) [Frontex 2015a] and the Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems [Frontex 2015b]) were updated. In 2016, Frontex also contributed to enlarging the group of travellers eligible to use the e-Gates by publishing Guidelines for Processing of Third-Country Nationals through Automated Border Control [Frontex 2016]. Frontex stays active in this field, and new common procurement guidelines for ABC solutions are expected this year (2017). On the other hand, the airports have shown considerable interest in automated systems throughout the ABC development period. This is because they see clear benefits of ABC implementation in the forms of security enhancement and traveller facilitation [Passenger facilitation 2017], and also infrastructure usage. Last year IATA also published a guide especially focused on the ABC implementation project: Automated border control implementation guide [Automated border control implementation guide 2015]. In addition, some individual countries have published guidelines. [Canadian Transportation Agency 2015]

This document is aimed at all experts and practitioners developing or using ABCs or ABC-related technologies, or who plan to implement them in the near future. Furthermore, it can to be used for updating knowledge related to passenger processes. The report provides a wide perspective on the policy and legal issues as well as acceptable system design. The aim has been that this report would serve stakeholders from various backgrounds, e.g. the technology developers, traveller interaction and process designers, implementers and policy makers.

2. Development of highly accepted ABCs solutions

Section 2 provides background information and recommendations for developing highly accepted systems that are in compliance with the current legislative framework. The first section “Success of ABC solutions” provides general criteria of the aspects which a successful ABC must confirm. It does not go into details but tries to provide a general view of the aspects that lead to a successful implementation. The section “Engaging policy makers” elaborates the research on the political viewpoints of the ABC development and implementation in the context of shared competence in border security and control issues between the EU and Member States. “Assessing the impact of a technology implementation” concentrates more on the societal side and presents the research results from assessing the impact a technology implementation might have on a society. “

Legal requirements” discusses the legal framework, legislation and regulations that must be fulfilled by the systems and their implementation. Finally, “Data protection impact assessment for ABC systems” discusses the privacy impact assessment methodology developed for ABC implementation. Some of the recommendations presented in this section may overlap, but as they are derived from a different viewpoint they are individually presented.

2.1 Success of ABC solutions

Sirra Toivonen, VTT

Border security and smooth border crossings are important public services. Travelling, and external border crossings in particular are increasing considerably. Efficiency and cost-effectiveness of border checks is of the utmost importance. Uncertainties of the global economy, austerity and increasing pressures on the national economies challenge the ability of most states to maintain their current level of public services. They are also important factors in the governments' economic austerity policy toolbox. Austerity forces governments to introduce more efficiency in border control; less border guards have to manage more passengers.

The development of a sound business case, which clearly identifies the key objectives of the implementation, should be the starting point for any ABC deployment. The Frontex guidelines [Frontex 2015a] make a note that political drivers can have a dramatic impact on the Business Case. Thus, a successful concept can provide a clear line of arguments in order to convince decision makers and select among available offers from the market. It also states that once the Business Case for the system is clearly defined, it is possible to begin defining how and where the system should be deployed. On the other hand, it must always be remembered that social acceptance and trust are key factors for the successful deployment of biometric solutions, including ABC technologies. The high-level success criteria have been established by carefully analysing the input received from the end-user interaction and the demonstrations (land, sea and air border scenarios) in the FastPass project.

In general, characterising a project or implementation as successful or failed is a very difficult task. The perception related to the success or failure of a project may also depend on time. The project is generally considered as an overall success if it meets the technical performance specifications and/or fulfils the mission to be performed, and if there is a high level of satisfaction concerning the outcome among: key people in the end user organization, key people in the project team, and key users or clients of the project effort.

This section summarises success criteria from a high-level perspective and it will not go into specific detail. The objective here is to increase thinking about the variety of the criteria having an effect on the implementation success and to provide a consistent and comprehensive perspective. The objective has been to identify the main criteria that are fundamental or of the utmost importance to the success of an automated system, this model is presented below (Figure 4).

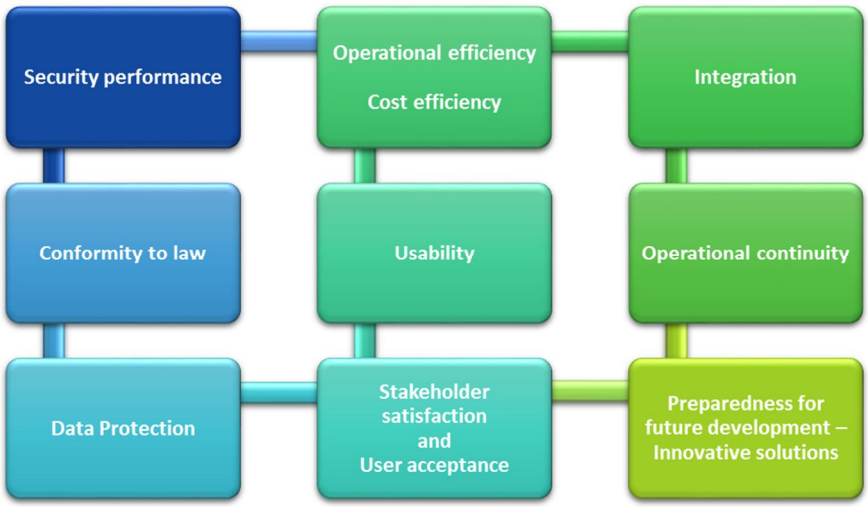


Figure 4. Automated border control system success criteria.

Security performance. Performance of the system and its components has high accuracy. The system provides increased security with high accuracy biometric matching (e.g. face match), including high quality ePassport authentication. The system functions in different environmental conditions.

Conformity with the law. This criterion means that the developed FastPass system is in compliance with the current regulatory regime in Europe and the European Union. It also means that the system has accordance with the specific national laws of the member states where the demonstrations will take place: Austria, Greece and Romania. The system is in compliance with the Schengen Borders Code. One example of this could be that of providing physical structures of the system maintaining physical separation of Schengen and non-Schengen passenger flows inside the terminal building. The system will also satisfy the recommendations and guidelines made by Frontex concerning border checks and automated border control.

Data Protection. The data design must take note of privacy and data protection principles and legislation. The Assessment is based on privacy and data protection principles and regulations. These principles aim to ensure: the minimisation of access to data based on the need to know principle: the proportionality between the amount of information collected and retained and the objective of the system; the safekeeping of the data collected and differential access control; the minimisation of negative outcomes in case of data breach; the monitoring of activities performed on data with the most appropriate granularity (keeping of records). The system processes traveller personal details in a secure manner.

Stakeholder satisfaction and user acceptance. Achieving a satisfactory traveller experience is the key for the success of an implementation. This includes more awareness and coaching of travellers before their arrival at the e-Gate, and ensuring that the ABC systems provide a user-friendly service, including a more comfortable, less intimidating immigration process. The system supports the use of pre-registered details of travellers. Acceptance of the ABC system by border guards is crucial for its successful operation, as is the carrier satisfaction. Greater harmonisation should help achieve a better traveller experience and encourage more people to use ABC.

Usability. Assessment is based on the ease of use of the system or the option proposed for all end-users including border guards, competent authorities and travellers. The system should be simple, intuitive and fast.

Operational efficiency. The system supports the effective use of resources in the border crossing processes. It accommodates growth in border crossing numbers without increasing the number of border guard staff, and provides the necessary capacity for effective border checks. The system supports the efficient use of space and resources with more streamlined processes, including reductions in missed connections due to immigration processing delays. It is applicable in servicing travellers crossing the border with different means of transportation. System design provides modularity and avoids complexity that would hinder updates and maintenance of the system throughout its demonstration and lifecycle.

Time effectiveness is crucial for the success of an ABC system. A smooth border checking process that does not exceed the duration of an equivalent manual procedure is important for the acceptance of users. A shorter processing time than the status quo can increase the throughput of border controls. This is valuable for border control authorities because they can concentrate their capacity to the checking of persons with higher risks. For infrastructure providers such as airports or sea ports, the higher throughput results in less space needed for the facilities.

Integration. The system is integrated to the other relevant border control processes of the border crossing point and provides easy integration with the existing infrastructure. The system is integrated to the records and databases of both national and international border control.

Operational continuity. Availability performance of the system is ensured with the focus on the reliability and maintainability performance of the system parts. Service is guaranteed for the system with the responsibilities defined for different actors. Component selections support the optimised and predictable lifecycle costs of the system. The cost effectiveness takes into consideration both investment and lifecycle operational costs such as software, hardware, communication, network, HR and maintenance alongside long term returns on any investments made.

Preparedness for future development – Innovative solutions. The system design proposes modularity that supports updates throughout its lifecycle. The system demonstrates the selected areas of the Smart Borders package.

As a summary, the conformity with the law and with data protection are considered as priorities. Cost efficiency has been identified as a comprehensive, essential criterion that must be taken into account throughout the development. The cost factor would be very important if building an industrial customer-ready product, although the costs are not defined very precisely to be a success factor in the FastPass project and have been given only minor priority in the analysis.

2.2 Engaging policy makers

Pinja Lehtonen, Pami Aalto, UTA

Maegan Hendow, ICMPD

RESEARCH DESIGN

European and national level legislation influence the overall design of and expectations set for the implementation of ABC systems in the EU area. Because the competence in border security and control issues is shared between the EU and Member States, such laws are actively discussed in the European institutions including the European Parliament and the parliaments of Member States. Therefore, the actors developing and implementing ABC systems need to be aware of the views of political stakeholders and the requirements they have for EU-wide harmonisation of ABC.

FastPass examined and compared systematically the views of 44 political stakeholders with the help of Q methodology. The group of participants was carefully selected and primarily drawn from the parliaments (Figure 5). The work sought to establish which political preferences and expectations drive the development of ABC systems, the extent to which they unite or divide the Member States, and consequently, what types of political objections or reservations may be ahead. Since ABC technologies are part of the functioning of society, and since national parliaments generally decide on the funds for commissioning ABC systems, operators and developers ignoring the views of political stakeholders take a very high risk.

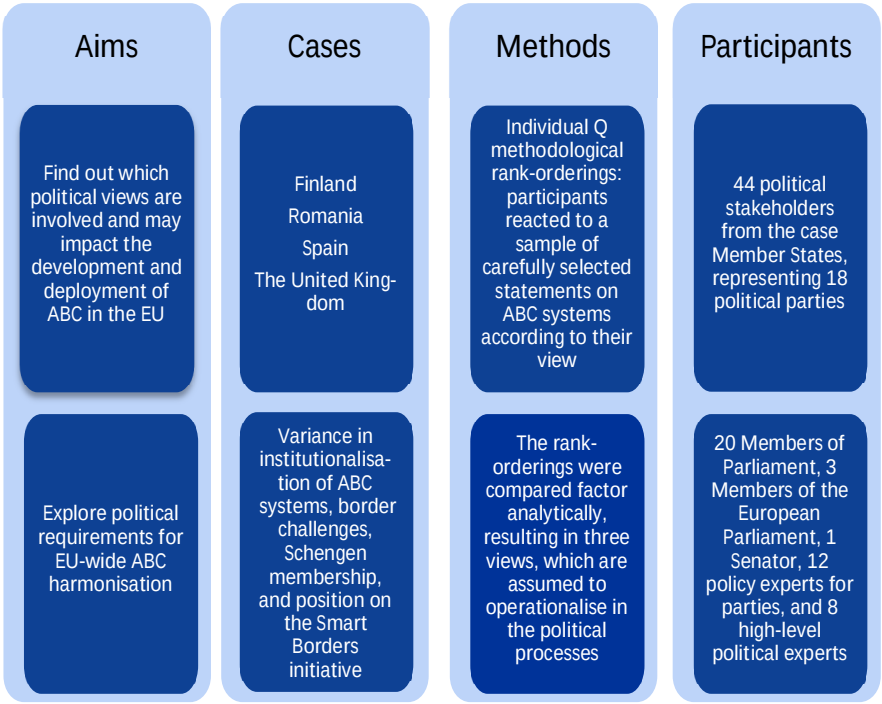


Figure 5. Summary of research design with political stakeholders.

In addition, an empirical research was conducted through semi-structured qualitative interviews with stakeholders at the European Union level, in Romania, Portugal and Austria, as well as in two non-EU contexts (the United States and Hong Kong) in order to examine best practices and lessons learned in developing ABC systems within and outside the EU context. Interviews were conducted with policy makers, as well as with social and ethical stakeholders, particularly those advocating and/or involved in the policy development process. In total, 66 interviews were conducted, 48 of which were with EU or Member State stakeholders. These interviews aimed at collecting stakeholder views with regard to ABC systems. The knowledge gained

from these interviews was used not only in case study development and the analysis of the Smart Borders proposal (an initiative often referred to by EU and Member State interviewees), but it also fed into the development of the requirements of the FastPass system.

FINDINGS

Three 'Views' and five points of consensus emerged from the Q methodological analysis conducted with political stakeholders from Finland, Romania, Spain and the UK. We now describe those and elaborate further, how they align with the findings of the semi-structured interviews with other EU and Member State stakeholders.

1. **Privacy and fundamental rights** view, explaining 24% of the variation among the individual rank-orderings: Left, social democrat and green party participants report suspicions of ABC and Smart Borders eroding the privacy of the travellers. Possibilities of data misuse and function creep evoke reservations. Therefore, in the view of this group, data use should be strictly limited to the monitoring of border crossing. A strong legal regulation of ABC and Smart Borders is demanded due to their implications for fundamental rights. ABC's risk profiling and fingerprinting Third Country Nationals for Smart Borders are seen as potentially discriminatory practices. The just treatment of asylum seekers is required as a part of the ABC design.

   This was also a strong finding among interviewed stakeholders. Stakeholders of this group tended to have stronger opinions about the broader use of technology in border control systems or for border management policy objectives, rather than on ABC technology specifically (although there are still relevant objections). Interviewees emphasised the fallibility of technology, where for example false positives, interference ('skimming') and forgeries can undermine the reliability and trust in the system. They also highlighted privacy and data protection concerns related to system set-up and data breaches, as well as different cultures of privacy – both across different European countries (for example comparing approaches in the UK and in Germany) or with non-European countries. Other highlighted fundamental rights issues related to child protection (for example unaccompanied minors), discrimination and access to remedy.

2. **ABC-positive security and integration View,** explaining 17%: Right and centre-right party stakeholders see ABC as a means of enhancing security and European integration. Harmonisation of ABC is required, together with a risk profiling based ABC solution. Risk profiling is seen beneficial for security, as it would allow border guards to concentrate on threats that are more direct. This makes ABC a worthwhile investment. Use of biometric data is encouraged but it should be transparent. Collecting biometric data

in EU-wide databases for ABC and sharing these with law enforcement authorities represents welcome European security integration. Legal integration should proceed from the creation of a legal base for EU border control.

This was also a strong opinion amid interviewed stakeholders. Semi-structured interviews emphasised the consistency and security of ABCs, particularly with potential future biometric systems currently under development and (at the time of research) under consideration in the Smart Borders proposal package. ABC is considered non-intrusive, and is argued as a potential means to improve certain fundamental rights protections such as privacy (by for example preventing identity theft and the usage of fraudulent identity documents) and non-discrimination (limiting ethnic profiling through automatic processing). In addition, policy makers emphasised the economic and practical benefits of using ABC systems, where they are viewed as increasing throughput at border crossing points in view of increasing future passenger numbers and limited border management personnel budgets. For those stakeholders who held an ABC-positive view, this was emphasised more so than their arguments regarding increased data protection and privacy aspects.

3. **Anti-immigration Eurosceptic View,** explaining 9%: Far-right populist party members plead the 'people' being rightfully concerned about increasing immigration and governmental surveillance. The data protection systems of some Member States are suspected of not being reliable. National sovereignty is claimed in organising border control practices. Harmonising ABC does not cause enthusiasm, but land and sea ABC solutions are encouraged to halt irregular immigration. The argumentation is not always concise, which is typical of populist versatility; e.g. transparency in data use is demanded while encouraging hidden surveillance of passengers.

   This view was not elicited in any of the in-depth semi-structured interviews, yet these interviews did not set out to explicitly include policy makers with a Eurosceptic background as compared to the Q analysis target group.

Consensus across the Views

The political stakeholders participating in the Q methodological research converged on five issues. They all required accessibility for disabled passengers, data minimisation, transparency in biometrics use, as well as legal instruments and monitoring mechanisms for EU-wide IT-systems in border control, and democratic legitimacy of ABC prior to proceeding with it (Figure 6). This consensus is important as it may serve as a politically sustainable starting point for developing and harmonising ABC systems on the EU level.

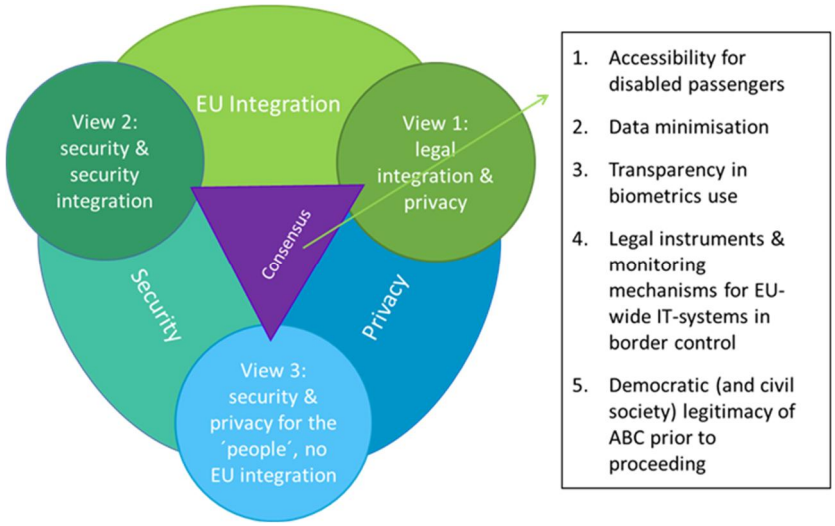


Figure 6. Three political views found. Their main differences and shared goals/consensus.

Lessons learned from the Hong Kong case analysis

Several best practices have been highlighted by the research in Hong Kong, which has implemented ABC extensively at border crossing points since 2004. The cultural and societal approach to ABC (and technology in general) in Hong Kong differs significantly from the European context, and the ABC gates used in Hong Kong are of the registered type, which are waning in usage in the EU. Nonetheless, there are still important lessons they have gleaned from the policy development process that can be taken up in the development of ABC systems in the EU in the future. In particular, three key lessons have been identified:

1. Management of the full identity chain and linkage of electronic identity document development to the ABC solution development has allowed assessing where biometric systems can be developed and processes strengthened. Strategic planning of multiple systems from the beginning strengthens the future usage and acceptability of the systems.
2. Involvement of all relevant stakeholders, from the beginning and continuously, based on specific requests has supported a smooth implementation process. Co-ownership by non-border management stakeholders has allowed for a smoother implementation process, while engagement with non-traditional users (for example visually impaired persons) suggests a transparent and open process that is flexible to the needs of its citizens.
3. Expansion of ABC to new users (for example non-Hong Kong residents) is considered as an important priority of the future, in order to further improve control point throughput and traveller experience (of visitors).

Based on the analyses of the political aspects of ABC, we recommend the following:

Biometric data use in ABC

- The data minimisation principle must be followed when compiling biometric information from passengers.
- Biometric data compiled by means of ABC must not be used for any other purposes than border control.
- Security-maximising ABC solutions with multiple biometrics should be avoided, as they are highly unlikely to constitute a politically acceptable basis for harmonised ABC within the EU.
- Passengers must be informed transparently and efficiently on the purposes of the use of their personal data. The design of the passengers' user interface must provide adequate information.

Political legitimacy

- Decisions on EU-wide harmonisation of ABC must be made democratically to gain democratic legitimacy. Due political processes, including discussions and decisions in national parliaments, must result in a legal basis for ABC. Note that Euro scepticism may significantly complicate the efforts of harmonisation.
- Accessibility for disabled passengers must be addressed in the design of ABC: universal design principles should be followed because accessibility represents a fundamental rights principle shared by the politicians and policy makers.
- Political stakeholders should be informed on the development of harmonisation solutions to help them formulate their positions for forthcoming political debates. We expect significant numbers of undecided political stakeholders; informing them would most likely improve the prospects of EU-wide harmonisation.

Strategic policy development

- Policy makers should engage non-traditional and non-border management stakeholders in the process at an early stage. This ensures co-ownership and increased acceptance of the developed system or policy, as important alternative views are taken into account from the beginning and integrated into the policy and system.al

2.3 Assessing the impact of a technology implementation

Benjamin Taylor, Sirra Toivonen, VTT

Recent shifts in EU and national policies towards greater automation in border check processes mean that it is important to assess what kind of impacts such changes might have on end-users and other stakeholders. The widespread implementation of automated systems is expected to reduce costs for border authorities and increase throughput of travellers, but as yet it is difficult to assess what negative impacts might be borne by societies in general.

During the FastPass project, research was performed which developed a set of criteria to be used for assessing the impact a technology implementation might have on a society [Taylor 2016]. The research utilised Q methodology and involved reviews of previous projects on topics such as Privacy Impact Assessments (PIAs), Surveillance Impact Assessments, Societal Impact Assessments (SIAs), and Technology Impact Assessments (TIAs), as well as reviewing literature to identify important criteria. Once the criteria had been identified, they were presented to 25 stakeholders mainly from professionals working in areas of technology, law, ethics, border control, research, or a combination of these. Respondents were asked to rank these criteria in order of agreement. However, they were also forced to rank the criteria against each other, that is, they had to choose whether Criteria A was more important to them than Criteria B, C or D.

The research aimed at discovering how many, and what kind of groupings exist in terms of important aspects to consider when assessing border control technology. The results indicate that three main groupings exist: Technologists, Humanists, and Concerned Pragmatists, with the remaining not falling into any of the categories. The first and largest group (about 60% of the respondents) was called the “Technologists” due to their focus on issues relating to the specific functioning of the technology, such as ensuring that it performs the required tasks adequately, usability and security while issues of negative impact on jobs, effects on social cohesion, and impacts on third countries were ranked low. The second group was called the “Humanists” (16%), due to their focus on social and legal issues such as potential hazards to society, proportionality and necessity and effects on social cohesion. This second group ranked lowest issues of ensuring new technologies are adequately cost-assessed, easily upgradeable, and usability. The third group, “Concerned Pragmatists” (16%), were a mix of the first two. They focused on issues of technology such as dependability, but had also social and ethical concerns such as rights to good administration, non-discrimination, and impacts on jobs, while they ranked lowest issues of consent, preventing against misuse, and ensuring the technology is the best available option and has been tested adequately.

During the research, one particular criterion received an overwhelmingly negative result. This criterion was related to the concept of responsible technology development and was formed as a statement, which suggested that technology developers are the best actors to ensure their products are compatible with existing laws and ethical norms from conception to the final stages of production and implementation.

The feedback received on this particular criterion was overwhelmingly that technology developers could not be trusted to design technology that conforms to legal and ethical norms without the involvement of external actors. On the one hand, this statement is inherently true: the best place to ensure ethical and legal compatibility with a technology is during the design and development process, and thus the best actor to ensure this happens are the developers themselves. However, on the other hand this statement could be understood as suggesting that technology developers should be able to set the legal and ethical agenda themselves, without external oversight.

In reality, this result reminds and reinforces us to keep in mind that there is a mistrust of technology and those who develop it, especially when questions of social impacts and ethics are raised. It also reminds us that in order to safeguard acceptability it is important to ensure that technology is developed in transparent ways, and interaction with end users is promoted. However, and perhaps more importantly, it also reinforces that external actors should be involved in providing the assessments of new technology. A number of other results of the research point to similar conclusions. For example, ensuring that data is protected according to regulations, and that the technology conforms to relevant health and safety, environmental, and technical standards and regulations were ranked high.

In order to ensure that the implementation of new technologies is acceptable in the eyes of society and to ensure ethical, legal and technical conformity to relevant norms, laws, standards and certifications it is necessary that the technology itself is assessed from multiple perspectives. This is a process, which could be performed throughout the development and implementation stages, by external actors using impact assessment methodologies, which aim to provide guidance to the developer. Ideally, this is a process, also promoted by recent initiatives such as the push towards Responsible Research and Innovation and the focus on public engagement that developers perform by themselves, with engagement with appropriate balance of relevant stakeholders.

Based on the research results we propose a number of recommendations:

- New and developing technologies should be assessed for impacts on societies from social, ethical and legal compatibility and perspectives throughout the technology lifecycle, from conception, design development through to implementation and even beyond and utilize feedback loops to improve the acceptability of the technology.
- Stakeholders engaged should include different groups (Technologists, Humanists and Pragmatists) in order to guarantee broad viewpoints.
- By developing technology in a responsible manner, there is a greater likelihood that it will meet the needs and expectations of stakeholders.

2.4 Legal requirements

Diana Dimitrova, Els Kindt KUL

The operation of technologies for border control in the EU, such as innovative ABC solutions, needs to comply with the applicable EU legal framework. In the EU, the applicable legal framework for such technologies is composed of several Schengen and data protection instruments[1]. At present there are no specific EU laws which regulate the operation and usage of ABC as such and which lay down lex specialis data protection provisions for ABC technologies. In FastPass, this "legal vacuum" raised questions about the application of the above-mentioned instruments to the different ABC technologies and solutions. Thus, an important part of the legal research work focused on producing legal requirements and recommendations for the ABC development and implementation in the EU/Schengen with a view of complying with the existing legal framework. While the recommendations were created in the framework of the FastPass ABC scenarios and concepts, they can be equally addressed to national and European lawmakers as well as at Border Guard Authorities who (intend to) operate ABC technologies. The recommendations, as derived from the main legal instruments, are briefly summarised in this chapter, focusing on ABC in general and not on particular ABC solutions or architectures. The decision-making process on ABC should follow the steps outlined below:

NECESSITY AND PROPORTIONALITY

The decision-making process should start with the necessity and proportionality consideration:

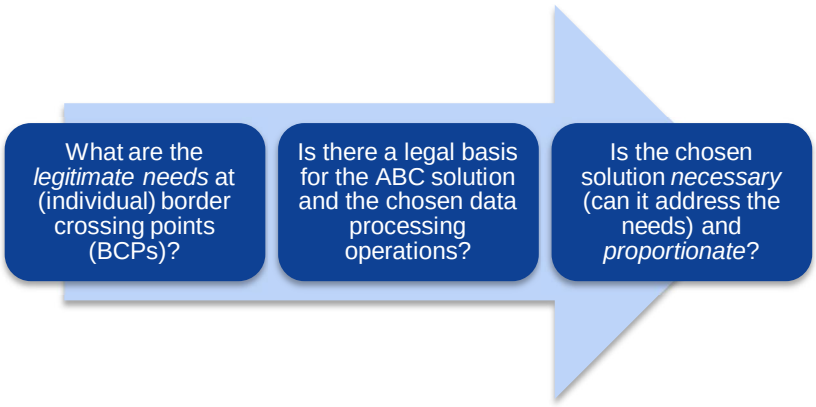


Figure 7. Necessity and proportionality consideration.

[1] Check Annex I on the main legal instruments applicable to ABC in the EU/Schengen.

Clarification: The requirements above can be traced back to Article 8 of the European Convention on Human Rights (ECHR) and Articles 7, 8, and 52 (1) of the Charter of Fundamental Rights of the European Union (CFREU)) and they establish privacy and data protection as fundamental rights. They have to be complied with as ABC technologies have at their heart personal data processing operations. Automation should not turn into an aim in itself but come as a response to an actual and legitimate need experienced at a particular border or BCP. This need should be translated into clearly formulated purposes of ABC. For example, if the purpose is to increase effectiveness, one should clarify if this means higher throughput in general or faster process for the individual passengers, etc. The other question is whether ABC can effectively achieve the purpose and in the case of more purposes – if they are compatible with each other. ABC should not be merely "useful," "reasonable" or "desirable."[European Court of Human Rights 1976] It should be demonstrated that the legitimate aims could not be achieved otherwise. Such a necessity assessment should be made also when deciding on the individual components/architecture of ABC e.g., whether it is necessary to set up a central database with personal data such as biometric data or have tokens in the possession of passengers themselves.

If necessity is demonstrated, the decision-makers should check if the chosen solution fulfils the proportionality requirement, i.e. whether the objectives cannot be achieved through less intrusive means, e.g. through technologies that involve fewer risks for illegitimate storage and further re-use of data, etc. Like necessity, proportionality is to be applied also in the consideration of the individual ABC elements.

Most importantly, ABC should have a basis in law which is accessible to ABC users and in which the processing and restrictions on the processing of their personal data is foreseen, including safeguards. *It would be best if the safeguards were harmonised on EU level to allow for equal level of protection of the passengers' fundamental rights, in particular the rights to privacy and data protection.* In addition, as will be discussed further below, there should be clear policies allowing passengers to exercise their data protection rights, i.e. of information about the processing of their data, access to it, rectification, erasure blocking and objection to processing.

COMPLIANCE WITH THE SCHENGEN BORDERS CODE

When ABC technologies are used, they should perform the checks stemming from the Schengen Borders Code (SBC), in particular Article 8 thereof. The checks vary, depending on whether a passenger belongs to one of the main passenger groups: EU/EEA/CH and Third Country National (TCN) who can be residence permit-holders, TCN visa holders, TCN visa exempt or local border crossing permit holders.[2] The former are subject only to a "minimum check," while the latter – to a thorough one. Some TCNs, e.g. those who are family members of EU/EEA/CH, are subject also only to a minimum check. The major requirements are presented in Figure 8.

[2] Other groups such as passengers with diplomatic passports, seamen, etc., were not examined separately.

The details of the check can be found in the SBC and for brevity purposes, the figure below is a very basic outline. *An important observation is that ABC technologies may not create additional check, even if these could be technically easy to implement, e.g. record the entry and exit records of EU/EEA/CH when there is no legal basis for such a record.*

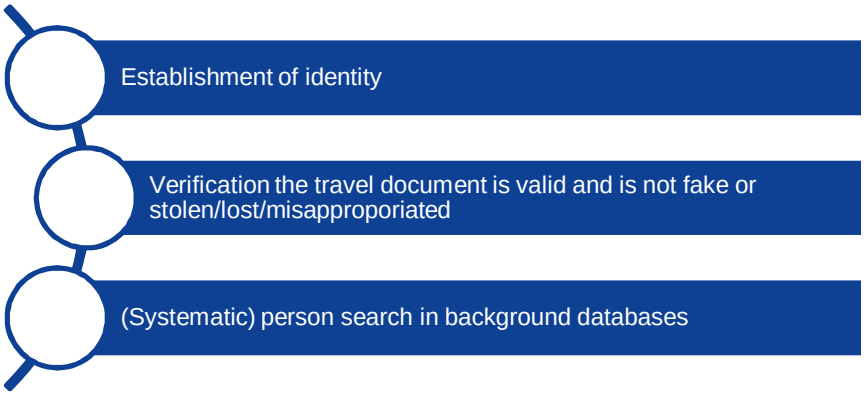


Figure 8. Common checks on all passengers pursuant to Article 8 Schengen Borders Code. Additional checks apply to TCN passengers, e.g. interview of the TCNs, stamping, visa and residence permit checks pursuant to Article 8 SBC.

It is expected that in the future a new category of passengers would be created, namely those TCNs who would visit the EU for a short stay and who would be subject to the Entry-Exit System (EES) [COM/2016/0194 final – 2016/0106 (COD)].

This would also create new processes, which will have to be observed, e.g. enrolment and storing of alphanumeric and biometric data on an EU-wide database, including the entry and exit records of the concerned passengers. Other possible new entry requirements could be created by the ETIAS proposal, e.g. checking whether a TCN visa-exempt has been granted the authorisation to enter the EU [COM/2016/731 final].

The envisaged ABC process and data flow should be carefully described because automation could introduce some differences to the manual process. For example, unlike the one-step manual process, in two-step ABC solutions, where data are sent from an enrolment kiosk to an e-Gate, the operators should know and document which data is processed where, when, how, why and to which other components of the technology it is sent. It is also important that all data for whose storage there is no legal basis is deleted from all parts of the system that processed them. Keeping track of this “data flow” and the operations performed on the data is important not only for compliance with the data protection provisions, but also for ensuring that all the checks as prescribed by the SBC have been started and completed and no additional checks have been performed. Documenting these details is essential for the transparency and accountability of the process and for maintaining its proper functioning.

Other requirements should also be observed, namely separate lines for the different passengers, i.e. having ABC for EU/EEA/CH and for TCNs, which might need to be functionally different.

COMPLIANCE WITH FUNDAMENTAL RIGHTS TO PRIVACY AND DATA PROTECTION

Any personal data processing must be in compliance with the fundamental rights, in particular to privacy and data protection[3] and with the provisions on data protection as prescribed in Directive 95/46/EC and its replacement, i.e. Regulation 2016/679 (GDPR) that will become applicable in May 2018[4]. It is important to note that also Directive 2016/680 on data processing in the law-enforcement sector is applicable as some of the border checks are performed for law-enforcement purposes, e.g. checking whether a passenger is a wanted criminal, e.g. in SIS II and national databases. Further data protection provisions can be found in instruments such as SIS II, VIS and the proposed EES and ETIAS.

The main data protection provisions and principles are set out in the table below. These provisions aim to ensure that the personal data is processed fairly and lawfully and that there are mechanisms for ensuring that passengers can exercise their rights. This seeks to avoid the negative consequences for the integrity of the border checks, e.g. occurrence to false acceptances, and for the passengers, e.g. their entry is denied because of false rejections or false hits against SIS II. Identifying the fundamental rights risks, esp. in terms of data protection, defining and implementing adequate measures to address these risks is essential for ensuring a data protection compliant technology solution.

Finally, the automated decisions taken by ABC technologies should be reviewable by Border Guards, i.e. these should be in a position to examine the results of the check, handle problematic cases and overrule ABC decisions if necessary. [Frontex 2015a]

[3] Articles 7 and 8 CFREU and Article 8 ECHR

[4] These were identified as the applicable data protection instruments as the processing of personal data for border control purposes is an administrative and not a criminal law task, except for searches in the SIS II on wanted individuals and stolen/lost objects, which are subject to Framework Decision 2008/977/JHA, to be replaced by Directive 2016/680 as of May 2018.

Table 1. Data Protection Requirements derived from Directive 95/46/EC and the General Data Protection Regulation.

Principle/ requirement	Application to ABC
Legal basis	For ABC in general and for the individual data processing operations carried out by it (e.g. consent, legal obligation of the controller).
Purpose limitation	Specify narrowly the purposes of the ABC and of *each data processing operation*. Ensure that the data are not re-used for incompatible purposes.
Data minimisation	Select the minimum data necessary for carrying out the border check depending on the requirements for the different passenger groups as per SBC. For example, if the check can be reliably performed with one biometric identifier, other identifiers should not be added.
Data accuracy	It entails accurate (biometric) enrolment and matching to avoid false acceptances and/or rejections. This would play a role in deciding whether 1:n searches instead of 1:1 verifications could be equally reliable. It includes also the accurate processing of alphanumeric data, e.g. reading and matching of the passport data for the background database searches.
Data storage	Unless there is legal basis with safeguards (e.g. on an entry-exit system), personal data may not be stored after a passenger has exited the gate.
Data security	It should be ensured that no one will illegally access and further process the data or the data is lost or tampered with.
Right to information	Passengers should be informed in a transparent manner of the data processing operations of the ABC technology, e.g. purposes of the processing and categories of data, their rights and the complaint mechanisms available.
Right of access	Passengers may at any time request to know if any data has been stored on them and if yes, which ones.
Right of rectification	Passengers should have the right to have data concerning them rectified if it is incorrect, e.g. correct their name on an RTP.
Right to blocking	This means that data is not processed (but not deleted either) if its accuracy is contested or the passenger needs it for legal claims, e.g. to prove that it was illegally stored.
Right to deletion	If a certain piece of data was stored illegally e.g., an illegal database was created of the biometric data of all ABC users, then the data should be deleted.
Right to object	The use of ABC should be voluntary.
Accountability	ABC controllers should implement a data management plan, documenting the data processing operations and performing regular audits.
Data Protection Impact Assessment Art.35 GDPR	It should be carried out before introducing ABC. The purpose is to identify the risks for the passengers and define mitigation measures.

The design and implementation of ABC in the EU should comply with the legal regulation of the border control processes in the EU. It should also respect the EU privacy and data protection requirements to avoid the risks related to new border control technologies.

Phrased broadly, the major recommendations for ABC are:

- Ensure that all ABC carries out all checks on the different passenger groups as prescribed by the Schengen Borders Code and ABC does not create additional checks. This includes also providing for separate ABC lanes for the different passenger categories.
- Operate ABC under a clear legal basis.
- Clearly specify the legitimate purposes of ABC, i.e. the real needs it has to meet.
- Assess the necessity of having ABC solutions in general and individual BCPs.
- Assess the proportionality of the chosen solution.
- Detail clearly the process and data flow.
- Operate the chosen solution and its data processing operations in compliance with the principles of purpose limitation, data minimisation, data accuracy, storage and security.
- Carry out the Data Protection Impact Assessment and update it regularly.
- Set up and implement privacy and data protection policies with the aim of
  1) Ensuring the security and confidentiality of the data,
  2) Informing ABC users of the processing operations to be performed on their data, the controller of their data and the other rights they enjoy under Directive 95/46/EC and the GDPR as of May 2018,
  3) Allowing ABC users to exercise these data protection rights, i.e. the right to access to their data, to have their data rectified, erased or blocked, and possible recourse to the respective data protection authorities and judicial remedies.
- Systematically check the EU and national legal frameworks for amendments and adapt the ABC technology accordingly.

2.5 Data protection impact assessment for ABC systems

Günter Schumacher, JRC

A NEW OBLIGATION

As any other system in which personal data is processed, an ABC system has to comply with the relevant data protection legislation. According to the new General Data Protection Regulation [EU 2016/679] (GDPR), this implies – among other obligations for the data controller – the conduct of a so-called Data Protection Impact Assessment (DPIA). This will become compulsory as of May 2018 for all new ABC deployments, with yet unclear implication for older installations. There have been other types of impact assessment around that could be applied to an ABC system, in particular

- Privacy Impact Assessment
- Ethical Impact Assessment

If at all, these impact assessments have been conducted on a voluntary basis, with no legal requirement from the older data protection legislation, despite the undisputable value in conducting them. None of them has been adopted for the GDPR. The actually introduced concept of the DPIA comprises of the following elements (according to GDPR, Article 35, paragraph 7):

a) "a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects (…); and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data (…) taking into account the rights and legitimate interests of data subjects and other persons concerned."

Despite the universal applicability of fundamental rights (pursuant to the Charter of Fundamental Rights), it is interesting to note that the reference to "rights and freedoms of the data subjects" coincides with certain obligations arising from the Schengen Borders Code25 (SBC). Its Article 3a emphasises the respect of those "rights and freedoms": *"(…) Member States shall act in full compliance with relevant Union law, including the Charter of Fundamental Rights of the European Union (…)"*. Apart from that, particular fundamental rights are in addition explicitly mentioned in SBC, such as human dignity (Article 6(1)) and non-discrimination (Article 6(2)).

Thus, it is even more important to focus with the conduct of a DPIA not only on data protection and privacy (as just two particular fundamental rights), but more broadly on all those rights concerned. FastPass took therefore the position to consider an ABC system as "monolithic data processing apparatus" that cannot be decoupled for the purpose of a DPIA into data processing and non-data processing parts. A traveller needs to accept the impact of the whole system in order to have his/her data processed and compared to his/her (biometric) appearance. Thus, all elements of the ABC system (whether directly linked to data or indirectly in the mentioned sense) have to be explored with respect to a potential negative impact on fundamental rights.

ESSENCE OF THE ANALYSIS

The GDPR suggests that a DPIA shall be conducted "prior to the processing" (Article 35(1)). Ideally, this should happen already prior or during the design phase in order to decide at the earliest point in time on appropriate mitigation measures should the DPIA reveal relevant risks. With this focus on proper design (similar to the privacy-by-design principle), the scope of considerations of a DPIA for ABC has been structured along the following three major categories, derived from the relevant fundamental rights:

- Design for Privacy and Data Protection: This category covers all aspects directly related to the disclosure and processing of personal data (passport data, biometric information) in relation to third parties (other travellers or unauthorised persons). In particular, the data protection principles of data minimisation, purpose limitation, retention limitation and the rights to appeal have to be addressed.
- Design for Inclusion: This category covers all aspects that potentially impose discrimination on any ground (e.g., disabilities). It also covers the treatment of minors and children because there could be (and actually are) limitations in the usage of ABC due to age.
- Design for Dignity: This category covers such aspects as intimidation (harassment), exposure of disabilities, health or safety risks, but also the right to effective remedy. The latter is in particular important in case of system failures. Inappropriate reactions to failures could harm the dignity of the concerned traveller.

Under each category, all relevant aspects of the planned system shall be examined that is associated to a certain risk. Does the design prevent such risks per se, or does it on the contrary induce such risks?

THE DPIA CONCEPT

Following some examples of existing DPIAs for other sectors, FastPass proposed a 7-step approach that encompasses all the required elements of the GDPR. These steps provide the basis for a structured dialog with all involved stakeholder:

Step 1: Mission statement and legal basis for the DPIA: Agreement has to be achieved what the DPIA should cover and how the results are used. Most importantly, the DPIA shall assess the risks to the rights and freedoms of travellers when passing through an ABC. The purpose of the DPIA is to allow review by the proper data protection authorities and other relevant fora.

Step 2: Organisational provisions: It needs to be organised who shall conduct the DPIA, either a dedicated team inside the operator's organisation, or through an independent third party (preferably). Similarly, reviewing of the DPIA report needs to be organised.

Step 3: Description of ABC processes: The system boundaries need to be defined, along with the precise description of the processes, actors and the data involved. Preferably, data flow diagrams shall illustrate the presence and usage of the data.

Step 4: Risks to fundamental rights: Risk management will be applied according to ISO 31000 [ISO 31000:2009]. According to that, the management process is composed of the elements risk assessment (analysis and evaluation), risk treatment and risk acceptance. Risk assessment will be structured according to the three categories "design of privacy and data protection", "design for inclusion", and "design for dignity". For each category, a catalogue of questions need to be developed and answered that should reveal the level of risk and its prioritisation.

Step 5: Risk Mitigation: For each identified risk, an appropriate mitigation strategy needs to be defined. This strategy usually follows any of the four generic options "modification", "avoidance", "retention", or "sharing"

Step 6: Documentation: The performance of the DPIA following the phases identified above should be appropriately documented and its results presented in the final DPIA report.

Step 7: Review process: The purpose of this phase is to ensure that the execution of the DPIA is carried out properly.

DPIA goes along with a certain governance concept that involves the national supervisory authorities as well as the newly established European Data Protection Board. As a first step, the FastPass partners involved in the development of the DPIA approach aim to promote this approach to the relevant association of data controllers (e.g., the ABC working group coordinated by the FRONTEX European agency).

FASTPASS PROOF OF CONCEPT

FastPass not only developed and proposed the DPIA approach described before, but also demonstrated its usefulness. The involved risk management process was combined with a parallel security analysis that revealed about 100 threats and vulnerabilities. Those relevant for the DPIA have been further complemented with a catalogue of risk associated to the three categories explained before. In total, a catalogue of about 55 risks to fundamental rights was evolved, that were discussed and assessed with respect to their impact and potential mitigation.

The application of the new DPIA approach to the FastPass system successfully demonstrated the value of such a concept. Future developments can benefit from the additional insights into risks, impacts and potential mitigation actions. For the future, the proposed DPIA approach should be further maintained and revised by the relevant ABC community, with the involvement of the European Data Protection Board. It may help to harmonise the usage of ABC across Europe in contemplation of fully respect privacy, data protection, inclusion and dignity of travellers.

As a recommendation, the Data Protection Impact Assessment (DPIA) should:

- Be a comprehensive reflection about the fundamental rights implication of using an ABC system
- Use a method of structured dialogue with the stakeholders involved
- Use a structured, systematic method that is well documented.

3. Towards operational harmonisation of future automated border checks

Harmonisation and optimisation aims at ensuring that all passengers have similar experiences at different border crossings. This is said to speed up the processes significantly and give the passengers the feeling of comfort and security, while enhancing the acceptability of the ABC gates at the same time. Process harmonisation and optimisation is to ensure its efficiency and proper management of all resources (people, technology).

3.1 Stakeholder needs

Sirra Toivonen, VTT

Minna Jokela, FBG

Automated Border Control (ABC) has been introduced already on quite a few major airports handling Schengen external traffic. The aim of the FastPass end User needs gathering challenge was to combine the stakeholder needs from various stakeholders from different environments and to collect an analysis for the development of the harmonised border control system that would be well accepted and beneficial to all the partakers of the automated border checks. The main stakeholders having the most interest and influence on the usage of the ABCs were defined as being: 1) Border controlling authorities in Europe; 2) Travellers; 3) regulators and community and 4) Other stakeholders including the airport operators and other authorities etc. (Figure 9)

It is important to take account the experiences already gained of the automated solutions that have been used. Thus, on those that have pioneered the development and implementation of ABCs at different locations. The stakeholder analysis can be performed different ways. A good way to do it is to analyse the operations in real environments and to involve the stakeholders in gathering the needs, analysis of the requirements and planning the solutions. The border controlling authorities have the key responsibility of the border security and traveller flows including the focus on core processes of the checks in the particular checkpoint. They pose the technical and operational objectives and requirements with respect to the main building

blocks of the system (e.g. input/output of the processes, participating actors, roles and organizational units), used technologies, it-systems and hardware, interoperability, services, tasks (manual, users, system tasks) and information exchange. When the stakeholder needs are analysed and prioritized, the whole life cycle of the system should be considered: e.g. from acquisition, deployment, operation and support, to decommission phases. In most cases the border authority organization is also the owner of the system but also other possible ways of ownership are possible. The ownership may cause effects that have to be considered in the prioritization of the needs. Sometimes the stakeholders at a checkpoint can have viewpoints of the main needs for the automation of the border; for the border authorities, security is always prioritized but again for the other stakeholders e.g. the infrastructure operators the speed of the flow is a key performance indicator.

In order to better structure the prioritization, the border authority needs were structured according to their role in the organisation to strategic, operative, tactical and technical levels. For harmonisation perspectives also the different checkpoint operational environments; terminal, outside 8no-terminal) and mobile, must be considered.

The automation is a self-service from the traveller point of view, which means that the taking into account the traveller needs has a key role in the success of the systems. The acceptability, throughput and effectiveness finally define the success of the system. If travellers do not accept the system, the goals will not be reached. The traveller needs gathering should guarantee a good level of acceptability, efficiency and optimized throughput. Needs and requirements analysis should focus on the on operational considerations including human factors and usability, harmonisation, flexibility and robustness, user acceptance and guidance needs, and adaptability in the three types of borders considered in the project. The travellers value especially speed, smoothness of the border check and positive user experience with the self-service technologies.

As already mentioned there are also other stakeholders that need to be considered when planning the new systems. These include airport operators and other authorities, airline companies, etc. These stakeholders have profound experiences among other things on the traveller flow management, customer services and risk mitigation measures. They are especially interested to of systems that support their main duties and businesses. It is beneficial to gather the needs and new ideas for the system development, interoperability and harmonization from them. The point of views of the technical stakeholders and developers are also important in order to understand the possibilities, limitations and current practices better.

Bearing in mind that the project pursued to introduced the harmonised concept for the automated border control solution the interviews were carried out in a number of European countries and the interviews included all the above-mentioned stakeholder groups. In addition to the mentioned, stakeholders, the regulators' and social community viewpoints as well as the legal analysis outcome are presented in the following chapters of this report.

As already mentioned, when developing harmonized systems on the European level, the stakeholder needs analysis need to be comprehensive enough to be able

to model the needs extensively and to discover the main issues from the possible noise. At each of the environment, the prioritization of needs may differ and that have to be considered carefully when the analysis is further developed to requirements. Many of the needs interact closely with other needs and often in a contrary way. If we take the example of the speed of the border crossing that may be in a relation to the passenger need related to usability but may have great implications to the security of the system if not considered carefully. At all times it must be kept in mind that the system must fulfil the profound security requirements of border checks at external Schengen borders.

The following categorization for the stakeholder needs was defined, and it served as the baseline for the system requirements.

1. ABC system is designed to support officers' decision-making and guarantee high level of security performance. This includes efficient border officer operating environment and user interface for ABC. Process development supports security and smooth flows of travellers.
2. ABC is well accepted by traveller groups. Traveller interaction is effective, usability supports process fluency and assisted with instructions and guidance
3. Technical functions: Chip and passport reading functionality and features; Fingerprint process functionalities and features; Liveness detection; Face capture functionalities and features; Data transfer and management; The physical (gate) design effectively supports the security performance and the fluent user experience; Implementation of modular design; Adequate security characteristics of the token
4. Availability performance of the system is ensured by careful consideration of the reliability and maintainability aspects related to the system parts. Component selections supports efficient lifecycle management of the ABC system.
5. Smart Borders compliance and future proof system.

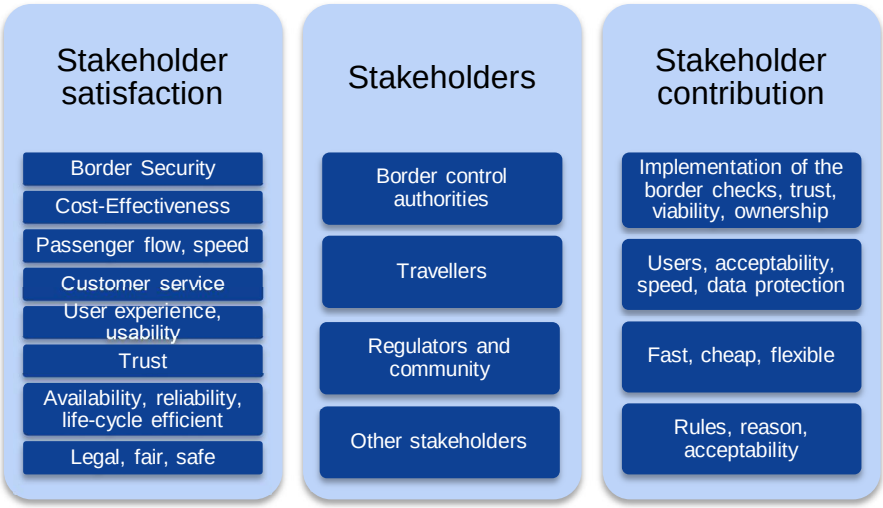


Figure 9. Stakeholder needs analysis.

Recommendations related to stakeholder needs analysis

- The user needs and stakeholder analysis related to the harmonised automated border control systems need to engage sufficient stakeholder groups in the work, take a, at both times a broad view to the stakeholders' needs but dig deep enough to understand their profound needs.
- The analysis should state the interests of stakeholders in relation to automated border checks, including the stakeholders that will be directly affected or could affect the outcome and the potential conflicts of interest.
- The needs must be interpreted so that also room for the technical innovations is left open. In FastPass the end user needs gathering was made very detailed though in the requirements stage some of them were transformed to a more general because the research wanted to provide comprehensive harmonised requirements for automated border checks at different locations and in different system configurations. If the development only address one location the user needs can be developed into technical requirements in a more straightforward manner.

3.2 Harmonised future border control processes

Piotr Gmitrowicz, Lukasz Szklarski, ITTI

Since the border control faces increasing efficiency requirements throughout Europe on key point to reach these demands is to enhance harmonisation of the automated border control processes and experiences. It has been noted in many instances that the traveller plays a key role when the total throughput is concerned and harmonised and congruent traveller experiences play a key role.

Cambridge dictionary defines harmonisation as the act of making systems or laws the same or similar in different companies, countries, etc. so that they can work together more easily [Cambridge dictionary]. Generally, harmonisation can be defined as "actions or processes that through matching and blending bring about agreement, reconciliation or standardisation". Harmonisation implies a high level of mutuality among the involved parties, regardless of different affiliations and viewpoints. Yet another definition indicates that harmonisation means the "adjustment of differences and inconsistencies among different measurements, methods, procedures, schedules, specifications, or systems to make them uniform or mutually compatible" [BusinessDirectory].

In order to guarantee best outcome while harmonising processes it is important to take onto account the process optimisation and current best practices point of views. Border authorities with ABC experiences have contributed to the Frontex best practices work. Harmonisation and optimisation can also serve for the identification of bottlenecks, which affect the smoothness of transaction and identification of process steps' weak points that may confuse and eventually deter travellers from using ABC gates. Through harmonisation, also the acceptability of the ABC gates can be enhanced. When border checks are concerned different countries, different processes, technologies and traveller profiles must be considered. Instructions such as how to place a passport during document verification or how to behave during biometric identification have great impact on the process duration and correctness.

The purpose of the harmonisation and optimisation is to ensure that passengers have similar experiences at different border crossings. This will speed up the processes significantly and will give passengers a secure and comfortable feeling, while also enhancing the acceptability of the ABC gates. Another reason of harmonisation and optimisation is to ensure process's efficiency and proper management of all resources (e.g. people and technology).

In FastPass, the project took the challenge to harmonise and optimise processes for different border crossing types, air, sea and land in locations where no automated process has been used. Processes for travellers and border guards have been designed in accordance to the guidelines from Schengen Border Code and Frontex publications relating to ABC implementation and TCNs processing. The results of harmonisation indicate that all process aspects (= different stages and elements of border crossing process), regardless of their differences, allow achieving a common goal in the efficient way. As it occurs, the results of harmonisation and

optimisation of automated border control processes show that the total harmonisation (unification) is not possible due to the specific conditions of different borders border. On the other hand, even though the processes and technologies differ it is possible to develop solutions where the most important criterion, the traveller perspective, is adequately harmonised and the processes look similar among all border crossing points from travellers' perspective. Harmonised processes offer the travellers the possibility to familiarise themselves with border crossing procedures and act in a similar way at any crossing point.

Harmonised processes also offer the border authorities the possibility to develop solutions to different border checkpoint, facilitate standardisation of equipment, processes and working practices, and consequently reduce life cycle costs. For optimised outcome, ABC lines need to be constantly monitored by border guards responsible for the process flow supervision and traveller assistance.

In the following tables, border guards' and travellers' perspectives on automated border check processes designed for air, sea and road borders are presented. In Table 2 an enrolment in a registered traveller program (RTP) is required and in Table 3 an e-Gate process harmonisation recommendation at different border type installations is presented. In the process harmonisation also the land border process has been taken into account with addition steps of vehicle related document check phases. In FastPass, these processes were included in the registration phase. It must be notified that in general the enrolment may be required every time a traveller crosses the border or on certain time intervals. After the enrolment the traveller may proceed to the e-Gate process or he/she may also take a manual control. It must be notified that if consents from travellers are required these phases must be included in the processes.

Table 2. Summarisation of harmonised enrolment process from traveller and border guard perspectives.

ENROLMENT PROCESS	
Traveller	**Border guard**
Traveller approaches the Kiosk	The border guard supervises the process and verify that the one person at a time is using the Kiosk
Travellers chooses the language of the operation	
Accepts consent	
The Traveller inserts the ID/passport to the Kiosk	
	Border guard initiates the background searches for EU citizens. TCN searches are made automatically.
(if driver, land border) the traveller steps out of the car to use the enrolment Kiosk	
The traveller looks into the camera for facial recognition and acquisition or put his fingers on the scanner	Border guard verifies the procedure.
The traveller takes the travel document back	
(if driver, land border) the traveller scans the registration certificate, then takes it back	
(if driver, land border) the traveller scans driving licence, then takes it back	The border guard verifies if the right person is in the vehicle.
(if driver, land border) the traveller scans green card, then takes it back	
(if driver) the traveller returns to the vehicle	
(if driver) the traveller approaches the e-Gate	
The traveller proceeds to the e-Gate	

Table 3. Summarisation of harmonised e-Gate process from traveller and border guard perspectives.

E-GATE PROCESS		
Traveller	**Traveller (if driver, land border)**	**Border guard**
Traveller approaches the e-Gate	The car drives to ABC lane	The border guard supervise the process
Traveller enters the e-Gate	The driver opens the window	
The traveller inserts the ID/passport to the document reader	The driver inserts the ID/passport to the document reader	The border guard verifies that the right person is in the car
The traveller removes the ID/passport from the document reader	Driver takes the travel document back	
The travellers looks into the camera to provide their biometrics (face)	Driver provides face according to instructions shown on the terminal	The border guard checks whether face matching was successful
		The border guard opens exit barrier and let the vehicle leave the e-Gate
The traveller leaves the e-Gate	The driver leaves the e-Gate	

An additional aspect to the harmonisation of processes may be presented from the airport where border check processes are in the heart of the airport process in general in multi-stakeholder environment. In this environment, the results of the modelling and process development work show the importance of distinguishing the processes of different stakeholders from each other and to developing the border checks in cooperation with other stakeholders. At the airports in general, the processes differ according to the passengers' origins, nationality and country of the departure or the destination. From the process harmonisation point of view, the difficulty of the transfer passengers often lies in the fact that the various processes at the airport are different for the passengers depending on their route before the arrival (e.g. country of departure) and their destination. Processes for the travellers whose destination is inside Schengen or EU are different from the processes for travellers with destination outside EU. Furthermore, states that are non-Schengen but EU or Schengen but not EU have their own processes. The customs authority is also very integrated to the airport process.

It's essential to identify potential risks for every step of the process. The risks concerning ABCs could be of dual nature: IT-related or User-related. The risk analysis focuses on raising awareness and addresses the issue of the threats at an early stage of the development and implementation of an ABC system (security by design).

Recommendations related to process optimisation

Traveller perspective:

- Traveller's awareness and education before the e-Gate: when drafting ABC processes for travellers one must take into account means to increase passengers' general awareness of automated border control and availability of self-service alternatives. Information should be consistent at all types of borders.
- Traveller's awareness and education at the e-Gate: since e-Gate installation vary, it's essential to ensure that travellers are well guided throughout the process. Details on usability are presented in the chapter 4.5.

Border guard perspective:

- Schengen Border Code (SBC) instructions set the basic process requirements that must be followed.
- Rules requires (where circumstances allow) separate lanes to be provided. This recommendation has been taken into account when harmonising the processes for different border types. There needs to be a separate lane for self-services and registered passengers to use for their convenience. Such solution is bound to increase passengers' safety and overall security at ABC gates.
- Border guards should have full control over the process and should be able to interfere at any time on the suspicion of any inconsistencies. This is essential as border guard's intuition still plays a significant role in detecting any attempts
- Border guards should be well trained and manual lines need to be available. This influences the rapid uptake of any innovation, especially the one directly affecting daily work of border guards.
- It is essential that border guards needs and requirements are always taken into account when drafting border control processes for different border control points.

Technology/legal perspective:

- Hardware and sensors: At the edge of process-related harmonisation, but with clear impact on travellers' experience, sensor and hardware selection is a critical issue affecting border check processes. Surveillance sensing technologies and setup inside the ABC Gate should be well defined. Selected solution should not be intrusive, yet it should provide high level of security.
- Legal aspects: It is recommended to have a (harmonised) list of safeguards for the ABC users as ABC hides additional risks to the manual border control process. Also, the (data protection) rights of ABC users should be clearly articulated. Legal certainty is needed with regards to whether the pre-enrolment or pre-border checks are covered by the existing legislation. More details on legal aspects are presented in the chapter 3.5.

3.3 Harmonised ABC requirements engineering and management

Toni Ahonen, Sirra Toivonen, VTT

In the FastPass project, the system requirements for ABC systems were analysed and defined based on the needs accruing through end user and stakeholder engagement and profound analysis of the drivers, challenges, possibilities, and solutions related to ABS in different operating environments. Figure 10 presents an overview of the process from needs to requirements concerning the FastPass solutions and scenarios. Furthermore, a compilation of relevant requirements from the available sources (e.g. [Frontex 2015a; 2015b] Austrian national project catalogue) was used as a starting point for further analysis.

The general challenge in the requirements management is usually the massive number of requirements, because even a simple machinery may involve hundreds of requirements. Therefore, considerable effort was made to decide on what basis to categorize the requirements: by source, by context, by priority, by requirement type, etc.

The key objective in the requirements analysis is to avoid e.g. redundant and inconsistent requirements. In addition, all the requirements should be traceable and reflect perfectly the customer needs. This task is easy to define in theory, but can be very burdensome in practice if not handled properly. There are a wide variety of different methods and tools for system builders and their sub-contractors to manage the requirements. The FastPass project tested two of these methods during the development – one tool developed on the SharePoint and one commercial tool. The former provided a workspace where all project partners contributed to the requirements capture and analysis. The latter on the other hand provided a tool for further analysis, refinement and prioritising done by the industry partners. A main challenge in the project was to define an appropriate level of detail of the requirements. Since the project demonstrated harmonised and modular solutions in three border checkpoints at different border types in different countries, the requirements were divided into general requirements and border checkpoint specific requirements. Subsequently, as cost optimisation was not the main priority of the project, the cost consequences of particular requirements were given only modest attention.

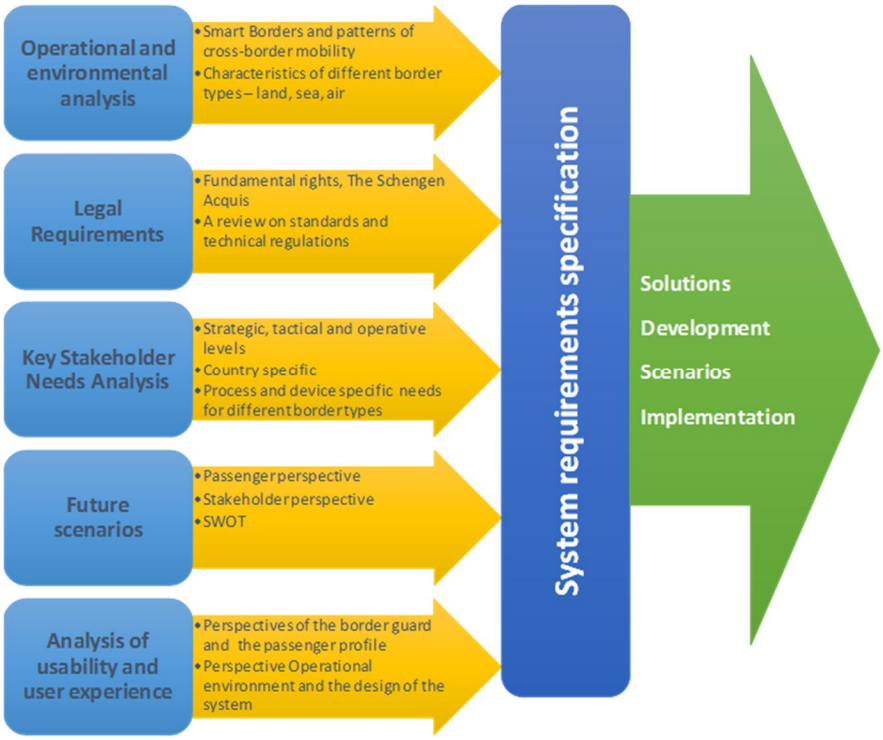


Figure 10. Outline of the phases in the FastPass requirements management process.

Recommendations related to requirement analysis tools

- Try building requirement libraries in order that the requirements can be re-used.
- Use a responsive requirements management tool to enable agile management of requirements
- Selection, development and effective utilization (and maintenance) of the requirements management system is crucial.
- Handling of the requirements should be made fluent for all contributors.
- A visual approach for handling the requirements is preferred, whereas a list of requirements with a number of attributes is not easily obtainable.

A preliminary collection of requirements was derived from the stakeholder needs analysis (Section 4.1), augmented with the input from a literature study and discourse with border guard representatives. The set was subjected to project internal consortium expertise iteration before finalisation. The material was modified and

enriched with the results of wide-ranging stakeholder engagement. This meant re-structuring the stakeholder needs based on their connections to each other and providing further explanation related to the needs from a technical perspective. The system requirements have also been iterated with complementary interviews among technical specialists.

Figure 11. presents the top-level categorization for system requirements, under non-functional and functional classification. Whereas stakeholder requirements have been reviewed, assessed, prioritized and balanced, the technical view of the system has been formulated and each system requirement has been given a place in the structure. Furthermore, priorities have been given according to the MoSCoW method, with the following classification: must, should, could and won't.

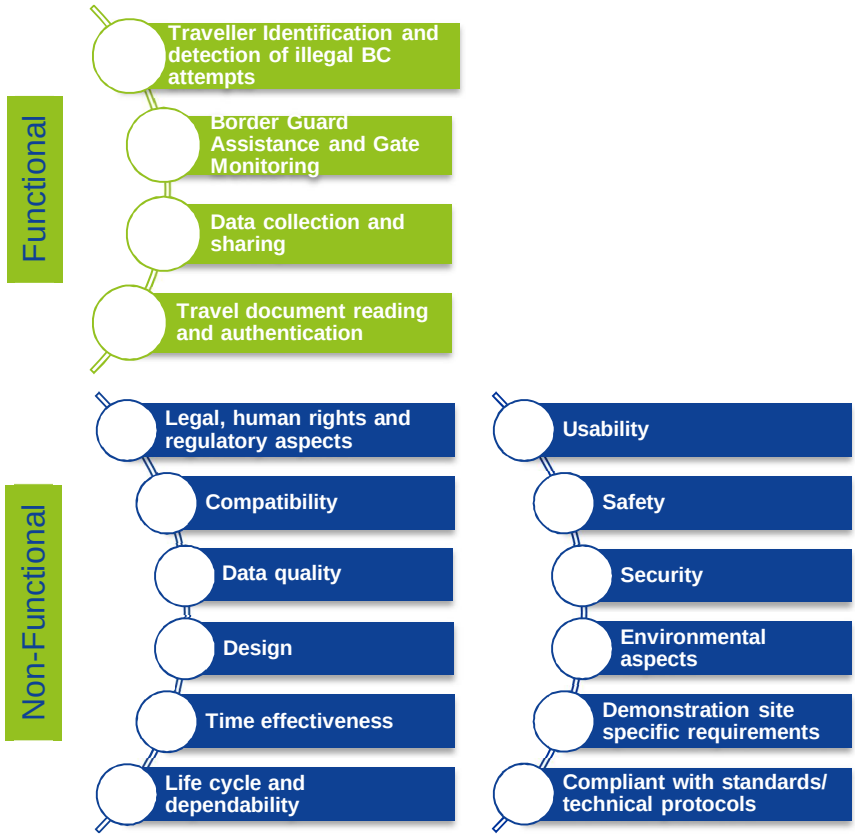


Figure 11. Categories applied in the requirements analysis.

LESSONS FROM THE REQUIREMENTS SPECIFICATION

The foundation of a high quality requirements definition has been an effective and extensive end-user and stakeholder involvement. Although a large number of stakeholders are involved in the process, and different sources of knowledge from specialists need to be integrated, there should be a systematic approach for analysing the stakeholder needs and translation of these into a technical view of the system. The stakeholder interaction took place at strategic, tactical, operational and technical levels, which guaranteed that viewpoints at management level could be enriched with technical knowledge and experiences from operational practices. Sufficient feedback, evaluation and iteration are needed in order to formulate the requirements at an adequate level. With a number of stakeholders involved in the process, the gathering of the input should be managed well and carried out in an open manner in order to promote discussion on the topics with an influence on several development activities.

Recommendations for the requirements management process

- The starting point for any ABC deployment should be a sound business case, which clearly identifies the key objectives of the implementation.
- Requirements and success criteria should be derived and analysed from the key objectives.
- Attention should be paid to the formulation, measurability and accuracy of the requirements.
- To guarantee the traceability of the requirements, the origin must be described and the changes and their reasons as understood during the process must be documented in adequate detail.
- When applying requirements from previous installations, best practice guides and external sources as candidates, as was the case in FastPass, the candidates should be analysed thoroughly and relevant ones systematically refined according to the business case.
- The requirements engineering process should consider systematically the installation-specific effects and required trade-offs.
- Allocation of the responsibilities related to the requirements should be made in adequate detail, particularly in the case of requirements with effects on multiple development activities.
- The classification of the requirements should follow the asset hierarchy developed for the purposes of managing the assets on an adequate level of detail.

3.4 Cost – benefit considerations for the development

Toni Ahonen, Sirra Toivonen, VTT

The Frontex Research & Development Unit has introduced tools for modelling Automated Border Control systems with respect to their design, configuration, benefits and costs [Frontex 2013, 2015]. This Cost Benefit Analysis (CBA) model is specifically focused on supporting decision-makers in evaluating the costs and benefits when making decisions on how to implement an ABC system. More specifically, the model supports answering the following questions: how to select the most appropriate solution from several competing proposals; how best to evaluate a project during its execution; and how best to make use of available knowledge about the project to forecast a project failure and initiate its early closure in order to prevent further drain on resources. The CBA model applies economic modelling, decision trees, influence diagrams, sensitivity and probabilistic analysis and multi criteria analysis. It is a part of a larger framework for financial analysis (F3A). Because the tool developed is primarily intended for the purposes of decision-making in ABC investment projects and for outlining the value of ABC in a larger context, the scope of the tools is to a certain degree different from what is needed in the early development phases of ABC systems and during considerations of the value and costs of individual functionalities. Therefore, in FastPass, it was decided that a more streamlined process for considering the Cost-Benefit issues should be developed.

The main objective of the application of this framework was to make the perspectives and concerns related to costs and benefits visible and to encourage discussion on the real benefits and sacrifices related to the proposed functionalities and innovations. Based on this, decisions can be made concerning whether the functionality will or will not be implemented or whether another option should be preferred. More specifically, the objective is to support developers of the system parts in their practical decisions between different functionalities and technologies.

Thus, the Cost-Benefit assessment was divided into two areas: the selection of technologies for the implementation of an existing (already on the market) or new (innovative) functionality and the decision-making concerning whether a recently innovated functionality should be added. Concluding discussion needs to be carried out so that cost and benefit assessment and related qualitative descriptions are examined side-by-side.

The following tables provide a framework for the discussion of how the considered functionalities will affect the important performance factors of the system. The table can be applied as a coarse assessment tool for the aspects covered that are strongly connected to the high-level requirements identified for FastPass. In certain cases, it may be justified to create a more detailed model including life cycle costing and profit calculations. In these cases, a comparative analysis is recommended, in which the lifecycle costs, profits and benefits are analysed with selected scenarios. In the proposition below, the selected performance factors have been collected from the description of the Frontex ABC model, high-level system requirements derived for FastPass and existing models for lifecycle costing.

In the table, the different identified aspects are described and evaluated according to the kind of positive and negative effects they will provide and how meaningful the effect is from the ABC implementation point of view. Since both benefit and cost assessments are qualitative in nature, the discussion related to the assessment needs to be documented well.

The following table covers direct and indirect influences of the technology addressed. The costs are covered from the perspectives of the development and implementation phase and cost implications over the lifecycle of the technology. The costs are analysed in terms of how the selected technology will influence the costs (reduced, increased, no effects). The framework below only provides a coarse approach, and for significant effects or cases found to be complex it is necessary to analyse the cost items in more detail, for example maintenance costs divided into classes for a more thorough analysis (e.g. corrective, predictive and preventive maintenance, spare parts and consumables, contract services, training, IT support, operator maintenance).

Table 4. Recommendation for a cost-benefit assessment during ABC design.

The amount/significance of the benefits shall be evaluated for the functionality with respect to the following cost items.	**Evaluation scale** A) positive effects B) negative effects C) no effects How: …….. 1) Low 2) Medium 3) Significant
BENEFIT	
PROCESS THROUGHPUT AND MANAGEMENT OR TRAVELLER FLOW	
Discuss how the considered functionality or technology will affect the traveller flow and the throughput.	
EFFICIENT USE OF STAFF FOR DIFFERENT FUNCTIONS IN BORDER CONTROL	
Discuss how the considered functionality or technology will affect the resource management in border control. - e.g. allocation of assets based on the improved predictability of the process	
OFFICERS' MONITORING CAPABILITIES (WITH USABILITY, ERGONOMICS AND EFFECTIVENESS ASPECTS)	
Discuss how the considered functionality or technology will affect the way officers can perform their primary task - how are the usability of the system interface and ergonomics affected and how will they affect the performance? - how are the working methods and fluency of the work of the border guard influenced and how is the performance affected?	
TRAVELLER EXPERIENCE AND SATISFACTION	
Discuss how the considered functionality or technology will affect - queuing time for the traveller - processing time (inside the gate/process) - feeling of a smooth process - attractiveness of the gate.	

TRAVELLER EXPERIENCE AND SATISFACTION SECURITY PERFORMANCE	
Discuss how the considered functionality or technology will affect the passenger identification and profiling - false acceptance rate, - false rejects rate.	
HUMAN SAFETY	
Discuss how the considered functionality or technology will affect the safety issues.	
READINESS FOR FUTURE DEVELOPMENT	
Discuss how the considered functionality or technology will affect the level of readiness for future initiatives.	
LIFECYCLE MANAGEMENT	
Discuss how the considered functionality or technology will affect the - components' lifetimes - upgrade needs during the lifecycle (technical and commercial lifecycles to be considered)	
INTEGRATION	
Discuss how the considered functionality or technology will affect - the possibilities to integrate the system into different port infrastructures. Also, consider the applicability of the functionality in different border types: air, sea and land.	
COST ASSESSMENT	
DIRECT INVESTMENT COST	
Assess the acquisition / direct investment costs related to the technology	
INDIRECT COSTS OF THE DEVELOPMENT PHASE AND IMPLEMENTATION	
Discuss how the considered functionality or technology will affect - the total costs related to an installation phase (possible changes or additions related to the facilities, physical structures, electronic connections, connection to the existing technical infrastructure)	
MAINTENANCE COSTS	
Discuss how the considered functionality or technology will affect - preventive MAINTENANCE need and related costs (preventive maintenance intervals, complexity of maintenance, downtime required for maintaining the equipment, daily upkeep of the equipment – e.g. cleaning)	
OPERATION COSTS	
Discuss how the considered functionality or technology will affect - utilisation and number of personnel - preventive MAINTENANCE need and related costs (preventive maintenance intervals, complexity of maintenance, downtime required for maintaining the equipment, daily upkeep of the equipment – e.g. cleaning) - upkeep of the assets during the lifecycle (upgrades, software updates etc.) - risk of unexpected FAILURES (the inspectability of the system part (monitoring capabilities), operational reliability in different environmental conditions) - energy consumption	

3.5 Usability as a key success factor for ABC implementation

Mari Ylikauppila, Minna Kulju, Sirra Toivonen, VTT

As with any self-service systems with high efficiency demands, ABC systems need to have user-friendly and intuitive interfaces that are easy to remember, give full guidance for the users, and provide universal access. The design of e-Gates must provide both convenience and performance for travellers. A positive user experience is usually based on convenience (timesaving or a reduction in physical or mental work), confidence that the system is functioning correctly, and its perceived utility. Highly practiced (frequent) users can overcome some usability problems. However, in comparison to many other self-service technologies, a large proportion of ABC users will interact with e-Gates very infrequently. Training and regular use improve the users' interaction with the system (learning curve) and improve the users' confidence in and satisfaction with the system. Therefore, for infrequently used systems the ease of use for untrained and non-habitual users with no technological background must be even more carefully considered. In order to increase the usability of automated gates, the system must adapt to the user as much as possible rather than asking the user to adapt to the system. The usability of self-service technologies in a border control context had not been considered much in scientific publications before the beginning of the FastPass project.

While usability relates to the ease of use, i.e. how users can achieve their goals in relation to effectiveness, efficiency and satisfaction when interacting with a product or service, user experience (UX) is concerned with the way users perceive their interaction with a product or service [Hassenzahl 2008]. User experience is subjective, dynamic and contextual; it is dependent on the user and the context of use, and it also might vary during the service or product use. The Technology acceptance model (TAM) predicts how users will accept and use technology and it is divided into two main factors: ease of use and perceived usefulness [Davis 1989]. These factors, usefulness and ease of use, are also the most influential predictors of self-service technology (SST) acceptance [Blut et al. 2016].

In ABC context, ease of use and user satisfaction (good user experience) would increase efficiency and performance; the smoother the interaction with the system is, the more positive is the user experience. And when the experience is positive the user is more likely to use the system again. On the contrary usability challenges faced by the travellers in their interaction with the ABC may slow down the control process, extend the queues, increase the number of interrupted processes and retries, and ultimately decrease the travellers' willingness to use the system. In addition the passenger's challenges in using the self-service systems have a direct influence on the border guard's work and performance [Ylikauppila et al 2014].

In this section, the best practices related to ABC usability and factors supporting positive user experience are presented separately from the points of view of the traveller and the border guard. The best practices are based on the literature, passenger observations and surveys, border guard interviews conducted in a number

of border crossing points in Europe and most importantly on the experiences of the FastPass e-Gate development for three different border control points. One piece of the literature studied was the guidelines published by Frontex [Frontex 2015a, 2016], on the design, deployment and operation of ABC. In these publications usability is mainly considered from the traveller's point of view and best practices are presented. Nevertheless we try to avoid repeating the Frontex guidelines in this document.

3.5.1 ABC usability – the traveller's point of view

ABC USABILITY CHALLENGES

Although the required tasks in an ABC gate to perform self-service border control are rather simple, there are several usability challenges that passengers come across when interacting with current installations. These challenges can be due to the passenger himself, the operational environment, or the ABC system (Figure 12).

The passengers enter the ABC gate one by one and perform the check independently. In some locations there might be assistance available, but usually passengers perform the check alone. Thus the operational environment and the ABC gate design must support and guide the passenger to make correct actions and decisions in each phase. The challenges are often related to the passenger's earlier experience with ABC systems, other self-service systems or technology in general. Different operational environments can be challenging, since passengers have to navigate in in large, complex and unfamiliar surroundings to find diverse checking points areas. They may be stressed or tired. This will have an impact on their concentration and ability to interact with a self-service system. The usability challenges related to the ABC system could be due to the design of the installation. Intuitive gate design, user guidance and especially the document reader operation play the main role in supporting the smooth and effective use and in preventing errors.

Information and clear signs about how to proceed have an important role in encouraging passengers to try the system and guide them successfully through the process. However, the great challenge related to guidance is that often the guidance and instructions are not noticed, or they are read only when problems occur. The importance of the first time experience with the self-service system should be highlighted because it on one hand influences the passenger's future willingness to use the self-service option for border control and on the other hand enables a fluent process and positive experience.

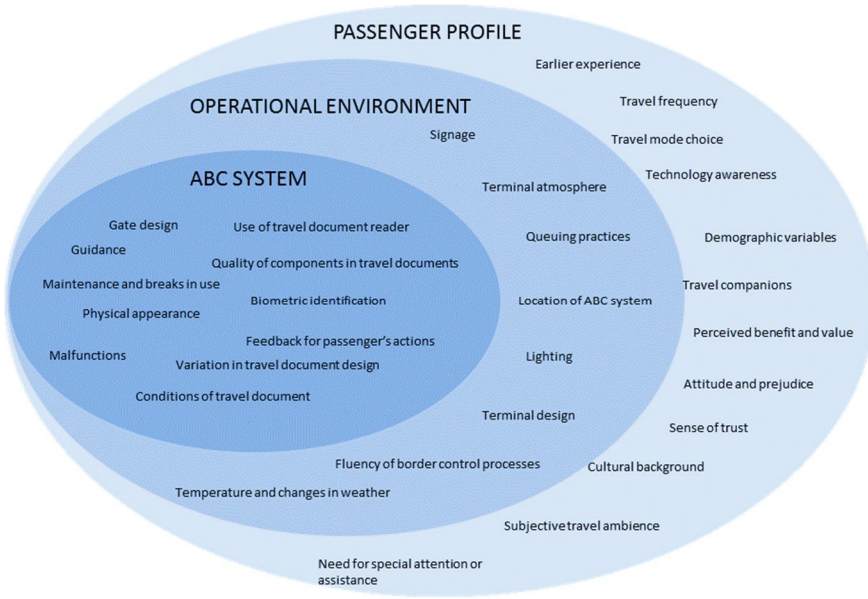


Figure 12. Usability requirements must be addressed comprehensively [Ylikauppila et al. 2014].

PASSENGER PROFILE

The traveller profile in different border checkpoints (land, sea and air) varies considerably and the experiences related to border control are diverse. In general, in the air border, travellers are overwhelmingly from various different countries and cultures, whereas in the land border travellers are mostly from the nearby areas and are usually more experienced in crossing the border. The time of the year, seasons and special events have an effect on the traveller profile. Generally speaking, the business travellers are usually more familiar with different processes related to travelling (including border control) than average holiday travellers. Travellers' experiences of technology also have a considerable effect on the willingness to use and acceptance of the self-service border check.

ABC SYSTEMS IN DIVERSE OPERATIONAL ENVIRONMENTS

The design and outward appearance of the physical installation have an important impact on how easily travellers (especially 'novice' users) identify the system, how obvious is its purpose and how attractive it appears. For some people the physical appearance, the height, width and materials used in the walls and barriers of ABC systems may also give rise to negative feelings and even anxiety towards them.

The purpose of guidance before the area of border crossing is to inform passengers about the border control in general and about the possibilities to use ABCs. It

is also to inform the passengers about who are entitled to use the automated alternatives and what is required to pass the control successfully. Passengers, especially the non-EU citizen, are only rarely aware of the option to conduct the border control processes via self-service. This indicates that information channels have not been used sufficiently to inform people about the existence of self-service systems. In addition, Frontex [Frontex 2015a] recommends that any information related to the e-Gates and given in advance should be oriented towards creating awareness of the system and developing willingness to use it.

In passenger terminal environments, careful design of passenger itineraries and guidance of passenger flow are essential for efficient functioning. In unfamiliar situations, people have a tendency to try to get hints about how the system works and what they are expected to do by observing other passengers interacting with the e-Gates. Crowds of people in a terminal area may obscure the signage and instructions and prevent passengers from seeing the system in action. At land borders where vehicles are involved, the design of traffic lanes and signage has a key role in ensuring effective traffic flow.

Clear instructions at the gate or kiosk and careful design and positioning of the different components could help to make the use of the system more intuitive, to guide the passenger successfully and smoothly through the different steps and to prevent usage errors. The document reading that usually starts the process is the key challenge. Different types of travel documents may cause challenges in ABC usage because despite international standards (e.g. ICAO), the documents have different realisation in their design (e.g. the dimensions of documents or materials used may vary). Furthermore, besides passports, EU member state national ID-cards can be used for border crossing within Europe. The diversity of travel documents causes usability problems when the passenger is unsure how the document should be placed on the document reader. Difficulties often appear as an extended control time and as a number of rejections. For the users it may be difficult to understand the reason for the rejection, which makes it difficult for them to correct the action. Furthermore travellers may be unsure when exactly to enter or exit the system, where objects are located and how they are used. This indicates that users are not very well aware of the steps of the process and what kinds of actions are required. This is often observed as passengers' restless behaviour, cancelled actions and failures in task performance. The importance of traveller guidance has also been highlighted in Frontex guidelines [Frontex 2015a]. The importance of guidance increases particularly when the process is divided into separated phases.

Recommendations to enhance traveller's user experience: ensure ease of use and a fluent and efficient process.

Guidance and feedback are the most important factors to support use of ABC technologies.

- System design should be so clear and unambiguous that no human assistance is needed.
- The amount of guidance should be minimized; the purpose of the information given is to advise the passenger in the efficient use of the system and to prevent error situations and uncertainty.
  - Instruction must be synchronized with the steps of the process. It is recommended to use step-by-step image/animation instructions changing along the process to ensure that the information is available at the moment when it is needed.
  - It is recommended to use clear, common and standardized symbols and icons and to minimize written instructions. The symbols and guidance for ABC should be harmonized and standardized (e.g. Frontex 2015a, p. 56)
  - Clear audio guidance can be used to guide passengers' actions and give feedback on the progress of the process (e.g. when the fingerprint scanning is completed). Complex audio guidance should be avoided.
- Guidance must be adjusted according to the context and specific needs of the control point in question. Especially at land borders, the driving routes and signage must be considered. Clear instructions should be given about how to locate the vehicle so that the devices are reachable.
- The system must provide feedback related to user interaction and progress of the process. A passenger must be provided with clear information of rejection of the inspection process in any phase and, if the checking process fails, the passenger must be provided with an instruction on how to proceed.
  - It is recommended to provide additional guidance in the case of abnormal or incomplete activity (recognised by the technology). For example, if the travel document is incorrectly placed, the passenger is wearing glasses, or has inserted the wrong finger on the fingerprint reader.
- If the border check is segregated into two phases, it must be clearly stated in which order the tasks are to be performed and where.
- If various passenger groups have different processes (e.g. enrolment or stamping for TCN (Third Country Nationals) these should be clearly indicated.
- Guidance and instructions should enhance also the progress of the experienced passenger.

Design processes carefully to support self-service usage and efficient flows.

- It must be clearly stated what kind of phases and tasks the self-service process consists of. Especially if the process is divided into separated phases (e.g. enrolment and e-Gate), it must be clearly indicated what has to be done and in what order the tasks need to be performed.
- The timing of different tasks and steps of the process must be logically synchronised. For example, face capture should be at a moment when a passenger is naturally looking in the direction where the camera is located.
- The system should allow for multiple attempts before rejection, but the maximum time and number of retries must be kept quite low in order not to increase the discomfort of the passenger or slow down the process.
- From the user experience viewpoint, it is recommended to allow the passenger to continue forward regardless of the results of the inspection process and then based on the results direct the passenger accordingly. For example, if the biometric identification has failed, the passenger is not sent back against the flow, but is allowed to continue ahead and then directed by doors or barriers to the border guard for a further check.

ABC design should support purpose of use, encourage and guide correct way of usage.

- The design of the system should be so intuitive that passengers could use it with a minimum amount of guidance. Correct use of the system must be ensured by system design and logical placement of components.
- Different components of the system (document reader, biometric capture unit) must be easily detectable and the intended use easily recognisable.
- All the components must also be ergonomically reachable. This is especially important at land borders, where the system is used from a vehicle.
- The physical dimension of the gate should allow smooth passage for travellers with trolleys or other luggage. It should be possible to complete different phases with e.g. trolley or backpack.
- Needs of special user groups related to physical dimensions and process design must also be carefully considered.
- Gate design should help prevent the passenger from forgetting luggage or any personal items. For example, level surfaces on which to place items should be avoided, and the document reader could be designed so that the passenger cannot accidentally leave the travel document on or in the reader. As an example, the gate door should only open when the passport has been removed from the reader.
- In order to avoid too long waiting and processing times the system should be able to recognise faulty behaviour and advise the passenger immediately. For example, if the document reader recognises that the travel document is not positioned correctly, the passenger should be advised to correct the positioning and to take into account various passport layouts.
- If the passenger is asked to give background information related to the travel, the installation should provide a usable interaction and an easy way to input

and check the information. On the other hand, the system should provide an easy way to cancel the process and delete all information already entered by the passenger.

The operational environment should support the usage by providing conditions with limited disturbing factors.

- The gate design should provide appropriate lighting conditions, in which external reflections and disruptive light beams are avoided in order to ensure proper functioning of the biometric captures and make sure that the passenger can see/read the signage and the given instruction.
- The operational environment and weather conditions must be considered in order to ensure usability and proper functioning of the system. For example, humidity may damage paper documents, and hygienic issues also affect travellers' willingness to use the systems.
- It is especially important to provide proper shelter when the usage occurs outdoors. Humidity, temperature, wind and light must all be considered.

3.5.2 ABC usability challenges from the border guard's point of view

Although border checks are more automated and the travellers use self-service, the responsibility for the final decisions is still in the hands of the border guard. To support this decision making process, the security and speed requirements are critical. The border guard must ensure that no "unclear" persons/cases cross the border, but still ensure fluent passenger flows. Therefore the border guard should be provided with the means to monitor, manage and intervene with the ABC process when needed in the time limit required by the traveller flows which is normally anyway in seconds.

The location of the monitoring station should provide the operator an efficient and sufficient way of profiling passengers through personal data and observed behaviour and appearance. The information provided, volume of information, pictures, symbols and buttons and the usage of information all play an important role in the overall user experience and in the BG ability to fulfil his/her tasks effectively. Compared to the manual check, BGs should not only have all the same information about the passenger and a possibility to intervene, but in addition the system should support automated and the transparent progressing. The system usage should also be consistent with other IT systems. The BG user interface should take into account the BG needs and requirements. During the design phase usability should be ensured with iterative and systematic assessments in dialog between the end users, and professionals.

The border guard UI should provide the information in a harmonised manner at all border types, taking into account the border type and process type specialities. At segregated two step processes with kiosks, the border guard also sees the kiosk registration or enrolment information. In FastPass the UIs have been adapted to

each of the demonstration site needs, which has meant for example adaption to mobile user interfaces and various supported languages. Already from the beginning of the project, it was clear that one key point in designing the border guard UIs and assistance concepts was the information contents of the screens, their clearness, process support as well as the overall user experience.

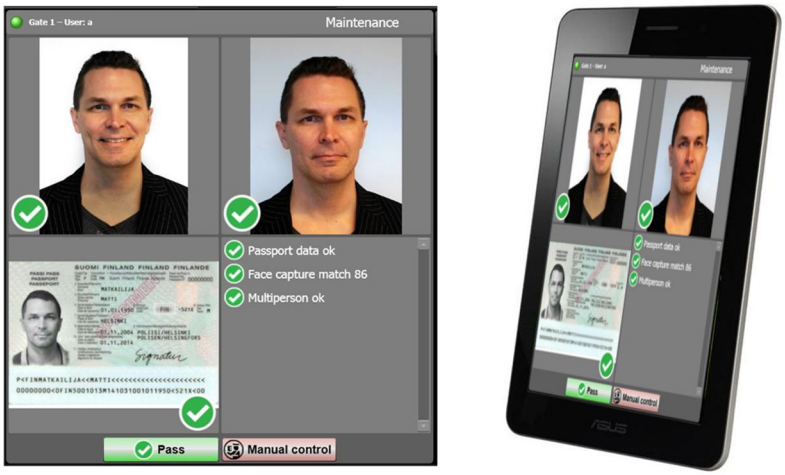


Figure 13. The border guard UI on a mobile tablet.

The border guard user interfaces include the following information: an image of the passport data page, passport photo, face images and the success indicator of face match (yes/no, there is no score) (Figure 13 and Figure 14). The operator's console also include information on the person separation, the surveillance camera from the surrounding area and the result information of the background and security checks. Monitoring should provide a general overview of the situation at a number of gates and a detailed insight into the particular data or performance of a particular gate.

Figure 14. Border guard user interface for the land border.

In the case of a hit in a national or European database, the border guard must be able to intervene and take the final decision to grant or refuse automated entry and to pick the traveller for further check. For this purpose, there are buttons for accepting the control and forwarding the traveller to manual control. There is always a possibility to take the passenger to a manual check when the BG considers it to be necessary, and to open the gate doors manually if there is an emergency or if this is otherwise needed.

Recommendations to enhance the border guard's system usability

At ABC monitoring the border guards must be able to focus on border controlling work.

- Only relevant information and functions should be displayed on the primary screen.
- Distinction between trivial and important messages is important in order to ensure that border guards can quickly react to those that need action.
- The system should not involve the officer in the handling of too many streams of visual information or too many near-simultaneous events. The UI must be designed so that all the required passenger data is seen at a glance and indicators of different process phases are visible for the BG.
- All kinds of administrative tasks and settings modification should be clearly separated from the routine monitoring tasks.
- The user interfaces should be automated to the extent that is feasible and convenient, without requiring continuous attention and intervention from border guards.

Operational environments and national differences must be carefully considered

- The requirements related to different border types and countries have to be taken into account during the development. A modular interface enables personalized modifications of border guard user interfaces according to the contextual differences.
- Location of the monitoring room and terminal design must be designed so that it supports profiling and observing the passenger flow.
- Border guard booths quite often have only limited space available, and user interfaces should take this into account. The monitors should be 100% utilized for the user interface; no space should be wasted and all information of the user interface should use 1 or 2 monitors but no more.

Good ergonomic design to ensure the monitoring station functionality.

- Environmental factors affecting the ability to work, such as lighting, temperature, air condition, noise and humidity must be carefully taken into account when designing a monitoring station.
- All the needed equipment, should be placed in positions which allow border guards to work comfortably and without physical or mental stress.

4. Technical aspects when implementing ABC

4.1 Modular architecture of an automated border control

Sebastian Zehetbauer, OeSD

Philipp Mayr, Veridos

In this chapter, the architecture for the FastPass System is described. The architecture is based on an RM-ODP [Cambridge dictionary] approach. This has been selected for the design of the FastPass architecture as the primary objectives of RM-ODP, such as support for aspects of distributed processing, provision of interoperability across heterogeneous systems, and hiding consequences of distribution to systems developers, are largely coherent with the FastPass objectives.

The system architecture supports harmonisation for ABC gates for different border types (air, land, sea) and provides generic interfaces in order to facilitate and harmonise the integration of software and hardware components. As such, the architecture supports different possible e-Gate solutions for example with and without kiosks. The same software can also be used for manually operated border stations. This enables harmonisation of systems in the country independent of the control process used at the checkpoint or the control point type.

The FastPass Architecture (FPA) is designed to be secure, privacy conserving, modular and flexible. Due to the unforeseeable dynamics of such systems and processes, FastPass Architecture and processes have been designed to have readiness for change, i.e. for highly configurable workflows. Consequently, some of its components are optional and can be removed from the configuration in order to support different types of concepts for an automated border control process, like a Registered Traveller Programme (RTP) or others, and to support different types of biometrics to be used (face, iris, fingerprint) or combinations of them.

To allow an easy exchange of components (biometric devices, e-Gate hardware, databases, token printers and document readers) standardised interfaces shall be defined and used. By the usage of such interfaces the components can easily be removed and replaced during maintenance and updates, and different vendors can provide different implementations of one device without the need to change the entire system.

The architecture contains a specification framework for the design of e-Gates (e.g. service components/networks) and provides a platform neutral specification. The architecture is based on the requirements and published guidelines on design, deployment and operation of ABC gates.

The described FastPass Architecture:

- The design of an architecture enables for an ABC system where special attention is paid to providing a solution for the modular and flexible combination of data and services taking into account privacy and data protection. The FastPass Architecture contributes to the FRONTEX, ICAO system definitions and specification and takes into account the FPA and the European Entry/Exit discussions.
- The FastPass Architecture contributes to the harmonisation, interoperability and information security of ABC systems.
- Provides a software infrastructure that enables a fast and convenient automated border control (e.g. taking into account border crossing workflows) and different implementation scenarios (one-step, segregated-two-step) and supports manual border stations.
- Supports services for various automated border control applications based on the architecture (e.g. passport verification, biometric verification, ABC system monitoring and communication to external systems).

The FastPass Architecture and (thematic) services was validated in a multi-scenario environment (e.g. air, land and sea borders) as well as different programs (e.g. RTP). It provided software standards for ABC applications. In addition, the architecture provides the basis for a comprehensive risk and security analysis.

The overall architecture entails different subsystems as explained in the following chapters in more detail. These subsystems include

- The e-Gate itself.
- The subsystem kiosk for a document check before entering the gate and / or checking biometrics. The kiosk can be separated from the e-Gate or directly attached to it.
- The subsystem of the border inspector with a monitoring application.
- The subsystem for the gate management and the servers.
- The subsystem for enrolment and pre-registration e.g. for a Registered Traveller Programme.

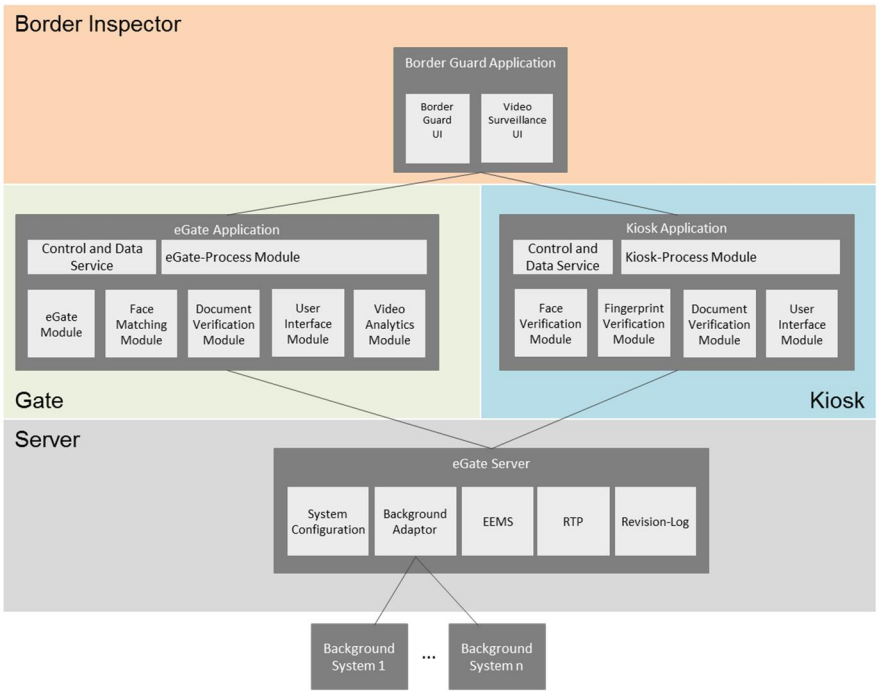


Figure 15. Generic ABC architecture.

The system overview for air, land and sea border ABCs is presented on the following diagrams. These diagrams are simple representations of the current system state and are not UML compliant.

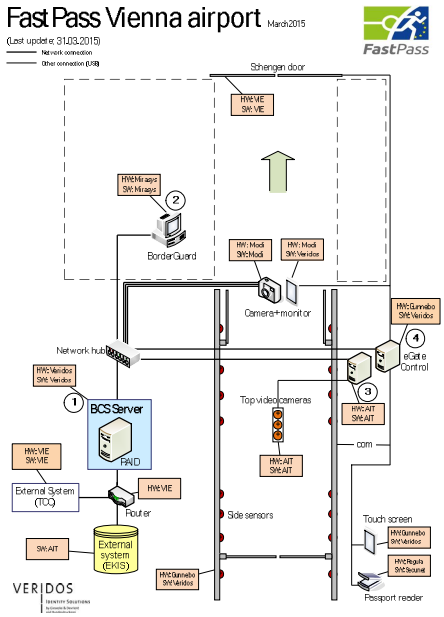
The FastPass air border solution demonstrated multiple solutions, e.g. scenario K1 "Passport-Token Kiosk Segregated 2-step Kiosk". This “K1” solution consisted of the border guard interface, 4 Kiosks, 2 e-Gates, connected background databases, and a Schengen door. Both Schengen area citizens and Third Country Nationals (TCN) were allowed to use the solution. The border guard interface allows the supervision of the traveller enrolment at the Kiosks and e-Gates passage. The border guard is broadly supported in his decision concerning a manual border control by a variety of data offered by the border guard interface, e.g. personal data, document data, results of face recognition, document checks, person search, document search, single person detection, as well as video surveillance. Via border guard interface the Kiosks and e-Gates may also be administered, the Schengen door can be opened and closed. At the Kiosk the mandatory traveller enrolment is done. After selecting the language and accepting the declaration of consent concerning data-storage and the terms and conditions, document checks and face recognition take place. Person search and document search are initiated. In some predefined cases, travellers are directly sent to the manual border control. After entering the e-Gate, face recognition and single person detection are carried out. In

case of any abnormality, e.g. on a person search hit, the border guard is requested to open the e-Gate via border guard interface and a manual border control may subsequently be carried out. A border guard can request manual inspection of a traveller at any time. In case of emergency, the traveller may use an e-Gate alarm button to talk with the border guard via an intercom. The border guard has different options for releasing a trapped traveller from the e-Gate. In some predefined cases travellers are not allowed to enter the e-Gate and are directly sent to the manual border control

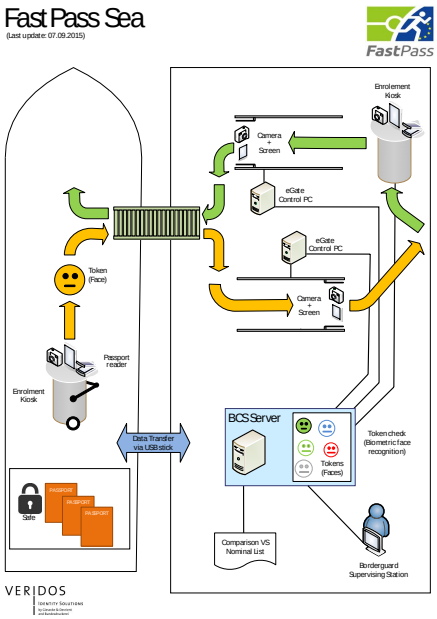
The sea port scenario is more complex than the airport scenario because there exists a new type of kiosk, the offline kiosk. The offline kiosk is located on the cruise ship and hosts not only the Kiosk System Controller but also a local RTP service along with configuration and revision logging components. The offline kiosk is so called because it has no network connection. Once in the port, the enrolled traveller data will be exported and transferred to the online kiosk where automatic import will take place and populate the RTP system. After the import has taken place, the travellers are free to enter the country using the entry e-Gate, provided they are mentioned in the nominal list. The e-Gate contains a single door. If the traveller is enrolled and is in the nominal list, the e-Gate door opens and allows the passenger to pass. Otherwise, the door stays closed and the Border Control Officer is required to handle manually the traveller. The following diagrams and pictures show the sea border scenario.

The land border scenario differs from the others considerably because it is vehicle oriented. A vehicle trap has replaced the traveller e-Gate, and is equipped with an entry and an exit barrier. An enrolment kiosk exists where travellers wishing to use the ABC system have to register themselves and their car first. The kiosk corresponds to the enrolment kiosks used in other scenarios. The main difference being the addition of a scanner that is necessary for scanning larger documents like insurance green cards and vehicle registration documents. The enrolment data is stored in the RTP on the server as in the other scenarios. This data includes the number plate of the car and, as in the air border scenario, the combined template of the face produced in infrared light.

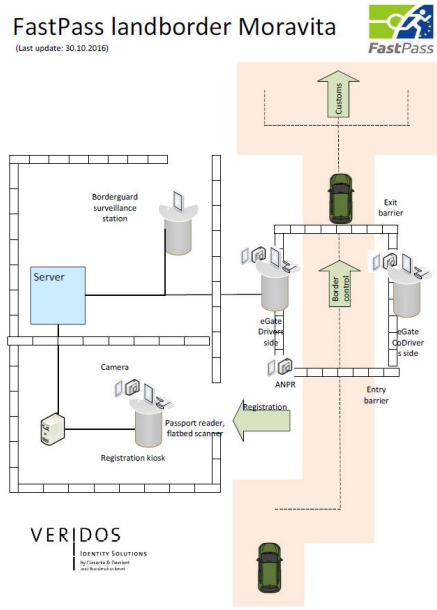
After enrolment, the car can drive up to the vehicle trap. The entry traffic light displays red at this time. The forward-looking camera recognises the license plate and, if the car has been enrolled previously, triggers the e-Gate System Controller by Veridos to open the entry barrier and to switch the traffic light to green, thus signalling the driver the permission to enter the vehicle trap. Once the car is inside and has come to full stop then entry barrier closes and two terminal units move to the car windows. These terminals contain each a display for guiding the driver and the passenger through the border crossing workflow. In addition, each of the terminals contains a face camera working in infrared light and a passport reader provided. The driver and, if present, the passenger put their passports on the reader and look into the camera. The data of the documents and the results of the face matching against the template are displayed in the Border Guard Application allowing the Border Control Officer to decide if the border crossing process is complete. The Officer opens the exit barrier manually at his discretion.



Air border Diagram



Sea Border Diagram



Land border diagram

Figure 16. Diagrams with a simple overview of the system state showing the harmonised architectural solution.

Recommendations for the architecture of an ABC system:

- The system should support different implementation scenarios and different border types
- The system should use standardised interfaces to interchange components easily
- The system should use standard software components to adapt to new laws or integrate / change biometric sensors and document readers easily
- The system should support different implementation scenarios

4.2 High security solution

Anna-Mari Heikkilä, Heta Kojo, Sirra Toivonen, VTT

Sebastian Zehetbauer, OeSD

Automated Border Control (ABC) systems have been introduced for making border control more efficient while maintaining or even improving the current level of border security. However, there remains the question to what extent efficiency and convenience for the involved actors might affect security.

The answers to this question must be fact-based and require some methodology of systematic analysis. FastPass provides a commonly accepted security evaluation framework for ABC as one of its most important missions. Without such a commonly agreed framework, Europe risks eventually having first- and second-class borders with respect to security. FastPass has made recommendations about the appropriate methodology and has provided most of the relevant information for that methodology. In this way, FastPass can provide future harmonised security assessment of ABC installations across Europe and potentially worldwide.

Although the main purpose of ABC gates is to facilitate border crossings for legitimate travellers, there is also an equally important need to prevent illegal border crossing. Moreover, should such an unauthorised act occur despite all countermeasures, the system should provide support for monitoring and properly following up such an incident. On the other hand, the group of legitimate travellers benefitting from the ABC facilitation should be as large as possible. The work on security assessment had a strong impact on the proper fulfilment of this requirement.

APPROACH

Security evaluation in FastPass aimed to provide the future system owners with the necessary assessment framework that should enable them to conduct a security evaluation of the integrated border control process. Thus, the framework has been tested by assessing the security of installations at air, land and sea borders.

The methodology for the security evaluation as used in FastPass follows mainly the existing standardisation on security and risk evaluations. FastPass has performed a comprehensive scan of existing standards and methods for risk assessment, which has been utilized during the project security for evaluating and assessing the safety aspects of the development. No operation manual for border guards, IT staff or ongoing (IT) service management has been provided by FastPass, but means for the operational risks analysis focusing on the primary usage of the e-Gate process (crossing the border) have been successfully used.

Due to the topic independent approach of the 31000 standard family, it has been chosen as the framework for the FastPass security evaluations. Whereas ISO/IEC 27005 [ISO/IEC 27005:2011] focuses on Risk Management for Information Security Management and is tightly bound to the ISO/IEC 27001 Information Security Management System, ISO/IEC 31010 provides the basic principles and generic guidelines without being biased towards a specific area. This allows broader adoption of different objectives (IT-related, user-related, IEMI et al). Both standards address the risk management process in a similar fashion but differ primarily in their intended purpose.

Standards ISO 31000:2009 [ISO 31000:2009] and IEC 31010:2009 [IEC 31010:2009] are introduced because they provide common principles for risk management and risk assessment, and they can be applied to all types and forms of risk (technical, human, security, safety etc.). Common principles are considered important for development projects involving many partners, such as FastPass.

RESULTS

The FastPass risk analysis methodology covers the identification of risk indicators based on both IT-related and user-related threats with an impact on the operation of e-Gate systems for different border control types. A security risk analysis of the ABC system including risks associated with IT systems and with the processes and operations of an e-Gate has been carried out based on a high level e-Gate process. As a final result, it can be said that the risk analysis provides the basis for the system security and availability.

Security and operational risk analysis is recommended to focus on a detailed threat evaluation as well as classification of threats by affected components and applicable border scenarios. In FastPass, $DREAD_{FastPass}$. has been successfully used for the threat identification, and $STRIDE_{FastPass}$ for classification of the identified threats.[5]

In the IT-related risk analysis, it is recommended to address IT components and communication interfaces identified within each process step in the indicative implementation environment of e-Gate. Special attention is advised to be given to the electromagnetic threats (IEMI) to which passport readers might be exposed. The risks regarding information systems need to cover at least hardware, software (e.g.

[5] $DREAD_{FastPass}$. and $STRIDE_{FastPass}$ are customized from the DREAD and STRIDE tools developed by Microsoft.

operating systems such as Windows, Linux and applications running on the operating system), communication (e.g. TCP/IP) between the components and special devices and their software (e.g. gate controller, gate communication based on proprietary protocols).

For the user-related risks, special attention needs to be given to the passenger using an e-Gate system and border guards operating such a system (in a later stage risks related to e.g. maintenance personnel and life cycle issues may also be considered). Following the IEC/ISO 31000:2009 [ISO 31000:2009] the next fundamental questions need to be asked:

- What mistakes and errors (by accident or intentionally) might the users of an automated border check make (what can go wrong and why)?
- What are the consequences of those mistakes?
- How serious are the consequences? Are there any factors that could mitigate the consequences of the risk or are suitable to reduce the probability of identified risks?

In FastPass, it was recognized that the traveller and the border guard work in parallel in a border crossing situation. Thus, both travellers and the border guards' actions and tasks were modelled. In the end, mistakes made by the border guard turned out to be very rare.

As a conclusion, the land border scenarios proved to be more complex than the air borders from both the IT and user-centric points of view. However, the risks were similar, and thus the methodologies used for e-Gate risk and security assessments can be recommended to be used at crossing points at air, land and sea borders.

Moreover, based on the analysis of vulnerabilities that could be exploited for illegal border crossing, the design of the systems for the individual border types has taken into account appropriate protective measures. Where technical measures cannot immediately be found, the future operator should be made aware of potential gaps by the self-assessment that has been derived from the security analysis. Furthermore, risk management also suggested in certain cases that it would be advisable to introduce appropriate monitoring and logging techniques that at least allow for later follow-up in case an illegal border crossing has occurred.

On the other hand, there are certain FastPass innovations that enable reducing the likelihood for certain vulnerabilities significantly. For example, the 2-step approach allows for better early warning about certain risk profiles.

WHAT IS NEEDED IN THE FUTURE?

High security solutions such as e-Gate need to be considered to have a well-established life cycle, starting from initial concept and definition through realization to a final completion which might include decommissioning and disposal of hardware. Through this life-cycle, risk assessment must be applied at all stages and is usually applied many times with different levels of detail to assist in the decisions that need

to be made at each phase. Life cycle phases have different requirements and need different techniques. Thus, an EU-wide harmonized and interoperable solution for ABC systems is required.

Based on the research results on secure solution we propose a number of recommendations:

- e-Gates and other ABC systems are high security solutions that must follow a life-cycle approach with appropriate risk and security assessments at all stages (especially at an early stage of the development).
- Technical, operational and process-related changes need to be evaluated by risk and security management before implementation
- It is important to cover in a common manner all different technical, operational and process-related risks for overall security of new technologies such as e-Gates and other ABC systems.
- IT-related threats should describe the threats to which each process step is exposed, covering all the involved hardware and software components; on a process step level, on a system level, in communication infrastructure and in tasks associated with the overall system.
- The user-centric risk analysis should concentrate on risks related to human beings: the passengers using an ABC system and the border guards operating the system.
- New findings that arise as a result of the risk assessment (either self-assessment or detailed interviews) require further iterations to ensure that the assessment of the process steps covers all identified threats.
- A standardized, holistic, transparent framework for e-Gate risk and security management generates trust towards the ABC systems and their use at different borders.
- Ensuring the highest level of transparency with respect to potential illegal border crossing through high security ABC systems.

4.3 Technical considerations for ABC gate and housing hardware at different border types

Thomas Bürgin, Lothar Lais, Magnetic Autocontrol GMBH

LANDBORDER ABC

According to the Schengen Border Code [EU 2016/399 2016] it is recommended that the driver and passengers may remain inside the vehicle during checks. Schengen recommendation refers to manual checks, and applying it to an automated self-service system operable from inside the vehicle is a challenge that requires new solutions also from the mechanical design.

To accelerate the checking procedure, it is necessary to perform the process at both sides of the car, at least for the driver and the co-driver simultaneously. Due to this and the fact that each car has different dimensions, the devices for the border process have to be automatically moveable and their position adjustable for different cars. When no car is present, or the process is finished, these terminals are driven to their home positions away from the car. Due to the width of different cars, the distance between the left and the right hand terminals in their home position has to be at least 2.5 m.

Figure 17. Vehicle width and height.

Preferably, the devices used for checks should be protected from being touched and damaged by entering cars by a protective housing (later called terminals). When no car is present or the process is finished, the terminals need to be driven to their home position, a position most far away from the vehicle. Due to the width of different cars, the distance between the left and the right hand terminals in their home position has to be at least 2.5 m.

Steel bollards or a guiding for the wheels should be installed to protect the terminals from being touched and damaged by entering cars. Also for these protectors the width of the passage hast to be at least 2.5 m.

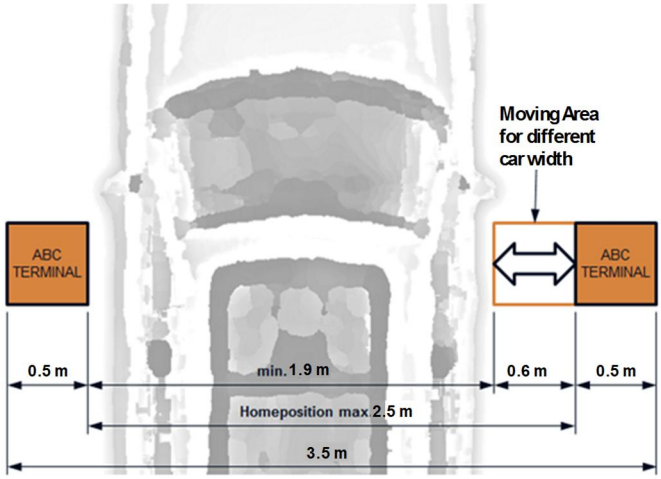


Figure 18. Terminal positions related to the vehicle.

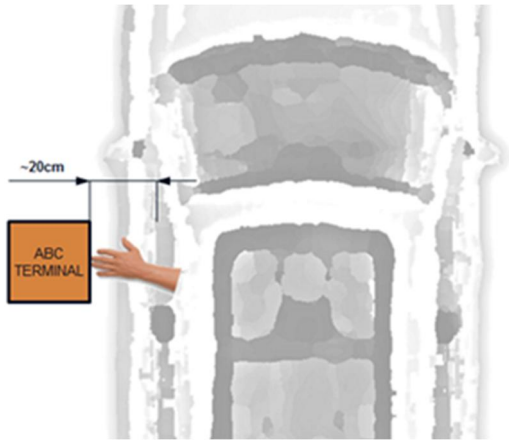


Figure 19. Best user distance.

It is necessary to move the checking equipment automatically to a most comfortable position towards the passengers. The best horizontal operating position is about 10 cm to 20 cm in front of the side windows of the car.

Due to different types of cars, the terminals have to be driven maximum 60 cm towards the car and maximum 60 cm up- and downwards to reach the best operating height between 90 cm and 1.5 m above the road. A manual adjustment of the vertical position should also be possible. The different driving behaviour with right-hand and left-hand driven cars has to be considered. So, both terminals for the driver and the co-driver should be moved towards the car.

By means of suitable safety sensors, the terminals may never touch the car. In addition, it has to be guaranteed, that the moving terminals never squeeze persons, neither in front nor at the backside of the terminal.

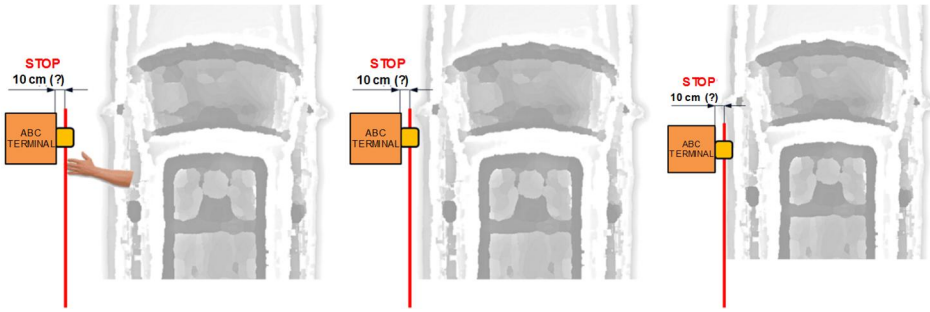


Figure 20. Safety sensor.

The complete automatic border control area, the ABC gate, should be arranged as an air lock, with entry and exit barriers. Due to the possible presence of persons, the barriers have to comply with the requirements of EN 12453 [BS-EN 12453:2001] (“Industrial, commercial and garage doors and gates – Safety in use of power operated doors – Requirements”). Especially the impact force of the barrier boom must not exceed the valid level of 400N. Protection devices have to be installed to prevent persons from being injured by the closing barrier boom. Traffic lights should avoid that no more than one car enters the gate. Suitable protection devices like inductive loops have to be installed to prevent the barrier from closing the boom while a vehicle is present.

The gate should be as small as possible, so that existing border checkpoints can be retrofitted without losing a lot of space in the passages. The width of the gate should not exceed 3.5 to 4.0 m. The length of the gate should be about 8 m.

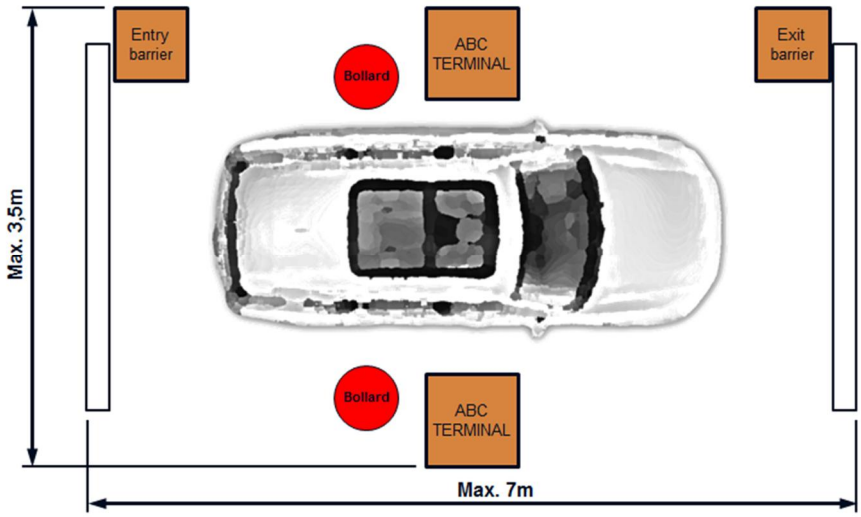


Figure 21. Gate arrangement and dimensions.

The complete equipment for the ABC gate has to be designed for outdoor use. The protection class has to be IP54. The devices have to operate in a temperature range between -30 and +55 °C.

The integration of the gate software into the superior system should be simply done by DLL drivers. With a user-optimised graphical interface (GUI) the status of the gate should be easily supervised.

Summary of mechanical recommendations for land border e-Gate:

- Passage width in terminal home position: 2.5 m
- Horizontal moving distance of each terminal: max. 60 cm
- Vertical moving distance of each terminal: max. 60 cm
- Operating distance range above the road: 90 cm to 1.5 m
- Recommended gate width: max. 3.5 to 4.0 m
- Recommended gate length: max. 8.0 m
- Protection class against water and dust: IP54
- Operating temperature range: -30 to +55 °C
- Requirements for barriers according to: EN 12453

E-GATE INSTALLATION IN THE TERMINAL – AIR BORDER

Automated border control in the airport environment is already a well-known process in some regions of the world. However, from country to country, the process can vary, different biometric verification is used or a pre-registration is necessary, etc. Nowadays, the benefit often is limited to a group of travellers. The aim here was to develop a process for European wide application and a technical solution to facilitate the use and make it common between Schengen and non-Schengen areas. The request is to have a fast but reliable entry control in a special, restricted area without the need of increasing the number of Border Guards.

The e-Gates in terminals should have the same harmonised look and feel. In addition, the Air Border e-Gate shall have the advantages in terms of

- User friendliness
- Inviting design
- Illumination of the glass panels
- Fast processing
- Reliability
- Safety for passengers, Border Guards and service personnel.

The gate must handle different travellers with different luggage e.g. trolleys.

Moreover, due to the need that the gate hardware should support only one person entering the gate at a time, in other words to prevent tailgating, the complete length of the housing is about 3.0 m. This length also guarantees a comfortable position for being detected by the face recognition camera system. The width of the passage should be about 70 cm. So, passengers do feel comfortable, hand luggage can be handled easily and the width of the complete gate is not too space consuming. It is recommended to fix the gate directly onto the floor with anchor bolts. If this is not possible or not allowed, the gate also can be glued to the floor. A support ramp as used for the test gates is not advisable because this can introduce hazards.

To get a high acceptance of the passengers, the gate should have an attractive, appealing, transparent and a trustworthy design and effect. This can be reached by careful design and using a lot of glass and an attractive illumination. Usability issues should also be properly addressed in the design.

The following requirements were defined by the stakeholders for the e-Gate design:

- The kiosk is designed to be adaptable for an easy modification for future generations of readers and screens.
- Fast processing time
- Secure and reliable immigration check via face recognition
- Face recognition camera adjustable
- Safe
- User friendly
- Appealing design
- Space saving dimensions
- Silent operation using Brushless DC motor technology
- Connective via WLAN
- Low power consumption
- Low total cost of ownership

Summary of mechanical recommendations for an air border e-Gate:

- Passage width: 70 cm
- Gate length: 3.0 m
- Protection class against water and dust: IP43
- Operating temperature range: +5 to +55 °C

E-GATE INSTALLATION IN THE TERMINAL – SEA BORDER FOR THE CRUISE SHIP BORDER CHECKS

Passengers of Cruise ships are so called “low risk passengers” having special requirements for border checks in Schengen code as well. This is because they already have been checked before entering on the Cruise ship. Therefore, the immigration process when leaving the Cruise ship is normally done fast. Depending on the size of the Cruise Ship, more than 2.000 passengers may to leave the ship within a very short time. In addition, there is often not enough space in the arrival halls to install many immigration lanes. Instead, the passengers leaving the ships are often selected according risk analysis for a detailed check.

The objective for automating the border check process is to have a fast but still reliable immigration control in a special, restricted area without the need of increasing the number of Border Guards. An additional requirement of the Sea Port of Piraeus was, that the same e-Gate should be used for passengers entering or leaving Cruise Ships. As arrival and departure take place in different halls of the terminal, it is necessary to transfer the e-Gate from one hall to the other regularly. This transfer must be done in one hour or less. Therefore, the fixing of the e-Gate on the floor was not possible. In addition, the e-Gate must be transported through existing sliding doors with restricted height.

Immigration control processes at airports were found to be similar to the needs in seaports. Air Border e-Gates use passport readers and/or fingerprints as additional tokens to the face recognition. Passport checks and/or fingerprint checks however need more processing time and consideration was given to the vast amount of cruise ship passengers that need to be processed in a short time. Especially the passport handling was found time-consuming and the data check against a database needs time. In addition, in general Air Border e-Gates are physically very long and heavy so that the requirement for movability cannot be fulfilled. Air Border mantrap e-Gates therefore were not seen practicable for the use in Sea Ports.

To overcome the said difficulties, the process had to be adjusted to the requirements in Sea Ports. Because of the pre-checks on the Cruise ships and the registration via separate kiosks, it was found not necessary to check again the passports at the e-Gate. It had been defined that a biometric check (face) at the e-Gate will be sufficient. A Border Guard is close to the e-Gate and is able to intervene manually if necessary. Furthermore, the permanent presence of a Border Guard makes it possible to use a single door e-Gate instead of a mantrap. This allows a much shorter and a lightweight e-Gate that is a basic prerequisite for a movable gate. Nevertheless, the Sea Border e-Gate shall have the advantages and the look and feel of the Air Border e-Gates.

The complete length of the housing was designed to be about 1.6 m. This length guarantees a comfortable position for the face detection by the recognition camera system. The width of the passage is similar to the installation at the air border. Also the recommendations concerning the fixing of the gate.

Due to a necessary moving to different operation sites, like in Piraeus, a supporting base frame for a transport with a lift truck will be an ideal solution. Because of the restricted height of the existing sliding doors between the halls of the terminal, the e-Gate needs to be foldable to a maximum height of 1.9 m.

At a foldable gate, the connecting cables need to be guided and fixed safely, for example inside the framework structure or inside a cable duct. Especially if the cables are routed from the ceiling to the e-Gate this has to be considered.

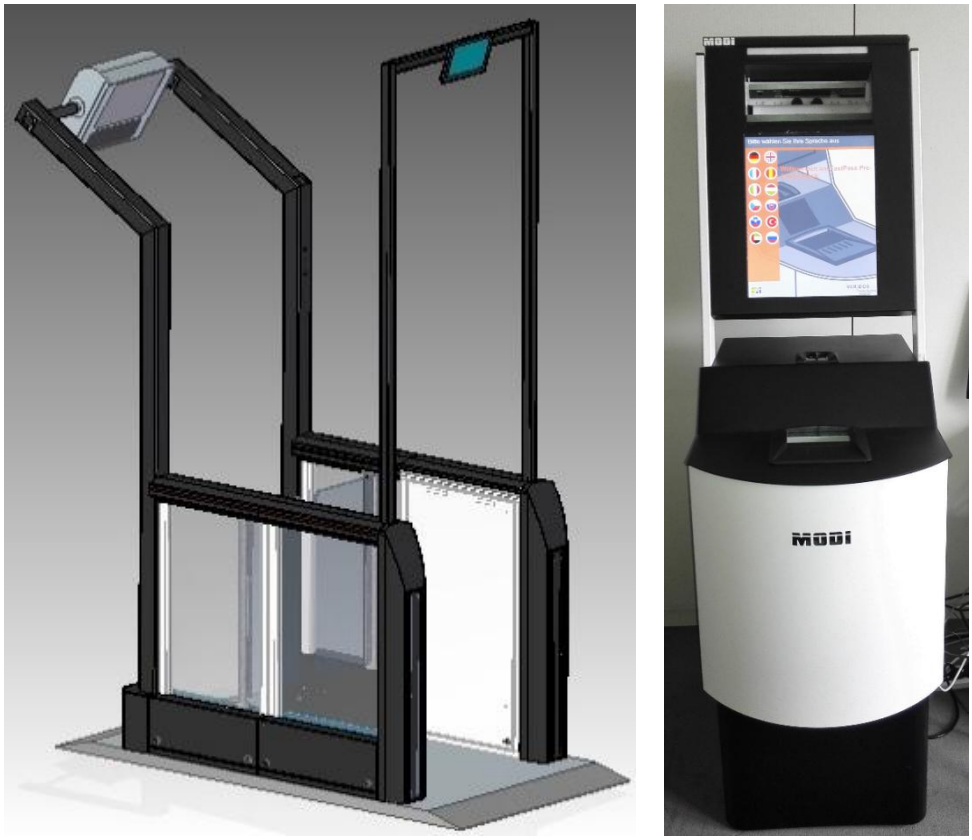


Figure 22. Design of e-Gate and kiosk for the sea border installation.

In order to get a high acceptance of the passengers, the gate should have an attractive, appealing, transparent and a trustworthy design and effect. Especially for the single gate the illumination and the light signals need to be clearly defined. These signals need to be comprehensible to the user. Particularly the fact, that only one person may enter the gate at a time must be clearly indicated. A kind of discretion line in front of the gate may be very helpful. In addition to the air border e-Gate requirements, the following attributes defined by the stakeholders must be fulfilled:

- Easily movable
- Easily fit through existing sliding doors with restricted height
- Stable without fixing to the floor
- Exonerative Border Guards
- Connect via WLAN or LAN

The general recommendations for the cruise ship scenario are in general identical to air border scenario. Below are some special recommendations regarding the mechanical design.

Summary of mechanical recommendations for cruise ship scenario:

- Passage width: 70 cm
- Gate length: 1.6 m
- e-Gate must allow connecting cables coming either from the ceiling or from the floor.
- Protection class against water and dust: IP43
- Operating temperature range: -5 to +55 °C

4.4 Document authentication

Nikita Kolesnev, Maris Kaminskis, Regula

Frank Steffens, Matthias Niesing, Petr Vyletal, Secunet

Automatic security document verification systems play a vital role in the automated border control (ABC). Operation of all automated border control systems (ABC gates) is based on processing electronic machine-readable travel documents (eMRTD). MRTDs have to be checked in the context of border checks. The goal of this check is to make sure that the document is authentic, integer and valid. The eMRTDs incorporate the booklet itself with different physical security features and the electronic component – RFID chip. Verification of eMRTD should be done for both parts: optical and electronical [Gariup & Soederlind 2013].

The Technical Guideline 03135 (TR-03135) from the German Federal Office for Information Security (BSI) describes the processes and requirements necessary for machine based verifications of Machine Readable Travel Documents (MRTDs). The document check can be applied to the entire document, or be limited to parts of the document and refers to the optical or electronic attributes of the document. In order to guarantee traceability and verifiability, the individual verification processes must always lead to well-defined and verifiable results. A single check process is either completed, according to its algorithms, until it terminates and returns a well-defined result corresponding to its definition, or prematurely aborted if it does not return any useful results for the corresponding border control. The results of the individual check processes are generally cumulated to an overall result, which is the basis for the final evaluation of the individual border control.

The document reader captures the information units and attributes of a machine-readable document according to its respective characteristics. The document reader transmits this data to the control application for further processing. Difficulties

in document inspection process appear to the passenger normally as an extended control time needed and as rejects.

DOCUMENTS VERIFICATION MODULE (OPTICAL PART)

Verification of optical security features, which are unique for each type of document, is an essential part of border control process in ABC Gates. This verification depends a lot on hardware (passport reader) performance.

For the optical-physical document check, optical properties of the document are scanned and transmitted to the control application for further processing. The optical check of the physical security attributes of the document usually includes the verification of special printing image properties. These images are also recorded under different light sources (e.g. IR- and UV-light) for further processing (Figure 23). In addition to the optical check of the physical properties of the document, the machine readable areas have to be processed too. This includes especially the MRZ.

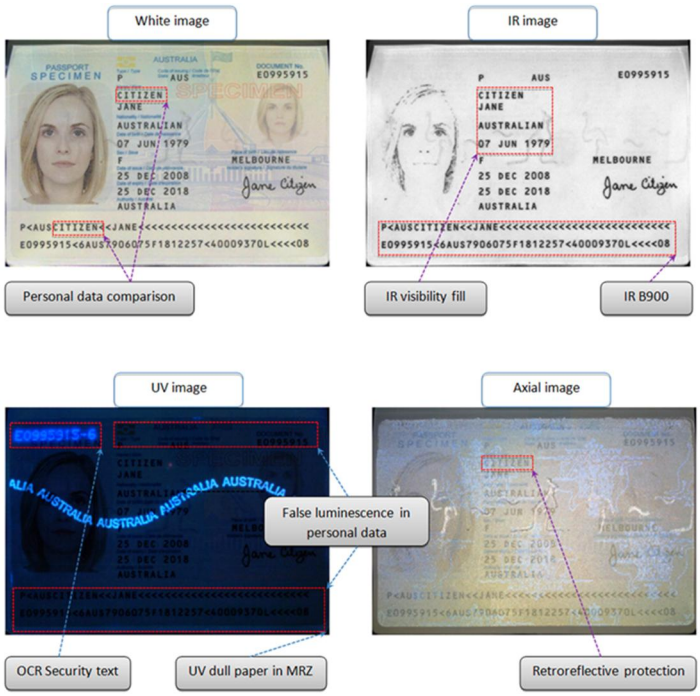


Figure 23. Security features in different wavelengths for typical passport.

Recommendations on the document inspection module functionality:

- Reading of the machine readable zone (MRZ) OCR
- Reading of the visual inspection zone (VIZ) OCR
- 1D barcode reading: Codabar, Code 128, Code 39 (+extended), Code 93, EAN-13, EAN-8, Interleaved 2 of 5 (ITF), STF (Industrial), Matrix 2 of 5, IATA 2 of 5 (Airline), UPC-A, UPC-E
- 2D barcode reading: PDF-417, QR Code, Aztec, Datamatrix
- Verification of control sums in MRZ against Doc 9303 ICAO
- Checking the contrast of MRZ printing against Doc 9303 ICAO
- Checking UV dull paper (separate checks for MRZ element, photo element and whole data page)
- Cross-verification of textual data retrieved from: MRZ, VIZ, Barcode, RFID-chip
- Checking luminescence of fibres under UV light
- Checking the photo application method: printed or pasted
- Checking of the image patterns in visible, IR and UV light
- Detection of false luminescence
- Reading a luminescent text and comparing it with data obtained from MRZ and VIZ (OCR Security text)
- Checking visibility or invisibility of specified areas under IR light
- Invisible personal information visualization
- Checking barcode format
- Detection of holograms (OVD), OVI
- Photo comparison between DG2 (RFID) and printed photo from the data page
- All checks mentioned above should be adjusted to documents with different degrees of wear and tear
- The choice if checking operations mentioned above depends on security features available in a questioned document

ACCESS AND VERIFICATION OF ELECTRONIC CHIP DATA

To guarantee the security and reliability of the border control process the electronic content of the eMRTD chip has to be checked in detail [BSI TR-03135 2014; ISO/IEC 10746-1:1998]. The result of a biometric verification is trustworthy only if the integrity and authenticity of the source of the reference data is validated. For this purpose, the Passive Authentication mechanism as specified by ICAO [ICAO Doc 9303 2015] has to be used. Although this mechanism is specified in detail there are several options how to implement it.

Considerations for analysing the access and verification of the electronic chip data:

- Local vs. central PA
- Trusted sources for CSCA certificates and their exchange (PKD, nPKD, Masterlists, ...)
- Handling of known defects (e.g. in DS certificates, data groups etc.)
- PA for different types of eMRTDs (EU ePassports, 3rd country ePassports, national eIDs)

Usually the eMRTD chip data is protected by access control mechanisms. The currently used ICAO BAC mechanism will be replaced by SAC in the near future. For EAC protocol the version 1 is used in EU ePassports. The new version EAC2 is also specified and already used in national ID cards. Thus, an ABC system has to deal with different types of access control mechanisms. Using EAC (this is needed to get access to fingerprint data stored in the chip) the document reader needs to have certificates and the relevant private keys from an EAC-PKI. In this context, the following issues have to be analysed:

- Local or central key storage
- Certificate management (national and international)
- Integration to background infrastructure

COMBINED OPTICAL AND ELECTRONIC DOCUMENT CHECK

A combined optical and electronic document check is a mixed form of the optical and electronic document checks. It is a hybrid check that requires both optical and electronic attributes. A good example is the comparison of the optical MRZ and the MRZ from the data group 1 (DG1) of the chip. Another example is the comparison of optical recorded facial image with the facial image stored on the chip in the DG2.

Recommendations related to combined optical and electronic document checks:

- In order to guarantee security at automated border control document security checks the document verification should be based on both optical and electronic security checks
- Electronical checks should include Passive Authentication (PA), Active Authentication (AA), Chip Authentication (CA)
- It is essential that the optical verification solution is hardware independent and resistant to external attacks.
- All passport readers used in ABC system must be fully certified by BSI or similar authority for compliance with EAC, SAC, EAC2 (PACE).
- Document authentication systems should be evaluated and tested against known attack scenarios increasing security of ABC systems.

4.5 Innovations in the biometric area

4.5.1 Fingerprint

Jukka Hosio, Deltabit

In FastPass, it was evaluated how different fingerprint capturing technologies perform under varying conditions. Usually performance is measured under optimal conditions. In real life the conditions vary and requirements may be very different depending on the use case. For example, in air border, conditions can be controlled well, while in the land border it is more difficult to keep the conditions stable.

There are many different technologies to capture fingerprints. The most common ones from these are optical and capacitive sensors. Their characteristics on size, price and speed vary greatly. In general, fingerprint capturing performance is not directly dependent on the technology that is used, but it is possible to capture good quality fingerprints with any technology. Also, technological development continues and gradual development can still be expected. Therefore, is not is not possible to recommend a technology that would fulfil all the demands in an optimal way and that could be recommended as the most suitable technology for automatic border control use.

Also, within a single technology, solutions from different vendors have significant differences in the capture performance. External conditions may have a big impact on the quality of the fingerprint that is captured. Especially fingerprints from a dry skin are difficult to capture. This typically happens when the temperature outside gets close to or below zero degrees. In this temperature, the air gets drier and skin dries more. Examples of fingerprint images from different manufacturers can be

found below. Thus, the changes in external temperature have an impact on the capture rate and the matching performance leading to an increased false reject rate even when the temperature in the operational environment is kept stable. The impact on the capture rate with certain manufacturers can be the tens of percentages and may lead to a situation where the operation is not possible due to too high reject rates.

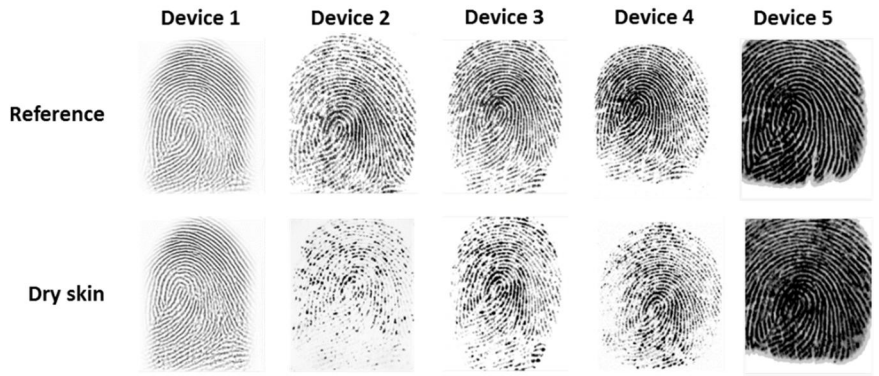


Figure 24. Fingerprint images with dry skin from the same finger from different manufacturers.

In the Best Practice Technical Guidelines for Automated Border Control (ABC) [Frontex 2015b]. Frontex recommends that the performance of the fingerprint verification algorithm is measured by an independent test laboratory or an official agency and that the tests are performed in the actual operational environment with representative catalogue of test users.

By testing both the devices and algorithm under the most challenging expected conditions, the differences can be found before the operations start. After the system is operation, wrong technology selections are impossible to correct without changing the technology providers.

Another challenging condition is rain. Most fingerprint sensors cannot capture good quality images if there is water on the surface of the sensor. Water isolates the surface of the finger from the surface of the sensor and image cannot be captured from those areas. See the image below for sample images taken from the same finger with different fingerprint sensors.

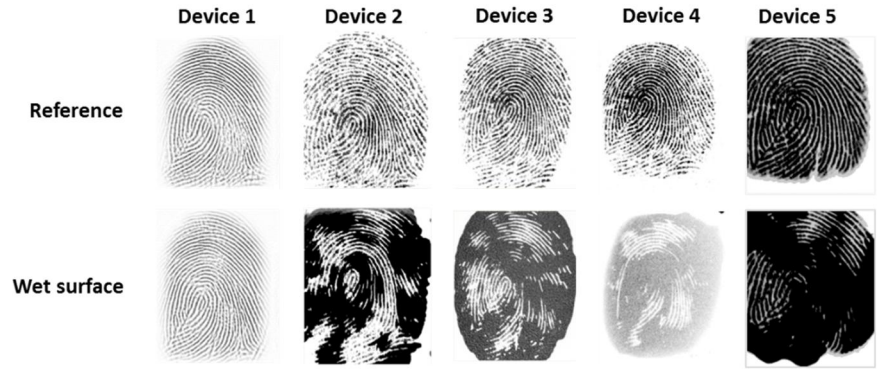


Figure 25. Fingerprint images with a wet sensor surface from the same finger from different manufacturers.

Based on the developments and operational observations we recommend the following:

- The more fingers are added the more complex it becomes for travellers to use the ABC system without assistance from border guards. By using two fingers, usability remains in such a good level that the system can be used without assistance and matching performance improves.
- To find out the differences between different fingerprint capture devices, we recommend extending the algorithm tests to cover also fingerprint capture devices that are considered to be used. This way unassisted performance in all ABC conditions can be improved.
- The performance tests should be done when the external temperature represents the lowest local annual temperatures to ensure that ABC travellers are identified reliably during cold weather.
- If the ABC gate is outdoors, there may be situations where a combination of rain and wind cause mist to flow into the capture environment and to the sensor surface. To avoid this, it is recommended to protect the fingerprint sensor area both from direct and indirect rain with a suitable mechanical construction.

4.5.2 Face

Lulu Chen, University of Reading, and Dieter Klawunder, MODI

Face recognition has been widely integrated in many applications, and is the main biometric trait used in automated border control. To ensure robust and accurate face recognition at the border crossing, capturing enough face image quality is crucial. There are several factors that are important to obtain good image quality: 1) Density

of information of the face characteristics (high-resolution face images), 2) Sharpness of the images (good focus), 3) Suitable illumination without shadows or overexposed areas, and 4) Frontal face image with a substantially parallel orientation to the camera axis.

However, several challenges are present even in the current eGate systems where a person's face is captured inside an eGate while the person stops. For instance, varying position and orientation of the user's head relative to the camera, varying lighting conditions, different facial expressions and occlusions, etc. An ABC gate should be able to automatically detect and recognise people at all heights (generally between 1.50 m–2.10 m). A single camera with fixed position will not be able to cover the range and capture faces in a high resolution as the faces could appear in different positions and heights in front of the camera. In order to overcome these challenging tasks, and to capture good quality of face images, face recognition systems deployed in the existing/traditional eGate systems mostly used two solutions: 1) moving camera and monitor mechanical up and down to match the person's height, 2) using multiple cameras (e.g. an array of cameras).

FastPass has achieved face recognition without stopping by using an innovative technology. During the FastPass demonstration, speed of face detection and face recognition on-the-move has demonstrated good performance. However, the most challenging issue observed through the operation is that users' cooperation has significant impact on the face image quality presented at both the kiosk and gate. Manufacturers have developed different ways for dealing with this situation, which have in common that they use a display as an eye catcher in order to gain the passenger's attention and thereby guiding their viewing direction to the camera. In general, we would like to stress the importance of attracting users' attention to ensure that they would look directly into the camera, in which case a good frontal face image can be captured.

In a border crossing environment, external lighting condition also has a big impact on the face image quality. Lighting changes, which could happen often at a land border, can significantly affect the image acquisition under visible spectrum. Thus, additional hardware or software to correct lighting impact is recommended. Face recognition systems are generally divided into two categories: visible range based and near infrared based. Most traditional face recognition systems capture faces under the visible spectrum. One of the main challenges for these systems is the facial appearance change under visible illumination. Recently, the focus has been moved to using near infrared face images. Thus, using near infrared face recognition could be another option against illumination impact. However, the images stored in a passport is generally an traditional colour image, thus, robust face recognition algorithms are also required for matching between near infrared face to the passport colour face.

Based on the developments and operational observations we recommend the following:

- Additional sound or light signals should be deployed to attract attention from the users to ensure that they will look into the camera
- Face camera position could be modified in order to attract more attention from the users and capture good qualitied frontal face images
- Automated camera calibration should be improved to protect the system against wrong manual settings
- Additional correction on uncontrolled external light influences should be applied to ensure robust and high quality face capture
- Face spoofing detection against 3D masks is challenging while the person is on-the-move especially when the user is less cooperative. Thus, faster detection is necessary for on-the-move scenarios

4.5.3 Iris

Lulu Chen, University of Reading

In a biometric verification system, recognition accuracy is the first important aspect we need to consider. Iris as a biometric characteristic is widely recognised as a biometric identifier because of its high universality, distinctiveness, permanence and performance properties. Iris patterns are epigenetic and possess a high degree of randomness. Iris patterns are believed to be stable over a person's life. These all make iris ideally suited for biometric systems run in identification mode, especially for high security required applications, such as ABC.

However, in the current ABC solutions, iris has not been widely deployed in the e-Gate systems, as iris for ABC is still a challenging task. This is due to the limitation in various aspects.

Firstly, iris is very small in size, thus, it is a very challenging task to acquire good image quality that would be enough for identification task from distance or even on-the-move. To acquire iris on the move, we need to have high-speed camera, otherwise we will capture motion blur. At the same time, to capture iris from distance, we need high resolution cameras while able to find a wider focal range, otherwise we will capture images out of focus. Illumination is another important component for iris acquisition. Iris is normally captured under near infrared spectrum, therefore strong near infrared illuminators are required to give enough light into the small iris region. However, how to balance between eye safety and image quality needs to be carefully considered.

Iris cameras that work in a distance up to 0.5 m are in a price range of 1 K€ to 5 K€. These cameras generally need cooperation from the user. Travellers need to position their head at the right distance to the camera, and position their eyes in the

correct camera field of view. This means that it is each traveller's task to make sure of the iris acquisition quality. This could be a complex or intrusive process for many travellers. This can potentially slow down the entire e-Gate process.

On the other hand, iris cameras that work in a distance of up to 2 metres requiring less cooperation with the user are in a price range of 15 €K to 40 €K. These cameras are also very big and heavy, because of mechanical camera moving equipment and special near infrared light beamers. This makes them unpractical for wide deployment across borders. As iris requires its own special equipment and illumination, this also makes it challenging to integrate iris in any existing systems. Therefore, it is important to design the system to allow iris capture harmonised along with other biometrics and their existing capturing sensors and illumination

Another practical reason why we have not been able to use iris widely is that iris is not currently stored in travellers' ePassport. In addition, the majority of the public are not yet well aware of the facts about iris, for instance, what iris recognition is, how secure it is, if it is safe to use, and how the privacy concerns would be addressed. Previous research has suggested that people are much more accepting of those biometric systems that they are aware of (e.g. fingerprint) and which are more convenient to operate (e.g. signature), rather than the systems that they believe to be more secure (e.g. iris). The acceptance of using iris by the public is very limited currently [Furnell & Evangelatos 2007]. In order to improve this, convenience and practical experience are essential requirements for the public acceptance. Smart phones have recently started using iris as an option for device authentication (e.g. Samsung Galaxy S7), this should help raise public awareness of the advantages of iris recognition.

Above all, we can see that it is a very challenging task to implement practical iris recognition in ABC, especially under a reasonable cost. However, because of its robustness and uniqueness, iris is highly recommended to be deployed in a border control system. Novel iris recognition technologies should be adopted to balance between recognition reliability, usability and cost.

Based on the developments and operational observations, the following is recommended:

- Iris is a more robust and accurate biometric trait as a person identifier compared to other biometric traits, e.g. face. Thus, iris should be included in an ABC system.
- Image quality is very important for accurate iris recognition, and it can largely affect the segmentation of the iris pattern.
- Strong near infrared illumination is very important for capturing good iris image quality and against external light influences, however, it also needs to ensure eye safety
- An iris system for ABC should be non-intrusive and require minimal cooperation from the users. This is also to ensure each operation speed and high throughput

- While maintaining iris image quality, iris recognition accuracy and usability, cost of an iris acquisition system needs to be reduced to make iris practical to be widely deployed in ABC

4.6 Innovations in the video surveillance area

Andreas Kriechbaum-Zabini, AIT

In traditional ABC solutions, CCTV cameras (video surveillance cameras) are used for monitoring of the entrance to the by border guards. Since there is no direct manual contact of any border guard with the passengers we recommend a different use of CCTV cameras for ABC:

The cameras should detect automatically the number of persons in the e-Gate area in an integrated border process like in manual checks (manual assignment 1 passenger/passport). The automatic detection – if exactly one person per passport is crossing the border – is a very useful support for the border guard if the false alarms are minimal. Total number of false alarms of the system should not be increased by an additional technology (passport reader, biometrics, video surveillance) and for this reason, false alarms should be in total < 5% (proposed FRR by Frontex for just for biometrics). For this reason, such an algorithm (for detection of number of persons) should be deployed and integrated for detecting tailgating and piggybacking – detection of the correct number of persons in very difficult cases e.g. persons are very close and touching each other.

Next, an ABC system should be able to detect if it is in a useable status e.g. if the gate is empty – For this reason a video surveillance system should be enhanced by a left object detection (e.g. detection of passports, trolleys in the eGate area) to allow passengers to pass the system if it is empty. With a 3D based approach it is possible to find small objects and large objects even in the same colour as the floor.

Last but not least, a guidance support is useful to shorten border waiting times for passengers. For this reason, a queue length detection system which can detect waiting times is needed. This system helps to automatically request the required number of open systems and therefore we know the optimum number of border guards. If the waiting time is shown at the border lane, the passengers know which border lane should be used to queue in a minimal time for a minimal border time.

The integration of video surveillance systems influences the construction of the e-Gate: Such systems are relying on stable illumination (shadows from outside or persons from second e-Gate, reflection from the floor).

Based on the developments and operational observations we recommend the following:

- Automatic video surveillance (person counting, left object detection) is a helpful tool to support the border guard if the false alarms are minimal
- Video based surveillance systems can visualise the results understandable to the border guard (just visualising a bounding-box in the area where the system detected the problem) and there is maybe no need for any additional sensor (observation camera is typically already in use)
- Queue-Length detection shall be used as a guidance service
- Queue-Length detection systems (detecting waiting time) can help to reduce the border crossing time for passengers
- Queue-Length detection systems can help to automatically open an optimal number of systems (border guards) for a desired waiting time
- Video surveillance tools should have a 3D approach in order to provide high quality results
- Plan the video surveillance systems already in the construction phase of the e-Gate: The integration of different systems relying on cameras should be setup at the same time: e.g. if the environment light is changed for best biometrical results it might change the quality of video surveillance results and vice versa. Different systems might influence each other: not every system needs IR reflectors -> filters are needed for some of them
- The integrator should design the video surveillance part in the entire system process in order not to influence the border process

4.7 Data fusion and alarming

Niko Reunanen, VTT

Biometric data fusion (BDF) combines multimodal biometric data, which include iris and face recognition results, into a single coherent representation. This fused representation encodes the characteristics of the multimodal data in a compact form. The fused and encoded information is a source of information for alarming, which automatically determines the risk level of a passenger. However, the alarming incorporates additional sources of information arising from events that are triggered independently (e.g. a person walking against the flow).

BDF and alarming are data-driven tasks. The availability of good data is the most important factor for successful research and development of BDF and alarming. It can be stated that some models work with good data but no model survives bad data. Therefore, for the success of the BDF and alarming, it is of paramount importance to implement and acknowledge the following recommendations:

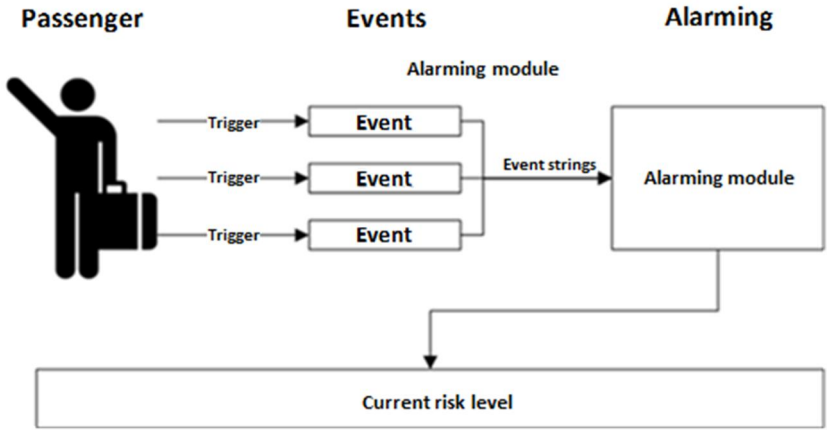


Figure 26. Alarming module fuses event data and triggers alarms based on optimized rulesets.

Based on the developments we recommend the following:

- Define carefully how to acquire the required data, which are the basis for the biometric fusion and alarming.
- Obtain data that characterize the inspected phenomena. The data for BDF should originate from properly functioning biometric recognition devices.
- Obtain data that does not have inconsistent or mixed information. For example, it is not possible to identify and discriminate two passengers from each other if they have identical records.
- Consider the availability of good data as a major asset in data-driven research work.
- Collect data as early as possible to enable the research of advanced data analysis models. The worst-case scenario is to acquire data near the end of project.
- The biometric fusion and alarming should be standardized for a set of biometrics and events. This allows rapid deployment and fine-tuning of the mathematical models.
- The ABC system should implement a convenient mechanism for updating their mathematical models. This would allow a mechanism to maintain multiple ABC systems simultaneously.

5. ABC implementation project

5.1 ABC implementation recommendation

Andreas Kriechbaum-Zabini, AIT

In the previous chapters, challenges in getting stakeholder interests (requirements), operational process definition and the resulting technical solution have been described. Nevertheless, a couple of important factors have additionally to be considered for the deployment of the system.

The local administration of an infrastructure (airport, port, etc.) needs to check the specification of the system if it is accepted by national. They might provide any technical constraints (e.g. type of glass) or safety constraints for the location (e.g. enough escape corridor). Before the installation, inspect the site where the ABC system will be deployed in order to get environmental conditions that may have an impact on parts of the system (e.g. direct sunlight impairing the quality of biometrics). Even though FastPass developed a harmonized concept, adaptions according to specific national requirements (e.g. interface to the background database, integration of door separating the international arrival area from the Schengen area) and operational needs from the operators are still important. In general, the success of the installation depends on a continuously, qualitative test and feedback by operational users.

Figure 27. E-Gate installation at Vienna airport.

Once all relevant stakeholders accept the technical system, the individual components of the overall system have to be delivered by individual suppliers. In order to clarify all responsibilities and the suppliers confirm the delivery of each component and therefore a deployment plan hast to be developed.

The most important part during the planning of the deployment phase is to acquire the requirements from the local stakeholders (e.g. airport, port, cruise ship, border infrastructure, and border guards) and their availabilities. With these requirements, the deployment plan has to be further extended (e.g. when each component will arrive, when the suppliers will deploy the system and when local stakeholders are needed for the deployment phase). This should include enough buffer time to handle unexpected delays.

It is advisable that the system is being tested in a laboratory before the installation on site. This allows you to not only verify the functional, performance, and reliability requirements, but will also help you to find any interferences that different technologies may cause (as an example, using biometrics with a strong IR light source may have a direct impact on other optical systems in the system).

Of course it is mandatory that after the deployment is finished, to do a system test. Here, the complete system is being tested thoroughly and in a structured way. In case hardware and software come from different vendors, it is recommended to test the complete system after the software integration. During this testing phase it is recommended that all involved partners are on site, in order to configure the system and to be able to handle unforeseen issues. If the system is in an operational, it is helpful to make first test runs with real travellers, closely monitored by the end-users and the technical staff. After these tests, an additional acceptance test by an independent party is needed to receive the approval by the end-users and ordering

party. The results should be discussed with all involved parties, end-users, system providers and major stakeholders.

Once customer accepts the system, and allows to starts the operation of the system, it is recommended to limit the operational time in the very beginning and having system integrators on site. Provide a first level support to the customers, and define a process for a support. Quick and responsive support is crucial for the successful operation of an ABC system – for this reason do not under estimate the budget for maintenance. Furthermore, it is mandatory to train the end-users and provide an easily comprehensible, but nevertheless complete user manual.

Based on the experience in deploying an iteratively enhanced solution for operational use at the Vienna International Airport (3 years), setting up a demonstration for cruise ship-scenario and for the land border scenario the following recommendations are presented:

- Gather all technical requirements from end-users and involved local stakeholders (e.g. integration of a “Schengen door”)
- Requirements for deployment by stakeholders (e.g. day-time, when the partners can work, storage, addresses)
- Make a deployment and a risk management plan and follow it throughout the project
- Acceptance of the local administration to the technical concept and the location
- Test of a system prototype by end-user
- Testing the system by SW-integrator and with relevant partners together at the spot to configure the system
- Acceptance test (with friendly cooperative users)
- Confirmation of the end-user to start a limited operation with integrator
- Training on the working system
- Technical contact during operational time and a clear process how to handle problems of the system

5.2 Training as a part of the implementation project

Arabelle Bernecker, ICMPD

All training was based on tailor-made Standard Operating Procedures and Training Manuals, which had been developed for each scenario. The topics covered always included (but were not limited to) the following:

- Overview of the FastPass project;

[6] A door in addition to the ABC system that separates the Schengen area from the Non-Schengen area in a terminal. This is a national requirement in some countries.

- Aim and basic functions of the e-Gates and kiosks of the scenario at hand;
- Components of the installation;
- Standard processes ('green process');
- Deviating processes ('red process');
- Emergency procedures;
- Basic troubleshooting procedures.

A typical end-user training session would take 2 hours for up to five border guard participants. For future trainers, in contrast, it could last up to six hours, broken down into several parts and including also presentations, to provide the participants with a solid theoretical background and the opportunity for additional questions and deeper discussions.

In both cases however the focus was on making the sessions as practical and hands-on as possible. Trainees got a chance to use and test the e-Gates and kiosks not only from the perspective of a border guard, but also from the perspective of a traveller. Furthermore, in most cases it was also possible to go 'live', by inviting actual passengers to use the kiosks and e-Gates.

After each training feedback was collected from the participants in writing (by questionnaire) or verbally, on the following topics:

- Level of understanding of the e-Gate processes;
- Motivation to use the e-Gate in the future;
- Training-related technicalities like group size, venue and duration of the sessions;
- Recommendations.

The feedback was very positive as far as the training itself and the trainers were concerned: not only did the concept, group size and settings receive high ratings, the vast majority also reported feeling motivated to use the e-Gate and confident about their understanding of its processes. Whenever relevant and feasible, recommendations were used to further improve the trainings.

Based on the experience gained during the implementation of the trainings, and the feedback received from the participants, a number of lessons were learned, which could be of relevance for future border guard trainings on automated border controls.

- Motivation is a key element for success: Many border guards are suspicious of or have reservations against automated border controls. Getting them on board at the beginning of the training therefore is essential.
- Learning by doing: The training should be as practical as possible. The time spent letting the trainees "play" with the e-Gate, e.g. by posing as travellers of by trying to outsmart it, is well spent because it not only familiarised the BGs with its functions, but also creates trust in the system.
- The group size needs to be small, to allow everybody to use and test all elements of the e-Gates and Kiosks.
- All trainees should furthermore be able to fit comfortably into the BG booth or the control room, with proper view of the e-Gate and Kiosk screens. This can mean holding a series of sessions for groups of maximum 5 border guards. This small group size makes it also possible to keep the disruptions to the border guards' shift plans to a minimum.
- It is important to see the installation work "live", not only in test mode. In FastPass, the processing of actual travellers was already done whenever the opportunity presented itself. Based on this positive experience, it is recommended that it should be a fix, scheduled element in all training.
- For practical purposes – especially in the case of a 2-step process (Kiosk and e-Gate) it is convenient to have 2 trainers: one demonstrates certain scenarios, while the other one explains.
- If e-Gate assistants are employed guiding the travellers through the automated border control, their training (and motivation!) is crucial.
- Since the training success absolutely depends on the functioning of the kiosk and e-Gates, the presence of technical support during the whole training should be considered a requirement.

5.3 End user acceptance testing

Sirra Toivonen, Mika Rautila, VTT

The FastPass system underwent thorough acceptance testing before the systems were put into operational use at the different border demonstrations. When high security systems are implemented, testing of the systems is of crucial importance. It is a formal testing with respect to user needs, requirements, and business processes, and is conducted in order to determine whether a system satisfies the acceptance criteria and to check whether the system is acceptable to the users.

In general, acceptance testing is a pure functional testing to check the system behaviour using real data. End users perform acceptance testing to check whether the system is built to match the business requirements of the organisation. In this testing, all the interfaces are combined and the complete system is tested. The end users also execute the tests to check the usability of the system. This type of testing focuses mainly on the validation testing of the system [Myers et al. 2011].

The design of test cases that completely test a system is often a very difficult task. The full complement of acceptance tests may test individual features, combinations of features, or total system operation and may even specify examinations that do not require program execution [Myers et al. 2011].

In FastPass, each test case consisted of the overall scope, a description of the requirements against which the test was performed, features to be tested, and a procedure description and erroneous result. The procedure description contains input and expected output data, and details for each test step. The tests were planned carefully – a test protocol was created that covered not only the usual use cases but also the unexpected and intentional misuse cases. It was important that the plan covered the system usage comprehensively. The tests in FastPass were organised by the project and followed by the border guard end user organisations. In Vienna airport, the Interior Ministry also performed tests as there the system was operational and connected to the background systems.

The acceptance testing used a testing protocol that took into account the different usage scenarios of the system as well as possible ways to bypass its security features. The test protocol served for systematic execution of the tests. Clearly defined procedures for the individual test cases enabled methodical execution of the tests, repetition of the tests at different demonstration sites, and identification of problems. The aim was to provide clear information to perform the test, to define which tasks should be better defined and to enable implementation, repetition and easy adaption to different border installations of the tests by different stakeholders in the project. The acceptance tests were performed with the system when the individual equipment and systems had been tested by the technology providers, and the main emphasis of the tests was in testing the system integration with defined use cases. These use cases were adapted to the border type specific configuration.

The test protocol was planned in order to test both the whole system and the individual equipment. The system sub-component technology providers had already tested and assessed their components against the system performance objectives. This meant that the acceptance tests were built upon the tests made by the technology providers.

The acceptance tests concentrated on the correctness, completeness, functionality, performance, reliability, security and usability of the system. The test cases were derived from the FastPass system requirements and the developed processes. The aim of the tests was to guarantee that the final ABC solution corresponds to the defined requirements, and that all procedures are carried out correctly. In the test protocol document, the system test plan of the proposed ABC-system for the pilot was described in order to test the necessary integrated elements of the system. Each test case included the following information: test name, relevant

system requirements, description of the test procedure with test objectives and description of the erroneous actions or outcomes. Additionally, it provided the acceptance protocol in order to provide a test tool for the system. In FastPass it was decided that the acceptance tests would be performed in the implemented systems after system tests but before their introduction to operative usage. In addition, time for corrective measures was reserved.

Acceptance tests were recorded with multiple synchronised cameras (Figure 28). This was important as the system is operated in a different place to that which is monitored. Furthermore, in the two-step systems, the operation occurs in two places and the monitoring also uses two separate monitors. With the help of a camera system, all of the events could be evaluated professionally. The figure below shows the installation of one camera that was installed to record the operations at the movable terminal in the land border acceptance tests.

If the acceptance tests were to be used for final acceptation of a border check system, they would have to be formally executed. Furthermore, the acceptance criteria would probably have been stricter than the ones that were used here. In this case, the acceptance test in the project also served to provide information concerning how the user is interacting with the system, which issues occur, and what improvements might be recommended to enhance the user experience. However, the actual tests with travellers were performed separately.

Figure 28. Acceptance tests were recorded with multiple synchronised cameras. The picture also shows the moving land border traveller terminals equipped with passport readers, cameras and intercom.

Based on the acceptance tests during deployment of ABC at different border types we propose a number of recommendations:

- Perform systematic acceptance tests with a suitable protocol before operational use and acceptance of the system
- System tests must be passed before starting acceptance testing.
- Reserve the necessary personnel to participate in the test: end user, authority, technical support, etc.
- If necessary, film the tests for better analysis possibilities afterwards
- Take into account the test equipment needed: fake passports, additional lights, pictures of passport photos, beards, different glasses etc.
- The system might act differently when it is connected to the background databases. Therefore it is recommended to test the system in its real operational settings.

6. Conclusions

The challenge to design and harmonise automated border control systems at different border types can be resolved. The use of novel document readers, biometrics and advanced information processing for ABCs can enable more efficient, secure, cost effective and fast border control processes for travellers, while increasing the passenger flow and reducing the burden on border guards. It will, however, require the analysis of a wide spectrum of information, cooperation with various stakeholders and deep understanding of the problems and of the technological resources needed. On the other hand, the building of harmonised systems for borders may be more challenging than expected, because systems are tailor made and they must be adapted to the needs of individual borders.

This report aims at providing the versatile information in the form of recommendations for the different stakeholder groups targeting to develop or implement automated solutions in the future. In order to support the ABC and self-service system development and uptake in general, it also provides background considerations for example about the political and operational landscapes. Legal implications of ABCs must be carefully considered. The gathering, storing and utilization of data should be undertaken in accordance with relevant best practices. Furthermore, it is essential that the introduction of ABC technology in the EU should comply with a number of legal requirements that have been derived from the current legislation on privacy and data protection, and other fundamental rights. In addition to this, the operational landscape is evolving rapidly. As an example of this, the new General Data Protection Regulation (GDPR) requires the conduct of a Data Protection Impact Assessment (DPIA) as of May 2018 for all new ABC deployments.

The project hopes to have shown the way forward towards designing highly acceptable solutions and technologies. We have seen border checks being automated in many large European airports already, and, automating of the border checks will be accelerated if or when the current proposals of Smarter and Stronger borders with Entry-Exit-systems and ETIAS proceed. The proposals push forward a change which would incorporate a large number of new TCN travellers in self-service and automated systems. With the growing number of people crossing the borders, the need for an easy and smooth, but at the same time secure border check is effectively addressed by automation. This means that certain challenges must be resolved as increasingly varied traveller groups begin to use the combinations of self-

service solutions, for instance kiosk and e-Gate processes. The viewpoints and recommendations presented in the report will provide background based on our real life experiences when implementing the systems in accordance with the new legislative framework. However, as has been noted in the responses of many interviewees during the project, the way forward should take into account also the broader impact of the use of technology, both on individuals and on society at large.

The report is targeted to different stakeholder groups that design and implement automated systems. The recommendations are based on the project experiences and the structure of the reports is chosen to support the development and implementation processes. The operational harmonisation starts from the stakeholder needs and operational environment aspects. Environmental conditions must also be accounted for, especially in outdoor settings where the impacts of extreme temperatures, dust, rain, snow and wind may influence the operability and longevity of ABC devices. Harmonised processes expand the viewpoint at additional border types. Vehicular traffic at land borders poses additional challenges when border guards must be able to ascertain the identity and number of passengers travelling in a vehicle and the goods being transported, as well as to ensure that the vehicle's documents are in order. Functional and non-functional system requirements are presented, again with an emphasis on differences between the land, sea and air border crossings.

Harmonised usability and user experience (UX) considerations need to reflect the perspectives of both the passengers and the border guards. The potential to gain efficiency and fluency of traveller flows at border check points with usability considerations is definite. When making efforts to rise these to a higher level the user interface and interaction designs as well as adaptable guidance realisation cannot be underestimated. The report and the proposed best practices drive towards making self-service a self-evident choice for passengers crossing the borders at European border crossing points. The concepts aim at providing a harmonised and fluent border crossing for frequent and also for non-frequent travellers, who may be less accustomed to different passenger processes and expected behaviour at border crossings. For border guards it provides solutions to customise a border guard user interface at different border types.

Recommendations are also provided for the automated border control technologies and their implementation. The harmonisation of system architecture supports ABC gates for different implementations (air, land, sea) and provides generic interfaces for facilitating and harmonising the integration of software and hardware components for e-Gate solutions with and without kiosks. And although the report concentrates on the automated solutions the harmonised architecture also supports manual control.

The technologies enable new possibilities to identify the traveller, authenticate that he or she is the rightful owner of the travel document and ensure anti-spoofing of the system. Advances on biometric identification, surveillance and data fusion enhance the security of the deployment. The risk analyses with IT- and user-related threat identification support development of a harmonised security standard for ABCs.

The need for automated solutions and self-service processes is at all borders independent of the border type. At other borders than the airports, it has not been easy to find the best and most suitable solution and processes. The passenger profiles, border processes, infrastructures and operational environment must first be carefully examined and innovative opportunities must be evaluated. We hope that this report will serve as necessary background but also as a source of inspiration.

E-Gate designs need to be adapted to the border specific needs. For this reason, the recommendations give a profound view to physical hardware design, taking into account the specific properties of the different border types. The report also provides detailed technical considerations for ABC gate and housing hardware at different border types. For the terminal environment at airport, that already have commercial solutions are available, the development focused on European wide application and technical solution to facilitate traveller flows to and from Schengen area. The concept was demonstrated by e-Gates from two different providers. For the cruise ship a rapid and innovative border check concept with pre-checks during the voyage and a biometric (face) based check at the e-Gate was evaluated. The concept included mobile monitoring of the e-Gate flows which enable border guard to intervene manually if necessary. In addition, the project also demonstrated a foldable e-Gate construction that enables moving the e-Gate to different operational sites according to the needs of the border authority. The report also presents a novel solution for an ABC to conquer the challenges of the land border ABC. Due to the requirement that travellers should stay in their cars and the fact that each car has different dimensions, the devices for the border process have to be automatically moveable and their position adjustable for different cars and they must work reliably outdoors.

With reference to the experiences from successful demonstrations at different borders (a demonstration in Vienna International Airport (3 years) for air border, a demonstration for cruise ships in Piraeus Port and on the Cruise Ship and for the land border in Moravita), the report also shares the implementation experiences. Like any implementation project, the ABC design and implementation project needs careful planning and pushing through with commissioning tasks.

Many challenges still need to be considered and handled in order to reach a unified, standardized and harmonized approach to border control automation. Different border types have different passenger profiles and different needs for both the border guard and the passenger. The existing environment, infrastructure, practices and information systems must also be considered; there is no solution that could replace all that has been in use before. By publishing this information, knowledge and experiences of the FastPass solutions and demonstrations, the report aims to contribute to the harmonisation of the automated and self-service solutions of the future.

Along with other actors in this area, FastPass has been an important part of ABC development in Europe, and has provided indicators for the way ahead. When implementing ABCs, many issues need to be considered in order to guarantee that the system is financially efficient, accepted by all users including both the travellers and the border guards, and provides smooth traveller flows. In general, in this report we do not make a comparison between benefits of automated and manual control

but look mainly at the criteria and possibilities to implement harmonised automated border control technologies at different European borders. Innovative technologies must be developed and implemented. It aims to provide both general aspects that must be taken into account and the information needed for the system development and implementation, as well as details of the system and technology aspects.

As cross-border travel is expected to increase in the coming decades, there is much positive potential to further implement technological solutions at border crossings. The possibility for fast and smooth border crossings, with a high level of security and social acceptance, is a core aim of a standardised ABC process. Socially accepted, reliable, flexible, and harmonised solutions are needed to ensure this aim. We are confident, that our recommendations can contribute further steps to guide the future solutions towards this goal.

Acknowledgements

We thank the following organisations for providing a platform and support for the project pilots:

Hellenic police,
Celestyal Cruises and
Piraeus Port Authority S.A

References

Automated border control implementation guide. 2015. International Air Transport Association. Retrieved from http://www.iata.org/whatwedo/passenger/Documents/ABC-Implementation-Guide-2nd-Edition.pdf .

Blut, M., Wang, C., Schoefer, K. 2016. Factors Influencing the Acceptance of Self-Service Technologies. Journal of Service Research, 19(4): 396–416.

BS-EN 12453:2001. 2001. Industrial, commercial and garage doors and gates. Safety in use of power operated doors. Requirements.

BSI TR-03135. 2014. Machine authentication of MRTDs for public sector applications, version 2.0, German Federal Office for Information Security. Retrieved from https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03135/index_htm.html.

BusinessDirectory. http://www.businessdictionary.com.

Cambridge dictionary. http://dictionary.cambridge.org/dictionary/english/harmonization.

Canadian Transportation Agency. 2015. Implementation Guide Regarding Automated Self-Service Kiosks. Retrieved from https://www.otc-cta.gc.ca/eng/publication/implementation-guide-regarding-automated-self-service-kiosks .

Clabian, M. 2016. The FastPass project – Research on ABC Systems to secure EU borders and improve border-crossing efficiency. SMI Boder Security Conference. Rome, Italy.

COM/2016/0194 final. 2016. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0194&from=EN .

COM/2016/731 final. 2016. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624. Brussels, 16.11.2016.

COMMISSION RECOMMENDATION of 06/XI/2006. 2006. Establishing a common "Practical Handbook for Border Guards (Schengen Handbook)" to be used by Member States' competent authorities when carrying out the border control of persons. (2006) Retrieved from http://ec.europa.eu/transparency/regdoc/rep/3/2006/EN/C-2006-5186-F1-EN-MAIN-PART-1.PDF.
amendment: COMMISSION RECOMMENDATION C (2015) 3894 final. Retrieved from http://ec.europa.eu/transparency/regdoc/rep/3/2015/EN/3-2015-3894-EN-F1-1.PDF.
amendment: COMMISSION RECOMMENDATION C (2012) 9330. Retrieved from http://ec.europa.eu/transparency/regdoc/rep/3/2012/EN/3-2012-9330-EN-F1-1.PDF.

Davis, F.D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3): 319–340, doi:10.2307/249008.

EU 2016/399. 2016. Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), O.J. L 77, 23.3.2016.

EU 2016/679. 2016. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

EU 7864/09. 2009. EU Schengen Catalogue External borders control. Return and readmission. Recommendations and best practices. 7864/09. Retrieved from http://www.schengen.mai.gov.ro/English/Documente/utile/catutil/Updated%20EU%20Schengen%20Catalogue.pdf.
Updated Catalogue of recommendations for the correct application of the Schengen acquis and best practices: part on the Schengen Information System. 15443/02 SCHEVAL 43 SIS 97 SIRENE 75 COMIX 703. (2015) Retrieved from http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2016613%202008%20REV%202 .

European Court of Human Rights. 1976. Handyside vs the United Kingdom. Application No. 5493/72, 7 December 1976, par. 48.

Frontex. 2013. Frontex 8th Workshop on Automated Border Control (ABC) and Cost Benefit Analysis (CBA) demonstration/training. Sofia, Bulgaria. 24–26 April 2013.

Frontex. 2015a. Best Practice Operational Guidelines for Automated Border Control (ABC) Systems. Warsaw. Retrieved from http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_ABC.pdf.

Frontex. 2015b. Best Practice Technical Guidelines for Automated Border Control (ABC) Systems. Warsaw. Retrieved from http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_ABC.pdf .

Frontex. 2016. Guidelines for Processing of Third Country Nationals through Automated Border Control, ISBN 978-92-95205-50-5. Retrieved from http://frontex.europa.eu/assets/Publications/Research/Guidelines_for_Processing_of_Third_Country_Nationals_through_ABC.pdf .

Furnell S., Evangelatos, K. 2007. Public awareness and perceptions of biometrics. Computer Fraud & Security, 2007(1), January 2007: 8–13. ISSN 1361-3723.

Gariup, M., Soederlind, G. 2013. Document fraud detection at the border: preliminary observations on human and machine performance. Proc. European Conf. Intelligence and Security Informatics (EISIC), (pp. 231–238). Uppsala.

Hassenzahl, M. 2008. User experience (UX): towards an experiential perspective on product quality. In Proceedings of the 20th Conference on l'Interaction Homme-Machine (pp. 11–15). ACM.

ICAO Doc 9303. 2015. Machine readable travel documents, 7th edition. International Civil Aviation Organization. Retrieved from http://www.icao.int/publications/pages/publication.aspx?docnum=9303 .

IEC 31010:2009. 2009. Risk management – Risk assessment techniques. International Organization for Standardization.

ISO 31000:2009. 2009. Risk management – Principles and guidelines. International Organization for Standardization.

ISO 9241-11:1998. 1998. Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on Usability. International Organization for Standardization.

ISO/IEC 10746-1:1998. 1998. The Reference Model of Open Distributed Processing. International Organization for Standardization.

ISO/IEC 27005:2011. 2011. Information technology – Security techniques – Information security risk management. International Organization for Standardization.

Myers, G.J., Sandler, C., Badgett T. 2011. The Art of Software Testing. Wiley. ISBN: 978-1-118-03196-4.

Passenger facilitation. 2017. Retrieved from International Air Transport Association (IATA) website http://www.iata.org/whatwedo/passenger/Pages/passenger-facilitation.aspx.

Taylor, B. 2016. Developing qualitative criteria for assessing the impacts and acceptability of border control technology. Tampere University. http://urn.fi/URN:NBN:fi:uta-201608152165 .

Ylikauppila, M., Toivonen, S., Kulju, M., Jokela, M. 2014. Understanding the factors affecting UX and technology acceptance in the context of automated border controls. In Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint, (pp. 168–175). IEEE.

Appendix A: Legal Instruments

The following lists the legal instruments in Europe related to automated border checks.

SCHENGEN ACTS

Regulation (EU) 2016/399 f the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), O.J. L 77, 23.3.2016.

Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, O.J. L. 385, 29.12.2004.

Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, O.J. L. 142, 6.6.2009.

Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), O.J. L. 381, 28.12.2006.

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), L 205, 7.8.2007.

Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), O.J. L. 218, 13.8.2008.

Commission Decision of 9 October 2009 laying down specifications for the resolution and use of fingerprints for biometric identification and verification in the Visa Information System, 2009/756/EC, O.J. L. 270/14, 15. 10. 2009.

European Commission, “Practical Handbook for Border Guards (Schengen Handbook),” C (2006) 5186 final, Brussels, 6.11.2006 and its updates.

PROPOSED ACTS

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System, COM (2016) 196 final, Brussels, 6.4.2016.

Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, COM (2016) 194 final, Brussels, 6.4.2016.

Proposal for a Regulation of the European Parliament and of the Council amending Regulation No 562/2006 (EC) as regards the reinforcement of checks against relevant databases at external borders, COM (2015) 670 final, Brussels, 15.12.2015.

Proposal for a Regulation of the European Parliament and of the Council establishing a touring visa and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 562/2006 and (EC) No 767/2008, COM (2014) 163 final, Brussels, 1.4.2014.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Union Code on Visas (Visa Code), COM (2014) 164 final, Brussels, 1.4.2014.

Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorization System (ETIAS) and amending Regulations (EU) 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM (2016) 731 final, Brussels, 16.11.2016.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the use of the Schengen Information System for the return of illegally staying third-country nationals, COM (2016) 881 final, Brussels, 21.12.2016.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006, COM (2016) 882 final, Brussels, 21.12.2016.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, COM (2016) 883 final, Brussels, 21.12.2016.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, COM (2017) 8 final, Brussels, 10.01.2017.

DATA PROTECTION ACTS

Charter of Fundamental Rights of the European Union, O.J. C 364, 2000/C364/01, 18.12.2000.

European Convention on Human Rights, Council of Europe, 4.11.1950.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data, O.J. L 251, 23.11.1995.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. L 119, 4.5.2016 (applicable only as of May 2018).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, O.J. L 119/89-131, 4.5.2016 (applicable only as of May 2018 and only in case personal data are processed for law-enforcement purposes).

Appendix B: Partners of the FastPass -project

The following organisations have participated in the research work in the FastPass Project:

	Partners	Contact person
	AUSTRIAN INSTITUTE OF TECHNOLOGY	Markus Clabian (project coordinator)
	TEKNOLOGIAN TUTKIMUSKESKUS VTT OY	Sirra Toivonen
	BUNDESMINISTERIUM FUER INNERES	Johann Riedl
	OESTERREICHISCHE STAATSDRUCKEREI GMBH	Sebastian Zehetbauer
	FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V	Gunther P. Grasemann
	KATHOLIEKE UNIVERSITEIT LEUVEN	Els Kindt
	MINISTRY OF THE INTERIOR, FINLAND	Minna Jokela
	SECUNET SECURITY NETWORKS AG	Petr Vyletal
	MIRASYS OY	Mari Matinlassi
	REGULA BALTIJA SIA	Maris Kaminskis

	THE UNIVERSITY OF READING	James Ferryman
	INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT	Maegan Hendow
	UNIVERSITY OF TAMPERE	Pami Aalto
	GUNNEBO ENTRANCE CONTROL LIMITED	Kevin Taylor
	VERIDOS	Michael Brandau
	MODI MODULAR DIGITS GMBH	Dieter Klawunder
	Magnetic Autocontrol GmbH	Thomas Bürgin
	JRC -JOINT RESEARCH CENTRE-EUROPEAN COMMISSION	Günter Schumacher
	ITTI Sp.zo.o.	Lukasz Szklarski
	DELTABIT OY	Jukka Hosio
	THE CHANCELLOR, MASTERS AND SCHOLARS OF THE UNIVERSITY OF OXFORD	Anne-Marie Oostveen

	INSPECTORATUL GENERAL AL POLITIEI DE FRONTIERA	George Ion
	FINAVIA OYJ	Timo Koivisto
	DIMOTIKO LIMENIKO TAMEIO MYKONOU	Nikos Vardalachos
	FRAPORT AG FRANKFURT AIRPORT SERVICES WORLDWIDE	Vinh Nguyen-Xuan
	FLUGHAFEN WIEN AG	Manfred Wimmer
	INTREPID MINDS LTD	Chris Hurrey

Series title and number

VTT Technology 303

Title	**Recommendations for future ABC installations** Best practices
Author(s)	Sirra Toivonen & Heta Kojo (Editors)
Abstract	This best practice report summarises the practical findings and results of the FastPass-project in the form of best practices and recommendations. It provides recommendations to design, deliver and implement automated border control systems based on the research and practical demonstrations at air, land and sea border checkpoints. It aims at providing the productive information for the different stakeholder groups targeting to develop or implement automated solutions in the future. Putting the user in the centre of the developments, considering versatilely the aspects of social and legal implications and integrating the views of all involved stakeholders, FastPass settled the requirements of a harmonised next generation ABC system. It bases its results on a profound analysis of policy development, legal requirements and data protection analysis. The report also gives recommendations on the technology areas of passport scanning, biometrics, video surveillance, sensors and ABC hardware that can be implemented in current and novel processes. This document will look at the automated border control development and implementation with an interdisciplinary approach, taking into account the underlying factors as well as operational, technical, conceptual and organisational aspects to be addressed when developing automated systems for different borders. Harmonisation of the ABC designs between various border type implementations is one of the key answers to conquer the efficiency, security and financial conditions of ABC implementation. The report hopes to show the way forward towards designing highly acceptable and effective ABC systems for various needs.
ISBN, ISSN, URN	ISBN 978-951-38-8559-5 (URL: http://www.vttresearch.com/impact/publications) ISSN-L 2242-1211 ISSN 2242-122X (Online) http://urn.fi/URN:ISBN:978-951-38-8559-5
Date	June 2017
Language	English
Pages	113 p. + app. 6 p.
Name of the project	FastPass
Commissioned by	European Union’s Seventh Framework Programme
Keywords	Automated border control, harmonised reference system, best practices, recommendations, FastPass
Publisher	VTT Technical Research Centre of Finland Ltd P.O. Box 1000, FI-02044 VTT, Finland, Tel. 020 722 111

VTT TECHNOLOGY 303

Recommendations for future ABC...

Recommendations for future ABC installations

Best practices

ISBN 978-951-38-8559-5 (URL: http://www.vttresearch.com/impact/publications)
ISSN-L 2242-1211
ISSN 2242-122X (Online)
http://urn.fi/URN:ISBN:978-951-38-8559-5