



Co-funded by
the Internal Security Fund
of the European Union



Smart Borders Pilot Project

Report on the technical conclusions of the Pilot

Volume 1



ISBN 978-92-95203-94-5

doi: 10.2857/086263

© European Agency for the operational management of large-scale IT systems
in the area of freedom, security and justice, 2015

Reproduction is authorised provided the source is acknowledged.

The opinions expressed are those of the author(s) only and should not be considered
as representative of the European Commission's official position.

Table of Contents

Executive Summary	5
Background	5
Smart Borders: a unique and large-scale EU pilot	6
Pilot results	6
Key findings from operational testing.....	7
Key findings from desk research	13
Survey conducted by the FRA – key findings.....	14
Conclusion.....	14
1. Introduction	15
Background	15
Objective.....	15
Scope	15
Out of Scope	17
Attention points	17
2. Operational testing	20
2.1 Fingerprints.....	21
2.2 Facial image	38
2.3 Iris pattern.....	49
2.4 ABC gates	58
2.5 Kiosk	67
3. Desk research	83
3.1 Fall-back scenario.....	83
3.2 VIS border check using travel document number	101
3.3 Web service.....	109
3.4 Equipment and costs	128
3.5 Spoofing vulnerability of iris enrolment and counter-measures	135
3.6 Reading chips in e-passports	148
4. Conclusion of the Pilot	161
4.1 Biometric-identifier outcome	161
4.2 Process-accelerator outcome	163
4.3 Desk-research outcome	164
4.4 Summary	165
4.5 Considerations for the future of Smart Borders	166

Page intentionally left blank

Executive Summary

Background

Border management is currently going through significant transformation. To address the need for the Schengen Area to move towards more modern¹ and efficient border management by using state-of-the-art technology, the European Commission proposed the 'Smart Borders package' on 28 February 2013. This package contained legal proposals for establishing two systems that should help to speed up, facilitate and reinforce border-check procedures for third-country nationals (TCNs) travelling into the Schengen Area:

- **EES** – a central entry/exit system to record the time and place of entry and exit of all third-country nationals travelling to/from the Schengen Area;
- **RTP** – a uniform registered traveller programme to allow pre-vetted and frequent travellers from third countries to enter (and exit) the Schengen Area with minimal border checks.



In order to further assess the technical, organisational and financial impacts of the various possible ways to address border-management challenges, the Commission subsequently initiated – with the support of the European Parliament and the Member States – a proof-of-concept exercise aimed at identifying, assessing and testing technical options for implementing the Smart Borders package.

This exercise consists of two phases:

First phase – a Commission-led Technical Study aimed at identifying and assessing the most suitable and promising options and solutions, as well as cost estimates. This study was delivered at the end of 2014; and

Second phase – a pilot (also called 'testing phase') entrusted by the Commission to the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA).

The main objective of the pilot was to test a limited set of technical options (identified within the Technical Study) against specific measurable criteria in operational and relevant environments. These criteria are accuracy, effectiveness and impact on border-crossing duration. The testing phase aimed to contribute to defining the best technical solutions for faster and more secure border-control processes, respecting the highest principles on data protection and fundamental rights.

The Commission announced it would submit a modified legal proposal by early 2016 which – once adopted by the co-legislators – would allow eu-LISA to develop the system and start operations by 2020.

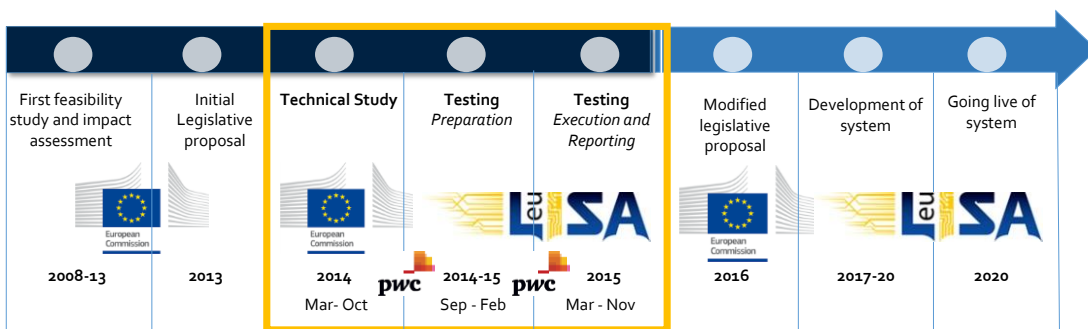


Figure 1 Indicative timeline of the establishment of Smart Borders

¹ e.g. removing manual stamping and increased reliance on automated verification and identification methods.

Smart Borders: a unique and large-scale EU pilot

The targets and challenges set for the pilot were high and unique. More than 100 questions had to be addressed through either desk research or operational testing (or both). The limited technical options to be tested and

Smart Borders Pilot in a nutshell

Scope	Air, sea and land borders crossing points (BCPs)
Member States	12 (DE, EE, EL, ES, FI, FR, HU, IT, NL, PT, RO, SE)
Border crossing points	18
Test cases	78 test variations
TCN travellers	58.000
Border guards involved	About 350
Biometrics	Fingerprints (FP), facial image (FI) and iris
Process accelerators	ABC gates, kiosks
Desk research	Spoofing, VIS and travel document number, web service

researched amounted to 13 different test cases (TCs), such as the enrolment of four, eight and ten fingerprints, or the use of self-service kiosks.² It required the involvement of numerous stakeholders.

Therefore, eu-LISA involved the EU institutions and other agencies in both the preparation and execution phases, such as the European Data Protection Supervisor (EDPS), the Fundamental Rights Agency (FRA) and

Frontex. Progress reports were regularly communicated to the European Commission, the Member States as well as to the European Parliament. The tests in the pilot were carried out successfully across Europe in 12 volunteering Member States between March and September 2015.

The scope did not include end-to-end³ testing with real data from travellers. The pilot was conducted in compliance with existing legislation. Traveller participation was completely voluntary. All the tests were conducted by the Member States under the close supervision and cooperation of national data-protection authorities.

The pilot lived up to expectations: it managed to deliver evidence-based results based on high participation rates from travellers, who were of various nationalities and all ages. One out of two travellers also provided feedback, and 89% of respondents said that they were satisfied or very satisfied with their experience of the pilot. Participating border guards expressed positive feedback. eu-LISA also invited the FRA to look into the use of

biometric technology on third-country nationals at the borders. The aim was to complement the third-country nationals' experience of the pilot with perceptions regarding the use of modern technology. Following this, the FRA carried out an independent small-scale survey at seven border-crossing points where the Smart Borders pilot took place to look into attitudes of third-country national travellers regarding the use of biometrics at BCPs and their opinions on various associated fundamental rights aspects.

Pilot results

This report presents the results of operational testing and desk research, providing **an important evidence basis** for the feasibility of the system(s) and processes proposed by the Smart Borders package.

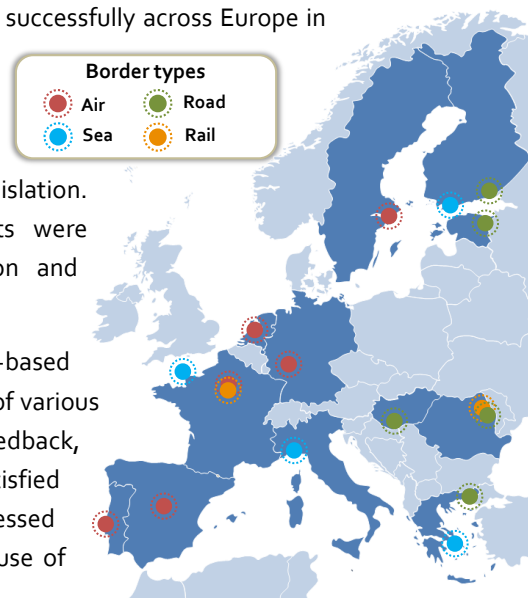


Figure 2 Participating Member States and types of border-crossing points

² All 13 Test Cases processes are depicted in the Methodology chapter and in BCP Chapters annexed to the main report.


³ An end-to-end pilot would have encompassed recording personal data at entry into a central database simulating the EES and matching this data at exit. In that instance, the tests would have required a mock-up central EES system to be set-up and personal data to be stored in that system. This would have required a specific legal framework allowing it.




















Where possible, the results have been consolidated according to the same biometric identifiers. However, due to the differences in border crossings (e.g. conditions, volumes, processes, integration and set-up level of new testing equipment), not all the results from the same test cases at the different border-crossing points could be compared.⁴ Instead, similarities and differences were considered from a duration, security or equipment-performance perspective.

Key findings from operational testing

Fingerprint (FP) enrolment

Table 1 Summary of locations per type of border where fingerprint enrolment was tested

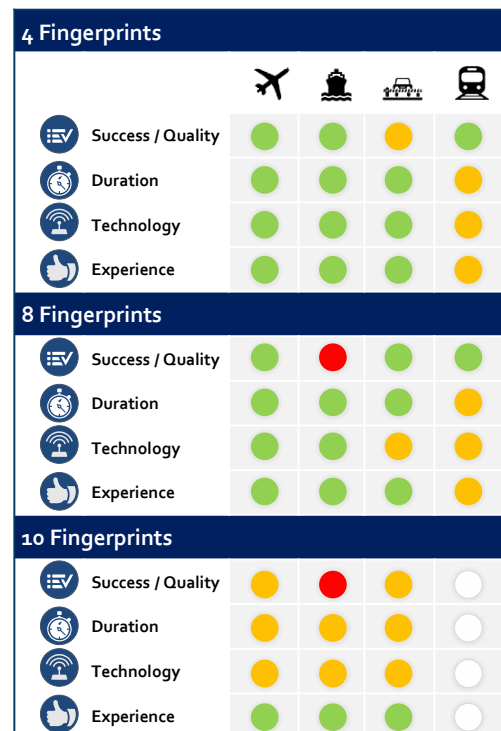
 4 fingerprints (TC1) – at 11 border-crossing points, 8 FPs (TC2) – at 8 BCPs, 10 FPs (TC3) – at 6 BCPs	
Air	Frankfurt (DE) Schiphol (NL) Madrid (ES) Charles de Gaulle (FR)
Sea	Helsinki (FI) Piraeus (EL) Genoa (IT)
Land (road)	Kipoi (EL) Udvar (HU) Vaalimaa (FI)
Land (train)	Iași (RO)
<p>Outcome: the pilot confirms that it is feasible to enrol fingerprints at all types of borders in various set-ups. However, in practice, enrolling four fingerprints is faster than enrolling eight or ten, although a higher number of fingerprints will deliver better accuracy for subsequent use. The quality of the fingerprints enrolled is generally fit for purpose. Enrolling fingerprints in controlled conditions is seen as the biometric identifier that is the least intrusive to travellers, according to both travellers’ and border guards’ feedback.</p>	

 Success / Quality	 ≥ 75%	 ≥ 50% - <75%	 <50%	 N/A
 Duration	 < 30 s	 ≥ 30 s - <60 s	 ≥ 60 s	 N/A
 Technology	 Mature	 Medium maturity	 Low maturity	 N/A
Experience	 ≥ 65%	 ≥ 35% - <65%	 <35%	 N/A

Main findings

Success/quality

- The quality of fingerprint enrolment cannot be directly linked to the number of fingerprints enrolled;
- There are currently no certification standards for contactless scanners;
- When the success rate was below 30%, this was mainly due to set-up and technical constraints;
- Identification accuracy can reach around 99.3% based on performance predictions provided by a number of vendors and



⁴ In addition, a comparison of the results according to different biometric identifiers has been made with great caution due to the following factors:

- verification could only be tested for facial image and not for fingerprints and iris;
- only the vendors’ quality thresholds could be used for FI and iris;
- kiosks were implemented only in limited operational settings; and
- iris is the newest biometric type and mostly unknown to border guards, whereas FP and FI are already used (FP for verification against the VIS; and FI at ABC gates).

with a database containing four FPs each from 100 million records. When performing a verification of a known traveller, performance is known to be a fraction less than 100%.⁵

Duration

- The added duration of the border-control process is directly linked to the number of fingerprints enrolled and the desired quality: enrolling four FPs had the least impact on time and is considered to have a relatively limited impact⁶ on the border-crossing process, with the vast majority of cases being performed in under 30 seconds on average. At air borders, average durations ranged from 17 seconds for 4 FPs to 60 seconds for 10 FPs. At sea, duration ranged from an average of 20 (4 FPs) to 46 seconds (10 FPs), and at land borders from 21 (4 FPs) to 49 seconds (10 FPs);
- In a nutshell, enrolling eight fingerprints took roughly twice as long as enrolling four ($\approx +126\%$), while enrolling ten fingerprints took almost three times longer ($+185\%$).

Technology⁷

- The technology used to acquire four fingerprints was assessed as mature at all locations. A specific set-up might still be required at certain locations. In general, enrolling FPs in outdoor and moving conditions can sometimes raise issues (e.g. extreme temperature conditions, direct UV light on the optical lens);
- It is important that the system provides real-time feedback to both the traveller and the border guards during the enrolment process.

Experience

- Fingerprints are the type of biometric tested which seem to be the most favoured by travellers and border guards;
- Enrolling eight or ten fingerprints is perceived to be substantially more time-consuming.


⁵ Data on single-finger verification transactions is available from the on-going Fingerprint Verification Competition run by the University of Bologna (<https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx>).

⁶ Based on the conclusions outlined in the European Commission's 2014 Technical Study.

⁷ Technology is assessed as "mature" if it is already widely available on the market and in working condition, and is not highly impacted by environmental conditions. Medium maturity means being available on the market but sensitive to environmental conditions. Immature means that the equipment available on the market is not fit for purpose, has shown too many deficiencies and/or is too heavily impacted by the environment and therefore cannot be deployed at this type of border.

Facial-image (FI) enrolment and verification

Table 2 Summary of locations per type of border where facial image enrolment and verification were tested

 Enrolling live facial image (FI) (TC4): capturing FI from eMRTD (TC6), verifying FI captured from eMRTD against live facial image (TC7) – at 10 BCPs	
Air	Madrid (ES) Charles de Gaulle (FR) Arlanda (SE)
Sea	Helsinki (FI) Piraeus (EL) Cherbourg (FR) Genoa (IT)
Land (road)	Vaalimaa (FI) Sculeni (RO)
Land (train)	Iași (RO)
Outcome: the pilot confirms that enrolling a facial image, capturing the image from the eMRTD chip and performing the verification are technically feasible at all types of borders in terms of success rate, quality, duration and experience.	

Main findings

Success/quality

- Live facial images can be acquired using a standard off-the-shelf (web) camera, which can produce a high image quality for verifying travellers’ identity. Very high success rates can be obtained, with verification accuracy reaching 93%;
- Facial image as the unique biometric identifier cannot be used for identification purposes with large-scale databases.

Duration⁸













- The duration of the process was generally deemed acceptable except at border crossings on moving trains, where acquiring a live image was affected by changing conditions due to the movement of the train. In general, chip-image capture never lasted more than 3.5 seconds on average at air, sea and road borders; live image capture took 5.5 seconds on average; and verification was always done in less than 1 second at all types of borders.



Technology⁹

- To ensure that the live facial image captured is of a high quality and to guarantee subsequent high verification success rates, backlighting and reduced lighting should be avoided;
- The technology needed is widely available on the market today;
- Capturing the image from the chip can be done using equipment which is already available at most borders;
- The camera must be user-friendly and suitable for local environmental conditions at the BCP;
- An auto-adjustable camera is an advantage as it ensures image quality by adapting to travellers’ height and position.

Experience

- Taking a facial image is very common at borders where ABC gates are in use, which could explain the positive

Key			
	Success / Quality	 ≥ 75%	 ≥ 50% - <75%
	Duration	 < 15 s	 >15 s - <30 s
	Technology	 Mature	 Medium maturity
	Experience	 ≥ 65%	 ≥ 35% - <65%

Facial Image				
				
 Success / Quality				
 Duration				
 Technology				
 Experience				

⁸ For comparison purposes, the thresholds set for assessing FI duration were adapted in order to reflect the difference in processes of enrolling FP and iris. Indeed, for FI the assessment was made on the whole facial image process (i.e. enrolment of biometrics, capture of chip and verification) which performed extremely fast.

⁹ Ibid.

feedback left by travellers;

- Feedback from border guards and travellers was positive; automatic verification increased the border guards' confidence in the correctness of their decisions.

Iris enrolment

Table 3 Summary of locations per type of border where iris enrolment was tested

Iris pattern enrolment (TC5) – 5 BCPs, at 2 of which the test was combined with FI	
Air	Lisbon (PT)
Sea	Cherbourg (FR)
Land (road)	Sculeni (RO) Kipoi (EL)
Land (train)	Iași (RO)

Outcome: the pilot confirms the feasibility of using the iris as a biometric identifier within the context of a future EES system at all types of borders, and validates it as a possible complementary biometric identifier along with a facial image and/or fingerprints for registered travellers. Facial image and iris appeared to be a more effective combination than iris and fingerprints.

Main findings

Success/quality

- High success rates for enrolment were achieved at a set quality threshold.

Duration¹⁰

- Using fixed equipment for enrolment added only limited time, while the use of mobile equipment was more time-consuming. Indeed, at sea and road borders where fixed equipment was deployed, enrolment never took longer than 4 seconds on average. This duration increased by up to 20 seconds on average with mobile equipment.

Technology¹¹

- The technology required currently exists and is available in terms of both fixed and mobile solutions;
- Fixed devices are easy to use, and capturing irises at a distance (usually around 1 m) worked in under five seconds in 78% of cases;
- Enrolling an iris pattern in outdoor conditions or on moving trains is more problematic due to time and space constraints. It took about 26 seconds on average;
- Hot weather conditions and bright or dim light conditions impacted the functioning of the mobile equipment;
- Elderly people were reported to have difficulties in enrolling their irises, as well as people with almond-shaped eyes with epicanthic folds (majority of Asian travellers);
- Iris enrolment was assessed as being no more prone to spoofing than any other biometric identifier.

Experience

- Feedback from border guards and travellers was generally positive;




¹⁰ For comparison purposes, thresholds set for assessing the duration of iris enrolment are the same as for fingerprints.

¹¹ Ibid.

- Based on border guards' feedback, capturing irises seems to require fairly little training and instructions.

ABC gates

Table 4 Summary of locations per type of border where ABC exit of TCNs was tested

















 ABC gates for exit checks for TCNs (TCg) - at 7 BCPs	
Air	Charles de Gaulle (FR) Schiphol (NL) Lisbon (PT) Frankfurt (DE)
Sea	Helsinki (FI)
Land (road)	Narva (EE)
Land (train)	Gare du Nord (FR)

Outcome: the pilot confirms that using ABC gates at exit for TCNs and performing bearer verification on the basis of the facial image are technically feasible.

Main findings

Success/quality

- ABC gates performed as well for TCNs as they currently do for EU citizens.

























Key			
 Success / Quality	 ≥ 75%	 ≥ 50% - <75%	 <50%
 Duration	 Lower than baseline	 ≥ Baseline - ≥125%	 > 125% of baseline
 Technology	 Mature	 Medium maturity	 Low maturity
 Experience	 ≥ 65%	 ≥ 35% - <65%	 <35%

Duration

- The time taken to cross the border was assessed as comparable with manual control times. Average durations for the whole process ranged from 14 to 41 seconds;
- Passive authentication took less than 6 seconds.

Technology¹²

- The main environmental constraint identified was lighting, which impacts live facial-image capture and subsequently verification;
- The technology is already in place and operational at several borders across the Schengen Area;
- While the BCP environment may need to be adapted in some cases, the two primary remedies (removing or adding light) can be implemented easily;
- In terms of security, authenticating the travel document automatically was seen as having a positive impact on border guards' confidence in the decisions they make at the border.

ABC Gates				
				
 Success / Quality				
 Duration				
 Technology				
 Experience				


Experience

- In general, feedback from travellers was very positive;
- Border guards highlighted that ergonomics and a user-friendly, uniform interface are essential for ensuring traveller acceptance and usability.

¹² Ibid.

Kiosk

Table 5 Feasibility assessment of kiosk per type of border where the use of kiosks was tested

 Use of self-service kiosks (TC10) - at 3 BCPs , pre-border checks at land borders (TC11) - at 1 BCP	
Air	Lisbon (PT) Madrid (ES)
Sea	Helsinki (FI)
Land (road)	Sillamäe (EE)
Land (train)	N/A
<p>Outcome: the pilot confirms that using kiosks at entry for capturing data from travel documents (eMRTD) and enrolling/verifying four or eight FPs and FI are technically feasible in controlled environments. Land borders seem less suited to kiosk deployment at entry lanes due to constraints in available space (i.e. waiting area). However, the number of participants in the kiosk test case at land borders remained too low to draw meaningful conclusions. There was no kiosk test case at a train station or on a moving train.</p>	

Main findings

Success/quality

- In general, kiosks are able to capture data from the travel document and enrol fingerprints at a similar quality to that achieved with manual booths.

Duration





- Less time is spent at the manual booth when tasks are performed at the kiosk, i.e. there was a reduction of up to 35 seconds (including capturing four fingerprints).

Technology¹³

- Unfavourable light conditions can impact the quality of the live facial-image capture;
- The technology needed to assemble a kiosk exists today. Some further refinement in terms of their user interface would be an improvement;
- The impact of extreme weather conditions could not be assessed, since kiosks were always installed in indoor environments;
- Human supervision is required to strengthen security, primarily to prevent unauthorised persons being enrolled;
- Automatic height adjustment resulted in good facial-image verification (often superior to manual booths).

Experience

- Feedback from travellers and border guards was generally positive;
- According to border guards, travellers almost always need guidance, when using these systems for the first time;
- A friendly and human interface and ergonomics are essential for guaranteeing traveller acceptance and usability.

Key			
	Success / Quality	<ul style="list-style-type: none"> Green: > 70% completion of the process without errors Yellow: 50% - 70% completion Red: < 50% completion White: N/A 	
	Duration	<ul style="list-style-type: none"> Green: +/- 20% difference with manual booth Yellow: 20-50% difference Red: >50% difference White: N/A 	
	Technology	<ul style="list-style-type: none"> Green: Adapted and working Yellow: Some constraints Red: Not adapted White: N/A 	
	Experience	<ul style="list-style-type: none"> Green: ≥ 65% Yellow: ≥ 35% - <65% Red: <35% White: N/A 	

Kiosks				
				
 Success / Quality	Green	Yellow	Red	White
 Duration	Green	Green	White	White
 Technology	Green	Yellow	Red	White
 Experience	Green	Green	Green	White

¹³ Ibid.

Key findings from desk research

In addition to operational testing, desk research was conducted to address some further issues covered by the Terms of Reference of this pilot, in particular:

- Potential fall-back scenarios in the event that the EES is unavailable or unreachable, and describing related procedures, architecture and consequences;
- VIS border checks while using the travel document number (instead of the visa-sticker number);
- Web services for travellers and carriers; and
- Equipment costs.

The table below summarises the key findings for each of the four topics.

Table 6 Key findings of desk research

Desk-research topic	Key findings (the following measures should be considered)
Fall-back scenario	<ul style="list-style-type: none"> • High-level availability (similar to the level of SIS II, i.e. 99.99% per month) should be developed at central level; • Member States should aim to achieve the same high level of availability; • If the EES is temporarily unavailable, solutions for local electronic buffering and later synchronisation with the central system should be developed and implemented; • Manual (correction) procedures should be developed in case an entry or exit record is missing from the EES.
VIS border check using travel document number	<ul style="list-style-type: none"> • Searching the VIS by using the passport document number simplifies the border-control process and makes it easier for visa holders to use automated solutions (i.e. self-service kiosks and ABC gates); • Several options for consulting VIS based on the travel document number (instead of the visa sticker number) were assessed and considered feasible from a technical perspective. The technically preferred option is to use the alphanumeric search engine.
Web service for travellers and carriers	<ul style="list-style-type: none"> • For travellers to be able to consult the system, the proposed option would be to use data from the passport and provide a simple but discrete OK/NOK answer; • A credential-based system is proposed for carriers, whereby using travellers' passport data as an input, a simple OK/NOK answer is provided if a single day of stay remains. The option to introduce a proof-of-check mechanism was also assessed in order for the carriers to confirm that they performed the check.
Equipment costs	<ul style="list-style-type: none"> • The estimated average acquisition prices²⁴ for biometric devices have been provided in the report. However, the final costs will depend on the choice of biometric identifiers made.

²⁴ Installation and maintenance costs have not been included in the analysis.

Survey conducted by the FRA – key findings

There are a number of fundamental-rights implications related to the use of identification and verification technology in the context of border control. A small-scale survey conducted by the FRA looked into third-country-national travellers' attitudes and opinions regarding the use of biometrics at BCPs and various associated fundamental-rights aspects (e.g. the right to dignity, the right to respect for private and family life and the right to protection of personal data). Travellers' perception is believed to be an arguably subjective yet highly relevant element that needs to be taken into account when assessing the compliance of certain measures with fundamental rights (in addition to legal analysis).

The results show that the majority of respondents do not perceive that the use of biometrics at borders might compromise their right to dignity. There is also a tendency not to perceive the provision of fingerprints and facial image at borders as compromising the right to privacy. This is however not the case for iris-scan, which is considered the most intrusive option.

However, travellers expressed concerns with regard to the reliability of the system in the future. The majority of respondents believed that they would not be able to cross the border if the system malfunctioned. Similar concerns emerged in relation to the right to rectify the data, whereby half of the respondents believed that if there was a mistake in the data, it would be difficult to correct.

Conclusion

The pilot confirms the feasibility (in terms of accuracy, effectiveness and impact) of deploying biometric identifiers at Schengen external borders. Depending on the choice of biometric identifiers, the use of biometrics adds relatively little duration to the border-crossing process. Desk research proves that this time can be saved if some processes are better streamlined (e.g. by searching the VIS using the passport number).

The deployment of accelerators such as ABC gates and kiosks could further decrease border-crossing times. It was observed that the technology set-up and integration, as well travellers' interaction with it, influences the results much more than the type of border.

In addition, border guards felt that training was needed to prepare them for new equipment and processes. These key observations and considerations should now be put together and analysed further in developing successful combinations of biometrics for the future of Schengen borders.

The final report of the pilot was submitted to the European Commission as planned. The results of the pilot are representative and conclusive given the broad support provided by the Member States for the pilot, the number of the executed test cases for all types of borders and the amount of statistical evidences collected. The results of this unique project, conducted over a year, will contribute to the work on the modified legal proposal for Smart Borders.

1. Introduction

Background

During the first examination of the Smart Borders Package, the Council and the European Parliament (EP) voiced concerns about the overall feasibility of the Registered Traveller Programme (RTP) and the Entry/Exit System (EES). In particular, they expressed a need for more clarity on some technical and operational matters as well as the overall costs of the proposed systems. Prevalent issues noted included the choice of biometric identifiers, the impact on the border-crossing process and the extent to which existing national EES systems could be integrated and/or reused.

In order to further assess the technical, organisational and financial impacts of the systems and the various possible ways to address the highlighted issues, the European Commission (COM) subsequently initiated – with the support of both co-legislators – a Proof of Concept exercise to identify options for the implementation of the Smart Borders package. This exercise was conducted in two stages:

- A European Commission-led **Technical Study**¹⁵ (the Study) that identified and assessed the most suitable and promising options and solutions, with the assistance of eu-LISA;
- A **pilot** (or Testing Phase of the proof of concept) which was intended to verify the feasibility of the options identified in the Technical Study and validate the selected concepts for both automated and manual border controls. This pilot was entrusted by the European Commission to eu-LISA.

eu-LISA executed the pilot project from January to November 2015. The European Parliament, the EU Presidency and the Working Party on Frontiers were regularly informed on the progress of the project, which was carried out in full cooperation with the European Commission. This report is the main deliverable of the pilot project, detailing overall pilot outcomes.

Objective

The objective of this report is to present the results of the pilot and to allow conclusions to be drawn thereof regarding the feasibility of the options identified in the Study. Thus, for each of the test cases that were planned in order to address the various questions posed at the outset of the pilot, the key findings are noted so that the decision makers can avail of a comprehensive and accurate evidence base that should allow for appropriate consideration of the general feasibility of the system(s) and processes proposed for Smart Borders. The range of test cases, the means of test execution and the conditions that needed to be met by Member States supporting the tests were described in the test Roadmap, prepared by eu-LISA.

In all, 13 different Test Cases (TCs) were planned so that all specific technical options to be tested and researched were fully and appropriately analysed. The TCs included the enrolment of four, eight and ten fingerprints, the capture and verification of the facial image, the enrolment of iris patterns and the use of ABC gates and self-service kiosks (see table below for the full list).

Scope

The pilot was designed as a continuation of the Technical Study as both efforts make up the same Proof of Concept exercise. It was based on the Terms of Reference (ToR) drafted by the European Commission, which detailed precisely the options to be tested, the questions to be examined and the conditions to be met.

¹⁵http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/smart_borders_report_/smart_borders_report_en.pdf;
http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_Study_en.pdf.

eu-LISA identified a number of test cases that could be examined through operational testing in the roadmap and assigned the different TCs to selected Border Crossing Points (BCPs) (air, land and sea borders) with the goal of ensuring that the outcomes of testing across all locations would be representative of results that would be obtained at the variety of Schengen border conditions (e.g. different border types, different ABC gate configurations, various traveller types, different environmental conditions). Particular attention was given to the special conditions found at land borders.

Desk researches complemented operational testing in the following particular cases:

- For specific topics as specified by the ToR (e.g. anti-spoofing methods for iris enrolment);
- When other projects / experiences had already provided meaningful findings;
- When it was impractical or not feasible to perform real-life testing;
- To complete and to support the findings or some aspects of operational testing.

Table 7 List of the Test Cases that make up the Smart Borders Pilot

Test case	Operational testing at BCP ¹⁶	Desk research	Chapters
TC1: Enrol 4 fingerprints at first-line border check	x	x	2.1, and cost information provided in 3.4.2.1
TC2: Enrol 8 fingerprints at first-line border check	x	x	2.1, and cost information provided in 3.4.2.1
TC3: Enrol 10 fingerprints at first-line border check	x	x	2.1, and cost information provided in 3.4.2.1
TC4: Enrol live facial image	x	x	2.2, and cost information provided in 3.4.2.2
TC5: Enrol iris pattern	x	x	2.3, cost information provided in 3.4.2.3 and iris spoofing in section 3.5
TC6: Capture Facial Image from eMRTD	x	x	2.2, cost information provided in 3.4.2.2 and eMRTD desk research in section 3.6
TC7: Verification of FI captured from eMRTD against a live facial image	x	x	2.2, and cost information provided in 3.4.2.2
TC8: Searching VIS by Travel Document Number		x	3.2
TC9: Automated Exit Checks of TCNs	x	x	2.4
TC10: Use of Self-Service kiosks	x	x	2.5
TC11: Pre-border checks at Land Borders	x	x	2.5
TC12: Fall-back options		x	3.1
TC13: Web-interfaces to the carriers and to the travellers		x	3.3

¹⁶ For further details on the overall approach followed within the pilot, please see Methodology Chapter annexed to the main report (Volume 2 – Chapter 3).

The tests were conducted across Europe in 12 volunteering Member States between March and September 2015 and required the involvement of numerous stakeholders. eu-LISA consulted EU institutions and other Agencies in both the preparation and execution phases, including the European Data Protection Supervisor (EDPS), the Fundamental Rights Agency (FRA) and Frontex.

In compliance with EU data protection regulations, the pilot scope did not include end-to-end¹⁷ testing with real data from travellers and eu-LISA did not collect nor store any personal data, instead only recording anonymous statistics and performance indicators. All the tests were conducted by the Member States under the close supervision of national data protection authorities and traveller participation was completely voluntary.

The following pages of the Final Report are structured as follows:

- **Chapter 2** presents results of operational testing conducted at border crossing points aggregated per biometric identifier (**fingerprints 2.1, facial image 2.2 and iris 2.3**) and per accelerator (**ABC gates 2.4 and Kiosk 2.5**). In the cases of ABC gates and kiosks, the results are provided on the basis of both operational findings and desk research;
- **Chapter 3** gives answers to technical questions that could only be addressed by conducting desk research. The operational test report is further enriched by the findings from pure desk research (**fall-back scenarios 3.1, VIS border check using travel document number 3.2, web service 3.3, costs and equipment 3.4, iris spoofing 3.5 and chip reading 3.6**);
- **Chapter 4** serves as a conclusion for the entire pilot exercise;
- **The appendixes are in volume 2 of this report.** They present results per Border Crossing Point (BCP) chapters. These are grouped per type of border (air, land and sea). In addition relevant information for the reader can be found in the Appendices, such as methodologies employed for operational testing and technical analyses, as well as for data protection and analysis.

Out of Scope

The following aspects were considered out of scope and are therefore not considered further in this report.

- Simulation of a central system for the execution of biometric verification and identification was not considered. Estimations of verification and identification performance were made based on test results, specifically the quality of biometric samples captured;
- The pilot was not intended as a benchmarking exercise for biometric devices. Thus, the type of equipment/technology is referred to as appropriate and necessary (e.g. mobile/fixed, contact/contactless) but no comparisons are made of the equipment used in testing. Furthermore, no supporting vendor is named;
- No judgement is made about participating Member States, their national authorities, the set-up of border crossing points or process efficiency.

Attention points

- **Legal Compliance:**
The testing phase was conducted in compliance with existing legislation (e.g. the SIS II and VIS regulations, the Visa and Schengen Borders Code) and data protection regulations.
- **National Pilots:**
Some Member States (i.e. France and Germany) conducted additional test activities in parallel to the Smart

¹⁷ An end to end pilot would have encompassed recording personal data at entry into a central database simulating the EES and matching this data at exit. In that instance, the tests would have required a mock-up central EES system to be set-up and personal data to be stored in that system. This would have required a specific legal framework for test execution.

Borders pilot. These national pilots and tests may offer additional perspectives on the results presented in this report; however, the results are not presented herein.

- **FRA survey:**

The Fundamental Rights Agency (FRA) offered to conduct a survey on users' perceptions in parallel to the pilot. The results are presented as an Annex 7 to the Report and some relevant points are noted in the executive summary.

- **Test results:**

- Gathered results rely on Member States' border control processes and the ways in which the individual tests were set-up and performed. Nevertheless, individual results (of different BCPs, TCs and equipment) have been assessed and carefully processed in an attempt to make them as comparable as possible;¹⁸
- Where possible, the results have been consolidated according to the same biometric identifiers. However, it should be noted that not all results from the same TCs executed at different BCPs could be compared. Instead, similarities and differences were considered, particularly looking at the durations of the processes, the security of the implemented devices and procedures and equipment performance. The main challenges were:
 - Different types of border crossings in terms of conditions, TCN throughput and processes;
 - Different integration levels of new testing equipment;
 - Variations in the set-up and implementation of test cases;
 - Different quality thresholds being set for different equipment and by different vendors during the pilot;
 - Variations in equipment used for the same test cases in the different locations.
- Only cautious comparisons of the results of testing with different biometric identifiers are made due to the following factors:
 - Verification could only be tested for the facial image. It was not possible for fingerprints, or iris because of the lack of an available reference sample for comparison;
 - Only the vendors' quality thresholds could be used for facial image and iris;
 - Kiosks were implemented only in limited operational settings;
 - Border Guards were unfamiliar with processes and procedures for using the iris whereas fingerprints and facial image are already in use (fingerprints for verification against the VIS and facial image at existing ABC gates).
- Feedback from Border Guards relates to the pilot and the tests made at each BCP. It is therefore difficult to draw direct conclusions for future use of the EES where the set-up will be integrated and optimised;
- Exclusions and deviations from the test Roadmap¹⁹ were accepted when necessary. However, eu-LISA reserved the right to exclude results of tests when the sample size achieved was too low to draw meaningful conclusions.

¹⁸ This has been done by removing outliers and considering only the last successful attempt to enrol/verify a biometric identifier. In addition, the analysis took on board various types of input where relevant, such as baseline measurement, vendors' predictions and practical/operational interpretations based on MS feedback.

¹⁹ The Roadmap with specific instructions for the execution of Test Cases was delivered to the volunteering MS at the end of February 2015.

The results presented in this report have been obtained in an experimental environment, without tailoring the proposed solution optimally to the challenges at the given BCP, nor adaptation of the processes used. Therefore the results should be interpreted cautiously, and can only be taken to indicate likely results attainable with out-of-the-box solutions without any tailoring of hardware, software, environment or processes. In a future (permanent) deployment, one should assume that optimisations of both processes and solutions would be carried out and performance results would likely improve.

Page intentionally left blank

2. Operational testing

2.1 Fingerprints

2.1.1 Introduction

The use of fingerprints (FPs) as a means of identification dates back to at least the 19th century. Today, fingerprints are a commonly used biometric modality for automated verification and identification of persons at border control points. Within Europe, fingerprints are already being enrolled and used to verify the identity of visa holder travellers at borders as an important component of the Visa Information System: the visa holder's fingerprints are enrolled at the consulate and afterwards verified at the border.

However, the feasibility of enrolling different numbers of FPs at border crossing points is one of the biometric options for the EES, which was tested in the Smart Borders pilot. The scope of the pilot included three test cases (TC₁, TC₂ and TC₃) testing the enrolment of 4, 8 and 10 fingerprints respectively. Those three test cases were executed in total in 25 combined instances with different numbers of fingerprints enrolled at 12 different BCPs in 10 countries.

The feasibility of enrolling FPs depends on a number of factors that may be related to the user, the acquisition device deployed, the environment in which the enrolment takes place and the background systems that may process the data enrolled. In the pilot, a number of these influencing factors have been assessed - a variety of devices aiming to capture one, two and four FPs at the time have been tested (fixed and mobile, existing and newly deployed) with different underlying technologies and capabilities. Tests have been carried out at a variety of BCP types including on board a moving train and a moving cruise ship and both indoors and outdoors in various weather conditions. In some cases, the devices used were integrated into the current operational border management processes and, in others, they were deployed in a completely standalone manner.

The objectives of the tests are outlined in the next section of this chapter. In subsequent sections, a description of the methodology and conditions in which the tests were performed is provided, and indicators aimed at assessing the feasibility of using fingerprints as a biometric identifier in the context of border checks are presented.

2.1.2 Objectives

The main objective of this section is to evaluate whether it is feasible to enrol fingerprints, for later use as a biometric identifier within the context of a future EES system, at all types of borders with various set-ups (e.g. enrolling the fingerprints of occupants of cars and buses at land borders, FP enrolment on trains with mobile equipment) and in various conditions.

This question will be answered based on the operational results of tests in which the following test cases were assessed:²⁰

- TC₁: enrolment of four fingerprints (index, middle, ring, little) of the right hand;
- TC₂: enrolment of eight fingerprints (index, middle, ring, little) of the left and the right hand;
- TC₃: enrolment of ten fingerprints.

²⁰ It should be noted that tests carried out as part of TC₉ (Automated Exit Checks of TCNs) and TC₁₀ (Use of Self-Service kiosks) typically also included enrolment of fingerprints. For clarity's sake, the results of tests on these TCs are analysed in the respective chapters of the report and are not dealt with herein.

2.1.2.1 *Specific objectives*

The objective of feasibility outlined above was also split up in several specific questions that the pilot project set out to provide answers to:

1. **Operational and technical questions for each BCP type (land, moving train, sea, air)**
 - a. Success / failure: what was the success / failure ratio?
 - b. Enrolment quality: what was the recorded quality of enrolled samples?
 - c. Duration: what was the duration of the process steps added?
 - d. Equipment: can the enrolment be done with the equipment present at BCPs today (e.g. used for FP verification of visa holders)?
2. **Users' perception**
 - a. Perception of TCNs: what was the traveller's perception of the enrolment of fingerprints?
 - b. Feedback from Border Guards: how did border guards experience the added step of enrolling fingerprints?
3. **Constraints:** what constraints influence the quality of the biometrics (fingerprint) and/or the duration of the enrolment (e.g. ambient light)?

The costs related to the equipment needed for capturing fingerprints at the borders are addressed in Chapter 3.4.

2.1.3 **Methodology**

All information about the methodology used for the operational testing of fingerprints during the pilot can be found in Annexes of the main report (Volume 2 – chapter 3).

The following aspects are noteworthy:

1. **Fingerprint quality** was assessed in the pilot using the NFIQ metric as well as using counts of the number of minutiae per print;
2. **Prediction of the performance** of a future AFIS system when used for identification was calculated based on the quality metrics captured²¹;
3. The **duration** of the process was recorded based on software logs;
4. The **users' perception**, based on results of debriefing sessions, questionnaires and surveys, was assessed;
5. **Factors** affecting results were monitored where possible and deemed useful **environmental conditions** were logged and considered during field visits and in discussions with border guards.

In general, tests were carried out according to standardised approaches.

²¹ Such an approach was required as no reference samples were available against which to compare the enrolled prints in order to get direct measurements of performance. At this stage, it is important to note, however, that the actual level of performance will depend not only on the quality of individual fingerprints but also on the algorithm used by the matcher, the size of the database screened during identification and on the number of fingers used. As the database increases in size, the accuracy of identification decreases whereas using more fingers will increase both the accuracy and speed of comparison.

Key remarks

- It was recommended to reject low quality samples during biometric enrolment, in order to improve the eventual AFIS performance. Common NFIQ based thresholds were thus applied and a maximum of three attempts were made to capture the fingerprints to the demanded level of quality. Enrolled samples were generally not retained in memory from one attempt to the next during the pilot, implying that all fingers enrolled in a single slap needed to exceed applied thresholds at once; in some cases, however, fingerprints with good quality at one attempt were retained while the rest of fingers were recaptured individually on subsequent re-attempts;
- Capture was always performed under the supervision of a border guard;
- The devices were deployed in as effective a position as ergonomically possible given constraints of space and security. However, no extra building work was undertaken at any location and no special extra devices were deployed in order to remediate any perceived negative influencing factors. Possible remedial actions that could be taken in the future were discussed with border guards during debriefing sessions.

2.1.4 Testing locations and configuration

The table below gives an overview of the BCPs where enrolment of fingerprints was tested, specifying the type of border, tests performed and the type of device.

Table 8 Testing locations and configuration overview

BCP Type	BCP	TC ₁	TC ₂	TC ₃	Equipment
AIR					
	Frankfurt	X	X		4FP contactless
	Frankfurt	X	X	X	4FP scanner
	Schiphol	X			4FP contactless
	Schiphol		X	X	4FP scanner
	Madrid	X			Existing 2FP scanner configured to capture 1FP at once 4FP scanner
	Charles de Gaulle		X		Contactless 4FP scanner contact 4FP scanner
LAND (road)					
	Udvar (HU)	X	X	X	Existing 4FP scanner
	Kipoi (EL)	X	X	X	Mobile 2FP scanner, enrolment of 2 fingers per step
	Vaalimaa (FI)	X	X	X	Fixed 4FP scanner
LAND (train)					
	Iași (RO)	X	X		Mobile 2FP scanner, enrolment of 2 fingers per step
SEA					
	Helsinki	X	X	X	Fixed 4FP scanner
	Piraeus	X			Fixed 4FP scanner deployed in a portable suitcase
	Cherbourg	X			Mobile 1FP scanner
	Genoa	X			Existing 1FP scanner 4FP scanner

2.1.5 TC1, TC2 and TC3 (technical and operational) summary results

The combined results of all tests undertaken in which fingerprints were enrolled at a manned border control booth are presented in the following subsections. The sections successively deal with the quality of fingerprints enrolled at the different BCPs and using different equipment types (including information on the success of enrolment at the applied quality thresholds) and the duration of the enrolment processes.

During the testing and due to the specific configurations at individual BCPs, different thresholds were applied in various cases and re-enrolment attempts were not consistently carried out due to operational limitations. Some devices also made use of auto-capture functionalities²². These individual configurations were seen to have an influence on both quality and duration results. Thus, precise comparability of all results between different locations and border types cannot be implied and each result should be taken as indicative of the success that can be obtained with a particular (possibly non-optimal) deployment at a particular BCP.

In general, quality and duration are inversely correlated: to achieve a higher quality of sample, multiple enrolment attempts might be required, thus increasing the average duration of the whole FP enrolment process. On the other hand, application of less stringent quality thresholds will permit enrolment of lower quality samples (and subsequently to lower performance) but also imply shorter process durations based on a lower number of re-enrolment attempts.

Implementation of quality thresholds also plays an increasingly significant role when more fingerprints are enrolled, as each step of the process (e.g. the three attempts at enrolling 4, 4 and 2 fingers for 10-finger enrolment) may each have to be attempted several times. Furthermore, it is clearly more difficult to enrol several fingers above threshold at once compared to a single or few fingers.

More information about each BCP configuration and results can be found in the respective BCP chapters found in Annexes of the main report (Volume 2 – chapters 4 to 6).

2.1.5.1 Quality

Throughout the operational tests, the quality of fingerprints captured was measured by recording:

- The success rate, i.e. the percentage of participants for whom it was possible to enrol a full set of fingerprints (4, 8 or 10) at the implemented threshold (within a maximum of three attempts) and by extension, the FTE rate, i.e. the percentage of participants whose 4, 8 or 10 fingerprints did not simultaneously reach the defined threshold when enrolled;
- Distribution of NFIQ scores calculated from each fingerprint image enrolled on the first attempt;
- Distribution of number of minutiae²³ automatically extracted from each fingerprint image obtained on the first attempt.

²² Auto-capture implies implementation of software at the point of capture that analyses successively enrolled images based on metrics such as image contrast, ridge separation and clarity and selects the best image to be submitted onwards. In such instances, use of a quality threshold, for example based on the NFIQ metric, could only be applied subsequently.

²³ The term minutia describes the distinguishable features in a fingerprint sample, for example ridge endings or bifurcations, that are used in both manual and automated fingerprint comparison processes.

The table below provides an overview of the results obtained at the various test locations for test cases 1, 2 and 3. In order to prepare the table, average success rates and quality scores measures using NFIQ were both considered in order to examine whether fingerprints could be enrolled from travellers generally and, if so, whether their quality was above defined levels. This dual level composite analysis is particularly appropriate because enrolment thresholds applied were sometimes based on vendor scores, potentially allowing enrolment of variable quality prints; thus, the examination of NFIQ scores in all cases permits a harmonised and horizontal comparison to be made.

It should be noted that the analysis of whether good quality fingerprints can be enrolled at different types of BCPs made herein is drawn without consideration of the technology used at a specific BCP and any variability in process, passenger types or environment, despite the fact that these and other variables doubtless have effects on the results of operational tests. Further information on such uncontrolled variables and their relevance in operational testing is provided in the section on methodology.





Results were categorised into three pools during analysis, based on the following parameters:

- a. Green: enrolment was possible to a high level of quality: high success rates ($\geq 75\%$) at the set threshold and thus, generally good NFIQ scores;
- b. Orange: difficulties were observed with the enrolment of FPs with success rates between 50% and 75%. In such cases, it may have been possible to achieve higher success rates by adjusting test procedures or technical devices. Without such adjustments, the level of quality obtained might have adverse effects for either the border control process due to the many re-attempts or for the central system;
- c. Red: the majority of the attempts resulted in poor quality images. These instances are those in which low success rates were recorded, a high number of errors was noted or poor NFIQ distributions were obtained. This would ultimately lead to poor performance of the central AFIS. In these instances, the process (re-attempt policy), employed the threshold for enrolment and the devices and software used would have to be evaluated for suitability and likely modified if improved results were to be obtained in the future.

Table 9 Overview of enrolment quality for four, eight and ten FPs across the different test configurations²⁴ and equipment

BCP	Equipment Type	Success / failure		
		4 FPs	8 FPs	10 FPs
Air				
air-1	Contactless			
air-2	Contactless			
air-3	4FP scanner			
air-4	4FP scanner			
air-5	2FP scanner			
air-6	contactless			
air-7	4FP scanner			
air-8	4FP scanner			
Land: Road				
road-1	Mobile 2FP scanner			
road-2	4FP scanner			
road-3	4FP scanner			
Land: Train				
train-1	Mobile 2FP scanner			
Sea				
sea-1	Mobile 1FP scanner	Insufficient data		
sea-2	4FP scanner			
sea-3	1FP scanner			
sea-4	4FP scanner			
sea-5	4FP scanner			

Key:

	A majority of the attempts (>= 75%) were enrolled at the set quality threshold
	Difficulties enrolling FPs at the set quality threshold (>=50% and <75%)
	A majority of the attempts resulted in poor quality (success rate <50%)
	N/A: TC not performed at the BCP

Observations

Throughout the tests, the following points were noted:

- About devices and physical or software configurations:
 - In most instances, more than one attempt was required to successfully capture fingerprints. This was particularly true as more prints were enrolled;
 - Auto-capture functionality can significantly influence the results as quality control is enforced during the capturing process itself. At locations including Genoa and Kipoi, the implementation of auto-capture helped achieve good quality scores already at the first attempt;
 - Fingerprints obtained from contactless devices²⁵ ²⁶ had consistently poor NFIQ quality scores (i.e. below average) despite enrolment being frequently successful when carried out according to vendor-set thresholds. As the NFIQ metric was developed based on prints enrolled from optical contact scanners only, its validity as a

²⁴ Different thresholds for enrolment have been applied. Further details can be found in the specific BCP chapters annexed to the main Report (Volume 2 – Chapters 4 to 6).

²⁵ Such devices may also be described as touchless, non-contact or 3D in the literature.

²⁶ None of the contactless scanners tested within the pilot were FBI Appendix F certified at the time of writing.

predictor of AFIS performance in a database of prints enrolled from contactless scanners is unclear.²⁷ Contactless devices nevertheless can capture a larger area of the finger and as a result higher numbers of minutiae were typically extracted from prints collected using such devices. Thus, the utility of prints collected from such devices is not obvious. This may be a worthwhile topic for further consideration;

- Poor results in some test instances could be explained based on configuration issues or due to the positioning of the scanners relative to the travellers (i.e. too high or too low). Use of an ergonomically favourable set-up was often observed to be an important contributor to enrolment success.
- About the results:
 - It became more difficult to enrol all fingerprints with the demanded level of quality as more prints were enrolled, as all fingerprints simultaneously had to reach the quality threshold. Thus the successful rate for TC₃ was lower than for TC₂ and for TC₁;
 - Use of some devices in particular conditions, including cold weather or in direct sunlight or for the enrolment of travellers' fingerprints in cramped conditions, led to poor results, even for enrolment of four fingerprints;
 - At Madrid and Genoa BCPs, the enrolment of four FPs was possible using 1 and 2 FP scanners (currently used to query the VIS) to capture one finger at a time and resulted in similar quality prints being obtained as when using 4-finger scanners. Use of a mobile 2-finger scanner also resulted in good performance when enrolling four fingers.

Predicting AFIS performance based on quality scores

Quality assessment as described above was undertaken as a means to estimate the performance of an automated fingerprint identification system (AFIS) that would contain prints of the quality enrolled when used for identification (1:n) transactions. Leading vendors active in the field of AFIS design and development were consulted and based on the NFIQ score distributions and distributions of number of minutiae provided to them, provided such estimates for a database of 100 million travellers, taking into account the assumptions noted in the Methodology Chapter in Appendix of the main report (Volume 2 - Chapter 3).

In order to provide a baseline, predicted performance levels for identification purposes (1:n) are firstly provided for search using four fingerprints. The table below shows the performance predictions provided by one vendor for the most optimal setup and configuration tested at an individual location of the type specified (i.e. from the location providing the best quality prints). In these cases, some manual confirmation of grey area results would be possible. It is emphasised that the results should be considered indicative because of the various factors affecting the results, including the environment and operational configuration.

Table 10 Estimated 1:n performances per border type (best result)

BCP Type	Expected performance (TPIR ²⁸)
AIR	93.6%
SEA	99.0%
ROAD	96.8%
TRAIN	97.2%

²⁷ Initial results in the literature seem to suggest that the NFIQ metric is in fact not suitable for assessing the quality of such prints. See, for example, the article 'Neural-based Quality Measurement of Fingerprint Images in Contactless Biometric Systems, Labati RD, Piuri, V and Scotti, F, 2010 International Joint Conference on Neural Networks, 2010.

²⁸ True Positive Identification Rate (see Glossary).

The principle conclusion from the table above was that **the quality of prints enrolled at various border types varied little**. In fact, the technologies used are the most relevant determinant of quality obtained and thereby of AFIS performance. Although poor quality prints were sometimes obtained as elaborated in the individual BCP chapters – generally because of environmental or operational influences - devices were identified that allowed successful fingerprint capture at all types of border. In terms of setup, devices with auto-capture functionalities generally provided the highest quality prints per attempt.

Inclusion of more fingerprints in an AFIS database and execution of an identification task using more than four fingers improves both the accuracy of the results and the speed with which results are produced. In order to calculate performance based on search with eight and ten fingerprints, estimates were made based on population of a database with the full range of fingerprints enrolled throughout testing in the pilot and compared against the predicted performances for four fingerprints when the database included all the variable quality prints enrolled. For such predictions, execution in full 'lights out' mode was envisaged. It is suggested that, in an operational environment:

- 1:n identification in a gallery of 100M using sets of 4 fingerprints would give at best a TPIR of 97% at a false positive identification rate (FPIR) of 0.01%;
- 1:n identification in a gallery of 100M using sets of 8 fingerprints would yield at best a TPIR of 99.3% at a false positive identification rate of 0.01%;
- 1:n identification in a gallery of 100M using sets of 10 fingerprints would yield at best a TPIR of 99.3% for a false positive identification rate of 0.01%.

Based on results from the Fingerprint Vendor Technology Evaluation (FpVTE) 2012 benchmark performed by the NIST²⁹, values of 98.9%, 99.69% and 99.83% for 4, 8 and 10 fingerprint 1:n queries were calculated respectively. However, it should be noted that these results were obtained in a non-operational setup in which performance is maximized without consideration of the costs of doing so, and therefore they likely overestimate the performance that could possibly be obtained in any Smart Borders type system.

Although results for 1:1 verification transactions were not calculated based on quality measures obtained in operational testing, it has been known that verification based on fingerprints is possible with very high degrees of accuracy. The FpVTE test of 2003³⁰ indicated that single finger verification transactions could provide for a 99.4% true accept rate (TAR, see glossary) at a FAR of 0.01% in the best instances and perfect or virtually perfect performance with use of four or more fingerprints for such queries.

Conclusions

Consideration of quality suggests that fingerprints could be enrolled at all types of borders using both fixed and mobile devices and in all cases sufficiently high quality prints can be obtained that allow good AFIS performance. The most significant determinants of performance were the choice of equipment used - in particular, some devices were unsuitable for use in the environment in which they were deployed - and the configuration of both hardware and software, with successful enrolment processes possible at all types of borders and in various different environments.

According to the procedures used in testing, enrolment of four fingerprints generally resulted in the lowest failure to enrol rates. Successful enrolment was more difficult when higher numbers of FPs were to be enrolled, although the individual quality per finger was similar when enrolment was successfully completed. When enrolling 10 prints, success rates comparable to those obtained for four print enrolments were only obtained at a single air border crossing point. It is suggested that enrolment quality thresholds may have to be lower than those used in the pilot if

²⁹ <http://www.nist.gov/itl/iad/ig/fpvte2012.cfm>.

³⁰ NISTIR 7123, http://biometrics.nist.gov/cs_links/fpvte/report/ir_7123_summary.pdf.

eight or ten prints were to be more frequently enrolled with success, whereas the thresholds used were quite appropriate for four finger enrolment.

2.1.5.2 Duration

The duration of FP enrolment was measured in order to assess the added duration compared to the current situation where no biometric identifier is enrolled, and thus to measure how adding this step would impact the current border check duration.

Clearly, the overall added duration will depend on the device used, particularly its capacity to enrol several fingerprints at once. The underlying software also plays a key role. In particular, during enrolment of 8 or 10 fingerprints, there is a typical lag time as the software moves from modes to capture the different hands and minimisation of this lag time at software level will minimise overall enrolment durations.

The table below provides an overview of the results related to the duration of the fingerprint enrolment obtained across the various test locations for TC1, 2 and 3. The assessment is based on the duration of the fingerprint capture recorded by the software logs. This duration encompasses the re-attempts when they took place; however, it does not include the guidance that was provided to the travellers before starting the capture.

Based on this evaluation, there are three categories of test instances according to the atomic duration for FP capturing:

- a. Under 30 seconds, in green, which is considered to have a limited impact on the possible throughput. The 30 seconds value was identified within the simulation carried out during the Smart Borders Technical Study as the limit value beyond which there would be an impact on the queue at a border control in an airport;³¹
- b. Between 30 and 60 seconds, in yellow, which is considered to have an impact on the BCP and might warrant some changes in the local infrastructure or in the passenger flow;
- c. Higher than 60 seconds, in red, which is considered to be the value above which the current processes and infrastructure would be unlikely to be able to provide a sufficient throughput.

The impact of added duration also depends on whether the BCP is already saturated and whether the BCP has to process a high number of passengers within reduced time windows as opposed to a moderate number of travellers spread evenly over time. This is the case on cruise ships, ferries and trains, where there are stringent time constraints for the completion of the border control.

Further details on the duration, including the end-to-end duration measurement and its comparison against the baseline, can be found in the chapters dedicated to each BCP.

³¹ 2014, European Commission, Technical Study.

Table 11 Overview of the duration of the fingerprint capture

BCP	Equipment Type	Duration		
		4 FPs	8 FPs	10 FPs
Air				
air-1	Contactless			
air-2 ³²	Contactless			
air-3 ³³	4FP scanner			
air-4	4FP scanner			
air-5	2FP scanner			
air-6	contactless			
air-7	4FP scanner		Not available	
air-8	4FP scanner			
Land: road				
road-1	Mobile 2FP scanner			
road-2	4FP scanner			
road-3	4FP scanner			
Land: train				
train-1 (on the train)	Mobile 2FP scanner			
Sea				
sea-1	Mobile 1FP scanner	Insufficient data		
sea-2 ³⁴	4FP scanner			
sea-3 ³⁵	1FP scanner			
sea-4	4FP scanner			
sea-5 (moving vessel)	4FP scanner			

Key:

	Average duration under 30 seconds
	Average duration between 30 and 60 seconds
	Average duration equal to or higher than 60 seconds
	N/A: TC not performed at the BCP

Observations

Throughout the tests, the following was observed:

- The addition of the biometric enrolment does not increase the end-to-end duration linearly by the same amount as the time for the enrolment. In most cases, part of the additional duration simply reduces the time available for the border guards to perform the other tasks, such as asking questions to the TCNs;
- The need to perform reattempts is a lengthy process, which in some cases resulted in the border guard interrupting the biometric capture;
- The tests confirmed the train as one of the most difficult scenarios for the capture of fingerprints. Enrolling 4FPs, using a 2FP mobile scanner, took longer than 30 seconds on average, without calculating the additional time for enforcement of re-attempts;
- Using 4FP scanners helps save time compared to 1FP scanners: in two distinct test instances where both types of

³² Test with three-attempt policy enforced by the software.

³³ Idem.

³⁴ Idem.

³⁵ Idem.

enrolment have been tested, the 4FP scanner made it possible to save between 6 and 10 seconds on the average duration;

- Using 4FP scanners in acquiring a single slap avoids the problem of inverted sequence of fingerprint acquisition (i.e. finger sequence error) which is a recurrent human error when using single finger scanners;
- Comparing the durations for enrolling four FPs, with and without the re-attempts, the observation is that the enforcement of re-attempts for the captures below threshold seems to lengthen the average duration by 7 to 10 seconds while using a 4FP scanner. However, this is strongly dependent on the quality threshold enforced: too stringent a quality threshold would cause more frequent re-attempts resulting in longer durations and lower user acceptance;
- Tests using contactless devices highlighted that the possible time savings can be hampered if the number of re-attempts is significant. In one test location in particular, the recorded overall duration – with up to three attempts enforced in the event of insufficient quality – had durations comparable to or higher than using a contact device. On the other hand, when the enrolment is successful at the first attempt the duration is very low. Specifically for TC2, test results were inconclusive for contactless devices, with very different results in the two test locations where they had been deployed (averages from 6.5 seconds to 44 seconds).

Conclusions

In TC1, the enrolment of four FPs could be completed within a limited time. The majority of test instances had averages between 11 and 24 seconds for 4FP scanners; only single FP scanners or mobile scanners would have durations longer than 30 seconds.

In TC2, the enrolment of eight FPs in most of the test instances took between 45 and 66 seconds on average, approaching the estimated limit where the enrolment duration might create an impact on the throughput of the BCP and might thus require a redesign of the processes or of the infrastructures at the BCP. In some test instances, where re-attempts had not been enforced systematically, the average durations for TC2 ranged between 16 and 39 seconds; however in these same locations, the success rate using a set threshold for all the eight fingers was low.

Finally, for TC3, i.e. the duration for the enrolment of ten FPs, durations exceeded the 60-second threshold in the test location where the three attempts were enforced, reaching averages between 73 and 82 seconds. In the locations where the re-attempts have not been systematically enforced, the length of the capture was observed as shorter (with an average duration ranging from 42 seconds using fixed equipment to 59 seconds using mobile devices); however, those results will not show the correct impact of TC3. It is clear that, overall, enrolling ten fingerprints has a significant negative impact on the throughput of the BCP, especially if stringent quality thresholds or re-attempt policies were to be enforced.

The results using contactless scanners were not conclusive as the recorded average durations ranged from less than 10 seconds in a test instance to more than 40 seconds at another location. The importance of the right threshold, the correct positioning and ergonomics of the FP reader had a clear impact on the duration, as they determine the frequency of the re-attempts required.

2.1.5.3 Constraints

Environmental conditions

The table below shows a summary, indicating whether environmental aspects had an impact on the testing performed in outdoor conditions.

Table 12 Overview of environmental constraints observed in outdoor locations

Location	Comment
Udvar (TC _{1, 2,3})	No relevant constraint observed.
Kipoi (TC _{1,2,3})	The mobile equipment tested used a sunlight-resistant sensor which proved to work with no particular interference from outdoor light.
Vaalimaa (TC _{1,2,3})	Fingerprints negatively influenced by the environment, particularly with cold or damp weather, and strong light conditions.
lași (TC _{1,2})	The device would overheat and stop working during hot weather (over 35°C).
Port of Piraeus (TC ₁ - moving vessel)	No relevant constraints observed.
Genoa (TC ₁)	Ambient luminosity and the direct light coming into the booth would interfere with the FP capture. This prompted the installation of some shading which mitigated the problems.

Other constraints

Other aspects, observed during the testing that affect the enrolling process and should thus be addressed at the border check, were the following:

- Physical constraints:
 - Some travellers with large hands have difficulties placing their hands/fingers on the scanner;
 - In some locations the platen of the scanner needed to be cleaned frequently due to accumulation of dirt or other material;
 - Travellers had to exit their cars or buses to permit fingerprint enrolment. The use of mobile devices for capturing prints from those in vehicles was possible but rarely practical.
- Ergonomics:
 - The exact position and orientation of the device plays a very important role to facilitate the fingerprint capture, and should thus be chosen carefully;
 - Mobile equipment must be ergonomic for both the border guard and the traveller. This aspect is especially important when capturing four FPs (or more) using a mobile device on a train, as enrolling the little finger sometimes posed problems, mainly due to the cramped space that limited how the device could be held and used;
 - When enrolling ten FPs, capturing the thumbs was seen as rather cumbersome and took extra time, in particular when using mobile devices; nonetheless, thumbprint quality is usually higher than the rest of the fingers. The use of mobile devices to enrol this amount of fingerprints was in general a challenge for the border guards;

- The position of the device influences acquisition speed (height, inside/outside the booth, in the middle/lateral).
- Feedback and instructions
 - Assistance or guidance provided to the travellers (by the border guards or by other means) is essential to increase usability and efficiency. This is especially the case when reattempts are involved, as the traveller is not familiar with the process and the need for re-tries is not easily understood. There were measurable differences of performance when border guards could give instructions in the traveller's language as compared to situations where both did not share a same language.
 - Real-time feedback provided to the border guard (user interface) and/or to the traveller (visual or audio indications such as colour LEDs, videos showing how the equipment shall be used, etc.) usually helps to improve the results.



2.1.6 Users' perception


2.1.6.1 Border guards' feedback

During the execution of the fingerprint test cases, border guards were surveyed on their perception of the enrolment process, their experience using the equipment and their perception of traveller acceptance. The results were collected for analysis. In addition, whenever possible, border guards were included in the de-briefing sessions of field visits to gather more qualitative feedback through discussions of test case execution.

In this section, the border guards' feedback has been consolidated across three dimensions (process, equipment and traveller) to present a higher-level overview. Where relevant, observations related to specific BCPs are provided.

Table 13 Overall border guards' feedback for the fingerprint enrolment

Summary of border guards' feedback	
<p>Process</p> 	<ul style="list-style-type: none"> • Fingerprint enrolment was generally well accepted if there were no systematic issues with the test equipment; • It was suggested that the number of fingerprints to be enrolled should be minimised as far as possible to reduce times and overall process length, particularly if a 2FP scanner is being used; • Road BCP-specific: requiring travellers to get out of their vehicles to participate in the tests increased process duration, and it was suggested that this should be taken into consideration when designing the future process; • Train BCP-specific: it was difficult to find a good method for enrolling fingerprints inside a train compartment due to limited space, since the border guards had to sit down next to the passenger, where possible, to carry out an effective enrolment.
<p>Equipment</p> 	<ul style="list-style-type: none"> • The overall experience of the test equipment was mixed and largely dependent on the type of scanners used; • Mobile devices were generally well received in terms of ease of use and mostly functioned according to expectations. Suggestions were made that they could be useful as a "process accelerator" and used to process TCNs, as required, when the majority of travellers in the queue were EU citizens. In some cases, feedback was received that the ergonomics and bulkiness of these devices could be improved. There were also a few cases where environmental conditions (hot weather) affected their performance; • In many cases, there were reports of issues with the test equipment being used due to hardware malfunction, signal/system failures or ergonomics. In some cases, there were issues with readings when they were taken outdoors; • There were several cases reported where it was difficult to obtain readings due to the misplacement of fingers, from elderly travellers (e.g. illnesses such as Parkinson's, less distinct fingerprints with age etc.) or from people with large hands;

	<ul style="list-style-type: none"> • In several cases, it was suggested that more guidance with regard to the use of equipment should be provided both to border guards and to travellers particularly when new equipment is being used; • In some cases it was highlighted that contactless devices were considered to be hygienic while, in separate cases, it was indicated that contact devices were considered to be unhygienic; • Train and sea BCP-specific: it was sometimes difficult to obtain acceptable readings from the equipment due to the movement of the train or ship.
<p>Traveller</p> 	<ul style="list-style-type: none"> • Overall, travellers were perceived as being accepting of fingerprint biometrics and the associated enrolment process. Any dissatisfaction was mostly due to queue size or when several attempts were required to obtain a reading; • In several cases, particularly at road and sea BCPs, language was seen as a barrier during the testing, resulting in difficulties in communicating with travellers and guiding them through the tests. It was also cited as a reason for travellers refusing to participate in the tests. There were also some reports of travellers being suspicious of biometrics. Implementing measures to reduce the impact of the language barrier (e.g. a sheet of commonly used phrases or training border guards in phrases to use for guiding travellers) improved results somewhat; • In some cases, cultural and social traditions seemed to impact traveller acceptance and some male travellers refused fingerprints to be taken from their wives or daughters.

Conclusions

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- Fingerprint biometrics were generally well received when the number of attempts were kept low and when the scanner used were reliable;
- Human factor and communication are paramount:
 - Border Guards generally reported that travellers accept fingerprint biometrics provided queue sizes remained acceptable and number of readings were kept low;
 - Addressing potential language barriers may enhance traveller acceptance. Language barriers in fact may impact the capacity of border guards to explain how biometrics are going to be used and the ability to provide assistance to the travellers within the enrolment process;
 - Consideration of traveller's social and cultural norms may enhance traveller acceptance;
 - Border guards and traveller require sufficient guidance and support regarding the use of equipment;
 - Attention to hygiene is becoming more important and may influence the traveller acceptance, giving further support to contactless biometrics and equipment.
- Equipment usability, ergonomics and stability should be adequate:
 - There were cases of equipment malfunction (hardware, signal/system failure, etc.) which caused dissatisfaction among border guards and travellers. Though this can be attributed to the test equipment which was used in specific cases, it highlights the quality of the equipment as being a key success factor;
 - Some type of equipment are more suitable than others for a particular BCP type or use-case (e.g. dedicated equipment for obtaining prints on a train or for obtaining prints from seated drivers in a car or truck);
 - Equipment deployed should be suitable for the number of fingerprints being obtained (e.g. using 4-FP scanners to obtain 8 or 10 fingerprints is more convenient than 2 FP scanners);
 - FP readers should clearly signal to travellers and border guards whether a fingerprint capture has been successful.

2.1.6.2 *Travellers' feedback*

This section summarises the overall results obtained from a voluntary survey presented to travellers after they had taken part in the tests.

The results obtained are overall very positive, with satisfaction level above 81% for TC1 (four fingerprints) and of around 75% for both TC2 (eight fingerprints) and TC3 (ten fingerprints), however this latter had a higher percentage of unsatisfied people and a lower number of people which indicated a neutral perception of the tests. No significant variations in performance were observable across the different type of borders.

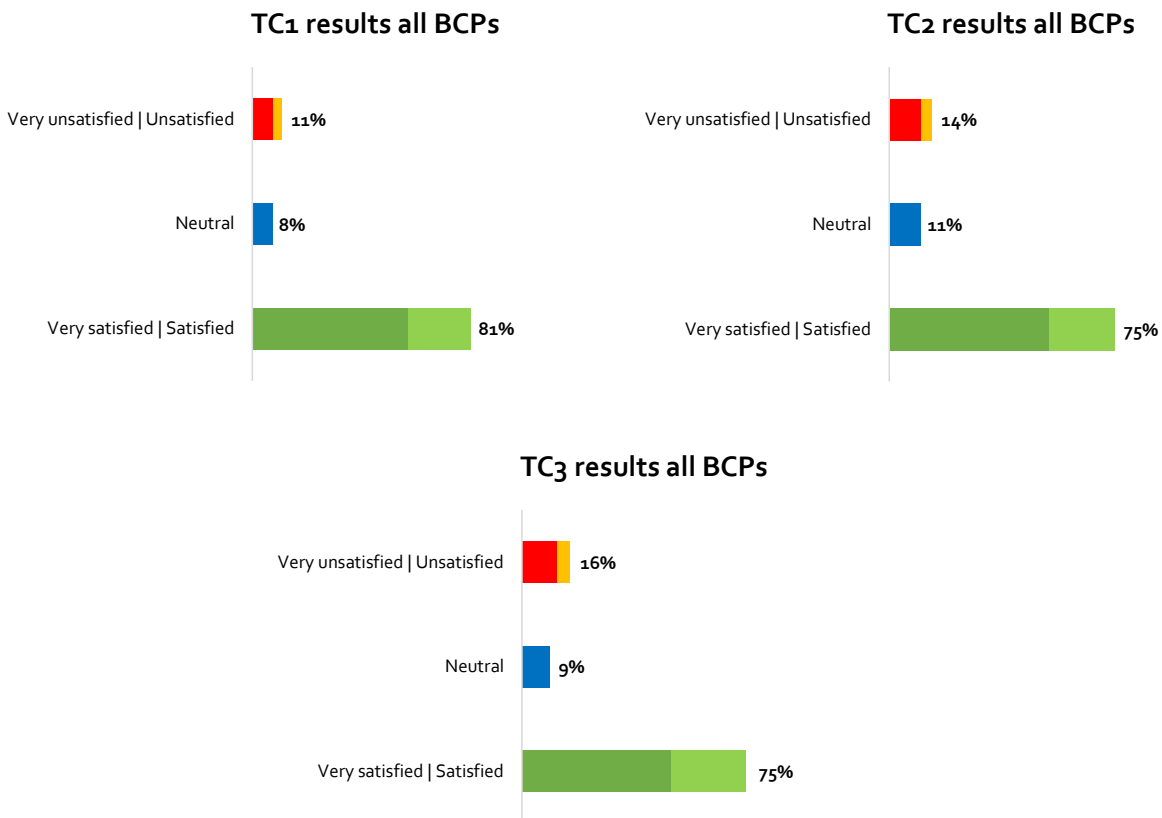


Figure 3 *Participating travellers' feedback on the tests (TC1, 2 and 3)*

An independent survey conducted by the Fundamental Right Agency (FRA) with travellers who did not participate in the tests reported that for approximately 20% of the people interviewed it was uncomfortable giving fingerprints (and 7% did not answer). For further details, please refer to the full report annexed to the main report (Volume 2 – Annex 7).

2.1.7 **Feasibility**

This section assesses the feasibility of enrolling and further using fingerprints as a biometric identifier within the context of a future EES system, at all types of borders with various set-ups. Feasibility is assessed based on based on the definition given by ISO/IEC/IEEE 29148:2011 as explained in the Methodology chapter in Appendix to the main report (Volume 2 – Chapter 3).

Building on the results presented on the previous sections regarding quality and durations, it is possible to draw some conclusions and observations concerning the overall feasibility of the three options considered for fingerprint enrolment.

2.1.7.1 TC1 - enrolment of 4 fingerprints

Technical achievability

Table 9 (quality) and **Table 11** (duration) confirm the technical feasibility of the enrolment of four FPs at all border types. In the vast majority of test instances, the enrolment process took less than 30 seconds. Exceptions were noted with tests involving capture with mobile scanners or 1FP scanners. It was possible to capture prints of high quality in at least one test setup at each type of border; in fact, the quality of the sample obtained seemed to depend mostly on the equipment used and its configuration with no location presenting insurmountable obstacles to high quality enrolment.

Ensuring a consistent high quality during fingerprint enrolment at all locations is crucial to ensure subsequent accurate identification, particularly when only using four fingerprints. Alternatively, the addition of a second biometric modality, such as the facial image, should lead to more accurate outcomes.

Not requiring major technological advances

Testing results suggest that current technologies can be used to enrol four fingerprints and that no major technological advances are needed. Indeed, current solutions are already deployed for the purpose of fingerprint enrolment from travellers, e.g. for the VIS. Devices enrolling one or two fingers per step, were also demonstrated to be usable. However, their deployment implied a longer duration of enrolling four prints than with a device enrolling four fingerprints in a single step (i.e. increases between 6 and 11 seconds on average) and a lower success rate. The summarised quality score³⁶ was very similar (just two points difference) in both locations where both 4FP scanners and 1/2FP scanners were tested.

Users' perception

Feedback from border guards and travellers was generally positive in relation to their experience of enrolling four FP.

Fitting with system constraints

In certain extreme weather conditions (i.e. cold weather and very hot weather above 35°C), enrolling FPs in outdoor conditions became more difficult. Procedures for switching to indoor checks in cold weather could be necessary. It is suggested, nevertheless, that implementation of mitigating measures in very hot conditions would be more difficult to identify (changes in the environment for process execution on board ships or trains may be more difficult to accomplish).

2.1.7.2 TC2 - enrolment of eight fingerprints

Technical achievability

Table 9 (quality) and **Table 11** (duration) demonstrate that eight fingerprints can be enrolled at all types of borders. However, the use of eight prints is less acceptable for travellers and/or border guards and the enrolment process is notably longer than for four prints enrolment. Recorded durations are, with a few exceptions, in the range of 30 to 60 seconds, which would likely increase queue times at many BCPs. Looking at the median values of all the results collected for fingerprint enrolment, the time needed to enrol eight fingerprints is roughly double the time needed to enrol four fingerprints ($\approx +126\%$ ³⁷).

Using mobile equipment for enrolling eight FPs was also seen as difficult, in particular when performing the enrolment in a constrained space (e.g. in a train).

³⁶ NFIQ quality was summarised as described in the methodology chapter. For comparability purposes, only the values for the first attempt were considered.

³⁷ Without considering different quality thresholds.

Not requiring major technological advances

1FP and 2FP scanners can be used to enrol eight fingerprints; however, durations become much longer and the success rate decreases significantly. This was also observed in Iasi (constrained space aboard a moving train) where testing had to be interrupted due to the difficulty – and sometimes traveller discomfort – in using mobile scanners to capture two fingers at a time.

One and two-fingerprint scanners were the most commonly found at the BCPs visited as the standard equipment used for the VIS check, which suggests that an upgrade of these devices would be necessary in these BCPs in case of enrolment of eight (or ten) fingerprints.

Users' perception

Border guards' and travellers' feedback was less positive than for the test case of enrolling four FPs.

Fitting with system constraints

Same as for enrolling four FPs.

2.1.7.3 TC₃ - enrolment of ten fingerprints

Technical achievability

Table 9 (quality) and **Table 11** (duration) show that enrolment of ten fingerprints would have a negative impact on the queue times and throughput of BCPs. Enrolment took longer than for eight FPs and much longer than for four FPs, and success in enrolling an entire set of fingerprints was harder to achieve. The re-attempt policy was considered particularly burdensome for the users when ten prints were enrolled. Looking at the median values of all the results collected for TC₃, enrolling ten fingerprints took 185% more time than enrolling four fingerprints and 26% longer than enrolling eight fingerprints.

Not requiring major technological advances

The additional duration and reduced success rate would have the biggest impact on BCPs when required to capture ten FPs. This was already an identified difficulty for TC₂, so it can be inferred that the enrolment of two additional fingers would be more difficult.

Users' perception

Border guards' and travellers' feedback identified the enrolment of ten fingerprints as being more problematic. It is suggested that the process of ten fingerprint enrolment was perceived as burdensome.

Fitting with system constraints

Same as for enrolling four FPs.

2.2 Facial image

2.2.1 Introduction

In border check processes worldwide, verification of the traveller against his or her travel document is accomplished using facial recognition. Travel documents typically display a frontal photograph of the traveller's face, allowing comparison against the person presenting at the border. Such a manual process performed by a border guard has been used to verify identity at the border for decades. Since the 1990s, eMRTDs including e-passports have been introduced that store the facial image in an electronic chip and improve security by facilitating detection of manipulation and falsification of the printed photo on the biographic page. This development has permitted the introduction of automated facial image comparison processes into border checks at manual booths, as well as at ABC gates and self-service kiosks.

When considering the use of the facial image as a biometric identifier in a future proposed EES, the Technical Study highlights the reliability of the method, both in automated and manual scenarios. The ease of its use and the fact that the facial image is typically the only biometric accessible on the chip of the travel document³⁸ and therefore a good means of biometrics-based document bearer verification³⁹. The facial image on the chip is accessible in a non-contact manner (through a RFID reader), quickly and easily without dependence on travellers being accustomed to any unusual enrolment procedure. As a result, it is an important if not the main method of document bearer authentication.

During operational testing within the Smart Borders Pilot, tests were executed that focussed on operational processes taking place at the border:

- Enrolment of a live facial image from the traveller;
- Capture of the facial image from the chip contained in the eMRTD;
- Verification of one against the other.

The objectives of the tests are outlined at the beginning of this chapter. In subsequent sections, a description of the methodology and conditions in which the tests were performed is provided, and indicators aimed at assessing the feasibility of using the facial image as a biometric identifier in the context of border checks are presented.

³⁸ Countries are able to include several types of biometrics on the chip (see chapter 3.6) but ICAO Member States are mandated to include the facial image only.

³⁹ Bearer verification (verification that the bearer is the rightful owner of the passport) using FI from eMRTD against live photo.

2.2.2 Objectives

The main objective of this section is to evaluate whether it is feasible to enrol and use the facial image as a biometric identifier within the context of a future EES system at all types of borders with various set-ups (e.g. enrolment of a live facial image (FI) for travellers in a moving train or on a moving vessel).

This question will be answered based on the assessment of the operational results of tests in which the following test cases were performed:⁴⁰

- TC6: capture of the facial image from the chip of an eMRTD;
- TC4: enrolment of a live facial image;
- TC7: verification of the facial image captured from an eMRTD against the live facial image.

Within the pilot, the three tests cases 6, 4 and 7 were typically undertaken in a single process,⁴¹ with the common goal to enrol a live image of sufficient quality to permit matching against the chip image according to the defined thresholds.

2.2.2.1 Specific objectives

The following questions are considered in the sections below:

1. **Operational and technical questions at different BCP types (air, sea, train, road, moving train, moving vessel)**
 - a. Success/failure: what are the combined and individual success/failure ratios for the different steps of the process - live facial image enrolment (i.e. failure to enrol (FTE) rates), image extraction from the chip and verification based on thresholds described below?
 - b. Enrolment quality: what was the recorded quality for both live and chip facial images?
 - c. Duration: what was the duration of the process steps added?
2. **Users' perception**
 - c. Perception of TCNs: what is the traveller's perception of the introduced border control process?
 - d. Feedback from Border Guards: how do border guards perceive the changes made to the border control process?
3. **Constraints:** Which constraints influence the quality of the biometrics (facial image) and the duration of the process?

Some aspects of using the facial image as a biometric that have been investigated through desk research are addressed in Chapter 3.6. In particular, questions regarding the duration of Passive Authentication (PA), the complexity of executing PA and the possibility of simultaneously capturing the live facial image and extracting the image from the chip are assessed therein. The costs related to the equipment needed for capturing live facial image and its verification at the borders are addressed in chapter 3.4.

⁴⁰ It should be noted that tests in the frame of TC9 (Automated Exit Checks of TCNs) and TC10 (Use of Self-Service kiosks) typically also included use of facial image biometrics. For clarity, the results of tests on these TCs are analysed in chapters 2.4 and 2.5 of the report and are not dealt with herein.

⁴¹ TC4 was performed in isolation was in Cherbourg, where the enrolment of a live facial image was performed separately from any image extraction from the eMRTD or image verification. In these tests, the quality of the facial image captured was measured as a key metric along with the duration of capture.

2.2.3 Methodology

The approach to tests focussed on the facial image is described fully in the Methodology chapter annexed to the main report (Volume 2 – Chapter 3). A summary of the main elements is presented below.

- Metrics assessing the quality of the chip and live facial images were calculated where possible in order to allow comparison of the suitability of the images for automatic verification. Verification performance was examined by calculating False Rejection Rates (FRR) at thresholds corresponding to indicative False Acceptance Rates (FAR) provided by the supporting vendors based on their own testing and experiences. Where possible, tables or curves such as DET (Detection Error Trade-off) curves were also obtained to allow estimation of performance at different FAR rates and thus comparability between results. ICAO indicators were also collected, where possible, and reviewed to support the analysis. For locations where these indicators influenced directly the re-attempt policy of the live facial image capture (i.e. Arlanda and Sillamae), an analysis was included in the respective dedicated chapters;
- The duration of the whole process, as well as the different sub-steps of the process, was recorded, in logs from the equipment;
- Users' perceptions were assessed during debriefing sessions and through analysis of the results of distributed questionnaires and surveys.

Uncontrolled factors envisaged to effect the results of operational tests, such as temperature and humidity, were monitored using devices specifically deployed for this purpose, as well as being considered during field visits and when discussing testing with border guards. Note that tests on facial image were the only ones within the pilot in which a reference sample – extracted from the eMRTD chip – was available. Therefore, the approach to results analysis was different compared to the other biometric modes. Rather than using quality scores as a predictor of Automated Biometrics Identification System (ABIS) performance, verification performance was directly assessed. Information on quality was used to explain variations in performance in post-analyses. At the operational level, all tests were carried out according to standardised approaches. The following points are notable.

- Systems with various degrees of automation were tested, ranging from an automatic video capture system that operated without border guard action to single shot cameras activated manually by the border guard;
- A maximum of 3 attempts were made to capture the live facial image in case of single shot capture, while timeouts were typically applied with video capture;
- Live facial image capture was always performed under the supervision of a border guard.

2.2.4 Testing locations and configuration

The table below gives an overview of the BCPs where tests examining the use of the facial image as a biometric were undertaken.

Table 14 Testing locations and configuration overview

BCP Type	BCP	TC	Live FI capture equipment	eMRTD capture equipment
<i>AIR</i>				
	Madrid (ES)	6, 4 and 7	New, Fixed, Video Capture	Fixed, Full-page
	Charles de Gaulle (FR)	6, 4 and 7	New, Fixed, Video Capture	Fixed, Full-page
	Arlanda (SE)	6, 4 and 7	New, Fixed, Single Shot	Fixed, Full-page
<i>LAND: road</i>				
	Vaalimaa (FI)	6, 4 and 7	New, Fixed, Single Shot	Fixed, Full-page
	Sculeni (RO)	6, 4 and 7	New, Fixed, Video Capture	Fixed, Full-page
<i>LAND :train</i>				
	Iasi (RO)	6, 4 and 7	New, Mobile, Single Shot	Mobile, Swipe, RFID reader
<i>SEA</i>				
	Helsinki (FI)	6, 4 and 7	New, Fixed, Single Shot	Fixed, Full-page
	Piraeus (EL)	6, 4 and 7	New, Fixed, Single Shot	Fixed, Full-page
	Cherbourg 1 (FR)	4	New, Fixed, Video Capture	N/A
	Cherbourg 2 (FR)	6, 4 and 7	New, Mobile, Single Shot	Mobile, Swipe, RFID reader
	Genoa (IT)	6, 4 and 7	New, Fixed, Single Shot	Fixed, Full-page

2.2.5 TC6, TC4 and TC7 (technical and operational) summary results

This section is divided into two main subsections: *Quality* and *Duration*. The success rate is considered as part of the subsection dealing with quality.

More information can be found in the relevant BCP chapters found in the annex to the main report (Volume 2 – Chapter 3), where the results for each of the tests are further detailed.

2.2.5.1 Quality

The quality of the biometrics enrolled has been measured by assessing:

- The rate of success when verifying a traveller's identity based on comparison of his/her live facial image with the facial image from the chip of the presented document at a matching threshold that should provide an FAR of 0.1%⁴² (as explained above in section 2.2.3 and further in the Methodology Chapter annexed to the main report (Volume 2 – Chapter 3));
- The success rate of live facial image enrolment;
- The success rate of facial image extraction from the eMRTD chip;
- Vendor provided quality scores based on their own proprietary algorithms⁴³;

⁴² As suggested in "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, Research and Development Unit, Frontex. Version 2.0, August 2012". This is further explained in the Methodology Chapter in Annex to the main report (Volume 2 - Chapter 3).

⁴³ Specific vendor scores are not analysed and are presented only for allowing comparison of the quality of the live and chip facial images.

- A selection of ICAO quality scores (based on the metrics defined in ICAO document 9303) describing the quality of the facial images.

The table below provides an overview of the results obtained across the various test locations for TCS 4, 6 and 7. When examining the table, the following considerations should be borne in mind:

- The success rate for enrolment of the live facial image is calculated as the proportion of participants whose live facial image was enrolled, considering any enrolment thresholds if implemented at the point of capture;
- The success rate for the capture of the facial image from the eMRTD chip is calculated as the proportion of eMRTDs presented for which a facial image was successfully retrieved (regardless of the quality)⁴⁴;
- The success rate for verification is calculated as the proportion of verification scores that exceeded the threshold required to reach a FAR of at least 0.1% according to the supporting vendor.

Table 15 Overview of success rates for capturing facial image (live and from chip) and matching them across the different test instances

BCP	Equipment	Success		
		Live FI enrolment	Chip FI capture	FI verification
Air				
BCP A	Fixed, Video capture			
BCP B	Fixed, Video capture			
BCP C	Fixed, Single shots			
Land: Road				
BCP I	Fixed, Single shots			
BCP J	Fixed, Video capture			
Land: Train				
BCP K	Mobile, Single shots		Not recorded	
Sea				
BCP D	Fixed, Single shots			
BCP E	Fixed, Single shots			
BCP G	Fixed, Video capture			
BCP H	Fixed, Single shots			

Key:

	Success rate \geq 75%
	Success rate between 50% and 75%
	Success rate below 50%
	N/A: TC not performed at the BCP

Observations

- Facial image enrolment/capture success rates were similar across all types of BCP. The verification success rate varied more notably, with verification at sea and road borders proving to be less successful generally;
- Chip reading errors were recorded in several locations though normally with low frequency. Qualitative feedback from border guards did not highlight major issues with reading the chip itself;
- The quality of the image on the chip photo was typically better than the live image captured during the test, indicating that the picture taken from the chip eMRTD, once authenticated, would likely be a better candidate for usage as a reference picture for subsequent verifications than an image recorded at the manual booth of the BCP;
- An analysis of the ICAO indicators recorded for the chip facial images showed that the level of compliance with

⁴⁴ In some cases where the eMRTD had an inactive chip, in order to handle further the passport, it was considered as an MRTD. However, the number of eMRTDs with a broken or inactive chip "downgraded" to the MRTD-status could not systematically be recorded.

ISO/IEC 19794-5:2005⁴⁵ varied based on the issuing country. For example, the eye distance, expressed in pixels, varied by nationality from an average of 60 pixels to 140 pixels for issuing countries presenting more than 500 samples while the ISO 19794 standard specifies a minimum of 90 pixels. In fact, 5 out of 12 issuing countries (42%) typically included photos in their issued documents that had an average eye distance below the threshold;

- The majority of locations where live facial image enrolment took place did not attempt to modify the BCP environment to allow better image quality to be obtained (e.g. no lighting change, no protection). The results could likely be improved by optimising conditions that could affect the process in a negative way;
- At one BCP, the live facial image of car passengers was captured while the subject remained in the vehicle (the driver and one rear passenger). The success rate for the capture remained high despite the constrained conditions.

Conclusions

The capture of facial images – both live and from the eMRTD chip – was highly successful. In more than 90% of cases, a successful enrolment/capture could be performed. Despite implementation of a stringent threshold applied to comparison scores to determine verification success (corresponding to a FAR of 0.1%), up to 93% of participating travellers could be successfully verified at the border based on their facial image, even in outdoor conditions.

The success rate was neither significantly affected by movement, as encountered during testing on a moving train and a moving sea vessel, nor by the type of equipment. In most locations, a simple webcam was sufficient for enrolment of live images of sufficient quality to perform automated comparison. Bearing in mind that most photos within the tests were taken without controlled background or lighting, this result appeared impressive.

However, poor lighting was seen to contribute to a lower success rate. The integration of the equipment within the process and the technical environment also seemed to play a large role, indicating that the test results for those tests that were performed with standalone equipment were probably lower than what can be achieved with some integration effort.

2.2.5.2 Duration

In order to assess the added duration of the test steps compared to the existing end-to-end process where no biometric identifier is enrolled, the durations of the following additional process steps were measured:

- a. TC6 (capture of the facial image from the chip of an eMRTD);
- b. TC4 (enrolment of a live facial image). TC4 and TC6 were in most cases executed together;
- c. TC7 (verification of the facial image captured from an eMRTD against the live facial image).

The table below provides an overview of the results obtained that relate to the duration of the facial image capture and verification obtained across the various test locations. This duration includes the time needed for re-attempts when they took place, but does not include the time needed to provide prior guidance to the travellers.

Further details on the duration, including the end-to-end duration measurement and its comparison against the baseline, can be found in the chapters dedicated to testing at each individual BCP, found in the Annex (Volume 2 – Chapters 4 to 6).

⁴⁵ ISO/IEC 19794-5:2005 defines acceptable values for the indicators outlined in ICAO Doc 9303 and measured during the pilot.

Table 16 Overview of the total duration of the live facial image enrolment, chip facial image capture and matching of the two facial images

BCP	Equipment	Duration
		Live FI enrolment + Chip FI capture + Verification
Air		
BCP A	Fixed, Video capture	
BCP B	Fixed, Video capture	
BCP C	Fixed, Single shots	
Land: Road		
BCP I	Fixed, Single shots	
BCP J	Fixed, Video capture	
Land: Train		
BCP K	Mobile, Single shots	
Sea		
BCP D	Fixed, Single shots	
BCP E	Fixed, Single shots	
BCP G	Fixed, Video capture	
BCP H	Fixed, Single shots	

Key:

- Average duration below 15 seconds
- Average duration between 15 and 30 seconds
- Average duration equal or above 30 seconds

Observations

Automated facial recognition could be efficiently executed. Capture of the live facial image was typically possible in a short period - in less than 15 seconds at every type of BCP (except inside a train) - and should not have any noticeable impact on the overall duration of BCP operations. Furthermore, extraction of the facial image from the chip (as described fully in the chapter on chip reading) and the execution of the comparison software added only a couple of seconds to the overall process.

In tests using a mobile device on the train, the duration of live image enrolment was often longer than 15 seconds. The longer duration could be explained by two factors: the more difficult environment (e.g. motion, lighting, space constraints) and the use of a mobile device. The relative impact of each could not be measured. Nevertheless, results show that verification was often (i.e. in 90% of cases) successful on the train once the facial image was captured.

2.2.5.3 Constraints

Environmental conditions

Environmental conditions did not seem to affect the capture of the facial image from the chip of the eMRTD, nor the verification. On the contrary, the capture of the live facial image was affected by environmental conditions. Results of environmental monitoring suggested the following:

- Temperature: no direct signs of impact were identified. Indirect effects considered included increased wearing of hats during winter, making capture and hence successful verification more difficult. At very high temperatures, inside a train, some mobile devices would not work properly;
- Humidity: no direct signs of impact were identified;
- Light: a direct impact was identified. The three main issues observed were:
 - Light directly affecting the camera sensor;

- Light directly affecting the face of the traveller, leading to over- or under-exposed portions on parts of the facial image;
- A lack of light, typically occurring in indoor environments or in outdoor environments at night;
- Backlight also affects the quality of the picture captured.

The identified constraints could, to a certain extent, be controlled, by adding protection from direct light in case of overabundance of light and additional lighting systems in case of a lack of light or uneven lighting at the point of capture. Some systems tested had integrated lighting capabilities and provided improved results in poorly lit environments, including in some airports.

Other constraints

- The placement of the camera plays an important role;
- Guidance and assistance to the travellers usually improves the process of capturing a live FI;
- Ergonomics should be also taken care of, especially in the case of mobile equipment.

2.2.6 Users' perception

2.2.6.1 Border guards' feedback

To gather feedback from participating border guards across test locations, feedback forms were used and a varying number were returned per BCP. In addition, whenever possible, border guards were included in the de-briefing sessions of field visits to gather more qualitative feedback through discussions of test case execution.

Below is a summary of the overall border guard feedback for the test cases involving the use of the facial image as a biometric identifier. Feedback per BCP can be found in the relevant annexes.

Table 17 Overall border guards' feedback for facial image test cases







Summary of border guards' feedback	
<p>Process</p> 	<ul style="list-style-type: none"> • Mainly positive feedback: capturing of a live photo and performing facial verification worked well; • Using facial verification (possibly against a central database) would increase the confidence of the border guard when verifying traveller identity.
<p>Equipment</p> 	<ul style="list-style-type: none"> • The devices worked well and associated processes were quickly completed.
<p>Traveller</p> 	<ul style="list-style-type: none"> • Travellers were mostly positive about the process; • In one location, the border guards reported that the travellers felt that the test was intrusive if performed together with TC5 (enrolment of iris pattern); • More guidance to travellers would be an advantage if given at an earlier point in their approach to the control.

Table 18 Potential impediments and areas for improvement identified by border guards' for facial image

Potential challenges and improvement points	
 <p>Process</p>	<ul style="list-style-type: none"> • Space: limited space in environments such as a train carriage can make it difficult to capture the live picture; • Language may influence the capacity of border guards to explain how biometrics, including the facial image, are used and their ability to assist the travellers within the enrolment process; • Duration: border guards felt that is important that the total process time is not extended compared to today's process time. Verification using the facial image was noted to minimally extend the process duration; • Setup: the environment inside a train is not adapted for the process and necessitates improvements to obtain good results; • Training: guidance on how to best use the equipment was needed.
 <p>Equipment</p>	<ul style="list-style-type: none"> • Devices sometimes became unresponsive for a variety of reasons, and had to be restarted; • Environmental conditions such as lighting and movement were noted as impediments. Issues noted included backlight blinding the sensor and motion of the traveller in a train making it more difficult to capture an image fulfilling the quality threshold; • The equipment would still benefit from efforts to improve user-friendliness. Generally, the devices used could be better integrated and more conveniently positioned at the BCP. Suggestions included the use of hand-held cameras and implementation of automatic camera height adjustment and automated capture.
 <p>Traveller</p>	<ul style="list-style-type: none"> • Guidance and assistance should be provided to travellers – in advance if possible; • Travellers often need to adjust their position in case of space-constrained usage or in cases in which the camera angle or zoom could not be appropriately modified; • In a couple of locations, the border guards reported issues related to the traveller's cultural traditions in the performance of the tests. In some instances, travellers indicated that a female border guard was required to assist a female traveller; • Old age or certain illnesses (Parkinson and others) were also reported as a potential impediment.

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- Human factors and communication are paramount:
 - Passengers felt more confident following border guard explanations and when they assisted the process;
 - Difficulty to communicate with some TCNs (because of language) caused abortion of tests in some cases;
 - Border guards felt that training was needed to prepare them for new equipment and processes.
- Equipment usability, ergonomics and stability should be improved:
 - Many border guards included comments on equipment and suggestions for improvements (mainly setup and ergonomics) to ease process execution by making it easier and quicker to enrol the facial image – automation of the process and automatic height adjustment of the camera were frequently requested;
 - There were issues with reading of and use of the chip and use of the stored facial image in all locations. In some instances, up to 10% of efforts to read the chip gave some error. Border guards were not able to determine if these were related to the chips themselves, the quality of the photo on the chip or related to the passport reader.

- **Environmental conditions** should be taken into consideration
 - Lack of light, direct sunlight and backlight can all cause difficulties;
 - Movement made efficient FI capture difficult.
- **The setup** played an important role:
 - Current infrastructure is not always suitable – sometimes light protection was an issue;
 - Processes requiring travellers to exit their car for the live facial image capture introduced complexities, especially in case of families;
 - Simple changes in moving train cases, such as in training to ask travellers to sit down for having the picture taken, could improve the process.

2.2.6.2 Travellers' feedback

This section summarises the overall results obtained from a voluntary survey presented to participating travellers after they had taken part in the tests.

The results obtained are generally very positive, with satisfaction level above 87% for facial image related test cases. Only 6% of respondents across all test locations expressed themselves to be unsatisfied with the process. No relevant differences were detected across the different types of borders.

This contrasts with the findings of the survey performed by FRA with travellers who did not participate in the tests, in which more than 21% of surveyed people indicate that they are uncomfortable with use of the facial image as a biometric identifier at the border. This discrepancy could be explained by the fact that those submitting to testing were more familiar with how the facial image might be used following testing or by the fact that travellers who were not inclined to have their facial image captured probably did not participate in the tests in the first place. Additionally, feedback provided by test participants related to the test process as a whole whereas questions posed by FRA were more detailed and examined different aspects individually.

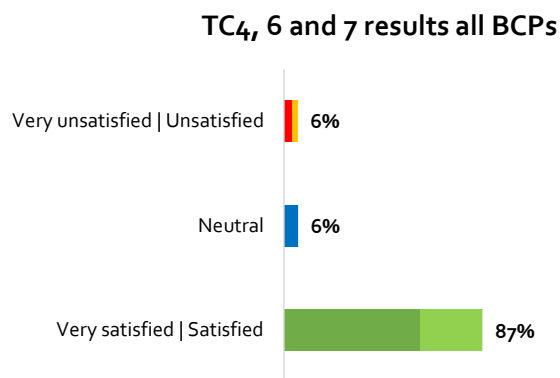


Figure 4 Participating travellers' feedback on the tests (TC₄, 6 and 7)

2.2.7 Feasibility

This section assesses the feasibility of using the facial image as a biometric identifier within the context of a future EES system, considering the above results. The assessment is based on the definition given by ISO/IEC/IEEE 29148:2011 as explained in the methodology chapter in Annex to the main report (Volume 2 – Chapter 3).

2.2.7.1 Technical achievability

Table 15 (quality) and **Table 16** (duration) confirm the technical feasibility of using the facial image as a biometric identifier for Smart Borders at all types of borders.

2.2.7.2 *Not requiring major technological advances*

The technology required to use the facial image as a biometric identifier at the border exists today and is readily available:

- Live facial image enrolment can be accomplished using a standard off-the-shelf web camera which is able to capture the image to a high level of success;
- Extraction of the chip image is possible using the equipment (a passport scanner with RFID capabilities) that is already available at most European borders;
- Facial image verification: A number of algorithms for facial image comparison were tested and found to be very capable of accurately comparing good quality facial images. Many of the algorithms are already used in border control worldwide.

2.2.7.3 *Users' Feedback*

Feedback from border guards and travellers was generally very positive following the execution of facial image test cases.

Most border guards are already used to capturing the facial image from the eMRTD chip. Automated verification of the image was seen as a positive support to the border guard's decision making process.

Travellers are also used to this type of technology, which is currently used to verify travellers at ABC gates.

2.2.7.4 *Fitting with system constraints*

In limited light and weather conditions (e.g. strong or weak lighting), problems may arise when enrolling good quality facial images. Lighting has been highlighted as the primary influencing factor on verification success rates. While adaptation of the BCP environment might be needed in some cases, implementation of the two primary remedies (light obstruction and light addition) should be possible without significant challenges.

2.3 Iris pattern

2.3.1 Introduction

Iris images were first used as a biometric for facilitating border crossing in Europe in the year 2000 in Frankfurt Airport in Germany. To pass through an iris-capture access control system, the unique pattern of the iris of the eye has to be verified against a previously enrolled template in order for a passenger to be positively authenticated. Iris images can also be used for identification, with a provided probe image being compared against the samples in a database of enrolled images and a ranked list of likely hits being provided as output. In both cases, the use of the iris involves both enrolment and verification steps.

Enrolling the iris pattern typically occurs at the first interaction between user and system. One or both irises can be enrolled depending on the setup, with the latter typically being preferred as both irises are independent and thereby use of both improves performance, while simultaneous dual iris capture guards against rotation of one iris image compared to the second. The travellers stand in front of a camera and have their eyes (irises) digitally photographed using visible light and/or invisible infrared light. The capture distance can vary from device to device, with portable devices usually having a short capture range (in some cases, goggle-devices can be used) but some other devices (including some tested during the pilot) operating at a distance longer than one meter.

Verification of the iris patterns occurs when the passenger is checked by the system on subsequent occasions. As for enrolment, the passengers stand in front of an iris camera and have their irises photographed again. The system processes the iris patterns, extracts the templates and compares them to those stored.

The European Commission Technical Study on Smart Borders did not include an analysis of the impact of using the iris as a biometric identifier. Yet the Study highlights that there are examples around the world of using iris biometrics for border checks. As a result, the Study recommended that the pilot should include tests examining the feasibility of enrolling the iris pattern from travellers at various locations.

Thus, during operational testing within the Smart Borders Pilot, tests were executed enrolling travellers' iris patterns (left and right) at the border. In some of the tests, the iris capture was combined with capture of the facial image (sometimes simultaneously) – see **Table 19** below.

The objectives of the tests are outlined in the next section of this chapter. In subsequent sections, a description of the methodology and conditions in which the tests were performed is provided, and indicators aimed at assessing the feasibility of using the iris as a biometric identifier in the context of border checks are presented.

2.3.2 Objectives

The main objective of this chapter is to ***evaluate whether the iris is a valid complementary biometric identifier to facial image and fingerprints.***

This question will be answered based on the assessment of the operational results of tests in which the following test case was performed:

- TC5⁴⁶: Enrolment of iris patterns (for both right and left irises).

⁴⁶ The process of testing TC5 is built upon a single step: capture iris pattern.

2.3.2.1 *Specific objectives*

In order to examine the feasibility of iris enrolment, the following specific questions were examined during operational testing:

1. **Operational and technical questions for each BCP type (land, moving train, air)**
 - a. Success / failure: what was the success / failure ratio?
 - b. Enrolment quality: what was the recorded quality of enrolled samples?
 - c. Duration: What was the duration of the process steps added?
 - d. Dual capture of iris and facial images: Could the facial image be captured in the same step as enrolling the iris?
2. **Users' perception**
 - a. Perception of TCNs: what was the traveller's perception of the enrolment of the iris pattern?
 - b. Feedback from Border Guards: how did border guards experience the added step of enrolling the iris?
3. **Constraints:** what constraints influence the quality of the biometrics (iris) and/or the duration of the enrolment (e.g. ambient light)?

Only questions with regards to technical and operational achievability are dealt with in this chapter. Costs aspects are dealt with in Chapter 3.4. Security aspects, such as the iris spoofing likelihood compared to other biometric modalities are addressed in Chapter 3.5.

2.3.3 **Methodology**

All information about the methodological grounds used for the operational testing of iris during the pilot can be found in the Methodology chapter annexed to the main report (Volume 2 – Chapter 3), while a summary of the main elements is presented below.

The following aspects are noteworthy:

1. The **quality** of the iris patterns captured was measured based on NISTIR 7820 and vendor-specific algorithms. The aim was to predict the performance of an ABIS for identification of travellers at the border;
2. The **duration** of the process was measured based on logs from the equipment;
3. **users' perceptions** were assessed based on results of debriefing sessions, questionnaires and surveys;
4. The most likely external factors influencing performance were measured when possible – thus, **environmental conditions** were monitored during testing using logs, examined during field visits and discussed with border guards.

At the operational level, standardised approaches were requested from the test operators. The following points are notable.

1. Both the right iris and the left iris were always captured in parallel by the device;
2. The capture was always performed under the supervision of a border guard;
3. Attempts were always made to position the devices as optimally as possible given constraints of space, security, time and budget.

In some cases, BCP facilities were modified to address factors that would have negatively influenced results such as strong extraneous lighting ahead of testing. During the tests, some modifications were also made and logged, both related to the process and the equipment. Possible remedial actions that could be taken in the future were discussed with border guards during debriefing sessions.

2.3.4 Testing locations and configuration

The table below gives an overview of the BCPs where enrolment of iris was tested.

Table 19 Testing locations and configuration overview

BCP type	BCP	Iris capture equipment	Combined facial image capture?
AIR	Lisbon (PT)	<ul style="list-style-type: none"> - Fixed self-enrolment station (kiosk-like) - Short acquisition distance (c. 60 cm) - Facial image capability, not simultaneously - Automatic height adjustment 	No
LAND (road)	Kipoi (EL)	<ul style="list-style-type: none"> - Mobile, handheld - Short acquisition distance (c. 20 cm) - Facial image capability, not simultaneously 	No
	Sculeni (RO)	<ul style="list-style-type: none"> - Fixed - Long acquisition distance (c. 120cm) - Facial image capability, simultaneously - Automatic height adjustment 	Yes
LAND (train)	Iași (RO)	<ul style="list-style-type: none"> - Mobile, handheld - Short acquisition distance (c. 20 cm) - Facial image capability, not simultaneously 	No
SEA	Cherbourg (FR)	<ul style="list-style-type: none"> - Fixed - Long acquisition distance (c. 120cm) - Facial image capability, simultaneously - Automatic height adjustment 	Yes

2.3.5 TC5 (technical and operational) summary results

This section is divided into two main subsections: *Quality*, *Duration*. The success rate is considered part of the subsection on quality.

More information can be found in the relevant BCP chapters in appendix to the main report (Volume 2 – Chapters 4 to 6), where the results of each of the tests are further detailed.

2.3.5.1 Quality

The quality of the biometrics enrolled was measured by assessing:

- The success rate of enrolling both right and left iris patterns above a given threshold within three attempts;
- The vendor proprietary quality scores associated with iris patterns⁴⁷, where available;
- A selection of NISTIR 7820⁴⁸ (extract) scores associated with the iris patterns.

⁴⁷ Specific vendor scores will not be analysed, and they are presented only for the purpose of allowing comparison of the quality scores between the left and right iris patterns. Absolute values of the scores are not assessed.

⁴⁸ NISTIR 7820 scores have not been analysed systematically, and they are presented only for the purpose of allowing comparison of the quality scores of the different attributes of the iris pattern. Absolute values of the scores are not assessed.

The table below provides an overview of the results obtained across the various test locations for TC5.

Table 20 Overview of success rates for enrolling iris patterns across the different test instances

BCP	Equipment	Quality / success rate (enrolment of both iris patterns simultaneously)
<i>Air</i>		
BCP A	Fixed, medium acquisition distance	
<i>Land: Road</i>		
BCP C	Mobile, short acquisition distance	
BCP D	Fixed, long acquisition distance	
<i>Land: Train</i>		
BCP E	Mobile, short acquisition distance	
<i>Sea</i>		
BCP B	Fixed, long acquisition distance	

Key:

	Success rate greater or equal to 75%
	Success rate between 50% and 75%
	Success rate below 50%

Observations

- Regardless of conditions and equipment, more than 75% of participants could enrol both their iris patterns successfully. At three BCPs out of five, the capture success was superior to 90%;
- The success rate was not significantly affected by movement (e.g. moving train) or constrained conditions (e.g. inside a car or a train);
- The high rate of success could be maintained when simultaneously capturing a live facial image;
- The success rate at outdoor BCPs was achieved after adaptation of the BCP environment to improve the success rate of the tests (e.g. building protection around the devices, light protection, guide rails for cars).

2.3.5.2 Performance prediction of the BMS in non-controlled outdoor conditions

Following consultation with the industry, it was possible to estimate the expected performances of the iris matcher on the basis of the quality scores obtained at two BCPs where irises were enrolled at a long distance (i.e. approximately 1.2 m) in outdoor conditions using a particular product provided by one vendor. This is the most difficult use case envisaged at any border and the predictions made should be considered what could be achieved 'at worst'.

The estimation was based on the following assumptions:

- Performance is indicated for 1:n searching in a database size of 100 million records. As there is an inverse relation between the database size and the accuracy of the ABIS in identification, a different use case (e.g. a registered traveller programme with a smaller database size) would result in different performance;
- Identification would be performed using the two iris patterns;
- The threshold for identification would be set such that the false positive identification rate (FPIR) would be 0.01%.

By using a database with data having similar quality scores to those obtained in the tests at the two outdoor BCPs, a false negative identification rate (FNIR) between 15% and 23% could be estimated by this vendor.

This high false negative rate needs to be put into perspective as it was obtained:

- With a process focussed on duration instead of quality (less than 5 second acquisitions in 80% of the cases);

- With eye obstructions in some cases (e.g. glasses or car frame);
- With the gaze of the traveller not completely facing the camera (i.e. with more modification of the BCP the enrolment apparatus could have been placed to better enrol iris pattern images);
- In outdoor conditions with direct lighting impacting the sensors and the travellers' faces (and due to strong light, sometimes causing pupil constriction) and without any specific optimisation of the ergonomics of the setup having been undertaken as would normally be done ahead of deployment for full use.

It was estimated that with better lighting control, user ergonomics and removal of obstructions (e.g. asking the traveller to remove glasses), the expected FNIR at these outdoor BCPs could be significantly reduced. It is suggested by the same vendor that, in the same conditions, use of a shorter-range capture device (i.e. goggles in contact with the face, but not with the eye could reduce the rate of false negative identification to about 2.5%).

The NIST IREX IV tests, described in NISTIR 7949⁴⁹, detail results of identification transactions based on iris images, run using a variety of vendor algorithms against databases of variable sizes containing iris images collected in the field and sometimes collected in outdoor conditions. In a database of 10000, the best algorithm had an FNIR of 1.7% at an FPIR of 0.01% and an FNIR of 2.0% in a population of 1.6 million when set up for positive identification tasks (i.e. verifying that the person is who they say they are) and using just one enrolled iris pattern as a search probe. The results highlight the relatively low increases in error rates when population size increases, a typical feature of identification using iris biometrics. Algorithms setup for de-duplication transactions were able to produce an FNIR of 2.0% at an FPIR of 2.0% in a population of 1.6 million. Switches to searches using two iris images typically reduced FNIR rates by a factor of two at the same FPIR rates – thus FNIR rates of approximately 1% were attainable.

2.3.5.3 Duration

The duration of enrolling of iris patterns (left and right, simultaneously) is measured in order to assess the added duration compared to the end-to-end process and the current situation at the borders tested in which no biometric identifiers are enrolled.

The table below provides an overview of the durations of iris pattern enrolment at the various test locations for TC5. The assessment is based on the data obtained from the software logs. This duration includes the time required for re-attempts when they took place⁵⁰, but does not include the time needed to provide prior guidance to the travellers. Further details on the duration can be found in the chapters dedicated to each BCP.

The ranges applied to perform the assessment originate from the Technical Study, which assessed that addition of steps that add no more than 30 seconds additional time per traveller per border crossing would have a negligible impact on the dwelling times at BCPs, while steps adding up to 60 seconds would have a small impact.

Table 21 Overview of the total duration of iris patterns enrolment

BCP	Equipment	Duration (enrolment of iris patterns)
Air		
BCP A	Fixed, medium acquisition distance	
Land: Road		
BCP B	Mobile, short acquisition distance	
BCP C	Fixed, long acquisition distance	→
Land: Train		

⁴⁹ Quinn, G.W., Grother, P., Ngan, M. IREX IV, Part 1: Evaluation of Iris Identification Algorithms. August 2013.

⁵⁰ Re-attempts (up to three in total) in case of failure to enrol at first attempt were almost systematically made at all locations

BCP D	Mobile, short acquisition distance	
		Sea
BCP E	Fixed, long acquisition distance	→

Key:

→	Average duration below 15 seconds
	Average duration below 30 seconds
	Average duration between 30 and 60 seconds
	Average duration equal or above 60 seconds

Observations

- With devices activated by border guards, 80% of attempts took less than 5.5 seconds, 90% less than 7 seconds and 95% of attempts took less than 8 seconds;
- With devices configured as enrolment stations to be used independently by the traveller, 80% of attempts took less than 35 seconds, 90% less than 40 seconds, and 95% less than 40 seconds (the timeout was 40 seconds);
- With mobile devices, 80% of attempts took less than 32 seconds, 90% less than 51 seconds and 95% less than 71 seconds;
- Enrolment of the iris patterns generally took less than 30 seconds and often less than 5 seconds and thus should have only negligible impact on the overall duration of BCP operations;
- Fixed devices could enrol samples most quickly, with 75% of the enrolments being complete in less than 5 seconds;
- In some cases (8% of all attempts), enrolment duration when using mobile iris scanners at land borders was more than 60s. This may be related to the usability of the device or the behaviour of travellers in certain conditions (e.g. closing their eyes in strong sunlight);
- The iris enrolment process was very straightforward and transparent for travellers. It required little guidance compared to fingerprints for example;
- The capture of the facial image on top of the iris pattern was possible in the majority of cases and added only a few seconds (less than 5) to the process when using adequate equipment (i.e. with the same acquisition range for both modalities).

2.3.5.4 Constraints**Environmental conditions**

Some environmental conditions seemed to affect the capture of the iris patterns.

- Temperature: no direct signs of impact identified;
- Humidity: no direct signs of impact identified;
- Light: direct impact identified during test setup. The constraints of light could, to a certain extent, be controlled by adding protection from direct light or additional lighting systems in case of lack of light (just like for facial image capture) – indeed steps were taken during testing in this direction and found to be effective. The two main issues observed were:
 - Light directly affecting the camera sensor;
 - Light directly affecting the face/eye of the traveller, creating reflections in the eye, causing the traveller to close his/her eyes or causing pupillary constriction, altering the typical iris dimensions.
- Movement: direct impact.⁵¹

⁵¹ Iris enrolment was tested in a moving train during the pilot. However, it should be noted that enrolling the iris pattern when the train was actually moving, was only possible for a short period.

- Based on the success rate, movement did not seem to have a substantial negative effect on the capture of the iris patterns. However, border guards highlighted the difficulty of using the device when the train is in motion.

Other constraints

- The ergonomics of the device play a role in the usability of mobile equipment. The mobile device used during the tests had a weight of approximately 1.2 kg. Lifting the device and holding it steady at the height required for iris capture can be difficult, even more so after longer durations of use;
- The success rate of the facial image capture and of iris enrolment, when performed simultaneously, are following the same trend throughout the tests. Indeed the success rate of both operations seems to slightly drop at a similar rate at certain times of the day (e.g. morning and evening), which indicate that the varying lighting conditions had a similar influence on both captures during the tests. As such, the lighting conditions in which high quality iris patterns were obtained were similar to those in which high quality facial images were obtained;
- Travellers by car: while the tests demonstrated that it was possible to capture the iris while volunteers stayed inside their vehicle, they also highlighted the difficulties in obtaining a good quality enrolment for the purpose of identification (see the performance prediction section 2.3.5.2). The position of the camera relative to the travellers, variable and possibly uncontrolled light conditions and the need to provide guidance to the travellers all reduce the practicality of this option for enrolment purposes.

2.3.6 Users' perceptions

2.3.6.1 Border guards' feedback

Feedback from participating border guards across test locations was gathered from weekly updates, end-of-testing questionnaires and additionally, where possible, discussions during de-briefing sessions in which border guards participated.

Below is a summary of the overall border guard feedback for the test cases involving the use of iris as a biometric identifier. Feedback per BCP can be found in the relevant annexes.

Table 22 Overall border guards' feedback for iris enrolment







Summary of border guards' feedback	
 <p>Process</p>	<ul style="list-style-type: none"> • Positive feedback regarding iris pattern enrolment in general; • No specific issues when executed alongside facial image or fingerprint test cases.
 <p>Equipment</p>	<ul style="list-style-type: none"> • Overall, the devices worked quite well and enrolled samples quickly, with the train case proving to be slightly more challenging due to usability limitations (e.g. holding the device in the correct position in a constrained space). However, it did not impact the success rate.
 <p>Traveller</p>	<ul style="list-style-type: none"> • Travellers were mostly positive with the capture of their iris patterns; • No reported complaints about the user-friendliness of the process.

Table 23 Potential impediments and areas for improvement identified by border guards' for iris enrolment

Potential impediments and areas for improvement	
 <p>Process</p>	<ul style="list-style-type: none"> • Set-up: process for enrolment needs refinement, in particular in trains. On the train, it is easier to take the iris scan when the traveller sits down and when the backlight or reflections from the window can be avoided; • In the case of iris patterns capture in cars, guidance to travellers on how to position the vehicle compared to the device helps to shorten the process duration.
 <p>Equipment</p>	<ul style="list-style-type: none"> • Existing mobile equipment can still be improved, in particular in terms of usability; • Devices with an acquisition distance of less than 50 cm seemed to be intrusive for travellers (reported mainly in the moving train tests); • Environmental conditions such as lighting and movement were reported as challenges (e.g. proximity with windows, train motion).
 <p>Traveller</p>	<ul style="list-style-type: none"> • Physical constraints were reported as potential impediments, for example light coloured eyes, those with epicanthic folds⁵² and senior travellers' eyes.

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- Equipment usability, ergonomics and stability could be improved:
 - Some border guards included comments on equipment and suggestions for improvement (mainly related to set-up and ergonomics) to ease process execution by making it easier to enrol biometrics more quickly.
- Environmental conditions should be taken into consideration:
 - Both excess of light and a lack of light can hinder the capture of iris patterns.
- The set-up played an important role, especially outdoors:
 - BCP adaptation was needed to obtain the best results.

2.3.6.2 Travellers' feedback

This section summarises the overall results obtained from a voluntary survey presented to participating travellers after they had taken part in the tests.

The results obtained are generally positive, with satisfaction levels above 84% for TC5. Only 2% of respondents reported being unsatisfied with the process. No relevant differences were detected across the different types of borders.

This contrasts with the findings of the survey performed by FRA with travellers who did not participate in the tests, which shows that more than 30% of surveyed people are uncomfortable with having their iris scanned. This discrepancy could be explained by the differences between expectations and reality when it comes to the process of iris scanning, but also by the fact that travellers who were not inclined to have their iris scanned probably did not participate in the tests in the first place. Additionally, the survey assesses generally satisfaction levels regarding the tests, rather than the levels of satisfaction with the biometric enrolment aspects specifically.

⁵² The epicanthic fold is a phenomenon whereby a fold of skin covers the inner corner of the eye, mainly occurring in many eastern regions of the world, which makes completely opening the eye difficult.

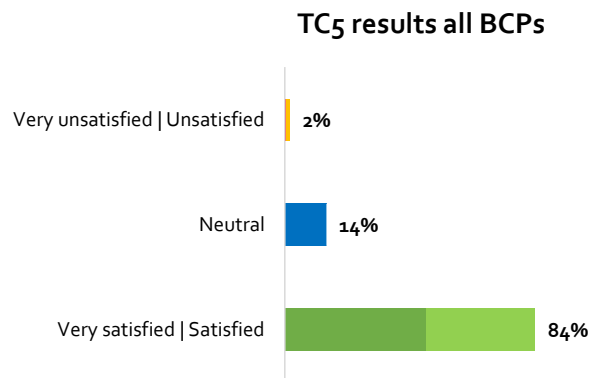


Figure 5 Participating travellers' feedback on the tests (TC5)

2.3.7 Feasibility

This section assesses the feasibility of using the iris as a biometric identifier within the context of a future EES system and at all types of borders, as well as focusing on whether the iris is a valid complementary biometric identifier compared to facial image and fingerprints. The assessment is based on the definition given by ISO/IEC/IEEE 29148:2011 as explained in the methodology chapter annexed to the main report (Volume 2 – Chapter 3).

Building on the results presented in the previous sections on quality and durations, it is possible to draw some conclusions and observations concerning the overall feasibility of using the iris as a biometric identifier at borders.

2.3.7.1 Technical achievability

Table 20 (success) and **Table 21** (duration) confirm the technical feasibility for all type of borders.

2.3.7.2 Not requiring major technology advances

The technology required to enrol the iris as a biometric identifier at the border currently exists and is readily available:

- Different types of iris capture device are available: fixed and mobile;
- Capture devices with different acquisition ranges exist to fit particular purposes and setups.

However, the estimation of the accuracy of the ABIS, based on the sample quality enrolled at long distance and outdoor, showed the limitations of this setup with the current technology deployed outdoor.

2.3.7.3 Users' feedback

The feedback from border guards and travellers in relation to their experience of enrolling irises was generally positive.

2.3.7.4 Fitting with system constraints

Difficulties in enrolling iris patterns were observed in certain weather/environmental conditions (mainly related to excess extraneous lighting or a lack of light). Light protection or extra light should reduce the impact of these constraints in the affected BCPs. The position of the traveller relative to the capturing device and its distance was observed to have a strong influence on the quality of the iris patterns captured.

Train motion was also identified as a challenge for this specific type of border control location. Nevertheless, steps that could be taken to address the issues noted were identified by border guards, e.g. requesting the traveller to sit down to perform the capture.

2.4 ABC gates

2.4.1 Introduction

The increased use of ABC gates is a worldwide trend, with more and more countries deploying e-gates at various BCPs for use by travellers of different nationalities according to criteria set at national level.

By enabling the most routine elements of the border-crossing process to be automated and by accelerating low-risk border crossings, e-gates have been demonstrated to allow efficient handling of growing traveller numbers and allow resources at borders to be used rationally (FRONTEX, 2011).

The current requirements established within the Schengen Borders Code (SBC) provide for more extensive checks to be performed at entry (i.e. VIS check and asking questions to travellers), thus limiting the possibilities for automation. For this reason, the Smart Borders Technical Study identified the possibility of e-gates being used only for exit checks of TCNs holding an eMRTD.

It is assumed at this point, without prejudice to any future policy decisions, that TCNs could cross the border through ABC gates (like EU citizens do), which currently use facial matching as a means of verifying that the bearer of the travel document is its rightful owner (bearer verification), and could be systematically checked against the SIS and other required databases. In this regard, the main challenges are related to the possibility of performing passive authentication of TCNs' eMRTDs, ensuring that the facial image contained in the passport chip has not been altered, and ensuring the validity of facial-image matching for TCNs.

Facial recognition is the principal biometric verification method, as most of the e-gates currently deployed in Europe use it. Storing the passport holder's facial image is compulsory under ICAO standards. Nevertheless, in some cases, the testing carried out as part of the Smart Borders Pilot also included ABC gates equipped with FP scanners, in addition to the facial image.

2.4.2 Objectives

The main objective of this section is to evaluate whether it is feasible for TCNs holding an eMRTD to undergo automated checks at exit. The prerequisite is that the ABC gates use facial matching as a means of verifying that the bearer of the travel document is its rightful owner. Passive authentication – a cryptographic procedure made to verify the integrity of the travel document – should also be performed and its results, reported.

This question will be answered based on the assessment of the operational results of tests in which the following test case was performed:

- TCg: automated exit checks of TCNs.

2.4.2.1 Specific objectives

1. Operational and technical questions for each BCP type

- a. Success / failure: what was the success / failure ratio?
- b. Duration: what is the average time for the automated border crossing compared to the manual booth?
- c. Security: Is the authenticity of the Travel Document checked?

2. Users' perception

- a. Perception of TCNs: what was the traveller's perception of using e-gates?
- b. Feedback from Border Guards: do border guards perceive a benefit having part of TCN's using the automated exits?

Herein, questions of technical and operational achievability are mainly dealt with. The question of risks specific to ABC gates is addressed by analysing passive authentication. Cost aspects are dealt within their own specific chapter (see Chapter 3.4).

2.4.3 Methodology

Success rate

ABC gates are operational at BCPs around Europe for European citizens, registered travellers and in Finland for TCNs of certain citizenships. The aim of this test case is to assess whether the use of ABC gates could be extended to all TCNs at exit. For this purpose, the regular checks performed at the manual booth and a biometric verification based on the facial-image modality should be performed inside the gate. To guarantee the integrity of the facial image stored in the travel document, a passive authentication of the eMRTD should also be performed.

Bearer verification based on the facial image matching should provide enough confidence to supplement a border guard's professional judgement with an automated assessment to help the BG make a decision. For this purpose, the document "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems" was published by FRONTEX in 2012. This publication recommends that facial matching should guarantee a false acceptance rate of not more than 0.1%. While most gates were configured with this threshold, a minority of gates were configured with a less stringent threshold (up to 1% FAR).

The passive authentication of the travel document is also checked, and the success/failure ratio of the operation is indicated to represent added confidence in the bearer-verification process.

The regular checks performed at the manual booth currently also include the border guard calculating the duration of stay and stamping the passport at exit. During the Smart Borders Pilot, these steps could not be done inside the gate, and thus were still done after the ABC gate by a border guard in a manual booth.

Duration

Another important element in the context of an overall feasibility analysis involves comparing the duration of a border-check procedure when performed at an ABC gate with one performed at a manual booth. The ABC gate should represent a faster alternative to the manual booth and improve traffic fluidity.

For this objective, the average duration of an ABC-gate crossing was measured at each testing location and compared to the local baseline that equated to the average current duration of a border crossing (at a manual booth). For the purpose of comparison, the closest process to that of the ABC gate is taken as a reference: at exit of both TCNVH and TCNVE.

The duration of the passive authentication is also measured separately, to provide an indication of the cost, in terms of time taken and additional confidence in bearer verification.

Users' perception

Users' perceptions were assessed based on results of debriefing sessions, questionnaires and surveys. More information can be found in the Methodology chapter annexed to the main report (Volume 2 – Chapter 3).

2.4.4 Testing locations and configuration

Existing e-gates located at the exits of five different BCPs⁵³ have been adapted to also accept TCNs travelling with an eMRTD. In addition, new e-gates were set up at the Gare du Nord and Charles de Gaulle solely for testing. Stamping was performed once the TCN had passed through the e-gate.

The process tested in the scope of the pilot comprises the following steps:

1. Passport authentication,⁵⁴
2. Retrieving the facial image from the chip of the eMRTD;
3. Acquiring a suitable high-quality live facial image;
4. Checking the facial image from the chip of the eMRTD against the live facial image.

Two gate configurations were used in the tests:

- A **one-step process** where the travel-document check and biometric verification take place inside the gate; and
- A **two-step integrated process** where the travel document is first checked outside the gate, and its successful reading is a prerequisite for the traveller to enter the gate and perform the biometric verification.

One-step ABC gates

The verification of the traveller and their secure passage through the border are combined. This design allows the traveller to complete the whole process in one single step without the need to move from one section of the gate or mantrap to another stage.⁵⁵

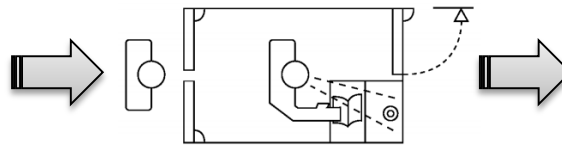


Figure 6 One-step process with mantrap⁵⁶

Integrated two-step ABC gates

In an ABC system designed as an integrated two-step process, the traveller initiates document verification and checks that they are eligible to use the system at the first stage, and then, if successful, moves to a second stage where biometric verification (including checking the live FI against the image retrieved from the eMRTD) and other applicable checks are carried out.⁵⁷

⁵³ In Narva, the ABC gates had been installed just before the start of the tests.

⁵⁴ In some cases, the outcome of the passive authentication was recorded separately, and did not affect the process, while in others a passive authentication failure would result in process abortion and failure.

⁵⁵ Ibid.

⁵⁶ Ibid.

⁵⁷ Best Practice Operational Guidelines for Automated Border Control (ABC) Systems, FRONTEX 2012.

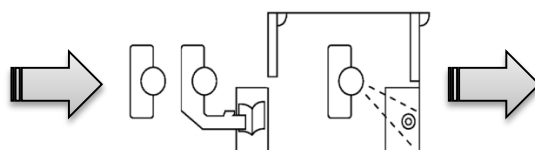


Figure 7 Integrated two-step process with mantrap.⁵⁸

The tests were conducted either as part of the real border-check process (under supervision of a border guard and with subsequent stamping) or as a completely stand-alone test:

- Stand-alone: in this mode, only the processes in the specific scope of the tests were assessed, at an ABC gate outside of the regular border-control zone. Once the test process had taken place, the traveller would then proceed to a real border crossing;
- As the real border-check process: in this mode, existing operational ABC gates were adapted to accept TCNs, and the Smart Borders tests were integrated into the real border process.

Table 24 Testing locations and configuration overview

BCP type	BCP	One-step or two-step ABC gate	Integrated or stand-alone
AIR	(FR) CDG	Two-step	Stand-alone
	(NL) Schiphol	One-step	Integrated
	(PT) Lisbon	Two-step	Integrated
	(DE) Frankfurt	Two-step	Integrated
LAND (road)	(EE) Narva	One-step	Integrated
LAND (train)	(FR) GDN	Two-step	Stand-alone
SEA	(FI) Helsinki	Two-step	Integrated

2.4.5 TC9 (technical and operational) summary results

This section is divided into three main subsections: Quality, Duration and Security. More information can be found in the relevant BCP chapters found in Annexes to the main report (Volume 2 – Chapters 4 to 6), where the results for each of the tests are further detailed.

2.4.5.1 Quality

The aim of the tests was to assess the possibility of using e-gates for the exit checks of all TCNs holding an eMRTD. The success rate encompasses the feasibility of verifying a TCN traveller's identity based on matching a live facial image with the facial image retrieved from the eMRTD chip, at an acceptable FAR of between 0.09% and 1% (as explained above in the section on Methodology 2.4.3).

The table below provides an overview of the results obtained across the various test locations for TC9.

⁵⁸ Ibid.

Table 25 Overview of success rates of ABC gate usage for TCNs holding an eMRTD

BCP	Equipment	Matching threshold	Success rate
Air			
BCP A1	Two-step	0.1% FAR	
BCP A2	One-step	1% FAR	
BCP A3	Two-step	1% FAR	
BCP A4	Two-step	0.09% FAR	
Land: Road			
BCP A5	One-step	0.2% FAR	
Land: Train			
BCP A6	Two-step	0.1% FAR	
Sea			
BCP A7	Two-step	1% FAR	

Key:

	Success rate equal or above 75%
	Success rate between 50% and 75%
	Success rate below 50%

Observations

The following points were noted throughout the tests:

- The main cause of test failure was errors in reading the chip. Some nationalities seemed particularly prone to problems with chip reading, due to a number of causes such as MRZs that were not ICAO-compliant and chips that were wrongly encrypted;
- When the chip was successfully read, facial-image verification was rejected in between 6% and 11% of the remaining cases;
- At one BCP, passive authentication was a prerequisite for continuing to the next step of the process, which explains the lower results obtained;
- A comparison between the quality of the live facial image and the chip facial image indicates that the images from the chip are of a higher quality. Therefore, an improvement in the quality of the live facial image captured in the gate is likely to improve the success ratio of facial-image matching;
- As demonstrated by the tests performed at train and maritime stations, ABC gates could potentially be deployed in train station and at sea border, replacing manual border checks aboard trains or boats;
- At BCPs that have not been designed to host ABC gates (e.g. train and maritime stations), traveller flow would need to be adapted to ensure that each traveller exiting the Schengen area goes through border checks;
- At these BCP types (i.e. train, sea), passengers can carry luggage and/or large backpacks, which the gate's security system may sometimes confuse with an additional passenger in the gate.

2.4.5.2 Duration

In order to compare the time needed to perform a border-crossing procedure at an ABC gate with that at a manual booth, the following durations were measured:

- a. Duration of TC₉, from the moment the traveller places a travel document on the reader to the moment the door opens after the procedure is complete or aborted. Only attempts where the traveller was able to enter the gate (i.e. could complete the step of reading the travel document) are used for assessing the duration:
 - In all cases, biometric verification was performed based on the facial image from the chip and the one captured live at the gate;
 - In all cases, passive authentication was attempted;

- In some cases, fingerprints were captured inside the gate (on average, fingerprint capture took eight seconds).
- b. Duration of a baseline manual check:
- When possible, at exit of both TCNVH and TCNVE, as it represents the same use case as the ABC gate.

The two values were then compared to assess whether the ABC gate process was indeed faster, or how much longer than the manual-booth process it took.

Table 26 Overview of the total duration of the ABC gate process compared to the respective manual-booth baseline

BCP	Equipment	Matching threshold	Duration
Air			
BCP A1	Two-step *	0.1% FAR	
BCP A2	One-step	1% FAR	
BCP A3	Two-step**	1% FAR	
BCP A4	Two-step	0.09% FAR	
Land: Road			
BCP A5	One-step	0.2% FAR	Comparison with baseline made based on border guard assessment
Land: Train			
BCP A6	Two-step*	0.1% FAR	
Sea			
BCP A7	Two-step	1% FAR	

*Tests and baseline include fingerprints

**Passive authentication was excluded from the duration calculation because failures prevented subsequent steps from being performed

Key:

	Average duration below or equal manual-booth baseline
	Average duration up to 25% higher than manual-booth baseline
	Average duration more than 25% higher than manual-booth baseline
	N/A: Comparison with baseline not available

Observations

- Overall, ABC gates can be considered an accelerator, as the process was faster than the manual process at almost all of the test locations;
- One-step configurations were seen to be faster than their two-step counterparts. This is partly due to parallelisation, as a live facial image could be captured at the same time as the passport was read;
- The threshold used seems to have a limited impact on the duration needed to perform bearer verification.

2.4.5.3 Security

Passive authentication was systematically attempted at all locations. In the majority of cases, the result of the passive authentication had no effect on the rest of the procedure and was recorded separately. However, at two test locations, the outcome of the passive authentication could not be recorded.

The duration of this specific step could not be recorded uniformly with each equipment type. Therefore, some durations include the time taken to read the chip, while others only include the cryptographic part of the passive authentication.

Table 27 Overview of the success rate and duration of passive authentication

BCP	Equipment	Success	Duration
<i>Air</i>			
BCP A1	Two-step		
BCP A2	One-step		
BCP A3	Two-step		
BCP A4	Two-step		
<i>Land: Road</i>			
BCP A5	One-step		
<i>Land: Train</i>			
BCP A6	Two-step		
<i>Sea</i>			
BCP A7	Two-step		

Key:

Success		Duration	
	Success rate greater or equal to 75%		Average duration under 7 seconds
	Success rate between 50% and 75%		Average duration between 7 and 10 seconds
	Success rate below 50%		Average duration greater than 10 seconds
	Data on PA not available		

Observations

- Passive-authentication was successful in close to 100% of cases, except when there were problems affecting specific nationalities. In that case, up to 26% of passports (and travellers) had to be refused in the e-gate and pass through manual control;
- Passive-authentication problems seemed to affect specific nationalities and batches of travel documents based on issuance date. Some passive-authentication issues could be solved during the period of the tests;
- The duration of passive authentication never exceeded 11 seconds, including the time taken to read the chip. As passive authentication is a process that could be done in parallel with other tasks (e.g. biometric capture and verification), it is assessed that this process would not be a bottleneck in terms of duration.




2.4.6 Users' perception**2.4.6.1 Border guards' feedback**

Feedback forms were used to gather feedback from border guards across ABC gate testing locations. 85% of all responses collected came from just two locations; however, the synthesis presented below attempts to reflect the different opinions collected during the pilot tests.

In addition, whenever possible, border guards were included in the de-briefing sessions of field visits to gather more qualitative feedback through discussions of test case execution.

Border guards' feedback related to a specific BCP can be found at the end of the chapter dedicated to BCPs. In this section, the border guards' feedback has been consolidated across three dimensions (process, equipment and traveller) to present a higher-level overview.

Table 28 Overall border guards’ feedback for ABC gate usage at exit

Summary of border guards’ feedback	
<p>Process</p> 	<ul style="list-style-type: none"> • The majority of the feedback received regarding the implemented process was positive; • In many cases, it was reported that the authentication mechanism provided by the ABC gates made the border guards feel more confident; • In many cases, and across various locations, border guards indicated that more guidance should be provided to travellers, particularly first-time users.
<p>Equipment</p> 	<ul style="list-style-type: none"> • The majority of the feedback received regarding the deployed equipment was positive; • In general, the equipment functioned well, though there were occasional technical problems resulting in downtime or requiring the ABC gates to be restarted. This was reported in a couple of locations; • In a couple of locations, there appeared to be recurrent document-reading errors associated with specific issuing countries regarding the capture of the chip image from the eMRTD.
<p>Traveller</p> 	<ul style="list-style-type: none"> • The majority of the feedback received regarding border guards’ perception of traveller acceptance was positive; • In many cases, travellers seemed enthusiastic to experience the process. In a few cases, travellers refused to participate upon being presented with a consent form (a requirement of the testing); • There were many cases where travellers seemed to have difficulties using the ABC gates and required guidance from the border guards; • In some cases, language seemed to be an impediment to the process.

Based on the qualitative replies, the following observations and conclusions should be highlighted:

- Overall, ABC gates were well received by border guards and participating TCNs;
- Providing more guidance to travellers regarding the use of e-gates could further enhance traveller and border-guard acceptance;
- Border guards seemed happy with the duration of the process and there were no complaints reported in this regard;
- Recurrent document-reading errors associated with specific issuing countries had a noticeable impact.

2.4.6.2 Travellers’ feedback

This section summarises the overall results obtained from a voluntary survey presented to travellers after they had taken part in the tests.

The results obtained are overall very positive, with satisfaction level above 84% for TC5, with only 11% of travellers unsatisfied with the process. No relevant differences were detected across the different types of borders.

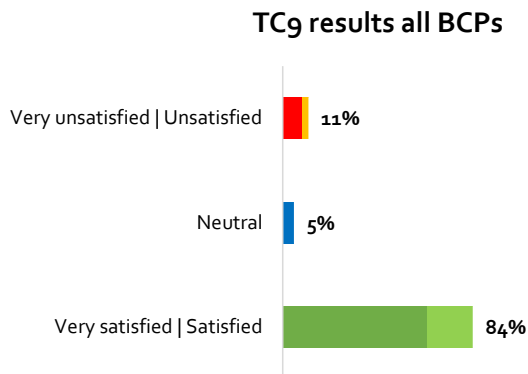


Figure 8 Participating travellers’ feedback on the tests (TC9)

2.4.7 Feasibility

This section assesses the feasibility of applying ABC-gate checks at exit for TCNs, based on the definition given by ISO/IEC/IEEE 29148:2011 as explained in the methodology chapter annexed to main report (Volume 2 – Chapter 3).

2.4.7.1 *Technical achievability*

The aim of the tests was to assess the possibility of using e-gates for the exit checks of all TCNs holding an eMRTD. The success rate encompasses the feasibility of verifying a TCN traveller's identity based on matching a live facial image with the facial image retrieved from the eMRTD chip, at an acceptable FAR of between 0.09% and 1% (as explained above in the section on Methodology 2.4.3).

The table below provides an overview of the results obtained across the various test locations for TC9.

Table 25 (quality) and **Table 26** (duration) confirm the technical feasibility of using ABC gates at exit for TCNs and performing bearer verification on the basis of the facial-image biometric modality.

2.4.7.2 *Not requiring major technological advances*

The technology required at the border already exists and is already operational at several European BCPs.

2.4.7.3 *Users' feedback*

The feedback from border guards and travellers has been very positive. Most border guards are already used to supervising ABC gates, and authenticating the travel document was seen as having a positive impact on the confidence that border guards have in the decisions they make at the border. Travellers are also used to this type of technology, which is becoming standard across the world.

2.4.7.4 *Fitting with system constraints*

Lighting was highlighted as the primary system constraint. While the BCP environment might need to be adapted in some cases, the two primary remedies (light obstruction and light addition) should not present unreasonable challenges and should be able to be implemented.

2.4.7.5 *Can be executed with an acceptable level of risk*

A passive authentication can be performed that reduces the risk incurred by the lower level of supervision/manual document checking during the border-check procedure.

2.5 Kiosk

2.5.1 Introduction

In recent years, self-service kiosks have been introduced at various international border crossing points (mainly outside the EU) with the aim of accelerating the border crossing process. They facilitate delegation of some important but time-consuming tasks concerning the checking of travellers, thereby freeing up time for the border guard to pursue other activities in which his/her involvement is deemed more necessary. Often, the intention is also to speed up the overall border crossing process, thus increasing the throughput without further investments in human resources. The deployment of self-service kiosks is expected to bring the following benefits:

- Higher throughput of passengers (relative to a single border guard);
- Shorter queues;
- More efficient use of the existing space at the BCP;
- Better use of the time that travellers spend waiting ahead of border checks, resulting in potentially improved satisfaction;
- More support in the decisions made by the border guards, given that responses from database consultations would be already available when the traveller arrives at the manual booth/e-gate.

In line with these expected benefits, the Technical Study concluded that pre-border checks could have a positive impact on border crossing time by limiting manual intervention by the border guard and thus make it possible to allocate more time to decision-making. Using a kiosk would be most beneficial at entry, where a lengthier process is currently followed at the EU's external borders than at exit.

It should nevertheless be noted that the use of kiosks as facilitators of pre-border checks or devices which make it possible to capture data in advance are not a complete solution for the entire border check process by themselves. Once the travellers have performed the specific tasks offered by the kiosk, they still need to approach either a manual booth or an e-gate in order to finish the border crossing process, using a token to link both steps.

Kiosks have found an increasing number of applications across the world. For instance, they have been deployed at various airports in and outside the United States⁵⁹, for two US programmes: the Automated Passport Control (APC)⁶⁰ and the Global Entry programme⁶¹. While both aim to expedite the border clearance process, APC kiosks enrol biographic information from the passport and capture a live facial image only, while Global Entry kiosk also enrolls fingerprints. In Europe, kiosks have been deployed at some European consular posts (e.g. in Swedish and Spanish consular posts) for capturing visa applicants' information for VIS and as the first step in two-step segregated ABC gates at some European airports. No kiosks for biometric enrolment have been deployed at borders in Europe to date.

For this reason, the devices used in the pilot were new deployments made purely for trial purposes. Testing therefore provided a good opportunity to assess possible benefits of further automation even where ABC gates are not or cannot be deployed.

Kiosks can accomplish a variety of tasks that together comprise the border clearance process as defined in the Schengen Borders Code. These tasks can be grouped as follows:

- Retrieval of data from the travel document (e.g. optical scanning of eMRTD and MRTD documents; electronic reading of the chip in eMRTDs)

⁵⁹ <http://www.cbp.gov/travel/trusted-traveler-programs/global-entry/locations>.

⁶⁰ <http://www.cbp.gov/travel/us-citizens/automated-passport-control-apc>.

⁶¹ <http://www.cbp.gov/travel/trusted-traveler-programs/global-entry>.

- Verification of personal information (biometric and/or alphanumeric)
- Enrolment of personal information (biometric and/or alphanumeric)
- Questioning of the traveller (e.g. regarding purpose of travel, duration of stay, etc.).

Testing within the pilot focussed on the use of a self-service kiosk for the capture of data from the eMRTD and for biometric enrolment ahead of final checks at a manual booth, in particular in lanes where passengers entered the Schengen Area.⁶² In this chapter, the results of such testing are described and outlined.

The illustration below shows a possible workflow at a kiosk coupled with a manual booth.

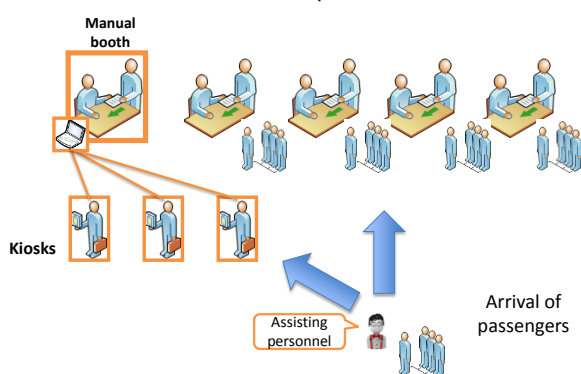


Figure 9 Possible workflow with kiosks linked with a manual booth

2.5.2 Objectives

The objectives of this chapter are to evaluate the usefulness, usability and security of self-service kiosks. These questions are answered based on the operational results of testing on test cases (TCs) 10 and 11, with the latter focusing especially on the use of kiosks at the waiting areas that exist at some land borders.

This question will be answered based on the assessment of the operational results of tests in which the following test cases were performed:

- TC10: Use of Self-Service kiosks;
- TC11: Pre-border checks at Land Borders.

2.5.2.1 Specific objectives

Kiosks test results are used as a basis for answering the following questions and considered according to the following structure. In each section, where possible and appropriate, differences with manual booth processes are highlighted:

1. Technical and operational aspects

- Quality: does the quality of the enrolled data and biometrics vary compared to that obtained elsewhere? If so, why is this? If the quality of biometrics is lower, can measures be taken to prevent this?
- Duration: how long on average does it take a traveller to go through border control from the moment s/he leaves the queue, uses the kiosk and then faces the border guard, compared to the case where all steps are completed at the manual control?
- Security aspects: how can the risk of travellers switching documents and/or spoofing biometric verification/enrolment be addressed?

⁶² In accordance with the Terms of Reference of the Smart Borders pilot project.

2. Users' perception

- a. Perceived benefits for border guards: Do border guards perceive a benefit when self-service kiosks are used?
- b. Perceived benefits for travellers: Do travellers perceive a benefit when using self-service kiosks?

3. Constraints

- a. Which environmental conditions influence the successful use of self-service kiosks?

4. Feasibility

- a. For which type of large border crossings is the self-service kiosk suitable? Which border control operations could be performed by the traveller?

2.5.3 Methodology

The feasibility of using kiosks at European borders is assessed herein through analysis of the following aspects and indicators. Further details on the overall methodology used can be found in the methodology Chapter annexed to the main report (Volume 2 – Chapter 3).

1. Technical and operational aspects:

a. Usability

The process completion rate is provided. It expresses the number of people who could complete the entire workflow of the kiosk without any error, which translates into usability for the end users.

b. Difference in quality and duration of the biometric capture

In comparison to tests described in previous chapters where the focus was on assessing the feasibility of biometric enrolment at different types of borders, in this case the focus was on the benefits in terms of time saved at the manual booth and, by extension, the increased travellers' throughput possible at the BCP. For this reason, the duration of border crossing using a kiosk is compared to the same process carried out at the manual booth.

Furthermore, to be a viable solution for the self-enrolment of biometrics or for their verification, the kiosk must be able to ensure capture of biometrics with at least the same level of quality as those obtained at manual booths under the supervision of a border guard. Therefore, the quality recorded at the kiosk was compared with the aggregated results obtained in testing at manual booths located in the same locations as the kiosks. To allow this comparison for fingerprints, a summary quality score based on the individual NFIQ quality measures of the fingerprints of the right hand (index, middle, ring and little finger) was calculated according to the NIST recommendations⁶³⁶⁴ as explained in the methodology chapter.

The success/failure of verification at a threshold that would result in an FAR of 0.1% was used as the main basis of comparisons of performance based on the facial image biometric across all sites.

c. Security aspects

Experts from Member States and Frontex were consulted regarding possible security concerns surrounding the deployment of self-service kiosks.

2. Users' perception

User perception is assessed from two different perspectives and sources

⁶³ NISTIR 7422 (Tabassi, et al., 2007)

⁶⁴ In cases where no acceptable print was enrolled for a given finger, an NFIQ score of 5 was assigned.

a. Border guards' feedback

The main observations and perceptions of the border guards present during test execution were collected by disseminating questionnaires throughout and by probing some aspects in more depth in discussions following test completion.

b. Travellers' feedback

The perceptions of the travellers who took part in the tests were collected through the posing of a question about their satisfaction following test completion. The question was shown on a touch-screen tablet device and the passenger could choose to answer if he/she desired.

3. Constraints

The various elements that could influence the effectiveness and usability of the kiosks have been summarised based on the feedback received from the assisting personnel and border guards that were overseeing the execution of the tests.

2.5.3.1 Testing locations and configuration

The table below gives an overview of the BCPs where kiosks were tested. In all cases, data was captured from the eMRTD and some biometrics were enrolled. The table specifies the type of border, the biometrics enrolled, the level of supervision of the kiosk during use by travellers and the extent of integration of the kiosk into the existing border check process.

Table 29 Kiosk testing: Overview of test configurations

Border type	BCPs	Integrated/not integrated ⁶⁵	Biometrics enrolled	Assistance provided at the kiosk
Air	Lisbon (PT)	No	8FPs and FI	Continuous: border guard nearby at all times
	Madrid (ES)	Yes ⁶⁶	4FPs and FI	Continuous: border guard nearby at all times
Sea	Helsinki (FI)	Yes	4FPs and FI	Continuous: border guard and/or assistant nearby at all times
Land	Sillamäe (EE)	No	8FPs and FI	None: No (or limited) assistance was provided

While operational testing results are the prime source of material referenced in this chapter, information has been complemented with knowledge provided during consultations with MS experts and Frontex.

2.5.3.2 Limitations

The tests performed had the following limitations:

- **Testing with stand-alone kiosks:** when not integrated, kiosks have been set up in the operational environment with no connection to the real border management IT systems and their use was not part of the border control process. This limited the possibility of testing the full function of an integrated system and only made it possible to compare kiosk usage durations with those for transit through the manual booth according to a different process;

⁶⁵In this instance, integration implies both technical integration into national IT infrastructure as well as use in an integrated process, this is further explained in the relevant BCP Chapters annexed to the main report (Volume 2 – Chapters 4 to 6).

⁶⁶With the exception of VIS consultation, which did not take place at the kiosk during the tests.

- **Limited possibility to test security:** it was not possible to perform comprehensive security tests to assess the ideal level of security, as it would have required the installation of several kiosks and a simulated use of the kiosk by impostors;⁶⁷
- **Non-optimised process:** It should be noted that kiosks are not currently used for checks on TCNs crossing the Schengen zone's external borders. The introduction of this equipment would thus lead to a change in current border crossing processes, as optimisation would doubtless be necessary to both reduce process durations and improve user acceptance. Throughout pilot testing, kiosks were tested without redesign of the existing processes or refinement of the kiosks themselves;
- **Repurposed solutions:** As kiosks for pre-processing of TCNs are not in use in Europe today, the solutions tested were adaptations of kiosks used for other purposes (data enrolment for issuance of passports or kiosks used in segregated two-step ABC gates). The kiosk processes, workflows, interfaces and configurations were not optimised based on user pre-testing or similar;
- **Limited deployment:** within the pilot tests, only a single or very few enrolment kiosks were deployed at each location, making it impossible to measure the actual level of supervision and assistance required. In a real-life scenario, multiple kiosks would likely be deployed and a single border guard or supervisor could potentially supervise multiple kiosks at the same time, thus increasing the benefits;
- **New process:** it is likely that travellers would gradually familiarise themselves with the purposes, functionalities and interfaces of self-service kiosks given repeated use (as has been the case with ABC gates) and the results would therefore improve compared to those described below.

2.5.4 TC10, TC11 (technical and operational) summary results

The information presented in the following points is introduced in order to help assess whether, and to what extent, the introduction of kiosks could improve existing manual border checks for TCNs.

2.5.4.1 Overall success / failure of the kiosk process




This section details the frequency of process errors that meant that a third country national participating in the pilot could not complete the full procedure at the kiosk. Errors were associated with technical faults as well as human error, and sometimes may simply have resulted from the traveller cancelling the process at some intermediate point.

These values provide an indication on the usability of the kiosk but do not consider the quality of biometrics enrolled.

Table 30 Overview of the percentage of cases for which the entire process could be completed at the kiosk in the various test instances

BCP	Process completion at the kiosk
air-1	Orange
air-2	Green
sea-3	Orange
road-4	Pink

Key:

	above 75% completion of the process without errors
	between 50% and 75% completion of the process without errors
	below 50% completion of the process without errors

⁶⁷ The term "impostors" in this case should be understood to imply use by persons actively attacking or misusing the system, thereby trying to deceive the enrolment process.

Observations

- By increasing the number of tasks performed at the kiosk, the overall probability that a traveller successfully reaches the end of the process decreases. This is particularly the case with fingerprint enrolment. Border guards reported that travellers often became confused when re-enrolment attempts were necessary. They also noted that some travellers had difficulties following steps on screen, leading to more issues when more steps were necessary;
- Technical breakdowns of the system caused issues in some cases and influenced the above figures somewhat;
- Some kiosks allowed the traveller to choose which hand to enrol. In some cases, the system became confused, believing that the other hand had been enrolled. In such instances, the traveller often abandoned the process;
- Success rates were significantly lower when both fingerprints and facial image were enrolled, ranging from 33% to 56%.⁶⁸ Enrolment of the FI was more successful than for FPs in all test instances.

2.5.4.2 Quality aspects

Kiosks can be used to capture biometric information for purposes of enrolment and/or verification. The tests that were carried out included the capture of facial image and fingerprints.⁶⁹

The main difference compared to manual processes (in which the same biometrics were captured) was the lack of direct supervision by a border guard to provide feedback, guidance or assistance or to ensure the security of the process through observation. The following aspects could therefore be considered relevant factors that influenced the quality of biometrics enrolled at kiosks:

- The familiarity of the traveller with the process;
- The ergonomics and user friendliness of the kiosks, including the clarity and usefulness of instructions and feedback provided;
- The availability of assistance where required;
- The security of the process and, in particular, the measures taken for the prevention of presentation attacks.

FP quality

As elsewhere, (TCs 1, 2, 3), the quality of fingerprints captured was assessed using NFIQ v1.0 values and counts of the number of minutiae extracted from the prints enrolled. In order to assess whether the self-service nature of kiosks had an impact on the quality of the FPs enrolled, the quality of the fingerprints obtained at the kiosk was compared to that obtained at the manual booth.

⁶⁸ These values are computed ex-post on the data using the standard pilot threshold (NFIQ 2,2,2,3) for fingerprints and for the FI verification a threshold corresponding to a FAR of 0.1%. These thresholds were, however, not necessarily enforced by the device. In these cases, due to reduced demand for re-enrolment, the figures likely underestimate the success rate that could be obtained.

⁶⁹ Enrolment of iris images at kiosks is dealt with elsewhere in this report.

Table 31 Overview of the FP quality comparison between kiosk configuration and manual booth

Test instance ⁷⁰	Summarised quality index ⁷¹	Assistance provided at the kiosk
Air 1	85	Continuous : border guard nearby at all times
Air 2	85	Continuous: border guard nearby at all times
Sea 1	87	Continuous: border guard and/or assistant nearby at all times
Land 1	Insufficient data. On the basis of 21 observations the result would be 90 ⁷²	None: No assistance was provided
Aggregated manual booth results	86⁷³	

Observations

- There were no significant differences in the quality of fingerprints enrolled at the kiosks and at the manual booth. This could be related to the fact that in almost all the test instances, border guards or assistants were present to provide assistance when required;
- The results did not vary significantly across border types. Kiosks were always deployed in indoor environments and thus the environmental conditions varied little;
- Testing at Madrid provides useful comparative information as four fingerprints were enrolled using a 4FP scanner at the manual booth and at the kiosk. The average summarised quality scores calculated were identical, although at the kiosk, a higher quality threshold was implemented and re-attempts had been consistently made when needed.

FI quality

In order to measure any possible difference in the quality of the live facial image captured both at the manual booth and at the kiosk, the success rates of verification were used. Thresholds corresponding to a FAR of 0.1% for FI verification were obtained based on large-scale vendor tests and applied to the data collected in an ex-post manner as necessary in order to allow comparison of results, even if a different threshold was implemented during the testing.

The table below shows the results of facial image verification at the kiosk compared to values recorded at manual booths across all the test instances⁷⁴ for TCs 4, 6 and 7.

⁷⁰ The sample size for the calculation was approximately 1000 observations for each test instance, with the exception of "Land 1".

⁷¹ The figure shown is the average of the index calculated for the four fingers of the right hand, considering also the missed.

⁷² Only a small number of observations were available for this test instance.




⁷³ Calculated based on the observations of all the aggregated manual booth tests.

⁷⁴ For all locations – i.e. the same reference value was used for each of the rows in the table, regardless of the type of borders.

Table 32 Overview of the FI: comparison between kiosk configuration and manual booth for the successful verifications⁷⁵

BCP	Success / failure rate of the FI verification (threshold at 0.1% FAR)
air-1	
air-2	
sea-3	
road-4	<i>Insufficient data</i>

Key:

	success rate equal to or greater than the overall avg. at the manual booths
	success rate lower than the overall avg. at the manual booth with a difference between 10 and 20%
	success rate lower than the manual booth with a difference of more than 20%

Observations

- All the data recorded indicates that there is no reduction in the success rate of automated FI verification when executed at a self-service kiosk rather than a manual booth. In fact, kiosks generally appear to give more reliable verification results than a manual booth equipped with a webcam;
- The success rates also prove that a live facial image could be captured with a sufficient level of quality to be matched to the facial image contained in the chip of the eMRTD;
- In three instances where kiosks enrolling live facial images were tested and in which such live images were also enrolled in another manner (e.g. at manual booth or in an ABC system), verification was most successful at the kiosk. Possible reasons for this could be: a) the assistance provided to the travellers that was typically not offered at ABC gates; b) the auto adjustment of the camera height in the kiosks to optimise the pitch angle which is known to be an important factor to be controlled when enrolling images for automated comparison; c) possible variations in algorithms.

2.5.4.3 Duration⁷⁶

The extent to which kiosk deployments can increase the throughput of travellers going through a BCP, by reducing the time necessary for the border guards to complete the border clearance process, could not be fully assessed within the testing due to the limitations previously explained in section 2.5.3.2.

However, it is possible to perform an estimation based on the test results collected in Madrid, given that the kiosk was integrated with the border control process and the same biometric modality and steps had been tested at the manual booth. Nevertheless, one should note that the duration of the end-to-end process recorded only indicates the time needed for checks to be performed, and not any actual negative or positive impact on traveller throughput for a given BCP. The throughput will depend on the number of kiosks set up, the number of manual booths available and the overall setup of processes, as well as the time needed to proceed through both manual and kiosk-assisted checks noted here.

⁷⁵ Excluding errors that prevented the FI verification taking altogether (e.g. errors reading the passport chip).

⁷⁶ It should be noted that new process definition and optimisation to include the use of kiosks would play a crucial role in this aspect. These testing results should thus be considered with caution. On the other hand, the duration of this end-to-end process only considers individual travellers. The throughput of travellers being checked would also depend on the specific number of kiosks and booths available. It shall be taken into consideration however that the time at the kiosk is time subtracted from the waiting time of the travellers. A number of kiosks can be deployed in parallel, increasing the throughput by saving time at the manual booths.

During the tests in Madrid, it was observed that at a manual booth equipped with a 4FP scanner and a web camera for live FI capture, the entire process took 66 seconds on average. This process consisted of:

- a. Passport reading and consultation of the relevant databases;
- b. Live facial image capture;
- c. Bearer verification based on the FI;
- d. enrolment of four FPs;
- e. Questioning;
- f. Passport stamping.

Steps a) to d) took 30 seconds on average when using a kiosk. In this case, obviously, the process still needed to be completed at the manual booth (for token reading, questioning and passport stamping), which took additional 31 seconds on average. The data suggest that, with this setup, approximately 35 seconds can be saved for each border guard-traveller interaction at the manual booth when the kiosks are deployed as in Madrid. Therefore, assuming continuous flow of passengers to a single manual booth, the throughput at the manual booth could double if enough kiosks are available for travellers to perform the pre-checks.

These benefits would be independent from the type of borders as long as the infrastructure would allow for the deployment of the necessary number of kiosks.

If the kiosk was not used for enrolling biometrics, the savings would be more limited. In Madrid, the passport was used as a token linking kiosk and booth processes. Thus, the border guard needed to scan the passport again despite the fact that the passport had already been scanned and checked at the kiosk.

Estimation of the time saving according to the different use cases of kiosks

As complement to the above results, it is useful to examine what time savings might be achieved with various kiosk configurations. By analysing the average durations for each task undertaken at the kiosks deployed in testing, it is possible to estimate the possible gains that could be obtained by encouraging travellers to undertake tasks at a kiosk rather than a manual booth. The analysis is carried out herein, according to the different use cases of a kiosk that may be envisaged within a potential future EES/RTP process.

The table below summarises the results obtained by using average or estimated atomic durations. These values are likely to be maximum values as it is likely that the process at the manual booth could be optimised to perform some of these activities in parallel, hence reducing their actual impact on the overall end-to-end duration at the manual booth. On the other hand, the actual durations and savings will also depend on the technology chosen for the enrolment of biometrics and on the token selected.

Table 33 Estimated time savings in seconds at the manual booth following the introduction of kiosks (in seconds)

Activities / Kiosk functionality	Passport check Kiosk	Verification kiosk	Enrolment Kiosk		
			4FPs	8FPs	10FPs
Passport check and consultation of DB	15	15	15	15	15
Questions to traveller	10	10	10	10	10
Token verification ⁷⁷	-10	-10	-10	-10	-10
Capture live FI and verification against the passport		15	15	15	15
Verification using FP		7			
Enrolment of 4 FP			15		
Enrolment of 8 FP				35	
Enrolment of 10 FP					44
De-duplication			10-15	10-15	10-15
Maximum time savings (seconds)	Up to 15	Up to 37	Up to 55-65	Up to 75-85	Up to 84-94

Travellers announcing their arrival

An advance passenger check kiosk could be compared to systems that allow passengers to announce their arrival to the BCP. For instance, Estonia has deployed the GoSwift system⁷⁸ that allows travellers to book their appointments for border crossing at three Estonian land BCPs. The benefits of such systems are mainly related to capacity and queue management (particularly critical at land borders) and they allow the forecasting of travellers arrival and the allocation of resources.

The possible benefits of a kiosk integrating such a booking system would be similar to those enumerated for the passport check kiosk, specifically the reduction of the duration of the border crossing process at the booth due to the provision of advance information for database queries, watchlist checks or in case that biometrics are enrolled, biometric information for identification or verification. Nevertheless, it is clear that such a kiosk could be integrated into such booking systems to allow for the prediction of passenger arrivals at the BCP.

2.5.4.4 Security aspects

When kiosks are deployed, elements of the border check process may take place away from the area in front of the border guard. Thus, it is evident that measures should be taken in order to compensate for this possible reduction in supervision.

The main security risks are:

- Spoofing of biometrics (e.g. fingerprints);
- Use of another person's eMRTD to enrol biometrics or to cross the border.

⁷⁷ Token verification is to be added to the process time at the manual booth. The durations will vary according to the choice of the token and of its implementation.

⁷⁸ <https://www.estonianborder.eu/yphis/index.action>.

The required security measures or level of supervision will depend on different aspects, discussed with experts:

- **Functionalities** provided by the kiosk, mainly whether biometric enrolment is offered;
- **Location** of the kiosk;
- Establishment of a clearly demarcated area in which no more than one person is allowed would make it easier to spot people trying to switch identities;
- Kiosks should also be located in an area that allows visual supervision by an assistant or a border guard, even if this means facilitating the supervision of several kiosks at the same time;
- In addition, the use of video surveillance cameras would be advisable to detect if more than one person is using the kiosk. Moreover, cameras could be used to allow remote surveillance of the location of the kiosks and could work as a deterrent against spoofing attempts;
- **Implementation of technical anti-spoofing measures** at the kiosk, such as liveness detection (please refer to the anti-spoofing desk research chapter 3.5 for further information on possible techniques);
- **Token** used to link the kiosk to the manual booth: the most straightforward choice of token is to use the same biometric identifiers as the one enrolled at the kiosk. It reduces the risk of spoofing and confirms that the biometric identifier has been correctly enrolled (the verification would take place at the manual booth in front of a border guard).

While all the above elements will determine the actual need for supervision, one may assume that the location where kiosks may be deployed would require a level of oversight that is equal to or greater, in case of enrolment kiosks, than that advised for ABC gates as both are automated border control devices. According to Frontex's "*Best Practice Operational Guidelines for Automated Border Control (ABC) Systems*", "a single border guard can typically supervise from three to ten e-Gates, although the average number in MSs with operational ABC systems currently sits at five" (FRONTEX, 2012).

However, a key difference exists between ABC gates and kiosks: after passing the ABC gate, a traveller would be authorised to cross the border and for this reason it is essential that the process is supervised by a border guard. This is not the case for the kiosks and thus 'stewards' could be responsible for supervision as a border guard would still take the final decision at the end of the kiosk workflow.




2.5.5 Users' perception

2.5.5.1 Border guards' feedback

To gather feedback from participating border guards across test locations, feedback forms were disseminated throughout testing and a varying number were returned per BCP. In addition, whenever possible, border guards were included in the de-briefing sessions carried out at the end of testing to gather more qualitative feedback on test case execution.

Below is a summary of the overall border guard feedback for the test cases involving the use of kiosks for pre-border enrolment and checks. It should be noted that for the tests in Sillamäe (kiosk at waiting area) there were no border guards on site and consequently no feedback was provided. The feedback in this case came from the border guard authority and the person acting as host at the site. Another point of interest is that in one of the BCPs the kiosk was fully integrated into the operational flow, meaning that when border guards expressed "more confidence", the results appeared to be particularly notable and valid. In other cases, the expressed confidence should be seen more as a general impression.

Table 34 Overall border guards' feedback about kiosk usage

Summary of border guards' feedback	
<p>Process</p> 	<ul style="list-style-type: none"> • A majority of the border guards felt more confident and considered the concept of using a kiosk interesting for future use; • Doubts expressed were in all cases related to the pilot test as such (e.g. how the test was set up, communication/network issues) and concerns as regards the travellers ability to use the kiosk without guidance; • Many noted that the workflow of the kiosk needed to be better adapted to the type of traveller (e.g. visa holder, visa exempt); • Capture of the facial image was less troublesome than fingerprint enrolment; • Many highlighted that the instructions given to travellers when using the kiosk are essential, and should be preferably integrated into kiosk workflows and be available in the most common languages; • Several border guards felt that the kiosks should be designed so that their guidance would not be necessary. Technical functions such as automatic adjustment of camera height were needed, they said; • Most argued that travellers must see a concrete benefit in using the kiosk if they are to be successful in a full deployment.
<p>Equipment</p> 	<ul style="list-style-type: none"> • Most of the border guards found that the equipment worked well; • Overall issues raised were linked to technical problems and the location of the kiosks during the tests. The cases where the kiosks were set up in locations with good ambient lighting and in locations that allowed an easy flow of travellers showed how important these factors are; • Ergonomics and the human interface are essential factors for the optimal use of kiosks; • Technical problems, sometimes related to the specific equipment and how this was set up in the pilot, were reported. Some problems, such as reading of the passport chip, were general issues described that are not specific to kiosks; • Border guards suggested that fingerprint enrolment could work better with provision of real time feedback to the traveller as regards the success of the enrolment; • People with larger hands sometimes had difficulties due to the size of the scanner area in some kiosks.
<p>Traveller</p> 	<ul style="list-style-type: none"> • A majority of travellers were quite enthusiastic about using the kiosks; • The traveller's age seems to be relevant. Elderly travellers had more problems operating the kiosks.

2.5.5.2 Travellers' feedback

This section summarises the overall results obtained from a voluntary survey presented to travellers after they had taken part in the tests.

The results were largely positive, with a satisfaction level above 90%.

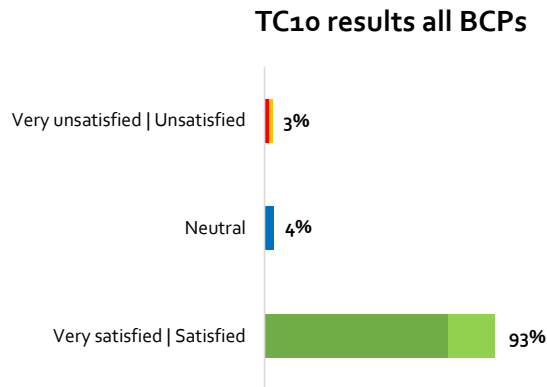


Figure 10 Participating travellers' feedback on the tests for TC10

2.5.6 Constraints/ challenges

During the execution of the testing activities, several points were identified as key success factors for the implementation and usage of the kiosks. All these points require careful consideration ahead of any kiosk deployment at a given border crossing point.

- **Environmental conditions**

When kiosks are used for capturing biometrics (i.e. facial image and fingerprints), light conditions affect the quality of sample enrolled and the rate of process success. Too much external light or shadows can cause problems when capturing both facial images and fingerprints.

- **User-friendliness and ergonomics**

Technical faults and provision of unclear instructions caused losses of time during testing and border guards frequently referenced such issues.

Travellers were more favourable towards solutions that were user friendly and well designed. They were also more positive when assistance was offered.

The clarity and completeness of the instructions provided by the kiosk are important. Border guards frequently mentioned language barriers as having caused problems in kiosk use and language is particularly important when dealing with TCNs.

- **Learning curve of the travellers**

The level of assistance required by the travellers will differ from case to case, depending, among other things, on:

- a. Their familiarity with kiosks of the nature deployed;
- b. Their general technological disposition;
- c. Their level of education.

- **Process optimisation**

It is important to consider how to optimise processes and protocols as decisions made impact overall durations, not only of the individual border crossing, but also on overall throughput of the BCP. One aspect of particular importance is the choice of token for linking kiosk and manual booth processes.

2.5.7 Feasibility and conclusions

This section assesses the feasibility of kiosks for future use in the context of Smart Borders. It is important to note that feasibility can only be fully assessed when knowing the functionalities to be provided by the kiosk. The analysis below takes the most complex kiosk- the biometric enrolment kiosk – as a first example, before examining passport check kiosks as simpler solutions. Only the most complex use case, the enrolment kiosk, was deployed in the tests.

2.5.7.1 *Biometric enrolment kiosk*

Technical achievability

The comparative results previously shown in section 2.5.4 confirm that it is technically feasible to use kiosks to capture data from e-passports and to enrol/verify four or eight FPs and FI. The enrolment could be carried out with the same underlying technology as that deployed at manual booths (contact 4FP scanners and standard cameras), but additional elements are necessary to ensure the security of the enrolment, for instance, additional cameras to detect if other people are in the proximity of the kiosk during the enrolment process.

Not requiring major technological advances

Even though the technology is available, the feedback from the border guards highlights the need for further refinements and a well-designed user-interface.

Users' perception

The feedback from border guards and travellers was generally positive.

Border guards reported that travellers found it difficult to enrol fingerprints, in particular eight prints. This was especially the case when re-attempts were required. Moreover, border guards also noted that elderly travellers appeared to find use of the kiosk interfaces challenging.

Fitting with system constraints

All the kiosks were installed indoors; therefore, the only environmental condition that could negatively affect their functioning was extraneous light from windows.

The main constraints and challenges noted in the pilot related to the travellers from different cultures and backgrounds. Language difficulties were common while development of ergonomic and intuitive user interfaces is a challenge for going forward.

Risk and security

An enrolment kiosk would require high levels of supervision in order to avoid the risk of having impostors enrol. The supervision at the kiosk could, however, be provided by a steward as the final decision to allow the person to cross the border would still remain with the border guard in the manual booth at the end of the kiosk workflow.

By using a biometrics token, the security of the transaction at the kiosk and then at the manual booth would be strengthened, as the biometric verification would take place at the manual booth. Moreover, compared to the setup at the manual booth, additional anti-spoofing technologies might be deployed in order to mitigate risks linked to a self-enrolment.

2.5.7.2 *Biometric verification kiosk*

Technical achievability

Same as the enrolment kiosk above.

Not requiring major technological advances

Same as the enrolment kiosk above.

Users' perception

Same as the enrolment kiosk above.

Fitting with system constraints

Same as the enrolment kiosk above.

Risk and security

A verification kiosk is technically identical to an enrolment kiosk, but one could likely accept a lower level of supervision as the risk relates to that specific verification rather than a first enrolment where impostor enrolment would have negative consequences subsequently.

2.5.7.3 *Kiosk for the passport check*

Technical achievability

There are no technical constraints for the implementation of this kiosk. Assuming that the border-crossing process would rely on the facial image as a biometric identifier, the expected error rate for this would be the same as that described in section 2.2 and in the specific desk research where the reading of the chip of the passport is analysed in more details. There is no specificity related to the kiosk usage.

Not requiring major technological advances

Modern passport scanners are perfectly fit for the purpose.

Users' perception

N/A

Fitting with system constraints

Kiosk would only require sufficient indoor space to allow for their deployment in a controlled area.

Page intentionally left blank

3. Desk research

3.1 Fall-back scenario

3.1.1 Introduction

This chapter presents desk research related to managing situations where the EES is unavailable. The objective of the EES provides the means for abolishing the stamping of passports, thus speeding up border-check procedures and providing information that could be used to prevent and fight terrorism and illegal migration. In order to do so, the EES must record all entries and exits of third-country nationals at the Schengen Area's external borders. In principle, no entry or exit should be possible without being recorded in the EES.

For reasons related to possible infrastructure outage either at national or central level, the EES may not be available to provide the services necessary to fulfil the abovementioned objective. In such cases, there is a need to find solutions that mitigate the consequences of this unavailability: in this document, they are called "fall-back solutions".

3.1.1.1 Objectives

This desk research aims to present potential solutions and procedures for managing cases of EES unavailability and the possible consequences of such cases.

It focuses on EES unavailability, **regardless of the specific individual cause of that deficiency**, without addressing generic border-management issues and without covering the complete border-control process.

3.1.1.2 Attention points

The potential unavailability of the RTP is not explicitly mentioned in this document. The general principle for RTP travellers would be that they enjoy the RTP's benefits at the BCPs where and when it is available. In other cases, RTP travellers would simply need to use the normal process at a manual gate.

Business continuity planning elements are presented as a means of assessing risks and putting the likeliness of EES unavailability into perspective. This must be taken into account when looking at the proposed fall-back solutions.

The use of biometrics and a number of other vital elements of the EES are yet to be decided on. This desk research can therefore only identify potential solutions. In the process of defining the EES, a decision must be made as to how to use the results of the desk research, and only then can the solutions selected be fully developed for future use.

The availability of VIS is a critical factor in being able to verify TCNVHs, a verification that the EES, as concept, relies on. However, it is not in the scope of this desk research to analyse or propose fall-back solutions related to VIS availability per se. The architecture of the EES, and possibly also the architecture of VIS and other central components, are yet to be decided on.

3.1.2 Methodology

The potential solutions in this desk research are based on:

- Exceptions causing EES unavailability, in which a fall-back solution is needed, as identified in the Technical Study on Smart Borders published by the European Commission in October 2014;
- Feedback from consultations with appointed experts from Member States, from the Technical Study on Smart Borders and from eu-LISA's experiences with the existing mission-critical large-scale IT systems operated under its responsibility.

It is based on the following **assumptions**:

- The EES would provide services and carry out functions as described in the Technical Study on Smart Borders taking into account the options presented in the Study. These functions relate to searches in the EES and the verification, identification and registration of data in the EES;
- Although availability requirements have not been defined for the EES, it is assumed that the requirements for searches and registrations would be comparable with, or more stringent than, those for SIS II⁷⁹ and VIS⁸⁰. These systems - as would be also be the case for the EES - already come with a binding obligation to perform consultations on third-country nationals at external borders;
- Unavailability of the EES would have a direct negative impact on the traveller. This would not be the case if SIS II is unavailable and for VIS unavailability its more limited, which needs to be taken into account;
- The policy for the EES is assumed to include a rule stating that all entries and exits must be recorded with 100% coverage. Missing entries or exits will therefore be treated as exceptions in this research;
- The reasons why the EES would be unavailable are not explored in this desk research, unless the reason has a direct impact as regards how to handle the unavailability; and
- This desk research does not address partial unavailability or response-time problems. The solutions presented are aimed at handling cases when it is not possible to use the EES at all.

The **approach** of the desk research is as follows:

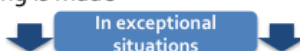
- Firstly, to look at the measures for making the EES highly resilient at central and national level,⁸¹ including the main elements of a business continuity planning process;
- Secondly, to identify and analyse measures that can mitigate the consequences of EES unavailability;
- Thirdly, to look at solutions in exceptional circumstances where no mitigation measures are available.

The approach is presented below from a conceptual standpoint:

- High availability solutions on central and national level could potentially provide an overall availability of 99,94 % for the end-users



- Solutions for electronic buffering would make it possible to search and register in the EES after the crossing is made



- Manual procedures
- Notification system keeping track of outage per BCP (time, date, etc.)
- Status indications in EES related to specific incidents
- Border guards using dedicated web services to get the number of days allowed

Figure 11 Conceptual approach

The overall availability mentioned in the figure above is based on the assumption that the business continuity plan presented in Chapter 2 is fully implemented.

⁷⁹ Commission decision 2007/171 states: "The CS-SIS and the LNI and BLNI must be able to deliver an availability of 99.99 % over a 28-day rolling period excluding the network availability. The availability of the Communication Infrastructure must be 99.99 %."

⁸⁰ The eu-LISA report to the EP in 2014 states: "VIS was designed to offer a high level of reliability, implying full system availability, robustness and data integrity; as such, the system should be fully available to all end users 99.99% of the time."

⁸¹ Including communication networks.

The assumed level of availability at end user level, presented above, could be seen as ambitious, particularly at national level. However, it should be noted that such requirements are related not only to the EES, but also to the mandatory use of SIS II and VIS at the external borders. In relation to the unavailability of the EES and solutions for fall-back scenarios, passenger volumes are a critical issue.

Take, for example, a large airport that handles more than 200,000 entries and exits of third-country nationals (TCN) in 4 weeks.

If the national systems/infrastructure have a required availability level of 99.94% in a “month”,⁸² the number of missing entries/exits would potentially be a maximum of 120. As explained in the figure above, these cases could be handled by buffering and/or other technical solutions or manual procedures (see Chapter 1.4 for details). For lower levels of availability, the number of missing entries/exits would increase as in the table below, for the airport in this example.

Table 35 Consequences of unavailability of national level - volumes

Availability at end-user level (%)	Number of unrecorded entries/exits
99.00	2000
98.00	4000
97.00	6000
96.00	8000
95.00	10,000

This example aims only at showing that the volumes that need to be handled by fall-back solutions would become significantly higher as the level of unavailability decreases. The higher volumes also place more demands on the fall-back solutions. If manual solutions need to be used in exceptional circumstances, the volumes, with an accepted availability level of 95.00%, become quite difficult to manage.

A similar example as the table above but looking at the consequences of central availability is showed in the table below. In this example the estimated volume of border crossings is set to around 240 million (20 million/month in average). This figure reflects the estimate for 2020, mentioned in the Smart Borders Technical Study.

⁸² In this context, a “month” is considered a rolling period of 28 days.

Table 36 Consequences of unavailability of central level - volumes

Central availability (%)	Number of unrecorded entries/exits - month
99.99	2 000
99.98	4 000
99.97	6 000
99.96	8 000
99.95	10 000
99.94	12 000
99.93	14 000
99.92	16 000
99.91	18 000
99.90	20 000

The desk research uses 99.94% (in one "month") as the desired availability level of EES services at end-user level as a baseline in order to minimise the impact of a potential EES outage. The proposed solutions could, however, handle a lower level of availability, though the impact on technical solutions and manual resources would increase proportionally to the degree of unavailability.

Business continuity planning

The implementation, and related costs, of fall-back solutions should be balanced against the likeliness and impact of the EES not being available. To assess this balance, further elements of a hypothetical business continuity plan are outlined below.

It is important to note that the desk research defines unavailability of EES functions as queries/verifications/identifications not being able to be made and **an entry or an exit not being able to be recorded at all**. Any case where checking and recording in the EES takes substantially longer than expected is not taken into account. For example, mobile devices used at border crossings do not always function well. The consequences could be that the checking process could be prolonged and/or checks have to be made at a gate/booth with fixed equipment. This is not considered "unavailability" in the context of the desk research, since the checks and registrations are eventually made. Examples such as this must be handled in national continuity plans using reserve routines for still being able to make the recording/check even if it takes longer.

The outline is based on a conceptual view of the end-to-end solutions for the EES, simplified as an architecture consisting of six levels.

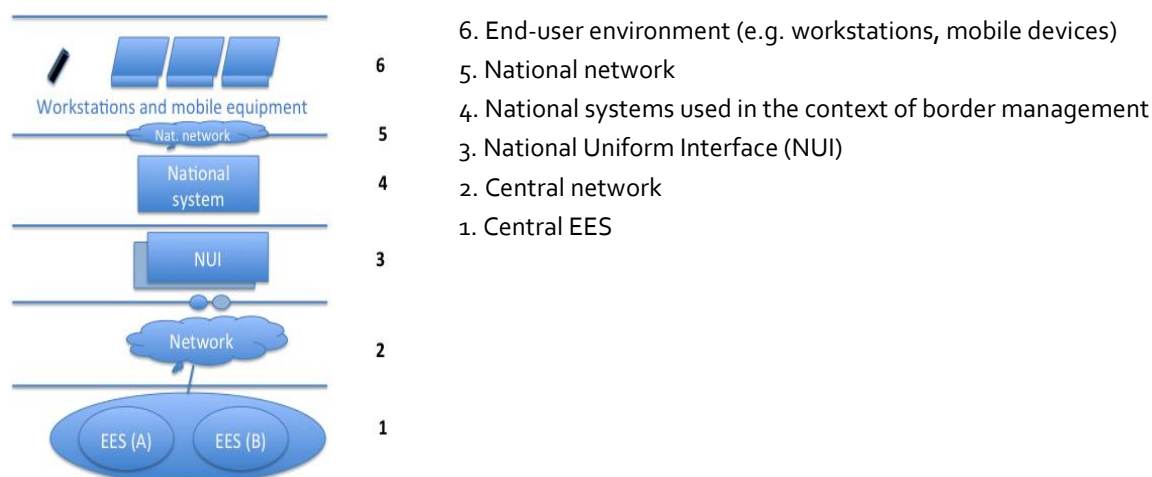


Figure 12 End-to-end solutions for the EES

3.1.3 Architectural requirements

Central EES and central network (level 1-2)

The central EES's availability must be high to ensure that its objectives are reached. It could be assumed that the services of EES, including the central network and any related central components, would have a service-level agreement (SLA) corresponding to an availability of 99.99% in a "month". To reach such a level, the following main elements are needed:

- A central back-up system, mirroring the EES, preferably with an "active-active" configuration;
- High availability, overcapacity and redundant components at a network level, including back-up access points for Member States' connections to the network;
- An infrastructure that includes solutions for an uninterrupted power supply (UPS) at central and network level, in line with the SLA;
- Procedures and routines for supervising, managing and taking countermeasures promptly when blocking incidents occur;
- A fully integrated and enforced testing and release management policy, including the possibility to simulate the process in a near-operational technical environment;
- Maintenance would be planned for periods and times of day with very low volumes in relation to EES queries/updates, thereby keeping to a minimum the volumes that need to be buffered at NUI level (see Chapter 3.1.4.1 on Electronic buffering) and the amount of queries that could not be performed.

NUI (level 3)

The NUI would basically function as an intermediary between national systems and the central system, providing the services for accessing the EES and taking care of the necessary buffering, etc. It should have at least the same SLA requirements as the central EES and would therefore require fundamentally the same elements of resilience to reach this level, tailored to the size and throughput of the NUI. It should be noted that even if the NUI has this high level of availability, its usefulness depends on whether national systems and networks are available and can access the NUI.

National systems and national networks (level 4-5)

The use of the term "national systems" is quite widespread. In this context, it includes all the national systems that contain the business logic for serving the border checks, excluding the presentation layer to end users. These systems fall fully within the remit of the Member States. To achieve the full objectives of the EES, it must be assumed that these systems, and their related infrastructure, would need to be designed with the same SLA as the central EES. The

same features designed to provide high availability as described for the central EES should be addressed (e.g. UPS, redundancy, procedures, advanced testing of releases and monitoring).

End-user environment (level 6)

The end-user environments are also assumed to have the same level of SLA as the central EES. The IT architecture is different for each Member State but it can be assumed that the main elements related to the availability of end-user environments will have an uninterrupted power supply and will perform exhaustive testing on new/changed applications.

3.1.3.1 Overall availability of the EES

The assumption for the business continuity plan presented is that each of the 6 levels presented above would have the same SLA requirement (i.e. 99.99%). Should this not be feasible to achieve, the proposed solutions for electronic buffering are still valid but the volumes needing to be handled during buffering would increase.

In a worst-case scenario, when unavailability at all levels occurs in the same timeframe, this would mean a total availability of 99.94% at end-user level. In practice, this means 26 minutes of potential unavailability for a given BCP during one month.

It should be noted that in the potential period of unavailability, it is only the lack of performing EES searches that has a direct impact on border guards' work. With the solutions for electronic buffering described in the next section, the EES search and entry/exit updates could be made after the person has left the border crossing point.

3.1.3.2 TCNVHs - specific conditions

When looking at solutions to mitigate EES unavailability, the difference between handling TCNVHs and handling TCNVEs must be considered. The future architecture into which the EES, RTP and also VIS will be implemented is yet to be studied and decided on. At any rate the need to enrol fingerprints at the border should not concern TCNVHs. It is also assumed that these travellers' credentials should be verified against VIS, as is the case today, and not against the EES.

In other words, if the EES is unavailable, the inability to run a search in the EES is not as vital for checking a TCNVH as it is for checking a TCNVE and there is less data to register in the EES. Nevertheless, creating an entry/exit record is mandatory for TCNVHs, and this must be considered in the business continuity plan.

VIS currently resides on a dedicated platform, with its own infrastructure and its own usage of the central network. The Technical Study outlines options where the EES and RTP are separate systems, as well as alternatives where they are part of a common architecture, including the current VIS functions. In a scenario where the EES and VIS share resources, the unavailability of central resources would have a different impact, and this would have to be taken into account in business continuity planning.

The desk research primarily addresses the unavailability of the EES, though the availability of the VIS needs to be taken into account for TCNVH travellers. As long as VIS can be accessed at end-user level, these travellers can be verified. This would be possible even if the EES is not available, if these systems are separated in terms of architecture and infrastructure.

3.1.4 Fall-back solutions

The measures outlined in the business continuity plan would enable the central EES and the functions of the EES at end-user level to reach a high level of availability. However, in the event of EES functions being unavailable, there would need to be other solutions for maintaining the data in the EES. This chapter looks at a number of potential solutions.

3.1.4.1 *Electronic buffering*

When the central levels (levels 1 and 2) are unavailable, electronic/automated solutions could be used for capturing and buffering travellers' alphanumeric data and biometrics at national level, which would be entered into the system later. It should therefore be possible to capture all alphanumeric and biometric data necessary for full EES registration. A successful implementation of electronic buffering would, to a large extent, mitigate the consequence in terms of missing entries and exits.

The buffering solution does not cover cases where the EES should have informed the border guard that a person is an over-stayer. The border guard cannot provide the traveller with this information. A possible solution would be for the border guard to use the web services proposed in the Smart Borders Technical Study to check the number of days for a given person. If the web services are not available, the problem could only be dealt with at subsequent crossings.

There is no way of determining whether it is the first time that the traveller is crossing the border at entry. Data and biometrics for the individual file must therefore be acquired and buffered for every traveller.

The data buffered locally must be automatically flushed after its registration in the EES is acknowledged as complete.

Once the EES is again fully available to end users, search and registration could be performed with a high degree of automation, meaning that the buffered data is used for automated searches and batch registration with little intervention needed from the border guards. If the EES search shows that it is the first border crossing for a traveller, the individual file is created.

If the buffered data indicates a first-time crossing by a TCNVE, the fingerprints buffered could be used for identification purposes (1:n)⁸³ in the EES. If it is found that the person appears in other individual EES files, this could possibly be flagged for later action by looking at a method for "marking" the EES record (i.e. setting a status flag) in order to check the person more thoroughly the next time they make a border crossing.

The value of identification (1:n) of a TCNVE in this scenario is somewhat doubtful, since the person is no longer present to answer any questions related to possible findings or problems when performing these checks.

When using the buffered data and finding the person in the EES, and where the person is a TCNVE, their biometrics (i.e. fingerprints or facial image) could be used to verify their identity. If the verification yields negative results, this could possibly be handled by looking at a method for "marking" the EES record (i.e. setting a status flag) in order to check the person more thoroughly the next time they make a border crossing.

Border-control process

This section describes an excerpt of the border process related to a situation where EES functions are unavailable and where electronic buffering is used. The process described is on a logical level and does not take into account technical solutions not yet decided on. In the process below, the VIS is therefore regarded as a separate source of information not impacted by the EES being unavailable.

⁸³ 1:n identification is proposed as an option in the Smart Borders Technical Study. The text regarding this option is only valid if it is retained in the final solution for the EES.

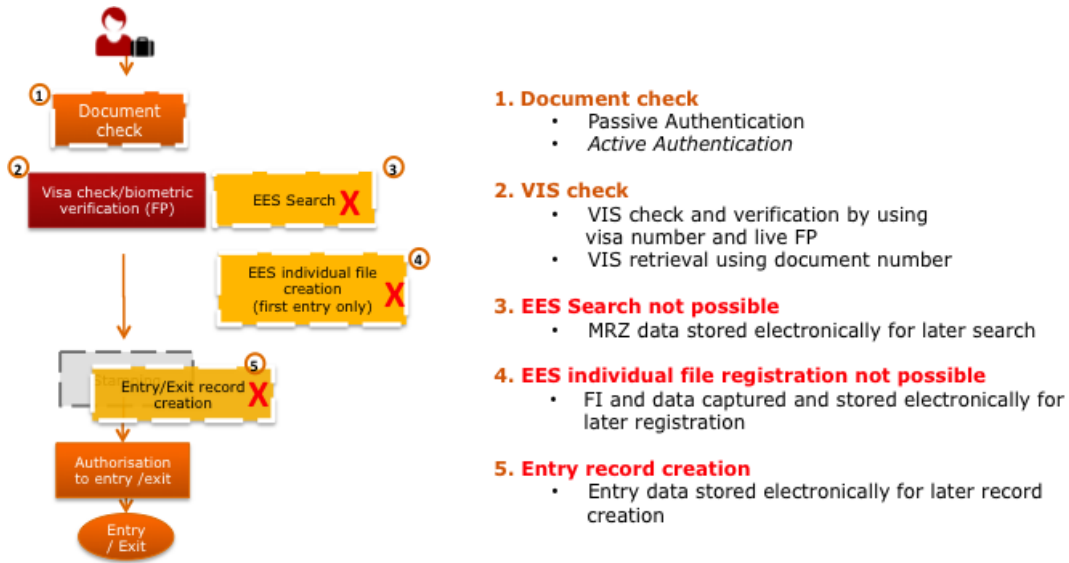


Figure 13 Process for border check at entry when the EES is not available - visa holders

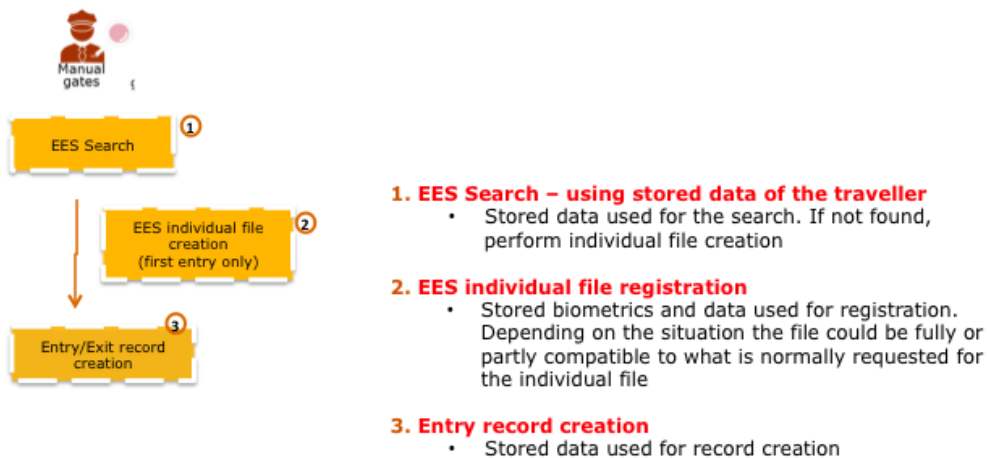


Figure 14 Search and registration of data and biometrics at entry - visa holders

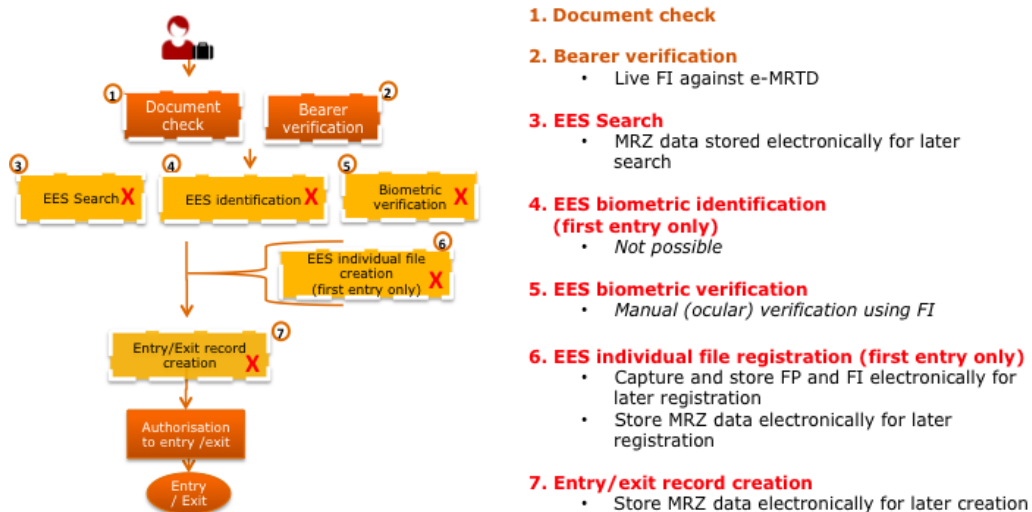


Figure 15 Process for border check at entry when the EES is not available - visa-exempt

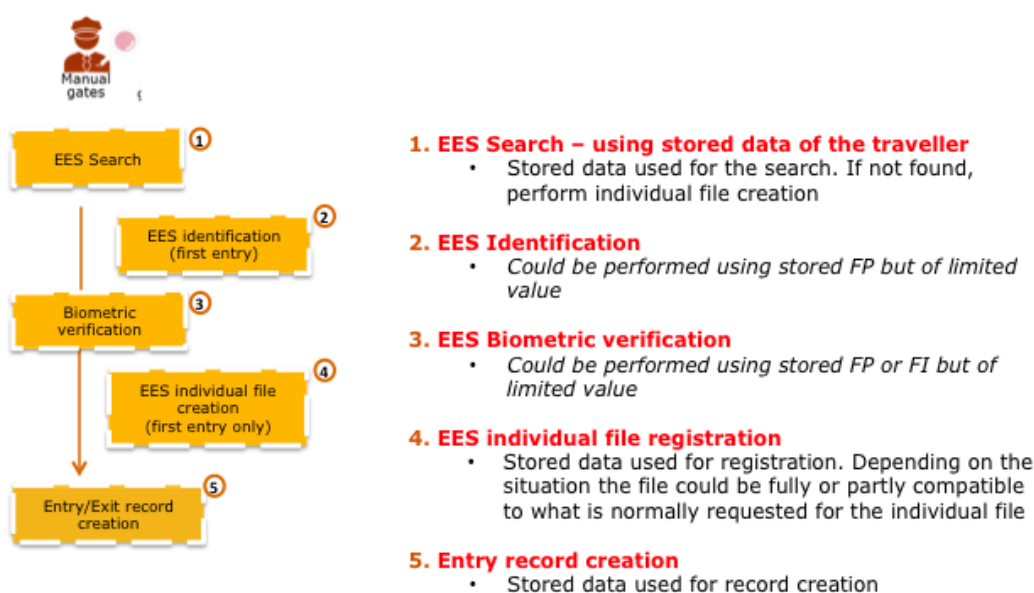


Figure 16 Searching and registering data and biometrics at entry - visa exempt

Process at exit

The process at exit contains a subset of activities from the process at entry. According to the current version of the Schengen Borders Code, some checks are not mandatory at exit. As regards the EES, it is proposed that creation of the individual file and, possibly, 1:n identification, would only happen at entry.

However, an EES outage at entry could make it necessary to create an individual file at exit and - if chosen as an option for the EES - to make an identification. It is also important to note that if a traveller arrives at exit, then a missing entry caused by an EES outage could make the process cumbersome. These and other impacts are described in the "Business impact analysis" section.

3.1.4.2 Technical and architectural aspects

The solutions for electronic buffering can be implemented on different levels nationally, where the last resorts for buffering are workstations or mobile devices used by border guards. One can safely assume that mobile devices are designed to cope with a shorter period of outage than workstations, the national system and/or the NUI.

Of the six levels of architecture presented in the business continuity plan, the upper three levels, on the national side, would all be targets for implementing solutions that can buffer data and biometrics. At each level, it should be possible to buffer data independently of the other levels. Each level is further elaborated below.

Aspects to consider:

- National end-user applications, devices and systems would have to be adapted in order to cater for buffering and the lack of a search function against the EES;
- Asynchronous communication should be possible between the architectural levels, in the event of an outage, when electronic buffering is used;
- Depending on the architecture of the national systems, it may or may not be possible to perform electronic buffering at workstations and/or on the mobile devices used. In those cases, it is proposed that the national systems should handle the necessary buffering. In the cases where buffering can be done at workstations/on mobile devices, it would be an option not to have any functions for buffering in the national system;
- Buffered data must be secured for data-protection reasons.

Buffering at NUI level

The NUI could contain functions for storing data and biometrics when the EES is not available, as well as functions for automated searches and registrations once the EES is available again. It is possible for automated registration to cover all types of cases, thereby avoiding the need for manual intervention. Exceptions would be notified to the border guards (i.e. back-office functions of the BCP).

This solution would have the benefit of enabling border guards to continue to work more or less as normal, except for real-time searches, which cannot be performed at the time that the person is checked. If the central EES or the central network are out, the national systems could in principle continue to function as normal.

As regards the technical challenges for performing the buffering, search and registration, the following factors should be considered:

- Concurrent updates of a traveller's EES data from other end users (e.g. another NUI) are quite unlikely to occur since the update relates to the individual traveller crossing (or having just crossed) the border. The NUI function for creating EES records can be built on this assumption;
- EES data for a specific individual should not be dependent on or related to data pertaining to other individuals in the EES. There should therefore be no need to implement a complex queuing and transaction-handling process to perform the registration;
- The registration function should not need to update existing data, but instead would add data into the EES, either a new EES individual file with an entry/exit record or only an entry/exit record. Corrections or updates of individual fields in existing files should not need to be included as a function;
- The NUI should be able to buffer data coming from the national systems when the central EES is not available, and once the EES is available, it should be able to balance the frequency of batch searches/updates (i.e. Flow control implemented) sent in order to minimise the impact on the central system. However, the central system does also need to be able to handle peaks, within reasonable limits, in buffering and batch searches/updates made by the NUI.

Buffering in national systems

If the NUI is not available or cannot handle the abovementioned electronic buffering, the national systems in the Member States could be implemented with the aim of covering the need for electronic buffering.

It would be quite complex to centrally develop the function needed and implement it into the national systems. It could, however, be feasible to develop common specifications for buffering at national level that MSs would use to develop their national systems. As part of the solution, there should be corresponding functions of the NUI, to be used for "batch" searches and registration once the EES is available.

This kind of solution could be used as a complement to buffering by the NUI, thereby limiting the risk of not having electronic buffering available.

Buffering at workstations/on mobile devices

In certain cases, an alternative option could be buffering data and biometrics locally at border guards' workstations and on their mobile devices. Member States would - as in the case with buffering in national systems - implement these kinds of solutions, preferably through common specifications used by all Member States. The NUI could contain functions for later "batch" searches and for registering data buffered at workstations/on mobile devices.

3.1.4.3 *Alternative solutions for exceptional circumstances*

The electronic buffering described in the previous section should in principle cover 100% of cases where the EES is not available. In rare cases where the electronic buffering described is unavailable (i.e. buffering at levels 3 to 6 is not possible), alternative solutions could be explored.

The table below summarises potential solutions looked at for handling buffering in exceptional circumstances. A scoring system of - up to ++ is used to assess the solutions, with ++ being the most positive in relation to the column's heading. If it is decided that the solutions described here are worth pursuing, they would need to be studied further and elaborated in detail. This is outside the scope of the desk research.

Table 37 Summary table of alternative solutions

	Usefulness	Basic functions	Maintenance	Cost efficiency	Security
Common mobile devices	+	+	-	--	-
Mobile application	+	+	-	-	-
USB for workstations	--	-	--	+	--
Alternative communication channel	-	++	--	-	+

Common mobile devices

An idea could be to set-up and make mobile devices available to all BCPs, or to BCPs that are seen as having high priority. These would be used only in cases where "normal" electronic buffering does not work, for instance if a power outage goes beyond what the UPS can handle, leaving end-user workstations without electricity.

Existing mobile devices already used by the Member States for regular checks could also be used to buffer data. However, they would be integrated into the national infrastructure, which could make them more vulnerable in the event of an EES outage. Still, this is an alternative and should be part of a business continuity plan.

The mobile devices would include basic functions for capturing and storing alphanumeric data, and possibly also biometric data. As soon as the national infrastructure starts working again, these devices could empty their buffered data to be forwarded to the NUI via national systems and processed into the central EES.

The basic functions would be developed centrally and uniformly across the devices deployed.

In general, this idea was considered worth pursuing further by the participants at the experts meeting. However, the experts also saw a number of issues that need to be looked at and analysed further.

Comments from the Member States' experts and internal discussions at eu-LISA point to the following areas that need further investigation.

Basic functions of the devices

The basic functions would be the same as what the border guard normally uses for the EES, with some limitations. Search functions are not possible and the device would be offline when used for buffering. The core functions would be capturing data and biometrics for the individual file and recording the entry/exit. An option put forward at experts' meeting was to agree only to gathering and registering alphanumeric data, thereby reducing complexity and costs. The consequence of this agreement would be that in cases where biometric data is not registered in the individual file at entry and biometrics, it would not be possible to verify a traveller's identity on exit.

Once it is possible again, the device would connect with the NUI via national systems and empty the buffered data. This would be treated by the NUI as any other buffered data coming from national systems.

Maintenance

The devices would have to be kept under central maintenance by eu-LISA, including normal activities such as release management, troubleshooting/incident management, regular function tests and correctional updates. Remote access to the devices would be needed, either through national networks or via separate communication channels. There would also be a need for continuous training activities to ensure that the border guards are familiar with how to use the devices.

Cost efficiency

Given the high availability of the central and national solutions, as well as electronic buffering solutions in the case of EES unavailability, the devices would be used relatively rarely. It is safe to assume that they would stay untouched for long periods. The balance between the devices' added value and their costs would have to be considered. For instance, only selected BCPs could be provided with the devices, with a priority for those with high volumes. A risk of the rare use of these devices could be unfamiliarity with the devices when needed, causing users problems and leading to incomplete registration.

Security

National security rules and technical solutions must be taken into account when defining a solution that includes mobile devices deployed by an external entity, as seen from a national perspective. The problems of solving these issues are less complex when it comes to using the device for offline buffering of data and biometrics. The challenges in this area relate to how to transmit the buffered data in the devices, via national systems, to the NUI, where it is necessary to pass through national firewalls and other security solutions. Firewalls and other relevant components would normally have different configurations in each Member State, and communication from the device must be compatible with all of them.

Mobile application

An alternative to the mobile devices could be to develop an app that would contain the basic functions needed for buffering data and electronics. The buffered data would have to be transmitted to national systems via secure communication and passed on to the NUI. This would mean that MSs already have a mobile device available.

Basic functions of a proposed app

The basic functions would be the same as in the mobile device. The app would have to be compatible with the main mobile operating systems available on the market (e.g. Android, iOS), downloaded via a secured website (or a public catalogue if security solutions exist for such a solution).

Maintenance

The app would be centrally maintained, including normal activities such as release management, troubleshooting/incident management, regular function tests and correctional updates. Specific procedures or solutions would be needed to ensure that end users regularly update the app to the newest release and always do so before using the app for buffering. There would also be a need for continuous training activities to ensure that the border guards are familiar with how to use the app.

Cost efficiency

Compared with mobile devices, the possible advantage of an app is that there are no extra costs if the app remains unused. Maintenance costs are therefore likely to be lower and there would be no need to prioritise the BCPs, which would be provided with the app.

Security

National security rules and technical solutions must be taken into account when developing and using an app for buffering. As is the case for mobile devices, offline buffering should not be a security issue but communication from the app to the NUI must be compliant with national security rules and solutions.

USB with mobile communication network at workstations

An idea proposed by MS experts was to look at using USB with a mobile communication connection (3G or future versions) to store and later communicate buffered data to the NUI. This would work as a fall-back solution when workstations are available but the national systems are not.

Basic functions

Using the USB for buffering and communicating buffered data would require either that all end-user workstations contain a specific centrally developed application only used for this purpose and these situations, or that national end-user applications are designed to be able to switch to interface with the USB instead of their normal communication route.

Maintenance

The USB would have to be developed and deployed centrally. A specific application to be used for this purpose would also have to be developed and maintained centrally. The problem in this case could be the mechanisms used in each Member State for including a new application at workstations and/or for updating them. The central functions for propagating the application would have to comply with all variants in this area used by Member States. There would also be a need for continuous training activities to ensure that the border guards are familiar with how to use this separate application in exceptional cases.

Cost efficiency

The USB as a solution would only work when the workstations are still functioning. It therefore does not cover the business needs in the same way that a mobile device or an app for mobile phones would. USB would have to be deployed to all workstations at all BCPs, or to the ones that are selected due to defined priority rules, as is the case for mobile devices. If a common application is used, it must be deployed to and maintained at all BCPs, or the ones that have been given the USB. A central application would also have to be updated and tested in the cases where the workstation environment is changed at national level. If the national applications are to interface with the USB, they must do so at all BCPs using USB and maintained in accordance with central changes to EES data.

Security

National security rules and technical solutions must be taken into account when integrating solutions to the end-user workstations. This puts requirements on compliance for the USB, its communication ability and a common application used for registration to the USB. Communication from the USB using 3G (or future versions) would also have to comply with national security rules, firewalls, etc. An alternative would be to use the USB only for buffering; in that case, the USB would have no external communication feature. The data would then have to be emptied to the workstations and forwarded as buffered data to the NUI.

Alternative communication channel

A solution already used in one Member State is to have the workstation and the concerned applications adapted so that they can use an alternative communication channel when national systems or networks are experiencing an outage. This could mean, for instance, that buffered data would be sent directly from the workstation to the NUI without passing through the national systems and the “normal” national networks.

This solution would be an alternative that is not developed centrally. It would be up to each Member State to assess whether it would be of added value, hence why there is no further detailed assessment in this document. The

buffered data sent and communicated to the NUI would have to comply with the specifications of the NUI's functions for the purpose of receiving buffered data.

3.1.5 Manual procedures

A business continuity plan similar to the one outlined in this document, together with solutions for electronic and mobile buffering, means that manual procedures would only need to be used in exceptional circumstances.

If it were not possible to buffer and register data, the EES would have a missing entry/exit, and if the earlier crossing were the traveller's first crossing, it would contain no data on that person.

In accordance with the existing procedure in the Schengen Borders Code (Article 11 on procedures when stamps are missing), there could be a similar procedure for amending/completing EES registration for travellers arriving with a missing entry or exit.

Another slightly more radical option would be to amend the Schengen Border Code to instruct border guards to modify the EES by marking the entry or exit that corresponds to the missing entry/exit (explained below) as not valid for calculation of the travellers stay. Either Option A or Option B should be chosen by the legislator as a way to handle such situations.

3.1.5.1 Option A

The border guard could enter the missing entry or exit record separately, register the individual file where relevant, or register the entry/exit for the present border crossing made by the traveller. A notification system could serve as complementary information to ensure that the traveller's information/evidence on which the BCP was passed and on what date, could be better validated.

Besides the actions mentioned above, the border guard should carry out all relevant registration, identification and verification procedures for the TCN, as is mentioned for cases where electronic or manual buffering is possible, taking into account that any potential earlier border crossing is not recorded in the EES.

A status indication in the EES should appear whenever a missing entry/exit is entered onto the system retroactively.

For the manual procedure of making the EES data complete, there is a future choice to be made as to whether to retain physical stamping or a similar solution.⁸⁴ The purpose of the physical stamp would be to serve as additional evidence of the missing entry or exit. A trade-off would be to accept - for the extremely limited number of cases that occur - that there would be less firm evidence, in the form of stamps, of the date and place of the missing crossing. It should be noted that any solutions involving stamping must be implemented at all BCPs in the Schengen Area if they are implemented to serve the purpose described here.

Basic functions

This solution is built on the existing procedures of the Schengen Borders Code and does not require any additional specific technical solution to be implemented.

⁸⁴ The notion of "physical stamping" could include alternatives to the existing way of stamping, for instance by using a note with a unique number to the traveller, using a printed sticker or automated stamping mechanism. However, all of these alternatives would involve costs, continuous training and maintenance.

Maintenance

With stamping: the routines and equipment for manual stamping would have to be kept and updated continuously. Stamping would be very rare but there would still be a need for regular training to retain knowledge of it.

Without stamping: no maintenance needed - the procedure would at any rate be included in standard training.

Cost efficiency

With stamping: costs for keeping the stamping procedures, training, equipment, etc. would still remain.

Without stamping: no costs for maintaining stamping and virtually no costs at all for this alternative.

Security

With or without stamping, there is no security impact related to border management systems or procedures, compared to the current level of security.

3.1.5.2 Option B

This option is built on a further simplification of the process where it is also taken into account that the burden of proof on the traveller would be lower for the very rare cases where manual procedures are needed.

For example: a traveller arriving to make an entry has a missing exit linked to a previous visit to the Schengen Area. Depending on how much time has elapsed since this missing exit, it could be difficult for the traveller to present any evidence. On the other hand, it could be difficult to prove that the missing exit is not due to a malfunction of the system or to human error.

A radical step could be too simply - using the example above - to mark the data regarding the last entry (in cases where a subsequent exit is missing) and continue with ordinary processing, including recording the traveller's current entry. This record would then not be used in calculation of the duration of the stay.

Basic functions

This solution is built on amending the Schengen Borders Code and does not need any specific technical solution to be implemented.

Maintenance

No maintenance needed, including for stamping since this is not needed. But at any rate, the procedure would be included in standard training.

Cost efficiency

No costs for maintaining stamping and virtually no costs at all for this alternative.

Security

There is no specific security impact related to border management systems or procedures, compared to the current level of security. The loss of already recorded data is itself inducing a risk there would be a number of days for the stay concerned that are neither recorded in nor subtracted from the total duration of the traveller's permitted stay. However, this would only occur in the very rare cases where the procedure is used.

Table 38 Comparing manual procedures for EES completion

Option	Basic functions	Maintenance	Cost efficiency	Security
A.1 Border procedure for completing EES registration (possibly using a physical stamp as evidence for the missing recording)	N/A	+	+	Neutral ⁸⁵
A.2 Border procedure for completing EES registration	N/A	++	++	Neutral ⁸⁶
B Border procedure for completing EES registration by removing an entry or exit that has is not complete	N/A	++	++	-

3.1.6 Additional supporting solutions

Besides electronic buffering, there are other solutions that could help provide relevant information when the EES is unavailable, giving end users or travellers the information they need.

3.1.6.1 Notification system

Information on outages can be used for helping border guards make a decision when travellers appear without a complete EES registration and it is necessary to prove that this incompleteness occurred at a BCP and at a time when there was an outage. It could also be useful data for statistical purposes. Therefore, it could be an option to implement a notification system. This would involve national systems, where information on local outage would be sent to the central level and central EES functions could also detect outages not related to the central system itself.

3.1.6.2 Status indications in the EES

When the EES is updated using buffered data, or in other situations where normal routines are not followed, a status indication could be set in the EES. This would indicate, for example, the need for extended checks of the EES to ensure quality or the need to complement the EES file.

3.1.6.3 Web services for border guards

Even with electronic buffering, there may be situations where the EES search is unavailable. This means that the border guard would not be able to see whether the traveller has enough days left and the traveller would not be able to be informed about this. A proposed mitigation for this would be for the border guards to use web services intended to serve carriers and travellers with information on the number of days of the authorised stay that have been used. **The usefulness of this proposal depends on how the web services are to function and if it is permitted (e.g. in relation to security requirements) to use a separate network.**

3.1.6.4 Limited dataset - used as an exception

A proposal from the experts' meeting was that a limited dataset (i.e. alphanumeric data only) might be used to register the individual file in the EES, in exceptional circumstances and if this measure would make for a more feasible solution for electronic buffering. This solution would mean that the biometrics would have to be enrolled and added to a person's individual file the next time they cross the border.

⁸⁵ Making the registration in the EES complete should have the same impact on risks as the current procedure for handling missing stamps.

⁸⁶ Ibid.

3.1.7 Business impact analysis

The business impact analysis below is a summary of the impact of different scenarios of EES unavailability for travellers and border guards. The analysis is built on the assumption that solutions for electronic buffering would be implemented. For each scenario, the impact is firstly described for the crossing when the EES was unavailable and secondly for the subsequent crossing.

Table 39 Business impact analysis in case of EES unavailability

	At entry	At exit
A: Electronic buffering and later registration of all data and biometrics is possible		
Impact on border guard (at crossing)	<ul style="list-style-type: none"> No search can be made in the EES; No verification of the number of days remaining for the authorised stay. The planned web interface could, however, be used to obtain this information if it resides on a separate network; Identification of TCNVEs (if first entry) is not possible; No registration of the individual file in the EES (if first entry); No biometric verification of travellers already entered in the EES can be made in the central EES; No entry record is created. 	<ul style="list-style-type: none"> No search can be made in the EES; No way of using the EES to verify the number of remaining days. The planned web interface could, however, be used to obtain this information if it resides on a separate network; No biometric verification of travellers already entered in the EES can be made in the central EES; No exit record is created.
Impact on traveller (at crossing)	<ul style="list-style-type: none"> No information from the EES concerning the number of days remaining for the authorised stay. The web interface could be used for providing this information to the traveller. 	<ul style="list-style-type: none"> No information from the EES concerning the number of days remaining for the authorised stay. The web interface could be used for providing this information to the traveller.
Impact on border guard (at subsequent crossing)	<ul style="list-style-type: none"> Limited. All data registered when the EES became available, and the EES itself, can be fully used; Issues detected when registering the buffered data, such as problems carrying out the biometric verification using the buffered data, would have to be addressed. 	<ul style="list-style-type: none"> Limited. All data and biometrics registered when the EES became available, and the EES itself, can be fully used; Possibly, for TCNVEs having made their first entry at the earlier crossing, the border guard could run a 1:n identification. If a 1:n identification has been performed earlier using buffered data, it could be an option that the result of this is available in the EES for the purpose of subsequent checks; Issues detected when registering the buffered data, such as problems carrying out the biometric verification using the buffered data, would have to be addressed.
Impact on traveller (at subsequent crossing)	<ul style="list-style-type: none"> The lack of information as regards the number of days at the earlier crossing could result in the traveller mistakenly exceeding the number of days allowed. The web interface could be used for providing this information to the traveller. 	<ul style="list-style-type: none"> The lack of information as regards the number of days at the earlier crossing could sometimes result in the traveller mistakenly exceeding the number of days allowed, i.e. s/he could forget the date of the earlier crossing. The web interface could be used for providing this information to the traveller.

	At entry	At exit
B: No buffering and registration		
Impact on border guard (at crossing)	Same as for Scenario A but for the possible addition of a stamp in the passport.	Same as for Scenario A but for the possible addition of a stamp in the passport.
Impact on traveller (at crossing)	Same as for Scenario A.	Same as for Scenario A
Impact on border guard (at subsequent crossing)	<ul style="list-style-type: none"> An exit record would be missing in the EES. The border guard would have to add an exit record based on the stamp or on oral and other information from the traveller. 	<ul style="list-style-type: none"> If the earlier crossing was the traveller's first entry, there would be no data in the EES but possibly a stamp in the passport; All additional checks and registration procedures normally done at entry would have to be done at exit. The border guard would have to add an entry record based on the stamp or on oral and other information from the traveller; If the earlier crossing was not the first crossing, an entry record will be missing. The border guard would have to add an entry record based on the stamp or on oral and other information from the traveller.
Impact on traveller (at subsequent crossing)	<ul style="list-style-type: none"> The lack of information as regards the number of days at the earlier crossing could result in the traveller mistakenly exceeding the number of days allowed. The web interface could be used for providing this information to the traveller; The border crossing could take longer than usual due to the need for the border guard to input the EES data. 	<ul style="list-style-type: none"> The lack of information as regards the number of days at the earlier crossing could result in the traveller mistakenly exceeding the number of days allowed. The web interface could be used for providing this information to the traveller; The process could take longer than usual due to the need for the border guard to input the EES data.

3.2 VIS border check using travel document number

3.2.1 Introduction

This document presents desk research aimed at assessing the feasibility of retrieving visa information from VIS using the Travel Document Number (TDN) for verification at external border crossing points, instead of using the Visa Sticker Number (VSN), as is currently the case.

Among other things, it should be investigated whether this change will provide:

- The same information to border guards as when using the visa sticker number (VSN);
- The same information to border guards when the visa stickers of family members are affixed on one travel document;
- A simpler border control process and whether there will be a measurable decrease in the time taken for all other conditions remain equal.

It should be noted that VIS current legal basis⁸⁷ only allows access to its data for verification at external border crossing points using the visa sticker number (in combination with fingerprints to allow the border guard to verify the visa holder's identity). Since the pilot must not deviate from VIS current legal basis, access to VIS using the TDN cannot be tested in this pilot. Therefore, the above points will be assessed from a desk-research perspective.

3.2.2 Background and objective

VIS central system offers a set of services (operations) that can be used by the Member States (via their national systems) to accomplish their business activities. Depending on the specific national authority accessing VIS and the business objective, a set of these operations can be used.

The following operations are currently available at VIS central level as far as border checks are concerned:

- **First line control operations in VIS:** a unique visa application is returned to the national system.
 - *AuthenticateByFingerprint, VerificationBorder* variant: the VSN together with the prints of 1, 2 or 4 fingers are sent to VIS. In return, VIS provides the information pertaining to the visa application record associated with that VSN and states whether fingerprint verification has been successful or not (hit/no hit). This operation is processed by the BMS system;⁸⁸
 - *Retrieval, VerificationBorder* variant: VIS receives a VSN and returns the unique visa application record associated with that VSN.
- **Second line control operations in VIS**
 - *Search, IdentificationBorder* variant: an alphanumeric search in the VIS database, performed by the search engine. This operation allows data access with specified search fields but without a unique identifier. Each search variant results in either a no-hit message, a hit list or a detailed record if only one match is found.

Different types of searches can take place:

- Exact: the submitted search value exactly matches the value stored in VIS; or
- Inexact: in cases where end users do not know the exact value of a field, they can use the inexact search features of the system to get a list of possible search candidates.

⁸⁷ Article 18 of Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

⁸⁸ Backend Biometric Matching System that processes VIS operations involving fingerprints.

- *SearchByFingerprint, IdentificationBorder* variant: the prints of 1 to 10 fingers are sent to VIS and are searched for in the whole biometric central database, using the BMS system. VIS returns either a no-hit message, a list of all visa applications that are found to match, or a detailed record if only one match is found;
- *Retrieval, IdentificationBorder* variant: VIS receives a VSN or an application number and returns the visa application associated with that VSN/application number.

Currently, from both a technical and a legal viewpoint, VIS consultation at first-line control can only be performed using the VSN. This involves an extra step within the existing border-check process for visa holders, as the visa sticker needs to be scanned for the VSN to be extracted automatically from the MRZ (machine-readable zone).

The diagram below presents a general overview of the border-check process for TCNs, even if the specific process could vary depending on the MS, highlighting the extra step referred to above:

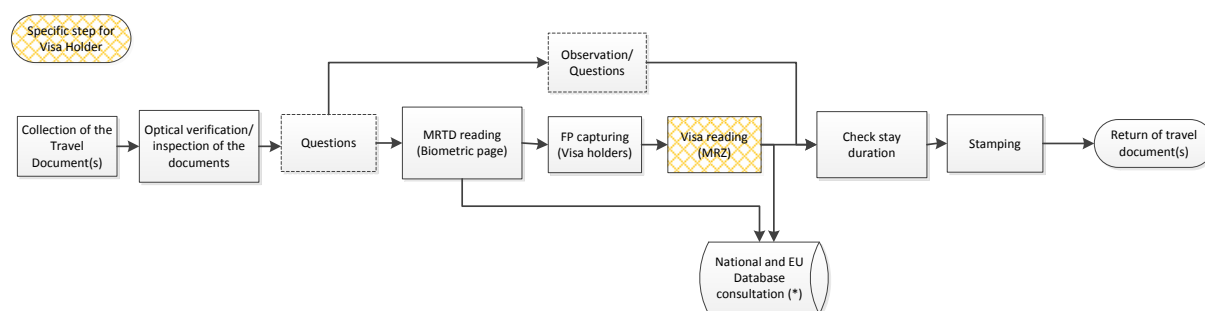


Figure 17 Steps of the border-check process

3.2.3 Benefits and challenges

From a business perspective, the following benefits can be gained by consulting VIS using the TDN:

- **Simpler border-check process:** if the TDN could be used for consulting VIS, there would be no need to scan the visa sticker, thus saving one step of the border-clearance process for visa holders;
- **Reduction in end-to-end time:** by removing one of the steps from the current workflow, the total process would require less time. The time saved will vary depending on each Member State's specific process, but it would be at least the scanning time, as the visa sticker will probably be checked manually;
- **Easier automation:** the use of ABC gates or kiosks by the VH TCN would be simplified, as only the passport would have to be scanned. This would avoid confusion and difficulties in dealing with visa stickers;
- **Fewer difficulties when scanning the visa sticker,** which tend to occur more frequently than when scanning passports for various reasons: visa sticker not properly placed on the passport page, problems with the ink, presence of stamps on top of the MRZ; etc.
- Easier implementation of systematic visa checks on exit, which are currently voluntary; and
- **Enhanced security:** in cases where the visa sticker cannot be properly scanned or when visas have been filled in manually.

On the other hand, the following challenges have been identified:

- **The TDN is not a unique identifier for the visa application,** as the relationship is not always one-to-one. Possible occurrences are:
 - Several visa applications have been registered with the same travel document, even though only one visa is valid at a given time;⁸⁹

⁸⁹ According to statistics extracted by two MS from their own national visa system, this is the case for approximately 10% of the visa applications stored at national level.

- Visa stickers of family members are simultaneously valid and affixed on one travel document;⁹⁰
- Several LTV⁹¹ visas are simultaneously valid and affixed on one travel document;⁹²
- The visa sticker has been affixed to another TDN belonging to the same person (e.g. a new passport has been issued as all pages of the previous one were full, the previous travel document has expired⁹³, etc.);
- Errors or anomalies occurred when filing the visa application at the consular post, and have not been rectified.
- **Data quality in VIS:** the travel document number was not properly filled in and entered in VIS when the visa was issued;
- Business logic is required so that the national system uses the MRZ in the travel document to identify whether the traveller requires a visa and thus, consultation in VIS is necessary. This could be implemented at both central and national level, and in some cases the border guard should still make the decision as there are many exceptions. Systematic searches in VIS for all TCNs will not be allowed, as it will - among other things - overload VIS.

In light of the above constraints, it might be interesting to retain the possibility to still be able to consult VIS at the first-line border check by using the VSN if desired as a fall-back, as the relationship between the visa issued and the visa sticker number is always one-to-one.

3.2.4 Technical options

As explained above, the current implementation of VIS does not include any operation which would always allow a visa record to be retrieved using the TDN. Any modification to the current implementation and functionality will need to be reflected in the legal basis as well as in the technical documentation, which will need to be updated accordingly.

On the other hand it shall be noted that the TDN alone will not be sufficient to identify a traveller, as different countries might use the same format for numbering travel documents. Therefore, together with the TDN, it is recommended to use as well the issuing country shall be used as well.

From a technical point of view, the following technical alternatives have been identified.

3.2.4.1 *Option 1: new search operation combined with database consultation*

Description

A search operation could be performed at the first line using the existing search engine, using the TDN and the issuing country/authority⁹⁴ as search fields.

1. If there is only one hit for that search, the unique application record will be returned by the central system, and the information will be the same as is currently the case using the VSN;
2. If there is more than one visa application registered in VIS for that TDN, a list containing all matching applications will be provided. Two options have been identified:
 - a. Manually explored by the border guard to select the relevant application. Once an application is selected, then a retrieval operation is executed to recover all data of that specific visa application by automatically using the VSN, and thus the already existing *Retrieval-VerificationBorder* operation; or
 - b. Automatically processed, so that only the application records associated with a valid visa at the time of consultation are returned.⁹⁵ This information is available in the database.

⁹⁰ According to statistics extracted by two MS from their own national visa system, the occurrence of these cases is below 0.2%

⁹¹ Limited territorial validity.

⁹² According to statistics extracted by two MS from their own national visa system, the occurrence of these cases is below 0.8%.

⁹³ According to statistics extracted by two MS from their own national visa system, the occurrence of these cases is below 0.4%.

⁹⁴ IssuingAuthorityOfTravelDocument field in VIS, which shall include a code table value (from the table CT02_Country_Of_Nationality) with optional free text field DescriptionOfIssuingAuthority.

⁹⁵ The relevant table in the database has a foreign key that is the application ID, and the query is not significantly impacted as it is indexed.

- i. If there is only one record, i.e. only one application is linked to a valid visa for a given TCN, all information pertaining to the visa application will be returned to the border guard.
- ii. If there is more than one record for which the visa is valid, then a list containing all of them should be returned.

These cases will be considered exceptions and will have to be further analysed by the border guard, in order to identify and retrieve the relevant visa record. Another possibility would be to rely on the fingerprints to identify the relevant record.

The diagram below provides an overview of this option.

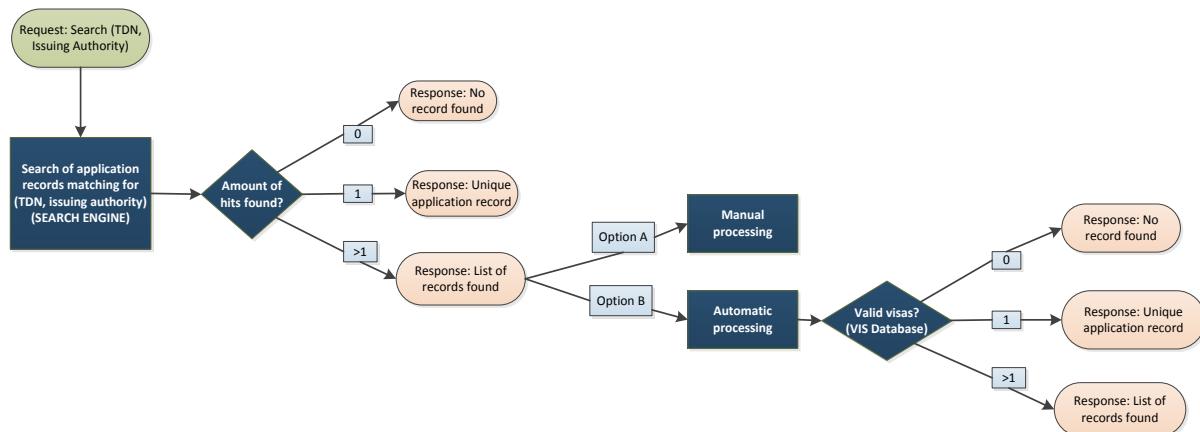


Figure 18 Illustration of technical option 1

Advantages

- For the first step above, the existing search functionality would have to be adapted and extended to first line – for example, by creating a *VerificationBorder* variant. The search would also accept in input the TDN and the issuing authority as search fields;
- The difference between the time it takes to retrieve a record at central level and the time it takes to perform an exact search is negligible. Therefore, this first step above is expected to be as quick as the current method;
- The second step described above, if implemented automatically, would mean modifying the VIS application by triggering processing and database queries. This modification is not complex, as the database itself does not need to be modified. The new search operation mentioned above must include a second step to check in the VIS database to see which of the applications retrieved currently have a valid visa. This information is already stored at application level;
- In the cases where a unique record is returned, the information returned is exactly the same as for the current VIS consultation using the VSN;
- From the perspective of a national system, the technical impact of implementing this functionality is very low. The search operation at central system will be implemented by offering a new web service; at national level it is required a new mechanism to consume this web service;
- It can be technically implemented quickly.

Impact

- Some modifications are still needed at central and national level, as a new operation – even if similar to existing ones – needs to be created;
- This approach will have an impact on the search engine as it will receive more requests and the response time could be negatively affected. The current solution should be easily scalable, but the impact ought to be properly assessed;
- The current agreed SLA is higher for searches than for retrievals and should therefore be adapted to provide for the same short response time;

- The current capacity allocation in terms of operations per channel will have to be re-examined.

3.2.4.2 Option 2: enhancing the search engine

Description

A (new) search operation could be performed against the existing search engine using the TDN and the issuing authority as search fields, while only filtering applications that have an issued visa which is valid at the time of consultation. The result could be no application record; all the information concerning an application if one unique hit is found; or a list of hits.

This configuration will limit - or even reduce - cases where more than one application is found and a list is thus returned. Therefore, as there would be only one hit in the vast majority of cases, the central system would in these cases return information relating to the application record.

However, to achieve this goal, the current visa search engine needs to be modified to include more fields (such as the expiration date of the visa⁹⁶ and other fields related to the decision made regarding the visa application), and the VIS application needs to be modified accordingly to be able to feed this new information into the search engine.

The diagram below provides an overview of this option.

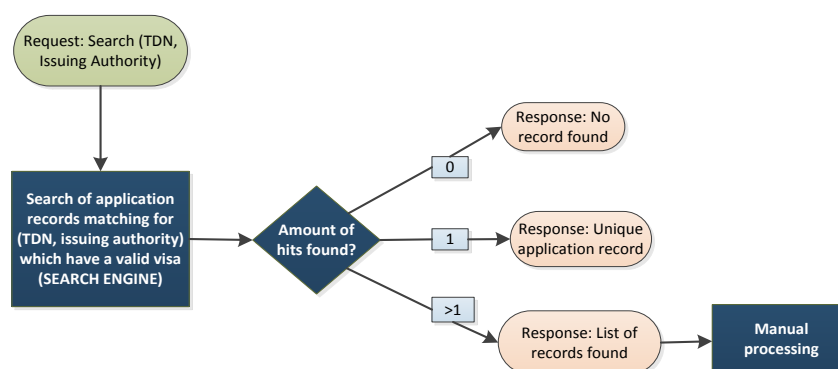


Figure 19 Description of technical option 2

Advantages

- The central system will almost always return one unique application in one step, containing the same information as the current consultation using the VSN;
- The difference between the time it takes to execute a retrieval and the time it takes to perform an exact search is negligible;
- There is a minimal technical impact on national systems. The search operation at central system will be implemented by offering a new web service; at national level it is required a new mechanism to consume this web service;
- Using the search engine is more efficient and reliable than querying the database, especially for exact searches;
- The technical implementation can be done in a short timeframe.

Impact

- The search engine needs to be reconfigured to include more fields as well as support more requests, which will have an impact which is yet to be properly assessed;
- The central VIS application needs to be changed and adapted to be able to feed the search engine with this new

⁹⁶ The expiration date is always present in the visa application, as it is automatically calculated based on the validity start date.

information that has to be stored systematically when visas are issued. The impact of this change should be assessed, but it is expected to be major, as many tables will need to be queried and the search engine will need to be updated for each visa decision;

- Cases where several visas are simultaneously valid and affixed to one travel document will, at any rate, be treated as exceptions;
- The current capacity allocation in terms of operations per channel will need to be re-examined;
- The current agreed SLA is higher for searches than for retrievals and should therefore be adapted to provide for the same short response time.

3.2.4.3 Option 3: redesigning the VIS database

Description

A new data model could be designed and implemented to enable querying the database using the TDN - probably combined with issuing authority or other fields.

Advantages

- A new retrieval operation similar to the existing one could be implemented afterwards;
- Database aligned and optimised to the new VIS consultation by TDN.

Impact

- Major change to the current implementation of VIS;
- Potential side effects to the functionality of the rest of VIS. This would subsequently imply a high technical impact also at national level and a deep impact assessment is thus required;
- The technical implementation is a lengthy process: thorough analysis and development phase need to be considered;
- Deployment of the solution could have a high risk and data migration and exhaustive regression tests campaigns would be expected, both at national and central level.

3.2.5 Conclusions

The above described options show that, from a technical perspective, it would be feasible to implement a solution which would allow the VIS consultation at the external Schengen borders with the TDN and the country that issued that TDN, while providing in most cases the same information as the current consultation using the VSN.

The table below compares these three identified options:

Table 40 Comparison of the three options

Option	Ease of Implementation	Performance	Impact on current VIS	Impact on national system
Option 1: new search operation combined with database consultation	++ modifying the VIS application to trigger a query to the database in specific cases	+ both the search engine and the database are involved	+	+
Option 2: reconfiguration - enhancing the search engine	+ modifying the search engine to include more fields and modifying the VIS application to feed the search engine	+++ only the search engine is involved in the execution	+	+

Option 3: re-designing the VIS database	-- complete change of VIS data model	++	---	-- Potential side effects
--	---	----	-----	------------------------------

Out of the options explained above, the alphanumeric search-engine solution in VIS is proven to be very efficient and reliable, and should therefore be the preferred option from a technical perspective, above the option of increasing the amount of queries to the database. On the other hand, the technical implementation of this option is much faster and easier than completely redesigning the database, as well as less risky.

Therefore, technical option 2 would be the preferred one in the following cases:

- Where one TDN issued by a given authority only has one valid visa associated with it, the same information will be returned to the border guard as when the consultation is done with the VSN;
- Where there are several valid visas affixed to the same TDN, or where the traveller has a new TDN while the visa is affixed to a previous one, these will need to be treated as exceptions and be further analysed by the border guards;
- The impact on the current system will be further assessed:
 - Some adaptation and modification is required, at both VIS and national-system levels, even if these changes are not expected to have a major impact as most of the functionalities have already been implemented. This will also mean that the ICD needs to be modified;
 - The current capacity allocation per VIS channel will be re-examined;
 - The search-engine capacity will have to be re-examined;
 - The process may take longer due to the fact that an exact search will be performed, rather than merely a retrieval. The current contractual SLAs are different for each type of operation.

However, it should be noted that implementing a technical solution to address VIS consultation using the TDN will not solve some of the challenges previously identified, which should be addressed at a different level:

- Data quality in VIS: the travel document number was not properly filled in and inserted in VIS when the visa was issued;
- Business logic is required so that the national system identifies from the travel document's MRZ whether VIS needs to be consulted.

3.2.6 Complementary information

Even if fingerprint verification has not been explicitly covered in the previous points, from a legal perspective this is a mandatory step of the border-checking process for visa holders. In order to enable this to happen, the following approach is suggested.

- The new search operation used at the first line to consult VIS using the TDN will also include fingerprints, which will be used to complement the execution of the operation;
- The operation will be executed to obtain the relevant application record;
- VIS will automatically extract the identifier from that application record, which will allow VIS to verify the fingerprints. This procedure would be very similar to the current *AuthenticateByFingerprint* operation and will be performed in a transparent way;
- A response specifying whether the verification has been successful will be sent back to the border guard.

Cases where a list of visa records with a valid visa for a given TDN is returned, will be treated as exceptions. In this regard, either of the following approaches could be followed:

- i) The border guard will have to select the relevant record manually from the list and retrieve its information. In order to verify the fingerprints, the *authenticatebyfingerprint* will need to be performed by sending both the visa sticker number and the fingerprints to VIS to be verified; or

- ii) The fingerprints that have been sent to VIS are used to ascertain which is the relevant record from the list. To achieve this, the central system would have to try to match the fingerprints with the ones stored for those records; the record for which verification results in a hit will be returned to the border guard. This option has its own limitations, as there are cases where the fingerprints might not be present in VIS.

3.3 Web service

3.3.1 Introduction

The current border check process involves the visual inspection of the travel document and the search for physical evidence of entries and exists (in the form of physical stamp(s) on visas and passports). If stamps on visas and passports are abolished when the EES is implemented, then the associated physical evidence will no longer be available. As a consequence:

- Travellers will need to be in a position to calculate the remaining number of days of authorised stay. Such information could be useful to the traveller, for instance when booking flight tickets;
- Carriers will need an alternative means to comply with their obligations to establish whether a visa has already been used by the traveller as established in the Schengen Convention and the Schengen borders code.

This chapter analyses the possibilities for implementing a web service for carriers and travellers to query travel-document validity (visa) and the remaining days available to stay in the Schengen Area. The web service would be available to the public (travellers and carriers) and should be user-friendly while remaining secure and affordable.

3.3.1.1 Objective

The objective of this desk research is to explore what information the web service could deliver to travellers and to carriers – and how and at what cost this could be done.

It is also necessary to examine how to minimise the security risk for the central system (EES system), as it would be the first time that information stored in an EU wide large-scale IT system is exposed to the outside world (e.g. eu-LISA link to carriers and via a public website to travellers).

In summary, the desk research addresses three main questions:

1. Data: defining options for delivering information to carriers and travellers;
2. Security: identifying necessary security measures;
3. Costs: estimating the cost of the various solutions.

3.3.1.2 Assumptions

The options are explored with the following assumptions regarding future conditions and restrictions in mind:

- No data will be hosted in the servers of private companies⁹⁷ (except as specified under 'output');
- The web service will be available over the public Internet. There will be no dedicated communication infrastructure between the web service provider and travellers or carriers;
- It will not be possible to connect directly to the central system from the web service;
- Visa related data is part of the EES dataset in accordance with the Technical Study;
- An extract with the necessary records is taken from the central system on a regular basis. The queries will be performed only against this extract;
- Carriers' legal obligations remain unchanged.

3.3.2 Methodology

The desk research looked at the approach followed by other countries in a benchmarking exercise, where publicly available information on similar services was examined and - where possible - further information was sought through questionnaires and interviews with the relevant authorities and specialists.

⁹⁷ This does not exclude the possibility of outsourcing some parts of the infrastructure, provided that the data is encrypted.

The identification of the options for the design of the web service builds on the Technical Study⁹⁸ and the solutions already identified therein. The potential solutions and their evaluation takes into consideration feedback from consultations with appointed experts from Member States, consultations with industry and relevant expert EU organisations such as Europol and ENISA, as well as on eu-LISA's experiences with the existing mission-critical large-scale IT systems operated under its mandate.

The options for the web services are assessed taking into account elements of privacy, information security and costs (both initial investment and ongoing operational). The options identified will have to balance:

- Privacy, (which data to request to identify and authenticate the traveller or carrier and which data can be provided safely);
- The service level provided to travellers and carriers: user friendliness, usability and completeness; and
- The complexity of the solution.

3.3.3 Benchmarking

An increasing number of countries offer electronic public services online aimed at foreign citizens, such as visa application services. Even if these systems might have a different purpose, all of them share similar challenges:

- a. User access and identification;
- b. Information security and privacy protection;
- c. Availability and usability of the service.

In general the services must remain user friendly and provide a good level of service to a very diverse demographic of users, while at the same time be adequately protected to ensure personal data is not compromised and that the service remains available.

These systems have been explored as benchmarks to identify best practises or case studies that could support the definition of a European solution.

The following sections provide a brief overview of the functioning of the electronic systems used in different countries to provide information to foreign travellers, about visa or travel authorisation.

3.3.3.1 *Australia*

Australia has three categories of electronic visa, each with their respective systems and procedures that apply to different categories of foreign travellers. Therefore, Australia offers three different applications, aimed at allowing the submission of different visa categories depending on the nationality:

- 1.- **eVisitor**: available to most European citizens (including from some non-EU countries) to request short-term visas.
 - User authentication/management: the user/traveller has to create and access to its account, the so called "ImmiAccount", which also allows him/her to access to additional services.
- 2.- **ETA (Electronic Travel Authority)**: similar to the eVisitor programme, the ETA system provides travel authorisation for short-term visits to Australia for travellers holding an eligible passport.⁹⁹

⁹⁸ European Commission, Technical Study, 2014, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf.

⁹⁹ To apply for an ETA online through this website, travellers must hold a passport from one of the following countries or territories: Brunei-Darussalam, Canada, Hong Kong (SAR PRC), Japan, Malaysia, Singapore, the Republic of Korea (South) or the United States of America.

- User authentication/management: providing nationality, passport number, date of birth and a reference number provided during the application process

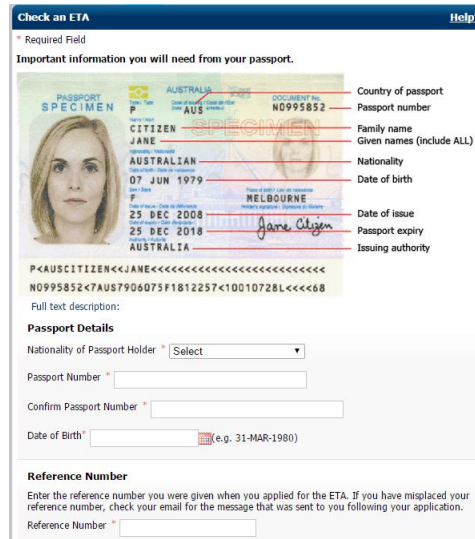


Figure 20 ETA webpage to enquire about the status of an application for authorisation to travel

3.- **VEVO (Visa Entitlement Verification Online):** all passport holders eligible for an electronic visa can use the VEVO system to verify online the records (no physical visa is available). It also supports organisations such as travel agents across the world and airlines. The organisations have to register before being able to use VEVO to verify someone’s right to work, study or stay in Australia.

- User authentication/management: providing date of birth, passport number, country of the passport and a reference number linked to the visa or alternatively the credentials of their “ImmiAccount”. By using an account-based system, Australia is able to directly engage travellers and provide multiple services through the same gateway (ImmiAccount). However, creating accounts for travellers requires the collection of additional information, such as email addresses, credentials and additional security questions to allow access to the account to be recovered if the password is forgotten.



Figure 21 VEVO webpage to verify the visa of a certain individual

3.3.3.2 US - ESTA

The US Electronic System for Travel Authorisation (ESTA) is one of the most well-known and used electronic systems of its kind, with between 12 and 13 million applications submitted annually. From January 2009 it became mandatory for all travellers arriving in the US by air or cruise ship.

The system allows travellers to retrieve and check a previously submitted application using their passport number, date of birth and the application number. However, the latter can be replaced by the family name, first name and country of citizenship.

Carriers also have dedicated connections to ESTA so that they can verify whether a passport has a valid ESTA and whether the person can board the plane. The data used to query the system comes from APIS (Advanced Passenger Information System), specifically the passport number and country of citizenship.

RETRIEVE INDIVIDUAL APPLICATION

The following information is required to retrieve your application. If you know your application number, select the first option. If you do NOT know your application number, select the second option.

[-] I Know the Application Number

All fields are required.

Passport Number*

Date of Birth* Day Month Year

Application Number*

[-] I Do NOT Know the Application Number

All fields are required.

Passport Number*

Date of Birth* Day Month Year

Family Name*

First (Given) Name*

Country of Citizenship*

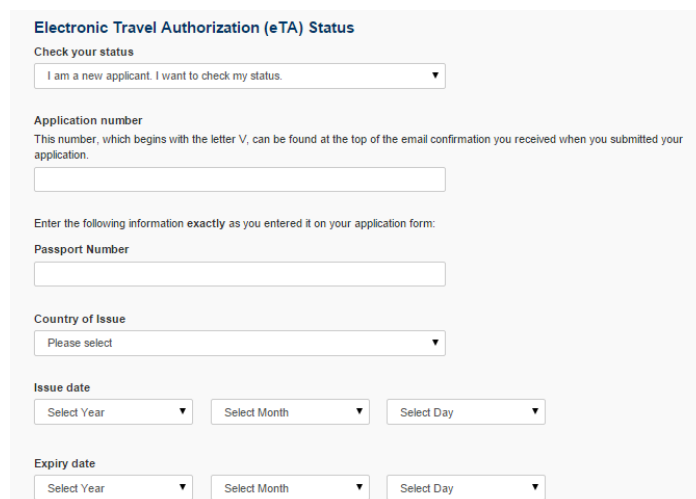
RETRIEVE APPLICATION

Figure 22 US ESTA - retrieving an individual application

3.3.3.3 Canada - eTA

From March 2016 it will be mandatory for visa-exempt foreign nationals (except US citizens) arriving in Canada by air to obtain an Electronic Travel Authorisation (eTA). The application for the eTA must be done online, by providing a range of personal information. Overall, the system is comparable to the US ESTA.

Once the application is submitted, the traveller can check the status of his/her application by providing his/her surname, date of birth, place of birth and an application code provided during the application process.



Electronic Travel Authorization (eTA) Status

Check your status

I am a new applicant. I want to check my status.

Application number
This number, which begins with the letter V, can be found at the top of the email confirmation you received when you submitted your application.

Enter the following information exactly as you entered it on your application form:

Passport Number

Country of Issue

Please select

Issue date

Select Year Select Month Select Day

Expiry date

Select Year Select Month Select Day

Figure 23 Canadian eTA page, allowing travellers to check the status of their application

3.3.3.4 Comparison

The table below summarises the data required by the aforementioned systems to access and retrieve information.

It is possible to observe that:

- All these systems require the passport number to perform a query, although in some cases like for Australia, it is possible to use a login and password instead;
- Biographical data is usually complemented by the use of a unique code (such as the application number) or a previously assigned credential. Only the US ESTA system allows the option to retrieve the status of the application using only biographical information that can be found on the passport;
- All of these systems request the email address of the traveller during the application process, which is then used as a means to provide information to the applicant or to recover the account created.

The person's identity within these systems is built during the first application, i.e. before the person has actually entered the country. This is the first major difference when compared to a possible web service linked to the data already collected by the EES. The application/reference number or email addresses are data that is not foreseen to be available within the EES database¹⁰⁰; therefore, introducing them would require additional data collection or an additional process to assign a unique code to each traveller.

¹⁰⁰ The proposed dataset for the EES is listed in chapter 5 of European Commission, Technical Study, 2014, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf.

Table 41 Comparison of the data used to query the systems

	Australian VEVO	Australian ETA	US ESTA	Canada eTA
Data required for querying the system				
Reference number / application number	✓	✓	✓	✓
Passport number	✓	✓	✓	✓
Date of birth	✓	✓	✓	
Country issuing passport			✓*	✓
Nationality		✓		
Name			✓*	
Surname			✓*	
Issuing date				✓
Expiry date				✓
Comments	Alternatively, the credential for the ImmiAccount can be used		* Necessary only if the application number is not available	

3.3.4 Background (Technical Study)

In 2014, the European Commission's Technical Study¹⁰¹ identified a set of possible options that would allow information to be provided to travellers and carriers as a means of replacing the information provided by passport stamping, which would be abolished following the implementation of Smart Borders.

¹⁰¹ European Commission, Technical Study, 2014, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf.

3.3.4.1 Travellers

The options initially identified in the Technical Study for providing information to travellers are the following:

- a. Email request sent to the competent authorities;
- b. Phone request sent to the competent authorities;
- c. Self-web service (OK/NOK return message depending if one remaining day of stay is left);
- d. Self-web service (OK/NOK return message depending on the anticipated date of return);
- e. Self-web service (remaining number of days + date of the limit of stay); and
- f. Self-web service (remaining number of days + date of the limit of stay + travel document validity date).

This desk research for this chapter focused on, and further explored, the options that would arise from the implementation of a web service (options c to f above).

3.3.4.2 Carriers

Under Article 26 of the Schengen Convention,¹⁰² carriers are obliged to ensure that a traveller is in possession of the travel documents required for entry into the territory of the MS concerned¹⁰³.

With the adoption of the EES system, the stamp(s) will no longer be available. Therefore, alternative solutions could be considered in order to enable carriers to comply with their obligations to establish whether a single-entry visa or MEV has already been used by the traveller.

The Technical Study proposed the following options:

- a. Relieve carriers from their current obligations;
- b. OK/NOK return message depending if one remaining day of stay is left; or
- c. Extend carriers' obligation to check the stay validity using an OK/NOK return message based on the anticipated return date entered.

Options a) and c) have been disregarded within this desk research, as they would involve a change of the responsibility of the carriers. In this chapter, further technical options for both carriers and travellers have then been identified and assessed.

3.3.5 Options

Travellers and carriers have slightly different needs, therefore the service might present a different view and provide different information.

¹⁰² Article 26 of the Schengen Convention provides as follows:

"1. The contracting parties undertake, subject to the obligations resulting from their accession to the Geneva Convention relating to the Status of Refugees of 28 July 1951, as amended by the New York Protocol of 31 January 1967, to incorporate the following rules into their national law:

a) If aliens are refused entry into the territory of one of the Contracting Parties, the carrier which brought them to the external border by air, sea or land shall be obliged immediately to assume responsibility for them again. At the request of the border surveillance authorities the carrier shall be obliged to return the aliens to the third State from which they were transported or to the third State which issued the travel document on which they travelled or to any other third State to which they are certain to be admitted.

b) The carrier shall be obliged to take all the necessary measures to ensure that an alien carried by air or sea is in possession of the travel documents required for entry into the territories of the Contracting Parties.

2. The Contracting Parties undertake, subject to the obligations resulting from their accession to the Geneva Convention relating to the Status of Refugees of 28 July 1951, as amended by the New York Protocol of 31 January 1967, and in accordance with their constitutional law, to impose penalties on carriers which transport aliens who do not possess the necessary travel documents by air or sea from a third State to their territories. 3. Paragraphs 1(b) and 2 shall also apply to international carriers transporting groups overland by coach, with the exception of border traffic."

¹⁰³ Annex V Part A of the Schengen Borders Code further provides that "if a third country national who has been refused entry is brought to the border by a carrier, the authority responsible locally shall: a) order the carrier to take charge of the third country national and transport him or her without delay to the third country from which he or she was brought, to the third country which issued the document authorising him or her to cross the border, or to any third country where he or she is guaranteed admittance, or to find means of onward transportation in accordance with Article 26 of the Schengen Convention and Council Directive 2001/51/EC of 28 June supplementing the provisions of Article 26 of the Convention implementing the Schengen agreement of 14 June 1985."(OJ L 187, 10.7.2001 p. 45.).

Options for both travellers and carriers are defined by the data used to identify and authenticate the person and perform the query (*inputs*) and by what would be returned as a result of the query (*outputs*).

These are then assessed according to three main aspects:

- Privacy impact;
- Quality of service provided to users;
- Complexity of implementation.

3.3.5.1 Travellers

User access

Identifying the traveller is particularly critical; in fact, requesting more data will increase the certainty of the identification and reduce the risk of unauthorised access. On the other hand, requesting more data could itself become have privacy impacts as this data would also have to be stored in the backend of the web service.

The traveller could consult the system by providing the following information:

- **Passport data only:** information from the passport, for example the passport number and code of the country issuing the travel document and date of birth;¹⁰⁴
- **Passport data + entry/exit information:** information on the passport AND information about the traveller's entry/exit (e.g. the country and date of last entry into the Schengen Area);
- **Passport data + unique traveller code:** information on the passport AND a code that is unique to the traveller and not present on the travel document. This code would be issued to travellers at the crossing - systematically or on request;
- **Account credentials:** the traveller has an account with a unique ID and password.

Depending on the type of information used as an input for the query, there are different implications in terms of the privacy and complexity of the service provided.

For the input option of **passport data only**, the identification of the requester and subsequent authorisation is based solely on information available on the passport - something the traveller has. This does not give a very high level of assurance that it really is the traveller requesting this information. The request could also have been made by someone having stolen either the passport, or having information contained in the data page of the passport. Although this would be the least complex technical option for the web service, it would also be the input option providing the lowest level of privacy protection.

The next option of **passport data + entry/exit data**, provides a slightly increased level of privacy protection, in that it adds a data element to the identification of the requestor - something the traveller knows. However, several people may have access to this information or may be able to guess it relatively easily. It does, of course, also presume that the traveller him/herself knows and can remember the information. Adding this extra data element to the input option also slightly increases the technical complexity of the option, as more data would have to be extracted from the central system and processed and protected in the web service solution.

The addition of a **unique traveller code** provides for higher assurance of the identification of the requestor. However, it also adds considerably to the technical complexity and to the logistical and operational set-up as to how the unique traveller code should be generated, issued to travellers and - possibly - re-issued in case of loss.

¹⁰⁴ As passport is a sequential number in most countries; additional information could be requested in order to increase the authentication level (i.e. names or date of birth).

Finally, having an **account**-based system would allow for a system design providing a high degree of assurance in terms of identification and authentication, and in this way also providing a high level of privacy protection. However, it would also be the most technically complex web service solution, as well as probably the most expensive in terms of implementation, maintenance and support to account holders. Moreover, it would entail the collection of additional personal information, such as email addresses, which would have to be stored in a European database. This option could resemble the Australian “ImmiAccount”.

The creation process of the account is a critical point; it is, in fact, important to establish with certainty the identity of a user before providing credential and associating the account to the record within the EES database. Possible solutions could include to request entry/exit data or to use an invitation code previously provided to the travellers.

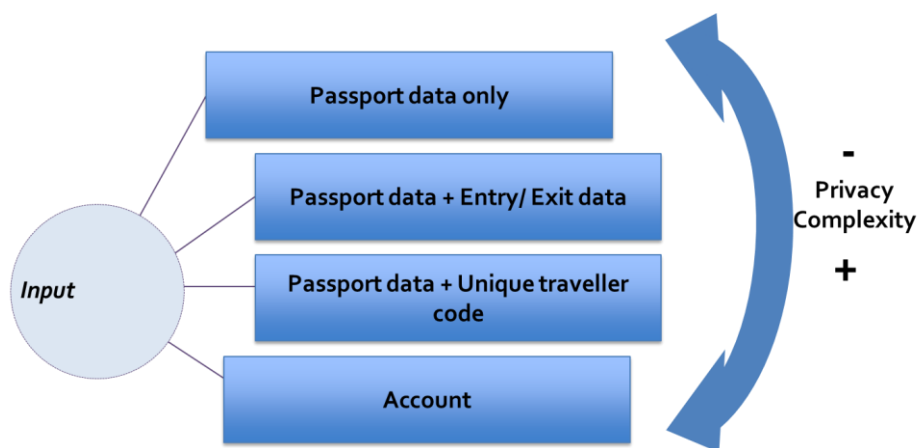


Figure 24 Data necessary for a traveller to query the system-ranked, in order of impact on complexity and privacy friendliness

Information returned

The system could return the following information to the traveller:

- **OK/NOK (one remaining day of stay left):** if there is at least one day of stay remaining (i.e. the visa has not been consumed yet), the web service will return an OK answer. Otherwise, the web service will return an answer of Not OK;
- **OK/NOK (based on anticipated date of return)¹⁰⁵:** the traveller will input their anticipated date of leaving the Schengen Area. If days remain or if the last remaining day is consumed on that date, then the web service returns an OK answer. Otherwise, it will return an answer of Not OK;
- **Remaining number of days + date of the limit of stay:** information on how many days of stay are remaining, and the date of the last permitted day of stay; or
- **Full history of the days consumed:** information on registered dates of entries and exits, and the number of days consumed.

The options described above include a minimal output of low sensitivity, little impact on privacy and - on the other hand - an option whereby the information returned is of limited further use for the traveller. At the other end of the scale, the output of the query provides a high level of service, but the privacy implications in the event of a data breach are also significantly higher and thus require a higher level of protection.

¹⁰⁵ Through a series of queries it could be possible to deduce the number of remaining days (as per the subsequent option described). To mitigate this a maximum number of requests per traveller, in a given timeframe, could be implemented.



Figure 25 Data necessary for a traveller to query the system-ranked, in order of impact on complexity and privacy friendliness

Assessment of the options for the travellers

In combination, the different options for inputs and outputs provide varying degrees of service to travellers, complexity and privacy implications. The table below shows these different combinations.

Some options have been excluded at an early stage (marked with an "X") due to, for example, input options providing an insufficient level of privacy protection in relation to the (high) level of information detail in the output option - or on the other hand, the input option being excessively complex in relation to the (low) level of information detail in the output option.

Table 42 Design option to deliver information to travellers from the combination of possible inputs and outputs used

Output Input	OK/NOK (one remaining day of stay left)	OK/NOK (based on anticipated date of return)	Remaining number of days + date of the limit of stay	Full history of the days consumed
Passport only	✓ (1)	✓ (2)	✓ (3)	X
Passport + entry/exit information	✓	✓ (4)	✓	X
Passport + unique traveller code	X	X	✓ (5)	✓
Account	X	X	✓	✓ (6)

For purposes of brevity only six assessments will be presented in this chapter, however the scoring for the remaining four options can be derived.

The six retained options (which are numbered in brackets in the table above) have then been assessed by assigning a score to the three evaluation criteria previously introduced (privacy, service and complexity) and according to the considerations previously explained while analysing the individual option for input and output. The scoring has been further refined through consultation with experts in the Member States and is presented in the following table:

Table 43 Assessments of the different options [0 = worst, 5 = best]

Option	Service to traveller	Privacy	Complexity management	Total
1) Passport data - OK/NOK if one day remaining	1	4	5	10
2) Passport data - OK/NOK using the date of return	3	3	5	11
3) Passport data - Remaining number of days	4	2	5	11
4) Passport data + entry/ exit data - OK/NOK using the date of return	3	4	3	10
5) Passport data + unique traveller code - Remaining number of days	4	5	1	10
6) Traveller account - Full history and number of days	5	4	1	10

The options have similar overall ratings. What differentiates them is how the scores are distributed across the three axis. Some options are clearly preferable when considering the complexity of implementation and operation (solutions 1,2,3), while others could provide a significantly better service to the travellers (option 6).

Options 2, 3 and 4 would provide the best balance of service, privacy and complexity. Among these, option 3 fare worst for privacy, however it is worth noting that this solution would be the closest to the current situation, as the information provided to the traveller is similar to what can be obtained from the physical stamps on passports. The risks and consequences in case of passport theft would be similar for the traveller.

The choice of the final design will depend on the importance given to each of the three criteria, ranging from a simple solution that aims at providing the bare essential (option 1) to an account based solution (option 6) which is much more complex and costly, but also provides richer information to the traveller and which could allow further future applications of use.

3.3.5.2 Carriers

User access

Carriers could query the system using:

- **Passport data only:** information on the passport of the traveller to be checked (such as the passport number and the code of the country issuing the travel document); or
- **Carrier credentials and passport data:** the carriers would authenticate themselves to the web service with credentials (and as such have an account), and then use the traveller's passport number and date of birth or nationality to perform the actual query.

As for the options for travellers, the option of using **passport data only** would not give assurance that the person querying the web service is authorised to do so. However, it would be technically the simplest implementation without the need to manage credentials. It would only allow one passport to be checked at a time, and not automated bulk checks. This option could also be used as a fall-back service for border guards to check whether a person at entry has the administrative requirements to enter the Schengen Area (for more details, please refer to the Chapter on fall-back scenarios 3.1).

The **carrier credentials** would be used to authenticate to the web service, and subsequently the passport data would be used to perform the actual query. The credentials would be foreseen per carrier, rather than per end-user station, similarly to what was observed while analysing comparable systems from other countries. Subsequent user management and monitoring would be the responsibility of the carrier. The use of carrier credentials would make it possible to set-up automated bulk checks.

Information returned

Carriers could receive from the system:

- **OK/NOK (one remaining day of stay left):** if there is at least one day of stay remaining, the web service will return an OK answer. Otherwise, it will return an answer of Not OK;
- **Number of days remaining:** the number of authorised days remaining for the traveller; or
- **Proof of check:** an acknowledgement that the query has been performed according to the carrier's obligations should be provided.

Providing an output of OK/NOK would enable carriers to fulfil their current obligations of checking whether the traveller has a valid travel document immediately before departure. It would not allow for a single check as to whether the traveller has a valid travel document on trips with multiple entries and exits into and out of the Schengen Area (as could be the case for a cruise in the Mediterranean Sea). This could be done by a single check with the output option of number of days remaining, which would allow the carrier to calculate this immediately before departure.

Assessment of the options for the carriers

The combination of these input and output options are presented in the following table.

Table 44 Input and output options

	Option A	Option B	Option C
Input	<ul style="list-style-type: none"> • Passport data 	<ul style="list-style-type: none"> • Passport data • Carrier credentials 	<ul style="list-style-type: none"> • Passport data • Carrier credentials
Output	<ul style="list-style-type: none"> • OK/NOK (one remaining day of stay left) • Proof of check 	<ul style="list-style-type: none"> • OK/NOK (one remaining day of stay left) • Proof of check 	<ul style="list-style-type: none"> • Number of days remaining • Proof of check

Similarly to what was done for the options for travellers, the options identified for carriers have also been scored according to the same criteria.

The table below show the results of the assessment.

Table 45 Assessment of the different options [0 = worst, 5 = best]

Option	Service to carriers	Privacy	Complexity management	Total
A) Passport data - OK/NOK if one day remaining	2	3	5	10
B) Passport data and Carrier's credentials - OK/NOK answer if a single day of stay remain and Proof of the check	3	5	4	12
C) Passport data and Carrier's credentials - Number of days remaining and Proof of the check	5	2	4	11

The distribution of the scores differentiates the three options. The final choice will then depend on how much importance will be given to each of the criteria.

Overall solution B) is the design option that scores the highest, with a good balance of all the three criteria examined and therefore could be a good candidate for the final implementation.

3.3.6 High-level architecture

When accessing to the web service, travellers and carriers would only have access to a read-only subset of EES data for a specific purpose.

Only the data needed for the identification of the TCN (previously referred to as input data), the information regarding the remaining allowance of days and any other information that the service should return to the traveller (output data).

On top of a web service application, it would be still possible to overlay either an SMS service or a mobile application, increasing the number of communication channels reached by the service.

Given the similarities between the service to be provided to carriers and to travellers, the infrastructure used could be the same. Access management and logical separation of data will help to ensure that each group of user can only access to the appropriate set of data.

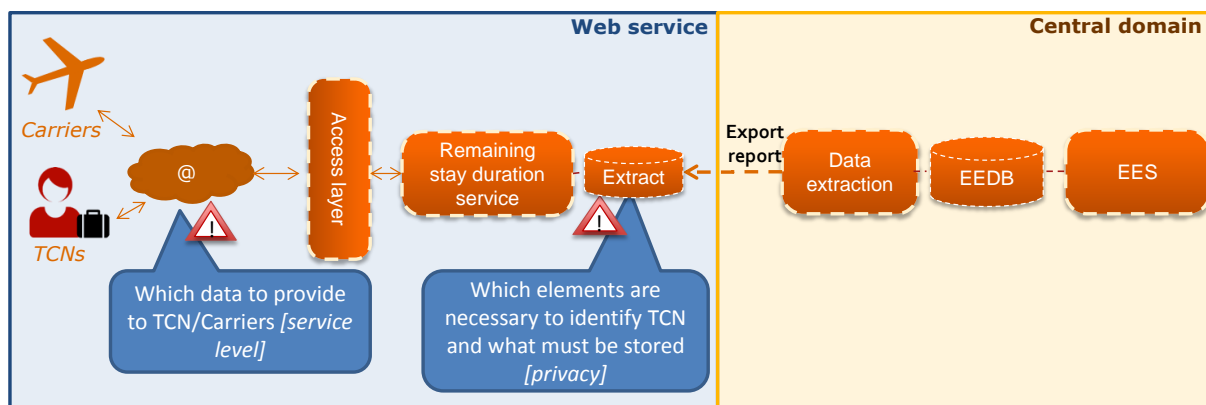


Figure 26 High-level overview of the possible architecture of the EES web service

3.3.7 Information security and privacy

Depending on the input and output options chosen, a full information security risk assessment, as well as a privacy impact assessment, should be performed:

- A **security risk assessment** which will look at threats and vulnerabilities to the system in terms of the classical security triad of CIA - confidentiality, integrity and availability;
- A **privacy impact assessment** which will seek to specifically focus on ensuring that all elements in the workflow of the web service have been addressed in terms of the fulfilment of data protection rules. The security risk assessment and the privacy impact assessment are tools to achieve privacy by design. The outcomes would be a prioritised list of privacy targets and security risks, as well as the recommended protection measures and security controls to be implemented.

3.3.7.1 Security control and resilience requirements

The defining feature of the web service explored above - that it is available over the public Internet - introduces attack vectors and an attack surface which are new to eu-LISA's operational methods and models.

The systems currently hosted by eu-LISA are only available to be accessed by specific authorised Member State authorities through dedicated private networks. Their protection profiles and security are heavily influenced by these factors. A web service provided by eu-LISA could benefit from synergies of the already implemented protection and resilience measures of the systems, in terms of organisational set-up, architectural and technical design and implementation, and physical security controls.

In addition to the above, the web service has a number of additional requirements for security controls and resiliency measures to counter threats coming mainly from the web technologies and the public Internet.

To protect the confidentiality and integrity of the web service, it would - for example - have to be protected against unauthorised access to its infrastructure and the data held therein, of course both for individual files and for a large-scale intrusion and potential data theft or modification of multiple or all records. Data breaches are a growing threat area,¹⁰⁶ and the fact that these could be caused by web-application vulnerabilities constitutes a major risk.¹⁰⁷ It is however worth to note that major data breaches resulting from attacks in both the public and private sector has been on richer data than what is foreseen in the web service.^{108, 109} The research and consultation for this topic has not found examples of attacks on similar services, such as those mentioned in the benchmarking section.

For the web service, access via the Internet also requires additional protection from unavailability threats. The availability of the back-end system could be designed and implemented to respect the same availability requirements of the central system - for example with the implementation of both geographical and local redundancy, and backup mechanisms. However, due to the front end of the web service having to be available over the public Internet, achieving similarly high availability goals would be challenging. In addition to the resilience and availability measures already implemented on the other systems operated by eu-LISA, the web service would have to be protected against the risk of becoming unavailable due to an attack on the front end of the system, for example through a DoS attack.^{110, 111}

3.3.7.2 Availability requirements

For both travellers and carriers, the availability requirements of the web service would have to be defined.

For travellers, the typical use-case scenario is expected to be for planning of trips to and from the Schengen Area. Although it is desirable that the web service is always available on a 24/7 basis at the moment when the traveller decides to query it, if the web service it is unavailable the traveller can reschedule the planning activities. If the traveller has an urgent need to book or plan travel, the following options are available:

- Calculate the remaining authorised stay in the Schengen Area based on previous tickets and receipts;
- Book travel with the risk of having to change or cancel travel (this might incur a cost to the traveller); or
- Visit and query a relevant authority of the Schengen Member State in which the traveller plans to arrive (such as a

¹⁰⁶ According to the ENISA Threat Landscape Report, data breach data increased by 25% in Q4 2014 in comparison with the same period in the previous year.

¹⁰⁷ According to the OWASP (Open Web Application Security Project) Top 10 Privacy Risks 2014, the number one risk is web application vulnerabilities. https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project#tab=Top_10_Privacy_Risks

¹⁰⁸ http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0

¹⁰⁹ http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/On-line_hoeringssvar_-_Nyhed_16_6-03/Datatilsynets_udtalelse_hackcase.pdf

¹¹⁰ A DoS is a denial-of-service attack whereby a service is attacked to make it unavailable. This can happen by overloading the service with many requests. In a DDoS (distributed denial-of-service attack), the attack comes from a range of sources that could be spread around the globe.

¹¹¹ DoS attacks are also a growing threat, according to the 2014 ENISA Threat Landscape Report.

consulate or embassy).¹¹²

For carriers to be able to fulfil their legal obligations, there would be high availability requirements of access. Not being able to verify whether travellers are carrying valid travel documents could, for example, result in boarding being denied and departures being delayed or cancelled. Due to the short time that the carriers have between a traveller arriving and the scheduled departure of (for example) a train or aeroplane, the web service would be unavailable for no more than a few minutes before this would have an impact. Alternatively, the carrier's procedures and terms and conditions might have to change so that the validity of the travel document is checked at the time that a ticket is issued. This would require the output option for the web service to the carriers to be "**number of days remaining**". Fall-back measures to be able to handle carrier queries in the event of web-service unavailability would have to be implemented.

3.3.7.3 *Baseline security measures*

Based on the outcome of the security risk assessment and the privacy impact assessment, specific controls would have to be implemented.

As a baseline, the general preventive, detective and response mechanisms that would be implemented for the central system in terms of people, processes and technology should also be implemented for the web service. There should be a strong separation between the web service and the central system to prevent data leakage. Additionally, in the event of a major incident where an intrusion into the web-service infrastructure is successful, the impact should be prevented from escalating by implementing a strong separation, so that the web service cannot be exploited to further compromise the central system. This would include defining one-way access from the central system to the web service for transferring data extracts; the implementation of a DMZ and firewalls; and monitoring and intrusion-detection mechanisms.

For the front end of the web service, the development of the interface must be carefully designed according to best practice to manage the risk of attacks and reduce any potential impact. This could, for example, include the best practice as defined by OWASP (the Open Web Application Security Project). The web service should be carefully monitored and regularly undergo security testing, such as vulnerability scanning and penetration testing, to ensure the early detection of attack vectors which could be deployed for malicious activities.

3.3.8 **Other considerations**

3.3.8.1 *Support services*

Apart from the technical considerations for the web service, it must also be considered which support services would be needed for the web service.

In the benchmarked systems examined under section 3.3.3, helpdesk services are provided to carriers and travellers. It must be decided if similar services are to be provided, and if so the scope and means of the service in terms of:

- The types of support and help provided:
 - How to use the service;
 - Providing content information (e.g. OK/NOK answers);
 - Re-set of credentials (if relevant).
- Hours of service - 24/7 or less;
- Languages that the service will be provided in;

¹¹² Please note that options to provide information via telephone or email were assessed as unfeasible in the Technical Study due to cost and operational considerations.

- Communication channels (phone, e-mail etc.).

3.3.9 Costs

A report with a cost analysis of the options in the Study was published¹¹³ to accompany the European Commission's Technical Study. In this section, the analysis and estimations in the previous Cost Analysis will be revisited in light of the aforementioned options for the web service which scored the highest (for both travellers and carriers).

This covers the dedicated infrastructure that would need to be implemented, as well as the main service costs. Other costs (e.g. IT room space and procurement) can either be distributed across existing infrastructure/manpower or can be assumed to be negligible compared to the overall costs.

The identified costs are:

- **Contractor:** the cost of developing the functionalities required in the central system for creating the extract, and the functionality of the web service itself;
- **Hardware:** the costs of hardware and the service for configuring the hardware needed for the back-end web service;
- **Website:** the cost of developing the front-end website and of the associated hardware and assets (e.g. domain names, content-management system);
- **Network:** the cost of the network bandwidth needed for communication between CU and BCU;¹¹⁴ and
- **Administrative:** staff costs for service support (helpdesk, monitoring and maintenance).

The findings of the "Smart Borders – Cost Analysis" are summarised below.

Table 46 *Web service – Cost estimation from European Commission's "Technical Study on Smart Borders – Cost Analysis"*

Cost type	Development and implementation costs (first three years)	Subsequent yearly operational costs
Contractor development	€160,000	€12,000
Hardware	€3,6 million	€650,000
Website	€1,1 million	€100,000
Network	€135,000	€80,000
Administration	€660,000	€660,000
Total	€5,7 million	€1,5 million

¹¹³ European Commission, Technical Study– Cost Analysis, 2014, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf.

¹¹⁴ In the Cost Study, the network cost was based on a scenario whereby the extract from the central system was transmitted to a location removed from eu-LISA's CU and BCU sites. It was estimated that this would be the same as a PTP connection between the CU and the BCU. This report assumes that the web service would be hosted by eu-LISA on current eu-LISA premises, and that eu-LISA thus bears the costs of CU-BCU network communication.

3.3.9.1 Contractor costs

The contractor costs in the cost study were calculated based on the number of tasks that would have to be developed. For the highest-scoring options, the number of tasks would remain approximately the same. The addition of an additional task would result in a cost increase of less than €27,000, which is approximately 0.5% of the overall cost estimate. Therefore variations in costs under this heading are considered to be negligible.

3.3.9.2 Security measures

As already mentioned, such a service – which would be available over the public Internet – introduces attack vectors and an attack surface which are new to eu-LISA's operational methods and models.

To implement adequate system monitoring, Security Incident and Event Management (a SIEM) will be required for the service. An estimated €500,000 would have to be budgeted for this system, or if it can be implemented as an extension of an already operational SIEM, the cost would be approximately €200,000. In addition, vulnerability scans and penetration testing should be budgeted for at an additional cost of €175,000.

To maintain service availability and prevent DDoS attacks, a service for guarding against such attacks should be provisioned. This would likely be from the eu-LISA's network service provider at an estimated cost of €400,000.

Moreover, as the highest-scoring option for the carriers assumes that carriers are identified in the system, additional costs would be expected for components to manage credentials. Developing and implementing such a component would likely cost in the range of €250,000.

A unified threat-management solution should also be implemented for the web service. This should include intrusion prevention, load balancing and data-loss prevention, among others.

These costs are based on eu-LISA's current experience of provisioning such services for existing systems.

Table 47 Web service – software security cost items

Cost type	Development and implementation costs (first three years)	Subsequent yearly operational costs
SIEM	€500,000	€40,000
Vulnerability scans and penetration testing ¹¹⁵	€100,000	€175,000
DDoS prevention service	N/A	€200,000
Credential management	€250,000	€250,000

The estimate for the above costs is expected to be included in the provision provided for in the "Security measures" section of European Commission's "Technical Study on Smart Borders – Cost Analysis",¹¹⁶ which envisaged €1.8 million in development and implementation costs and an additional €450,000 in yearly implementation costs.

¹¹⁵ These tests would be expected to be partly included under the cost of developing the website, therefore the initial costs are lower than the ongoing yearly costs of such services.

¹¹⁶ The "Hardware" cost component of the cost study included storage, database servers, application servers and security measures. See Section 4.4.2.2 of European Commission, "Technical Study on Smart Borders – Cost Analysis" report.

Table 48 Web service – overall cost estimation for security measures¹¹⁷

Cost type	Development and implementation costs (first three years)	Subsequent yearly operational costs
Set-up costs for two central nodes (CU and BCU)	€1.2 million	€300,000
Set-up costs for firewalls between the remaining nodes	€600,000	€150,000
Total	€1.8 million	€450,000

3.3.9.3 Cost of other options

The highest-scoring options for travellers are also estimated to be the least costly ones. The more complex options, including an account-based web service, would be more costly, particularly with regard to website development, hardware, credential management and administration.

Implementing a solution to additionally manage accounts for travellers is expected to add €300,000 to the budget of an identity and access management solution. Furthermore, the helpdesk would have to be expanded to provide support to travellers with account issues, and thus the costs of this function would double, adding €180,000 to the administrative costs.¹¹⁸ This still presumes that the helpdesk service is provided in English only. Finally, the additional personal information collected from travellers (e.g. email addresses) would require additional software measures, such as the deployment of an advanced threat-detection solution aimed at strengthening protection against data breaches, due the fact that this data would be accessible from the public internet. The yearly cost of these additional software packages is estimated at €750.000.

Depending on the solution chosen, the need for additional hardware (for example for storage) would also increase in line with the amount of data that would need to be available, the log files created and the data-retention period for this information.

In conclusion, the account-based solution is estimated to increase development and implementation costs by approximately 50% and to double the yearly costs (+100%) compared to simpler solutions.

3.3.10 Conclusions

As already mentioned, the choice of the final design will depend on the importance given to each of the three criteria: privacy, service, and complexity – in this desk research they have been given equal weighting for the scoring. The benchmarking exercise and the subsequent examination of different options combining various types of information used for input and output of the proposed web service, leads to a preference for simple solutions for the following reasons:

- Sufficient to provide information which is comparable to the level of information provided by the physical stamping of passports;
- Sufficient to provide a level of service and information which is comparable to the benchmarked systems, and thus match travellers expectations based on experiences with such similar systems;
- Limited complexity and cost of implementation and maintenance;
- Limited privacy implications.

¹¹⁷ European Commission, "Technical Study on Smart Borders – Cost Analysis", October 2014, Section 4.4.2.2, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf.

¹¹⁸ The cost component 'Administration' included 4 FTEs for 'Security Staff' at €440.000 and 3FTEs for the 'Helpdesk' at €180.000.

This is based on the assumptions as outlined in the beginning of the chapter. Should any of these change, especially with regards to the obligations of the carriers, then the options would need to be re-examined. The underlying requirement for the web service is the abolition of stamping. Should this not be the case, then the need for this particular solution and the options would again need to be re-examined.¹¹⁹

In addition the help and support services provided for the solution should be defined as this is likely to have a significant impact on the cost of operating the web service.

Finally, depending on the input and output options chosen and the definition of availability requirements, further analysis should be done to refine the security and privacy protection requirements, the organisational support needed and the cost of the solution.

¹¹⁹ Other options to compensate the abolition of the physical stamping could be proposed, such as another kind of receipt or token containing entry exit information. Such solutions are beyond the scope of this desk research and therefore are not examined within this chapter.

3.4 Equipment and costs

3.4.1 Introduction

Objective

When considering the feasibility of technical solutions for future biometric-based border checks, one aspect of obvious relevance in the assessment is the costs of equipment needed to enrol biometrics and subsequently to perform biometric checks. In this chapter, indicative costs are provided for equipment capable of:

Enrolling four (4), eight (8) and/or ten (10) fingerprints, a live facial image and/or the two iris images from a single person;

Capturing the facial image stored on the chip of eMRTDs and **verifying** that image against a live facial image;

Enabling automated or semi-automated checks (in the context of Smart Borders principally automated exit checks and pre-border checks at land borders).

The costs laid down in this chapter can be used along with the operational testing circumstances described in previous chapters of this report in order to consider the balance between costs and benefits of any particular biometric modality, set-up and equipment configuration.

An effort is made where possible to define minimum costs and average prices for particular device types and configurations that could be used at various locations. Obviously definition of minimum costs for equipment that would be required at any location requires minimum standards to be set for such equipment if it is to function appropriately and effectively. Thus, where possible, minimum standards for successful execution of the biometric processes at the following border types are outlined:

- Air;
- Sea;
- Land (road);
- Land (train – including moving train).

Thus, in each section of this chapter, minimum equipment standards are initially outlined before costs for such equipment are introduced. In general, costs for new equipment are provided, with average price ranges put forward for both single and bulk purchases in order to give a complete picture of possible future cost ranges. Costs are broken down to as fine a level as practical in order to allow some judgement on costs applicable for equipment upgrade when some relevant devices are already available at the border crossing point. Finally, where more expensive equipment would have some notable benefits, this information is provided based on the results of various operational tests executed within the pilot in order to aid cost-benefit analyses to be carried out by purchasing entities at a later stage.

Methodology

The information presented herein is mainly based on input from vendors and integrators of biometric solutions. A questionnaire¹²⁰ was distributed to the vendors and information subsequently added through meetings and bilateral discussions. Finally, literature was reviewed and on-line analyses executed to provide information that was lacking.

¹²⁰ Vendors were asked to provide the following information:

- List prices (in €) and bulk purchase prices;
- The costs for device purchase only without any associated service or maintenance costs that might be included in a contractual arrangement with a future purchasing entity;
- Separate costs for software and hardware when possible.

Note that installation costs were noted to vary and would have to be considered on a case by case basis.

All results have been aggregated and no single vendor data is referred to directly in this report. No comparison or assessment of specific equipment or vendor is made.

Five vendors replied to the questionnaire, providing details on the types of device. For analysis of price ranges and inclusion of such information in this chapter, it was considered that data should be available for at least three different devices within any category. Thus, when data for fewer than three devices was available from the questionnaire, additional information was collected during bilateral discussions, specific workshops and through literature review.

3.4.2 Solutions for biometric enrolment and verification

3.4.2.1 *Fingerprint enrolment*

Functionalities of equipment

To capture any number of fingerprints, the following equipment must be considered necessary:

- A Fingerprint scanner (hardware);
- Appropriate software to execute the fingerprint capture, and where appropriate, assess fingerprint quality in (close to) real time and activate user feedback loops and re-enrolment attempts as necessary to provide a suitable send sample.

In some cases, devices have software built-in and can therefore be used in a fully autonomous fashion (hereinafter referred to as “stand-alone”). When the software is not included in the device, the device must be integrated into some form of platform (hereinafter referred to as “integrated”). Most of the standalone devices can also be integrated into suitable platforms.

Fingerprint scanners vary greatly, offering different features that bring various benefits in different circumstances. Models of scanner may be categorised based on the number of fingerprints that can be captured in a single attempt (one, two or four) or whether they are contactless or require the user to touch the scanner to enrol the fingerprint, for example. Some devices are multimodal¹²¹ and perform fingerprint enrolment (and perhaps verification) in addition to iris and/or facial image enrolment (and perhaps verification). Naturally, given this variability, prices of devices vary significantly.

Some functions are very common:

- The majority of devices are optical scanners;
- Almost all devices enrol fingerprints at 500 dpi resolution;
- Almost all devices connect to other IT infrastructure through USB interfaces;
- Finally, most devices are FBI certified, except multispectral and contactless devices so far.

Cost components

Given the diversity of sensor types and functionalities, prices can vary significantly from one device to the next. As a consequence, fingerprint enrolment devices have been grouped by category according to the criteria that appear to have the most meaningful impact on costs:

- Number of FPs captured in one attempt;
- Contact vs contactless devices;
- Mobile vs fixed devices.

¹²¹ Multimodal devices were considered out of scope during research. However, to provide indicative information, it may be noted that a mobile device performing fingerprint, iris and facial enrolment can be purchased for approximately 10 000 €.

Table 49 Average prices (in EURO) of devices categorised by the number of FPs captured at the first attempt

	mobile	fixed	contact	contactless
1 FP in 1 attempt	1250	355	870	N/A
2 FPs in 1 attempt	9600	600	5100	N/A
4 FPs in 1 attempt	N/A	8410	1824	16643

Vendors indicated that discounts were normally offered for bulk purchases and dependent on the quantity of devices acquired as well as outcomes from management discussions and decisions. As a general guideline,

- Discount percentages range from 10% to 20 % for the purchase of 100 items;
- Discount percentages may rise to 25 % for the purchase of 1 000 items;
- Discount percentages may rise to 40% or more for the purchase of 10 000 items.

Notes from operational tests

When reflecting on operational results, it may be noted that standard set-ups were less suitable in some specific locations. Optical scanners typically performed poorly in outdoor conditions when direct sunlight shining onto the glass platen interfered with the enrolment process. However, as noted in Chapter 3.1, other devices could be used in such environments. Mobile devices offered process flexibility in certain situations and facilitated testing on the moving train, for example (although the use of a portable suitcase containing a standard optical scanner, as deployed on the moving vessel at Piraeus seaport demonstrated an alternative approach). Contactless devices typically offered the possibility of quicker fingerprint capture which may be more important in some locations than others. Obviously, enrolment of more fingers at once also provided for more rapid capture of a full fingerprint set. Durations of enrolment of 4, 8 and 10 fingers with different device types are outlined in full detail in the individual BCP chapters.

3.4.2.2 Facial Image enrolment and verification

Functionalities of equipment

To capture the facial image, the following devices or items may be considered as necessary at different locations or in different instances:

- A camera (hardware) (still or video capture);
- Software for capture and preferably image processing (for example cropping and scaling the image in order to provide an ICAO-compliant frontal image);
- Lighting device(s);
- Devices to screen windows and control extraneous light entering the room.

Lighting devices and equipment to screen windows have not been taken into account in this analysis. It may be noted that lighting devices could include lights deployed in the general area of a BCP or specific lighting on or attached to the capture device itself such as flash bulbs in cameras or ring lighting surrounding a camera aperture to provide uniform frontal lighting. Demands for ambient lighting, inclusion of lighting in capture devices or deployment of window shades will vary for each BCP and the processes and arrangement in place, and thus, full coverage of possible combinations would be impossible and was considered out of scope.

Cameras vary in terms of features and general functionalities.

Simple cameras for use in border checks should generally have a reasonable resolution (typically greater than 3 Megapixels) and autofocus capabilities for ease of use. If used in any environment with variable capture conditions (for example outdoors or in an indoor area with windows affecting lighting throughout the day), they should include capabilities to automatically adjust their light sensitivity and contrast.

More sophisticated devices can emit and detect infrared radiation as well as light in the visible spectrum in order to help create 3D representations of the face and also to counteract fraud by performing IR-based liveness detection (for more information see section 3.5). Some devices are multimodal and incorporate hardware for capture of fingerprints and iris images.¹²²

In addition, to perform verification, i.e. to capture the facial image from an eMRTD and verify it against a live facial image, the following devices are required:

- A document (passport) reader with RFID capabilities;
- Software for facial image comparison;
- The equipment can generally be either mobile or fixed.

Cost components

The table below provides further information on costs for the afore-mentioned equipment types. Devices are less diverse in terms of features compared to fingerprint sensors and prices are more homogenous as a result. Thus, a breakdown based on capabilities is not provided.

Table 50 Average prices (in EURO) for FI enrolment and verification (capturing eMRTD and verifying against live FI) devices

	Average price in €
Hardware (camera)	100€ (for the webcams used in pilot testing at various locations, incorporating full HD capabilities). Custom-built solutions with integrated lighting or flash were deployed in some locations and vendors indicated that the cameras used therein had a very similar cost, with additional costs related to additional customised hardware and software.
Document reader	€1938
Software	Software is almost always customised based on customer needs, and therefore prices can only be provided based on individual requests. A software providing fingerprint, facial image and iris capture with local matching capabilities for all modalities has been indicated to cost about 200€.

Vendors indicated discount percentages depending on the quantity for eMRTD reader hardware.

- From 10 % to 20 % for 500 devices;
- 20 % to 25 % for 1000 devices;
- 30% or more for 10 000 devices, depending on discussions and negotiations.

Notes from operational tests

Operational results indicated that standard cameras were very capable of enrolling suitable quality images for facial image verification. Capture was typically influenced more by environmental factors than the type of camera used or its particular capabilities. Document readers varied according to whether they were capable of capture without instalment of a hood to exclude ambient light. Some had clips that meant that an officer didn't have to hold the document throughout reading, freeing his/her hands for other tasks. Some included capabilities to check optical document features under UV and IR light and associated software to check results against databases as a means of assessing document legitimacy. All were capable of reading the document chips, with variable performance in that regard associated with the underlying software and for passive authentication, availability of the appropriate certificates.

¹²² Multimodal devices were considered out of scope during research. However, to provide indicative information, it may be noted that a mobile device performing fingerprint, iris and facial enrolment can be purchased for approximately 10 000 €.

3.4.2.3 *Iris enrolment*

Functionalities of equipment

Different types of equipment can perform iris enrolment:

- Dedicated iris cameras;
- Multimodal biometric platforms that incorporate an iris camera.

Iris cameras can be based on use of visible and/or more typically near infrared (NIR) light with wavelengths in the range of 700 – 900 nm. The required capturing distance may vary greatly depending on the capabilities and set-up of the optics within the device. Out of the 3 devices mentioned by vendors in their responses to the questionnaire, the capturing distance varies from 120 millimetres to 1 metre. Longer capture distances typically require higher resolution sensors, with sensors in iris capture devices typically having resolutions of up to 17 pixels/mm. Typically, 12 pixels/mm can be considered a minimum requirement in basic iris cameras. Depending on the border type and the processes used, different capture distances will be preferred. Similarly, process design will determine whether fixed or mobile devices are preferred.

Some devices can incorporate hardware specifically present for presentation attack detection or liveness detection. The inclusion of such capabilities will depend on a thorough risk analysis for any particular deployment that should consider matters such as the level of supervision of sample capture, the distance at which supervision is undertaken and the assessed vulnerability of other steps in the overall border crossing process. Further information on hardware and software for presentation attack detection in iris devices is provided in section 4.5.

Cost components

Prices vary greatly from one device to another and depend on any device's capabilities. The simplest iris cameras costs approximately 1000€ but more sophisticated devices were indicated to cost significantly more. The addition of in-built software for verification and inclusion of anti-spoofing features in the hardware also results in higher device prices. In operational testing, some devices used included a separate camera for facial image enrolment. The cameras included in such instance were standard low-cost cameras described in the previous section of this chapter. Their inclusion didn't affect the price of the capture device.

There was little apparent difference in costs for mobile and fixed devices.

Vendors indicated discount percentages depending on the quantity of devices purchased:

- 10 – 20 % discount for 500 items;
- 20 – 25 % for 1000 items.

Notes from operational tests

Fixed devices generally enrolled iris images more quickly than mobile devices. Their deployment typically involved some construction or modification of the border crossing point, however. Devices acquiring iris images at longer distances were found to be convenient for use but more susceptible to environmental influences, particularly strong extraneous light.

3.4.3 Solutions for automated checks

3.4.3.1 *Automated checks at exit - ABC gates*

Functionalities of equipment

ABC gates vary according to their functionalities and can have variable configurations. The majority take the form of e-gates that perform automated document bearer verification by comparing a live facial image enrolled in or at the gate against the facial image extracted from the eMRTD. However, some also execute enrolment and/or verification of fingerprints and/or iris images. Thus, ABC gates can use single or multiple biometric modalities. Configurations can variably involve use of a mantrap while ABC systems can involve 1, 2 or more steps.

This report includes results from testing involving one step mantrap gates, two-step integrated gates with mantrap and two-step segregated gates with mantrap. Herein, general price information is provided without attempting to distinguish costs for different configurations. In all cases, the costs provided necessarily include the gate infrastructure itself, the associated biometric enrolment devices, the background software, visual interfaces, installation services and software modification services as necessary to interface to border control systems in place at the BCP. Additional features that could be added include addition of supplementary hardware for presentation attack detection and inclusion of hardware and/or software for document fraud detection.

Cost components

The average price for a single ABC gate amongst those for which information was provided was 85,000€. Gates are often sold in banks of 4, 5 or 6 units, and discounts are typically provided in such instances. The indicated discounts for such multi-gate purchases ranged from 15-25%.

Notes from operational tests

All e-gates tested were capable of providing for automated border checks at all types of border. As for systems executing facial image-based verification generally, performance appeared to be as much dependent on the environment as the hardware and software deployed. Some configurations provided for quicker border crossing but any decision as to which configuration might be most appropriate would depend on the BCP layout, traveller flows and operational practicalities. Additional devices for fraud detection that might imply additional costs were not directly tested.

3.4.3.2 *Self-service kiosks and pre-border checks at land borders*

Functionalities of equipment

Self-service kiosks are highly customisable solutions, tailored for use at particularly border crossing points depending on operational demands. They may accomplish biographic and/or biometric data (uni-modal or multimodal) enrolment and/or verification, allow travellers to provide answers to questions associated with their border crossing and may be connected to national or international databases to allow for screening checks to be made in advance of the final step of border crossing. Depending on the tasks to be accomplished, they will variably include document scanners (either swipe or flatbed), devices for biometric sample enrolment, software for data processing and execution of the underlying process logic and some form of interface to allow the traveller to proceed through the process, typically involving touchscreens. Depending on security requirements and the level of supervision, associated infrastructure for monitoring use may be considered, such as monitoring cameras or inclusion of devices to ensure use by one traveller only at any given time. They may be deployed ahead of manual controls, with the kiosk designed to accomplish the time-consuming steps that might not typically require personal interaction between the traveller and border guard. Alternatively, they can be used as the first step in a two-step segregated ABC process; in such instances, all checks take place at the kiosk and a token may be captured to allow the traveller to proceed through the gate that is the second step of the whole process. Finally, they may be deployed at locations distinct

from the border to provide for processes being run in advance of border crossing. Within the pilot, a self-service kiosk was deployed in a waiting area at a land border crossing point to examine possibilities for time-consuming enrolment of biometric and biographic information to be performed away from the border in advance of the crossing. Additionally, the idea of deploying kiosks on moving vessels or other areas away from the actual BCP was proposed in some discussions with border guards, as described in various BCP chapters in this report.

Self-service kiosks tested in the pilot typically accomplished enrolment of fingerprints and a live facial image and also executed facial image verification by extracting the facial image from the eMRTD using a flatbed document scanner. In some instances, questions to be answered by travellers were included in the process. Two-step segregated ABC systems were also tested. Discussions of costs below relate to these kiosks only.

Cost components

A standalone kiosk with capabilities for scanning an eMRTD, enrolling fingerprints using a 4-finger optical scanner, capturing a live facial image and comparing live and chip images costs on average approximately 12000 €. Integration of the kiosks into border control environments may be necessary in instances where the results of enrolment and/or verification must be displayed in the manual booth, where queries of national or international databases might be required or where the kiosk is linked to an ABC gate as part of a two-step segregated process. In such instances, the average price of the full kiosk solution including integration services may be 3-4 times the price indicated for the standalone kiosk.

Notes from operational tests

There was little variation in the kiosks deployed in operational testing and therefore little can be said regarding the merit of various features that may lead to increased or decreased kiosk costs. Considerations outlined in previous sections will apply depending on whether the kiosk will include devices for fingerprint, facial image or iris enrolment. The main determinant of kiosk costs will, however, likely be the extent of customisation demanded and the number of kiosks purchased rather than the precise hardware to be included.

3.5 Spoofing vulnerability of iris enrolment and counter-measures

3.5.1 Introduction

Spoofing refers to use of a fabricated sample or physical trait to deceive a biometric system into believing the sample is provided by a live and authentic user that is not the person actually presenting him-/herself.

As spoofing typically involves presentation of a fake sample at the sensor, the term presentation attack is often used. In the diagram below, presentation attacks are shown to occur at the very initial point of a biometric system, namely the sensor.

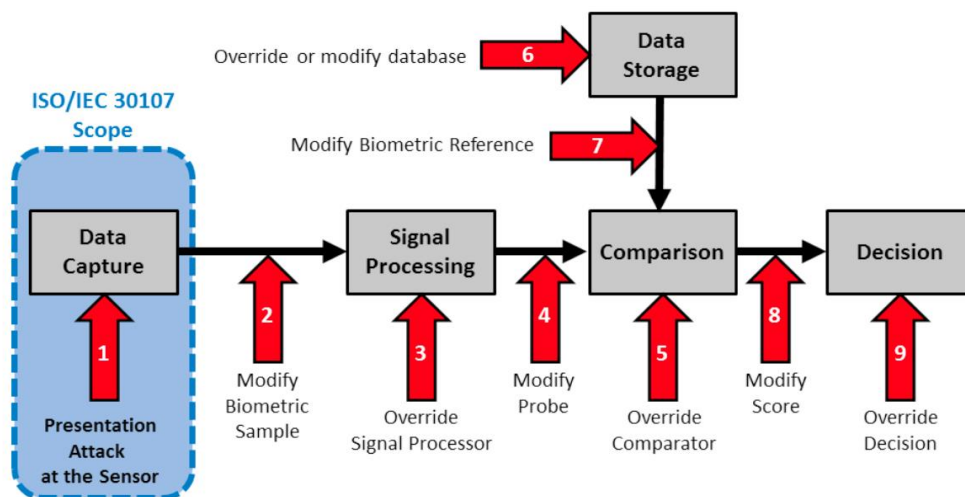


Figure 27 Presentation attacks at sensor

Typically, the person providing the spoofed sample wishes to achieve one of two outcomes:

- An Active Imposter Presentation Attack - when the subversive data capture subject intends to be recognised as an individual other than him-/herself. Two subtypes can be enumerated:
 - The attacker intends to be recognised as a specific individual known to the system and should provide a sample that ideally should closely match that of that other person;
 - The attacker intends to be recognised as any individual known to the system, without specification as to which one;
 - In a border control situation, this could be the desire if using a fake document and attempting to match the facial image recorded in that document using a mask or similar.
- An Identity Concealer Presentation Attack - when the subversive data capture subject intends not to be recognised as any individual known to the system. Two subtypes can be described:
 - The attacker will seek later repeatability of the disguised or altered biometric characteristic;
 - The attacker will seek no later use of the characteristic (a “one-time” deception);
 - In a border control situation, such efforts would be undertaken when a traveller might wish to avoid their presence being detected in some form of watch-list or database, for example.

Clearly, the second approach requires less effort and expertise than the first (as the sample requires less specificity in terms of design) although both types of action are of concern in border control situations.

As the Smart Borders systems are proposed to support advanced biometric-based border checks, the phenomenon of spoofing must be borne in mind when making decisions regarding the biometrics to be deployed and the approaches to such deployment - for example, whether self-service stations are appropriate for use. Aspects were considered in previous discussions and in the Smart Borders study, leading to the conclusions at the time that face,

fingerprint and iris biometrics characteristics be considered as both safe and effective for use in Smart Borders systems and that both manual and automated border controls, including self-service deployments, be considered as possibilities, either in supervised or unsupervised conditions. Based at least in part on the fact that European authorities typically have less experience with iris biometrics compared to face and fingerprint, it was noted that specific emphasis be placed on spoofing of the iris when undertaking research work within the pilot. This section aims to answer the following question, therefore:

3.5.2 **Is the iris as a biometric more or less prone to spoofing than other relevant modalities and which anti-spoofing measures need to be undertaken?**

It should be noted that although the question relates specifically to the iris, it cannot be answered without thorough consideration of counter-spoofing measures used with other biometric modalities that had to be assessed for purposes of comparison.

In the preparation of this chapter, the question above was considered based on a number of undertakings. Literature review was a significant element of work. Documentation and academic articles on counter spoofing measures and their effectiveness highlighted both different relevant approaches and the overall state-of-the-art. Documentation from NIST, ISO and the BSI as well as the EU-funded Tabula Rasa and Fidelity projects provided good material in this regard, Articles identified as particularly relevant to iris spoofing are listed in the appendix. Particular emphasis was placed on the analysis of results of competitions in which the performance of different counter-spoofing algorithms or systems were analysed, particularly the LivDet reports. Finally, the opinions of experts at European and international levels were sought. Aspects considered beyond the biometrics themselves included the equipment needed, the level of operator supervision in typical border control situations and the expertise of travellers.

3.5.2.1 *Terminology*

With regard to counter-spoofing measures generally, liveness detection is a crucial approach. As spoof samples are typically (though not necessarily) non-live, it should be possible to detect spoofing by detection of the use of samples prepared from non-biological materials. Approaches to present fake yet 'live' samples are typically drastic and involve surgical interventions. As pointed out by some Member State experts in discussions on the topic, significantly simpler methods of spoofing can be utilised in order to circumvent biometric checks at most borders and therefore such drastic measures don't really need to be considered seriously. Therefore, for our purposes herein, liveness detection is considered the appropriate approach to counter-spoofing at borders.

There are two major approaches to liveness detection:

- Hardware-based systems - these typically involve deployment of additional sensors and software beyond those needed for biometric enrolment itself. Thus, their use may include measurements outside of the primary biometric mode;
- Software based systems - these use image processing algorithms to detect features atypical of live samples. As these are purely based on software, this approach requires less specific equipment and it is amenable to central deployment (i.e. on a central AFIS or similar), which has benefits from cost-effectiveness, convenience and harmonisation perspectives.

An alternative approach to counter-spoofing often cited in the literature and in discussions is the use of multimodal biometrics. The argumentation in this regard is that through the deployment and use of different biometrics at once, safety is increased as it is more difficult to spoof two or more biometric systems at once than any single such system. This approach is not within the scope of this chapter, however, and therefore not considered further.

When reporting on spoofing, the following terms are commonly used:

- Ferrfake - misclassified fake samples ('false acceptance');
- Ferrlive - misclassified live samples ('false rejection');
- HTER- the half total error rate. It is the average of ferrlive and ferrfake rates when being applied in the context of

presentation attack detection and counter-spoofing.

Further terminology to be used is introduced in the ISO/IEC 30107 standard. In particular, part 1 of the standard, published in April 2015, provides a framework for work in the area of presentation attack detection and defines terminology to be utilised.

This full standard aims to establish:

- Terms and definitions that are useful in the specification, characterisation and evaluation of presentation attack detection methods (Part 1);
- A common data format for conveying the type of approach used and the assessment of presentation attack in data formats (Part 2);
- Principles and methods for performance assessment of presentation attack detection algorithms or mechanisms (Part 3);
- Classification of known attacks types (in an informative annex).

The work, begun in 2011 by the “Technical Committee ISO/TC JTC1, SC 37, Biometrics, WG3” continues to advance towards an anticipated publication date of 10.09.2016. As of 16.09.2015, the following status has been recorded:

- ISO/IEC 30107-1 Biometrics presentation attack detection -Part 1 Framework: DIS (Draft International Standard, voting closed);
- ISO/IEC 30107-1 Biometrics presentation attack detection -Part 2 Data formats: CD (Committee Draft) study/ballot initiated);
- ISO/IEC 30107-1 Biometrics presentation attack detection -Part 3 Testing and Reporting: CD (Committee Draft) study/ballot initiated).

Throughout this text, the terminology of ISO/IEC 30107-1 has been utilised insofar as possible.

Literature review - Presentation attacks targeting the iris

As a starting point in the discussions, approaches to spoofing iris-based systems are enumerated. The following possible approaches are noted:

- Use of an artificial eye - although possible in principle, this would typically involve surgical interventions. As already noted above, this would appear unlikely given the possible success rates of other less drastic approaches, and therefore consideration of presentation attack detection when the attack involves a replacement artificial eye is of little priority herein;
- Presentation of (a) high quality print-out(s) of the iris image. The printouts would be presented to the iris enrolment camera at enrolment time. The approach is equivalent to the presentation of facial image printouts to fool facial image recognition systems;
- Using an iris image as a mask on a real eye. In these situations, the iris image is printed onto a material that can be placed onto the eye, for example a contact lens. It is analogous to the use of a mask in facial recognition scenarios;
- Using cosmetic contact lenses. This is a variation of the above, where the commercial contact lens could be used at enrolment and then again at the time of verification, thereby obviating any need for the lens to actually represent the real iris of an individual;
- Display of an iris image on a handheld screen. This is equivalent of the display of a facial image on a phone or tablet device for duping facial recognition systems.

3.5.2.2 Presentation attack detection for the iris

As a preliminary point when discussing iris spoofing, it should be noted that a natural iris image is *per se* difficult to replicate. As per Daugman's original patent on the topic, US Patent 5.291.560, traditional iris codes are 256 bytes. Due to radial correlations, there is a standard binomial distribution of 173 bits. Thus, the odds that two different irises might generate an identical iris code are 2^{-173} or 10^{-52} . Active imposter presentation attacks require some level of detail and some expertise in implementation therefore if they are to be successful.

It should be noted that the iris is also innately resistant to spoofing. In a similar manner to how still photos of a particular facial image can be detected by seeking natural movements such as blinking or movement of the mouth, a live iris presents natural movements that may be detected in order to guard against still image presentation. Specifically, the pupil diameter of a living eye undergoes small oscillations ("hippus") one or twice per second and these movements can be used for liveness determination. Indeed, Dr J. Daugman, the holder of the first patent for iris recognition that lead to widely deployed solutions, stated in his patent that the algorithms he proposed provide inherent liveness detection and the method has been developed and refined in the ensuing years (Bodade et al. 2009, 2011, Huang et al. 2013 and Czajka 2015).

Other methods have been elaborated in recent years to complement these inherent capabilities. Throughout the literature, including work from the FastPass consortium, several approaches are noted. These include both hardware and software-based methods.

Hardware-based

- Chen et al. (2012) discussed examination of texture changes of the conjunctival blood vessel and iris patterns from multispectral images;
- More recently, Connel et al. (2013) proposed an approach to detect cosmetic contact lenses by projecting additional structured light patterns onto the eye.

Software-based

- Using image texture analysis, e.g. analysis of **high-frequency spectral** magnitude based on Fourier transforms (Daugman 2003). The method recognises spurious coherence from printed iris patterns;
- Galbally et al. (2012) described liveness detection based on a **set of image quality** related features;
- Galbally **also looked at optical properties** of different parts of an eye and retina reflection. High quality cameras are required for capturing these features;
- Combinations: (Lee and Son, 2012) **combined both optical and texture features** in iris anti-spoofing detection.

In Galbally, a two-stage protection scheme against masquerade attacks carried out with synthetically reconstructed iris images (as described in (Galbally)) was proposed. It consisted of two steps, namely edge detection involving detection of pixels outside the iris boundary and power spectrum analysis of the images to detect abnormal high-frequency energies.

The method was shown to be very useful, producing ferrfake rates of 0.0% and ferrlive rates of 0.3%.

Many articles describe similar stories of success in which methods have been developed and deployed that particularly target specific methods of presentation attack. In general, it can be concluded that today there is no 'Silver Bullet' therefore, and there is no single technology that stands out. Different technologies address different attack vectors and deployments would need to consider utilisation of several such methods in parallel, likely adapted to need based on a specific risk assessment of the vulnerabilities of a specific deployment.

3.5.2.3 Presentation attack detection baseline performance measures

In order to provide a baseline for later discussions, (Ruiz, 2008) described success rates for different vectors of attack on an iris system. Two different attack scenarios were considered as well as a reference scenario known as the normal operation mode:

- Normal Operation Mode (NOM): both the enrolment and the test were carried out with a real iris. In this context the FAR of the system was defined as the number of times an impostor using his own iris gained access to the system as a genuine user. The FRR (False Rejection Rate) denoted the number of times a genuine user was rejected by the system;
- Attack 1: both the enrolment and the test were carried out with a fake iris. In this case the attacker enrolled to the system with the fake iris of a genuine user and then tried to access the application with a fake iris of the same user. In this scenario an attack was unsuccessful (i.e. the system repels the attack) when the impostor was not able to access the system using the fake iris. Thus, the attack success rate (SR) in this scenario can be computed as: $SR = 1 - FRR$;
- Attack 2: the enrolment was performed using a real iris, and tests were carried out with fake iris. In this case the genuine user enrolled with his/her iris and the attacker tried to access the application with the fake iris of the legal user. A successful attack was accomplished when the system confused a fake iris with its corresponding genuine iris, i.e., $SR = FAR$.

In order to compute the performance of the system in the normal operation mode, all the images of the first session were considered as enrolment templates for a given user. Genuine matches were obtained by comparing the templates to the corresponding images from a second session with the same user. Impostor matches were obtained by comparing one randomly selected template of a user to a randomly selected iris image of the second session from the remaining users. Similarly, to compute the FRR in attack 1, all the fake images of the first session of each user were compared with the corresponding fake images of the second session. In the case of the attack 2 scenario, only the impostor scores were computed, matching all 4 of the original samples of each user with the corresponding 4 fake samples of the second session.

The decision threshold was fixed at FARs of 0.1, 1, 2, and 5% in the normal operation mode and the success rate of the two proposed attacks computed. Generally, the system was vulnerable to the two attacks, as shown in the table below (i.e. a success rate of about 35% or higher was observed).

Table 51 Vulnerability of system

NOM	Attack 1	Attack 2
FAR - FRR (%)	SR (%)	SR (%)
0.1 - 16.84	33.57	36.89
1 - 12.37	48.02	52.44
2 - 10.78	53.03	56.96
5 - 8.87	61.19	64.56

In (Galbally), the authors reverse engineered a synthetic iris image from an iris code (the template that would be stored in a database and used for matching purposes). At a nominal decision threshold of 0.1% FAR, success rates for spoofing attacks were 81% with the presentation of one engineered iris image and 96% when 5 reconstructed images were compared to 1 real image, thereby improving the chances of success. Despite the need for particular expertise in order to prepare a sample sufficiently detailed to fool an iris system, the authors demonstrated that it is possible to generate multiple synthetic iris patterns with iris codes very similar to the real one. In fact, in 50.9% of all cases, all 5 of the reconstructed images prepared within the research were positively matched to the original real image at the

same security threshold. Notably, reconstructed images prepared in this research fool humans in fewer cases than automated systems. Experts attempting to classify fake and real irises, given approximately 6 seconds to decide, produced error rates close to 10%; amongst non-experts error rates were closer to 40%.

In order to benchmark these results against those for facial recognition and fingerprint-based systems, a number of other relevant studies are noted. In (Erdogmus), a commercial 2D face matching system was attacked using 3D-printed masks purchased online following upload of 2D photos of the face to a commercial website. Using the equal error rate (EER) as a decision threshold for verification, 65.7% of mask attack attempts were misclassified as 'real' clients. Di et al (Di) reported that a commercial off the shelf (COTS) facial recognition system could be fooled. In 1:n searches against a gallery of genuine face images, a replayed video provided as the probe was placed as the highest scoring match (i.e. placed at rank 1), in more than 70% of cases. Fingerprint spoofing, meanwhile, has also been demonstrated to be relatively straightforward when systems are not protected, with spoofs being prepared both from cooperative and non-cooperative (i.e using latent prints) subjects as sources of the print. Marasco (Marasco, 2014) provides an excellent overview of false acceptance rates for spoofed fingerprints prepared from different materials, ranging from up to 100% false acceptance of gelatine prints with both optical and capacitive sensors through 82% spoof false acceptance rates with conductive silicon and 12% success rates for play-doh on capacitive DC scanners (albeit 58% on optical scanners).

It may be concluded that all biometrics being discussed herein are susceptible to spoofing. The importance of implementing counter-spoofing measures is emphasised and will involve a thorough risk analysis in order to investigate the most likely and dangerous attacks and ensure resistance to such attacks is built-in.

3.5.2.4 *Certification and standardisation of equipment resistance to spoofing*

Given the above assertion, it is natural to question whether particular biometric devices or systems have been certified to be resistant to the most relevant presentation attacks in any given scenario.

ISO/IEC 19792:2009 specifies the subjects to be addressed during a security evaluation of a biometric system. However, it does not define any concrete methodology for the security evaluation of biometric systems but rather just focuses on the principal requirements. In efforts to develop more concrete methodologies, the Common Criteria working groups have been working on adaptation of the evaluation scheme for the evaluation of fingerprints based systems (since 2000). Furthermore, national schemes (FR, ES, DE) have been established since 2007. Particularly the Spanish CCN works on the definition of a document for:

- Defining the attacks to be taken into account during an evaluation;
- Defining a testing methodology;
- Defining a rating table for quantification of the resistance level.

The German BSI has created Protection Profiles (BSI-CC-PP-0062-2010 Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7 and an enhanced version, BSI-CC-PP-0063 2010 Fingerprint Spoof Detection Protection Profile (FSDPP), Version 1.8) based on adapted Common Criteria norms. These profiles are limited to FP sensors. Vulnerability assessment is accomplished using a defined and large set of fake fingers.

The Biometrics Institute has developed a framework (BVA - Biometric Vulnerability Assessment) to assess the vulnerabilities in biometric systems.¹²³ Since 2007, it has been applied to face, finger and iris biometric recognition. It aims to provide a methodology to:

- Find unknown vulnerabilities in systems;

¹²³ Biometrics Institute White Paper: "Biometric Vulnerability: A Principled Assessment Methodology" (August 2008).

- Provide different levels of vulnerability assurance based on the proportion of attacks likely to succeed;
- Assess the full chain of security, including databases as well as sensors.

The aim of the BVA is to allow those implementing biometric systems to understand which risks need to be mitigated and to provide developers with a target for improving resistance to attack. Thus, it does not really support a comparison between different biometric set-ups or different modalities. In general, it may be concluded that standardisation of vulnerability assessment and certification of iris sensors for their anti-spoofing capabilities has been considered but has not been significantly advanced at this stage.

3.5.2.5 *Comparing iris to other modalities - performance challenges*

Having reviewed methods for iris spoofing detection and briefly considered some performance measures thereof, it may now be considered whether the methods outlined provide comparable performance to similar methods deployed for face and fingerprint biometrics.

In the field of biometrics, independently administered challenges are often used to compare modalities, different set-ups or different technologies. Performance challenges of note include ICE 2005, ICE 2006, MBGC 2007-2009, NICE 2007-2009 and NICE II 2009-2011. However these challenges did not specifically address spoofing.

From an anti-spoofing perspective, the Liveness Detection (LivDet) Competitions - which compare biometric liveness detection methodologies, are more relevant. They define a standardised testing protocol for:

- Large quantities of spoof and live samples;
- Software-based or system-based biometric liveness detection solutions.

LivDet competitions were hosted in 2009, 2011, 2013 and will be held during 2015. Currently LivDet competitions deal with iris and fingerprint liveness detection only.

Reports on liveness detection of fingerprint devices and systems are available from 2009, 2011 and 2013. Iris spoofing was only considered in 2013 and therefore only the report from that year provides relevant information for presentation attack detection with the iris. Furthermore, although results are available with fingerprint systems, for the iris the analyses only consider algorithms.

The 'LivDet 2013 Iris Liveness Detection Competition' involved three groups of participants, namely:

- ATVS - Biometric Recognition Group, ATVS Universidad Autonoma de Madrid;
- University of Naples Federico II;
- Faculdade de Engenharia Porto.

The dataset used for the evaluation contained images from 3 different datasets containing mixtures of real and spoofed iris images. Spoof images were collected using patterned contact lenses that obscure the natural iris pattern (the Clarkson and Notre Dame datasets, examples of an Identity Concealer Presentation Attack) and printed iris spoofs that aim to allow identification as another person (the Warsaw dataset, i.e. an Active Impostor Presentation Attack).

Results are shown in the figures below. Ferrlive values are shown in the first graph and varied between 12% and 29% across the two datasets against which all algorithms were tested. Ferrfake rates recorded were between 5% and 31% in two dataset averages.

More already noted, fingerprint spoofing has a longer history of analysis than does iris spoofing. Thus, there is more knowledge and awareness of typical attack vectors and the capabilities of hardware and software to detect presentation attacks. Common spoofing attacks include the use of scanned finger images, artificial fingers and fingertip covers (prepared using a variety of available materials and the use of cadaver fingers).

Counter measures can also be implemented at the software or hardware level, or indeed in combination. Indeed, evidence suggests that combinations of measures from one or more categories should perform better than any single measure (Barsky et al, 2012).

In the latter case, possible approaches include detection and/or measurement of odour, pulse, blood pressure, temperature, or electrical resistance. Devices to measure these aspects that sometimes must be added to the sensor include multi-spectral radiation emitters and ultrasound devices

The 'LivDet 2013 FP Liveness Detection Competition' for Fingerprint Presentation Attack detection was structured into two parts, focussing alternatively on algorithms (in which 11 algorithms were tested against datasets generated from 4 different devices, with at least 4000 images from each device) and on full systems (in which Dermalog and Morpho systems were assessed. Average reported ferrlive rates for algorithms were between 11% and 54% across all 4 datasets at ferrfake rates between 1% and 54%. Full results are shown in tabular format below.

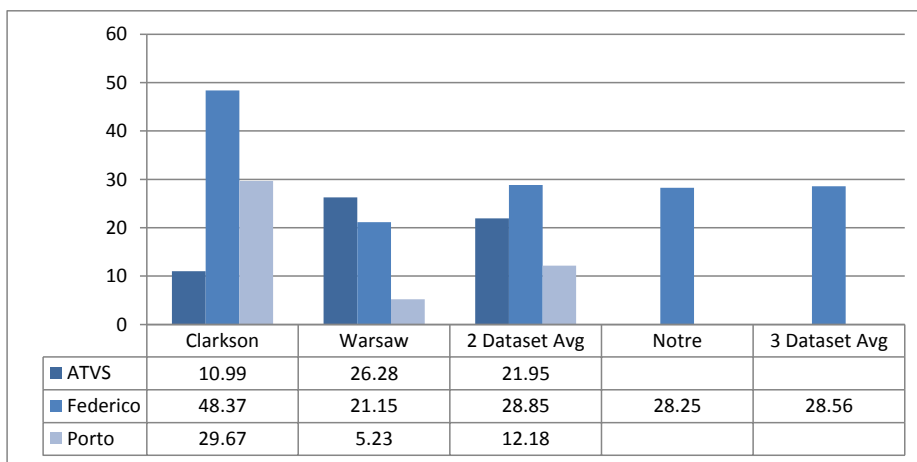


Figure 28 Rate of misclassified live iris images for submitted algorithms¹²⁴

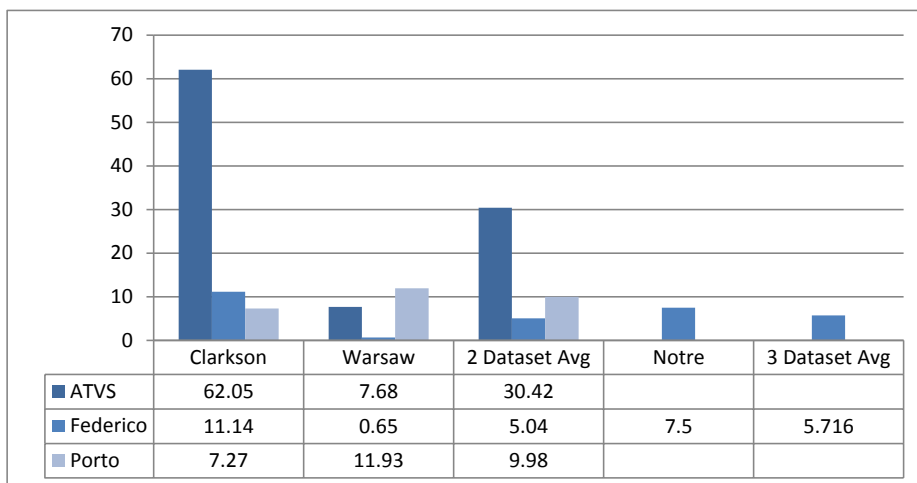


Figure 29 Rate of misclassified spoof iris images for submitted algorithms

¹²⁴ Source: LivDet 2013 Iris Liveness Detection Competition 2013.

Table 52 Rate of misclassified live fingerprints (*ferrlive*) for submitted algorithms¹²⁵

	Biometrika	Italdata	Crossmatch	Swipe	Average
Dermalog	3.30	0.50	99.84	3.82	26.86
Anonym1	1.50	0.50	86.96	N.A.	N.A.
ATVS	4.60	0.00	90.40	0.00	23.75
Anonym2	2.30	0.20	98.40	2.52	25.85
UniNap1	30	2.10	31.28	11.45	11.96
UniNap2	1.80	5.00	55.20	33.22	23.80
UniNap3	1.80	2.10	55.20	11.45	17.64
Anonym3	3.30	1.00	95.52	2.69	25.63
HZ-JLW	65.30	26.10	100.00	25.33	54.18
Itautec	1.10	1.30	64.96	N.A.	N.A.
CAoS	5.50	21.10	41.92	N.A.	N.A.

Table 53 Rate of misclassified fake fingerprints (*ferrfake*) for submitted algorithms¹²⁶

	Biometrika	Italdata	Crossmatch	Swipe	Average
Dermalog	0.10	1.10	0.00	3.20	1.1
Anonym1	2.40	1.70	2.40	N.A.	N.A.
ATVS	5.50	100.00	10.30	100.00	53.95
Anonym2	1.30	1.00	0.30	9.60	3.05
UniNap1	6.40	4.90	31.10	16.10	14.62
UniNap2	11.30	13.90	48.30	19.50	23.25
UniNap3	11.30	4.90	48.30	16.10	20.15
Anonym3	8.10	4.60	0.10	8.20	5.25
HZ-JLW	0.60	0.20	0.00	3.50	1.07
Itautec	16.90	6.50	13.90	N.A.	N.A.
CAoS	3.70	70.70	54.20	N.A.	N.A.

Table 54 Rate of accuracy for submitted algorithms¹²⁷

	Biometrika	Italdata	Crossmatch	Swipe	Average
Dermalog	98.30%	99.20%	44.53%	96.47%	84.63%
Anonym1	98.00%	98.85%	50.53%	N.A.	N.A.
ATVS	94.95%	50.00%	45.20%	53.55%	60.93%
Anonym2	98.20%	99.40%	45.20%	94.19%	84.25%
UniNap1	95.30%	96.50%	68.80%	85.93%	86.63%
UniNap2	93.45%	90.55%	47.87%	73.15%	76.26%
UniNap3	93.45%	96.50%	47.87%	85.93%	80.94%
Anonym3	94.30%	97.20%	46.89%	94.75%	83.29%
HZ-JLW	67.05%	86.85%	44.44%	84.81%	70.79%
Itautec	91.00%	96.10%	57.73%	N.A.	N.A.
CAoS	95.40%	54.10%	52.62%	N.A.	N.A.

¹²⁵ Source: 'LivDet 2013 Fingerprint Liveness Detection Competition 2013'-report.¹²⁶ Ibid.¹²⁷ Ibid.

For the Dermalog and Morpho systems:

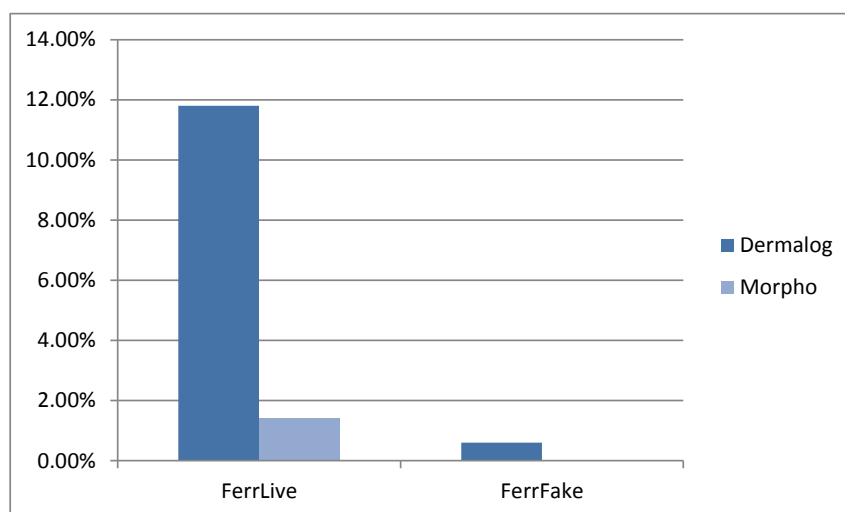


Figure 30 FerrLive and FerrFake for submitted systems - Dermalog and Morpho¹²⁸

Results with systems were, perhaps unsurprisingly, better. It can be observed in the figure above that the Morpho system had a ferrfake rate of 0% at a ferrlive rate of less than 2%.

Finally, regarding the spoofing of facial image comparison systems, typical approaches involve the presentation of a falsified face either as a printed photograph or as a video on a screen or using some form of mask, make-up or cosmetic surgery. Three main categories of counter-spoofing measures can be identified:

- Motion analysis, typically based on the difference between motions in planar objects and real human 3D faces. Presentation attack detection is possible at a HTER of 9% (Anjos, 2011);
- Texture analysis, which can be accomplished using various image analysis techniques, including frequency component analyse or use of local binary patterns. The former has been reported to be up to 100% effective in some datasets (Li, 2004) while HTER rates of approximately 15% have been reported with the use of algorithms based on the latter (Trefny 2010);
- Classic liveness detection based on searches for classic signs of 'life', such as eye blinking or lip movements or use of embedded sensors to measure temperature, for example. Although apparently simple, they have applicability and given the right conditions and dataset, can be extremely effective, as reported by Pan (2007) who described use of blinking analyses in a system with 96% accuracy in presentation attack detection. The use of embedded sensors has received renewed attention in recent years, as highlighted by the 2015 release by the Idiap Research Institute of the MSspoof database¹²⁹ of multi-spectral facial image for algorithm development and testing. In a similar vein, MODI have developed anti-spoofing measures based on the use of Near Infrared (NIR) cameras alongside those using visual light in the frame of the FastPass project¹³⁰ and reported 100% detection rates with iPads and iPhones and 97% rates for the detection of images on paper. According to reports, the methods can be executed while the subject is in motion except when detection of masks is sought, in which case the subject has to stand still for a minimum of 5 seconds.

Data with which to compare counter-spoofing measures with those available for other modalities is available from the '2nd Competition on Counter Measures to 2D Face Spoofing Attacks', 2013. [SEC2DFACE] In the competition, participants submitted to test their algorithms against a consisting of short video recordings of both real-access and

¹²⁹ <https://www.idiap.ch/dataset/msspoof>.

¹³⁰ For further details please see www.fastpass-project.eu.

attack attempts to 50 different identities. Three types of attacks were analysed: printed photographs, photographs displayed on the screen of a device and videos replayed on the screen of a device. Participants were provided a training set upon which to tailor their algorithm before submitting it to be applied to an 'unseen' test set. Ranking of submitted algorithms was based on HTER values that are depicted in the table below.

Table 55 Performance results for the proposed anti-spoofing algorithms (in %)¹³¹

Team	Development			Test		
	FAR	FRR	HTER	FAR	FRR	HTER
CASIA	0.00	0.00	0.00	0.00	0.00	0.00
IGD	5.00	8.33	6.67	17.00	1.25	9.13
MaskDown	1.00	0.00	0.50	0.00	5.00	2.50
LNMIIT	0.00	0.00	0.00	0.00	0.00	0.00
MUVIS	0.00	0.00	0.00	0.00	2.50	1.25
PRA Lab	0.00	0.00	0.00	0.00	2.50	1.25
ATVS	1.67	0.00	0.83	2.75	21.25	12.00
Unicamp	13.00	6.67	9.83	12.50	18.75	15.62

Putting all of the above into context, the attempt is made to compare the three modalities at once.

It may be noted that comparisons of modalities in terms of actual performance are readily available. The UK CESG undertook a comprehensive analysis of seven biometric systems in 2000, for example. [CESG01] The results are shown in the graph below, which highlights the fact that the iris was the highest performing modality at this time. This is of some relevance to the discussion on spoofing as the introduction of counter-spoofing measures may impact the performance rates negatively (in fact, the introduction of anti-spoofing measures introduces a second binary decision into the biometric system - the system must first decide on whether a sample is a spoof or not, before deciding if it is above a certain threshold for enrolment or verification. The introduction of the first decision can only negatively impact on the overall accuracy of the system performance, with the ideal anti-spoofing measures minimising this effect while maximising the accuracy in terms of spoof detection).

More recently, based on the results from the FRVT/ICE competition of 2006, iris and face biometrics were shown to have comparable levels of performance, as per the graph below which shows FRR values at an FAR of 0.001.

¹³¹ Source: 'Second Competition on Counter Measures to 2D Face Spoofing Attacks 2013'.

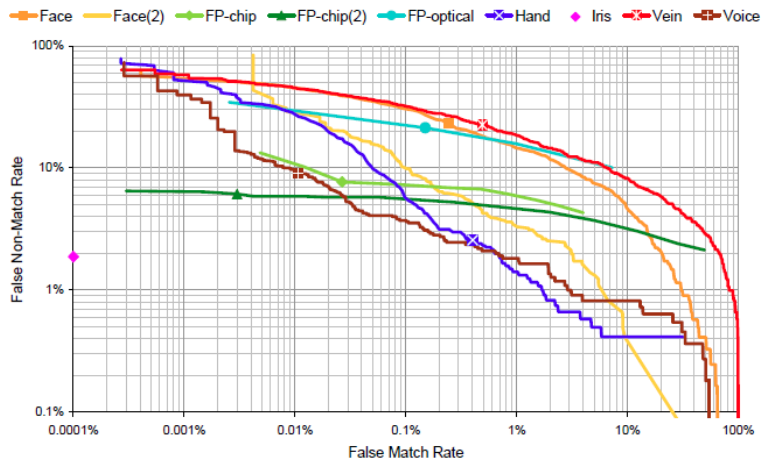


Figure 31 Performance of biometric systems

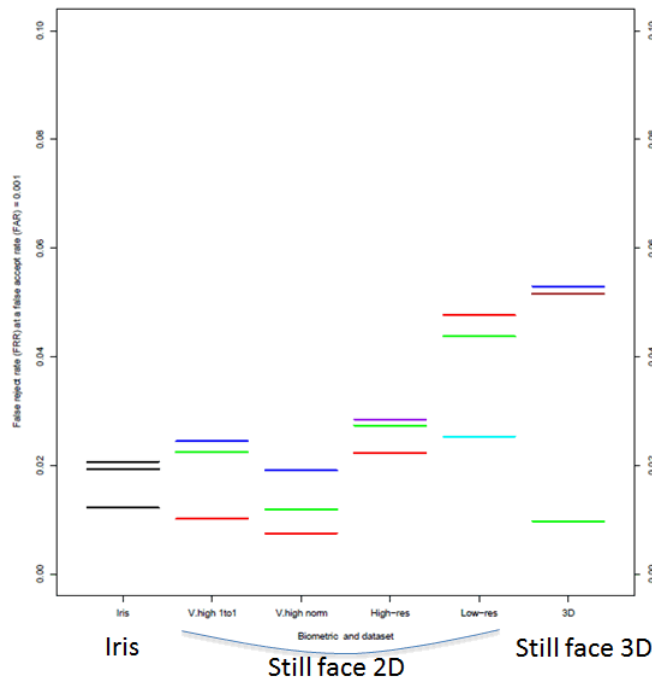


Figure 32 Performance of biometric and dataset¹³²

In order to compare counter-spoofing performance, ferrfake rates (misclassified false acceptance) are compiled from the afore-mentioned studies in the table below.

¹³² Source: FRVT 2006 and ICE 2006 Large-Scale Results - March 2007 – fig 10 p. 26 Graph shows FRR values at a FAR of 0.001; the different colours indicate the different algorithms.
 Columns are as follows: (1): median FRR for 3 evaluated iris algorithms; (2): FRR for the top 3 one-to-one still face recognition algorithms; (3): FRR for the top 3 normalised still face recognition algorithms; (4): FRR for normalised algorithms on the high-resolution and (5) low-resolution datasets; (6): FRR for normalised 3D face recognition algorithms.

Table 56 Comparison of counter-spoofing effectiveness

Iris (Livedet 2013)	FP (Livedet 2013)	FI (SEC2DFACE)
0.65% to 62.05%	1.07% to 53.95% across the individual algorithms	0.0% to 17.0% across the individual algorithms on 2D spoofing attacks
Average: 5.04%, 9.98% and 30.42% across two datasets	0% and 0.6% for systems	
Average: 5.7% across three datasets (the Federico algorithm was the only one evaluated over the three datasets)		

3.5.3 Post-analyses

The above analyses highlight that information from various sources on approaches to spoofing of different biometric modalities varies in type and nature and although a number of counter-measures have been developed, many of them are tailored to addressing one or a few of the attack vectors possible rather than being comprehensive alone. This, aligned to the fact that performance tests are non-standardised and output results on different scales and targeting different types of databases of attacks, makes absolute judgement on the relative vulnerability of the iris to spoofing difficult.

One addition to the analysis should be the inclusion of the relevance of certain attack vectors in border control environments. As already mentioned, drastic measures such as surgical interventions are not particularly relevant. It may be suggested that in supervised environments, approaches based on presentation of 2-dimensional printouts or videos playing on phone or tablet devices are very unlikely to pass unnoticed. Data presented above suggests that such approaches, meanwhile, are typically very well detected for all biometrics - in the case of facial image matching, the results from (SEC2DFACE) are impressive, as are those against the Warsaw dataset in the LivDet 2013 study. Thus, even in unsupervised environments, vulnerabilities can be minimised given deployment of state-of-the-art algorithms at the software level. It would appear that vulnerabilities remain in more sophisticated cases - the use of contact lenses in the case of iris, for example. Evidence is scarce regarding whether such attacks can be well detected by trained border guards, and this would perhaps be worthwhile to investigate further.

In any case, it is clear that evidence is currently too scant to answer the question posed at the outset completely. In order to provide final opinions on the matter, a number of experts were consulted from the Biometrics Institute Biometrics Vulnerability Assessment Expert Group (BVAEG). A questionnaire was disseminated to the experts in online format and a number of questions posed in order to ascertain whether all sources of information had been analysed as well as to check their opinions on the main question at hand. Experts were unanimous in their opinion that the iris was either equally or less prone to spoofing than other modalities. In fact, 66% of those surveyed considered it to be generally less prone. This was also felt to be true in the case of pure software-based measures and in both monitored and self-service environments. Taken alongside the literature reviews undertaken and the analysis of the results, the opinions would appear sensible although not necessarily fully defensible with formidable evidence. Nevertheless, the overall viewpoint would appear to be that in all situations that might be considered in the Smart Borders pilot based on the operational tests undertaken, the iris is a potential biometric of use and spoofing should be of no more significant concern in the case of iris deployments than for other modalities.

3.6 Reading chips in e-passports, extraction of the facial image for use and execution of passive authentication

3.6.1 Introduction

In recent years, the issuance of electronic passports (e-passports), or more generally, electronic machine readable travel documents (eMRTDs) in which certain biographic and biometric information is contained in a machine-readable electronic chip embedded into the document has become standard in a majority of countries across the world. Work on the issuance of machine-readable travel documents goes back to at least 1968 when ICAO created a Panel on Passport Cards¹³³ while specifications for a document containing an embedded Integrated Circuit chip were first published in the 1990s¹³⁴, highlighting the fact that both document issuance authorities and end users have extensive experience in this regard. As per standard 3.10.1 of Annex 9 to the Chicago Convention, all non-machine readable passports issued by ICAO Member States should be out of circulation by 24 November 2015. Based on data provided by Germany, 112 of 200 countries whose travellers crossed their borders in the period from January to May 2015 carried e-passports.

The use of machine-readable and particularly e-passports for border control brings a number of benefits. From a security perspective, a border guard or inspector can use the information derived from the chip to validate that present on the biographic page, the former having more advanced electronic security features that are more resistant to tampering or modification. As an example, the photograph stored on the electronic chip can be extracted and compared against that on the data page and to the person presenting the document in order to verify the holder and protect against photograph substitution simultaneously. The use of e-passports also brings potential for process automation, as information required to facilitate border crossing can be extracted by machine. Furthermore, bearer verification can be accomplished using automated facial recognition algorithms, comparing document photos against those captured live by camera at the point of interaction.

Within the Smart Borders proposals, capabilities to properly make use of e-passports at all borders will be important if the system is to function optimally and if the possibilities to facilitate travel using automation can be fully realised. The Smart Borders study proposed the use of the facial image as a biometric characteristic in the system(s), a proposal predicated in part on the fact that the facial image is stored in e-passports and therefore can be used for document bearer verification both manually and automatically. Indeed, the study concluded that the facial image from the electronic chip of e-passports was more suitable for automated facial recognition than a scanned copy of the photo from the data page of the document, emphasising the importance of e-passport capabilities in the decision-making process around the systems to date. It is therefore important that the facial image can be reliably extracted from the chip in different conditions and at different borders and that equipment for such reliable extraction of data is fully available at all required locations. Additionally, the afore-mentioned advanced electronic security features must be reliably assessed, particularly in the proposed cases of automation where visible security features on the paper document are not being scrutinised by a border guard or other trained person. Foremost amongst such features is Passive Authentication, a standard feature defined by ICAO in their Document 9303 Volume 2 standard that allows confirmation that the document is issued and signed by a valid issuance authority as well as detecting modification of passport chip data. Finally, given that Smart Borders seeks facilitation of travel and insofar as possible expedited processing of traveller processing at border control points, the optimal incorporation of document reading processes into the overall border control process should be assessed and the time required to add

¹³³ <http://www.icao.int/Security/mrtd/Pages/MRTDHistory.aspx>.

¹³⁴ Machine Readable Travel Documents (MRTDs): History, Interoperability and Implementation. ICAO, March 23 2007.

chip reading and authentication processes to document reading fully considered. This section therefore attempts to provide relevant information on the following questions:

- What are, technically and operationally, the most common and/or important conditions that affect the reading of the facial image from eMRTDs?
- What are the minimum standards for equipment for reading the eMRTD chip at each type of border?
- What does Passive Authentication add to the complexity of infrastructural and IT set-ups at locations where e-documents will be presented and checked?
- Can the chip be read while the live facial image is being taken?

The questions are considered based on information gleaned from literature review, expert consultations and operational experiences within and outside of the Smart Borders pilot.

3.6.2 A basic introduction to eMRTDs and reading the electronic chip of travel documents

In this section, some basic information regarding the integrated circuit chip embedded in eMRTDs and the extraction of data thereof is provided. Literature providing a more in-depth description of these topics is listed in the bibliography.

An integrated circuit chip embedded in a document is read using an appropriate Inspection System (IS) that emits a radio-frequency field that imparts energy to the chip itself to allow data extraction from the chip itself. Through exchange of commands between the chip and IS, the chip should become ready for data transmission. The data in the chip is stored according to a standardised Logical Data Structure (LDS) defined by ICAO Document 9303 and each Data Group (DG) of this LDS is read in turn by the IS including DG2 which contains the facial image data. The LDS is highlighted in figure 1 below. Mandatory and optional data elements are highlighted in the appendix.

Basic access control (BAC) is a security measure intended to ensure that the reader (i.e. the border guard or the appropriate machine in case of self-service processes) has physical access to the document (i.e. to prevent skimming) in which the chip being read is embedded and to prevent eavesdropping. Although an optional security measure (in the EU, it is mandatory, but some countries such as Nigeria are known not to implement it), it is commonly implemented in modern eMRTDs. It is based on the derivation of cryptographic keys from the visual machine readable zone (MRZ) present on the data page of the document that are used for mutual authentication between the IS and chip. This creates a secure messaging pathway between the IS and chip for further data transmission. Without access to the MRZ, it is impossible to read the information from the chip once BAC is implemented. Supplementary access control (SAC) has been introduced recently as an improvement on BAC although it targets the same security goals.

Passive authentication is mandatory for document issuance in ICAO Member Countries and provides assurance on document issuance and checks for malicious chip data modification as noted above. PA uses a digital signature to authenticate data stored in the data groups on the MRTD chip.¹³⁵ This signature is generated by a Document Signer (e.g. the MRTD producer) in the personalisation phase of the MRTD chip over a Document Security Object containing the hash values of all data groups stored on the chip. For details on the Document Security Object, Document Signers, and Country Signing CAs the reader is referred to [2].

To verify data stored on an MRTD chip using Passive Authentication the terminal has to perform the following steps:

1. Read the Document Security Object from the MRTD chip;
2. Retrieve the corresponding Document Signer Certificate, the trusted Country Signing CA Certificate, and the corresponding Certificate Revocation List;

¹³⁵ BSI, Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token.

3. Verify the Document Signer Certificate and the signature of the Document Security Object;
4. Compute hash values of read data groups and compare them to the hash values in the Document Security Object.

Passive Authentication enables a terminal to detect manipulated data groups, but it does not prevent cloning of MRTD chips, *i.e.* copying the complete data stored on one MRTD chip to another MRTD chip.

The protocol is elaborated further in (FTXBPGABCT).

Note that other security procedures are also commonly implemented, including active authentication (AA) and extended access control (EAC). However, these are not associated with the actual reading of the chip contents itself and therefore are not discussed further herein.

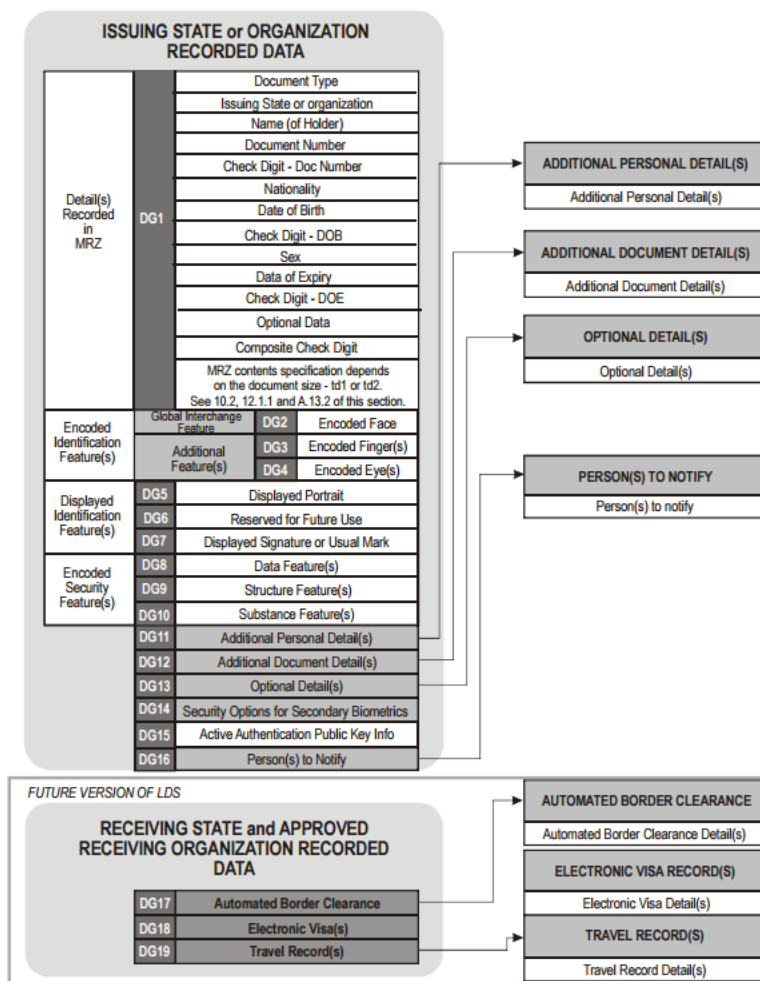


Figure III-2. Data group reference numbers assigned to LDS

Figure 33¹³⁶ Data group reference numbers assigned to LDS

Reading the facial image from the chip: impacting conditions and possible solutions

Given the above information, some possible conditions or circumstances can be identified that would interfere with the possibility to read a facial image from the eMRTD using standard procedures. The list of conditions identified have been developed and finalised in consultation with Member State experts. Operational data is provided as evidence to highlight the relevancy of the identified circumstances at border control points and similar environments

¹³⁶ Source: ICAO, Machine Readable Travel Documents, Part 3 Machine Readable Official Travel Documents.

where possible. Solutions to obviate, overcome or at least reduce the impact of some of these conditions are also proposed.

Issues with the chip of the document itself

- If the chip, antenna or the link between the chip and antenna is broken or defective, then clearly chip reading will not be possible. When considering chips embedded in travel documents, it must be remembered that holders will not necessarily treat their documents with equal care. By their very nature, such documents will be carried, sometimes bent or exposed to different negative environmental influences (e.g. application of overvoltage);
- The embedded chip itself may not comply with the required ISO standards, meaning that typically the initialisation of the reading process mentioned above will fail. Specifications have been defined by ICAO, that refer to ISO standards ([ICAO9303P3V2] and [ICAO9303SUP]). Subsequently reading the FI from the chip will not be possible. In operational testing within the pilot, it was observed that some non-compliant passports were presented at different BCPs from countries including Brazil, Malaysia, China, and Russia. Issues encountered in testing included problems with DG2 encoding, inconsistencies between the visual and electronic Machine Readable Zone (MRZ) leading to rejection of the eMRTD, use of incorrect Object Identifiers for the `IdsSecurityObject`, leading to PA failure (as per [FTXOTEP], section 2.5.6.1) and a lack of conformity in implementation of security safeguards (as per [FTXOTEP], section 4.3.2). Some 40 of almost 3000 documents processing records made at Arlanda airport within the pilot, including successful and unsuccessful reads, were associated with an inability to read the facial jpeg (data item 19) from DG2, possibly because of encoding issues, for example;
- Instances of broken cryptography have been noted as a particularly common case in which a lack of compliance with the relevant standards is observed. As for the case above, full and complete authentication of the document will not be possible in such instances and depending on the process implementation, this may lead to an inability to extract information of relevance.

Issues with the inspection system

- It is also possible that the IS would not comply with the required ISO standards;
- Both OCR and keyboard entry may fail. For those eMRTDs that implement BAC, the reading will then fail. In tests at Arlanda airport within the Smart Borders pilot, it was noted that approximately 40% of reading failures were associated with failure of BAC, typically associated with failed OCR. In fact that bulk of BAC errors failed with the reading of DGo, the EF.European Commission presence map, implying a failure at the very beginning of the BAC and therefore MRZ reading errors.

Issues with the reading process itself

- One possible issue could be the presence of multiple chips within the field emitted by the IS. If multiple chips respond and the anti-collision fails, it will not be possible to initialise communication with the chip (and subsequently read the FI from the chip).

Failures with authentication of the chip and/or its contents

Note that as mentioned above, such errors do not inherently prevent reading of the eMRTD and the facial image from DG2. However, they are required if full confidence is to be had in the output of the reading process. Furthermore, depending on process implementation, it may be the case that the reading fails in case that such authentication fails.

- Passive Authentication failure may lead to overall process issues. This can occur if the Document Signer's Public Key is unavailable. Typically, this key should be obtained in a certificate from the ICAO PKD and stored in the IS. Alternatively, it can be provided on the chip in the document itself, although in such instances it is recommended that the key is validated by an external source, either the ICAO PKD (or similar) or through use of the CSCA public key that has been used to sign the DS. The verification of the integrity of the Elementary Files (EF), which

constitute the individual files within the chip file system, will fail if either or both of these certificates are not available, or are revoked. In operational tests within the pilot, the success of PA varied depending on the certificates made available to vendors implementing the test systems. At Arlanda and Lisbon airports, PA was successful in 78% of cases, for example.

Based on information provided by Frontex, the Dutch Department of Justice and Germany, common issues associated with PA include:

- The use of expired certificates to sign documents;
- Errors in the encoding of the various data elements of the eMRTDs Logical Data Structure (LDS);
- New passports reaching their borders before the certificate does. It was noted that this issue, largely operational and administrative in nature rather than technical, occurs even with European passports. Looking globally, it was reported that only 4 countries regularly upload their certificates into the ICAO PKD, explaining much of this time lag.
- For eMRTDs that implement Active Authentication¹³⁷ (AA), failure of AA execution may be taken into consideration by the IS when processing information from the eMRTD such as FI. This may lead to unavailability/rejection of the FI.

The steps required for successful reading of the facial image from DG2 and issues that may be associated with each step are given in fuller detail in the table below:

Table 57 Steps for reading of the facial image from DG2

Step#	What	Possible reasons for failing to read the FI from the chip
1	Initialisation between chip and reader. Summary as per ISO/IEC 14443-3 Type A/B.	
1.1	eMRTD with embedded and personalised chip is moved into the field emitted by the ISO/IEC 14443 compatible reader (part of the Inspection System)	
1.2	Once the chip has harvested enough energy, its operating state is IDLE, in which it will only respond to REQA (request type A) or WUPA (wake-up type A, to wake-up from a previous HALT command) commands from the reader.	If chip and/or reader do not comply with the required ISO standards, the initialisation will fail. Subsequently reading the FI from the chip will not be possible. The same holds in case the chip, the antenna or the link between chip and antenna are defect.
1.3	Upon recognition of such a REQA or WUPA command, the operating state of the chip changes to READY and the chip sends an ATQA response to the reader.	
1.4	Upon reception of the ATQA response from the chip, the reader starts the anti-collision management sequence and sends a SELECT command to the reader to obtain the UID (Unique Identifier) from the chip	

¹³⁷ Active Authentication is available on eMRTDs that have their individual cryptographic key pair per chip. The public key will be made available in a certificate. AA involves using the chip's private key to transform an IS generated challenge into a response which can be verified by the matching and certified public key.

Step#	What	Possible reasons for failing to read the FI from the chip
1.5	Upon reception from the UID, the reader issues a SELECT command including the UID, to which the chip answers with a SAK (Select Acknowledge) response.	
1.6	In case of collision detection, the reader issues ANTICOLLISION commands to resolve the collision	If multiple chips respond and the anti-collision fails, it will not be possible to initialise communication with the chip (and subsequently read the FI from the chip).
1.7	Once the chip receives the appropriate SELECT command and any collisions are resolved, the chip changes its state to READY	
2	Activation of the communication between chip and reader conformant to ISO/IEC 14443-4 and ISO/IEC 7816-4 In the READY state, communication between chip and reader is done in a manner conformant to ISO/IEC 14443-4. Higher protocol level commands will now be processed by the chip as per ISO/IEC 7816-4	
2.1	Activation of the link and negotiation of frame size, bitrate, waiting time etc. The terminal sends a Request for Answer to Select (RATS) command	
2.2	The chip answers with an Answer to Select (ATS) response The negotiation yields a 4 layer communication model (physical, data link, session and application layer).	
2.3	Between chip and reader, Application Protocol Data Units (APDUs) conform to ISO7816-4 are now exchanged. The ICAO eMRTD issuing State Application is selected.	
2.4	The Elementary Files (EFs) of the required Data Groups (DGs) are read from the LDS. This is done using SELECT and READ BINARY commands. First EF.European Commission is read, whose tag list contains the DGs (stored in their EFs) that are available. ¹³⁸ Each EF is then read out to obtain the DG. The MRZ is normally the first EF read.	

¹³⁸ Addressing files using EF. European Commission may introduce risk depending on the DGs being read and authentication protocols implemented as EF.European Commission is not hashed and therefore not verified during passive authentication. With eMRTDs using ICAO LDS version 1.8 (introduced recently in ICAO Document 9303 version 7, part 10, although most eMRTDs in circulation use LDS version 1.7), the necessary information can be read from EF.SOD which is more secure.

Step#	What	Possible reasons for failing to read the FI from the chip
3	<p>Passive Authentication</p> <p>EF.SOD is read to allow the verification of the integrity of the EFs read.</p> <p>The IS verifies this integrity.</p> <p>Specified in [ICAO9303P3V2] Section 7 Specifications, Subsection 7.2 Inspection.</p> <p>Elaborated in [FTXBPGABCT].</p>	<p>For the IS to execute PA, the Document Signer's Public Key is required.</p> <p>This key should be obtained in a certificate from the PKD and stored in the IS. In case it is provided in the chip, the certificate may also be read from there.</p> <p>The IS should verify the certificate containing the DS Public Key using the Issuing State's Country Signing CA Public Key from a corresponding certificate unless the DS itself read from the document is validated using an external source.</p> <p>The verification of the integrity of the EFs will fail if the required certificates are not available or are revoked.</p>
4	<p>Further authentication</p> <p>Further processing is dependent upon the design of the IS application and the capabilities of the document, and may involve:</p> <ul style="list-style-type: none"> • BAC (optional) • AA (optional) • EAC (optional) • Decryption of additional biometrics (optional) <p>This optional processing involves ISO/IEC 7816-4:</p> <ul style="list-style-type: none"> • EXTERNAL AUTHENTICATE • INTERNAL AUTHENTICATE • GET CHALLENGE 	<p>Depending on process implementations, failure of any of these implemented authentication steps that may be designated as required within that process will result in failure to extract the facial image information from the chip.</p>
4.1	BAC (Basic Access Control) - optional	
4.1.1	<p>IS reads MRZ optically and uses SHA-1 to derive the BAC keys.</p> <p>IS' MRZ reader might fail (in which case data entry might be done via keyboard if this is available, and supported by the IS application)</p>	<p>Both OCR and keyboard entry may fail. For those eMRTDs that implement BAC, the reading will then fail.</p>
4.1.2	The IS and chip mutually authenticate and derive session keys.	
4.1.3	After successful authentication, secure messaging is available between IS and chip.	
4.2	AA (Active Authentication) - optional	
4.2.1	<p>AA consists of a challenge-response between reader and chip using a chip-specific public key pair.</p> <p>AA must be preceded by PA.</p> <p>The PA ensures that the chip's public key for AA is authentic and unchanged. The challenge-response protocol will ensure the chip is genuine and matches the data page.</p>	<p>For eMRTDs that implement AA, failure of a successful AA execution may be taken into consideration by the IS when processing information from the eMRTD such as FI. This may lead to unavailability/rejection of the FI</p>

Step#	What	Possible reasons for failing to read the FI from the chip
4.3.	EAC (Extended Access Control) - optional	
	This depends on the issuing State's internal specification or on the bilateral specifications between cooperating States. This is not relevant for reading the FI.	
4.4	Decryption	
	This depends on the issuing State's internal specification or on the bilateral specifications between cooperating States. This is not relevant for reading the FI.	

Finally, some possible solutions or approaches to addressing the enumerated issues are proposed.

When it comes to defective or damaged chips, one possible approach might be to invite travellers to pre-check their eMRTDs using something test readers at municipalities or other suitable locations or alternatively an app on RFID/NFC-enabled smartphones or tablets. This approach, while technically feasible, founders somewhat on the fact that eMRTDs with damaged or defective chips are legally valid documents; thus, even if found to be defective, there would be no obligation on the traveller to seek a replacement. Furthermore, it was indicated by some European Member State experts that a damaged RFID chip would not typically seen as sufficient reason to apply for a new document by national administrations. Thus, without necessity or indeed massive motivation on the part of the traveller, the use of such test applications or devices would be seen as unlikely given the current state of affairs. When considering defective chips, the possibility of intentional or malicious chip disabling must be accounted for. The issue with accepting documents with invalid chips as valid and thereby offering the possibility of passing through border controls with a document in which the electronic chip has been purposefully disabled has been described in the literature^{139, 140} Without wishing to make any judgement on the merit of stringent checks on any specific subset of travellers, it may be stated that one possible approach to dealing with this discussed during preparations of this document involved second line inspection of all documents in which the chip was present but found to be defective. Such an approach would also be possible in cases of broken cryptography alluded to above.

As regards non-compliance of documents and/or Inspection Systems, one possible solution deemed very appropriate in discussions on the topic was establishment of conformity assessment by either a central (e.g. European, ICAO) authority or a MS recognised CAB (Conformity Assessment Body). It was noted during research efforts that mandatory conformance testing is not defined or imposed. Frontex published various 'best practice guidance' documents of some relevance. However, they are not a substitute for a conformity testing methodology, and an obligation/recommendation to apply it. The CAB would need to be generally accepted by document issuance and document check bodies and utilise standardised procedures for certification of both eMRTDs and inspection systems and conformance subsequently enforced. In this regard, it was noted that Common Criteria protection profiles already exist in this field, including BSI-CC-PP-0055 (for BAC), BSI-CC-PP-0056 (for EAC) and BSI-CC-PP-0068-V2-2011 (for SAC), providing a starting point for efforts in this direction. Document BSI TR-03105 Part 5 also deals with testing for ICAO compliance for full inspection systems. Enforcement of conformance according to documents such

¹³⁹ (FTXOTEP), section 2.5.4

¹⁴⁰ ICAO Doc 9303 part 1 volume 2 section IV paragraph 2.6 [3]: "Since e-passports with a non-functioning chip are still valid, disabling the chip may be a way to make falsification easier, not placing a chip makes counterfeit easier "

as those mentioned would address some of the issues seen that may arise due to issues with the document and/or inspection system shortcomings.

Another possible approach to dealing with non-compliance at the document level involves consistent use of defect lists. In discussions on the topic, it was noted that the German authorities are already making use of such lists that define known issues with documents coming from a certain country or issuer or belonging to a certain batch. In cases where such defects are known and understood, it may be possible to implement variable processing methods to extract necessary information from the eMRTD in order to proceed with border checks. Communication of defect lists between countries could be encouraged both to allow expansion of the lists to be more comprehensive, to provide assurance on defects encountered (due to their being identified more frequently and in different locations) and in order to better standardise checks at different locations.

In relation to authentication failures leading to issues with facial image extraction from eMRTDs, only PA failure is dealt with in this section. The most common cause of PA failure is the unavailability of certificates, either DS or CS certificates, to the Inspection System. Although the German masterlist has been developed for a number of years now, it only contains the certificates from 63 of 200 countries whose travellers cross German borders per year, of which only 31 (of 80 issuing e-passports) are third countries. Germany report that 97% of e-passports of countries for which the appropriate CSCA certificate is on their masterlist are successfully verifiable. Another related issue can be lack of access to up-to-date revocation information, available as a certificate revocation list or otherwise. In either case, improvements must be addressed though insistence on regular PKI good practice throughout the chain of certificate maintenance, distribution and update document issuance and document checking. At the very minimum, the following aspects must be considered:

- Key generation needs to be controlled;
- A certificate creation procedure needs to be put in place between the DS and the CSCA;
- The CSCA and DSCA need to make up-to-date revocation information available (CRL or OCSP¹⁴¹);
- Exchange (bilateral or central approach) of certificates;
- Validation of received certificates by the relying party (or parties);
- Distribution of certificates and CRL/OCSP information to the Inspection System;
- Use of the appropriate certificates and up-to-date revocation information in the IS when performing the PA.

A useful approach to certificate dissemination is the creation and use of master-lists of certifications. This pools responsibility for the tasks of assembling and validating public key certificates with one or a small number of entities that make their validated list(s) available for others. Clearly, trust in the master-list publisher is an important element in such a process. In any case, the master-list approach has already been employed in the field of border control in Europe, with Germany, Spain, Hungary and Switzerland all maintaining their own CSCA master-lists and making them available publically. Recently, the European Commission has proposed the creation of a Schengen master-list of CSCA certificates that would lead to establishment of a similar, hopefully comprehensive and highly-trusted, list of CSCA certificates at the European level.¹⁴²

Alongside instigation of such technical measures in order to make certificates available for use, one should also consider the organisational aspects of work required. The foregoing points, particularly the observation that certificates are being disseminated slowly and irregularly, highlights the fact that currently there is a lack of mature procedures and harmonisation in work processes between different European Member States and other stakeholders. Such harmonisation is desirable not only to provide horizontal improvements in the status quo when it comes to eMRTD authentication but also to ensure consistent document verification processes as an important

¹⁴¹ On-line Certificate Status Protocol (OCSP), the de facto mechanism in today's PKI to provide revocation information in an interactive way, as opposed to the original but non-interactive approach to use CRLs.

¹⁴² c.f. Meeting of the European Commission with Member State experts, eu-LISA and Frontex on 13/05 on a future Schengen CSCA Master List

component of border control processes in every country of the Schengen zone. Standardisation can serve to incentivise some of these important organisation improvements. As an example, minimal operating conditions of an IS could be formalised and a conformity assessment thereof could be defined. Inspection Systems could then be subjected to operational conformity assessment before being put into operation as described for documents above.

3.6.3 Minimum equipment standards for reading eMRTD chips at borders

The in-depth description of chip reading above identified the necessary communication that must take place between the Inspection System and the placed document in order for successful data reading and facial image extraction. Based on this description, some minimum standards can be identified for an IS in order for it to function to the required standards. Successful reading will, of course, also depend on full conformance of the issued document and its electronic components to the relevant standards.

As depicted in the diagram below, no matter the scenario under discussion, the eMRTD will have to be placed onto the document reader to initiate the protocol. The inspection system will include an RFID chip reader that is able to activate and read information from the chip; as per ICAO Document 9303 Part 1 Volume 2, read-only access is the default. The document itself will comply with ICAO Document 9303 as noted and the Inspection System should be capable of executing all defined protocols (PA, AA, BAC, SAC, etc.); EAC and PACE are optional approaches defined in BSI TR-03110. The RF link should comply with ISO/IEC standard 14443 while the communication between the chip and the reader will be as per ISO/IEC 7816-4. Although not standards, additional relevant documents from Frontex and the BSI are listed in the appendix.

Extracted information should be formatted appropriately and communicated in a defined manner with back-end national systems and furthermore, where applicable, onwards to other systems such as the VIS, SIS II, Eurodac or the proposed Smart Borders systems.

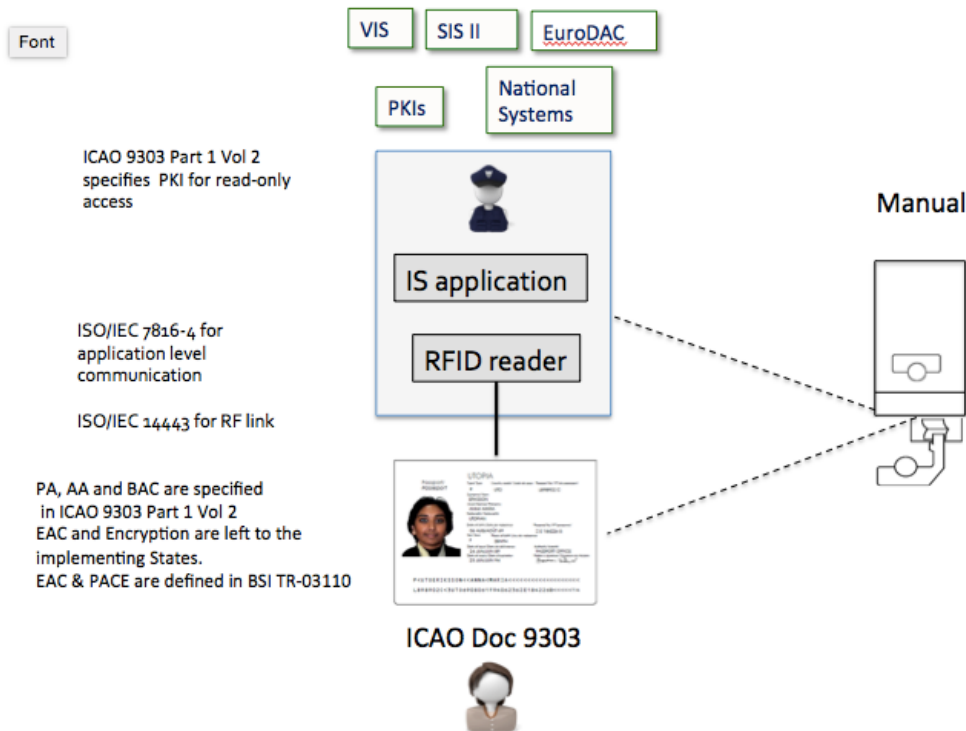


Figure 34 *Extracted information formatting and communication*

It is important to note that this is the minimum set-up that can be established for eMRTD reading in standard border control scenarios. Additions to these minimum requirements will not depend on border types *per se* but rather on specific conditions presenting at individual locations that will depend on the nature of that location and the border

control processes being implemented. For capture of information from the eMRTD in outdoor conditions, for example, equipment will have to be capable of accurately reading the MRZ in sunlight if BAC is to be consistently successful. This is typically possible using swipe readers (as seen in results from Kipoi Evrou in Greece within the pilot where such a reader was used to enrol biographic information in outdoor conditions), using full-page document readers with suitable covers to prevent interference from extraneous light or using uncovered full-page readers with the capability to adjust their reading sensitivity to outdoor light conditions (as used at Arlanda airport within the pilot, for example). Other specific location-dependent factors that might require additions to the above-stated minimum standards were not identified in the course of this research.

3.6.4 **Passive authentication - what does it add to the complexity of the set-up and the duration of the process?**

PA is described in detail above and analysis of the PA process highlights a number of requirements for successful execution of this important step in the overall document authentication procedure.

Successful interactions between the integrated circuit chip and the IS are obviously a first prerequisite. According to the 2014 [PRESSURV] survey (see APPENDIX A.1), some countries do not electronically read ePassports, obviously implying that PA is not executed. However, if it is the case that use of the facial image present on the eMRTD is mandated as part of a particular border control process or other requirements are introduced that mean that electronic document reading must be undertaken, then execution of PA adds no particular complexity at the level of establishing interactions between the chip and the IS and reading of the chip data.

As already mentioned, the greatest obstacle to successful PA is the availability of the necessary certificates - either a DS certificate to validate that stored on the chip itself (although this is not compulsory, it is normally the case) or a CSCA certificate public key to validate the signature of the DS. Complexity is certainly added if exchange of certificates and validation of the certificates received is to be pursued. This will require establishment of bilateral contacts with authorities in those countries from whom certificates are sought - not a straightforward process as it can be difficult to identify the appropriate authority and furthermore, despite the 'public' nature of these keys and the fact that there is nothing 'secret' about such keys, it can at times be difficult to convince some authorities in third countries of the security and/or the usefulness of such certificate provision. It will also require validation of these certificates, requiring technical knowledge on the part of the authority carrying out the certification and some method for out-of-band verification.

These steps are obviated for individual authorities if they make use of master-lists created by others. Within the operational tests undertaken within the pilot, this approach was seen to be convenient, with many supporting vendors making use of the CSCA certificates provided by European Member States in their master-lists without any notable difficulty and in the very short spaces of time available to set-up test equipment at various locations.

The main 'enforced' complexity, therefore, is associated with the appropriate distribution of certificates and CRL information to the Inspection System. This can typically be accomplished in one of two ways - either through update of certificates stored on all individual IS (this could be, for example, all systems at each border control point in a country) or through protocols in which certificate lists are stored centrally (perhaps a single list per country, per authority or per location) and accessed by the different IS during each document authentication process. The choice of which approach to follow will depend on individual preferences and the IT infrastructure implemented in any case. Within the pilot, certificates were generally stored in the individual devices whereas Germany has implemented a system in which certificates are stored, monitored and updated centrally. In either case, the complexity is not considered to be particularly high, particularly given the fact that a network-based interaction between all border-control IS with a centralised national system or point of control is necessary for other matters in any case. No experts involved in discussions on this topic considered that efforts to make certificates available to individual IS in their country would be particularly complex at the technical level.

The checks associated with PA do add to the duration of the document reading process and this particular aspect was assessed in the operational tests carried out. The precise duration of the PA process will vary depending on the technical implementation. Consultations with a certificate list present locally should be somewhat quicker than with a list located a central location, for example; in the latter case, network capabilities will make some difference. Successful execution of PA averaged at 73% across a variety of locations in which this information was collected, ranging between 62% and 99%. The highest figures were seen at Sculeni BCP where almost all travellers involved hailed from the Republic of Moldova. Hence, a limited number of certificates were required to execute PA at this location and all needed were available. In such instances, as already noted above, PA is almost always successful. Note that PA in this regard was taken to include all of the steps defined in the Frontex Best Practice Technical Guidelines for ABC, namely EF.SOD verification, DS certificate signature verification (including validity checks and checks on revocation status), comparison between EF.SOD and EF.European Commission and Data Group integrity checks. Germany have reported an average time for PA of 0.3 seconds in their operational systems across all TCN passports compared to a complete process time for data extraction and authentication of 3.9 seconds from placement of the document onto the reader until the end of the check. Across locations in which pilot tests were undertaken, an average time of 4.1 seconds was noted, indicating that aspects of testing associated with chip reading compare favourably with fully operational set-ups.

It should be noted that the quoted times generally do not equate to the time added to the border control process by executing PA. PA includes reading through the various DGs of the chip while calculating and comparing hash values, aspects of which are required if the chip is being read without any execution of PA. Furthermore, it is typical that some other parts of the border control process can be executed while the chip is being read and PA being executed. This could involve queries of databases using biographic information available from the data page, border guard questioning or biometric enrolment as just three examples. The latter case is examined further in the next section for the specific case of the enrolment of a live facial image.

3.6.5 Can the chip be read while the live facial image is being taken?

At the process level, enrolment of the live facial image to be compared against that obtained from the eMRTD appears to be one approach to accelerate the overall time to completion of bearer verification using automated facial recognition. By obtaining both facial images to be compared in parallel, they could be passed to the comparison software quickly. Thus, it is briefly considered whether the chip can be read and the facial image extracted from DG2 at the same time as the live facial image is being enrolled.

At the technical level, it should be noted that the two processes are essentially unrelated and use different technical equipment - a standard photo or video camera and a document reader with appropriate software. Thus, in this regard, there is certainly no reason that the two processes cannot be run simultaneously. The question must therefore be answered purely from the perspective of whether this is operationally possible. This assessment is made based on experiences in operational testing and analysis of some appropriate results.

Differentiation should be made between two alternative scenarios.

In the first, the border guard will accept the eMRTD presented by a traveller and place the document facedown onto a document reader within his/her workspace. It seems evident that while the chip is being read - a process that may take several seconds as noted previously - the guard could ask the traveller to look into a camera and the live photo be captured. In order for this to be possible, however, several aspects of the overall workflow would have to be designed to facilitate this:

1. The software for live image capture would have to run simultaneously to that for chip reading. If it is the case that the border guard activates the camera, then the interface for such activation would have to be available while the chip is being read - either in a separate window on the same screen, on a different screen or using some type of other shutter activation mechanism. A more likely approach would appear to be auto-capture of the facial image.

- This would require implementation of auto-focus capabilities or use of a light-field camera (a light-field camera has an array of lenses with different focal lengths which allow capture of in-focus images at different distances.);
2. In case of auto-capture, software for the automatic evaluation of the facial image quality and execution of re-enrolment in case of need would likely have to be deployed;
 3. Automatic adjustment of the camera height would be required to cope with travellers of different stature.

In pilot tests at various European BCPs, this process could not be assessed. Typically, software was configured such that live image enrolment took place subsequent to document reading. Furthermore, although auto-focus capabilities of cameras were used and generally found to be preferred (based on the border guard interviews carried out in various locations and reported elsewhere in this report, for example in Arlanda airport and Helsinki port), auto-capture and automatic height adjustment functionalities were not available at manual booths. This was generally related to the short time available to develop the equipment on the part of the vendors supporting the pilot enforced by the short project timescales rather than any specific inability on their part to develop, test and install such equipment given sufficient time and resources. Thus, it is suggested that with appropriate consideration, some overlap in document reading and photo capture processes should be possible.

One basis for this statement lies in experiences in the second scenario to be considered - automated passenger self-processing at either self-service kiosks or in automated border control (ABC) gates. In such cases, the passenger will place the document him-/herself and also submit to live photo capture processes without any direction. Passenger behaviour will be key to whether process parallelisation is feasible and it is clear that set-ups would have to be designed such that the camera would meet the gaze of the traveller as he/she places their document onto the reader. Continuous capture of photographs from travellers as a series of stills taken over time is already a default approach in some deployed ABC gates. Within the pilot, such an approach was applied at the ABC gates present in Schiphol airport and at Narva land BCP. Examination of data obtained at the former highlights that in many cases the sum of the times required for chip data reading and authentication, live image capture and image comparison was less than the overall time that the passenger spent in the gate. Obviously, image comparison could only proceed once live and chip images were available, implying some parallelisation of the chip-IS interaction with the live image capture. Thus, at least in instances when the passenger behaves appropriately, it is clear that the chip can be read while the live image is being taken in ABC gates.

Possibilities for parallelisation at manual booths should be clarified through further studies. However, it may be stated up front that there are some situations in which such process acceleration is likely to be difficult to implement. In particular, it is difficult to see how this could be accomplished with mobile devices where the camera must be held straight and upwards to capture the facial image.

Given all of the above, a final point to be made is whether parallelisation of live photo capture and document reading processes, albeit apparently desirable, would lead to significant benefits in terms of process duration. On the one hand, the time required for live capture in the pilot was often small - a median time of 1.8 seconds was recorded in testing in the ABC gates at Schiphol airport, for example. Additionally, with the advent of 'on-the-move' facial image capture technologies, live facial images can be captured as travellers approach a booth, ABC gate or other such location. In such situations, one may propose a process whereby the live facial image has been captured prior to any step involving document reading or authentication. With the promise of such technologies alongside the indications from ABC gate tests above that simultaneous processes are possible in stationary installations, it seems clear that processes can be designed to hasten the overall border control process by reading the chip while the live image is being taken once appropriate technologies are utilised.

4. Conclusion of the Pilot

The main objective of the pilot was to test a limited but key set of technical options (identified within the Technical Study) against specific measurable criteria (namely accuracy, effectiveness and impact on border-crossing duration) in operational and relevant environments.

The results and findings of this unique project (in terms of scope and the number of different stakeholders), which was conducted over one year, have been complemented by desk research that has analysed some aspects in depth.

The pilot's findings, as shown in this Chapter in more detail, confirmed the feasibility of using biometric identifiers at external Schengen borders, confirming that biometric samples can be enrolled to levels typically required for a system to be accurate and effective while introducing process steps that impacted little on the border check procedure generally. It was observed that both the technology used and travellers' behaviour with it influence the results more significantly than the type of border where the crossing occurs. It also allowed some relevant observations and considerations to be made.

All this information should help to design the modified legal proposal for Smart Borders.

4.1 Biometric-identifier outcome

The section below summarises the feasibility of the different biometric identifiers, looking at:

- **Technical and operational aspects:**
 - **Accuracy and reliability**, which is determined by the quality of the biometrics that can be enrolled at the borders;
 - **Impact on border crossing point throughput**, by measuring the duration for capturing biometrics;
 - **Technology readiness**, usability and the influence of environmental conditions on the results; as well as.
- **Users' perception** (both travellers and border guards).

4.1.1 Enrolling fingerprints is feasible at all border types

The test demonstrated that it is possible to enrol good quality sets of four, eight or ten fingerprints at all border types using technology available on the market. However, enrolling eight or ten fingerprints adversely impacts the enrolment time and the success rate of the enrolment at a set quality threshold, especially in border conditions that require the use of mobile scanners.

Average enrolment durations increase in line with the number of fingerprints enrolled. In the vast majority of test instances, the capture process took less than 30 seconds for four fingerprints. Capture of eight fingerprints took roughly double the time to capture four fingerprints (approximately +126%). Capturing ten fingerprints took 185% longer than capturing four fingerprints and 26% longer than enrolling eight fingerprints. The enforcement of a re-attempt policy with a stringent quality threshold proved to be particularly cumbersome when capturing eight or ten fingerprints as a result of the high number of acquisitions attempts often required to complete the full process.

In general, the level of quality achieved with four fingerprints would allow a traveller to be identified in a large-scale database with an expected accuracy that was estimated up to 99.0% and that could potentially be further improved by using additional data as support (e.g. a picture of the traveller or some biographical information). The enrolment and subsequent search using eight fingerprints would be an alternative means of improving performances (accuracy) compared to the use of four fingerprints. Outcomes of performance estimation using combined quality metrics from various locations indicated that the use of ten fingerprints would only marginally improve the accuracy of results compared to the use of eight.

The proportion of successful enrolments varied significantly depending on the technology chosen, the configuration of the device and the environment in which the process takes place. Outdoor conditions and direct sunlight can impair the fingerprint capture with some devices, although scanners that are not affected by extraneous light were tested and found to function well in outdoor conditions.

Feedback collected from border guards and travellers showed that the fingerprint enrolment was generally perceived positively. However, due to the lengthier duration, satisfaction progressively decreases the more fingerprints are enrolled, with ten fingerprints being the least favoured option and the one which had the highest potential impact on queuing times.

Overall, the enrolment of four fingerprints was the most feasible of the three fingerprint focused test cases examined, in terms of impact on the border check process and end user feedback. A higher number of fingerprints can be captured but would have a stronger impact on BCP throughput and on the satisfaction of travellers and border guards. Accurately verifying and identifying travellers using fingerprints is highly dependent on the quality of the enrolled sample, which is seen to vary significantly across different test instances, depending on the technology used, the quality thresholds implemented and on environmental conditions.

4.1.2 Traveller verification based on facial image is feasible at all border types

The pilot confirmed that capturing a live picture and comparing it against the reference picture extracted from the traveller's passport (eMRTD) chip is feasible at all border types. Verification worked well in most of the test instances, varying according to the quality of the images stored on the chip of the travel document and the environment in which the live image was captured, and hence its suitability for automated facial image comparison. The process could not be completed in a relatively small number of cases when the facial image could not be extracted from the chip of the eMRTD. Execution of passive authentication as a means to ensure process security was sometimes problematic, typically because of the unavailability of the appropriate digital certificates or, in fewer instances, difficulties using available certificates because of a lack of conformity with standards.

The duration of the whole process was generally short, with average durations well below levels that would have an impact on the BCP's throughput: capturing the image contained on the eMRTD chip never took more than four seconds on average, while capturing the live image for verification purposes took six seconds on average. Performing automated verification of the live facial image against the image captured from the eMRTD chip adds very little time (less than one second on average). Capture of ICAO-compliant live facial images was not strictly necessary for facial image verification but may be required if facial images were to be enrolled for storage in a central database for future use in automated processes.

For this purpose the image from the chip on e-passports could be used, although data obtained in the pilot suggested that facial images on documents were sometimes not ICAO-compliant themselves. Enrolment of high-quality live facial images may take longer than the six seconds mentioned and would require additional control of traveller behaviour. Use of a self-service kiosk was seen to be useful in this regard.

The technology required for capturing the facial image at the border is already available on the market and webcam-type cameras used and shown to be effective are relatively cheap. The technology proved to function well in all environmental conditions, although – as expected – light conditions may affect the results (e.g. insufficient or excess light). However, this can be easily remedied.

The feedback collected from border guards and travellers on facial-image test cases was very positive.

The overall process of facial-image capture, chip reading and automated verification could thus be a workable solution for Schengen border controls. While the tests proved that the verifying (1:1) a traveller's identity using the facial-image biometric modality – based on a facial image captured live and checking it against the picture on the

traveller's eMRTD chip – is feasible, the facial image is considered to be insufficient as sole identifier for identification purposes within a large scale database (1:n).

4.1.3 Iris-pattern enrolment is feasible

The pilot confirmed that enrolling both iris patterns as a biometric identifier is feasible, although the enrolment of high quality samples in outdoor conditions was difficult.

The lack of a mature industry standard¹⁴³ made it impossible to fully compare the quality results across different devices. An estimation of the performances of the matcher, based on the quality of sample obtained using devices located outdoors and at a distance (around 1m) from the travellers, seemed to indicate that the accuracy of identification in large-scale databases¹⁴⁴ would be lower than the estimated accuracy using fingerprints. Accuracy using samples obtained from short to mid-range distance devices could not be forecasted, but would be anticipated to improve compared to the use of long distance sensors, based on the results of the IREX activities¹⁴⁵ from NIST.

These results highlighted that devices capturing iris templates at longer distances were affected by extraneous light and vibrations, reducing sample quality. It would be worth investigating whether such samples are suitable for verification against a high quality template enrolled previously, which was not possible within the pilot's constraints related to data protection. The duration of the enrolment process was generally short: the vast majority of acquisitions took under five seconds, with some exceptions (e.g. up to 18 seconds on average for kiosk-like devices) – even if it was more difficult to capture the iris of travellers with epicanthic folds, common in east Asian regions. Even though border guards had very little or no previous experience with this technology, their feedback provided during and subsequent to testing was generally positive. Participating travellers were similarly positive.

The technology required to use the iris as a biometric identifier at the border is available, but is relatively new and in some cases costly (the most expensive class of devices compared to the ones for fingerprints or facial image). Literature review undertaken within the pilot provided sufficient evidence to conclude that the iris was not more prone to spoofing than other biometric identifiers.

The cost and the maturity of the technology compared to fingerprints and facial image, particularly at land border where it would typically be deployed outdoor, could reduce the overall feasibility of deploying this biometric identifier at Schengen borders.

Finally, the concurrent enrolment of a live facial image with the iris templates was possible in some test instances within the pilot. While introducing the possibility of convenient multi-biometric usage, the cost of such setups and the additional complexity introduced would need to be considered.

4.2 Process-accelerator outcome

4.2.1 ABC gates are effective but still require supervision

Exit checks for TCNs carried out by using ABC gates performing bearer verification on the basis of the facial image were confirmed to be technically feasible on the basis of measurements of process completion rates and overall process durations. The measured time required to transit e-gates ranged from 14 to 41 seconds at different types of borders, shorter – or in the worst case equal – to the process duration at a manual booth for the regular border check process.

¹⁴³ ISO/IEC 29794-6:2015, "Information technology -- Biometric sample quality -- Part 6: Iris image data" was published only on the 01.07.2015, after the setup of the test instances.

¹⁴⁴ Estimations calculated on a database size of 100 million samples.

¹⁴⁵ [Accessed November 2015] <http://www.nist.gov/itl/iad/ig/irex.cfm>.

The technology required at the border exists and is already widely deployed at many European BCPs, currently mainly for EU citizens.

The vast majority of the participating travellers, and of border guards, gave very positive feedback on the use of ABC gates at the border. Most border guards involved in the tests were already used to supervising ABC gates and could therefore thoroughly evaluate their performance and possible added value.

It is particularly important that Passive Authentication (PA) should be performed on passports presented at ABC gates in order to ensure security in the possible absence of physical document checks by the border guard. The execution of PA lasted a negligible amount of time (less than six seconds on average) and could be done in parallel with other checks (e.g. database and biometric checks). The percentage of passports that do not pass passive authentication could be reduced by having a Schengen master list of cryptographic certificates (CSCA certificates needed to perform PA) required for this check.

4.2.2 Kiosks can be valuable

The pilot confirms that using kiosks for enrolling biometrics (FP and FI) and for advanced border checks is technically feasible (in terms of completion rate, quality and duration). It also confirms that border guards' workload can be reduced as some tasks are delegated to the traveller: four or eight fingerprints enrolment, FIs enrolment and verification, reading passport data, etc.

The extent to which an enrolment kiosk could reduce the time spent at the manual booth would vary depending on the tasks accomplished. However, taking the enrolment of 4 fingerprints as an example test results, it indicates a time saving of 35 seconds per traveller. The maximum savings were calculated to reach up to 55-65 seconds per traveller. Most time would be saved if kiosks were to be set up in waiting areas at border crossings before entering into Schengen, as entry checks (including the questions of travellers, database checks and possibly biometric enrolment in the future) are more thorough and time-consuming than exit checks.

Although the technology is available, border guards' feedback suggested that setting up and using kiosk solutions still requires further refinement of their configurations and their usability. Participating travellers were generally positive about their experiences using a kiosk. However, for specific traveller groups (e.g. elderly persons) it was sometimes difficult to operate the kiosks. In these cases, instructional user interfaces and an element of a learning curve would help limit the need for supervision and guidance. Further analysis would be needed to address these areas in more detail, including further examining the possibility of replacing self-service kiosks with mobile app solutions. Such a solution could also potentially address the lack of space before the entry for land BCPs, as well as reducing the required floor space and investment.

The option of deploying self-service kiosks is valid for controlled environments, which allow a high level of supervision to avoid the risk of enrolling impostors. The choice of a biometric token (e.g. a single fingerprint or facial image) between kiosk and manual booth can also considerably increase the security of the self-enrolment or biometric verifications performed at the kiosk.

4.3 Desk-research outcome

Operational testing has been complemented by a review of literature and by specific desk research.

4.3.1 Fall-back scenario

Fall-back procedures are essential for avoiding any possible negative impacts on travellers. Although the high availability of both the central and national systems will have very high requirements (similar to the level of SIS II, i.e. 99.99% per month), manual procedures to correct data within the system should be defined and implemented to cater for missing or incomplete entry or exit records.

Buffering at local or at the nation interface / access point would mitigate unavailability issues and limit the need for manual interventions in case of downtime.

4.3.2 VIS border check using travel document number

Consulting the VIS by using the passport number instead of the visa sticker number would simplify the border-control process and make it easier for visa holders to use automated solutions (i.e. self-service kiosks and ABC gates).

The change in the way the VIS would be consulted has been assessed as technically feasible, and the best-scoring option for implementation would consist of expanding the use of the existing alphanumerical search engine by adding new fields. This change would avoid the need for a complete re-design of the VIS database while still allowing good performance.

It is worth noting that the travel document number's data quality would then become critical to the functioning of the system.

4.3.3 Web service for travellers and carriers

Different options for implementing a web service that would provide travellers and carriers with information on the remaining authorised stay in the Schengen Area have been examined according to the level of service, the level of data-protection impact and of the level of complexity of their implementation.

The best-scoring options, treating all criteria with equal weight, are the following:

- For travellers to be able to consult the system, the best scoring option would be to use data from the passport and provide a simple discrete OK/NOK answer;
- A credential-based system is proposed for carriers, whereby using travellers' passport data as an input, a simple OK/NOK answer is provided if a single day of stay remains. The option to introduce a proof-of-check mechanism was also assessed in order for carriers to confirm that they have performed the check.

Finally, the desk research confirmed the previous cost estimations¹⁴⁶ for this component of the Smart Borders system.

4.4 Summary

4.4.1 Feasibility, accuracy and reliability

The pilot has confirmed the overall feasibility of enrolling biometric identifiers (FP, FI, Iris) at Schengen border crossing points for the purpose of verifying the identity of travellers at borders and of identifying undocumented travellers. The use of process accelerators (i.e. ABC gates and kiosks) by third-country nationals was also deemed feasible. All of the tests were conducted with technology currently available on the market and using existing BCP set-ups. The influence of the different technology and set-ups used highlighted the necessity of defining standard quality thresholds to be met, regardless of the technological choices made at each BCP.

4.4.2 BCP throughput

Enrolment time was mostly below one minute for all biometric identifiers, with capture of the facial image and iris generally taking less than 15 seconds. Enrolment of eight and ten fingerprints were the most challenging scenarios, especially at land BCPs where mobile devices were used for enrolment.

¹⁴⁶ European Commission, "Technical Study on Smart Borders – Cost Analysis", October 2014, section 4.4.2.2 [Accessed November 2015]. Available from: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf.

4.4.3 Technology readiness

Among the biometric identifiers tested, fingerprints would allow for the identification of undocumented persons or de-duplication with a high level of accuracy even in a large-scale database (e.g. 100 million travellers), with as little as four fingerprints per traveller and with an increasing accuracy as the number of fingerprints increases.

Verifying the identity of a traveller based on their facial image (by comparing the image stored on the chip with an image captured live) proved to work reliably. However, the facial image alone would not allow travellers to be identified from a large-scale database. Enrolment of iris templates, while possible and fast, yielded an insufficient quality for identifying travellers in a large-scale database if enrolled at a distance and in outdoor conditions.

4.4.4 Combining biometrics

Finally, test cases were also combined to simulate a possible multi-modal setup (i.e. four fingerprints with facial image). The combination proved to be still feasible: both fingerprints and facial images could be captured together at the set level of quality and within a short amount of time for the end-to-end process, as could iris and facial images. The use of more than one biometric identifier would not only strengthen the system against spoofing but also improve identification accuracy.

4.5 Considerations for the future of Smart Borders

The pilot has been a considerable step towards smarter Schengen borders. It provided evidence based real-life tests and analysis, enabling decision-makers to move ahead.

The final considerations hereafter focus on the future. They outline the points needing attention for effective system implementation and leverage, regarding both the European Commission's Technical Study and the Pilot outcome. All points below are either direct outcomes of work undertaken or were made by experts consulted to support pilot execution.

4.5.1 Make border-crossings points more effective and secure

Facial image: enabling bearer verification

For all genuine electronic passports, the facial image is stored on the eMRTD chip and its integrity can be verified using the respective cryptographic certificate by means of Passive Authentication. Therefore, that facial image can be compared against the live facial image and thus ensure that the passport holder has been duly verified. This is referred to as 'bearer verification'. Implementing this check at all border crossings, while performing the Passive Authentication, would decrease the risk of allowing travellers with counterfeit passports to cross the border.

Fingerprint: enabling identification

The performance predictions provided in this report may be used to aid assessment of the likely accuracy of the identification operation with different biometrics (multi-modal) and different number of fingerprints.

4.5.2 Faster border crossing process

Although adding biometric enrolment or verification steps to border checks adds some time, the analysis of the border clearance process suggests that time can be saved if processes are further streamlined (e.g. searching the VIS using the passport number, eliminating physical stamping, etc.).

Moreover, extending the use of ABC gates to third-country nationals and deploying self-service kiosks would, when appropriately deployed, lead to increased throughput at the borders without having to increase the number of active border guards.

4.5.3 Delivering the expected results

In order to fully exploit the potential of Smart Borders and the use of biometrics in particular, the following key elements require additional attention:

- **Infrastructure:** the pilot revealed some constraints¹⁴⁷ in BCP infrastructure (set-up and processes) which limited the effectiveness and efficiency of capturing biometric identifiers. The future system should take into consideration the variety of current infrastructures and allow for certain flexibility in order to be effective and efficient at any border-crossing point;
- **Training and traveller experience:** to achieve the expected results, training must be provided to support border guards through the transformation before introducing new biometrics and updated processes. Users' interaction with the technology was seen as a concern among border guards, thus the processes and users' interaction (interface) with technology also need special attention;
 - **Standardisation:** across different forums, various experts from MS and the industry have expressed the need for further standardisation and harmonisation of tools across the Schengen Area. This need is considered paramount for the future, with the pilot demonstrating possible benefits of: standardisation of the biometric quality indicators used;
 - Standardisation of the required quality thresholds for the different biometrics;
 - Standardisation of user interfaces for travellers, both to enable an easier learning curve for travellers when using kiosks or ABC gates and to improve feedback provided by enrolment scanners;
- **New technology:** contactless technology used to capture fingerprints even more quickly is very promising and efficient, but typical metrics for quality assessment appeared to be of limited use for samples obtained from touchless devices. Moreover, there are doubts regarding their interoperability with databases and AFIS containing fingerprints obtained with traditional contact scanners, as the images obtained by the two types of scanners are inherently different;
- **Reutilising existing infrastructure:** The pilot has demonstrated the usefulness of re-using some existing devices (such as ABC gates or fingerprint enrolment devices) and the possible relevance of achieving synergies with already existing systems such as the VIS (to ease automation as shown when using kiosks in Helsinki port or to reduce the need to re-capture fingerprints from visa holders as was necessary at Madrid airport during testing).

¹⁴⁷ For instance, although iris enrolment at land borders could be very useful, the current infrastructure does not always allow for it to happen in optimum conditions.

Page intentionally left blank

Page intentionally left blank



Publications Office

ISBN 978-92-95203-94-5

doi: 10.2857/08 6263

Catalogue n°: EL-04-15-804-EN-N

© European Agency for the operational management of large-scale IT systems
in the area of freedom, security and justice, 2015