HORIZON 2020: The PROTECT Project

WHITE PAPER

December 2020

TABLE OF CONTENTS

Figure 1: Long immigration queue for arrivals of Non-Schengen travellers (stock photo)

INTRODUCTION

In 2015 the European Union's Secure Societies challenge of the Horizon 2020 Research and Innovation programme published a call for research projects to examine 'optimization of the use of current biometric modalities and consideration of how services offered by countries outside of the EU may result in a more efficient and user-friendly experience for the traveller'. The call also required 'the related ethical, societal and data protection aspects'. The reference to *services offered by countries outside of the EU* added a challenging dimension to the project. The Pervasive and UseR Focused BiomeTrics BordEr ProjeCT (PROTECT) project (www.projectrotect.eu) was selected for funding with a start date of 1st September 2016 and duration of 3 years.

The business of managing borders changes more quickly than we can sometimes handle. Not only have international passenger numbers been rising – and may well continue to do so once the effects of COVID19 have been mitigated – but the threats from persons engaged in smuggling, crime, irregular migration, people trafficking and terrorism (SCRIPT) show no sign of decreasing. All that might be manageable if government resources and border facilities matched the problem.

During the period of the project, the United Kingdom was part of the EU but not the Schengen Zone. Because almost all countries adhere to ICAO standards for travel document design (both physical and electronic), then non-membership of the EU ceases to be a technical design issue, though more of a legal and operational matter.

THE PROBLEM

The PROTECT's challenge might be summarised thus:

More travellers + higher threat level + reduced defensive resources =problem

PROTECT's possible answer, which could be prototyped and demonstrated in almost-real conditions might be summarised thus:

Pre-registered electronic passport data + pre-arrival processing + on-the-move biometric capture =potential solution

The HORIZON 2020 initiative has allowed the PROTECT consortium (a balance of academics, expert users and technology providers) to design and build prototypes of an Automated Border Control (ABC) system – a system which in future could handle high volumes of pre-registered bona-fide travellers while allowing EU border officers the ability to filter out suspect elements routinely and reliably. The prototypes should handle both walking passengers (airports, ferry ports) and those in vehicles (ferry ports and land borders).

PROTECT looked at ways to keep passengers moving, to minimise the amount of border control space and physical hardware, but at the same time to ensure that passengers were uniquely identified for admissibility. The central technologies which could possibly enable these advantages were the capture of electronic passport data and on-the-move biometric scanning and matching. Though EU nationals have a right to cross EU borders, third-country nationals (TCN) have to be *examined* (asked about length and purpose of stay) – though it may be possible in future to exempt certain classes of TCN passengers from examination because of the ETIAS system, political agreements or statistical evidence of non-offending against immigration law.

DEMONSTRATION Methodology

PROTECT investigated and proposed new less obtrusive approaches to biometric data capture and verification, particularly the use of emerging and contactless multimodal biometrics including hand vein, periocular and anthropometrics modalities.
Moreover, the PROTECT project explored how traveller identification may be performed on-the-move whereby the in-motion identification process takes place indoors (within a monitored access corridor where the traffic flow is controlled), or outdoors with travellers in vehicles in a non-motion identification setting.

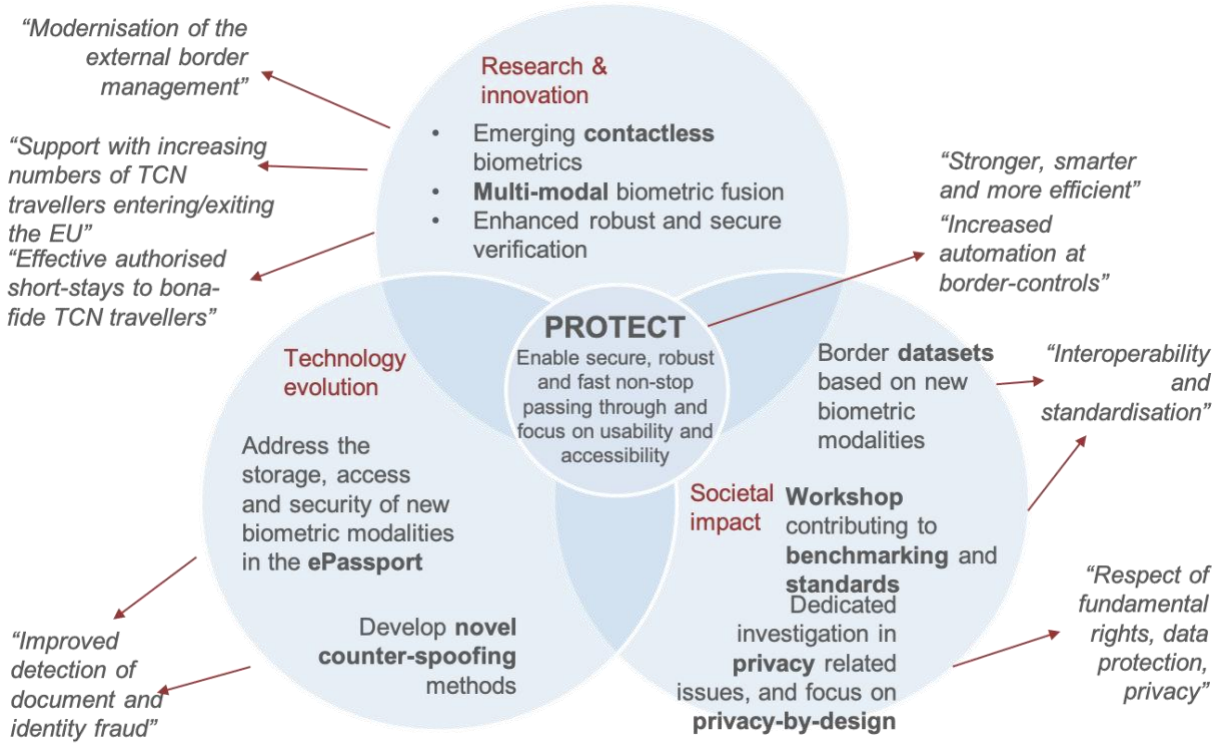

Figure 2: PROTECT and Smart Borders

The research was not purely technical. It took into account the everyday experience of border guards in managing automated border controls and the legal, social and ethical aspects of such an innovative solution. An early indication of the advanced nature of the concept was the fact that EU law did not yet provide for it.

Figure 3: The PROTECT passport data enrolment kiosk

The identification process is in two stages. In the first stage – enrolment – travel document data and multiple biometrics are captured at a PROTECT kiosk in a supervised manner via an informed consent process. This can be performed in any suitable location, for example at a non-EU airport departure point or a motorway rest area close to a land border. The collected data is encrypted and downloaded securely to the traveller's smartphone within a PROTECT *QuixBorder* app. If required, enrolment may minimally be performed once per lifetime of the travel document, and multiple biometrics enrolled in one step and used for verification both in the traveller-on-foot and traveller-in-vehicle use cases.

In the second phase – recognition – the identification process begins when the traveller arrives at the border and approaches the recognition area. Once the traveller is in close vicinity of the recognition area, the PROTECT *Quixborder* app on the traveller's smartphone processes signals sent by nearby installed iBeacons to inform the system that the traveller is about to pass through the recognition area. Then, the PROTECT app transfers the set of encrypted travel document and biometric data to the border control system. The transferred data is temporarily stored only for traveller verification within the recognition area.

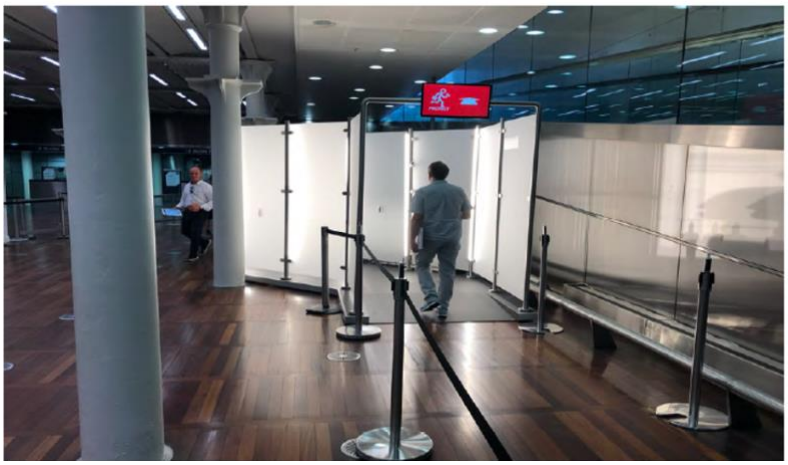

Figure 4: The PROTECT corridor installed at London St Pancras

As the traveller enters the recognition area at the border live biometrics are captured, verified and fused (according to ISO/IEC TR 24722:2015) in real-time. The process also incorporates presentation attack detection, according to ISO/IEC 30107-3, and detection of evasion of the identification process itself. Before the traveller reaches the end of the recognition area, a feedback signal is communicated simultaneously both to the border guard via a handheld device (or optionally a mixed-reality headset) and to the traveller via their smartphone PROTECT app.

If a traveller is not identified, is deemed to be high-risk (for example, via an alert list), attempts to spoof/evade the system or another exception occurs, the border guard can intercept and stop the traveller for questioning/2nd line check. The border control system also enables interoperability to information systems (for example, SIS, EES, ETIAS) for additional checks. Once the identification process is complete the traveller's travel document and biometric data is deleted from the border control system. In practice, identification within the recognition area is performed on a 1:N basis, where N is limited to the number of travellers physically within the recognition area at any time. Additionally, travellers are tracked through the recognition area via a network of CCTV cameras which further constrains the number of biometric templates to match against.

The indoor biometric corridor adopted a unique zigzag design which enabled optimal placement and capture of subjects in motion with strategically located attraction points in the centre of the field of view. The biometric modalities employed are face (visible and NIR), periocular (visible and NIR) and anthropometrics. Furthermore, the corridor was designed with accessibility by design, specifically use by wheelchair users with optimal positioning of the biometric capture devices.

Figure 5: The PROTECT vehicle demonstration

The outdoor vehicle use case adopts a similar process to the biometric corridor. The main differences are that a traveller in a vehicle approaches the border and stops at the border control post, which integrates the recognition area. The traveller remains within the vehicle. The traveller is then requested to submit their biographical and biometric data to the border guard. This is performed either via the traveller's smartphone or via a dedicated entry kiosk (terminal) alongside the vehicle at the border control post.

The data are transferred to the local border control system. Biometric verification is performed either by capturing all of the requested data by the sensors in the terminal or submitting the biometric features captured live on the traveller's smartphone, or a combination of the two. The biometric modalities employed are a selection from 2D face (visible, NIR, thermal), periocular (visible, NIR), 3D face, iris and hand vein. The border guard is presented with all the data submitted by a traveller in real-time. Following a successful check, the traveller's data are deleted from the border control system.

For both the traveller-on-foot and traveller-in-vehicle use cases, instead of the traveller's smartphone acting as the data carrier (mobile passport) an alternative is for the traveller to use an advanced passport equipped with a SUHF chip. This solution, while also supporting contactless on-the-move capability, requires the biometric data to be stored in a remote database.

The PROTECT system was deployed for demonstration in Kętrzyn, Poland, for land borders involving vehicles, in conjunction with the Polish Border Guard, and in London St. Pancras International train station, for travellers on-foot, in conjunction with UK Border Force and Eurostar.

Since greater use of personal [biometric] data impacts upon human rights, the PROTECT project also undertook a thorough investigation of privacy and data protection, ethical and social issues raised by contactless and multimodal biometrics on-the-move in the context of border security. PROTECT researched and evaluated new privacy enhancing biometric template protection schemes adhering to ISO/IEC 24745.

KEY FINDINGS

1 Does the technology work?

Overall PROTECT succeeded to build, demonstrate and evaluate, both from a technical and user perspective, a new biometrics on-the-move traveller identification system which improves the security and efficiency of the border identification process, is applicable to land, sea and air borders, and incorporates strong user-centric features. A variety of biometric modes were demonstrated, with varying levels of accuracy and usability.

2 Is it viable for future border control?

The PROTECT project marks the next stage on from current eGate-based ABC. eGates still present choke points to passenger flow in a situation where only a match of a physical body against a set of data is required. PROTECT takes away the choke point but retains the ability of border control systems to ensure eligibility to cross the border. It also offers an opportunity for border officers to mix with travellers (to make behavioral and other assessments) rather than sitting at remote control points. The security of personal data and sensitive biometric data is mostly a technical issue.

3 What are the expected benefits?

Where there are large and consistent flows of low-risk passengers (decided by nationality or advance passenger analysis), for example at major airport hubs, land borders or international rail termini, then on-the-move biometric recognition of voluntarily pre-registered travellers could have significant benefits in terms of reduction in queueing, savings in border control equipment and accommodation and increased flexibility of staff. More research and prototyping are nevertheless required to ensure a more perfect fit to future operational requirements.

4 What did PROTECT teach us?

The following detail some principles to keep in mind when designing systems to exploit the PROTECT concept:

- Move data collection away from the border and make it easy and convenient
- Keep travellers moving, not queuing
- Avoid large data stores and 1:many biometric matching
- Promote personal data security
- Passports and identity cards are just containers: it is the data that matters
- Mobile devices such as smartphones could replace passports in certain circumstances
- Ensure border guards can intervene effectively if necessary
- Engage both walking and vehicle travellers
- Interface with and exploit existing and future Advanced Passenger Information Systems
- Consider the value and impact of conducting medium- and long-term trials in near operational
- conditions with large populations of the travelling community.
- Too much distance needed between two successive passengers [in the biometric corridor] and not suitable for (small) groups (i.e. families)
- A few stakeholders remarked that connectivity with personal use devices of passengers is a
- limitation
- A short-term demonstration is not the same as a trial/long term validation of the developed
- system; for example, the London St Pancras demonstration highlighted networking issues which would need to be resolved in a longer-term deployment
- Legal issues are currently a barrier to (live) deployment of the PROTECT innovations within the EU
- Demonstration within a real live operational setting poses significant risks due to environmental and operational constraints.

CONCLUSION

How non-intrusive can we make identity confirmation systems for the border?

The collection of such personal data needs to be easy, quick, convenient and safe – and under the control of the traveller who has time to give informed consent. Ideally this could be done at home or in the workplace or at the start of the journey.
The collection of biometric samples is the sticking point in this vision since mobile devices and desktop PCs do not yet generally have accurate enough biometric receptors. However, conveniently placed PROTECT kiosks could contain the necessary devices and be available to use at, for example, airport departure lounges, motorway rest areas, post offices etc.
In any case, all modalities need to be captured in a passive manner, so that no potentially harmful radiation, for example, certain wavelengths of infra-red and ultra-violet light, lasers etc. are involved.
This is PROTECT's approach.
As 'on the move' and 'contactless' border management systems develop, the requirement to send confidential biographic and biometric data between travellers and border agencies will grow. As in PROTECT, the need for secure networks and secure hardware will become more and more relevant in a biometrically-enabled world. Any future research and development in these fields of operation should include security related topics in their briefs.
The question for whether the use of these kiosks need to be overseen by trusted supervisors to prevent identity fraud is a matter for further research.
A key problem which will affect ports of entry more in the future is the availability of space to manage passenger queues – space for border control booths, equipment and the queues themselves. Slowing the passage of travellers by more checking (and the collection of biometrics) will exacerbate the problem.

How fast and usable can we make these systems?

Modern border control systems in open, democratic countries have to compromise – between control integrity and passenger expectation; between speed/volume and limited resource.
Data collection should be fast and (as far as possible) error-free, or at least to an acceptable level given the risks of the day. This means that the user interface needs to be designed carefully and with disabled users in mind. As shown in PROTECT, a possibly useful feature of using mobile devices would be the ability to capture electronic data from ePassports (including biometric data) for storage and transmission via Bluetooth, Wi-Fi or Near Field Communication.
Better still would be for passport issuing authorities to load electronic data into applicants' devices alongside the issue of paper documents. Encryption and digital signing of the data in such a system should protect the data sufficiently against attack and misuse and assure border agencies of the provenance and integrity of the data when used at the border. The data might even be loaded into the dashboard computers of vehicles, the data being transmitted automatically (if the user desires) as the vehicle approaches the land border.
PROTECT showed that personal data stored in a mobile device was a workable approach.
It could also be possible to store the details of a complete family or other such group in a mobile device, the user being able to indicate via an app which members are actually travelling.

How do they fit with the EU's own future border control plans?

Travellers who are EU citizens, EU residents, EU visa holders and those Third Country Nationals who have an ETIAS authorisation could theoretically pass through controls on-the-move, provided that their physical bodies can be linked to their identity and eligibility details via biometric capture.

One possible solution is to eliminate *physical* interaction with border guards and machines for travellers who require no more than a check of their identity and eligibility to cross the border. Thus the 'no moving parts, just moving passengers' motto for PROTECT.

Probably further research and technical development beyond PROTECT is required (already moving ahead as commercial companies realise the potential income from biometric systems) to make identification of moving cohorts of passengers arriving in a stochastic fashion through open spaces accurate and comprehensive. Further ergonomic research into the user/machine interface could explore innovative ways of capturing and verifying biometric and Identity management data while the vehicle is still in motion.

It is likely that the categories named above will comprise the majority of travellers, leaving fewer individuals to be challenged by border guards at the manual control. Of course, those with legitimate objections to the use of biometrics or those unable to use a PROTECT-like system can still use traditional controls.

The transmission of traveller data to border agencies in advance of arrival or departure allows border guards time to react to any alerts.

Car and bus passengers and motorcyclists present a slightly different scenario. While pre-enrolment is certainly valuable, as is transmission of personal data just prior to border crossing, the difficulty lies in matching travellers to their respective biometric samples. It is currently not possible to device on-the move mechanisms for vehicles because of the difficulty in capturing biometric samples from within a metal box with maybe darkened windows. Thus the approach for now, as evidenced by the PROTECT Polish demonstration, should be a temporary stop of the vehicle to allow biometrics to be captured. This should in any case aim to be less time than a physical passport scan and visual match.

PROTECT managed this by having devices at car window height to collect face and finger vein samples. The use of iris pattern could facilitate the crossing of motorcyclists wearing full-face helmets.

Are there commercially exploitable products coming out of this research?

The PROTECT technical supplier has been able to build an innovative prototype and the experience gained will no doubt assist them to meet the needs of a new market – once it emerges. The dissemination and demonstration of the PROTECT concept should convince stakeholders in border control that gate-less, on-the-move, multi-modal biometric functionality, as well mobile-devices-as passport services are viable and will bring real benefits.
The potential for commercially exploitable products is wholly dependent upon the demands of the market.

What are the limits on the use of these technologies in terms of cost-effectiveness and human rights?

Citizens are rightly concerned about how governments and commercial enterprises might (mis)use their personal data. PROTECT operated on the basis of traveller consent:

- Whether or not to give such information
- Whether it should be kept or deleted after each use
- Which biometric modalities can be used
- To which uses the data is applied