FRONTEX

European Commission

2nd Global Conference and Exhibition on Future Developments of Automated Border Control (ABC)

Conference Report

10–11 OCTOBER, 2013
PEPSI ARENA, WARSAW

FRONTEX

European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union

Rondo ONZ 1
00-124 Warsaw, Poland

T +48 22 205 95 00
F +48 22 205 95 01

frontex@frontex.europa.eu
www.frontex.europa.eu

Warsaw, December 2013

Table of contents

Introduction

Frontex and the European Commission co-hosted the Second Global Conference on future developments of Automated Border Controls (ABC) in Warsaw on 10–11 October.

The Conference gathered government officials from national border management and immigration authorities from Europe and other parts of the world, such as Aruba, Canada, Southern Caucasus (Azerbaijan and Georgia), Hong Kong, Israel, New Zealand, the Russian Federation, the United Arab Emirates, the United States and the Western Balkans (Montenegro and Serbia); international organizations and EU Agencies including eu-LISA, the European Data Protection Supervisor and the Fundamental Rights Agency, the International Organisation for Standardisation, Interpol, to name a few; as well as airport authorities, academia, and private companies offering technologies and products related to ABC. In total 230 delegates, 50 high level speakers, 12 research institutes and universities, a number of international organizations and associations, and 23 technology providers have attended the event.

The Conference served as a forum to discuss the challenges of increased mobility, the benefits and risks linked to the use of automation, and how to balance the aims of facilitating travel and maintaining security at the borders. Furthermore, it highlighted the need for and the benefits of harmonization in order to increase levels of usage and achieve global interoperability. The Conference emphasized the importance of multi-stakeholder cooperation for the successful implementation of ABC solutions. Moreover, it addressed the societal implications of ABC technology and the future needs of ABC in the context of integrated border management. The present report is a summary of the key topics and discussions that have been addressed during the Conference.

Welcome address

Ilkka Laitinen · *Executive Director, Frontex*

Kęstutis Bucinskas · *Chair of the Strategic Committee on Immigration, Frontiers and Asylum, SCIFA of the Council of the EU, Lithuanian Presidency*

The conference was opened with a welcome address from Ilkka Laitinen, the Executive Director of Frontex and Kęstutis Bucinskas representing the chair of the Strategic Committee on Immigration, Frontier and Asylum (SCIFA) of the Council of the EU under the Lithuanian Presidency.

Mr. Laitinen warmly welcomed the delegates to the second Global ABC Conference and extended his special thanks to the European Commission (DG Home and DG Enterprise and Industry) and the Lithuanian EU Council Presidency for their support in its organization.

Mr. Laitinen emphasized that the ABC conference addresses an important need in the further development of ABC systems which requires multi-stakeholder involvement and a global approach. He went on to outline the key reasons why this approach is increasingly necessary. The traditional model of border control is under increasing pressure with a substantial projected growth in cross border traveller flows leading to even greater difficulties in providing effective border security whilst facilitating smoothly the vast majority of bona fide travellers. This is all happening in a context in which the hiring of additional staff is not an option due to budgetary constraints.

Mr. Laitinen concluded that he believed that the ABC conference will help address the following key issues during its two days of deliberations:

- ABC in the context of integrated border management
- Interoperability – how to balance security and facilitation
- Ensuring that ABC solutions are cost effective
- Latest research and development in the field of ABC
- Risk management of ABC implementation
- The social impacts of these processes.

In his address Mr. Bucinskas said that he was proud to be representing the Lithuanian Presidency at this important conference.

He stated that the overall aim of this event is to contribute to making Europe more safe, open and secure, and that one of the ways to help achieve this is through the incorporation of appropriate technological solutions such as ABC, which should be introduced to support agreed European and national policies in this area.

Ilkka Laitinen, Executive Director, Frontex, and Kęstutis Bucinskas, Chair of SCIFA of the Council of the EU, Lithuanian Presidency

Keynote Speech

Belinda Pyke · *Director of Schengen Directorate, Directorate – General for Home Affairs, DG Home, European Commission*

Belinda Pyke opened her keynote speech by stating how pleased she was to see that the agenda of the conference seemed to fully address the complexity of the introduction of ABC systems in Europe. She highlighted particularly that the issue of the social acceptance of ABC technologies by travellers and the broader society was going to be explored and stressed that without such social acceptance and trust the systems will not be able to work to their full potential.

She then put this conference in the context of some of the wider issues which are constantly affecting border management in the EU, in particular the tragic circumstances of the migrant boat sinking off Lampedusa the previous week and the continued conflict in Syria, as well as recent conflicts in Iraq and Afghanistan. These events help put into sharp relief the complexity of the issues being faced daily by border guard officers. Mixed flows at the borders include bona fide travelers, migrants and refugees but also persons engaged in criminal activities or indeed citizens of the EU who have been radicalized through direct participation in the above mentioned conflicts. Widely differing travellercategories currently end up in one queue at the border and are processed by a one-size-fits-all approach which is increasingly unsustainable.

In her speech Ms. Pyke went on to emphasize the central role of technology and state of the art IT systems in dealing with the complexity of managing the EU's borders. These systems allow for the intensive cross border exchange of information between EU member states and also selected third countries following strict guidelines. The European Commission is now supported in these efforts by the Frontex and eu-LISA Agencies who provide invaluable technical and operational advice to help in the development of the most appropriate technological solutions to the issues facing EU border management.

Belinda Pyke, Director of Schengen Directorate, DG Home, European Commission

Ms. Pyke outlined three border management initiatives in which IT systems play a central role:

- Second generation Schengen Information System (SIS II), which enables exchange of information on individuals crossing borders and can provide alerts on potential problematic cases. The SIS has already generated 49 million alerts and in its current format has the capacity to deal with up to 100 million alerts.
- Visa Information System (VIS), which went live in October 2011. VIS has already been rolled out to consulates in a number of the worlds' regions and will soon cover the remaining regions.
- European Border Surveillance System (Eurosur), which will go live on December 2, 2013. Eurosur will enhance the security at the EU's borders and allow for

an early detection of migrant boats in the Mediterranean which will help prevent the repeat of such events as the recent Lampedusa tragedy.

As for the future, Ms. Pyke referred to the Smart Borders package, currently being negotiated by the Council of the EU and the European Parliament. This initiative was launched to address the problem of the "one-size-fits-all" border management approach she had outlined earlier in her speech. The current average processing time of third country nationals at the borders – whether with visas or without – is too long. Moreover, the ABC solutions currently being deployed offer only a partial solution for third country nationals, as they are still required to have their passports stamped by a border guard on entry and exit.

As part of the Smart Borders package the Entry Exit System (EES) will allow for the automatic recording of third country national entries and exits to the Schengen area. In addition, the Registered Traveller Program (RTP), with its pre-vetting procedures for frequent third country national travellers, will allow for a speedier processing at border crossing points by facilitating them through the ABC gates.

The potential benefits of extending ABC gates to third country nationals through the RTP program are clear – in particular a reduction in the costs of operating border checks and a much improved service to bona fide regular third country travellers . In addition the Smart Borders package will significantly improve the tracking, locating and potential returning of visa over-stayers.

Ms. Pyke then addressed the important issue of privacy protection in the context of ABC and the Smart Borders proposals. She emphasized that that the EU Commission believes that there is no trade-off between privacy and security in this area, and that the Smart Borders package has incorporated the considerations of data protection from its inception following the principles of privacy by design, necessity and proportionality.

In conclusion Ms Pyke emphasized that the deployment of sophisticated technology in the area of EU and Schengen border management is a necessity, but that technology must always be deployed at the service of policy and not the other way around. She also emphasized the importance to the Commission of working in partnership on these matters with the EU Council and the European Parliament, as well as member states, and of engagement with the international community and the private sector.

In the Question and Answer session which followed the following issues were raised:

- Third Country Reciprocity in relation to RTP: The Panel agreed that this was primarily a political issue and that it is definitely on the agenda. Ms. Pyke noted that there are already a number of bilateral agreements in this area and that discussions continue.
- Human/Machine interface: The issue of the need for the education of the traveller, as well as the harmonization of his/her experience at ABC gates around the world. It was emphasized how this would enhance the traveller experience and make it easier for them to become comfortable with the new technological solutions, in much the same way that ATM machines went from being a novelty to a normal part of everyday life due to a harmonization of the machine/customer interface, customer experience with the machines and educational programs. The Panel believed that there is still a lot of work that needs to be done in this area.

PLENARY SESSION 1

Automated Border Control: state of play and national experiences – what has changed in one year?

The aim of this session was to hear the experiences from selected countries who have implemented ABC systems.

Moderator
Edgar Beugels
Interim Director of the Capacity Building Division, Frontex

Speaker 1
Brigadier Obaid Mehayar Bin Suroor
Deputy Director General, Directorate of Residency and Foreigners Affairs, Dubai, United Arab Emirates

Brigadier Obaid Mehayar Bin Suroor presented the current status of ABC deployment in Dubai and also the key learnings from its process of adoption. As an introduction he set the context of the geographic and geopolitical position of Dubai as a major hub in the Middle East for passenger traffic from Europe, Africa as well as India and China. In 2013 it is estimated that 65 million passengers will use the Dubai airport alone. This means that Dubai faces additional pressures on the borders in terms of facilitating travel for these large numbers of travellers and providing a high level of security.

He then stated that critical to the successful deployment of ABC in Dubai were the lessons learnt from an earlier approach to eGates which started in 2003, but failed to achieve its 50 percent target in terms of the share of travellers using the system (UAE citizens and residents). In particular, the first deployment was hindered by the following factors:

- eGates could only be used with an eCard, which could only be applied for at a separate location and by paying a fee.
- Convenient eCard registration points were lacking.
- Technical issues with first generation fingerprint scanning led to some problems with traveller/eGate interaction.
- A strong traveller marketing/educational campaign with guidance as to how to use the system was not conducted.

A new deployment phase began in 2013. The Brigadier gave an overview of the main reasons for its success:

- Second generation technology with face and iris biometric verification which can read both an electronic passport and eCard.
- On the spot registration at the gate.
- No fee.
- Registration outreach: available in Shopping Malls and at Universities.
- Passenger Marketing/education campaign: A dedicated team has been set up to market the eGates using a variety of tools e.g. information stands, brochures and an informational video on Emirates Airlines.
- ABC gates can be used by all UAE citizens and residents plus citizens from GCC-countries and 33 other countries who can travel to UAE/Dubai without a visa.
- Further training of staff.

In his presentation Brigadier Bin Suroor raised a number of other important themes which in his view have contributed to the success of ABC in Dubai and which are relevant to ABC roll-out in other countries.

- Focus on Best Service: A traveller's experience, including at the border crossing, is a crucial element in building a country's image. He emphasized the "Seven Star Service Strategy" where the Dubai government believes that a commitment to superior service at all points in the travel chain will continue to build their position as a major global trans-

port hub and contribute to economic growth. Currently at most borders in the world the 99 percent of bona fide travellers are treated in the same way as the less than 1 percent of travellers who pose any issues to the authorities. This is not a service based approach and the Brigadier believes that, with the help of ABC technology and the right strategic perspective, it will be possible to offer an excellent service at the border crossing for the 99 percent without compromising on security.

- International as well as local Liaison teams: International liaison is always a critical issue. In 2012 Dubai set up the UAE Regional Officer Team Dubai, which brings together liaison officers from Dubai and Germany, France, Netherlands, Australia and the UK. This working group shares information, knowledge and best practices with the aim of facilitating bona fide travel and preventing the spread of criminal activity across borders. The international liaison team also hold regular workshops, training sessions and conferences.

At the end of this presentation, the moderator Edgar Beugels concluded that the key issues raised were the move away from a system which relies only on an eCard/token, the setting up of the international liaison team which he believed could become a potential template for other countries working with ABC, and finally the focus on service which he agreed is central to the future of good border management.

Speaker 2
Gocha Kupradze
Head of "Imereti" Border Control Unit, Patrol Police Department, Ministry of Internal Affairs, Georgia

Gocha Kupradze started his presentation by outlining the context of border control in Georgia, which saw major law enforcement, corruption and border control issues in the post Soviet Union era. Since 2005 a new structure has been implemented with a new Border Police unit set up as a part of the Police department. The guiding theme of this new approach has been transparency.

Mr. Kupradze stated that since 2011 Georgia has implemented ABC solutions at four international airports and at the land borders with Armenia, Azerbaijan and Turkey. The ABC system is based on fingerprint verification and is currently available to Georgian citizens, however Mr. Kupradze expressed a willingness to enter into discussions with other countries to extend the program if an agreement on biometric database cooperation can be reached.

In conclusion, the moderator stated that Mr.Kupradze's presentation had shown well how Georgia had dealt with the twin challenges of implementing a major institutional overhaul of the Border Police institutions while at the same time introducing the latest technologies such as ABC.

Luis Gouveia's presentation provided an outline of the implementation of an ABC system (Rapid System) in Portugal. This project was started in 2007 to address the standard issue of ABC deployment – facilitating increasing numbers of travellers, especially at the airports, while maintaining security in a context of static budgets.

For Portugal the airports constitute a priority in terms of promoting facilitation as Portugal is a key transport hub for passengers from South America (in particular Brazil) and Africa, who often have very short transit times before catching connections to other Schengen countries. Mr. Gouveia mentioned that due to budget restraints, the ABC has appeared as a feasible solution to deal with scarce human resources.

The ABC system in Portugal is based on facial recognition and allows automated border controls of travellers with electronic passports without the need for enrollment. The system can also read fingerprints but this are not checked as facial recognition is deemed to be sufficient.

Traveller usage of the ABC system in Portugal has been growing rapidly with an estimated 1.4 million users in 2013 (growth from 1 million in 2012). The ABC system is also increasing its "share" or "quota" of total number of border crossings – so it would appear to be becoming normalized for many visitors to Portugal. Through a partnership with Vision-Box and the University of Algarve, research has been conducted regarding the performance of the system, and Mr. Gouveia shared the latest statistics of the performance indicators

Mr. Gouveia presented some preliminary findings from a recent research study which analyzed the ABC system usage by different demographic groups taken from a random sample of system users between January and March 2012. The users sampled were from the following countries: Portugal, UK, Italy, France and Spain. The research, which requires further validation, has provided some surprising results, in particular that the False Rejection Rate(FRR) is higher for females than males whereas the False Acceptance Rate(FAR) is equal between the genders. Furthermore, the FRR is highest for the 18–29 years old age group, and the FAR is the highest for the oldest age group in the study.

Mr. Gouveia then presented the most important recent developments in the ABC system in Portugal which include its extension to users of national ID cards through the installation of additional card readers, the installation of new sensors (depth and vision) at the eGates to enhance detection of travellers attempting to fraudulently cross the border, automatic light adjustment, and telescopic doors.

Furthermore, he referred to a planned pilot with Angola (for holders of diplomatic passports only) which will require a

Speaker 3
Luis Gouveia
Deputy National Director, Immigration and Border Service, Portugal

From the left: Luis Gouveia, Immigration and Border Service, Portugal; Pasi Nokelainen, Finnish Border Guard; Edgar Beugels, Frontex; and Brigadier Obaid Mehayar Bin Suroor, Directorate of Residency and Foreigners Affairs, United Arab Emirates

pre-enrollment and vetting phase. These travellers will not then require a visa to enter Portugal, however their passport will still have to be stamped when they cross the border. Mr. Gouveia stated that this is a one-off project and as such does not have wider implications for broader ABC implementation issues.

Finally Mr. Gouveia outlined the main challenges that he believes the ABC system in Portugal now faces. These are as follows:

- Need to keep the certificate exchange between EU member states up to date.
- Extension of the system to third country nationals who are holders of a residence permit in Portugal.
- Potential extension of the system to families and minors. It was emphasized that this is a sensitive issue and requires a safe and secure solution. How to best proceed in this area is currently a matter of debate and discussion.

The moderator concluded this section of this session by saying that it was interesting to hear about the further developments from a pioneer in ABC systems such as Portugal, and in particular the issue of the how to develop ABC systems to facilitate EU nationals travelling on their national ID cards.

Speaker 4
Pasi Nokelainen
System Manager, Finnish Border Guard, Finland

Pasi Nokelainen provided a summary of the situation regarding ABC implementations in Finland. Finland has ABC technology installed at three border crossing points, namely at the land border (Vaalimaa), at Helsinki airport and at Helsinki sea port.

The implementation process started in 2008 with a pilot scheme with three eGates at Helsinki airport, and from 2010 larger scale construction was initiated and there are now 33 eGates in total (five at Vaalimaa land border, three at Helsinki sea port and 25 at Helsinki airport). Mr. Nokelainen emphasized that ABC is now a normal and integrated part of border management in Finland.

At the moment, an ABC solution is not available in the car lanes of the land BCP at Vaalimaa. Consequently car passengers currently have to exit their vehicles to make use of the eGates. The technology will also still be available in the border crossing terminals to handle bus/coach passengers and pedestrians. At this land border there are currently between 6–7 million crossings annually with 65 percent of the people crossing being Russian citizens. The majority of the people crossing the border at Helsinki sea port are also Russian citizens.

In terms of the key ABC location at Helsinki Airport, there were 600,000 users of the system in 2012, and it is estimated that this will grow to 900,000 by end of 2013 and with more than 1 million users in 2014.

Mr. Nokelainen stated that from an operational standpoint it is most important to maximize traveller traffic through the eGates at peak hours – morning and afternoon. Currently 60–70 percent of EU citizens use the eGates at Helsinki airport and this quota is steadily increasing. However there will always be a number of people who use the manual border control because they prefer this option or do not hold an electronic passport.

Helsinki airport is an important transport hub between Europe and Asia with 50% of the travellers in 2012 being third county nationals, and this ratio is expected to in-

crease to 60% by 2017. This means that the issue of ABC usage by third country nationals is a particularly important one in Finland.

In fact a pilot scheme allowing Japanese and South Korean citizens(also planned for US citizens) to use the ABC gates when exiting Finland, is already in place, and 33% of Japanese passengers in 2012 used the dedicated eGates. Japanese citizens have become the second largest user group of the system.

The eGates used to facilitate these third country nationals are located in separate lanes as these passengers are still required to have their passport stamped by a border guard on exit. The pilot is for electronic passport holders and uses facial recognition technology. The system also checks the SIS II database for each third country national traveller – for EU citizens such checks are carried out on a random basis.

In conclusion Mr. Nokelainen said that their focus in 2013 in terms of ABC had been on technical updates and the third country pilot rather than broader construction/implementation as the system is already in place.

In terms of the future they are looking forward to further accelerate work on the Smart Borders package which will finalize the legal and operational framework for extending the usage of ABC to greater numbers of third country nationals.

DEBATE SESSION 1

Role of policy, harmonization and standardization in achieving interoperability

The goal of this session was to examine policy initiatives on ABC in light of harmonization and standardization needs. The European Commission Smart Borders package proposals were presented and their impact on future harmonization requirements reviewed. The session explored current and planned standardization initiatives and how these will contribute to streamline interoperability. A further aim concerned the identification of areas where further action is needed in this field.

Moderator
James Ferryman
Associate Professor, University of Reading, United Kingdom

Speaker Panel
Pascal Millot
Deputy Head of Unit, Transeuropean Networks for Freedom and Security and relations with eu-LISA: DG Home, European Commission
Paolo Salieri
Principle Project Officer, Security Research and Development, Directorate-General for Enterprise and Industry, DG ENTR, European Commission
Lisa Angiolelli-Meyer
Project Manager, Passenger Facilitation, International Air Transport Association, IATA

The Moderator of the debate started by asking the panel to consider the question of what do we mean by standardization and harmonization in the context of ABC technology. He referred to *harmonization* as a common look and feel for passengers and operators as well as broadly similar performance services; *standardization* as minimum quality standards for construction performance and safety; and *interoperability* as a system's ability to interact with other systems.

James Ferryman then briefly reviewed the status of the report on the mandate M/487 to establish security standards "Proposed standardization work programmes and road maps" by DG Enterprise and Industry (DG ENTR) which gives an overview of standards in the security area of ABC and biometric systems, identifies existing standardization gaps and sets out a road map for establishing a broader set of security standards. The final version of this report is available to the public on the CEN website.

The moderator highlighted three priority areas for ABC harmonization, given the belief that ABC systems are going to become a permanent feature of the European border management landscape. :

- Commonality of technical standards: to enable operators to know what they are purchasing.
- Commonality of "look and feel" for passengers: to help make systems intuitive for passengers.
- Commonality of standards for operators interface with the system: to reduce stress and strain for border staff

Each member of the panel then gave an overview of what are the key strategic policy initiatives in their area and how they are linked to ABC systems development.

First, Pascal Millot outlined the current status for EES and RTP programs for third country nationals in terms of technical standards and of remaining gaps in the systems which need to be considered by vendors and industry partners in their product development.

Concerning the EES, the system standards are basically already in place and there are no significant gaps. The EES will check if the third country national is already registered when he/she arrives at the EU Schengen border and will create a record if one does not already exist in the database. The system will hold biometric data on each third country national traveller and will record their entry and exit date and automatically and calculate the days left until the

expiry of their visa. The system will also provide details on visa over-stayers and other statistics.

In terms of the RTP the situation is somewhat different. This program is designed to facilitate border crossing for pre-registered and pre-vetted third country nationals. So the system will create records, check during the enrollment process and verify against the database and update it when people use the system. The main current gaps are related to the fact that this is no longer a stand-alone verification process at the eGate but one that requires the system to communicate with external systems e.g. checks vs. police databases. Another identified gap is the need to provide the traveller with information on entry and exit, e.g. length of visas and also the integration of fingerprint reading as most current systems are based on facial recognition.

Paolo Salieri then set out the issue of standardization of ABC from the perspective of DG ENTR. This area is being worked on in the context of an action plan to develop an innovative and competitive security industry presented in July 2012, the main goals of which are to better leverage the internal market, overcome market fragmentation, reduce the time gap from research to market implementation and better integrate the societal dimension. In terms of ABC system a complete process of harmonization and standardization will help reduce unnecessary testing and costs for industry and will greatly facilitate travel and tourism which are very important drivers of the European economy.

Mr. Salieri outlined that DG ENTR sees advantages in agreed standards becoming a common reference point and that over the next months they will be exploring how

From the left: James Ferryman University of Reading; Paolo Salieri, DG ENTR and Pascal Millot, DG HOME, European Commission

to move forward together on these issues with DG Home and Frontex.

Lastly, Lisa Angiolelli-Meyer noted that IATA is planning to publish an "ABC Implementation Guide" for airlines by the end of 2013, based on gap analysis carried out since last year on the state of ABC implementation. She particularly noted that the investment in ABC systems is increasingly coming from airports and also that they often provide the Project Manager to coordinate the implementation of ABC solutions. She agreed that airlines can play a central role in informing and educating the traveller about ABC, whether it is via the in-flight magazine, videos or other communication tools, and also stated that airlines could potentially play a part in the enrollment process for the RTP program.

The upcoming "ABC Implementation Guide" will also contain a chapter on future technology with an emphasis on how the all the different processes involved in passenger air travel(whether government, airport or airline owned) can be linked together so as to provide a more secure but also faster and better end-to-end passenger experi-

ence. An example of this could be the fact that with biometrics if may be possible to eliminate the need for boarding cards and the manual boarding card/passport reconciliation process, which is currently an integral part of the traveller's airport experience. It may also be possible to simplify the traveller experience in the area of the bag drop.

The moderator then passed on a comment to these points from Michael D. Hogan(Standards Liaison, NIST Information Technology Laboratory, United States), a panelist who was unable to attend the Conference. He stated that ABC deployment can and should take advantage of biometric standards which have been worked up over the last 10 years and that this will help ensure international interoperability.

At this point the panel addressed a number of questions from the audience. A representative of the German government raised the point that the standardization and interoperability of ABC systems is not only a technical and operational issue, but is also a legal one given the differences in legal regulations in the area of for example data privacy.

In response to this Lisa Angiolleli-Meyer stated that from the IATA perspective the most important element of harmonization is to look at it from the passenger's point of view rather than merely in the context of technical standards. In particular she raised the issue of different "competing" RTP programs from different countries, which will potentially require the traveller to do multiple registrations and multiple payments. IATA would like to see as streamlined registration and payment process as possible as this would increase the likelihood of passenger acceptance.

In response to this a representative of the UK Border Agency stated that the issue with a potential "global RTP gateway" was not so much the issue of data privacy but more connected to the sharing of security data which would be difficult to envisage. It was stated that the need for some degree of re-registration for RTP programs should be acknowledged.

Mr. Millot then gave more details of an important gap in the standardization of biometrics, in particular in the field of fingerprint enrollment and capture. Existing standards are not implemented in the same way and do not provide the same results. There is also a need to standardize the enrollment process itself, determining how many captures can be made, whether composite records are permitted, and better defining the required positioning of the finger. In this area standards do not exist, unlike the area of facial ID where they do and are followed. An important role can be played by Frontex in this process and their work on standards should get more visibility and should be introduced into the framework.

Another important gap that was raised concerns the area of international language, signage and symbols. Currently each government and country is producing their own symbols often in their own language which, without standardization, will inevitably lead to traveller confusion.

The panel then discussed the issue of what limits should there to standardization and harmonization processes. This issue of how to balance the need for standardization and harmonization on the one hand with the need to keep the traveller's interests at the heart of developments on the other was discussed. It is advisable that overly strict and rigid standards are not developed too early in the ABC development process, as this

could lead to standardization of mistakes. It was agreed that a well run standardization process should not freeze evolution and innovation, but should rather determine minimum performance parameters and requirements especially in the areas of security and safety.

For IATA the approach to ABC is similar in some respects to other initiatives the airline industry has worked on to simplify their business – such as the electronic ticket which after initial resistance is the now the accepted norm. As regards ABC, IATA plans to try and set up some pilot programs as a test and as such will be looking for government and airport involvement, e.g. two governments, two airlines and two airports to jointly organize an ABC pilot program – interesting in this context is the Netherlands/Aruba test case.

IATA has also set up a Passenger Facilitation Working Group open to all stakeholders with the aim of further improving traveler facilitation at all points of the travel chain. This group also considers issues related to streamlining and improving the speed and accuracy of the advance passenger information which is sent to government currently and also potentially integrating this process into the overall border management process with ABC.

For the airlines ABC is seen as being primarily an opportunity to improve their service levels to travellers, for example by shortening transit processing times if ABC is implemented in the transit areas of airports.

Conclusions

There were a number of conclusions to this session. First of all it was agreed that the traveller must be at the centre of ABC deployment and that this means that there should be a standardized approach to the traveller/ABC interface globally so that the process becomes as intuitive as ATM machines. A set of minimum standards should exist for the technological side of ABC, but the ABC standardization must also deal with "how to use it" as well as "how it works".

From the perspective of industry/producers the key conclusion is that standardization and harmonization must be completed to a pre agreed level, as if it is not this will drive up development and certifying costs for business.

For the airlines it is important that the discussion continues to be a global as well as a multi-stakeholder one including all interested parties. Their primary interest in ABC is in improving the service to travellers at all points in the travel chain and as such they are very interested in integrating ABC and biometric solutions into a total traveller service concept.

DEBATE SESSION 2

Benefits and challenges of automation: how to balance security and facilitation at the borders?

The purpose of this session was to discuss the benefits and challenges of automation and examine how ABC deployments strive to meet two seemingly contradictory goals: handling increasing traveller flows while meeting high security standards. To discuss these issues the expert panel was drawn from the various stakeholders involved in the process of ABC implementation: EU Regulator, Border Authority, Airport Operator and Industry representative. In addition the panel had the added value of expertise from Ram Walzer, an Israeli delegate who was able to give a perspective on ABC and biometrics deployment in a situation of heightened security concerns.

Moderator
Joseph Atick
Chairman, Identity Counsel International, United States

Speaker Panel
Philippe Van Triel
Project Officer, Transeuropean Networks for Freedom and Security and relations with eu-LISA, DG Home, European Commission
Andreas Reisen
Head of Division ICT Strategy of the Federal Police, Modern Border Control Management, Federal Ministry of the Interior, Germany
Ram Walzer
Biometric Application Commissioner, Prime Minister's Office, Israel
Jean-Francois Lennon
Director, Global Business Development and PMO, Vision Box, Portugal
Jurgen Wachtler
General Operations Manager, Hamburg Airport, Airport Council International, ACI World

To start the debate the Panel were first asked to address the question of what are the challenges and opportunities of ABC deployment from their stakeholder perspective.Philippe Van Triel from the European Commission addressed this question from the perspective of the regulator. He reminded the audience that 2009 figures show that there were 700 million border crossings to and from the EU Schengen area at its 1800 border crossings, of which 70 percent are EU citizens and 30 percent third country nationals. . The EU currently has 288 operating ABC gates in 13 member states, but as he said, this is just the beginning.

In addition to the smooth and fast processing of EU nationals, a major challenge concerns improving both the facilitation and the security related to the processing of third country nationals. He stated therefore that the biggest area of opportunity lies in the implementation of the planned EU RTP program, as this will open up the ABC gates to third country nationals who will have been pre-vetted and pre-screened and will be allowed to use the automated border checks.

Andreas Reisen then discussed the question from the perspective of the Border Police. He stated that for the traveller it is a convenience issue, however for the border police it is more a capacity issue. In other words – how many travellers can they process and with what resources to ensure a smooth facilitation and maximum security.He also highlighted the issue of resource efficiency. Finding the right balance between border guards and technological solutions; and an issue of security – they need a system that allows them to quickly cross check with existing data bases – SIS II, and national databases – and which also is able to be widened to incorporate other information architectures when these become needed and required – e.g. when EES is implemented. in his view a major advantage of ABC solutions is also that they can deliver substantial cost savings; their own cost/benefit analysis of the planned German Easy PASS project demonstrated that they expect to save between 30 and 50 million euros over 10 years (2014–2024) thanks to the ABC deployments.

Jurgen Wachtler presented the view of the airport operators in terms of the opportunities and challenges or ABC. He highlighted the key opportunities of ABC as being the potential speeding up of the whole traveller experience in the airport, the use of less space for the processing of

border checks and the possibility of reducing the overall amount of stress a traveller endures while being "processed" through an airport – from car park, to check in, bag drop, through security and border control. If this process can be made less stressful – then there is the opportunity for the traveller to take advantage of the food/beverage and shopping facilities available in the airport terminal to a greater extent. Another issue is the fact that from the airport's perspective a traveller should encounter a single "look and feel" in terms of ABC solutions at whatever airport he is at – whether European or from another region.

Jean Francois Lennon then presented an industry perspective on ABC. He stated that he believed that ABC solutions at border control will become a commodity and will be intuitive for travellers sooner rather than later. For the future there are a number of key issues such as the potential extension of ABC and biometrics to cover all 14 steps of a traveller's journey at an airport and in addition to this the issue of data sharing between different stakeholders.

Ram Walzer then gave his perspective from the position of ABC and biometrics in the context of heightened security threats. Israel's geopolitical status creates challenges and opportunities in this area. Security is always the main priority, however new technology and biometrics are part of a broad program of security and traveller facilitation that Israel is undertaking.

The debate then moved on to the issue of how ABC gates can enhance security, and if it is enough for a nation to trust travellers solely on the basis of them holding a genuine electronic passport.

Philippe Van Triel stated that for an EU national, he/she must keep the full benefits of citizenship so there is an element of

Philippe Van Triel, DG Home, European Commission and Andreas Reisen, Federal Ministry of the Interior, Germany

trust, however with the provision that with electronic passports the legal and operational framework for the exchange of information between member states must be completely implemented, which is not a hundred per cent the case at present. As regards third country nationals this issue will be partly addressed by the pre-vetting and screening envisioned in the planned RTP program.

On the issue of trust Jurgen Wachtler stated than his main concern was the potential creation of a two tier traveller experience, with on the one hand the frequent flyer, flying business class with convenient processing through border controls thanks to RTP programs , arriving at the airport 30 minutes before their flight, and on the other the infrequent traveller only flying twice a year, often increasingly elderly due to demographic changes, who must be at the airport three hours before their flight.

Ram Walzer said he believed that all border crossings should be treated as being part of a pre-planned and integrated security process with a few elements, for example

threat orientated security checks together with biometric support at all points of a complete A to Z process.

The issue was then raised in what situations a EU citizen with a valid electronic passport would be denied access to the ABC gates. According to EU law, one of such exceptional circumstances would be if there is an alert from the SIS II database watch list, which could reflect a situation in which the passenger is wanted as a witness in a court case and not only that he is directly wanted for some criminal matter. The other situation where there are restrictions in terms of using the eGates is in the case of minors as currently you are not permitted to take fingerprints from minors under the age of 12 in most member states. There are also exceptional circumstances when the eGate system can be closed for certain "high risk" passengers even if they hold an EU electronic passport –e.g. football fans. In the latter case, the border entry system should be customised at short notice to accommodate this kind of exception to normal procedure.

This was compared to the situation in the United States by moderator Joseph Atick, where the fact that a citizen holds an electronic passport does not give him/her the automatic right to pass through the eGate; it is a more discretionary process based on "do we know enough about this person to trust him/her". In other words, to use the ABC gates in the United States a person must be registered and pre-vetted and screened in order to prove to the government that one is a trustworthy citizen. The point was raised that for the EU this approach would likely be regarded as discriminatory and would not be permitted under current EU law.

The experience from New Zealand was shared in terms of its program with Australia. This is a universal program open to New Zealand or Australian citizens who hold a valid electronic passport which does not require any pre-registration or vetting. However it was emphasized that ABC is still a border check, which is simply more automated than it was previously and where the traveller can "fail" and not be permitted entry or exit. It was also emphasized that ABC gates if properly operated can offer a more consistent solution to border management than a purely manual system as the automation reduces variation, human error and the potential for border guard corruption.

The role of the human border guard in view of ABC systems was discussed as well. Representatives of national border agencies emphasized that they are not resigning from the use of border guards; they remain to supervise the eGates and intervene if they deem it necessary. For example, in Germany the border management authority wishes to maintain a ratio of one border guard to a maximum four eGates. The border guards are therefore still an integral part of the process, and in many cases are receiving additional training to ensure that the new combined human/eGate system works effectively and efficiently.

In general, the panel agreed that ABC systems if properly implemented as part of an overall security concept with proper human oversight do in fact enhance security. There is a lack of quantitative data to back up this assertion as it is hard to analyze what has been prevented, and it is harder to provide data on security than on efficiency. However, there is much anecdotal evidence in terms of offenders preferring to use manual gates and the border guards at the manual gates using the eGates as a back up to help them with their passenger assessment.

Every system can have vulnerabilities, including ABC, however it is important to remember the benchmark was a purely manual system which was far from perfect. There are also examples of airports in the EU which are implementing ABC gates purely for the improvement in the security aspects of biometric control of travellers, as from the perspective of traveller facilitation they did not really need to implement ABC solutions.

The moderator referred to the fact that in the United States the trusted traveler program has been extended to give the registered traveler a fast lane through the airport security checks, making the checks less time consuming, as the risk analysis has been partly carried out before the passenger arrives at the airport. Whether this could be a template for other countries was discussed. At an EU level there is no plan to introduce a RTP program for EU citizens, and such an approach would impact internal Schengen travel as all flights currently have security checks. The airports would welcome such a development and from a technology standpoint it is possible to imagine an automated biometric based process which covers all 14 steps of the passenger experience in an airport, not based on a registered program but with the use of a temporary token. In the EU context it was emphasized that from a legal and security perspective at least a minimum border check will always be applied no matter how trustworthy the passenger is deemed to be.

At the end of the session there was a discussion on future issues for ABC, including in the context of the mobile revolution and the expanse of social media. It was agreed that the potential of using mobiles for the traveller as a mobile holder of biometric data was an issue for the distant future.

Conclusions

This session brought together stakeholders covering a broad cross section of the interested parties involved in ABC. From the perspective of security the key conclusion was that ABC is only part of a broader border management concept which is risk oriented and uses a variety of security tools (e.g. intelligence sharing, advance passenger information) of which ABC is only one. The overall goal is to separate the bona fide traveller from other travellers as early as possible. In terms of the border crossing itself it was emphasized that human control of ABC is essential.

From the perspective of the airports the key goal is to maximize efficiency of traveller facilitation and to use technology including ABC to improve the traveller experience and make it less stressful. Airports would also like to see technological innovations which will allow them to reduce the space allocated to processing travellers, including security and border control.

PLENARY SESSION 2

Academic session – research and innovations in automated border control technology

Moderator
Sadhbh McCarthy
Director, Centre for Irish and European Security, CIES, Ireland

During this session selected research and innovations in the field of ABC were discussed. The presentations were chosen among the submissions presented in response to the call for extended abstracts launched by Frontex and the European Commission*.

Speaker 1
Andreas Kriechbaum
Engineer and Project Manager – Video and Security Technology, Austrian Institute of Technology (AIT), Austria (on behalf of Michael Gschwandtner and Svorad Stolc)

Document Security in the age of Fully Automated Border Control Systems

Andreas Kriechbaum started his presentation by reminding the conference audience that despite the increasing adoption of ABC solutions at border crossing points, the electronic passport was in fact developed with the manual border inspection process in mind where the scanning would still be performed by the border guard. This means that the security features of the current electronic passports are in fact better adjusted to manual processes rather than to automated ones.

This raises two key questions:

- Should the design of an electronic passport be changed to include features which take into account automatic scanning?
- Could we resign from using the optical security features that are to be found in the current electronic passport design?

Mr. Kriechbaum then listed some of the key security features which protect existing electronic passports, including on the paper side: micro text, special inks, special printing, security laminates, holograms, watermarks and security fibers and on the electronic side basic authentication features to protect against cloning and extended access control to limit who can read the passports.

The presentation then analyzed in more detail the integrity of current optical checks on electronic passports and whether this can be fully automated without a diminishment in security.

A number of examples prepared in laboratory conditions were shown, in which a automated document reader can be fooled and accept a travel document as valid, when it would be clear to the human eye that it was a fake. This is also the case with the typically more sophisticated document readers that are used commercially.

Another related security issue is that current document readers are potentially unable to distinguish between a genuine document and an image of a document with simulated security features (e.g. on an iPad).The conclusion therefore was that machine based checks on optical features on their own are problematic. The presentation then went on to look at a possible alternative which is to rely entirely on electronic security features, i.e. chip cards that only contain chips.

It was emphasized that these features are currently secure and will remain so if we assume that all security procedures are followed 100 per cent in all the 105 countries that issue electronic passports. However, there are a number of possible points in the security chain that could be open to attack and as such it is difficult to claim with certitude that current electronic security features will remain intact forever.

* Annex I to the present report includes abstracts selected for oral and poster presentations.

Given this Mr. Kriechbaum recommended a hybrid approach is best – a combination of optical and electronic security features. To this end he would like to conduct further research on developing extra additional electronic security features as a supplement to the optical ones.

Dependability Management in Automated Border Control

Speaker 2
Toni Ahonen
Research Scientist, Technical Research Centre, VTT, Finland

Toni Ahonen's presentation dealt with the area of system performance, dependability and reliability of ABC gates. As context to this subject the presenter pointed out that as ABC gates process increasing numbers of travellers, then issues of their dependability and reliability will become even more important than they are now. Any system failure will have the potential to negatively affect traveller acceptance of ABC solutions. Availability performance was defined as a percentage, so if a system has no failures then its availability performance is 100 percent.

Mr.Ahonen then went on to present three dimensions of availability performance and dependability as follows:

- Reliability performance (built into system by systems developers).
- Maintainability performance (shutdown length, cost).
- Maintenance support performance (capability of maintenance company).

It was also stated that dependability relates to the whole system – not just a single gate and that there is a need to manage the whole lifecycle of the system within the context of reliability and dependability. It is important to build in an awareness of these issues as early as possible into the systems design phase of product development, as in this way the potential cost of dealing with unforeseen reliability issues during the usage phase is greatly reduced.

To follow this, a number of guidelines were proposed to build a systematic approach to maximizing dependability and reliability which include:

- System dependability objectives: building all the key stakeholder's reliability and dependability expectations of the system into the system design phase.
- System reliability structure: using a top down approach in which the dependability objectives guide every aspect of system design and architecture.
- System and component failure behavior: reliability risk analysis through the whole lifecycle of the automated gates.
- Maintainability performance: analytical tools and methodology to measure maintenance performance.
- Reliability data: system to collect reliability data from system users so that this can be exploited in future system design. This will require close collaboration between the user maintenance function and the design function.

To conclude, Mr. Ahonen emphasized that the proposed systematic approach to systems reliability and dependability is an important requirement to ensure that ABC deployments go smoothly and are accepted by the end users. Such a dependability management framework will help manage the whole process with multiple sub-contractors to ensure that the money invested in such systems gets the best value return.

Speaker 3
Stephan Veigl
Software Engineer, AIT, Austria

Visual Surveillance Technologies for Enhancing ABC Secure Zones

Mr. Veigl introduced his presentation by setting out the three issues which his team is dealing with in its research:

- Checking whether one person at a time is going through an eGate.
- Checking whether the passenger leaves anything behind in the eGate.
- Queue length estimation – a convenient feature for the passenger and for the ABC operator for planning purposes

Prototype solutions to the first 2 points are currently being tested at Vienna airport and point 3 is in the research phase. The solutions to issues 1 and 2 are providing better quality and faster data than was previously available and for the issue of queue length this is a new feature that is not currently available.

Video surveillance technology, whether at two or one door ABC gates, combined with special computer algorithms can automate the response to all of the above issues in real time.

It was emphasized, that abnormal information received should be verified with other sources of information available, and should then be passed on to a border guard who will then be able to initiate appropriate action.

Speaker 4
Hong Wei
Senior Lecturer in Computer Science, University of Reading, United Kingdom

Biometrics in ABC: Counter-spoofing research

Hong Wei introduced her presentation by stating that ABC solutions require fast and secure ID verification, and since the verification process is automated, the system is more vulnerable to potential spoofing attacks. This is the area of her team's research as part of the EU funded Fast Pass project. The research project started in July 2013, so any findings and conclusions at this stage are preliminary.

Ms. Wei then went on to address the potential spoofing of the most common biometric feature to be currently verified at ABC border checks – the face. There are three types of anti-spoofing algorithms which can deal with potential attacks in this area.

- Motion analysis which finds significant differences between a 2D and 3D face: effective except in cases where masks are used.
- Texture analysis: generates an image of textural features of the face and then detects differences between the real face and the spoofing face.
- „Liveness" detection: analyzes life signs of human face, e.g. eye blinking, mouth moving. This method requires a moving image.
- Academic competitions are currently underway to develop the most effective spoofing counter measures in this area. In the 2013 competition there are eight academic teams taking part with seven of them working on texture based solutions, three on motion and one on "liveness".

In terms of the research challenges in face anti spoofing, a number of areas were mentioned, including: similarity between family members and twins, the necessity to capture the traveller's image while he is moving, the efficient fusion of sensor data to ensure a reliable result and the issue of 3D attacks (e.g. masks).

Next the presentation looked at fingerprint verification in the context of spoofing, and the ways which can be used to fool the biometric system based on fingerprints. Ms. Wei went on to outline a number of different anti spoofing measures. Firstly in terms of hardware, extra investment in temperature sensors could help solve the problem. In terms of software, analysis can be done of the fingerprint image itself, e.g. perspiration pattern, pore distribution and skin distortion. Other counter-spoofing measures include analyzing heart rate, smells and blood pressure. Future research challenges in this area include the issue of detection of the material with which a fake finger is made versus a real finger.

Finally, Ms. Wei discussed the iris biometric feature in the context of anti spoofing. This is not such a common measurement in ABC solutions despite it being stable over a person's lifetime. However spoofing attacks are still possible with for example the usage of printed iris, contact lenses or plastic or glass eye balls. Anti-spoofing approaches concentrate on the eye's reaction to light reflection and also in area of behavioral analysis.

For research purposes, in the area of anti-spoofing of iris recognition, a major issue is getting reliable data from the systems which use this parameter. There are also practical issues with the capture of iris data due to the size of the target, the distance, illumination issues and the probable need for close passenger cooperation.

Hong Wei, University of Reading, United Kingdom and Marc Atallah, Deloitte Business Consulting, France/United Kingdom

To conclude Ms. Wei stated that there are anti spoofing tools being used in biometric identity verification, but that they must be made more robust and they need to be constantly updated to deal with the evolution of spoofing threats. Moreover, she states mentioned that there is an "arms race" between the development of spoofing and counter-spoofing techniques.

Next Generation Smart Border Security

In his presentation Mr. Adamson focused on the future of ABC and border management to make smart border programs really smart. His thesis was that this is a much broader issue than simply a biometric algorithm and checks against watch lists at the border, but that we should move in the direction of the ability to assess multiple data sources in real time using big data so as to inform operational decisions. In addition, he stated that for prototyping a smart border analytics tool it is necessary to understand border traffic (including geographical and economical patterns) and define risk profiles for irregular migration and illicit activities. He suggested that the goal should be to use big data to make ABC gates smarter than they are currently and

Speaker 4
Marc Atallah, Paul Adamson
Directors, Deloitte Business Consulting, France/ United Kingdom

bring them closer to the intuitive performance of a border guard. He emphasized that this data on citizens is already out there (e.g. in social media), and the question is how and whether to access this data to provide for better and faster risk analysis.

Mr. Atallah then gave some more details about how their proposed data mining approach would work (Advanced Knowledge Discovery) where the objective is to provide a variety of areas of government with better quality analysis and predictive risk analysis tools. As an example, Twitter feeds could be used for feeding data into algorithms connected to the ABC system thus making them smarter.

DEBATE SESSION 3

Parallel session 1: From decision making to implementation – making ABC a cost effective solution

This session examined the decision-making process for the deployment of ABC systems, including cost effectiveness and cost benefit aspects. The importance of inter-stakeholders cooperation, and its impact on the successful implementation of ABC at the borders, was highlighted.

Moderator
Kier-co Gerritsen
Coordinating Specialist and Program Manager, Ministry of Security and Justice, the Netherlands

Speaker Panel
Lori Pucar
Acting Director, Border Programs Modernization Division, Canada Border Services Agency
Glen Wimbury
Assistant Director, Border System Programme, BSP, Border Force, United Kingdom
Marten Dijkstra
Senior Security Officer, Schipol Airport, the Netherlands
Ignacio Zozaya
Research Officer, Research and Development Unit, Frontex

To introduce the session Glen Wimbury and Lori Pucar gave a general overview of ABC deployment in the UK and Canada and Marten Dijkstra gave the perspective of Schipol Airport in the Netherlands, one of Europe's busiest hub airports. The first issue that the panel discussed was the involvement of the private sector in the deployment of ABC solutions and the private-public partnership involved. Quite often airports are the investors in the ABC systems and the border management authorities are the operators thus making the cooperation between the two important. The airports are interested in the commercial benefits from a faster and less stressful facilitation of travellers and better space optimization inside the terminals.

In the UK the presence of ABC solutions in airports is perceived as a service benefit by the airport operators and as something which can help them attract more passengers to their airport rather than to their competitors. Mutual trust is a key factor between government bodies and the airport operator which takes time to build up; however the panel agreed this kind of collaborative approach is essential. Private/public partnerships in the financing of ABC deployments is also developing with co-funding, leasing of infrastructure and pay-per-process solutions being developed.

The benefits of ABC deployments are different for the various key stakeholders but the panel emphasized the importance of having a strong business case before implementation. The key factors that drive ABC investments are from the airport operator side, increasing speedy and smooth traveller facilitation, frequent limitations on space inside the terminals and financial constraints.

From the perspective of the border authorities the case is related to the potential 100 percent consistency which ABC solutions can bring to facilitating the majority of low risk travellers, therefore freeing up limited border guard resources to deal with the more complex or high risk cases as well as the potential operational cost savings through the deployment of technology. Although it was emphasized that it is not so much a case of border staff reduction, but rather a more efficient and effective deployment of their existing human resources. In this context it was emphasized and confirmed by panel speakers that ABC solutions do not replace border guards. In addition to this, in Canada it has been noted that the implementation of ABC solutions has in fact positively impacted on the working environment of the border force, freeing some of them up to be deployed in a more roving capacity using behavioral observation techniques to identify potential high risk passengers before they leave the border zone. In fact there is no one business case template for investing in ABC solutions as every case is different. A key factor is always however is the need to involve all the stakeholders in the discussion so as to build a consensus on what the objectives of such a deployment are. This is not easy as the stakeholders normally have different objectives; however it is essential if the project is to be a success.

In terms of the airport operator and what return they can expect from investing in

From the left: Lori Pucar, Canada Border Services Agency; Marten Dijkstra, Schipol Airport, the Netherlands; Ignacio Zozaya, Frontex

ABC, it was pointed out by the panel that this can have a positive effect on port revenues in a number of ways. First of all ABC solutions allow the airport to facilitate more travellers in the same space therefore meaning more shoppers in the airport retail outlets. Another dimension is the fact that studies have shown that ABC solutions on average reduce the time each traveller must spend passing through border control, and we can assume that at least some of this time saved can be spent in the airport shops. Finally on a qualitative level ABC solutions can help reduce the stress and uncertainty associated with passenger travel which in turn should influence their "mood" and encourage spending in retail outlets as they will be more relaxed.

The case for successful ABC implementation is supported by the exponential increase in their usage by travellers in countries and airports that have deployed them. In the UK usage has gone from one million five years ago to ten million facilitated passengers in 2012. However it was again emphasized the importance of providing travellers with clear information as to the location of the eGates and how to use them. This is a critical factor influencing uptake and as such can have a big effect on the success or failure of an ABC deployment and its return on investment.

Another factor influencing the speed of ABC deployment in Europe is the lack of updated EU regulations in terms of data protection. It was confirmed that many member states are waiting for this issue to be addressed at an EU level, but in fact they have the freedom already to develop their own regulatory regime faster if they wished to. From the floor the issue was also raised that a single framework for security and border clearance operations is desirable despite the differences between local implementations, so as to avoid the potential development of bilateral port to port agreements.

The division of responsibility between stakeholders also differs between different countries making the development of a single decision making template more problematic. For example in Canada the Border Service mandate includes not only security but also the express need to facilitate legitimate travel, trade and the economy. In this case therefore it is not sufficient to rely solely on the private sector partner to provide a high service orientation, but it also falls on to the government agency as well.

Conclusions

The panelists, both from airport representatives and border authorities, all agreed that the ABC implementation in their locations were a success, and that they are now in an evaluation phase as to what the lessons are so that they can move to the next stage. In the future there is the potential to not only successfully automate a manual process but to reconfigure the base border process itself to take full advantage of the technological opportunities of ABC and biometrics.

The aim of such a reconfiguration would be to further speed up the facilitation of bona fide passengers while developing risk based security approaches for the small proportion of potentially risky travelers.

Parallel session 2: Why are risk management and vulnerability assessment important?

This session aimed to raise awareness about the importance of vulnerability assessment and testing as well as about the benefits of information sharing, albeit the high sensitivity of this subject matter. The main vulnerabilities of ABC systems and their known (an unknown) strengths and weaknesses both at the technical and operational level were discussed. The session also explored how to mitigate existing shortcomings to enhance the systems' robustness.

Moderator
Ted Dunston
Chair of the Technical Committee, Biometrics Institute, Australia

Opening the discussion, Ted Dunstone outlined the scope of the challenge facing border control in the age of automated checks. Referring to Donald Rumsfeld's now iconic distinction between types of threat, he outlined the state of play in terms of known and unknown strengths and weaknesses, real world biometric attacks, their implications and how to mitigate them, as well as the over-riding need to ensure vulnerability is included in the overall risk-management strategy of ABC systems.

On a more strategic level, he introduced the themes of existing methods for penetration testing, the current direction of research in the field, the need to encourage border management agencies to address potential vulnerabilities and ways forward in the sharing of experience on the topic.

Presenting the current state of play, he noted optimistically that after a slow start, things are now changing rapidly with new ISO standards addressing 'spoofing' rather than simply performance testing and that many governments now include "spoof resistance" in procurement specifications for automated systems.

However, vulnerabilities are still very real and ever easier to find, at least online. Mr.Dunstone presented some known spoofing methods including false fingerprints on invisible tape, sold complete with matching passports, and the well-publicised case of a Chinese national trying to fool authorities using a life-like latex mask and the phenomenon of certain medicines removing fingerprints.

Other methods meanwhile have become so mainstream, he noted, that a web search for Biometric Spoofing yielded 8,140,000 results with the results of more specific sub-categories bringing back equally alarming figures.

In such an environment, he concluded, it is essential that decision-makers are aware of the issue and willing to fund solutions as well as to improve communication between relevant authorities to increase understanding of how systems can be and have been tested.

The first speaker to address these topics was Günter Schumacher. He noted that the European Commission was involved in a number of research projects, most recently on false fingerprints with results to be released to member state authorities.

Mr. Schumacher went on to present his thesis that current approaches to testing the vulnerability of ABC systems underestimate the scale of the challenge and the complexity of the issue. He particularly emphasized the issue of the enrollment process of facial images which in most member

Speaker Panel
Sebastian Marcel
Head of Biometrics Group, Senior Research Scientist, Idiap Research Institute, Switzerland
Hans de Moel
Policy Officer, Royal Netherlands Marechaussee, the Netherlands
James Lipsett
Senior Analyst, Risk Analysis Unit, Frontex
Olivier Touret
Market Manager, Morpho, France
Gunter Schumacher
Principle Researcher, Joint Research Centre, JRC, European Commission

Fragment from the session

states is accepted with no security at all, which gives potential fraudsters the time to manipulate the image. The facial image is then included in a very secure document and becomes part of the security check.

Furthermore Mr. Schumacher raised the issue of the reliability and accuracy of performance figures. These are widely touted and often impressive, but are based on False Acceptance Rate and False Recognition Rate which are calculated under laboratory conditions and hardly ever use real imposters for this kind of performance testing. Current performance testing often does not properly assess an imposter's most likely attack on biometric verification, such as copying another face as closely as possible or 'morphing' faces together. Finally, he raised the issue of the security assessment itself. Is it a security system or a convenience system or both and what are the quantifiable security targets? Unless these parameters are clearly defined, be believes, it is hard to do a meaningful security assessment.

Hans de Moel then pointed out to the three essential elements of border checks: the person, the document, and other information e.g. in the form of checklists. Matching the biographical identity (name, age, title) with biometric identity (facial image, iris, fingerprint) is a process that has to be redesigned for ABC systems, starting with the face, he argued. He then showed a series of pictures with questions for the audience — Male or female? Same person or different person? Having established clear consensus from participants, he then presented the results of algorithms to the same questions, with radically different results. The conclusion was that facial algorithms do not always perform in the same way as human assessment, and we needed to find an answer to the question of at what level of certainty a person is allowed to pass.

Moving on to document authentication and their security features, again comparing human and machine performance, he asked the question: What can a document scanner do and what can't it do? And here the issue is software. Tests conducted in Portugal compared seven systems using 48 genuine and 48 forged documents. The discrepancies were stark with the lowest-scoring system detecting only 38 false documents while another recognised 68 as valid. Results were equally varied for false rejection. Mr. De Moel went on to show documents he had falsified himself — including using simple techniques— that had passed automated verification on four of the seven systems. He stated that vendors needed to address the vulnerability issues in ABC systems, and that everyone involved in the deployment of ABC systems had in fact a lot of work still to do in this area.

Sebastien Marcel then referred to the fact that Apple's iPhone5 with its cutting-edge fingerprint recognition system, bought for USD 365 million, was spoofed within 48 hours of its launch using a time-worn method known since 2001. He then posed three questions: How many spoofing attacks are there that we don't know about? Can we devise counter-measures and incorporate them into existing systems without increasing the false acceptance rates? And how can we certify biometric products with those anti-spoofing measures?

In answer to a question from the floor as to when a system can be considered sufficiently

secure, he responded that there would always be a trade-off between security and convenience and that those decisions depended on the level of risk a given authority considered acceptable. The moderator added that ignoring the issue was not an option. The important thing was to know that risks exist and to put in place appropriate measures to mitigate them.

The difficulty of measuring and quantifying risk in terms of evaluating specific vulnerabilities and the threats they imply was a subject addressed by Frontex's James Lipsett. The same methods may be used by someone trying to enter illegally or an organised terrorist group, though they represent very different levels of threat, he contended. Automated systems will never be perfect, he asserted, and should never be used in isolation, as human oversight by border guards remains essential. However it also needs to be remembered that the human element can also cause further vulnerability, and referred to a further challenge linked to imposter documents that are often recycled by diaspora communities of the same ethnicity.

Olivier Touret from Morpho gave the vendor's perspective. The security aspects of certain parts of ABC systems can be vigorously tested using sophisticated methods and their counter-measures tested as well, he claimed. Such work has been done on known threats such as false fingerprints but, applying it to a multi-component integrated system like an ABC solution is very challenging.

From a more operational viewpoint, however, it is more useful to look at more practical solutions. Here there are several important questions: What is the goal of the attacker? Is it to evade their own country's authorities or to enter another country without the right to do so? Is it to pretend a third party is crossing the border when in reality he or she is not? Will the attacker attempt to enter without leaving a record or leaving a record with false identity? All these aspects of the system need to be assessed. Are they 'attacking' the sensor, or using identity theft, vulnerabilities in the software or even employing cyber-attacks to get through surreptitiously. This creates what he called a matrix of risk.

Mr. Touret stated that in regard to this matrix of risks and vulnerabilities, he believes that the industry now has good and convincing answers and counter-measures. These include combined electronic and optical security features, solutions for forged names, sensing carpets, infra-red cameras, photo cells and others which, if used in combination, can offer a high level of protection.

The benefit of technology in this regard is its preventive capacity, he suggested. ABC software enables the detection of anomalies, i.e. things that are not yet at the level of threat but that show something is going wrong — potentially, unknown attacks. By combining multi-biometrics it becomes much more difficult to cheat the system. Additionally, it should be remembered that ABC systems should work in synergy with other operations, including better placement of human resources for oversight.

Conclusion

If there was one common theme, repeated by speakers, it was that ABC is here to stay and so is spoofing. And that whatever innovations border-control authorities implement, people-smugglers, human traffickers and other facilitators of illegal entry will adapt their methods to try and stay ahead of the game; a game that will often change but will never end.

DEBATE SESSION 4

The Societal implications of Automated Border Control

Moderator
Sadhbh McCarthy
Director, Centre for Irish and European Security, CIES, Ireland

Social acceptance and trust are key factors for the successful deployment of ABC. This session discussed societal considerations and concerns in relation to ABC systems and examined how these concerns are being addressed in ABC deployments.

Panel Speakers
Peter Hustinx
European Data Protection Supervisor, EDPS
Dalibor Sternadel
Parliamentary Advisor to Ioan Enciu MEP, Committee on Civil Liberties, Justice and Home Affairs, LIBE, European Parliament
Ann-Charlotte Nygard
Program Manager, Freedoms and Justice Department, European Union Agency for Fundamental Rights, FRA
Eric KK Chan
Director of Immigration, Immigration Department, Hong Kong, Special Administrative Region Government
Dominique Klein
Head of Sector, Transeuropean Networks for Freedom and Security and relations with eu-LISA, DG Home, European Commission

The session started by seeking to define the term "societal impacts" of ABC deployments. This can be seen as being a much broader issue than simply one of data privacy or technology issues. Any technology can bring about desirable and undesirable outcomes. In terms of traveller profiles there is no one-size-fits-all definition. They are diverse in terms of demography and ethnicity and it is important to ensure that one section of society does not benefit more from ABC technology than others. The aim must be to promote positive societal impacts and mitigate against the potential negative ones and ensure that all ABC deployments are to the potential benefit of all travellers.

The panel then started their discussion by looking at the issue in more detail of what are the societal or ethical implications of ABC. Mr. Sternadel from the perspective of the European Parliament recognized the need to both facilitate external cross border traffic and maintain security at a high level. He stated that there is concern that the new ABC developments and the Smart Borders package are not based yet on the principles of necessity and proportionality. In his view careful assessment should be done first of the existing large scale IT systems which have been put in place in the area of border management in order to learn the appropriate lessons before implementing on a broad scale the Smart Borders program and RTP.

In the opinion of Dominique Klein from the European Commission there are two major areas of societal or ethical issues related to ABC and border management. The first concerns the area of data privacy/protection, in particular as regards where is the passenger's personal data stored, how is it secured, are databases combined, and on what basis is information shared. Mr. Klein pointed out that these issues are in fact related to border management policy and not only to ABC as such as they also apply to manual border checks.

Secondly is the issue of universal access to the eGates. These are issues related to access for families and minors, the disabled, people with impaired sight, people who are too short to be able to be monitored by the sensors, people who are missing limbs so are not able to provide fingerprints, the elderly, and people who do not speak the language of use. He mentioned that human dignity was not solely related to societal issues and risks. On the other hand, Mr. Klein highlighted that ABC solutions are more egalitarian than humans, as they make no preconceived judgments of an individual.

In addition to this, the Panel also raised the issue that the traveller's right to information and redress must be respected. The passenger should be aware of what data is held, how it will be stored and for how long – an issue of transparency. Furthermore, they should be aware of their rights in terms of redress in case of a false rejection by the system, or if there is a technical problem with the machine while they are being processed. The traveller should be aware of his rights, know where the red

lines are in terms of data management and have access to legal redress and enforcement if necessary. It was confirmed that in the EU Smart Borders package there are a number of strong provisions which deal with these issues, providing protection to the citizen in the area of redress and data protection, backed up ultimately by the Court of Justice of the EU.

The challenge is to ensure that the convenience of eGates is not only available for a well educated, healthy businessperson who speaks fluent English and is travelling alone. It is recognized that enabling ABC access to 100 percent of travellers is impossible but all efforts should be made to ensure that the experience is not discriminatory, stigmatizing or humiliating. This is an issue of appropriate policy but also of technological solutions, which in many cases are in fact quite inexpensive and easy to implement.

The experience of Hong Kong shows that many of these issues can be addressed as part of an ABC deployment. The ABC system in Hong Kong is opt-in for residents who receive an eCard. Privacy and data protection issues were addressed from the program's inception, and are guaranteed by law, and only the minimum eCard data necessary for border control is displayed when the passenger passes through the ABC gates. The eGates can be used by all Hong Kong residents over the age of 11 and there is a special wide channel for wheelchair access. There are also channels available for the visually impaired which use voice navigation. In addition, a border guard can assist the passenger at all stages of the process if required.

From the perspective of the European data protection authority in the context of ABC deployments,Mr. Hustinx emphasized that this issue cannot only be perceived from the perspective of technological devices and efficiency. It always needs to be seen in the bigger picture of what will be the consequences of the implementation and use of these devices. A key concept is therefore impact assessment. This should be carried out as part of the planning process so that societal issues can be properly addressed prior to implementation. An example of where this was not done properly due to undue haste were early generation body scanners which did not have a proper respect for human privacy and dignity built in. This was rectified only with later models.

From the left: Sadhbh McCarthy CIES, Ireland; Peter Hustinx, European Data Protection Supervisor; Dalibor Sternadel, European Parliament

Another key concept is privacy by design, where data protection and privacy issues are built into the concepts from the very beginning. This is essential if proper societal control is to be exercised on new technological solutions such as ABC and the Smart Borders program. To build societal trust it is also necessary to have official institutions which safeguard the privacy laws and can enforce them if necessary.

Anne-Charlotte Nygard, from the Fundamental Rights Agency, addressed some fundamental rights implications of ABC solutions. She mentioned that whilst machines

do not discriminate, a denial to pass in an eGate could result in a passenger feeling singled out. Concerning the rights of children, Ms. Nygard suggested that it was necessary to consider the impact of the physical separation between the child and the parent. Additionally, she addressed the issue of human trafficking and how an identification of a victim could potentially be hindered by the absence of human contact from border control. The rights of persons with disabilities and the elderly were also mentioned, as ABC needs to have an adjustable physical design and time schedule adapted to these categories. Finally, Ms. Nygard also pointed out that there is a need to reassure the right to information and to protect the travellers against the wrongful use of data.

It was emphasized by Mr. Klein that without societal acceptance ABC solutions will be a failure as targets will not be met. In Europe the passenger will always have a choice between an eGate and a manual gate, something which will still apply when the EES and RTP programs are implemented. However, for all stakeholders it is in their interests to ensure that as many passengers as possible use the eGates as otherwise they will not meet their operational targets in terms of facilitation of legitimate travel in a secure way. The issue of whether sufficient resources are in fact put behind building societal acceptance and in educational programs was raised.

A very important plank in potentially building societal trust in such technological deployments is the work being done on updating the legal framework for data protection in the EU which is scheduled to come into force from spring 2014 and will impact on the area of ABC deployment – for example by mandating a privacy by design approach. This and other legal and policy initiatives at the EU level will only however set the framework and the stakeholders themselves will have the freedom and responsibilities to come up with the best solutions.

Hong Kong provides a good example of this in practice as without societal acceptance of their ABC solutions it would in fact be impossible to facilitate the scale of border crossings which they face and a double digit per annum traveller growth,without the possibility to increase their manpower by the same ratio per year. Societal acceptance in Hong Kong is also a result of the fact that fingerprint data on residents has been held for a long-time –since the 1950s and people are used to it, and also they trust that their data is protected and safe. Only the minimum data necessary is collected and if someone wants to withdraw from the program all their data is immediately deleted. Their ABC solutions were developed on the basis of privacy by design, and in fact they made changes to their plans on the basis of input from their Data Protection Commissioner. Hong Kong also invested time and money in informational and educational programs around the ABC gates, for example presenting the design options for ABC gates on their website and setting up mock up gates in offices and public places where people can try them and become accustomed to the technology in a neutral environment. It was stated that the ABC technology in Hong Kong is regarded as being convenient by passengers and is a natural part of life, just like the ATM machines mentioned on the first day of the conference.

For societal acceptance the panel agreed also that the border guard's professional judgment is still essential – both in terms of security issue(e.g. human trafficking, establishing adult/child relationship, victims identification) and in terms of respecting simple human dignity during a mainly automated process.

Conclusion

The main conclusions from this session was that societal acceptance of ABC is a requirement if they are to become a normal and intuitive part of the traveller border crossing experience, but ABC should be used as a tool which does not replace the human factor.

The Panel mentioned a number of key areas which will be required if this societal acceptance is to be achieved. These include ensuring that data protection and privacy controls are built into the technological solutions from their inception through the use of privacy by design and impact assessment, making sure that ABC solutions are available to a wide cross section of the travelling public on an equal basis, having clear and transparent redress procedures and finally consistent traveller information programs.

DEBATE SESSION 5

ABC and the future of border checks

Moderator
Tony Smith
Managing Director, Fortinus, former Director General of Border Force, United Kingdom

This session discussed future ideas as regards the integration of ABC solutions and other risk based facilitation initiatives into a broader management concept in order to provide increased security at the borders, a better traveler experience and improved overall cost effectiveness for the stakeholders involved.

Speaker Panel
Annet Steenbergen
Advisor, Preclearance Coordinator, Ministry of Integration, Infrastructure and Environment, Government of Aruba, Aruba
Matt Roseingrave
Customs Service's Counsellor, Embassy of Belgium, Bulgaria, Luxembourg, Romania, Sweden and Mission to the EU and NATO, New Zealand
Campbell McGhee
Biometrics Examiner, Police Forensics, Interpol
Edgar Beugels
Interim Director, Capacity Building Division, Frontex
Joao Nunes
Director, Lisbon Airport, Portugal
Jurgen Wachtler
General Operations Manager, Hamburg Airport, Airport Council International, ACI World

Tony Smith as moderator introduced the session about the future of ABC deployments and how they should be integrated into a broader set of risk based border management tools.

Annet Steenbergen presented how Aruba is progressing with its ABC deployment. For more than 20 years Aruba has hosted border pre-clearance for travellers to the United States so it already has considerable experience in such projects. Aruba is an overseas territory of the Netherlands, and its citizens hold Dutch passports (EU citizenship).

Ms. Steenbergen noted that Aruba is now working on a project called "Happy Flow" which aims to provide an integrated seamless passenger experience from curb to gate, with all government, airline and airport processes integrated with the support of ABC technology, eTokens and biometrics. This would then be linked with planned pre-immigration and customs clearance for travel to the EU Schengen area via Schipol airport in the Netherlands.

Currently Aruba is working on Step 1 of this project which is in the area of the curb to gate process integration at the airport. The goal of this is to both increase security and deliver faster traveller facilitation. In addition, it can potentially involve more satisfied vacation travellers, resulting in economic inputs for Aruba. Thus integration will include biometric enrollment of the traveller upon arrival to the airport, when he will receive a token. This token will then be used for identification at the flight check-in, bag drop, border check and flight boarding.

After Step 1 has been implemented the plan is to enable EU Schengen area pre-inspection and pre-clearance for immigration and customs (Steps 2 and 3 of the planned project). These steps are in the process of being discussed with relevant Dutch and EU authorities and if approved could possibly become a pilot program which could be extended to other EU member states' overseas territories.

Matt Roseingrave indicated that New Zealand is currently operating an ABC system which is available to New Zealand and Australian citizens who are holders of an electronic passport. In terms of the future, the New Zealand perspective is that this should also be in the area of creating a "traveller centric process", working with all the stakeholders, covering the whole process from arriving at the airport, to flight departure to arrival at the destination – to create a complete travel chain. The goal is to create an enhanced traveller experience which is largely self –directed, in which the traveller can navigate the system him or herself. In terms of security the goal is to manage threats as early in the travel chain as possible.

On the question of RTP programs and standardization issues, the point was raised that the best approach would be to have an internationally agreed set of minimum standards and then mutual acceptance between systems based on reciprocity. This would enable the passenger to use mul-

tiple systems based on one entry point – similar to the way that frequent flyer programs currently operate. On the subject of potential RTP implementation, Joao Nunes from Lisbon Airport in Portugal also suggested that a possible route would be a step by step implementation approach where for example, as a first step, EU citizens travelling from third countries could be processed via the ABC gates.

In the context of security, the conference was given an update on an Interpol project to add an international facial image database of most wanted criminals and fugitives to add to the already existing fingerprint and DNA databases. This database will greatly assist in crime prevention as it will be based on material from CCTV camera surveillance, and it is planned to go live in 2014, with high quality facial images. This system is being currently developed independently of border control issues, but it could possibly be integrated into border management security checks in the future.

From the airports operator perspective a number of key points were raised for the future, in particular, the need for collaborative decision making between all the stakeholders. The overall goal for every airport is always to ensure an efficient, managed traveller flow and to achieve this there must be a greater level of system interoperability and system harmonization than is the case currently. It is also important to remember that at the end of the day process optimization is only part of the picture – it is necessary to keep in mind the needs of the individual traveller and keep the system transparent and the traveller fully informed.

The panel agreed that two key trends are going to shape the future of ABC solutions in border management. Firstly ABC gates themselves are not a goal – they

From the left: Annet Steenbergen, Ministry of Integration, Infrastructure and Environment, Aruba; Matt Roseingrave, Customs Service's Counsellor, New Zealand; Tony Smith, Fortinus; Edgar Beugels, Frontex

are simply tools and are part of a complex multi-stakeholder chain. And secondly, the physical element of control at borders is going to decrease and the "virtual" control will increase – with "virtual" meaning data collection, processing and analysis. With this it is very important to ensure that it meets the twin goals of smooth and fast facilitation for the 99 percent of bona fide travellers with strong security.

A representative of the World Customs Organization further elaborated on how their organization approaches international cooperation and how this could perhaps serve as a template for mutual recognition of passenger RTP programs. The World Customs Organization sets a minimum set of global standards, which all member countries agree to adhere to when they are making their national customs programs. This makes the mutual recognition of programs much easier and this is supported by the exchange of information and validation. As with the flow of goods in trade, passenger travel is a chain and if it is looked

at in this way with international cooperation and multi-stakeholder cooperation (private and public) in a coordinated way then it should be possible to optimize total systems that use less resources and infrastructure than would be the case if they operated independently.

Conclusions

As a conclusion to the session it was reiterated that ABC solutions are not a goal in themselves and that they are part of a complex multi-stakeholder controlled travel process. Methods, standards and harmonized rules to support the facilitation of ever greater traveller flows while maintaining high security standards are essential and work should gather pace to build momentum behind these issues on a global level.

Closing Remarks

Edgar Beugels · *Interim Director, Capacity Building Division, Frontex*

In his concluding remarks to officially close the 2nd Global ABC Conference Edgar Beugels highlighted a number of key points which in his view came out from the two days of the conference.

Firstly the subject of the conference was ABC and its deployment, however very often during the conference the point was raised that ABC is only a part of a travel chain and it needs to be integrated with all the other steps wherever possible within the context of offering a service to the traveller whilst maintaining high security standards.

The "A" of ABC stands for automated, not automatic and another important theme was that the eGates are a tool in the hands of the border guard who remains essential.

The success of ABC implementations can be seen by the fact that travellers are willing to use them and upset if they do not work properly, and in this area the education and information the traveller receives in terms of how to use ABC gates was an important discussion point.

In terms of implementation the key theme of cooperation and collaboration in an atmosphere of mutual trust between public and private stakeholders was consistently raised.

In terms of security Mr. Beugels emphasized that all elements of the security chain including the check of the security features in the travel document are necessary, and if one element would be removed then security would be diminished.

Mr. Beugels then concluded by thanking the organizers of the conference and said that he hopes to see everyone again at the 2014 conference.

ANNEX 1

Extended Abstracts

Academic Session

Document Security in the Age of Fully Automated Border Control Systems

Michael Gschwandtner · *Austrian Institute of Technology, Safety & Security Department*
michael.gschwandtner@ait.ac.at

Svorad Štolc · *Austrian Institute of Technology, Safety & Security Department*
svorad.stolc@ait.ac.at

Abstract: Automated checking of identity documents is heavily used in border checks all over Europe. In the conventional scenario, document scanners are only assisting devices operated by trained border guards. In such a configuration the operator can compensate for classification mistakes made by the document verification subsystem, which is not possible in fully autonomous border control setting. In this paper we show possible risk scenarios in currently used optical security feature verification methods as well as electronic security feature verification.

Keywords: optical security features, electronic security feature, security documents, counterfeit detection, security analysis

INTRODUCTION

With the ever increasing number of travellers, border checkpoints are confronted with the necessity to increase the number of people to be processed. One popular solution to cope with such increased demand in almost any part of our daily lives is the automation. The same holds true for border checkpoints. Rise in demand is increasingly solved by putting automated border control systems in place. However, automating a process usually means that some steps have to be simplified. This can lead to a checking process which might be more vulnerable to certain attacks, when compared to a normal human-led border control [1].

In current border control scenarios, document scanners along with the document verification subsystem are mainly used as assisting devices. This configuration does not pose any serious security issue, as the final decision remains with the border guard operating the device. Therefore the document authentication can be tuned for maximum throughput even with the knowledge that some documents might slip through the automated check. On the other hand, in fully autonomous systems, such a bias towards acceptance of a document even if it might be forged or manipulated would have serious security implications. The tests in [1] show that current systems are already leaning towards accepting forged documents. In this paper we show that it is a non-trivial task to authenticate a document even if the automated document checks would be configured to be cautious and more likely reject a genuine document (false rejection) than accept a fake document (false acceptance).

OPTICAL SECURITY

Checking of optical security features is typically implemented by using special metrics (i.e., image quality metrics), which compare parts of the document against a reference stored in a database. This reference usually contains several numerical values such as mean and standard deviation, feature vectors characterizing certain areas within the document, reference image data like image patches, or even a sample of the whole document. The underlying assumption of those checks is that a counterfeiter cannot produce a document so that it would match the reference close enough to be ac-

(a) Original, (b) Rotated by 0.3 degrees, (c) Text overlaid increased brightness

Figure 1. **Three versions of the same image patch of a genuine passport**

cepted as genuine. However, in reality even the genuine document does not match the reference completely due to variations in the production process, aging, wear and tear, dirt, etc. Therefore the system has to allow for slight deviations from the reference, which in turn increases possibility to accept non-genuine documents.Image quality metrics are a thoroughly researched field in computer vision with a continued development of new methods to adapt to special requirements [4]. However, such metrics are not necessarily suited for detecting forgeries or document fraud.

In order to demonstrate problems which may arise from straightforward application of standard image metrics in the document authentication process, we conducted an experiment with the simulated modification of an Austrian passport. The original image patch extracted from a certain region of the genuine passport (see Figure 1a) was manipulated by using an image editing software and afterwards compared with the original unmodified image by means of commonly used image metrics. The image in Figure 1b was derived from the original image patch by a clockwise rotation by 0.3 degrees and a slight increase in brightness. The second manipulated image in Figure 1c has a faint text spelling "FRAUD" overlaid over an otherwise untouched image.

It is clear, that even an untrained human observer can immediately recognize the overlaid text in Figure 1c, even without any reference image available. On the other hand, the difference between Figures 1a and 1b may not be visible even for a trained border guard. However, with respect to many standard image similarity metrics, the image in Figure 1c is closer to the original than the one in Figure 1b. As a consequence of this, the underlying document of Figure 1c would be considered as more authentic than the document in Figure 1b (see Table 1). The biggest difference between the human observer and an automated method is that the human does not simply compare some values somewhat characterizing the document, but instead automatically reasons about the content of what he sees. Although a comparison of acquired images with the reference data based on image metrics is highly applicable in quality inspection tasks, if applied to the document authentication, where tailored attacks against a system must be expected, more sophisticated checks are inevitable.

In order to analyze the impact of an image manipulation on the real world document authentication, we conducted a second experiment with commercially available software that is nowadays in use at many

Table 1. **Distance between modified and original image patch of the passport image, using common image similarity metrics. The best values for each metric are marked with an asterisk**

	MSE	Normalized cross-correlation	Structural similarity
Rotated and brighter	25.360	0.974	0.931
Text overlay	*6.320	*0.975	*0.973

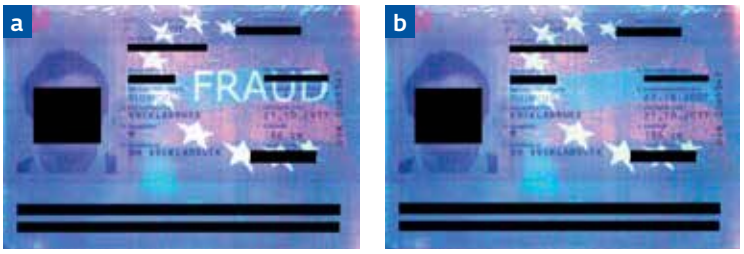


Figure 2. **Example of an UV image from a genuine passport (a) and a modified version of the same image (b). Both images are part of a visible light, UV and infrared image set and were considered as genuine by a commercially available document authentication system. The genuine passport has a similarity of 87% to the template in the database, while the modified passport has a similarity of 94% to the template in the database**

borders worldwide. The first step was to acquire a scan of a valid genuine passport. In our case, we used again an Austrian e-passport which at the time of our experiment was approximately 6 years old. The document scanner acquired 3 images associated with different spectral ranges: (i) visible light, (ii) infrared (IR), and (iii) ultraviolet light, denoted to as V_0, I_0, and U_0, retrospectively.

In Figure 2, one can find the acquired UV image U_0(a) and the manipulated image U_1 (b) derived from U_0 by overlaying the text "FRAUD" in big semi-transparent letters. The tuple (V_0, I_0, U_0) represents a genuine passport and the tuple (V_0, I_0, U_0) represents a passport with an obvious modification. Although the document authentication system is in principle a "black box", it does provide a list of checks performed during the verification process along with similarity scores and boolean flags signaling the decision for each individual feature. The similarity score, given in percent, determines how similar the acquired image is to the template stored in the database. The boolean value determines whether the similarity exceeds given threshold, meaning that the feature can be considered as genuine. The comparison of the genuine passport (V_0, I_0, U_0) against the template results in a similarity score of U_0 of 87%. The comparison of the modified passport (V_0, I_0, U_0) results in a similarity score of U_1 of 94%. Making decision just based on these numbers, one would consider the modified image U_1 (shown in Figure 2b) as significantly more authentic than the genuine image U_0 (shown in Figure 2a), even though any human observer would tell otherwise.

To increase the robustness against forgeries while maintaining the usability of a system, a number of security features are validated at once, where each feature has its own independent acceptance range. Correspondingly security documents should be designed so that a counterfeiter might be able to forge few isolated features, but it should be virtually impossible to produce a complete document falling within all acceptance ranges at the same time. In order to achieve this goal, security documents usually contain several security features operating in different spectral ranges [2]. Manufacturers of security documents use materials and inks that have special spectral properties very different from materials and inks available on a public market. Note that the precondition of this approach to the document security is that such materials are regulated by official authorities worldwide and cannot be bought through other than official channels.

Nevertheless, there exists a generic attack on optical security features, regardless of the spectral channel [3]. This attack utilizes electronic displays to simulate the expected responses of valid documents and exploits the fact that the document scanner has currently no way to perform the implicit task of ensuring that the presented document is in fact a real document. Such a task is performed by a border guard without even thinking about it.

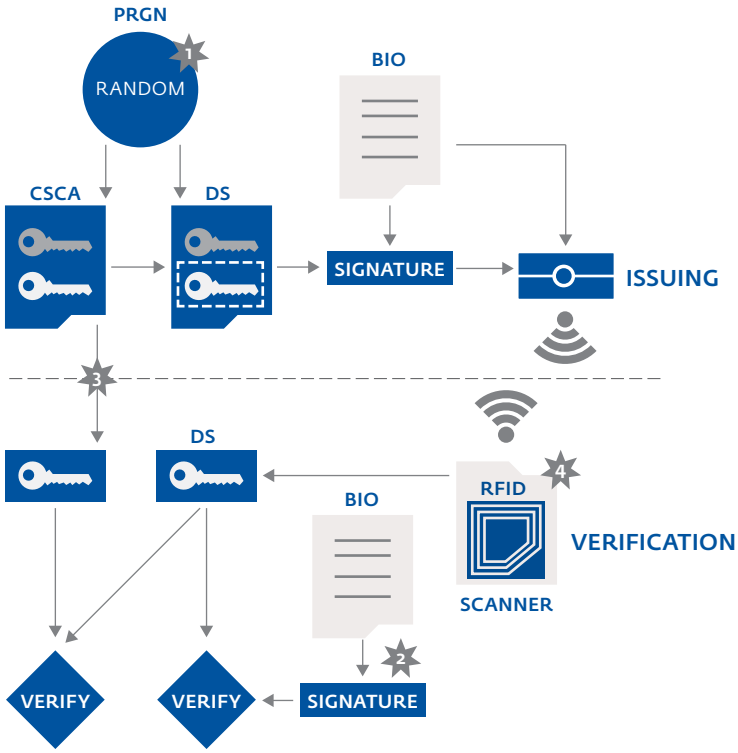
ELECTRONIC SECURITY

The electronic part of an e-passport is often cited as the be-all and end-all solution for securing identity documents. Although it is, under some circumstances, possible to clone a valid e-passport, there is still no known attack that can create a forged document. Nevertheless, replacing the current e-passport, containing both the optical and electronic security features, by a chip-only solution would cause the electronic part of the current passport to become the sole security feature, which might result in additional security risks.

The schematic in Figure 3 shows the most important parts involved in the issuing and verification of an e-passport with basic authentication (BA). It starts with the initial creation of the country signing certificate authority (CSCA) through the embedding of the biographical data (BIO) to the verification of the signature and the extracted document signer key (DS). Even though cryptoanalysis has not yet found a practical weakness in the signing process of current e-passports, the whole process has several attack vectors that range from man-in-the middle attacks up to social engineering. The following is a list of a by far non-exhaustive list of possible attack vectors on the current security model of electronic passports:

- Point 1 in Figure 3 shows possible problems with the creation of the CSCA and the DS itself. If the quality of the random number generator is too low, the resulting certificates are prone to attacks. Weak random number generators have been found for example in some versions of OpenSSL and some versions of Microsoft Windows.
- Point 2 is the signature creation itself. An attacker does not need access to the private signing keys in order to create a valid signed passport. He needs to store data which has the same hash values (also called collision attack) as the original passport it is derived from. While the currently used hashing functions are designed to be robust against collision attacks, cryptoanalysis has already found weaknesses in cryptographic hash functions that have previously been thought secure (e.g., MD5, SHA-0). Fortunately, this does not yet include hash functions used in electronic passports.
- Point 3 shows the transmission of the CSCA public keys to the participating countries. Some countries prefer to download them directly from the official servers of other countries, but these official servers are reached through conventional (insecure) connections. Other possibilities to compromise the trans-

Figure 3. **Schematic of the passive authentication. Gray stars mark a non-exhaustive list of possible attack vectors**



mission of the certificates are for example compromised web servers and DNS cache poisoning attacks.
- Point 4 shows the scanner itself which might get compromised by a malicious service technician. The simplest attack would be to introduce a fake CSCA certificate resulting in the ability to issue fake passports that cannot be detected.

CONCLUSIONS

We have shown that current optical security checks are insufficient to authenticate secure identity documents and thus might pose a problem for fully automated border control. In addition, the obvious solution to rely solely on the electronic security of current e-passports should be handled with care, unless one can guarantee with absolute certainty that no part of the whole issuing-verification chain can be compromised: neither through technical attacks nor through a social engineering. As a result of this work the research in automated checking of optical security documents should be increased and based on academically researched and publicly verified methods rather than commercial "black box" systems. An example for public research in this field is shown in [4].

ACKNOWLEDGEMENTS

The work has been supported by the *FastPass* project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007–2013) under grant agreement n° 312583.

REFERENCES

1. Gariup, Monica and Soederlind, Gustav. "Document Fraud Detection at the Border: Preliminary observations on human and machine performance", in Workshop on Innovation in Border Control (WIBC), 2013.
2. Gschwandtner, Michael and Štolc, Svorad and Vrabl Andreas. "Active display attack on automated security document scanners", (to appear) in Optical Document Security (ODS), 2014.
3. Khan, Zohaib and Shafait, Faisal and Mian, Ajmal. «Towards Automated Hyperspectral Document Image Analysis», (to appear) in 2nd International Workshop on Automated Forensic Handwriting Analysis (AFHA), 2013.
4. Ryu, Seung-Jin and Lee, Hae-Yeoun and Cho, Il-Weon and Lee, Heung-Kyu. "Document Forgery Detection with SVM Classifier and Image Quality Measures", in Advances in Multimedia Information Processing (PCM), 2008.

Dependability Management In Automated Border Control

Toni Ahonen · *VTT Technical Research Centre of Finland, P.O. Box 1300, 33101 Tampere, Finland*
toni.ahonen@vtt.fi

Laura Salmela · *VTT Technical Research Centre of Finland, P.O. Box 1300, 33101 Tampere, Finland*
laura.salmela@vtt.fi

Abstract: Expanding ABC deployments place dependability management at the forefront of system development. Current literature on immigration-related biometric applications is extensive and encompasses a wide range of perspectives to the technology and its application in different settings. However, issues associated with system reliability in terms of availability performance have received limited attention. Depending on the number of e-Gates, passenger volumes and set capacity levels, the failure of even a single e-Gate may significantly impact service availability and hamper passenger experience at a particular site. This paper addresses the practical relevance of systematic dependability management in automated border control. Depandability management has to form a strongly structured yet an integrated entity in the whole ABC development process. It supports the optimisation of border control capacity with respect to manual and e-service and other resources. Dependability management enables cost-effective operation for both system suppliers, maintenance suppliers, and most importantly, system owners.

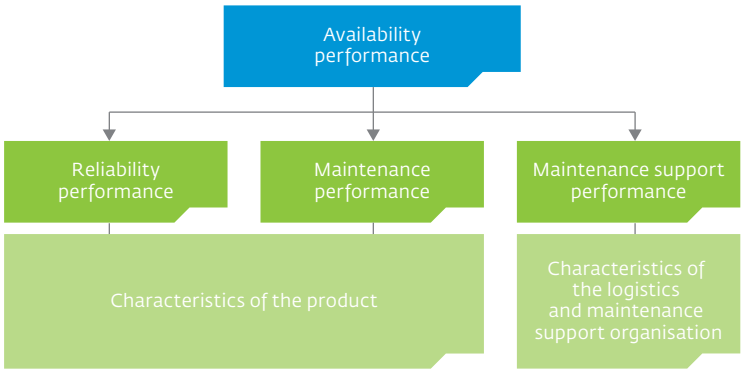
Keywords: Automated border control, dependability management, reliability, availability, maintainability.

INTRODUCTION

Passport inspection as self-service is becoming more and more everyday phenomenon in air travel in Europe. Access control based on biometrics such as automated border control systems are perceived as the key instrument in processing increasing amount of passenger traffic in a convenient and fluent manner (e.g. Morosan 2012, Jain and Ross 2008, European Commission 2013). Along with expediting border check processes, the installation of e-Gates is also expected to produce cost-savings as it alleviates budgetary pressure towards border controlling authorities in terms of reduced need to employ additional staff (Home Office 2012). Announcements of further deployments reaching a significant scope have been made for example by Germany. By the end of 2014, 90 new e-Gates will be installed to the country's five large airports. The signed ten-year contract also includes a reserve of 180 additional gates (i.e. Secunet 2013, Planet biometrics 2013). In the near short-term, notable investments are also to be made in the UK, as automation is designed to form the country's "primary clearance route for low risk passengers" (Home Office 2012, 29).

Despite new installation notifications, automated border control is yet to develop as off-the-shelf. As according to a UK Border Force official, "e-Gates delivery will be based on a continuous improvement cycle" (Border Force 2012). Nevertheless, the changing ratio between manual and e-service inclines rather strict requirements to future e-Gates. If e-service is to emerge more as 'mandatory' than optional for service choice, the operational reliability ABC systems will have a much higher weight in determining the fluency of overall border clearance processes. Depending on the

Figure 1. **System availability performance (modified from IEC 60300-1)**



number of e-Gates, passenger volumes and set capacity levels, the failure of even a single e-Gate may significantly impact service availability and hamper passenger experience at a particular site.

Given the intensifying competitive environment within airport markets (Hvidt Thelle et al. 2012), each point of engagement of a passenger needs to support the commercial relationships between different stakeholders (most notably airlines and airports). Even short ABC system downtimes at peak hours may significantly alter passenger perceptions of service quality (more on customer satisfaction formation and self-service technologies, see i.e. Meuter et al. 2000, Forbes 2008, Robertson et al. 2012). In the airport environment, the number of passengers influenced by an abrupt service failure due to hardware deterioration or software error may be particularly high. Moreover, ensuring the safety and integrity of maintenance activities often requires the built-up of temporary protective structures, such as full-height boarding which changes the flow of people through terminal facilities. Meandering passenger itineraries may cause congestion and potentially restrain access to more commercially-oriented establishments, such as foodservice or shopping. Furthermore, transferring customers to minimised manual capacity may cause severe delays in throughput times and frustrate system operators and administrators as the agreed service levels become unmanageable, even if it would concern a limited period of time.

Current literature on immigration-related biometric applications is extensive and encompasses a wide range of perspectives to the technology and its application in different settings. However, issues associated with system reliability in terms of availability performance have received limited attention (e.g. Palmer 2007, Optimum Biometrics Labs 2008). As such, the scholarly effort dedicated to dependability management in different settings has been versatile (e.g. Kiritsis et al. 2003, Zio 2009, Söderholm and Norrbin 2013), and there is also a variety of guidelines, models and methodology available for practitioners (e.g. O'Connor 2002). The expanding scope of ABC deployment nevertheless places dependability management at the forefront of system development. This paper addresses the practical relevance of dependability management in the area of technology-enabled border checks. The findings presented here are based on research work of the FP7 integration project FastPass.

DEPENDABILITY MANAGEMENT

The IEC 60300-1 standard defines *availability performance* as "the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided" (IEC 60300–1 2003, 25). In contrast, dependability unites availability performance and its influencing factors under one title. From a broad perspective, dependability expresses the confidence and satisfaction levels that users have towards a product's ability to reach expected performance. A dependable item is a product

that will deliver anticipated service upon demand. (IEC 60300–1 2003) The examination of system availability performance often involves the use of the acronym RAM which integrates the concepts of reliability, availability and maintainability. In this paper, availability performance and RAM are used interchangeably. The relationships between the different components of performance are illustrated in Figure 1.

In the context of biometrics, reliability tends to be associated with the system's performance in terms of accuracy (e.g. Jain and Ross 2008, Schouten and Jacobs 2009, Spreeuwers et al. 2012). Reliability is used to determine how the biometric system performs its matching function (measuring and evaluating system performance through i.e. FAR and FRR). More importantly, it indicates how different performance rates and their alteration affect the overall security and efficiency of the border check process.

Conversely, in dependability management, *reliability* refers to "a characteristic of an item, expressed by the probability that the item will perform its required function under given conditions for a stated time interval" (Birolini 2010, 2). In addition, *maintainability performance* is defined as "the ability of an item under given conditions of use, to be retained in, or restored to a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources" (IEC 60300–1 2003, 25). Finally, *maintenance support performance* characterizes "the ability of a maintenance organization, under given conditions, to provide upon demand, the resources required to maintain an item, under a given maintenance policy" (IEC 60300–1 2003, 25). Usually, the reliability and maintainability aspects of a product or a system are largely defined through decisions made during product development process (e.g. choices concerning component quality, system configuration and accessibility). Correcting the misguided choices made at the beginning of the product development process may prove costly or in some cases impossible correct at the later phases of the product's lifecycle. (Dhillon 1999)

Managing the dependability of a system and performing the required tasks defined in a RAM programme demands a definition of an appropriate system lifecycle. As emphasized above, the whole lifecycle of a product needs to be considered as early as possible in product development process (Murthy and Blischke 2009). While the phases of concept development and requirement definition to a large degree define the basis for lifecycle costs and dependability management of a system, dependability tasks have to be planned for the whole lifecycle. Figure 2 presents a generic lifecycle model which can be adopted as a top-level framework for discussing the requirements for system lifecycle management.

More specifically, the lifecycle model offers a platform for managing the dependability features of the system. In parallel with a holistic analysis of a system's lifecycle, the lifecycles of each individual subsystem and component at the lower levels of system hierarchy need to receive careful attention.

GENERAL GUIDELINES FOR RAM PROGRAMME

Successful management of the availability performance of an automated border control system requires the construction of an appropriate RAM programme. In order to support important aspects of the reliability performance, maintainability performance and maintenance support performance,

Figure 2. **A generic lifecycle model for a technical system (modified from Ulrich and Eppinger 2004)**

the following non-exhaustive list of general guidelines are proposed for system designers:

- specification, evaluation and allocation of dependability objectives based on end-user engagement providing a ground for the other RAM tasks (customer requirements for availability, pursued warranty period failure rate and warranty costs, pursued life cycle costs and costs related to reliability improvement)
- adoption of a deductive top-down approach guaranteeing that further maintenance and other actions focus to the most critical system parts,
- implementation of failure analysis studies (e.g. Failure mode, effects, and criticality analysis (FMECA) and Fault tree analysis (FTA)) for the different phases of the project starting already as a concept phase reliability risk analysis,
- implementation of an iterative maintainability study for early versions of the system design with a focus on safety issues, accessibility, working positions, competence requirements, needs for special equipment and time consumption of maintenance activities,
- acquisition and management of reliability-related data from equipment currently in operative use,
- exploitation of reliability-related data in system design.

The creation of a detailed availability performance programme should strongly take into account the system owner's point of view and consider the following aspects: 1) use and application of the system (e.g. expected passenger capacity, utilization rate and specific modes of operation in different border types), 2) definition of failures in the context (e.g. functional failures in passport scan), 3) use environment (e.g. system exposure to stress), and 4) environmental conditions (e.g. temperature and concentration of dust and dirt).

PRACTICAL IMPLICATIONS

The architecture of an ABC system integrates several technologies (hardware and software components), some of which may not share similar durability to extensive use rates and use modes. Furthermore, the mechanical and moving parts within each individual component may pose different kinds of reliability risks. Enhancing *the reliability performance of ABC systems* thus requires a careful analysis of the reliability structure of the whole system. This entails the identification of the most critical system parts upon which further decisions are to be made (design phase decisions or preparedness during the lifecycle). Customarily, the allocation of resources and reliability improvement efforts to most critical system parts results in best outcomes. Maintaining an up-to-date criticality assessment of the system also serves as a source of information for planning maintenance efforts taking into account also the availability of spare parts. Considering a line of several e-Gates, reliability bottlenecks resulting in common-cause failures should be avoided whenever possible. The solutions for potential common-cause failures can vary from the component selection decisions and inclusion of redundancy in the system design to maintenance strategy decisions, such as setting up the require-

ments for maintenance response times and availability of spare parts. If the border check process would be integrated to a whole series of airport processes, the reliability structure of the system would also become more complex. This might also influence degree of required maintenance work and potentially impose additional maintenance costs.

With respect to *maintainability performance*, one needs to recognise that biometric systems are under continuous improvement and development cycle. Subsequently, within the lifecycle of the whole system several upgrades will and need to eventually happen. Thus, the introduction and integration of new technologies and solutions as add-ons or updates to the current system should be allowed as much as possible. Furthermore, the system should have replaceable parts in reasonable units to allow the technological development and daily maintenance. In practice, modularity should be introduced into the system to minimise the Mean-Time-To-Restoration (MTTR) and to lower costs and time required for system upgrades. It must be ensured that the software can be updated during the lifecycle, and that the repair of failures (and software updates) does not require the whole hardware being replaced.

Considering *the maintenance support performance of an ABC system*, the lifecycle support from component suppliers needs to be adequate. Reliance on single contractors should be minimised allowing system owners to arrange maintenance activities according to their strategic choices and needs. Overall, attention should be paid to measures that minimise administrative delays, mean logistic delays and the probability of spare parts shortage. Enhancing remote diagnostics or remote software updates might promote cost-savings for both suppliers and system owners, and at the same time improve MTTR of the system.

CONCLUSIONS

In this paper, we have discussed the design of ABC systems from the perspective of dependability management. The practical implications presented in this paper emphasise the role of systematic dependability management methods in guaranteeing the overall effectiveness of an ABC system over its lifecycle. Dependability management has to form a strongly structured yet an integrated entity in the whole ABC development process. In order to reach this, continuous and solid collaboration between various stakeholders during the system's lifecycle is required. It supports the optimisation of border control capacity with respect to manual and e-service and other resources. Dependability management enables cost-effective operation for both system suppliers, maintenance suppliers, and most importantly, system owners.

ACKNOWLEDGEMENTS

The work for this conference paper has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007–2013) under grant agreement n°312583. This publication only reflects the authors view and the European Union is not liable for any use that may be made of the information contained therein.

REFERENCES

1. Birolini, A. *Reliability Engineering. Theory and Practice.* Berlin Heidelberg: Springer-Verlag, 2010. 6th edition.
2. Border Force. Border Technology Programme UK Border Automation – The Story So Far. Conference presentation made at the First Global ABC Conference & Exhibition organised by Frontex in Warsaw, 25 October 2012.
3. EN-50126. 1999. Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). European Committee for Electrotechnical Standardization - CENELEC.
4. European Commission. 2013. 'Smart borders': enhancing mobility and security. Press release. 28 February 2013. Accessed 2 September, 2013. http://europa.eu/rapid/press-release_IP-13-162_en.htm]
5. Forbes, L. 2008. "When something goes wrong and no one is around: non-internet self-service technology failure and recovery." Journal of Services Marketing 22: 316-27.
6. Home Office. 2012. "Home Office digital strategy." Accessed 30 August, 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/147943/strategy-document.pdf
7. Hvidt Thelle M., Pedersen, T., Harhoff, F. 2012. "Airport Competition in Europe." Copenhangen Economics. Accessed 1 September 2013. http://www.copenhageneconomics.com/Website/Publications/Competition.aspx?M=News&PID=2030&NewsID=498
8. IEC 60300-1. 2003. Dependability Management. Dependability management. Part 1: Dependability management systems. International Electrotechnical Commission, Geneva.
9. Jain, A. K., Ross A. A. 2008. "Introduction to Biometrics" in Handbook of Biometrics, edited by Anil K. Jain, P. Flynn, and Arun A. Ross, 1–22. New York: Springer, 2008.
10. Kiritsis, D. Bufardi, A. Xirouchakis, P. 2003. "Research issues on product lifecycle management and information tracking using smart embedded systems". Advanced Engineering Informatics 17: 189–202.
11. Meuter, M., Ostrom, A., Roundtree, R., Bitner, M. 2000. "Self-service technologies: Understanding customer satisfaction with technology-based service encounters". Journal of Marketing 64: 50–64.
12. Morosan, C. 2012. "Biometric solutions for today's travel security problems." Journal of Hospitality and Tourism Technology 3: 176–195.
13. Murthy, D.N.P., Blischke, W.R. *Warranty management and product manufacture.* London: Springer. 2005.
14. O'Connor, P.D. T. *Practical Reliability Engineering.* Chichester: John Wiley & Sons Ltd. 2002. 4th edition.
15. Optimum Biometric Labs. 2008. "Reliability, availability and maintainability of biometrics." Biometric Technology Today, March.
16. Palmer, A. 2008. "Criteria to evaluate Automated Personal Identification Mechanisms." Computers & Security 27: 260–84.
17. Planet Biometrics. 2013. "German eGate contract largest in Europe". Accessed 30 August 2013. http://www.planetbiometrics.com/article-details/i/1701/
18. Robertson, N.; McQuilken, L.; Kandampully, J. 2012. "Consumer complaints and recovery through guaranteeing self-service technology." Journal of Consumer Behaviour 11: 21–30.
19. Schouten, B., Jacobs, B. 2009. "Biometrics and their use in e-passports." Image and Vision Computing 27: 305–12.
20. Secunet. 2013. "Bundesdruckerei and secunet to deliver automated border control systems for German airports." Accessed August 30, 2013. http://www.secunet.com/en/the-company/news-events/news-events-in-detail/news/bundesdruckerei-und-secunet-liefern-automatisierte-grenzkontrollsysteme-fuer-deutsche-flughaefen-2/
21. Spreeuwers, L.J., Hendrikse, A.J., Gerritsen, K.J. 2012. "Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at Schiphol Airport." Conference paper. 2012 BIOSIG - Proceedings of the International Conference of the Biometrics Special Interest Group. 6–7 September 2012.
22. Söderholm, P., Norrbin, P. 2013. "Risk-based dependability approach to maintenance performance measurement." Journal of Quality in Maintenance Engineering 19: 316–29.
23. Ulrich, K., Eppinger, S. *Product Design and Development.* New York: McGraw-Hill. 2004. 3rd edition.
24. Zio, E. 2009. "Reliability engineering: Old problems and new challenges." Reliability Engineering and System Safety 94: 125–41.

Visual Surveillance Technologies for Enhancing ABC Secure Zones

Csaba Beleznai, Stephan Veigl, Michael Rauter, David Schreiber, Andreas Kriechbaum · *AIT – Austrian Institute of Technology, 1220 Vienna, Austria*
csaba.beleznai@ait.ac.at

Abstract: Traveller flows and crossings at the external borders of the EU are increasing and are expected to increase even more in the future; trends which encompass great challenges for travellers, border guards and the border infrastructure. In this paper we present three non-intrusive, vision-based technologies and research contributions addressing relevant security and efficiency requirements of border check procedures: (i) counting and separating humans within an eGate, (ii) robust left item detection in secure zones and (iii) estimating the queue length and the number involved persons at border crossing.

The proposed computer vision-based technologies will reduce delays and queues for travellers; improve the user experience at the border infrastructure, and at the same time support border guards in achieving a higher level of security by preventing unauthorized border crossings.

Keywords: visual surveillance, ABC secure zones, pedestrian detection, left luggage detection, queue length estimation

INTRODUCTION

The increasing worldwide travel capacities at airports pose new challenges in the area of border and security control. Travelers request a reduction of delays in the immigration process and a convenient, non-intrusive, attractive border crossing, while border guards must fulfill their obligation to secure the EUs borders against illegal immigration, terrorism, crime and other threats. Infrastructure providers demand maximum border crossing throughput and minimal border crossing area. An automated border control system shall accelerate the border control process by increasing the passenger throughput while maintaining the highest level of security.

Motivated by these challenges we propose several key technology elements targeting secure zones of an ABC infrastructure and its users: travelers and operators such as border guards. In line with the proposed 'smart border package' of the European Commission issued in 2013, our goal is to speed-up, facilitate border control processes and reinforce border check procedures at the external borders of the EU.

Our paper provides a task-oriented view on three computer vision based technologies addressing relevant security and efficiency requirements of ABC secure zones such as at airports. At the same time we also provide a detailed description of the proposed methodologies by putting them into scientific context and outline their advantages over existing technologies.

The addressed key challenges and the respective proposed technology components are:

- A vision-based solution to the problem of detecting tailgating/piggybacking events (person tagging along with another person) within eGates of an Automated Border Control infrastructure. The proposed user-friendly system facilitates the work of border guards and saves time for additional measures to prevent illegal immigration.
- A reliable left item detection framework operating within the eGate and providing immediate alerts on left-be-

hind items of various dimensions and appearances.
- A stereo vision based queue length detection framework which can successfully discriminate between waiting passengers and other slowly moving and stationary objects such as carried luggage pieces and other scene objects, also characterizing the dynamics (estimated waiting time) of the queue.

The above vision-based technologies all exploit the advantages of stereo vision based depth sensing, which allows for enhanced visual analysis in terms of more robust object detection, segmentation and tracking. Robustness in this context refers to the improved characteristics that the analysis can well cope with scene illumination variations, shadows and reflections, and occlusions between passenger-passenger and scene objects. Furthermore, the spatial sensing capability of these detection technologies allows for an easy registration into the global spatial context of the ABC infrastructure environment, thus detection results and associated alerts can be spatially referenced with respect to the infrastructure or to an existing surveillance camera network layout.

OVERVIEW

Major factors for security and mobility at airports are secure and efficient border control procedures and flexible management of traveler flows. All travelers wish to cross external borders with maximum convenience and without losing too much time at border controls. At the same time border guards must still fulfill their obligation to secure the EUs borders against illegal immigration, terrorism, crime and other threats.

Vision sensors and associated image analysis provide new means to assess relevant indicators on the presence and flow of passengers and on the specific location they are situated in. Typical observation scenarios in relevant secure zones at borders are complex: high density of passengers, many non-stationary objects (luggage, carts, and dividers) and variable illumination conditions. Traditionally, visual surveillance at borders and airports is a commonly used technology to support the task of border guards, by complementing human vigilance or providing additional information such as the estimated number of persons within an area. Fully automated surveillance, however, is nowadays still in a developing phase where it is increasingly becoming capable to meet the strict accuracy requirements imposed at border crossings.

In this paper we propose the deployment of a depth-sensing stereo camera sensor, which is the result of several years of hardware and software development at the AIT [1]. A real-time stereo matching process [1] outputs depth data, which well represents the scene geometry and it remains invariant with respect to illumination variations and shadows. The combination of this depth information with color image data (originating from one camera of the stereo setup) results in a significant increase in robustness when compared to conventional vision-based solutions. In the following we present the individual depth-sensing vision-based technologies in more detail.

ABC-ENHANCING VISUAL SURVEILLANCE TECHNOLOGIES

The process of eGate operation when using the proposed vision-based technologies is depicted in Figure 1. An outward facing stereo camera setup is observing the queue in front of the eGate and a visual analysis estimates the length of the queue. The queue length estimate can be used to provide an estimated waiting time in front of

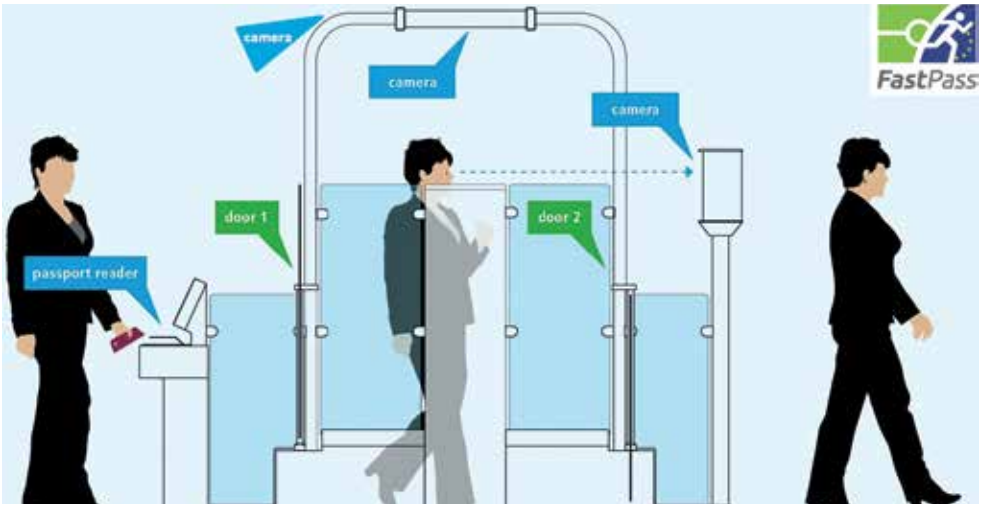


Figure 1. **Illustration for an integrated two-step border control process also depicting the employed camera setups**

the given eGate to both the border control operators and the travelers. When a traveler approaches the eGate, he places his ePassport on the passport reader, which then authenticates the ePassport, including electronic and optical security checks. If reading has succeeded, the first eGate's door opens automatically, and the passenger goes through the eGate. During his walk, recorded live images of his face are captured, and compared against the picture stored in the chip of his ePassport. In addition, a security check is performed against the Schengen Information System (SIS). At the same time, a surveillance system (top view sensor) ensures that only a single person is present inside the eGate (person separation). Once the identity of the (single) passenger has been authenticated, the second door opens automatically, and the passenger steps out of the eGate. The opening of the second doors activates the left luggage detection module. In case that any item was left behind in the eGate, the second door opens again, enabling the passenger to return and pickup his luggage.

Person counting and separation: In order to find human candidates within the eGate's volume, an area of interest is analyzed with respect to local maxima in the depth data which is computed from the images of the top-view stereo camera setup. The stereo camera setup is calibrated offline. The algorithm is designed to separately detect persons walking close to each other (piggy-backing) and to robustly discriminate between varying person-luggage (e.g. person carrying a backpack) and human-human configurations. Our algorithm is capable to detect and separate persons with varying body proportions,

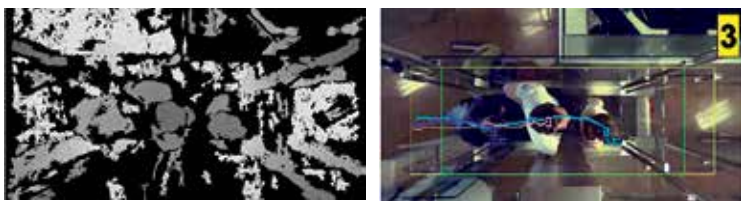


Figure 2. **Left: An example depth image depicting three persons. Bright areas are far from the camera (ground floor), dark areas are close. Entirely black regions do not contain any depth information Right: Corresponding detection, tracking and counting results and the estimated number of persons within the eGate**

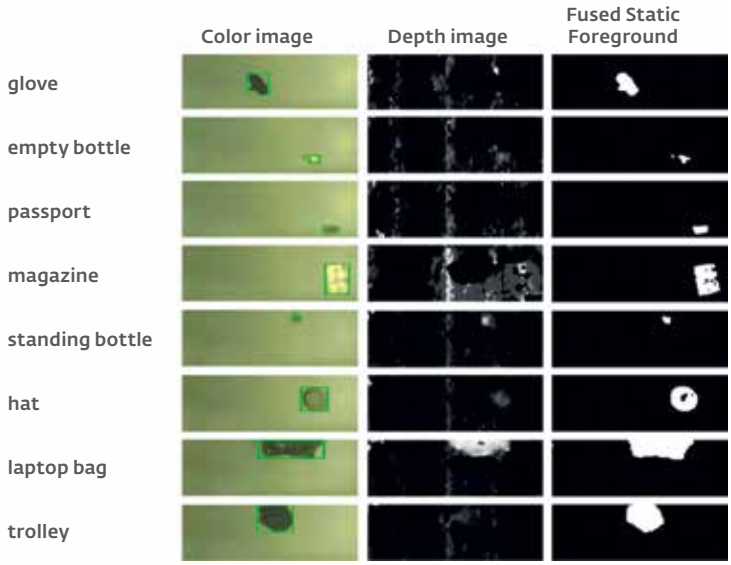


Figure 3. **Examples for left luggage detection. Color image with detected bounding box (left), depth image (middle) and resulting static object detection results after fusing color and depth information (right)**

clothing and hairstyles. We have evaluated our detector on a test data set of 5184 positive (piggy-backing attempt) and 7344 negative (no abnormality) samples. The rate of successfully detecting the critical events (true positive detection rate) of 0.93 and a correct recognition rate of normality (true negative detection rate) of 0.99 were achieved on the test data set. More details on the detection system can be found in [2] and [4]. The proposed depth sensing person detection and separation framework runs at a frame rate of 15 *fps*. This observation speed implies a great number of measurements during the traveler's presence within the eGate and it enables the high accuracy of proposed critical event detection.

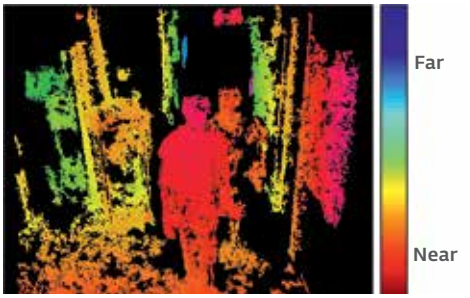


Figure 4. **A sample depth image showing two persons waiting in front of an eGate. Color coding represents the distance from the camera, as indicated by the color scale (right)**

Left luggage detection: Our left luggage detection module is based on the fusion of color- and depth-based change detection and static object delineation, both employing a reliable and efficiently computable background subtraction method [3], [4]. An image region is considered as static if it persistently reappears as a foreground region (deviation from a learned background) over a longer period of time. Each (depth and color) static object detection procedure produces an object segmentation estimate, independently from each other. Due to this independence the delectability in complex situations is enhanced: flat objects (such as a dropped passport) generate a change in the color image, but not in the depth image; while poorly contrasted objects (e.g. a trolley with the same color as the eGate floor) are difficult to detect in the color image, but they produce a marked depth deviation. The individual static object estimates (segmented regions) obtained for color and depth cues are fused via a union operation resulting in a reliable detection performance for various types of left objects (see Figure 3). The left luggage detection module is synchronized with the eGate's door signals. Thus, the analysis is stopped during the period where the traveler is inside the eGate, and detection of left items is activated for a short period of time after the person has left the eGate.

Queue length estimation: The depth sensing capability of the outward facing ste-

reo camera setup (see in Figure 1) can be well applied to estimate and monitor the number and dynamics of travelers waiting in front of an eGate up to a distance of approximately 12 meters. Depth images provide valuable visual hints where individual travelers are located (see Figure 4), since the measured depth ordering reveals how the individual, partially occluding persons are spatially arranged within the queue. Combining depth information with color image data furthermore enables a reliable long-term tracking of various parts of the queue, thus characterizing queue dynamics and providing information with respect to an estimated waiting time. Our queue length estimation framework is currently in development; nevertheless, initial results show that difficult indoor and outdoor situations can be successfully analyzed; scenarios where conventional single-camera surveillance solutions typically fail.

CONCLUSIONS

In this paper we presented a set of relevant vision-based technologies for supporting border guards in achieving a higher level of security by preventing unauthorized border crossings, and at the same time improving user experience at the border infrastructure. The presented concepts incorporate reliable hardware and algorithmic components in form of depth sensing vision sensors and illumination-invariant representations, which at the same time encode the appearance of humans and their environment in a highly specific manner.

Based on our extensive current testing results in applied settings and future plans for trials, jointly performed with end users and infrastructure providers we are confident that the proposed technology elements will achieve a significant impact on rendering border control procedures safer and an individual's travel experience more enjoyable.

ACKNOWLEDGEMENTS

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007–2013) under grant agreement n° 312583.

REFERENCES

1. M. Humenberger, C. Zinner, M. Weber, W. Kubinger and M. Vincze, "A fast stereo matching algorithm suitable for embedded real-time systems", CVIU, Vol. 114, Issue 11, November 2010, 1180–1202.
2. M. Rauter, "Reliable Human Detection and Tracking in Top-View Depth Images", In 3rd International Workshop on Human Activity Understanding from 3D Data, CVPR, 2013.
3. D. Schreiber and M. Rauter, "GPU-based non-parametric background subtraction for a practical surveillance system". In ECV Workshop, CVPR, pages 870–877, 2009.
4. D. Schreiber, A. Kriechbaum and M. Rauter, "A Multisensor Surveillance System for Automated Border Control (eGate)", 1st Workshop on Activity monitoring by multiple distributed sensing (AMMDS) at the 10th IEEE Int. Conf. on Advanced Video and Signal-based Surveillance (AVSS 2013)

Academic Session

Biometrics In ABC: Counter-Spoofing Research

Hong Wei, Lulu Chen, James M Ferryman · *Computational Vision Group, School of Systems Engineering, University of Reading, Reading RG6 6AY, UK*
(h.wei,ll.chen,j.m.ferryman@reading.ac.uk)

Abstract: Automated border control (ABC) is concerned with fast and secure processing for intelligence-led identification. The FastPass project aims to build a harmonised, modular reference system for future European ABC. When biometrics is taken on board as identity, spoofing attacks become a concern. This paper presents current research in algorithm development for counter-spoofing attacks in biometrics. Focussing on three biometric traits, face, fingerprint, and iris, it examines possible types of spoofing attacks, and reviews existing algorithms reported in relevant academic papers in the area of countering measures to biometric spoofing attacks. It indicates that the new developing trend is fusion of multiple biometrics against spoofing attacks.

Keywords: biometrics, ABC, counter-spoofing mechanisms

INTRODUCTION

The FastPass* project aims to build a harmonised modular reference system for all European automatic border crossing points. With growth in travellers and complexity of travel documents, it is desired to have fast and secure processing for intelligence-led border control. Biometrics, the identification of humans by their traits, is a key means used in automated border control (ABC). By automating identity checks, biometrics can confirm quickly and accurately that travellers are whom they claim to be. As early as in 2002, the US Congress had asked the General Accounting Office (GAO) to assess biometric technologies that can be used for US border control applications (News–1 2002). In Biometrics Review: 2008/09 (News–2 2009), it stated that biometrics at the border received a boost when the European Commission unveiled plans to strengthen Schengen zone border security, while facilitating travel for citizens, tourists and legal migrants. The recent survey conducted by Frost & Sullivan forecasted that the biometrics market in the global border control will expand steadily due to increasing international co-operation on travel security issues (News–3 2013).

The commonly used biometric traits in ABC are face, fingerprint, and iris. A typical biometric ABC may work in such a way that a passport is read by a document reader followed by machine checking the face, fingerprint, or/and iris. Then, a positive checking result opens the gate; otherwise the gate remains closed. For example, the UK Border Agency uses face matching for all its operational e-gate systems, which are currently only open to EU citizens holding electronic machine readable travel document (e-MRTD). The UK Border Agency also collects fingerprint scans (10 flat fingerprints) from persons applying for UK visas and these can be matched on arrival**. It becomes crucial to increase the reliability of biometric systems. In some cases, a multimodal biometric system is in place to enforce the security of a machine identification system.

However, machine intelligence is challenged by spoofing attacks. At the biometric sensor level, these attacks could be, for example of face, a printed face on a piece of paper, a face on an iPad screen, or a face mask (could be 3D) worn by an attacker. The vulnerabilities of algorithms used for

* FastPass is a collaborative project funded by the European Commission under the 7th Framework Programme, with grant agreement no. 312583 (https://www.fastpass-project.eu/).

** Acknowledgement: The information is provided by Chris Hurrey from IntrePID Minds Ltd, UK, a FastPass project partner, closely working with the UK Border Agency.

biometric based identification need further exploration to mitigate potential attacks. Software based solutions are under research to find counter-spoofing mechanisms to optimise performance of biometric recognitions (Gomez-Barrero, Galbally, and Fierrez 2013). This paper overviews the current research in the area of anti-spoofing attacks in biometrics. It particularly focuses on recent algorithm developments based on literature review. The review is categorised by three different biometric traits (i.e. face, fingerprint, and iris). In the next section, the detailed reviews are presented with the three categories, followed by a conclusion in the final section.

RESEARCH ON COUNTER-SPOOFING MECHANISMS IN BIOMETRICS: AN OVERVIEW

Depending on sensors and recognition algorithms used in biometric systems, counter-spoofing algorithms can be attempted. Software solutions may take place to improve performance of biometric systems against spoofing attacks. Mechanisms have been sought by research, and relevant counter-spoofing algorithms are developed. In this section, seminal algorithms used for countering spoofing attacks for face, fingerprint, and iris are reviewed.

Counter-spoofing algorithms in face recognition

A falsified face could be a printed photograph, a photograph displayed on a screen, and videos replayed on a screen. Techniques used in countering spoofing attacks for 2D face recognition can be broadly classified into three categories, i.e. motion, texture and liveness (Kahm and Damer 2012).

- Motion analysis: the analysis is based on the fact that there is significant difference between motions of planar objects and real human faces (3D). Algorithms of spoofing detection based on motion analysis are usually associated with optical flow. The assumption is that different patterns of optical flow fields reveal the difference between movements of 3D face (real face) and 2D face (spoofing face).
- Texture analysis: it is assumed that printed/LED faces contain outstanding texture patterns that do not exist in real faces. The other common observation is that images/videos with spoofing faces (printed or replayed) are usually noisier than those of real faces. In this case, noise variance may be used as a distinction feature for the detection.
- Liveness detection: Life signs may include eye blinking, lips movements, etc. This requires analysis of local movement against global movement. Developed algorithms under this approach focus on the movement of a certain identified part of a face.

Among the three categories, texture analysis dominants approaches to distinction of live and spoofing faces. In the recent competition on counter measures to 2D face spoofing attacks (Chingovska 2013), eight teams took part in the competition, and seven of them made use of image textures in their algorithms. These texture features include local binary code (LBP), gray-level co-occurrence matrix (GLCM), and Gabor features. LBP has shown its effectiveness as image features in face spoofing detection(Chingovska, Anjos, and Marcel 2012). Statistical features, such as first and second moments are also used as descriptors in the feature space. For motion analysis, optical flows are popularly adapted in algorithm development (Bao et al. 2009); and live signs are connected to both eye blinking and lip moving (Pan et al. 2007; Wang, Ding, and Fang 2009). With regards to classifiers, a variety of Support Vector Machines (SVMs) have seen their applica-

tions in face spoofing detection (Chingovska 2013).

Texture analysis has advantages of simple implementation, possible decision from a single frame, and no user collaboration needed. However it requires data covering all possible attacks, and may fail with low textural attacks. Algorithms based on motion and life sign detection are independent to textures and very hard to spoof by 2D images, but it needs a video sequence, and may also need user-cooperation. The new developing trend of 2D face anti-spoofing algorithms is fusion of different categories of cues, either in the feature level (a single classifier) or in the score level (multiple classifiers). Such an approach is effective in tackling a diverse set of face spoofing attacks (Chingovska 2013).

Counter-spoofing algorithms for fingerprint recognition

The fingerprint is another biometric trait widely used in biometric border crossing systems. Two types scanning technology dominate commercial products: optical sensors and capacitive sensors. After capturing fingerprints, a scanner performs one-against-one or one-against-all matching with enrolled data. Fingerprint scanners are robust and achieve high accuracy for identification tasks, however, they are potentially vulnerable to spoofing attacks, which reproduce fake fingerprints from original copies (Galbally et al. 2011; Espinoza, Champod, and Margot 2011). Common spoofing attacks use scanned finger images, artificial fingers, or cadaver fingers. The materials for making artificial fingers include silicone, latex, gelatin, play-doh, waxes, and wood glue (van der Putte and Keuning 2001; Matsumoto 2002).

Counter-spoofing algorithms incorporate liveness detection, which can be implemented in two ways: hardware and software. The hardware solution detects liveness based on natural features such as odour, pulse, blood pressure, temperature and electrical resistance. The obvious limitation of these methods is the requirement for additional hardware, hence extra security measures for the hardware. Software-based solutions analyse the image data directly and do not require extra hardware. A common method for liveness detection is based on fingerprint perspiration patterns (Derakhshani et al. 2003; Parthasaradhi et al. 2005; Abhyankar and Schuchers 2009). When touching the scanner's surface, a real fingertip becomes wetter over time due to the perspiration process. Especially, the pattern of the ridges on a fingerprint becomes darker on a capacitive fingerprint sensor. This will not appear on an artificial finger or a photocopy of the fingerprint image. Thus, by measuring the variation of the perspiration patterns over time, for instance 2–5 seconds, liveness can be detected. This method may cause false alarms when people have a skin condition which is not suitable for the detection, or may require a different period of touching.

It is reported that fake fingers will lose some details, such as pores, when they are fabricated from the materials listed above (Marcialis, Roli, and Tidu 2010). The size of the pores is less than 1 mm, so that they are very difficult to replicate on an artificial finger, i.e. real fingers have many more pores than artificial fingers. Therefore, counting the number of pores may be an approach to identify fake fingers. Skin distortion occurs during movement such as rotating the finger on the scanner surface, whereas fake fingers give less or different deformation. Signal analysis of fingerprint ridges and valleys has shown the difference between real and fake fingerprints (Tan and Schuckers 2010). Coli et al. (Coli, Marcialis, and Roli 2007) found that the frequency between

ridges and valleys is altered during the fabrication process. They use power spectrum analysis based on the Fourier transform to detect fake fingers. Various image features have been attempted to distinguish live and fake fingerprint images. Again, LBP has shown promising results among all the features (Nikam and Agarwal 2008a; Ojala, Pietikainen, and Maenpaa 2002). More recently, Ghiani et al. (Ghiani, Marcialis, and Roli 2012) proposed the Local Phase Quantization (LPQ) feature, which shows competitive performance. Fusion of multiple image features is popularly used in practice (Pereira et al. 2012; Nikam and Agarwal 2008b). It has been demonstrated to improve the performance of fingerprint spoofing detection.

Counter-spoofing algorithms for iris recognition

Iris patterns are epigenetic and possess a high degree of randomness (Daugman 2003). Like face identification, Iris identification is non-intrusive. This makes iris and face more suitable to be integrated in a future FastPass system. However, to capture high quality iris images from a long-distance moving target is currently still a challenging task. On the other hand, compared with face, iris provides a higher degree of uniqueness, and unlike face, iris is believed to be stable over a person's lifetime.

Similar to face and fingerprint, iris systems can be deceived using cheap spoofing methods, such as printed iris images, cosmetic contact lenses with a printed iris pattern, artificial eyes and handheld displays. Previous research has evaluated the vulnerability to such spoofing attacks and the importance of applying counter-spoofing mechanisms (Ruiz-Albacete et al. 2008; Galbally et al. 2012).

Daugman (Daugman 2003) proposed theories that using optical properties from different parts of an eye (blood, melanin pigment, tissue and fat), retina reflection (the red eye effect) and purkinje reflection. High quality cameras are required for capturing these features. Chen et al. (Chen, Lin, and Ding 2012) proposed an approach based on texture changes of the conjunctival blood vessel and iris patterns from multispectral images. They claimed that with a real iris texture varies with light frequency, whereas with a fake one it stays constant. Image texture analysis has also been popular in academic research. A simple method is to analyse high-frequency spectral magnitude based on Fourier transform (Daugman 2003). The method recognizes spurious coherence from printed iris patterns. However, this method would fail for partially blurred printed iris patterns or high-resolution printed patterns (He, Lu, and Shi 2009). Rather than using optical or texture features alone, Lee and Son (Lee and Son 2012) recently combined both optical and texture features in iris anti-spoofing detection. Galbally et al. (Galbally et al. 2012) proposed a liveness detection system based on a set of image quality related features. More recently, Connel et al. (Connel et al. 2013) proposed an approach to detect cosmetic contact lenses by projecting additional structured light patterns onto the eye. They found that without a contact lens, the reflected patterns have straight lines, whereas with a contact lens, the patterns had curved lines. Eye movement has also been used as a basis for spoofing countermeasures. Movement includes eye hippus, constriction and dilation of the pupil and iris, and eyelid blinks, which can all be captured by a normal camera. Bodade et al. (Bodade, Talbar, and Batnagar 2009; Bodade and Talbar 2011) calculated variations of pupil dilation from multiple iris images and recent research uses pupil constriction in iris liveness detection (Huang et al. 2013).

CONCLUSIONS

Biometrics have shown its practice in ABC, and will be continously used in the future ABC. Counter-spoofing attacks in biometrics have to be considered. An ideal ABC may have a nature of non-intrusive, efficiency, and effectiveness. These require advanced algorithms to identify/verify submitted biometric traits in such a way that both accuracy and computational cost are taken into account. In this paper, as one of the objectives in the FastPass project, we present an overview of current research of counter-spoofing mechanisms in biometrics. Algorithms and features used in these algorithms are broadly discussed. Their pros and cons are briefly summarised for reference. It has been noted that the new developing trend of counter-spoofing algorithms is data fusion at different levels, such as, feature level fusion, decision level fusion, and fusion of multiple traits.

REFERENCES

1. Abhyankar, A., and S. Schuchers. 2009. Integrating a wavelet based perspiration liveness check with fingerprint recognition. *Pattern Recognition* 42 (3):452 – 464.
2. Bao, Wei, Hong Li, Nan Li, and Wei Jiang. 2009. A liveness detection method for face recognition based on optical flow field. In *International Conference on Image Analysis and Signal Processing*, 233–236, 11–12 April 2009.
3. Bodade, R., and S. Talbar. 2011. Fake iris detection: A holistic approach. *International Journal of Computer Applications* 19 (2):1–7.
4. Bodade, R., S. Talbar, and A. Batnagar. 2009. Dynamic iris localisation: a novel approach suitable for fake iris detection. In *IET International Conference on Ultra Modern Telecommunications & Workshops*.
5. Chen, R., X. Lin, and T. Ding. 2012. Liveness detection for iris recognition using multispectral images. *Pattern Recognition Letters* 33 (12):1513 – 1519.
6. Chingovska, I. 2013. The 2nd competition on counter measures to 2D face spoofing attacks. In *The 6th International Conference of Biometrics (ICB 2013)*, 4–7 June 2013, at Madrid, Spain.
7. Chingovska, I., A. Anjos, and S. Marcel. 2012. On the effectiveness of local binary patterns in face anti-spoofing. In *International Conference of the Biometrics Special Interest Group (BIOSIG 2012)* 1–7, 6–7 Sept. 2012.
8. Coli, P., G Marcialis, and F Roli. 2007. Power spectrum-based fingerprint vitality detection. In *2007 IEEE Workshop on Automatic Identification Advanced Technologies*, 169–173.
9. Connel, J., N. Ratha, J. Gentile, and R. Bolle. 2013. Fake Iris detection using structured light. In *IEEE ICASSP 2013*.
10. Daugman, J. 2003. Demodulation by complex-valued wavelets for stochastic pattern recognition. *International Journal of Wavelets, Multiresolution and Information Processing* 1 (1):1–17.
11. Derakhshani, R., S. A. Schuchers, L. A. Hornak, and L. O'Gornam. 2003. Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. *Pattern Recognition* 36 (2):383 – 396.
12. Espinoza, M., C Champod, and P Margot. 2011. Vulnerabilities of fingerprint reader to fake fingerprints attacks. Forensic Science International. *Forensic Science International* 204 (1–3):41–49.
13. Galbally, J., A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia. 2012. A new vulnerability of iris recognition systems. *From the iriscode to the iris – White Paper for Black Hat USA*.
14. Galbally, J., J. Fierrez, F. Alonso-Fernandez, and M. Martinez-diaz. 2011. Evaluation of direct attacks to fingerprint verification systems. *Telecommunication Systems* 47 (3–4):243–254.
15. Ghiani, L., G. Marcialis, and F. Roli. 2012. Fingerprint liveness detection by local phase quantization. In *ICPR2012 – 21st International Conference on Pattern recognition*, 537–540, at Tsukuba Science City, Japan.
16. Gomez-Barrero, Marta, Javier Galbally, and Julian Fierrez. 2013. Efficient software attack to multimodal biometric systems and its application to face and iris fusion *Pattern Recognition Letters* (in press) available on-line 10 May 2013.
17. He, X., Y. Lu, and P. Shi. 2009. A new fake iris detection method. In *Proceedings of the Third International Conference on Advances in Biometrics – ICB09*, 1132–1139.
18. Huang, X. , C. Ti, Q. Z. Hou, A. Tokuta, and R. Yang. 2013. An experimental study of pupil constriction for liveness detection. In *IEEE Workshop on Applications of Computer Vision (WACV 2013),*.

19. Kahm, O., and N. Damer. 2012. 2D face liveness detection: An overview. In *2012 BIOSIG – Proceedings of the International Conference of the Biometrics Special Interest Group*, 1–12, 6–7 Sept. 2012.
20. Lee, E. C. , and S. H. Son. 2012. Anti-spoofing method for iris recognition by combining the optical and textural features of human eye. *TIIS* 6 (9):2424–2441.
21. Marcialis, G., F. Roli, and A. Tidu. 2010. Analysis of fingerprint pores for vitality detection. In *ICPR2010 – 20th International Conference on Pattern Recognition*, 1289–1292, 23–26 Aug. 2010, at Istanbul, Turkey.
22. Matsumoto, T. 2002. Gummy and conductive silicone rubber fingers. In *Proc. of ASIACRYPT 02*, 574–576, at London, UK.
23. News–1. 2002. GAO to study biometrics for border control applications. *Biometric Technology Today* 10 (5):2.
24. News–2. 2009. Biometrics review: 2008/2009. *Biometric Technology Today* 17 (1):9–11.
25. News–3. 2013. Frost & Sullivan forecasts expansion of border control biometrics. *Biometric Technology Today* 2013 (4):3–12.
26. Nikam, S., and S. Agarwal. 2008a. Fingerprint liveness detection using curvelet energy and co-occurence signatures. In *Fifth International Conference on Computer Graphics, Imaging and Visualisation*, at Penang, Malaysia.
27. Nikam, S., and S. Agarwal. 2008b. Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems. In *IEEE ICETET'08*, 675–680.
28. Ojala, T., M. Pietikainen, and T. Maenpaa. 2002. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 24 (7):971–987.
29. Pan, Gang, Lin Sun, Zhaohui Wu, and Shihong Lao. 2007. Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera. In *IEEE 11th International Conference on Computer Vision (ICCV 2007).*, 1–8, 14–21 Oct. 2007.
30. Parthasaradhi, S., R. Derakhshani, L. Hornak, and S. A. C. Schuckers. 2005. Time-series detection of perspiration as a liveness test in fingerprint devices. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 35 (3):335–343.
31. Pereira, L. , H. Pinheiro, J. Silva, A. Silva, T. Pina, G. D. C. Cavalcanti, T. I. Ren, and J. de Oliveira. 2012. A fingerprint spoof detection based on mlp and svm. In *The 2012 International Joint Conference on Neural Networks* at Brisbane, Australia.
32. Ruiz-Albacete, V., P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia. 2008. Direct Attacks Using Fake Images in Iris Verification. In *Biometrics and identity management*. Berlin: Springer-Verlag.
33. Tan, B., and S. Schuckers. 2010. Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. *Pattern Recognition* 43 (8):2845 – 2857.
34. van der Putte, T., and J. Keuning. 2001. Biometrical fingerprint recognition: don't get your fingers burned. In *Proc. of the 4th Working Conference on Smart Card Research and Advanced Applications*, 289–303, at Norwell, MA, USA.
35. Wang, Liting, Xiaoqing Ding, and Chi Fang. 2009. Face Live Detection Method Based on Physiological Motion Analysis. *Tsinghua Science & Technology* 14 (6):685–690.

Academic Session

Next Generation Smart Border Security

Marc Atallah · *Deloitte France*
maatallah@deloitte.fr
Paul Adamson · *Deloitte MCS Limited*
padamson@deloitte.co.uk

Abstract: Cross-border passenger travel is essential to the objectives of the European Union and the fundamental freedoms of movement of people and goods. By utilizing risk analytics, a registered traveller program and an entry/exit system that enables low-risk passengers to travel easily while providing enhanced scrutiny for those travellers who pose higher security risk, can be implemented efficiently.

Keywords: Risk, Analytics, Data Management, Security, Smart Borders.

INTRODUCTION

The migration of people and the movement of goods across borders have become increasingly difficult to track and manage in globalized economies. Cross-border passenger travel is a vital part of the way of life in the European Union (EU), and border crossings – both through the Union's exterior borders, and within internal borders between member countries – is key to facilitating passenger travel via air, land, and water. The Schengen Area enables travellers to move freely between internal borders without additional screening. As part of the Schengen agreement, however, external borders must be strengthened, which heightens the need for modern technology to support the safe and efficient screening of people entering this special zone.

Further complicating this need, the amount of people coming through major global checkpoints is growing. More than 210 million passengers passed through UK airports in 2010, and between 2011 and 2012, Australia processed more than 31 million international air and sea passengers. That number is expected to reach 50 million by 2020. Each individual represents a myriad of data points, ranging from demographics, travel patterns, visa authorizations, employment and education history, and criminal background. Risk-based decision making is key to operating a safe, secure, and efficient automated border security system that leverages this and other data to make informed decisions about where to focus border security resources, while ensuring smooth border crossings for legitimate travellers.

CONTEXT

In order to effectively meet the dual objectives of facilitating access of eligible travellers while mitigating security concerns, the EU must have a system in place that enables targeting at border crossings to identify travellers which present the highest risk. An Automated Border Control (ABC) system can facilitate this risk-based border security, but in order to be successful, the system must be supported by strong data management processes, analytics capabilities, and most importantly, an understanding of the characteristics that signal crossings that are likely to present potential security risks to the EU. By understanding the current state of passenger traffic travelling into and out of the EU, it is possible to establish a baseline for what constitutes "normalcy" in border crossings, thereby identifying those crossings that extend outside of the normal and may present a risk to se-

curity. By establishing the ability to identify tourists, regular crossings of business travellers, and other border crossings that benefit the European economy as innocuous and, therefore, requiring a lower level of scrutiny, a potential entry/exit system and registered traveller programme that enables the EU to focus its resources on crossings into or out of Europe that may threaten security, can be designed. This baseline information serves a dual purpose of not only enabling high-risk crossings to undergo additional scrutiny, but also shortens the time safe travellers spend at entry and exit points.

According to this baseline for safe or "normal" transit across the EU external border, an understanding of the composition of target groups can be built. The relevant authorities can then identify and analyse the behaviours of risk or target groups and design a registered traveller programme based on these parameters as a foundation. By collecting data and information on risk groups such as where they are geographically located, how they travel, and what economic and social drivers impact their choices, the EU can develop an ABC system that employs risk analytics to improve effectiveness and efficiency.

This type of system has been successfully implemented outside the EU. Australia employs an intelligence and risk-based approach for border security, based on an understanding that the majority of travellers and goods do not present a high risk. The system analyses advanced traveller data prior to arrival to determine if the traveller possibly presents a security threat, enabling passengers with an Australian or New Zealand passport identified as low risk to self-process their entry using the system. SmartGate scans passengers and utilizes biometric data to determine if a secondary scan is necessary – rendering entry simple and efficient for the majority of passengers. Furthermore, in 2010, the Australian government invested a 48 million Euro to introduce a biometric-based visa system used only for certain non-citizens. These steps have enabled Australia to focus security efforts on passengers who pose a potential security risk, while allowing low-risk passengers to enter with minimal interference, through automated, biometric screening. The system's use of risk-based analytics has been a success and can be replicated with the right balance of data, intelligence, and technology (Australian National Audit Office 2012).

RISK STRATEGY

Once passenger data is understood, it can be used to generate an integrated and dynamic risk model that addresses specific risks and their priorities. A true risk prioritization framework must take into account new and emerging threats based on actual and anticipated events, while weighting accordingly based on the likelihood of the event occurring and the government's tolerance for risk. Identification and prioritization of these threats comes through robust integration with intelligence and targeting capabilities. Border control organizations from the Member States and Frontex should engage with intelligence agencies early and often in order to work towards coordinated efforts to enable smart borders.

Multiple data sources, when combined, can be assessed using powerful analytics to identify and act on areas of potential threat as identified through the risk strategy. However, data analysis and risk modelling, once initiated, will likely result in the realization that the available data and intelligence does not provide all of the information required to make informed decisions. A strong risk strategy implies a continuous

feedback loop – as new information needs are identified, law enforcement, intelligence agencies, and policy makers must work together to determine what methods can be put in place to make sound assumptions, and work collaboratively to identify new processes and policies to continue to collect different forms of intelligence or data elements to improve decision making.

RISK MANAGEMENT

Understanding key characteristics and indicators in travel data can unveil deviations and patterns that form the basis of risk profiles. Leading edge technology has enabled new capabilities in data mining that outperform previously available statistics and risk modelling methods. One such development is Advanced Knowledge Discovery (AKD), a methodology which uses supervised machine learning to discover hidden combinations of influencing factors that can be used to detect, describe, explain, and quantify zones of risk, fraud, and propensity to specific behaviours that may indicate a suspicious traveller. Data is run through rule algorithms that produce understandable business rules to determine where problems are and better track movement in and out of a country.

Nascent activity, by its nature, is hard to discover. In order to detect and then isolate this activity, a rich and structured data ecosystem is needed. Internal factors in a single data set may not be sufficient to explain behaviours, but complex combination with exogenous data may prove extremely insightful. Treating each attribute as a factor, and isolating specific combinations of factors, enables the identification of high-value clusters – often times detecting weak or hidden signals that were not obviously apparent through basic analysis of trends and correlations – from which risk profiles can be defined. Such risk profiles may lead border agents to better target high risk travellers based on complex patterns that take into account multiple factors (including dates, origins, destinations, time of day, and frequency of travel).

INFORMATION MANAGEMENT

Agencies collect a wide range of "big data" that capture different facets of the migration of people and movement of goods across the border, and governments have an opportunity to address critical border security and immigration by using border analytics to turn this data into insight. For risk models and data mining to be effective, they must be underpinned by strong information management. AKD modelling has the ability to analyse huge amounts of "big data", processing millions of records of all types of data (including numeric, symbolic, and text values) with an unlimited number of variables. For data to be made available for use in this type of complex analysis, it must be properly stored, cleansed, and validated. Multiple data sets – often with different underlying data structures – must be consolidated and maintained in a single location. Data management should also take into account the integrity of the processes by which the data is collected, the validation through which missing values or inconsistency in data sets is detected, and the data warehouse structures through which data is stored and accessed (or exported) for use with analytics tools.

DATA PROTECTION AND PRIVACY

The risk management tool will use personal data from different sources. The quality of the risk analyses will to a high degree be dependent on the type and quality of data that will be possible to input into the system, which will vary between Member States and authorities. Furthermore, EU and national data protection and privacy

legislation will need to be respected in relation to the processing of available data.

In the EU, the use of personal data is restricted by Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. More specifically, collecting and processing personal data of individuals is limited for explicit and legitimate purposes, including situations where data is necessary to perform tasks of public interests or tasks carried out by government, tax authorities, the police or other public bodies (The European Parliament and the Council of the European Union 1995).

Further provisions are established in the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which covers data that are used to prevent, investigate, detect or prosecute a criminal offence or of executing a criminal penalty (The European Parliament and the Council of the European Union 2008). The Commission recently proposed a new data protection legislative framework and any processing of data for the purpose of the risk analyses will need to respect the relevant existing or new legal texts.

INFORMING OPERATIONAL DECISIONS

Finally, intelligence-driven, risk-based decision making methods need to be operationalized and leveraged to enable more efficient and effective resourcing and traveller flow at the border. Determining which transactions hold the highest risk and need to be prevented or mitigated, while enabling low-risk travellers to cross borders more efficiently, is a key consideration for border services agencies today. Policy mak-

Smart Border Analytics Tool

The Smart Border Analytics Tool provides enhanced information on the migratory patterns of individuals entering and exiting the Schengen Area through the use of "big data" and geospatial capabilities. It leverages AKD technology to be able to provide dynamic modeling and simulation of border security scenarios. Visualization levers show visa types, visa status, immigration clusters, and demographic information for immigrant populations It is fully customizable to incorporate various structured and unstructured data sets, including government data sources, commercial transportation information (i.e. airlines), law enforcement information, and open-source data.

Migration of People

- What are the common visa types that are typically used to illegally cross border?
- What are the primary countries of orgin for illegal migrants?
- Where are illegal migrants travelling within the country and can clusters be identified within certain regions?

Figure 1 **Smart Border Analytics Tool**

ers and border stakeholders are keen to learn more about the patterns, trends, and forensic analysis of the legitimate and illicit traveling population. Once sufficient data is collected to populate the information ecosystem and build comprehensive traveller profiles, it can be used to inform both operational decisions and risk management and mitigation. This information will be integral to determining which transactions carry the highest potential risk.

Continuous tuning of analytics tools and the risk profiles they generate can be used to dynamically inform operational decision and policy changes. Operationally, border staff can leverage this data to reduce wait times for the bulk of travellers crossing the border who would be classified as low-risk. Analysis of high-frequency periods would enable border staff to better manage throughput by determining the appropriate number of border services officers, automated border gates, and additional operators required during peak times. Such efficiencies allow low-risk travellers to pass through border security more quickly and be processed automatically, while enabling border staff to focus on the higher-risk transactions, directing those passengers to be further screened by border services officers.

Data can also be used to support strategic decision making among government policy leaders. Data can be input into a variety of visualization and geospatial tools. Visualizing patterns of risk and how they trend and change over time can provide concrete understanding for educated management decisions and policy making. Leveraging a highly immersive visual environment to sort through complex data and manipulate "what-if" scenarios can further support this decision and policy making. Such environments provide a collaborative workspace in which leaders engage together in exploring innovative ideas, using analytics tools to visualize the implication of potential operational or policy decisions as they are considered.

CONCLUSION

Analytical techniques are the underpinnings of successful automated border control. Methods such as predictive modelling, whereby patterns found in historical and transactional data are used to identify risks, can be used for traveller segmentation. Further, the bi-directional, real time collection of data enables anomalies to be detected instantaneously, enabling emerging threats to be identified before a traveller has crossed the border. The large volume of data collected to populate the information ecosystem can be augmented further by social network analysis, geospatial information, and shared data from other countries, including entry and exit data.

Data analytics will help speed the legitimate flow of people across the border and allow border officers to focus efforts where issues are more likely to occur. However, given the volume of data and complexity of the analysis required, this stage may create a bottleneck. In order for a data analytics strategy to be successfully executed, it will require an integrated capability across border services organizations. A significant focus needs to be placed on information sharing between and among national and local government agencies. Joint policies, operational programs, and training will need to be implemented to facilitate efficient and effective collaboration. This will also require standardization of the data collected to expedite the processing of travellers.

REFERENCES

1. Australian National Audit Office. *Processing and Risk Assessing Incoming International Air Passengers*. Audit Report, Canberra, ACT: The Publications Manager, 2012.
2. The European Parliament and the Council of the European Union. "Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters." *Official Jounal L350*, 2008: 0060–0071.
3. The European Parliament and the Council of the European Union. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of persoanl data and on the free movement of such data." *Official Journal L 281* (The Publications Office), 1995: 0031–0050.

Poster Session

Border Security: Public Perceptions and Experiences

Daniel Stevens · *University of Exeter, UK*
Nick Vaughan-Williams · *University of Warwick, UK*

Abstract: At a time when global travel is on the rise and government expenditure is stretched, ABC technologies promise to risk-assess more passengers at a quicker rate without the need to appoint additional staff. Yet, despite these rapid developments and the solutions promised by ABC, representatives from government and industry readily admit that relatively little is known about how citizens perceive biometric border security technologies, whether different members of the population have varying attitudes towards them, or if there is popular appetite to see these systems rolled out beyond the airport environment. Drawing on an ESRC funded study this paper seeks to address this gap by exploring experiences and perceptions of border control as a security threat, the influences on experiences and perceptions, the relationship between perceptions of security threats and attitudes towards public spending on border security, and attitudes and responses towards government's role in the provision of border security. We do so employing a mixed methods approach of mini-focus groups and a large-sample survey of British citizens. Among our findings are that there is consensus about the importance of border security but variation in the way in which people experience surveillance and security technologies that leads to wariness about their use, effectiveness, and unintended consequences; perceived threats to security are also associated, inter alia, with a desire for more spending on border security and a willingness to pay more in tax for the provision of border security; and that there is little public awareness of government strategies on border security or government messages about the role of citizens in border security. We conclude that without more research into public perceptions of and attitudes towards new security technologies such as ABC millions of Euros could be spent not knowing whether compliance is likely or if societal resilience will be enhanced or compromised as a result.

Keywords: societal aspects of EU border security; user experience at airports; public preferences for future spending on border security; public opinion and border security

INTRODUCTION

This paper presents original research on border security in the EU and sets out an agenda for future work on Automated Border Control (ABC) technology in response to the conference topics of "societal aspects", "human-machine interaction", and "user experience and satisfaction." Citizens are now central to border security, risk management, and resilience in the EU. They are expected to be vigilant in public spaces such as airports and to engage with biometric technologies when travelling. The success of initiatives such as ABC depends in part upon public interaction and cooperation. Some EU citizens may feel more "secure" as a result of such technological advances, and be willing to embrace them in their daily lives. Others, such as those from certain ethnic minority backgrounds, may experience heightened levels of personal insecurity and/or refuse to engage. For example, how are biometric kiosks based on facial recognition viewed by women who, for religious and cultural reasons, wear the niqab? Relatively little is known about everyday perceptions and experiences of border security, how the public view efforts to make them feel more secure, and whether or not they are aware of their own role in the risk management cycle. The overall aim of our paper is

to help address this pressing research deficit by presenting the findings of a recent ESRC funded study, and to outline strategic priorities for future research into ABC in policy and practice for the mutual benefit of key stakeholders.

(1) Scope and Objectives

This paper examines public perceptions and experiences of border security, as well as public preferences for border security as a policy solution to security threats, in the context of a broader exploration of what the public sees as being the most pressing security threats to the world, to the nation, to their communities, and to themselves as individuals. The objectives are: to explore how members of the public understand concepts such as "threat," "security," and "border security"; to examine how different members of the public experience border security in various ways, in particular at airports; to investigate the place of border security in the broader litany of contemporary security threats; to examine the relationships between perceptions of security threats, such as from terrorism and immigration, and policy preferences such as for spending on border security rather than on education or health; to ascertain the extent to which the public's views of border security coincide or diverge from government's; and to report on the societal and political dimensions that policy-makers, practitioners, and the private sector need to consider when developing and implementing ABC technologies.

(2) Literature

The existing academic literature in the fields of International Relations (IR), Security Studies, and Political Behavior does not address the above issues. In IR and Security Studies there is a burgeoning literature on biometric border security at airports (Adey 2010; Amoore 2006; Salter 2007), but citizens' perceptions and experiences remain elusive. This is arguably symptomatic of a deeper tendency for academics to overlook the role of public opinion and everyday views, stories and experiences in shaping securitizing moves and conditioning their ultimate success and/or failure (Balzacq 2010; McDonald 2008). Scholars of political behaviour and political psychology have been much more willing to examine public perceptions of security threats such as porous borders, but there are two primary weaknesses as we see it: first, a tendency to focus on a specific "threat of the moment," such as the terrorist threat in the wake of 9/11 (Huddy et al. 2002, 2005; Joslyn and Haider-Markel 2007; Maoz and McCauley 2009), which means that less extreme threats, or threats such as perceptions of border (in)security, have been largely ignored; and, second, a focus on the individual level causes of perceptions of security threats, such as personality traits (Altemeyer 1996; Hetherington and Weiler 2009), at the expense of efforts to understand their implications for governments and public policy.

(3) Methods

The research mobilized an unusual combination of mini focus group work and a national survey in Great Britain. The fieldwork was carried out in three stages: a first wave of ten 90-minute mini-groups – each comprising of three people ("triads") – took place in April 2012; an Internet survey of 2004 participants, including a "booster" sample of 251 British Muslims, was conducted in June 2012; and a second wave of ten 90-minute triads completed this phase of the research in September 2012.

(4) Overview of Main Results

- Although there is considerable variation in perceptions of the most press-

Figure 1. **Pen portrait stimulus**

Anne's niece is getting married in Florida. A week before she is due to leave for the wedding Anne checks the home office website and the threat level has been raised to severe. Should Anne still travel to the US?

ing security threats, there is consensus about the importance of border security that spans age, religion, and race. Sometimes this is a direct reflection of perceptions of a security threat such as immigration or international organized crime, but it can also be an indirect response to a concern such as economic insecurity.

- However, there is variation in the way in which people experience surveillance and security technologies that leads to wariness about their use, effectiveness, and unintended consequences. For example, Muslims often feel that they are victims as much as beneficiaries of border security and that the practices of border security exacerbate perceptions of Muslims as terrorists.
- Perceived threats to security, including weak border controls, tend to be associated with less tolerant attitudes towards groups such as immigrants.
- Perceived threats to security are also associated, inter alia, with a desire for more spending on border security and a willingness to pay more in tax for the provision of border security. These relationships are strong for people who see more national threats and who identify terrorism and immigration as particular threats but they are also strong for individuals who feel personally threatened in these areas.
- There is little public awareness of government strategies on border security or government messages about the role of citizens in border security. Indeed, there is evidence of some fear of involvement, beliefs that there is little ordinary members of the public can do, and an association between awareness of government messages and perceptions of more rather than less threat.
- Without more research into public perceptions of and attitudes towards new security technologies such as ABC millions of Euros could be spent not knowing whether engagement is likely or if societal resilience will be enhanced or compromised as a result.

METHODS

The research design of ten triads of three people, a large sample survey, and a second wave of ten triads allowed the findings of each stage to reflexively inform and shape the next, which meant that survey questions largely arose from the content of the initial tranche of group discussions. In turn, the results of the survey fed into the agenda of the second round of triads. Triads varied by region, life-stage, social class, and religion. They covered a great deal of substantive ground regarding security threats and subjects' experiences of, and thoughts about, specific security threats. This included encouraging them to describe a particular experience and also to discuss certain scenarios, for example:

Other group stimulus material included examples of various government campaigns designed to raise awareness of security threats and what to do about them. Participants were asked about their awareness of these various campaigns, whether or not they felt these initiatives were effective in

changing their behaviour and that of the public more generally, and if they had any ideas about how security-related communication of this nature could be changed in the future. For the analysis, the mini-focus group transcripts were examined in nVivo for narratives, recurring themes, illustrative experiences, and so on.

The 25-minute internet panel survey we conducted with ICM covered many of the same themes and also gauged other individual attitudes and characteristics in order to assess the relationships between perceptions and attitudes regarding border security and other variables. Among the questions were:

- Whether or not weak border control is a global, national, community, or personal security threat (one of 22 potential security threats listed, either emanating from the National Security Strategy (NSS), e.g., a health pandemic, or from the first wave of focus groups, e.g., online identity theft)
- How much of a £100 budget respondents would spend on border control, e.g. investment in new technologies such as ABC
- Support for paying £50 or £100 more per year in taxes for stronger border control
- Support for actions such as tougher border controls, deporting or excluding non-EU citizens who commit crimes, and more intrusive airport security as methods to prevent terrorism
- Awareness of strategies designed to enhance security such as eyeball and face recognition software, full body scanners and increased security at airports, and biometric passports
- The institutions or actors that are most important in tackling border control, including the "international system," the European Union, and individual citizens
- Trust in the UK Border Force

We used the survey data to assess statistically the strength and certainty of relationships using structural equation models, which allow us to simultaneously estimate the effects of perceptions of threats such as terrorism or immigration on the willingness to pay more in taxes for greater border security.

FINDINGS AND ARGUMENT

We used group discussions as an opportunity to discuss how participants perceive and experience border security. The triads demonstrated the extent to which concerns about border security, in keeping with the NSS's categorization of border control, are perceived as a priority risk:

> I think that the government should be taking more control of who is coming into the country. I think we are far too lenient. Watch any border control program. [...] I am worried about fanatics coming into the country, getting in and getting lost in the system and then meeting up, teaming up with others, online as we said, meeting up and joining together (younger white woman, Glasgow, Triad 12).

The range and strength of opinion on the need for "tougher border security" did not vary between our groups. Some of the most vocal and passionate calls for more rigorous border security came from our Muslim and Sikh participants:

> What happens if a bunch of Al Qaeda comes from Europe and we don't have our border security sorted? I think this is a massive security issue and I don't know whether they will be able to deal with it or not (older male Muslim, Leicester, Triad 3).

In general, groups said they felt less secure now than in the past. The invocation of 9/11 as a turning point was common and conversations with older groups in particular tended to contrast today's climate of fear and anxiety as being higher when compared to the eras of the Cold War. For other groups, however, it was not terrorism per se that mattered, but more specifically the threat of particular religious and ethnic groups being stereotyped and connected with terrorist activity.

Islamophobia was overwhelmingly cited among our Muslim triads (Triads 3, 7, 15 and 19) as the most significant security threat facing participants in their everyday lives. A common refrain among these groups was that Islamophobia is a relatively recent development in Britain: "9/11 changed everything." These dynamics were especially pronounced in the context of participants' encounters with airport security:

> When you go to places like the airport you can't challenge anything anymore. In the past if you weren't happy about something you could challenge it. Now you don't want to attract any attention you just say oh I'll keep quiet, I just want to get through this and go home (younger male Muslim, Oldham, Triad 15).

While all participants in triad 15 said that they recognized the need for enhanced airport security measures such as ABC and acknowledged that they benefited from it themselves, two members of the group summed up their overall frustration as follows:

> I can understand some profiling because obviously we want to fly and we want to be safe as well so I can understand some sort of security checks and all this, that's fine but I think sometimes they go that step too far (younger male Muslim, Oldham, Triad 15).

The survey data provide statistical support for these kinds of group differences—for example, Muslims in the sample had different perceptions of the greatest security threats, being more likely to cite Islamophobia and less likely to identify terrorism or religious extremism—but also allow broader examination of what the public is threatened by and the relationship between perceptions of threats and attitudes towards border security. Table 1 below, presents findings about where weak border control "fits" for the public as a contemporary security issue. It shows the proportion of the survey sample that identified an issue as a global, national, community, or personal threat (respondents could identify more than one) and where that issue ranked as a threat (out of 22). The table shows that weak border control is seen as a particularly salient global and national problem but not as a direct threat to communities or individuals, although perceptions of threats such as terrorism and immigration may be seen as indirectly related to border security.

The survey data also show a general association between perceptions of security threats, including weak border control, and a desire for more spending on border control and defence, less spending on international aid, a willingness to pay more in tax towards the provision of security services, and support for more punitive and aggressive measures against terrorists and "illegal" immigrants, but variation by age, sex, religion, and education. Our models also show variation by whether perceptions of threat are seen to be global or at a national or subnational level. Individuals who perceive more global threats are frequently shown to favour *less* spending on

policies such as tighter borders and more spending on international aid.

CONCLUSIONS

(1) Principles and generalisations inferred from the results

Data obtained from focus groups and survey responses lead us to argue that the idea of a singular "public" that will understand, cooperate, and participate in developments in border security is a chimera, even though there is consensus about border control as a leading security issue: rather, public perceptions of threat and security are analytical lenses through which difference and the politics of security comes to the fore. For example, there is a bifurcation between those for whom heightened surveillance necessitates and justifies suspicion of others and those for whom heightened surveillance means they feel unfairly targeted because of their race. In addition, our research suggests that government framing of threats as global rather than national resonates with different kinds of individuals, with different consequences for attitudes towards border security.

(2) Exceptions to, or problems with these principles and generalisations

The research took place in a single country and would benefit from an extension to other countries in the European Union and beyond. Our research is also reliant on recall and self-report of encounters with border security. Future research should draw on direct observation and on interviewing members of the public immediately following experiences with border security at airports, sea ports, and so on.

Table 1. **Weak Border Control and Perceptions of Other Contemporary Security Threats**

	Global	National	Community	Personal
Terrorism	69 (1)	48 (1)	8 (10)	10 (7)
Religious extremism	56 (2)	35 (3)	10 (8)	8 (9)
Economy	46 (4)	45 (2)	36 (1)	38 (1)
Environment	44 (5)	22 (8)	11 (7)	12 (5)
Racial/religious hate crime	41 (6)	26 (6)	14 (6)	9 (8)
Weak border control	27 (9)	28 (5)	6 (13)	5 (14)
Immigration	26 (12)	33 (4)	16 (4)	11 (6)

Reference: ICM survey, June 6-15 2012, n=2004. Numbers are %. Figures in parentheses are ranks.

(3) Conclusions and recommendations

At a time when global travel is on the rise and government expenditure is stretched, ABC technologies promise to risk-assess more passengers at a quicker rate without the need to appoint additional staff. Yet, despite these rapid developments and the solutions promised by ABC, representatives from government and industry readily admit that relatively little is known about how citizens perceive biometric border security technologies, whether different members of the population have varying attitudes towards them, or if there is popular appetite to see these systems rolled out beyond the airport environment. If ordinary members of the public are to be both subjects of and participants in the exercise of border security and ABC technologies there needs to be a deeper undestanding of the public, including a sensitivity to different perceptions and experiences. Public involvement in the development of border security as well as in its exercise will go further towards fostering cooperation. Thus more research is needed into everyday experiences with border security and on attitudes towards new technology such as automated border control gates. This will be of mutual benefit to national governments, EU agencies such as Frontex, stakeholders in the private sector, and EU citizens alike.

REFERENCES

1. Peter Adey, *Aerial Life: Spaces, Mobilities, Affects* (Oxford: Wiley-Blackwell, 2010).
2. Bob Altemeyer, *The Authoritarian Specter* (Cambridge, MA: Harvard University Press, 1996).
3. Louise Amoore, "Biometric Borders: Governing Mobilities in the War on Terror," *Political Geography* 25 (2006): 336–351.
4. Thierry Balzacq, *Securitization Theory: How Security Problems Emerge and Dissolve* (London: Routledge, 2010).
5. Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis* (London: Lynne Rienner, 2008).
6. Cabinet Office, *The National Security Strategy of the United Kingdom: Security in an Interdependent World* (Presented to Parliament by the Prime Minister, 2008).
7. Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (Presented to Parliament by the Prime Minister, 2010).
8. Marc Hetherington, and Jonathan Weiler, *Authoritarianism and Polarization in American Politics* (Cambridge: Cambridge University Press, 2009).
9. Leonie Huddy, Stanley Feldman, Charles Taber, and Gallya Lahav, "Threat, Anxiety, and Support of Antiterrorism Policies," *American Journal of Political Science* 49 (2005): 593–608.
10. Leonie Huddy, Nadia Khatib, and Theresa Capelos, "The Polls – Trends: Reactions to the Terrorist Attacks of September 11, 2001," *Public Opinion Quarterly* 56 (2002): 418–50.
11. Mark Joslyn, and Donald Haider-Markel, "Sociotropic Concerns and Support for Counterterrorism Policies," *Social Science Quarterly* 88 (2007): 306–319.
12. Ifat Maoz, and Clark McCauley, "Threat Perceptions and Feelings as Predictors of Jewish-Israeli Support for Compromise with Palestinians," *Journal of Peace Research* 46 (2009): 525–539.
13. Matt McDonald, "Securitization and the Construction of Security," *European Journal of International Relations* 14 (2008): 563–587.
14. Mark Salter, "Governmentalities of an Airport: Heterotopia and Confession," *International Political Sociology* 1: 49–67.

Innovative User Interface Concepts for the New German eGATES

Poster Session

Christoph Maggioni · *Bundesdruckerei GmbH*
Christoph.Maggioni@bdr.de
Georg Hasse · *Secunet Security Networks AG*
Georg.Hasse@secunet.com

Abstract: We will present the innovative user interface concepts used in the new German EasyPASS eGates to be deployed in 2014. Within our presentation we will describe new approaches to optimize the handling of ID documents as well as the reading process. This process is one of the main areas of problems with inexperienced users in today's eGate systems. Furthermore we will explain the general eGate setup with a focus on the optimized face capturing and recognition process and the throughput optimization generated by using a parallel process layout.

Keywords: user interface, ID document handling, document reader, biometric recognition, passenger flow

INTRODUCTION

In today's eGate deployments user guidance and user interfaces – especially between traveler and document reader – are one of the main problem areas resulting in sub-optimal processing times. In addition the passenger flow within the eGate is an area that requires improvements. Within our presentation we will highlight the approaches taken in the German EasyPASS eGates to be deployed in 2014. The focus of our presentation is on the interaction between traveler and document reader as well the interaction between traveler and face capture and matching unit.

METHODS

In the development of our innovative approaches we have worked closely with professional user interface designers, research groups as well as "sample travelers". To evaluate our findings we have compared them to the findings from our extensive analysis of the eGate projects EasyPASS at Frankfurt airport and EasyGO at Prague airport. In addition we have taken into account the results and improvements gained from the introduction of document readers into the private sector with totally inexperienced and untrained users and operators. By using a consistent set of graphical elements, icons and animations a uniform and pleasing user experience is ensured.

Structure of the presentation

The presentation is structured along the flow of a traveler through the eGate. Below we have highlighted the main steps, starting with identifying and approach-

Figure 1. **The passenger flow through the EasyPASS eGate**

Figure 2. **The new EasyPASS eGate**

ing a group of eGate, using the document reader, entering the inner part of the eGate, performing the biometric matching and finally leaving the automated border control system with an optional manual inspection step.

The main interaction elements of the eGate

Brief description and visualization of the main interaction elements of the eGate: the arc, the document reader and the biometric capturing and matching unit.

Optimal passenger flow and interaction positions

The main interaction positions of a traveler to be found are:

1. Identifying the border crossing point
2. Waiting position in front of the eGate
3. In front of the entry door
4. Within the eGate
5. Leaving the eGate

Interaction with the eGate arc

The eGate arc is a central communication element allowing the user to identify the eGate. In addition the operational status of the eGate can easily be seen.

Interaction the document reader

One of the main areas of problems with inexperienced users in today's eGate systems is the use of the document reader. Travelers often don't know how to place the document on the reading device and tend to retract the document too early.

By using interactive animations without written text we guide the user in placing the document on the reader correctly. Our software will provide real-time interactive feedback on how to place the document correctly and will start the scanning process automatically. In case the document

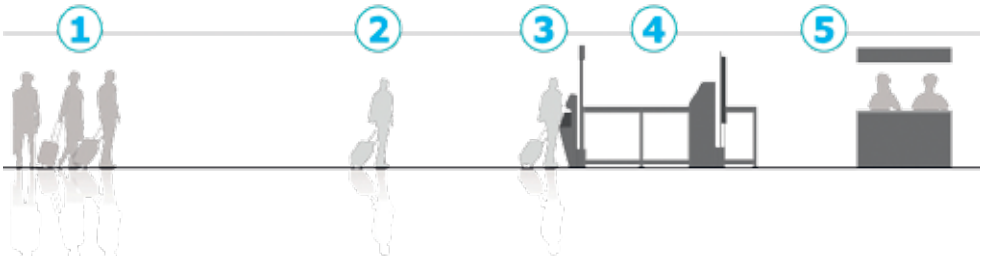


Figure 3. **The main interaction positions**

The video to be shown will demonstrate the optimal flow a passenger through the eGate including timing.

Figure 4. **Interactive Feedback for placing the document**

is misplaced we will display detailed feedback on the cause of the error. Among others we are using a well-known metaphor – the Xerox machine –to inform the user about the running scanning.

Interaction the biometric capturing and matching unit

Based on the fact that the biometric capturing and matching unit is fully integrated into the exit door a swift and reliable capturing of the traveler's facial image is bine ensured. Due to the positioning of the capture and matching unit no unnecessary and time consuming positioning of the traveler is needed. In the unlikely event that the traveler is outside the camera view interactive feedback will be provide via the "digital mirror" in the exit door.

Leaving the eGate and postprocessing

After a successful biometric verification the traveler can leave the eGate and cross the border. In case a manual (secondary) inspection is needed the traveler will be notified before leaving the eGate.

Figure 5. **Integrated biometric capturing and matching unit**

Figure 6. **Manual inspection needed**

CONCLUSIONS

We have shown the general setup, the principles and the user interface principles that will be used in the new German eGates. It can be clearly seen that these eGates will ensure a very efficient border crossing with a high throughput. On the user side the system will be easy to use – even by inexperienced travelers – due to the deployment of new feedback mechanisms and interactive user guidance.

Poster Session

On the Fly Technology

Sandrine Trochu · *Morpho*
sandrine.trochu@morpho.com

Abstract: The purpose of Automated Border Control is to provide security and facilitation to the Border Control Agencies and to the passengers. This objective must be derived into effective and efficient execution and passengers must experience a fluent journey despite the increase of security requirements. It is nowadays commonly admitted that the identification of passengers is performed with the use biometrics, namely face recognition, fingerprints or iris. This operation has to be done quickly, effectively and accurately. This is why we propose to study in this paper the last developments of the "On the Fly" technology, for the three ICAO recognised biometric technologies.

Keywords: Borders, Biometrics, On the Fly, Checkpoint of the Future.

INTRODUCTION – WHY DO WE NEED ON THE FLY TECHNOLOGY

The purpose of Automated Border Control is to provide security and facilitation to the Border Control Agencies and to the passengers. Ensuring users and passengers identity can be only achieved with the full check of biometrics, such as fingerprint, face or iris, when they enter and exit the country in accordance with the authorities' requirements and in full integration with current border control systems and watchlists. State-of-the-art technology to process passengers has to provide them with a fast and pleasant experience throughout their journey, while maintaining the highest levels of security and optimizing the use of resources and space.

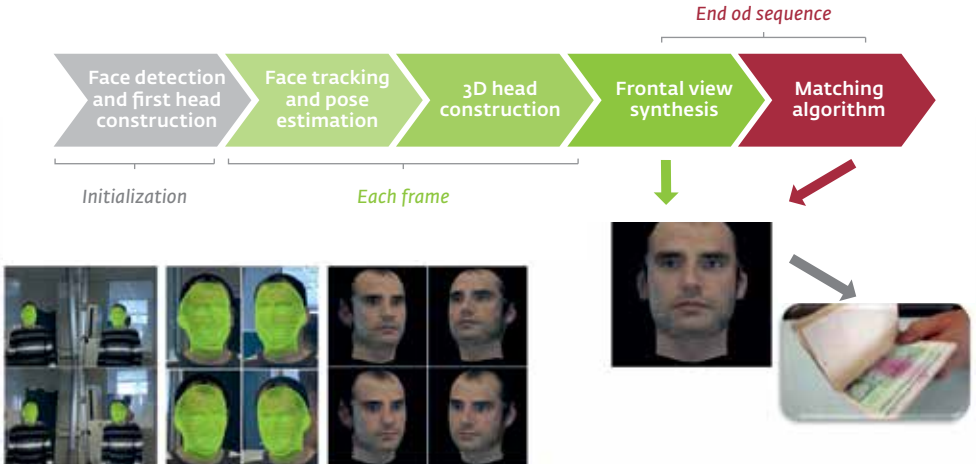
A truly efficient ABC needs to ensure:

- That the passenger is carrying a valid travel document on which personal embedded data and country of issuance have not been altered,
- That he or she is the person that the travel document claims them to be and this is ensured by a biometric check and match between the travel document data and its holder,
- That the person is eligible to cross the border, having been checked against national or international Stop Lists

An airport process needs speed, because the flows are huge, and it needs ease of use, because the passengers cannot be previously trained. This is why the technologies that will be described in this paper pertain to the concept of "On-the-Fly" technologies, i.e. the capture and comparison of biometrics, face, fingerprint and iris, without a physical contact between the machine, the device and the user.

The use of On-The-Fly technology consists of one of the steps of the process, the biometric one. Then, this kind of new technologies will allow performing both:

- An easy capture in the way that, instruction provided to the user are very easy to understand and then to execute without training by the user.
- A capture of less than 1 second for at least 90% of the users. The rationale for this required speed within the process of biometric acquisition relies on first – as previously explained – the need to increase the overall speed of the process, but also on the fact that the faster the better experience for the user



FACE ON THE FLY

Face On the Fly is an innovative technology. The purpose of this technology is to acquire facial images when a person passes through a control gate, without stopping and without having to look at a particular camera. Several images are acquired by a series of cameras to create a three dimensional view of the face. A frontal projection of this image can then be compared and used for authentication or identification purposes.

This technology requires very few learning steps. There are no constraints for the user, it is the solution that adapts to the human behavior. The result is less false rejection and thus a more reliable and faster solution

The diagram below details the process of how the latest versions of the capture technology work, from the moment a traveller enters the gate. Due to the combination of parallel video capture from three cameras being used alongside 2D/3D composite technology, travellers can enter the gate and achieve a very high confidence match without any need to stop and look at the camera. Also, the face capture is initiated as from the reading of the passport. All this results into cutting gate transit times down to a minimum.

From a user perspective, the only thing required is to keep natural and to roughly look in the direction of the screen, absolutely no need to stop and pose in order to cope with the technology requirements. The technology is the one who copes with the passenger behaviour.

FINGER ON THE FLY

This one of the more recent and the most innovative breakthrough technology from the last years: Fingerprints can be acquired JUST by swiping the hand over the device, leading to an acquisition done between 0.5 and 1 second!

In all scenarios, Finger On the Fly device captures and processes fingerprints in the following manner:

- The individual passes a hand over the sensor, positioning the hand up to one inch above the sensor. This is the only action required of the individual; the remaining actions take place within the device, and are transparent to the individual.

- The image acquisition module, consisting of a high-speed camera and lighting, captures successive frames of all four fingers. All images are captured during a single pass of the hand.
- In the processing unit, the 3D data is used to convert the round finger images into flat images.

The Finger On the Fly technology provides a comprehensive solution for the challenges faced by traditional biometric scanning systems. It supports superior identification accuracy by creating a three-dimensional (3D) image of the fingerprint and positioning the light to obtain the best ridge contrast. It provides fingerprint images compatible with other existing devices (one can be enrolled on standard slap device and be verified on Finger On the Fly). It can also provide ISO fingerprint templates.

The main advantages are:
- Usability;
- Acquisition time in less than one second while hand is in motion;
- No issues with dry or wet finger
- Minimal impact on Failure To Enrol due to contactless ease of capture;
- Does not annoy people not comfortable with contact with finger due to fear of hygiene issues;
- No latent left;
- Increased throughput as a result of the usability/time to acquire.

From the point of view of the individual, the four-finger image capture time depends only on the speed of the hand passing over the sensor. On average, image capture takes between 0.5 and 1 second. There is no need for a specific posture or manner of putting the fingers on the sensor. Using Finger On the Fly is easily demonstrated to first-time users, and requires little verbal and no written instruction.

The Finger On the Fly technology can be deployed at airports, bus stations, rail stations, harbors, nuclear facilities, embassies. Its ease of use and implementation scheme makes it easy to control pedestrians and car drives. They both can extend their hands from vehicle windows for rapid capture and verification by de-

vices mounted on flexible supports near gate posts.

IRIS AT A DISTANCE

Each human iris is unique, and offers high confidence in identification – it has been determined that there is an extremely low chance of one in 10^{78} that two random irises will be identical, making such a thing impossible for all practical purposes. Iris recognition uses camera technology to create images of the detail-rich, intricate structures of the iris. Converted into digital templates, these images provide mathematical representations of the iris that yield unambiguous positive identification of an individual.

Iris at a Distance is a state-of-the art solution that allows to acquire 2 irises & face extremely fast and comfortably. It relies on a breakthrough technology, which allows this simultaneous acquisition at a distance of 1 meter in ONE second.

Users only need to stand 1 meter in front of the device. The solution deals with any users: men, women, tall and small, it only needs to see the irises (hats or hair on the eyes are of course detrimental). Most of glasses holders would not be required to take their glasses off. The population's height disparity (coping with both smaller people – or people with reduced mobility in a wheel chair – & taller people) is no more an issue with this new solution. It can sometimes be an issue for some devices requiring, for example, multiple sensors.

When the user enters the acquisition area, the only instruction that the user should follow is to look at the screen. There is no need for further uncomfortable positioning instructions (such as: ask a tall person to bend down in order to perform the acquisition) since the solution is robust to user positioning.

The whole transaction is smooth and easy. Iris acquisition is based on Infrared light & cameras which are by definition invisible to human eyes, increasing the smooth & easy to use perception for the user. The infrared source light have been classified as "Risk 0: No Risk" by external labs.

LIVENESS DETECTION

As self-service biometric systems become more commonplace around the world across multiple market sectors, the need for liveness detection and anti-spoofing measures in general is becoming more significant than ever. Attacks like pictures under any form, fake (or 'dead') fingers, contact lenses are challenges that need to be addressed by face, finger and iris capturing solutions respectively. We indeed need to provide effective anti-spoofing algorithms and software for the detection of fraud and to continue to push the boundaries of the state of the art in this area.

For obvious security reasons, precise state-of-the-art anti-spoofing techniques cannot be described here in details. Nevertheless, we can say that a lot of improvements have been made, are ongoing and will be available in a not distant future. These techniques are a combination of software-based image processing and analysis of various aspects of the persons behaviors with an interaction with the biometric device, as well as hardware-based techniques measuring physical characteristics of the persons. It is needed to use this kind of combination of various and orthogonal techniques in order to best cover the spoofing threat space, oppose a necessary unpredictability and being able to adapt to future attacks.

CONCLUSION – THE CHECKPOINT OF THE FUTURE

We believe that On the Fly biometric technology will be one of the major tools for the automation of the passenger's process, in order to improve convenience and operations at the airport checkpoints, while preserving and even improving security.

ICAO (International Civil Aviation Organization) is in charge of regulating air transport since the convention of Chicago 1944 across the 192 nations of the United Nations. This convention includes a specific annex (Annex 17) regulating air transport security and as such issues Standards and Recommended Practices (SARPs) that all countries need to implement. Annex 17 has mainly evolved after terrorist attacks, and more particularly since 9/11, dictating new security measures at airports particularly related to weapons and explosives detection at checkpoint.

In this very specific and stringent frame, On The Fly technology will allow to secure passenger identities along the whole screening process without any burden on flows allowing to best monitor the process and adjust the needed human resources. This identification must be integrated into a global risk assessment, not limited to the place and time of the travel. Flows and process dynamics can then be adjusted in real time.

This technology, one of the many tools at our disposal today, will need to be used in combination with advanced and fast throughput detection technologies and passenger process automation means (automated doors and barriers, interactive signage) to fully deliver the security, operational and flow improvements.

In a time when the European Commission is building its Smart Borders, all the stakeholders, governments, industry, airports and airlines, we need to imagine together the check point of the future, and build it as smart as possible.

Interactive User Guidance for Capturing Fingerprints

Poster Session

Roberto Wolfer, Michael Weisbach · *Cross Match Technologies GmbH*

Abstract: Fingerprints are currently taken not only for criminal ID purposes, but also for a wide variety of civil use cases, such as Border Control. Whereas in law enforcement, the capture process is done by trained experts, in civil systems like an Automated Border Control (ABC) gate, the applicant himself is responsible for the capture process. A new revolutionary user guidance concept for fingerprint scanners has been developed to guide completely untrained users through the fingerprint capture process, avoiding the typical user mistakes. This approach improves the user experience and user acceptance of such biometric systems. It also decreases the processing time per traveller and lowers the overall cost of the Border Control operation.

Keywords: automated border control; user guidance; real-time feedback; unattended fingerprint capture; human-machine interaction

INTRODUCTION

Traveller traffic at EU airports rose 4.8%in 2011 compared to 2010 levels. This trend is predicted to continue over the next 20 years, with global traffic growing some 6% annually. (1)

As traveller numbers continue to rise, it can be expected that the current infrastructure at border crossing points will have greater difficulties in dealing with increased throughput. The dual objective of facilitating travel and maintaining security requires of the introduction of new approaches and innovative solutions to border management. The installation of Automated Border Control (ABC) systems at a number of European airports constitutes an integral part of this effort. (2)

An ABC system is defined as a self-service kiosk with no explicit trained personal to advice users how to capture biometrics. Therefore it will require comprehensive user guidance which enables even a totally untrained user to capture their biometrics in a timely and efficient manner. In other words the capture system must provide the best *Usability* as possible.

Current user guidance for fingerprint capture devices based on LEDs, a live capture screen, and some audible feedback are not designed for self-service scenarios, but rather for an attended, supervised capture process. Therefore they cannot be simply used and integrated into ABC system.

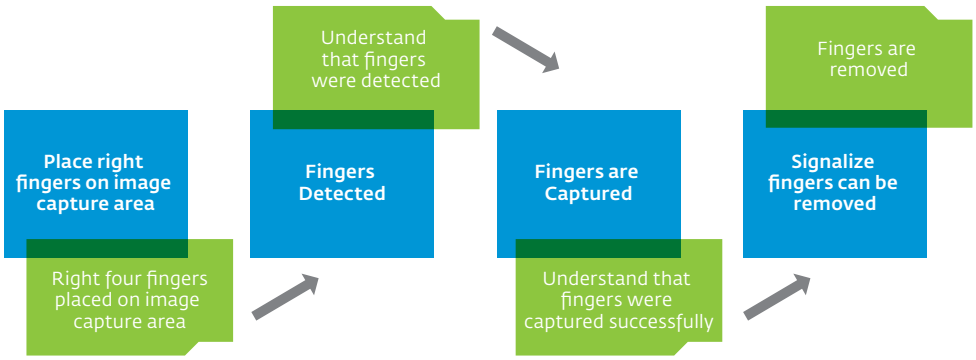
Usability

ISO 9241 is a multi-part standard from the International Organization for Standardization (ISO) covering ergonomics of human-computer interaction. According to the standard, Usability can be defined as the combination of the following major parameters:

- Effectiveness
- Efficiency

Figure 1. **Examples of current user interface elements for fingerprint capture devices**

Figure 2. **Interaction while capturing 4 flat fingers**



- Satisfaction
- Learnability
- Memorability

With regard to fingerprint capture devices these parameters can be utilized as the metrics to measure the usability of not only the fingerprint capture device, but also the system. To achieve the best usability it is important to consider not only technologies while designing and developing the system, but also "human" parameters such as height, age, gender, language, culture, disabilities, and much more.

To achieve the best usability you have to consider not only technologies within the development and design of your system but also "human" parameters like height, age, gender, language, education, culture, disabilities and many more.

METHOD

System Design

A technical system consists of several major design elements (4), with two of them essential to usability. They are Interaction Design and the Interface Design.

The Interaction Design defines the "communication" between the system and the user during operation.

Figure 2 shows an example for the necessary interaction while capturing fingerprints.

Where the Interaction Design defines the communication between the machine and the user, the Interface Design defines how the communication for each necessary interaction is done. For example, Figure 1 shows the interfaces of current fingerprint devices consist primarily of LEDs – permitting only very limited interaction.

Fingerprint capture process analyses

Lessons learned from proprietary field studies (4,5,6,7) and public studies indicate that the key element for interaction while capturing fingerprints process is not only to provide feedback about the current state, but also about the desired state. Implementing a user interface which provides feedback about the desired state requires a completely different approach and completely different technology than just providing a simple current capture state.

It is helpful if the complete interaction process is segmented into its atomic funda-

mental tasks and states, not only for the capture a single fingerprint, but also for the complete fingerprint capture workflow process. Figure 3 shows portion of the segmentation analysis created during the development of the UI for the new Cross Match Guardian:

Once the complete interaction process is analyzed, the different states of the capture process need to be analyzed. It is crucial to address not only Position of fingers for example, but also contrast, movement, number of fingers, and more. The last essential step is the definition of what feedback is required and how to provide it for both the current and the desired state.

FINDINGS

A new graphical interactive user interface

To provide feedback for both current status and desired status requires a break with the traditional Interface Design for fingerprint capture devices.

As a result of our proprietary research, the decision was taken to implement a new user interface using three fundamental principles:

1. **feedback must provide a realistic view** of the capture platen and must display in real-time;
2. **no live image** of the fingerprint should be displayed, as this provides no valid feedback for an untrained user;
3. **animated real-time interaction** should displayed on a screen, instead of static symbols and text based feedback. This allows the user to immediately visualize what they are being requested to do.

Following those simple design principles, the risk of misinterpretation is considerably minimized. Figure 5 shows two examples of the real-time feedback of the current and the desired status while capturing flat fingerprints of the left hand and both thumbs.

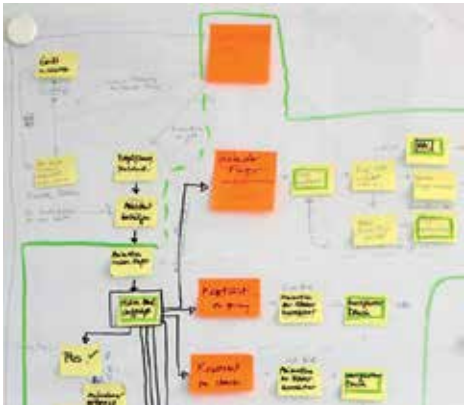


Figure 3. **Result for fractional analyses for capturing Flat fingers**

CONCLUSIONS AND RECOMMENDATIONS

Leveraging this new user interface approach, a livescan fingerprint capture device is optimized for use in next generation ABC gates or other non-attended application requiring fingerprint capture by untrained users. This unique approach not only provides real-time, quality based feedback of the current status-quo, but also delivers guidance on how to correct typical fingerprint capture mistakes. As such, it enables more efficient processing of passengers in a minimum amount of time

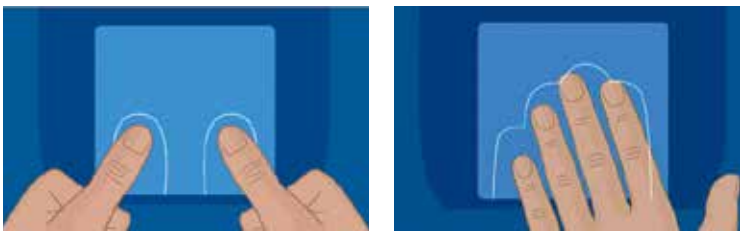


Figure 4. **New user interface showing live feedback while capturing 4 flat fingers and thumbs**

and reduces overall processing costs per passenger.

Further user studies will be required to determine the practicability of the chosen design elements and interactive speed for users from different countries, education and cultural background.

REFERENCES

1. Boeing, "Current Market Outlook 2012–2031 – Long Term Market", 2012.
2. Frontex: "Best Practice Guidelines for Automated Border Control, August 2012
3. J. Garret: The elements of User Experiences, User –centric design for the web, 2003
4. Theofanos M et al.; Does habituation affect fingerprint quality?, CHI, April 22–27, 2006 Montreal, Canada
5. Theofanos et al.; Usability testing of Ten-print fingerprint capture, NISTIR 7403, March 2007
6. Wong et al.; Interactive Quality driven Feedback for biometric systems, IEEE BTAS, 2010
7. Guan H et al.; Real-time feedback for usable fingerprint systems, IEEE Fifth International Conference BTAS2012
8. NIST contribution to ISO/IEC JTC1 SC37 WG6; 2779

ANNEX 2

Conference Programme

DAY 1 · THURSDAY 10.10.2013

09.30–10.00 Welcome address

Ilkka Laitinen · *Executive Director, Frontex*

Kęstutis Bučinskas · *Chair of the Strategic Committee on Immigration, Frontiers and Asylum, SCIFA, of the Council of the EU, Lithuanian Presidency*

10.00–10.30 Keynote speech

Automated Border Control in the context of integrated border management

Belinda Pyke · *Director of Schengen Directorate, Directorate-General for Home Affairs, DG HOME, European Commission*

10.30–10.40 Keynote Q&A

10.40–11.00 Coffee break

11.00–12.30 Plenary Session (I)

Automated Border Control: state of play and national experiences – What has changed in one year?

This session will present a general overview of selected ABC deployments in EU Member States/Third countries where these solutions have reached a sufficient level of maturity.

Moderator:
Edgar Beugels · *Interim Director of the Capacity Building Division, Frontex*

Speakers:
Brigadier Obaid Mehayar Bin Suroor · *Deputy Director General Directorate of Residency and Foreigners Affairs, Dubai, United Arab Emirates*

Gocha Kupradze · *Head of "Imereti" Border Control Unit, Patrol Police Department, Ministry of Internal Affairs, Georgia*

Luís Gouveia · *Deputy National Director, Immigration and Borders Service, Portugal*

Pasi Nokelainen · *System Manager, Finnish Border Guard, Finland*

12.30–13.30 Lunch break

13.30–14.30 Debate session (I)

Role of policy, harmonisation and standardisation in achieving interoperability

This session will examine current policy initiatives on ABC in light of harmonisation and standardisation needs. The European Commission Smart Border Package proposals will be presented, and their impact on future harmonisation requirements reviewed. The session will also explore current and planned standardisation initiatives and how these will contribute to streamline interoperability. A further aim concerns the identification of areas where further action is needed in this field.

Moderator:
James Ferryman · *Associate Professor, University of Reading, United Kingdom*

Speakers:
Pascal Millot · *Deputy Head of Unit, Transeuropean Networks for Freedom and Security and relations with eu-LISA, DG HOME, European Commission*

Paolo Salieri · *Principal Project Officer, Security Research and Development, Directorate-General for Enterprise and Industry, DG ENTR, European Commission*

Michael D. Hogan · *Standards Liaison, NIST Information Technology Laboratory, United States, and Convener of ISO/IEC JTC 1/SC 37/WG 4 on Biometric functional architecture and related profiles*

Lisa Angiolelli-Meyer · *Project Manager, Passenger Facilitation, International Air Transport Association, IATA*

14.30–15.00 Coffee break

15.00–16.30 Debate session (II)

Benefits and challenges of automation: how to balance security and facilitation at the borders?

The session will discuss the benefits and challenges of automation and examine how ABC deployments strive to meet two seemingly contradictory goals: handling increasing traveler flows while meeting high security standards.

Moderator:
Joseph Atick · *Chairman, Identity Counsel International, United States*

Speakers:

Philippe Van Triel · *Project Officer, Transeuropean Networks for Freedom and Security and relations with eu-LISA, DG HOME, European Commission*

Andreas Reisen · *Head of Division ICT Strategy of the Federal Police, Modern Border Control Management, Federal Ministry of the Interior, Germany*

Ram Walzer · *Biometric Applications Commissioner, Prime Minister's Office, Israel*

Jean-François Lennon · *Director, Global Business Development & PMO, Vision-Box, Portugal*

Jürgen Wächtler · *General Operations Manager, Hamburg Airport, Airport Council International, ACI World*

16.30 Adjourn

19.00–22.00 Dinner in town

The conference dinner will be held at the **Boathouse** restaurant. Please refer to the practical note for more details.

DAY 2 · FRIDAY 11.10.2013

09.00–10.40 Plenary session (II)

Academic session: Research and innovations in automated border control technology

Selected research and innovations in the field of ABC will be discussed during this session. The presentations have been chosen among the submissions presented in response to the call for extended abstracts launched by Frontex and the European Commission.

Moderator:

Sadhbh McCarthy · *Director, Centre for Irish and European Security, CIES, Ireland*

Speakers:

09.00–09.15 **Document Security in the Age of Fully Automated Border Control Systems** (Gschwandtner, Štolc)

Andreas Kriechbaum · *Engineer and Project Manager – Video and Security Technology, Austrian Institute of Technology, AIT, Austria*

09.20–09.35 **Dependability Management in Automated Border Control** (Ahonen, Salmela)

Toni Ahonen · *Research Scientist, Technical Research Centre, VTT, Finland*

09.40–09.55 **Visual Surveillance Technologies for Enhancing ABC Secure Zones** (Beleznai, Veigl, Rauter, Schreiber, Kriechbaum)

Stephan Veigl · *Software Engineer, AIT, Austria*

10.00–10.15 **Biometrics in ABC: Counter-Spoofing Research** (Wei, Chen, Ferryman)

Hong Wei · *Senior Lecturer in Computer Science, University of Reading, United Kingdom*

10.20–10.35 **Next Generation Smart Border Security** (Atallah, Adamson)

Marc Atallah and **Paul Adamson** · *Directors, Deloitte Business Consulting, France/United Kingdom*

10.40–11.00 Coffee break · Poster Session

11.00–12.30 Debate session (III) – 2 parallel sessions

Parallel session 1

From decision making to implementation: making an ABC a cost effective solution

The session will examine the decision-making process for the deployment of ABC systems, including cost effectiveness and cost benefit aspects. The importance of inter-stakeholders' cooperation, and its impact on the successful implementation of ABC at the borders, will be highlighted.

Moderator:

Kier-co Gerritsen · *Coordinating Specialist and Programme Manager, Ministry of Security and Justice, the Netherlands*

Speakers:

Carey T. Davis · *Acting Executive Director, Admissibility and Passenger Programs, Office of Field Operations, US Customs and Border Protection, United States*

Lori Pucar · *Acting Director, Border Programs Modernization Division, Border Services Agency, Canada*

Eric Byukusenge · *ICT Manager, Rwanda Directorate General of Immigration and Emigration, Rwanda*

Glen Wimbury · *Assistant Director, Border System Programme, BSP, Border Force, United Kingdom*

Marten Dijkstra · *Sr. Security Officer, Schipol Airport, the Netherlands*

Ignacio Zozaya · *Research Officer, Research and Development Unit, Frontex*

11.00–12.30

Parallel session 2

Why are risk management and vulnerability assessment important?

The session will aim to raise awareness about the importance of vulnerability assessment and testing as well as about the benefits of information sharing, albeit the high sensitivity of this subject matter. The main vulnerabilities of ABC systems and their known (and unknown) strengths and weaknesses both at the technical and the operational levels will be discussed. The session will also explore how to mitigate existing shortcomings to enhance the systems' robustness.

Moderator:

Ted Dunstone · *Chair of the Technical Committee, Biometrics Institute, Australia*

Speakers:

Sébastien Marcel · *Head of the Biometrics Group, Senior Research Scientist, Idiap Research Institute, Switzerland*

Hans de Moel · *Policy Officer, Royal Netherlands Marechaussee, the Netherlands*

James Lipsett · *Senior Analyst, Risk Analysis Unit, Frontex*

Olivier Touret · *Market Manager, Morpho, France*

Günter Schumacher · *Principal Researcher, Joint Research Centre, JRC, European Commission*

12.30–13.30 Lunch break

13.30–15.00 Debate session (IV)

The societal implications of Automated Border Control

Social acceptance and trust are key factors for the successful deployment of ABC. The session will discuss societal considerations and concerns in relation to ABC systems and examine how these concerns are being/ can be addressed in ABC deployments.

Moderator:

Juliet Lodge · *Director Jean Monnet European Centre of Excellence, Emeritus Professor of European Studies, University of Leeds*

Speakers:

Peter Hustinx · *European Data Protection Supervisor, EDPS*

Dalibor Sternadel · *Parliamentary Advisor to Ioan Enciu, MEP, Committee on Civil Liberties, Justice and Home Affairs, LIBE, European Parliament*

Ann-Charlotte Nygård · *Programme Manager, Freedoms and Justice Department, European Union Agency for Fundamental Rights, FRA*

Eric KK Chan · *Director of Immigration, Immigration Department, Hong Kong Special Administrative Region Government*

Dominique Klein · *Head of Sector, Transeuropean Networks for Freedom and Security and relations with eu-LISA, DG HOME, European Commission*

15.00–15.20 Coffee break · Poster Session

Poster session

15.20–16.45 Debate session (V)

ABC and the future of border checks

The session will discuss future ideas as regards the integration of ABC solutions and other risk based facilitation initiatives into a broader border management concept in order to provide increased security at the borders, a better traveler experience and improved overall cost effectiveness for the stakeholder involved.

Moderator:

Tony Smith · *Managing Director, Fortinus, and former Director General of Border Force, United Kingdom*

Speakers:

Annet Steenbergen · *Advisor, Preclearance Coordinator, Ministry of Integration, Infrastructure and Environment, Government of Aruba, Aruba*

Matt Roseingrave · *Customs Service's Counsellor, Embassy to Belgium, Bulgaria, Luxembourg, Romania, Sweden and Mission to the EU & NATO, New Zealand*

Campbell McGhee · *Biometrics Examiner, Police Forensics, Interpol*

Edgar Beugels · *Interim Director, Capacity Building Division, Frontex*

João Nunes · *Director, Lisbon Airport, Portugal*

Jürgen Wächtler · *General Operations Manager, Hamburg Airport, Airport Council International, ACI World*

16.45–17.00 Closing remarks

Edgar Beugels · *Interim Director, Capacity Building Division, Frontex*

17.00 Adjourn

European Commission

DG Home Affairs
B-1049 BRUSSELS
home-access-documents@ec.europa.eu
http://ec.europa.eu/dgs/home-affairs/

DG Enterprise and Industry
Brey 13/092
B-1049 BRUSSELS
entr-general-information@ec.europa/eu
http://ec.europa.eu/enterprise/dg/index_en.htm

FRONTEX

European Agency for the Management
of Operational Cooperation
at the External Borders of the Member
States of the European Union

Rondo ONZ 1
00-124 Warsaw, Poland

T +48 22 205 95 00
F +48 22 205 95 01

frontex@frontex.europa.eu
www.frontex.europa.eu