The practical recommendations for the application of Advance Passenger Information and Passenger Name Record System (API / PNR) were described in the article with the aim to use such system as a counteracting cross-border threats tool. Biometrics establishes a strong link between a document and its holder only if all electronic security features (signatures) are reviewed. That’s is the critical point of all system. Many EU countries don’t have Public key infrastructure in place and can’t use the mentioned security functions. There no joint EU system. Only ICAO has a commercial Public key directory, which provides PKI functions to some countries. Specific digital algorithms know and do many things better, like people, and can make a significant improvement. The order of actions for system implementing is proposed. He will be responsible for Risk assessment, Biometric verification accuracy, and Document verification.

It is mandatory to improve data management, mostly to cover all fields and flows of data. Improve legislation related to data management for the mentioned purpose and GDPR. Besides, we have to invest more in automatic border control systems infrastructure. It is mandatory to centralize Public Key Infrastructure and Certificates masterlist management and validation.
All measures will increase public security and save innocent lives from cross border crimes.

**Key words:** border security, entry-exit system, cross-border crime, border control, air BCPs, API/PNR, biometrics.

1. INTRODUCTION

**Problem Actualization.** The European Union has experienced significant pressure on its external borders in the last few years. There will likely continue to be high numbers of third-country nationals crossing Schengen borders in the future. A study for the European Commission has estimated that the total number of regular crossings will rise to 887 million in 2025, up by more than half in a little more than a decade. Consequently, there is a need to modernize border controls, migration, and security processes.

In the current situation, we have to remember our past failures and learn lessons very carefully. For instance, September 11, 2001 - New York – Washington DC showed the whole World that every society is vulnerable; October 12, 2002 - Bali/Indonesia: 188 people killed during terrorist bomb explosion; March 11, 2004 - Madrid/Spain: over 190 people killed during several bomb explosions.

As you know, some of the World’s policymakers try to exploit terror activity as the main instrument to reach their political goals. Terror usually has different stages and some parts of it in one, some elements in another country. Main actors try to hide their real identity from public security players, especially when they try to cross a Border. That is an essential part of the success of all operation.

The twenty-first century is an era when digital algorithms start to look over big data, things network, object location, and recognize individuals by this Face, fingers, or iris. Passengers API and PNR data are regularly collecting. Why fake identity phenomena still exist, make a breach in our security networks, and is one of the main threads in the twenty-first century?

Analyses of the recent research and publications.
Issues related to comparative context and also partially related to border protection issues covered in this article, devoted, in particular, to the research of Han, CR., McGauran, R. & Nelen, H.\textsuperscript{108}, Bellanova, R. O. and Duez, D.\textsuperscript{109}, Kęsek, R., Boroda, M., & Joźwik, Z. (Eds.)\textsuperscript{110}.

The goal for this publication lies in the comprehensive and comparative analyses of a set of issues related to the border control and national borders protection with a specific focus on the entry-exit system scope, API/PNR.

2. SITUATION ANALYSIS API/PNR

Let us start review form data analysis:
Do we have a sufficient amount of advance information about travelers who intend to cross our borders?

EU Directive 2004/82/EB (L 261/24) requires public passenger transportation companies to collect passenger data before traveling to the EU and sent it to Border authorities, but there many exclusions in case of land traffic. There no obligation for Train and Bus transport\textsuperscript{111}.

PNR Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offenses and serious crime is ground for col-


lection more passenger data before the travel. Still, such data is restricted to use widely, and if we don’t have intelligence information related to that particular traveler, it is useless\textsuperscript{112}.

Did we get information at a sufficient time prior?

Air companies should send data before a flight, but they’re no systematic approach in the EU to manage such data. Member States must build a national API data analysis system. It is a manual procedure in some countries, some automatic, but mostly everyone has trouble with data management and risk assessment. Different data standards used for companies create additional issues. Automatic PNR data management systems have only a few countries.

What kind of information we have about travelers?

Usually, risk assessment is based on official historical data. There no many risk factors or software solutions in place for analysis. No Biometrics indentificators.

We have the resources and bits of knowledge to analyze data qualitatively?

One of the essential things is qualified resources. Lack of professional analytics decrees the importance of all processes. As I know from My personal experience, it is the key in many EU countries.

3. SITUATION ANALYSIS. BIOMETRICS

The first legal act related to digitalized biometric verification was Recommendation for travel documents physical security features laid down in the ICAO doc. 9303 (Machine Readable Travel Documents) and Council Regulation (EC) No 2252/2004 of December 13, 2004, on standards for security features and biometrics in passports and travel documents issued by the Member States which

formed the basis for the upcoming European “Intelligent passport”

First biometric feature: Digital frontal portrait. Deadline for introduction - August 2006. Second biometric feature: Two flat digital fingerprints. A combination of the two will lead to enhanced biometric security. Both features are stored on a contactless radio frequency (RF) chip. They held as images in JPEG format — deadline for introduction – June 2009.

Reasons to introduce electronics in passports (and other travel E-documents) were to increase document security (more difficult to forge), start using cryptography, and establish a more vital link between the document and holder.

The RFID information is the same as printed on a travel document’s data page. The EU countries are not allowed to store additional information not published in the booklet (except fingerprints). Information is stored in the form of files. Data groups containing data (DG1 - DG16).

RFID is protected from fraud. Active Authentication (AA) is based on a cryptographic challenge-response algorithm that can verify if the RFID contains in its secure memory a secret key stored during the personalization by the issuing country. Optional security feature to prevent RFID cloning. The result of the AA is simple: PASS / FAIL. Fail suggests a forgery.

Privacy protection – EAC. Fingerprints (stored in DG3) in the 2nd generation European passports are protected with an additional mechanism called Extended Access Control (EAC). EAC requires an extra secret key and certificate provided by the issuing country of the passport. Authorized border authorities can only read EAC-pro-

---

tected data. Only fingerprints (DG3) are EAC protected. All remaining data (DG1-2,5-16) is BAC-protected. Cooperation between States on an exchange of EAC certificate isn’t sufficient.

After that, no strong need for improvement of travel documents’ physical security features anymore (if the minimum-security level has been achieved).

I have to underline that biometrics increase security of a document ONLY if it is checked in the right way. Biometrics establishes a strong link between a document and its holder ONLY if all electronic security features (signatures) are reviewed.

That’s is the critical point of all system. Many EU countries don’t have Public key infrastructure in place and can’t use the mentioned security functions. There no joint EU system. Only ICAO has a commercial Public key directory, which provides PKI functions to some countries. The better solution is to build a Masterlist of certificates and validation mechanism, but that aspiration doesn’t finalize yet.

4. SITUATION ANALYSIS. ENTRY/EXIT SYSTEM

EU Entry/exit Regulation (EU) 2017/2226 established a new digital biometric system\textsuperscript{114}.

The Entry/Exit System (EES) will be an automated IT system for registering travelers from third-countries, both short-stay visa holders and visa-exempt travelers, each time they cross an EU external border. The system will record the person’s name, type of travel document, biometric data (fingerprints and captured facial images), and the date and place of entry and exit, in full respect of fundamental rights and data protection.

It will also record refusals of entry. EES will replace the current manual stamping system of passports, which is time-consuming, does not provide reliable data on border crossings, and does not allow a systematic detection of over-stayers.

EES will contribute to prevent irregular migration and help protect the security of European citizens. The new system will also help bona fide third-country nationals travel more quickly while also identifying more efficiently over-stayers and cases of document and identity fraud. The system will also enable us to use automated border control checks and self-service systems, which are quicker and more comfortable for the traveler.

That system shall compensate for breaches in the security network and pay the related state’s trustworthiness to fake identity, document fraud, and human verification mistakes. Because humans are subject to error and therefore, it is possible that a traveler can pass the border with a forged/falsified travel document.

5. SITUATION ANALYSIS. ARTIFICIAL INTELLIGENCE (AI)

AI applications exist in the area of criminal investigation and law enforcement. However, it was clear that this is contrary to many other areas, such as migration and border control. Therefore, the EU decided to launch a study to analyze and describe how AI can be leveraged in border control, migration, and security\(^{115}\).

According to the study, we have to extract the main pros of using AI:

*They improved the risk assessment of TCNs. AI will ensure that every applicant is thoroughly examined, limiting the risk of granting visas to travelers with bad intentions (also called ‘mala fide travelers’). The border security will be enhanced by using AI to support risk assessment and decrease the dependence on the individual bor-

---

der guard (to mitigate against potential variation between personal border guards). AI should also ensure consistency in selecting travelers being called for the second line border check by using a data-driven decision process.

**Better resource management.** They were expected to increase the operational efficiency of the border resources allocation. A staffing mechanism that balances the risk of under- (capacity and hence security risk) or overstaffing (increased cost) is aligned to this concept of intelligent and efficient operations.

**Humans require fewer manual tasks.** Employing automating the process, both applicants and visa workers can spend less time on manual low-value-added tasks and focus on priorities (i.e., assessing an individual traveler posing a higher potential risk).

**They are strengthening the internal security (of the Schengen Area) through improved background checks.** Background data for risk analytics, requirements for future smart borders focusing on the human factor, and a Decision Support System (DSS) enable border guard practitioners to assess the potential impact of implementing new solutions for Smart Borders. These deliverables may provide handy guidance for deploying and scaling AI opportunities.

**Improve accuracy in biometric matching, more specifically for facial images.** The facial image is a new biometric identifier to be used in the context of the systems managed by Eu-Lisa, (either new or existing) together with the fingerprints. In particular, the use case would seek to add robustness and accuracy to existing biometric approaches. This could occur by developing models to augment biometric data (e.g., by training a neural network to pre-process an image so that the biometric information is enhanced) or developing models to perform or support the matching directly (e.g., with a convolutional neural network trained on face images).

**AI systems can detect the use of forged travel documents.**

To do so, it would analyze the captured image of the provided documents and assess if the physical characteristics of the document match an original one, if the information provided in the documents
6. VIEW FROM BORDER CHECK PERSPECTIVE

The process starts when the traveler shows intent to enter the Schengen Area (or somewhere). Here, the first step will be to check the traveler’s identity, based on a visual comparison between the travel document provided and the person trying to enter the Schengen Area. If the identity is not valid, the entry will be rejected. If the person’s identity is validated, they are triaged to a different step depending on nationality (either as a TCN or EU citizen).

If the traveler is a TCN, then both travel documentation and visa/permits are required (in the future, a traveler from a visa-exempt country will have to have a valid ETIAS authorization). If the traveler is an EU citizen, only a travel or identity document is required for crossing the external borders. In either case, the authenticity and validity of the document must be confirmed. At this stage, the border guards will check the documents to see if they are either falsified (an altered original document, potentially for use in a ‘lookalike attack’ where a lookalike tries to use a real document that does not belong to them) or forged (an artificial document designed to look like an original one).

If any of the requisite documents or authorizations are not valid, the process will not proceed, and the traveler will not be able to enter the Schengen Area. On the other hand, if the documents and the authorizations are valid, the entry process can proceed.

In the future, the traveler’s entry will be recorded in the Entry-Exit System (EES). First, the check is done to assess whether the traveler is already recorded in the EES (this first-line assessment can only be made to TCNs). If it is the case, the traveler’s entry record is registered, otherwise, the traveler’s individual file is created first and the entry record subsequently. The traveler’s travel document is then compared against the SIS and the stolen and lost documents database. Most often, in parallel, the border guard will repeat the same
activity against the national databases. If there is no hit, the traveler meets the conditions to enter the Schengen Area. The border check for TCN’s continues with a short interview where the border guard will question the traveler on whether the person can be considered a threat to the public policy, internal security, public health, or international relations with a third country. Here, the border guard might analyze travel information (such as the point of departure, the destination, and the purpose of the journey), if the traveler has sufficient means of subsistence for the duration of the stay, and if the return trip or transit to a third country is absolute (in case it is a TCN). If the border guard considers the information provided to be valid, the traveler will cross the Schengen border.

In case some of the conditions for accessing the Schengen Area are not entirely fulfilled, the traveler is likely to be put through a second line border check. This second part of the process can be applied to both EU citizens and TCN, but it is much more common in the latter. This second line of border checks either concludes that access to the Schengen Area can be granted or needs to be denied. Refusals of entry can only occur for TCN’s and are currently recorded in the passport and will also be recorded in the EES in the future.

On exit, the process starts with the traveler’s intention to exit the Schengen Area. As in the Entry process, the first step is to check the traveler’s identity to confirm that the traveler who wants to leave the Schengen Area is the valid owner of the documents presented. Following this step, the documents’ authenticity and associated permits will be assessed through the process explained before.

If no issue is found, the exit will be registered in the EES, and the traveler can exit the Schengen Area. Otherwise, the exit will be denied.

7. CONCLUSIONS

Fake identity is the main tread in the fight against cross-border crime. In my view, specific digital algorithms know and do many
things better, like people, and can make a significant improvement. He can learn the topic and will be better Humans soon. Why not build such an artificial intelligence algorithm for border control purposes? He will be responsible for Risk assessment, Biometric verification accuracy, and Document verification.

It is mandatory to improve data management, mostly to cover all fields and flows of data. Improve legislation related to data management for the mentioned purpose and GDPR. Besides, we have to invest more in automatic border control systems infrastructure. It is mandatory to centralize Public Key Infrastructure and Certificates masterlist management and validation.

All measures will increase public security and save innocent lives from cross border crimes.

LITERATURE


Сігітас Раткевічус. Слабкі місця в спроможності системи контролю в'їзду – виїзду та API/PNR
У статті запропоновано практичні рекомендації щодо застосування системи попередньої інформації про пасажирів та реєстрації даних пасажирів (API / PNR) з метою використання такої системи як інструменту протидії транскордонним загрозам.
Біометрія встановлює міцний зв’язок між документом і його власником лише за умови перевірки всіх електронних засобів захисту (підписів). Це критична точка всієї системи. Багато країн ЄС не мають інфраструктури відкритих ключів і не можуть використовувати згадані функції безпеки. Немає спільної системи ЄС. Лише ICAO має комерційний каталог відкритих ключів, який надає функції PKI для деяких країн. Спеціальні цифрові алгоритми функціонують у багатьох випадках краще людей, і можуть значно покращити ситуацію. Запропоновано порядок дій щодо впровадження системи. Вона відповідатиме за оцінку ризиків, точність біометричної веріфікації та перевірку документів.
Обов’язковим є вдосконалення управління даними, переважно для охоплення всіх полів і потоків даних. Необхідно удосконалити законодавство щодо управління даними для зазначеної мети та GDPR. Крім того, ми маємо більше інвестувати
в інфраструктуру систем автоматичного контролю на кордонні. Централізоване управління і перевірка інфраструктури відкритих ключів і основних списків сертифікатів є обов'язковим. Дані заходи посилять громадську безпеку та врятують невинні життя від транскордонних злочинів.

Ключові слова: прикордонна безпека, система в’їзду-виїзду, транскордонна злочинність, прикордонний контроль, пункти пропуску для авіаційного сполучення, API/PNR, біометрія.