POSITION PAPER

Strengthening security at the Schengen Area borders

Five key recommendations to support Member States in implementing the European Entry/Exit System

IDEMIA

Tourists and business visitors are great news for the economy, but the more people who visit a country, the stricter the security checks need to be. Not all visitors are well intentioned, therefore governments need to ensure that the border control checks are as thorough as possible.

The United Nations World Tourism Organization (UNWTO) estimated that the number of international tourist arrivals have reached a 56-fold increase over the last 70 years. The UNWTO states that Europe accounts for 50% of the world's tourist arrivals, making it the most visited region in the world before the Covid-19 crisis. In 2018, Europe welcomed over 710 million travelers and decided that it was time to implement a new set of regulations in order to better protect its borders.

IDEMIA

Standardizing the border control process within the Schengen Area

In order to have a foolproof border control system in place, all countries within the Schengen Area need a uniform solution and standardized regulations. This has led the European Union to upgrade its border control regulations by creating and implementing the European Entry/Exit System (EU-EES).

The EU-EES will be made available for all Member States, enabling them to access the same information and therefore to have the ability to see the bigger picture. This upgrade necessitates registering the data of Third Country Nationals (TCNs) crossing Schengen Area borders for a short stay at a European level and standardizing border control checks to ensure that all countries within the Schengen Area respect the same guidelines and apply the same vigor.

The EU-EES will have two specific impacts:

At the European level

A set of IT platforms (among those: the EES) need to be developed and existing IT systems need to be rationalized in order to ensure that each Member State can access accurate resources and tools (such as biometric matching) to implement the new border control processes.

At a Member State level

The collection of new data requested by the EU and the implementation of the new processes are to be implemented by February 2022.

The objective of this position paper is to effectively guide Member States on which solutions to employ in adherence with the new processes.

Key facts

2017

The regulation EU 2017/2226 which governs the EES was voted on November 30, 2017

26 Member States

The Schengen Area includes 26 European States, 22 Member States of the European Union, 3 members of the EEA and Switzerland

2022

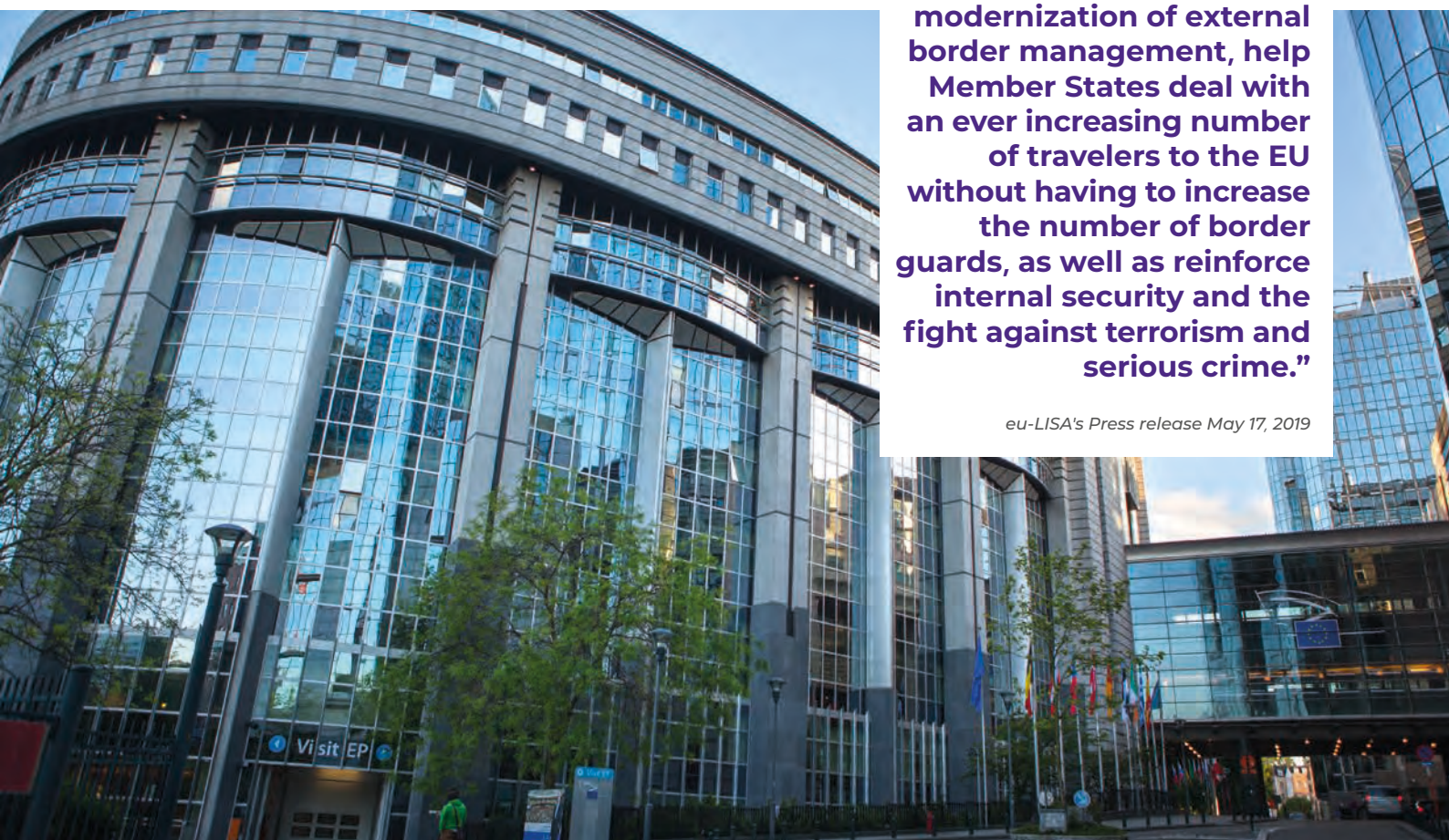
The European EES will come into force in 2022

1,800+

The Schengen Area has more than 1,800 land, air and sea border crossing points

“ the EU's new IT architecture [...] will contribute to the modernization of external border management, help Member States deal with an ever increasing number of travelers to the EU without having to increase the number of border guards, as well as reinforce internal security and the fight against terrorism and serious crime.”

eu-LISA's Press release May 17, 2019



The European Entry/Exit System: The main principles

The EU-EES aims to improve the management and security of all external borders by strengthening the current process as agreed upon with the Regulation (EU) 2017/2226 and the amendment of the Schengen Borders Code. This system will not only have an impact at the European level, it will also rely on additional means that need to be deployed at the Member State level at their border crossing points.

Who is concerned?

› Non-EU nationals referred to as Third Country Nationals (TCNs), visa-holders and visa-exempt travelers who enter the Schengen Area for a short period of time

What is the perimeter?

› The EU-EES applies to all external borders of the Schengen Area

› as well as the countries which have not yet gotten the Schengen acquis in full

What does the new system entail?

The future EU-EES will comprise of:

› **A Central System** for the overall management including a computerized central database of biometric and alphanumeric data owned and managed by eu-LISA

› A **National Uniform Interface** and a **Secure Communication Channel** through which each country will exchange traveler movement information with the Central System, including the information systems already deployed (SIS, VIS, EURODAC etc.)

› A **web portal for TCNs** to check their allowed duration of stay in the Schengen Area at any time

A key objective of the EU-EES is to replace physical passport stamping by electronically recording each border crossing into and out of the Schengen Area, and calculating the authorized stay for each traveler in accordance with the European regulations.

Each Member State shall develop and deploy a national solution to manage entry and exit movements in accordance with the Schengen Borders Code (EU) 2016/399 amended by the introduction of EU-EES in (EU) 2017/2225.

In order to do this the system will collect the following data for each TCN at every border crossing:

- Biographic information
- Biometric data (face and four fingerprints) and provide them to the EES
- All refusals of entry
- All movements of TCNs coming for a short stay in the Schengen Area

The collected data will be provided to systems such as VIS, SIS and Interpol in order to check the traveler's status. Biometric information will ultimately not be stored directly in the EU-EES Central System, but in a European automated matching system:

the Shared Biometric Matching System (sBMS)

This system will securely store the biometric information and will be in charge of travelers' authentication and identification for all of the European border crossing points using its biometric search and matching capabilities.

When will the EU-EES go live?

The EU-EES is scheduled to go live in February 2022. For all Member States to be able to meet this milestone, the system will be available a year in advance, allowing each country to complete functional and compliance testing.

What are the expected outcomes of the EU-EES?

Such a large project shall benefit Europe by improving the management of external borders, preventing irregular immigration and facilitating the management of migration flows.

Once live, in addition to the border control use case, competent Member State authorities, as well as some of the European agencies, will be able to access and use the data for law enforcement purposes in compliance with the EU-EES and GDPR regulations.

Five key recommendations for effective border control

The EU-EES imposes the secure enrollment of all TCNs to verify the identity of each person that is entering the Schengen Area. This data is then shared with external data management systems at both a national and European level.

Inevitably, these additional checks will increase the traveler processing time, resulting in longer queues and longer waiting times. There will also be a need for extra space, equipment and trained border guards to manage the flows and provide supervision of the processes. The additional checks mean that border guards will have further, and somewhat repetitive, duties to perform, which is why their daily jobs need to be streamlined as much as possible, enabling them to perform their core mission with ease.

Here are our top five key recommendations to limit the impact of EU-EES on border control personnel and travelers

1. Help border guards focus on added-value activities

Capturing high-quality pictures of a traveler's face and guiding them on how to properly put their fingerprints on the sensor are not added-value tasks for border guards. In order to help them focus on fraud attempt detection, suspicious behavior and security related situations, the three concepts below are key.

Self-service

Travelers can complete certain tasks such as scanning travel documents, capturing biometrics and answering simple questions required for border clearance by themselves at a **self-service kiosk**. This kind of equipment ensures the quality of data acquired and guides the traveler through the various steps of data acquisition. The kiosks can easily adapt to the traveler and therefore ask the necessary questions and enroll accurate data. This will enable border guards to focus on critical tasks, such as the decision-making process or investigating suspicious cases.

After data capture at a self-service kiosk, the traveler can then use an automated system or a traditional manned border control counter to finalize the border control process. In parallel, background verifications can be performed, optimizing the time spent at each stage.

Automation

Automated Border Control gates are widely used in Europe by Schengen Area citizens. The use of similar equipment could be extended to TCNs providing they come under one of the following categories: bona fide traveler, exit process, re-entry of a known traveler etc. **Biometric eGates** are field-proven and reliable, and help reduce the volume of genuine travelers that border guards have to process, enabling them to focus on cases that require special attention.

Operational supervision

It is a given that all self-service and automated solutions must be monitored. **Operational supervision tools** enable border guards to simultaneously monitor several eGates and/or kiosks. Centralized supervision permits border guards to follow data collection and result verification in real-time, taking any necessary actions. CCTVs can be displayed to the monitoring officer in order to see what happens during the biometric acquisition. Compliant with mobile usage (smartphone or tablet), this method enables border guards to handle exceptions or perform further checks while maintaining a steady flow in the immigration area.

2. Expect reliable results with biometrics

Each Member State will have to collect alphanumeric and biometric data (four fingerprints and face) from TCNs. This data will be verified and securely stored for a maximum of three years. However, we cannot forget that collecting and checking biometric data in heterogeneous environments such as borders is not an easy task. Member States should only consider top-tier suppliers that have been independently benchmarked by official authorities, such as the National Institute Standards and Technology (NIST).

Face capture

The current regulation requires a frontal face capture of 120 pixels between the eyes and a minimum framing of 800x600. In order to comply with the European requirements, various technical strategies can be implemented, but they all have an impact on the design and cost of building the equipment as well as the maintenance. For example, using a camera that moves up and down to capture a face is an interesting concept that complies with the regulation that requires a frontal picture. However, the moving mechanism will not only slow the process down due to camera adjustments, but it will also increase the maintenance costs. Noise can be an aspect as well. Other solutions can meet this quality criteria: tilting cameras, the use of several cameras at different heights, etc. Member States and all other operators should, above all, make sure the implemented solution is user-centric, efficient, robust, compliant with the regulations and is cost-effective to use and maintain for the long term.

The latest innovations in the field of biometrics include **on-the-move face capture and matching**. This optimized and contactless solution will significantly reduce the overall traveler processing time. When applied to a border control counter, it will allow the border guard to automatically retrieve the data collected at the self-service stage and the background verifications performed, while the person is heading to the counter, saving a few precious seconds.

The solution has to be user-centric, efficient and compliant with the regulations.

Fingerprint capture

Contact fingerprint systems are currently used. However, **high-tech contactless fingerprint solutions** are now also available on the market, allowing data capture to be done quickly and hygienically without compromising the level of security or matching precision. In this regard, the NIST recently published the results of the Interoperability Assessment 2019: Contactless-to-Contact Fingerprint Capture. This study aimed to assess how well touchless systems work with legacy databases. The study ranked certain contactless devices better than others in terms of matching rates, image capture sample rates, areas of overlap between probe and exemplar fingerprints, finger ridges and minutiae similarity.

Easy detection of spoofing attempts

Biometrics capture is a critical step in the identity verification of a TCN, which is precisely why it is paramount that Member States are able to detect all spoofing attempts. This is particularly important when the capture of biometric data is to be done directly by the traveler using a self-service system. The system should have the capability to automatically detect fake fingers, masks, images and/or video feeds etc. This is known as **presentation attack detection**. For ergonomics and ease of use, passive detection systems are recommended.

IDEMIA

Embedded quality assessment

The quality of the biometrics acquired is key for the effectiveness of the EU-EES. Embedded, real-time quality control of all captured biometrics is necessary in order for each Member State to comply with the EU-EES service level agreement. This will ensure the optimal matching accuracy for the future European sBMS, which is crucial for **embedded quality control**.

Ergonomics

The capture of biometrics, especially when being performed in a self-service system, should be as easy and clear as it can be for the traveler. Knowing where to place your hand and to position your face are elements that must be straightforward and obvious. The ergonomics of a system is important for a traveler's comfort, but also to **reduce stress and the overall processing time**.

IDEMIA

3. Pre-processing API and PNR data to anticipate threats and save time at arrivals

Risk assessments enable governments to analyze travelers' available data before their travel date to determine whether or not they may pose a risk. This helps to build a traveler profile, assisting border guards to make informed decisions and to spend time on those who present a threat, consequently streamlining border-cross checks for bona fide travelers.

Advanced Passenger Information (API) and Passenger Name Record (PNR) data is transmitted by airlines to governments prior to travel. This data allows border authorities to perform risk analysis on travelers a short while before they arrive at their destination. Leveraging this data along with other types of information such as visa applications, electronic travel authorizations (ETIAS) and data securely stored within national lists of interest, offers in-depth insight for border agencies.

At an EU level, directive 2004/82/AC regulates the collection and transmission of API data for all Member States. The use of PNR data is regulated by directive 2016/681. API-PNR data is available in the departure control and reservation systems of airlines. Preprocessing and integrating this data into an Entry/Exit solution provides border management authorities with additional time to allocate resources and examine possible issues with travelers before their arrival at the border.

In addition to immigration, the risk assessment of traveler's data brings value to other border security missions such as customs, intelligence and national security. The United Nations Security Council resolutions 2178 and 2396, encourage all countries to collect and process API-PNR data in order to fight against transborder crime and terrorism.

Risk assessments help border guards to make informed decisions and to spend time on those who present a threat.

4. One size does not fit all: adapt your solution to your border crossing points

Each country and border has its own specificities and therefore needs a variety of solutions that are best adapted to its environment. There are vast differences between the air, land and sea borders as well as their capacity.

Land and sea borders are set to be one of the biggest challenges for the implementation of the EU-EES. Land borders are frequented by pedestrians, cars, trucks, motorcycles, buses and trains, and each of these modalities represent operational challenges on how the EU-EES regulation could be applied to them.

- If dealing with cars, how many passengers are in the car?
- Does the passenger have to stay in or exit the vehicle?
- Is there a parking lot? Or are the vehicles queuing in a line?
- Does the border guard get onto the bus/train or are all passengers asked to exit the vehicle?
- Does the border guard stay in a booth?
- Can train stations or cruise terminals be redesigned to incorporate a border crossing point?

These questions highlight the differences in all available infrastructure and the processes that could be applied, emphasizing how complex the challenge is.

Land and sea borders are set to be one of the biggest challenges for the implementation of the EU-EES.

The same goes for sea borders. Individuals can enter or exit a country in a variety of vessels. From large cruise ships and ferries to smaller vessels, and cargo ships. Again, the possibilities are vast, and the challenges are different. Large cruise ships can have a capacity of 6,000 passengers, plus personnel. The sheer time it would take a border guard to process each individual is extremely consequential. Not forgetting that passengers have a narrow window to disembark and enjoy a few hours at the destination. Small vessels do not always have a predefined route and must be managed at the last minute.

In addition to the different modalities and infrastructures available, it is important to keep in mind that the traveler profile also adds a variable, making the situation even more challenging.

Some travelers are visa holders whereas others are exempt. Some are entering the Schengen Area for the first time and some are on a subsequent entry. There are also seasonal travelers, with a high volume expected at selected border control points during the vacation period, requiring border guards to adapt their capacity to deal with this peak. Some are frequent border crossers such as heavy goods vehicles, commuters etc. Transportation such as buses, coaches and trains carry many passengers and may even represent more than half the vehicles crossing the border.

In light of these observations, all border crossing points need solutions that are tailored to their requirements and constraints. It is clear that a one-size-fits-all approach is not suitable, therefore Member States will have to deploy various verification equipment to adapt to the different configurations.

Fixed, mobile or handheld equipment? Operated by a border guard or used in a self-service or automated system? There is an array of options that Member States can leverage to best fit their needs. As an example, a land border crossing point that faces a high volume of travelers and has sufficient space could:

- Deploy static counters, self-service kiosks and bi-directional eGates inside a hall/ terminal similar to the equipment used at airports
- Use mobile equipment to board a bus and check all passengers

Whereas a small seaport could be equipped with mobile equipment that would perform the checks when needed, knowing that the flow of travelers is not usually high. It is almost impossible to use a unique system or method for all borders for the reason of cost, space and maintenance. **System providers cannot offer a specific solution for every border crossing point, which is why flexibility and adaptation is key to the various use cases.**

5. How to avoid being the weakest link: ensure data security and privacy

Biometric and personal data is sensitive information, which is why eu-LISA ensures its security and data privacy from the Member State exit point and during all the subsequent data lifecycle. Having said that, Member States are responsible for this sensitive data from its capture to the transmission to eu-LISA to ensure its compliance with GDPR regulations.

Certain security principles must be respected in order to ensure the security and privacy of travelers' data every step of their journey.

Reinforce the security of all the public-facing equipment

In order to limit intrusion attempts, limit the usage of public-facing equipment to what it is designed for: disable all unnecessary ports and connectors, do not install unnecessary applications.

No storage on public-facing equipment

In order to avoid compromising data in cases of theft and intrusion, no personal data should be stored on the public-facing equipment, not even temporarily.

Secure transmissions

Mutual authentication and encryption of data is needed when it comes to data exchange. This is particularly true for exchanges between public-facing equipment and the back end. Security policies defining the renewal of credentials on a regular basis shall be coherent with the risks encountered.

No long-term storage at a national level

Storage of personal data at a national level should be limited to the duration of data transmission to eu-LISA. Buffers kept in case of EU-EES failure shall be properly secured to prevent the data being compromised.

Member States are responsible for TCNs sensitive data from its capture to the transmission to eu-LISA.

Key takeaways

A standardized EU-EES is essential in order to enhance security at EU borders, harmonize processes and create a uniform approach for TCNs entering the Schengen Area.

It is important for all Member States to securely share traveler information to verify who comes in and out of the country. By requesting TCNs to provide their biometric data, the Schengen Area is securing its borders and safeguarding its citizens, but also ensuring the security of visitors entering Europe. The service provider's role is to help Member States adapt to the new system as smoothly and as seamlessly as possible, but also for travelers to enjoy a convenient and stress-free journey.

Implementing new biometric systems and adhering to the new regulations will certainly be a challenge. This is why Member States should seek an experienced service provider who will be able to guide them through this transition. Following the five recommendations will allow Member States to implement a system that is GDPR compliant, efficient for all stakeholders and easy to use for travelers.

In addition to this, traditional security policies that are applicable to critical IT systems, such as tight control and auditability of access to personal data, careful management of system users, or encryption of databases shall be implemented.

Member States should seek an experienced service provider to guide them through this transition.

IDEMIA


IDEMIA

Strengthening security at the **Schengen Area borders**

idemia.com/**augmented-borders**

IDEMIA

Join us on

www.idemia.com