AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

The future of smart borders

New opportunities for better border management

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2016, directly supports more than 4.5 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Secretariat Point of Contact: Brendan Moran; bmo@amchameu.eu +32 (0)2 289 10 32

Executive summary

This paper highlights positive developments and a set of key legislative and operational areas of improvement with respect to the reviewed EU Smart Border legislative proposals released by the European Commission on 6th of April 2016. In general we welcome the changes proposed into this new legislative framework.

Introduction: Border management trends in europe

The European Union border management system is intertwined with global evolutions in travel and migration flows. In recent years, both these flows have increased the pressure on the current system, leading to a sharper focus on tightening security. A heavy hike in travel flows into the Schengen zone along with the increasing migration flows have sparked a crisis within the European Union, as countries struggled to cope with the influx.

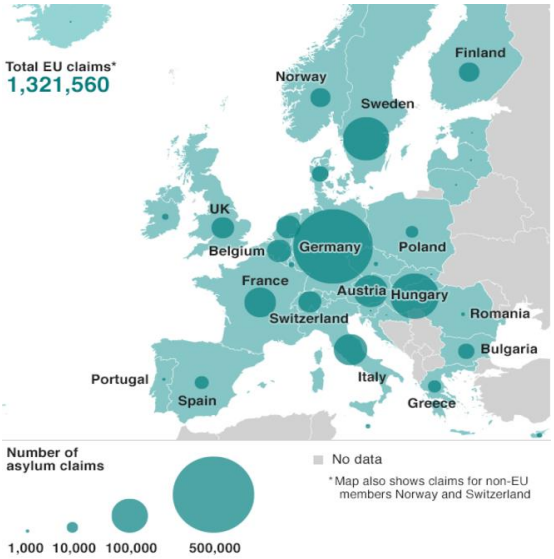
1. Increased demand and terrorism threat

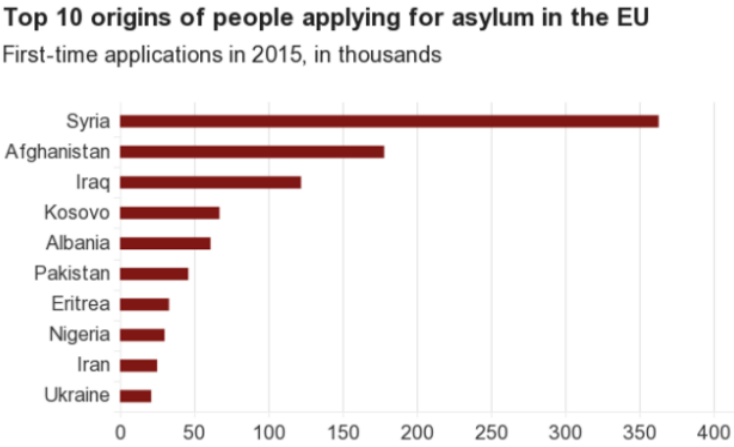
Regular travel flows are continuing to expand, with a total number of travellers to Schengen expected to increase to 887 million by 2025. One third will be non-EU nationals travelling for a short-term visit. Business travellers, short-term contract workers, researchers and students, third country nationals (TCN) with close family ties to EU citizens as well as EU citizens living in the EU neighbourhood, are all likely to cross the borders several times a year.

This trend collides with the rising threat of terrorism in Europe. The recent attacks in Paris and Brussels were executed mainly by EU citizens. Most often, these people were radicalised in a short time period, having spent some time fighting in Syria.

2. Irregular migration

Some 1.8 million migrants and refugees crossed into Europe in 2015. The International Organization for Migration (IOM) estimates over 1 million migrants arrived by sea in 2015, and almost 35,000 by land. This has sparked a crisis as EU Member States (and other European countries) struggled to cope with the influx. In 2015, EU member states only approved 292,540 asylum applications. Their response to the refugee crisis consists mainly of building walls and ramping up border controls to stop the refugees from continuing to travel within Schengen.





When looking at the origins of people applying for asylum in the EU (graph above from Eurostat), the conflict in Syria is by far the biggest driver of migration. The ongoing violence in Afghanistan and Iraq, abuses in Eritrea, together with poverty in Kosovo, lead people to look for new lives elsewhere. As these root causes still persist, many will continue to migrate to Europe.

Several sources state that ISIS use the refugee crisis to smuggle extremists into Europe to perform attacks. The Guardian speaks of more than 4,000 covert ISIS gunmen smuggled into western nations – hidden amongst innocent refugees. The head of Germany's domestic intelligence agency, Hans-Georg Maassen, said to the New York Times that ISIS was using the wave of newcomers to infiltrate Europe. Ahmad al-Mohammad, who blew himself up at the Stade de France in November 2015 is believed to have followed the regular refugee route, entering the EU through Greece.

3. Increased risk

Increasing travel and migration into Schengen indicates that there will be challenges, especially on the level of complexity in managing the data of non-EU travellers within the Schengen area. At the same time, in light of the Paris and Brussels attacks and other developments, even tighter security is required.

This, however, must not deny travellers from a pleasant experience by enforcing complex procedures which result in long waiting lines at security checkpoints, immigration control and customs. Facilitating access to the EU will ensure that Europe remains an attractive destination and will help boost economic activity and job creation.

4. Secure facilitation

A shift towards a user-centric border control process design is necessary. The processes must be designed from the point of view of, and in the best interest of travellers. Governments have traditionally designed processes or systems that focus on delivering regulatory requirements - often at the expense of user experience. Today, travellers expect an efficient and seamless journey. Although they understand the need for security checks, they want them to be almost invisible and not altering their experience. Governments need to find a way to create 'seamless' or 'frictionless' borders, whereby people and goods move smoothly into Schengen; but where effective security controls are not compromised.

Passenger expectations are rising as technologies have changed the way they interact with each other and organizations. Mobile applications are increasingly 'interactive'. Travellers can use near field communications to control the information they share with the government which could include biometric identifiers or biometric authentication on-device.

Today, airports provide augmented reality applications on mobile devices to enable passengers to navigate through airports. Combining this with beacon technology will also provide an immersive experience.

Border officers will increasingly rely on their mobile devices to perform many functions. These include scanning passports, taking photos, performing biometric verifications, filling out baggage examination forms, collaborating with their intelligence people, operating an eGate, hooking into a CCTV feed etc.

The experience for the border guard and other officers is equally important. Border officers need to be equipped with technologies to enable faster, more secure passenger clearance. The spectrum of applicable technologies ranges from border guard stations that enable automatic alerts prior to passengers arriving, to mobile devices that allow guards to clear passengers on the move and receive alerts to enable interdiction at the border. Others include wearables that detect wanted people through face recognition and allow officers to scan documents for authenticity and verification. From a process standpoint, legislation has already proposed the capture of four fingerprints as opposed to 10, which will reduce process times, but there needs to be a step forward to utilise available technologies to reduce process times even further.

Technology that can be applied to securing and facilitating border movements has advanced dramatically in the past two decades. Training officers to use new technologies, and adapt existing, typically manual, processes will maximize their effectiveness.

The Visa Information System, Schengen information System and EURODAC proved effective, allowing Member States to retrieve information while protecting privacy of individuals. However these systems are storing information on different databases, operating independently, requiring disparate queries resulting in disparate responses that demand manual review. As a consequence, valuable data is sub-optimally used.

We welcome the changes proposed in the new Smart Borders Legislation Proposals but there are still a set of legislative and operational issues to overcome.

2016 Smart border legislation: Key legislative issues

In April 2016, the Commission revised the proposal based, in large part, on the Smart Borders pilot report. In this proposal, new features were proposed for the Entry/Exit System (EES), while the Regulation for a Registered Traveller Programme (RTP) was withdrawn. The RTP would have become obsolete as a consequence of the new features on EES. Three main important changes to the EES were recommended. We highlight below some of our key concerns related to those changes.

1. Enhanced biometrics

The Commission's proposal for the Entry Exit System (EES) in 2013 relied on ten fingerprints. The revised proposal suggests a combination of four fingerprints and a facial image as biometric identifiers from the start of operations. This choice will allow for sufficiently accurate verifications and identifications, considering EES's expected size. The amount of data will be kept to a reasonable level while at the same time speeding up border controls and enabling a wider use of self-service systems at border crossing points. The four fingerprints are used at enrolment to check if the TCN was already registered in the system. The facial recognition allows for a quick and reliable (automatic) verification during subsequent entries confirming the individual is already registered in the EES.

The collection of four fingerprints will substantially speed up the first encounter between a traveller and border officer, positively impacting EES's primary purpose. However, concerns remain that limiting collection to four fingers would impede the ability to conduct security/law enforcement checks on the collected data (for example using latent prints collected a crime scene, de-duplication etc.).

From a technology and implementation point, the four fingerprints requirement should be a 'minimum' and systems must be designed to allow a future increase to 10 fingers if applicable.

2. Automation at the border

Border control officials need efficient and highly automated procedures at exit points, to be able to deal with the increasing number of travellers and security threats. Establishing automated identity and track exits, without increasing queues and labour-intensive checks at exit control points is recommended. Biometrics are a key facilitator for this development.

The use of facial recognition technology as a biometric will act as a key enabler to develop kiosk, mobile and self-service solutions.

For air travellers, we suggest a dual use for the Common Use Self-Service (CUSS) kiosks, enabling both carrier and immigration pre-processing. The CUSS kiosks may also collect information. This can facilitate the check-in and security procedures, if the passenger consents to share his/her data. This also works the other way around: existing airline check-in kiosks may be used to enable self-service border clearance. These measures will reduce the pressure and effort on border guard operations in a cost-effective way, while greatly impeding the risk of human error or forgery of documents.

For travellers passing border controls at land, a self-service registration could include a number plate and occupant registration to facilitate the land border inspection and enhance security by performing checks on TCNs and their vehicle.

The EU Travel Information and Authorization System (ETIAS) is an even further extension of the self-service system. Passengers will be able to indicate their intent of travel on their mobile phones prior to departure, speeding up the border control process for known travellers. This may be especially useful for passengers entering through land or sea borders where Advance Passenger Information (API) and Passenger Name Record (PNR) data is not available.

3. Data Retention

The retention time for stored data will be extended to five years. The period reduces the re-enrolment frequency and will be beneficial for all travellers. It will allow the border guards to perform the necessary risk analysis required by the Schengen Border Code before authorising a traveller to enter the area. The deletion of the EES record after 181 days, as proposed in 2013, would have removed any trace of the TCN's recent Schengen entry and exit history, which is required for a risk analysis. It would be a step back compared to what the border guard currently uses: consulting stamps in a travel document. This gives in many cases information that stretches a period of several years. A longer data retention period is necessary to allow the guard to perform risk analysis requested by the Schengen Border Code before authorising a traveller to enter the area.

Processing visa applications in consular posts requires analysing the applicant's travel history to assess the use of previous visas and respect of the conditions of stay. Abandoning passport stamping will be compensated by a consultation of the Entry Exit System (EES). Travel history available in the system should therefore cover a period of time which is sufficient for the purpose of visa issuance. The inclusion of a web service to check the stay status will also be an added benefit removing the need for passport stamps. The fact that this service (checking the stay status of a traveller) may be provided for carriers as well is an advantage. It can be extended in the case of a future ETIAS implementation, where carriers can check the status of a travellers' electronic travel authorization.

The increase of data retention to 5 years will effectively render each traveller a Regular Travel Program member. Consequently, even infrequent travellers to Europe will enjoy faster checks on subsequent visits while at the same time the security is enhanced.

The Implementation of the Smart Borders Legislation will create new opportunities for better border management. However, some operational issues need to be overcome.

The new Smart Borders Legislation will be a leap forward for Schengen border controls and customs and will effectively address security issues, along with issues related to the increase in the number of travellers. However, we believe that putting these measures in place will create new opportunities to enhance the border controls and customs if three main operational issues are to be overcome.

1. Interoperability and interconnectivity

In April 2016, the European Commission published its new strategy with regards to stronger and smarter information systems for borders and security. The strategy mentions the concept of interoperability.

Interoperability is tied to the 'Single search interface', which stipulates that Member States' systems will need to work together in order to share information. It implies pro-active, law-based sharing of information about TCNs, allowing decision-makers to make accurate and timely decisions about the risks and threats of a specific person within the Schengen area.

The development of interconnected systems (each managed by separate contractors) requires a stronger governance and setup of an enterprise architecture function to establish standards for interoperability and interconnectivity. The role of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (EU-LISA) should be extended to include an enterprise architect board with support from key industry partners.

They should be assisted by a stakeholder platform of public and private experts to address the legal, technical and operational aspects of the different options to achieve interoperability of information systems. This would also include assessing the necessity, technical feasibility and proportionality of available options.

In practice, checks of Interpol and other databases should be carried out 'outside' of the Visa Information System (VIS) rather than as part of VIS modifications as currently proposed, because these checks would be needed for non-VIS travellers as well. As a consequence, interchange formats (for messages and notifications), services, biometric sample quality, biometric capture device standards, data exchange, and access control (for both services and data) will have to be agreed upon.

However, rather than having various systems building peer to peer interfaces, a central ESB/workflow engine would be used to interface the various databases and consolidate responses. We could avoid the need of setting up a common messaging format between systems if there is a central ESB component with Extract/Transform/Load capability to translate messages between systems. Instead, the focus should be on ensuring compliance with common message standards (XML, NIST) across all systems. Setting up a common message format may be an expensive exercise and limit the flexibility of each core business system.

2. Emergent identities

The Single Search interface, as proposed by the Commission, must cover the aspect of risk-assessment enabling officers across agencies to assess any known risk associated with the person in consideration. A key element will be the ability to assess an individual over time as risk should be evaluated as a person's identity transforms, providing greater insights into identity and behaviour. Given the construct of Schengen, it would be ideal to have such a platform available centrally as a service to Member State agencies, who can have access to a 360-degree view of an individuals' identity. Access rights to the platform will ensure that Member State specific data is always protected, and will be shared only on the data owner's authorisation. Having this kind of central hub and spoke model of sharing identities will be key to implementing a central base for identities.

An emergent identity model is a powerful tool to help law enforcement and border management officers assess the threat posed by an individual. A key enabler to establish this type of federated search would be a common standard for scoring and adjudicating search hits across each business system.

3. Analytics

EU-LISA will set up a common central monitoring capability for data quality and analytics. Given the breadth of data EU-LISA operated systems contain, this important tool is currently overlooked in the border management context. Currently, Member States perform their own reporting on central system data by launching retrieval queries and building their own reports. Today, online data visualisation tools can allow Member States to access EU-LISA system data and build online reports on the fly and launch advanced queries across systems in real time.

Furthermore, the implementation of IT operational analytics would provide greater transparency from EU-LISA towards its stakeholders. It would create a detailed overview of the quality and availability of the information they are required to provide to Member States' officials and other stakeholders.

EU-LISA will set up this common central capability to monitor business and operations activity, data quality, and analytics. Data quality includes both biometric sample quality and the quality of ancillary biographic information related to people, places, and things for every encounter in the ecosystem. Business and operations activity dashboards will allow authorized stakeholders access to metrics needed to assign resources and make course correction. Analytics will enable authorized stakeholders to rationalize and visualize large amounts of operational (e.g., immigration, law enforcement, and carrier) and external data (public) into actionable information to enhance security and facilitation.

The stakeholder platform should investigate this proposal and address the legal, technical and operational aspects of introducing data analytics to the Smart Border System.