November 2018

**A blog by**

Michiel van der Veen
Chief Executive, EAB

# Biometrics at the border: facing new realities, four fingerprints at a time

As the EU raises its border security budgets, biometrics shine a new light on who's coming and going
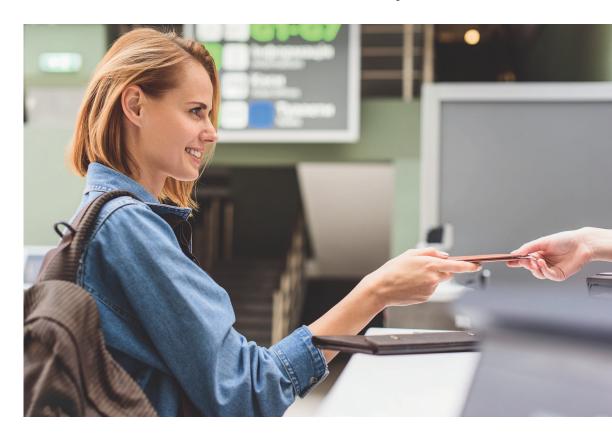
After having survived financial turmoil, economic downturns and national budget crises during the past decade, the European Union is for some time now facing its most pressing challenge of the moment: immigration. There is no denying that illegal immigration is first and foremost on most Europeans' minds, even if their governments haven't caught up yet. Populist leaders across the continent are pointing to undocumented African and Asian migrants as an existential threat to national identity and territory, loosely linking them to acts of terrorism carried out over the years.

Populist rhetoric and exaggerated fears aside, it is a given that Europe's outside borders are indeed porous and a centralized and automated border protection system absent. There currently is no European entry and exit framework registering the 700 million crossings into and out of Europe every year. Non-Europeans overstaying their visa are rendered unidentifiable as soon as they get rid of their legal documents, making it impossible to turn them back to their home country. ID fraud also continues to be a problem, the most infamous cases to date being the 2016 terrorist attacks carried out in Paris and Brussels, where the perpetrators used forged passports.

**Welcome to the future of border control**
In light of these developments, the European Commission is ramping up its border control processes. As of June this year, the EU is reserving a whopping 34,9 billion euro for border and migration management under the next EU budget (2021-2017). One of the programs being rolled out is the Entry Exit System (EES), which was approved by the European Council on November 30th last year, and is due to go in effect by 2020. Building on Frontex, the European Border and Coast Guard Agency oversees EES as a unified information system for recording data on the entry and exit of short stay 'third country nationals' crossing EU external borders. As a

central register of cross-border movements, it detects irregular migration through automated checks and controls for leaving and returning EU citizens, third country businesspeople and tourists.

Using biometric techniques, passport holders will have four of their fingerprints taken, as well as a picture of their face for recognition. Outside border forces will be able to access a uniform search portal linked to the central system, operated by the European Agency for operational management of large-scale IT Systems (EU-Lisa). Using a shared biometric matching service, the EES will be able to perform crosschecks with other databases, such as the system for visa holders (VIS), the fingerprint database for identifying asylum seekers and irregular border-crossers (EURODAC), the European Criminal Records Information System (ECRIS) and the Schengen Information System (SIS). For privacy and security reasons, only member states and European agencies are allowed access to the data, excluding third countries, international organizations and private companies.

**Biometrics is the way forward**
Human rights advocacy groups and privacy watchdogs rightly point out the dangers of collecting and storing massive amounts of citizens' personal data, and they have serious concerns about the treatment of undocumented migrants coming to Europe. But that does not take away from the fact that biometrics technology keeps evolving, offering many advanced options to protect the borders against outside threats real

or perceived. No matter what, biometrics is here to stay.

A number of challenges lie ahead, as Europe is turning to biometrics as a principal tool to reinforce the external border system:

*1. Technical:* for good recognition, high-quality and reliable biometric samples are a must-have, meaning state-of-the-art systems are required to render duplication and abuse (as good as) impossible. High-quality capture processes and algorithms are constantly being developed, but these costly systems are yet to be installed on all 1800+ EU border crossing points. One negative side-effect will be longer enrollment times and inefficiencies. And as a growing pain of early adoption, several technical limitations need to be addressed, such as the failure to enroll individuals (FTE), incorrectly accepting them (FAR) or falsely rejecting them (FRR).

*2. Privacy:* biometric data is extremely sensitive, touching on individuals' most intimate physical properties, and so the utmost care must be taken to protect the data collected. As biometric data is uniquely coupled to an individual, all kinds of personal information like gender, race, age, diseases etc. can be extracted from it. If it were to fall in the wrong hands, this data allows for real impersonation risks through the reconstruction of synthetic biometric images from standard templates. And while it is easy to change a password or replace a credit card, we can neither change nor replace our unique biometric data. Once compromised, the effects could last forever!

With the EU General Data Protection Regulation (GDPR) built on a privacy-by-design blueprint, an ambitious first step has been taken to safeguard the collection and handling of Europeans' personal data. But using advanced biometric technology at Europe's borders will ultimately and inevitably lead to calls for strengthening and expanding privacy rules to include the new technologies.

*3. Security:* the goal of applying biometrics in border systems is to increase trust and detect fraud. As a result, the payoff for circumventing or compromising the system becomes higher. The possibility of impersonation, where a fake identity is created using biometric data, poses a physical threat to the target and his legal identify in time. Using biometric morphing, a person could enroll into the system using morphed facial images that are a lookalike of the person, but cannot be matched with the facial recognition algorithms. These and other, yet to be foreseen, security risks need to be thoroughly studied and dealt with through a robust technical and legislative framework when implementing biometrics at the border.

**Time to get amongst ourselves**
As we are entering a volatile new era of security challenges at home and abroad, the EU turns to strengthening its external borders. Biometrics is the next logical step to take, but the challenges mentioned here as well as other problems still

need to be overcome. National governments need to work hand in hand with Frontex and EU-Lisa to properly integrate biometrics into their large scale IT-systems. Wherever knowledge gaps exist, authorities on both the national and EU-level should team up with specialized partners from the biometrics industry with the aim of developing and operating biometric ID systems that are fair, accessible and secure, while respecting privacy demands. Capacity building is key here, whether it's by sharing best practices, pooling resources and expertise, or creating global standards. Europeans can wish for nothing more and demand nothing less.



**eu-LISA and Frontex joint conference on "EU borders -getting smarter through technology"**
Michiel van der Veen is the Chief Executive of the EAB. At the eu-LISA and Frontex Joint Conference of October 17th in Talinn (Estonia), Michiel called on the ID stakeholders, the European governments and EU agencies to join hands and take biometrics in border management to the next level. You can read more about the event at www.eulisaconference.eu.

## About the Author

Inspired by "Good ID", and based on the values of trust and impartiality, Michiel supports the ID community with executive leadership and thought leadership in the field of digital ID & Biometrics ....... not to mention being a keen cycling enthusiast.

From 2000 onward, Michiel had several technical and leaderships roles in Philips Electronics, and received, in 2007, the Distinguished Employee Award. In 2008, Michiel founded priv-ID, an early innovator in biometric, digital identity and privacy-by-design. It later merged with GenKey in 2011, with Michiel appointed CEO. He has led GenKey through multiple stages of growth to become one of the most trusted brands in the market to provide Identity for Development.

In 2012 GenKey helped to deliver the world's first digital ID solution for Ghana's Presidential Elections. Since then, Michiel has been involved in many large-scale digital identity projects for governments and businesses, across Africa and Europe.

Michiel is Chief Executive of the European Association for Biometrics (EAB), a non-profit and vendor neutral organisation focusing on the strategic ID challenges that Europe is facing. Michiel is also senior advisor biometrics and digital ID to the Worldbank's ID4D program, and a regular industry contributor, speaking about digital identity and biometric; along with future thinking about innovation and market trends.

Michiel has a Ph.D from the Swiss Federal Institute of Technology (ETH Zurich) and further business education from Stanford.

Michiel van der Veen
**Chief Executive, EAB**

## Europe's Leading ID community

The European Association for Biometrics (EAB) is the leading voice for digital ID & biometrics in Europe. We are a non-profit, non-partisan association.

The EAB's mission is to tackle the complex challenges facing ID in Europe, ranging from migration to privacy rights. Our role is to promote the responsible use and adoption of modern digital identity systems that enhance people's lives and drive economic growth.

Through a series of EAB initiatives we support all sections of the ID community across Europe, including governments, NGO's, industry, associations and special interest groups and academia. Our initiatives are designed to foster networking and debate, whether at an EAB hosted event across Europe, or in providing impartial advice & support to individual members.

We ultimately serve the citizens of Europe in the advancement of modern biometric identity systems that are fair, accessible, secure, while respecting privacy.

More info: www.eab.org