

BIOMETRICS AT BORDERS

IMPROVING SECURITY ACROSS BORDERS BUT PRIVACY CONCERNS PERSIST.

By Mario Pierobon

Biometric technologies are changing the way people move across borders, redefining both passenger convenience and security assurance. Facial recognition and multimodal biometric systems are integral to airport operations worldwide. From automated eGates to digital identity credentials, these systems are accelerating passenger throughput while reinforcing border integrity. Yet, their growing adoption raises complex questions around privacy, compliance and data protection. As innovation advances, regulators, technology providers and airport authorities must strike a careful balance between operational efficiency and the responsible use of personal data.

MEASURABLE IMPROVEMENTS

Facial recognition is part of a broader spectrum of video image processing techniques, according to resources available from the European Data Protection Board (EDPB). "Some cameras can capture images of people within a defined area, particularly their faces, but they cannot be used as such to automatically recognize individuals. The same goes for simple photography; a camera is not a facial recognition system because photographs of people must be processed in a specific way to extract biometric data," the team says.

Françoise Bergasse, border marketing manager at Thales, points out

that implementation of biometric authentication at airports and border checkpoints shows an average time saving of 30% to 40% for travelers. "Biometric authentication achieves what was once thought impossible — increased security with faster processing. Real-time facial recognition at automated eGates combines the best of both worlds: speed and certainty. Travelers enjoy a smoother journey, while operators benefit from a highly reliable and tamper-proof identification process," she says.

Data from various sources show that biometric systems have improved processing efficiency at border checkpoints while maintaining high security standards, affirms Rob Sutton, director of solution



Biometric systems have improved processing efficiency at border checkpoints while maintaining high security standards, according to Rob Sutton, director of solution enablement for aviation at HID. HID image.

enablement for aviation at HID. "For example, automated eGates in Europe can verify a traveler's identity in less than 20 seconds, compared to several minutes for manual checks. In the United States, programs such as Global Entry and the Biometric Entry-Exit Program have reduced wait times by up to 70%, thanks to facial recognition enabling rapid, document-free verification," he says. "Multimodal systems, which combine face, fingerprint, iris, and voice recognition, add redundancy, ensuring reliability even if a biometric trait is compromised. Furthermore, decentralized identity frameworks and real-time data sharing between agencies help maintain productivity without compromising privacy or compliance. However, processing speed and productivity represent only one dimension of the benefits."

IDEMIA Public Security's biometric deployments at major airports in the Middle East and Asia have demonstrated the ability to process millions of traveler's annually with minimal manual intervention, affirms Marwan Elnakat, technology and marketing strategy manager at IDEMIA Public Security. "Today, over 15,000 passengers are processed per hour at UAE airports using automated multi-biometric eGates for border control. The system ensures border security with a comprehensive traveler database, enabling the secure storage of facial, iris, and fingerprint biometric data," he says. "To balance security requirements and traveler demands, we collaborate with individual clients and regulatory agencies to identify the best solution. Most of our solutions enable

contactless identity verification and can be seamlessly integrated into existing systems. The balance between security and productivity is achieved through intelligent system design."

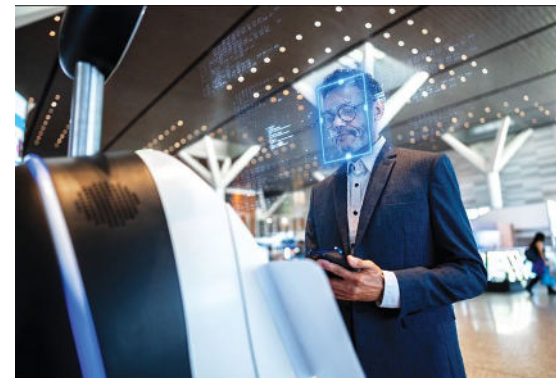
Risk-based orchestration ensures that pre-registered, low-risk travelers quickly pass through automated checkpoints, while those who trigger alerts or have poor-quality matches are seamlessly redirected for secondary screening by human agents, according to Elnakat. "Adaptive quality and match thresholds, an approach supported by NIST research on biometric performance, allow systems to dynamically adapt based on context, maintaining low false alarm rates and rapid throughput. Pre-registration programs and mobile or digital identity verification also contribute to speed. By pre-verifying traveler's identities via secure digital travel credentials (DTC) or mobile IDs, border systems offload part of the verification process, maintaining security and minimizing bottlenecks at physical checkpoints," he says.

DEPLOYMENT STRATEGIES

Sutton observes that airports and border agencies are implementing advanced security measures to prevent breaches and misuse of biometric information, such as facial images and fingerprints. "These biometric data are protected through a multi-layered approach that includes data transformation, encryption, strict access control, and policy-based reporting. The most critical security measure is not storing the raw biometric image. Instead,

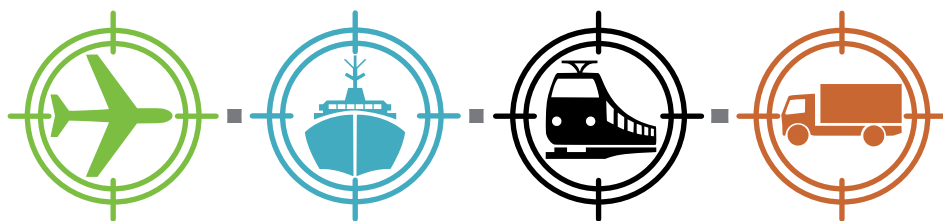
the raw data is converted into a biometric template. This template cannot be reverse engineered back into the original image, making it unusable to fraudsters in the event of theft. Many systems also feature vitality detection and anti-spoofing capabilities to prevent fraud attempts such as the use of masks or synthetic supports," he says. "A key innovation for protecting privacy is the biometric passport, which securely stores a traveler's facial and fingerprint data on a chip embedded in the passport itself. This means that personal biometric identifiers are not stored in centralized databases, reducing the risk of mass data breaches and giving travelers greater control over their information."

Airport operators and airlines around the world are increasingly experimenting with systems that allow passengers to more easily pass through various security



The European Data Protection Board cautions that facial recognition technology can lead to false negatives, bias and discrimination. The misuse of biometric data can also have serious consequences, such as identity theft or impersonation. Individuals should have maximum control over their biometric data, the group advocates.

checkpoints, the EDPB resources illustrate. "It is important to be aware that biometric data is particularly sensitive and that its processing can pose significant risks to individuals. Facial recognition technology can lead to false negatives, bias and discrimination. The misuse of biometric data can also have serious consequences, such as identity theft or impersonation. Individuals should have maximum control over their biometric data. In the EU, there is no uniform legal obligation for airport operators and airlines to verify that the name on a passenger's boarding pass matches the name on their ID, and this may be subject to national laws," the EDPB



says. "Therefore, where no verification of passengers' identity with an official identity document is required, such verification should not be performed using biometric data, as this would result in excessive data processing. We assessed the compliance of the processing of passengers' biometric data with four different types of storage solutions, ranging from those that store biometric data exclusively in the hands of the data subject to those that rely on a centralized storage architecture with different modalities. In all cases, only the biometric data of passengers who actively register and consent to participate should be processed."

The only storage solutions compatible with the principles of integrity and confidentiality, data protection by design and by default, and security of processing are those in which biometric data are stored in the hands of the data subject or in a central database, but with the encryption key held exclusively by that person, according to the EDPB resources. "These storage solutions, if implemented with a list of recommended minimum safeguards, are the only methods that adequately counteract the intrusiveness of processing, offering data subjects maximum control. The solutions based on storage in a centralized database, either within the airport or in the cloud, without encryption keys held by the data subject, cannot be compatible with data protection requirements by design and by default," the EDPB says. "Regarding storage limitation, data controllers must ensure they have sufficient justification for the intended retention period and limit it to what is necessary for the proposed purpose."

International regulations, such as the European Union's General Data Protection Regulation (GDPR), will continue to further shape implementation strategies and the evolution of privacy-protecting technologies, standards, and certifications, affirms Sutton. "For example, the GDPR classifies biometric data as 'special category' information, requiring explicit consent, transparency, and strict purpose limitation. These regulations have led to privacy-by-design approaches, decentralized identity frameworks, and

minimum data retention policies in global aviation systems," he says. "Furthermore, biometric systems are rapidly adapting to digital identity credentials, such as IATA's One ID and ICAO's DTC. These initiatives aim to create seamless, paperless travel by connecting biometric verification with mobile-based digital identities.

Thales designs its solutions to be cyber-secure by design, meaning data protection is built into every layer, from capture to storage and transmission, Bergasse affirms. "Biometric data is end-to-end encrypted, stored in secure environments and accessed only with strict role-based controls. Advanced encryption and anonymization ensure that, even in the unlikely event of a breach, data remains unusable outside of our secure infrastructure," she says. "Global standards like the GDPR and similar frameworks around the world have established a clear direction: citizens must maintain control of their data. We believe that cyber resilience is about anticipating, not reacting. It is not about knowing if a system will be attacked, but when, and ensuring that, when that happens, sensitive data remains protected and trust intact."

IDEMIA Public Security applies multi-layered security measures, including end-to-end encryption, hashing and template transformation techniques, ensuring that biometric images are never stored in an accessible format, Elnakat explains. "Role-based access control, rigorous audit logging, and real-time monitoring

strengthen data protection throughout the system's lifecycle. Templates are typically retained only for the minimum time necessary to complete the verification process, in accordance with privacy-by-design principles. To further ensure data integrity, we maintain compliance with international standards, including regular audits and independent benchmarking to ensure the security and reliability of all its solutions," he says. "Our research teams are strategically located across the EU, particularly in France and Germany, to ensure full compliance and a thorough understanding of the GDPR and the upcoming EU Artificial Intelligence Regulation. Algorithms are constantly being realigned to keep pace with evolving biometric regulations. Furthermore, international regulations such as the GDPR have significantly shaped the way biometric systems are implemented."

HID's cutting-edge facial recognition portfolio is transforming the airport experience, offering travelers a seamless and secure journey powered by innovation and design excellence. Deployed across major international airports, the system integrates Red Dot Design Award-winning Facepods and eGates to deliver a smooth, intuitive, and aesthetically refined user experience. Built on a modular architecture, HID's solution ensures effortless integration into existing airport infrastructures. It combines ethically trained AI algorithms with advanced multispectral imaging to provide industry-leading facial



IDEMIA's Marwan Elnakat says their IDEMIA Public Security product applies multi-layered security measures, including end-to-end encryption, hashing and template transformation techniques, to ensure that biometric images are never stored in an accessible format.

recognition accuracy and robust security. This fusion of technology and design sets a new benchmark for biometric travel, redefining how passengers move through airport environments. Biometric identifiers fall under the "special category data" category under the GDPR, which requires a legal basis and robust data minimization measures, affirms Elnakat. "European data protection authorities have pushed implementers to conduct formal Data Protection Impact Assessments (DPIA) and apply retention and deletion rules that define when and how biometric data can be used," he says. "At the same time, emerging regulations such as the EU AI Act are introducing additional transparency and accountability requirements for biometric technologies. These regulatory frameworks have encouraged developers such as IDEMIA Public Security to strengthen documentation, auditing, and third-party testing, referencing NIST benchmarks to ensure responsible and compliant use of biometric AI in border environments."

IMPLEMENTATION INITIATIVES

While there is no official ranking for the adoption of biometric border controls, several regions stand out in terms of both infrastructure and traveler flow, Sutton affirms. "The EU leads the way in terms of reach and implementation, with its entry/exit system (EES), implemented in the 29 Schengen countries. This system requires biometric registration; namely facial images and fingerprints, for non-EU travelers, replacing manual passport stamping with automated checks. With millions of travelers crossing EU borders each year, the EES will likely become the most comprehensive biometric border system in the world," he says. "In terms of traveler volume, the United States leads the world. U.S. customs and border protection (CBP) has implemented facial recognition at over 50 airports and border crossings, processing hundreds of millions of travelers through programs such as Global Entry and the Biometric Entry-Exit Program. The United Arab Emirates are also piloting high-flow biometric corridors."


Several regions are leading this new era of safe and seamless travel, according to Bergasse. "India, with its DigiYatra initiative, is a pioneer in offering biometric travel experiences at scale. Singapore and other major Asian hubs are setting global benchmarks for seamless AI-powered passenger processing. Thales' biometric border control solutions have been recognized internationally, earning a Frost & Sullivan award for its eGate automated border control (ABC) technology and for its leadership in next-generation border management," she says. "With deployments in Europe, the Middle East, Latin America, Africa and North America, we support governments in strengthening border integrity, ensuring interoperability and preparing their systems for the era of digital travel credentials and secure digital identity."

Elnakat points out that several countries and regions are now recognized as leaders in the adoption of biometric border control. "Australia has implemented IDEMIA Public Security's automated border control solutions at several airports, ensuring swift and secure processing for both incoming and outgoing travelers. Major U.S. airports are conducting real-time trials of biometric verification to streamline immigration and boarding. We have also collaborated with the rise of mobile identification on additional solutions to continue simplifying travel processes. In the U.S., we have partnered with the transportation security administration (TSA) to upgrade its credential authentication technology (CAT Solution), which now accepts state IDs and mobile driver's licenses at security checkpoints," he says.

Pioneering implementations share key characteristics such as clear regulatory frameworks, significant investments in national entry/exit systems, and a willingness to experiment with

technologies that integrate airlines, airports, and border agencies into a unified traveler verification ecosystem, according to Elnakat. "Biometrics are replacing the era of paper travel documentation and manual identity verification, evolving rapidly to support new forms of identity credentials. Biometric systems are being upgraded to verify DTCs and mobile IDs, in line with ICAO standards," he says. "These digital documents are protected by cryptographic keys and linked to the issuing authorities, allowing travelers to authenticate their identities using their smartphones or digital wallets, offering a simple and secure extension of traditional electronic passports."

AN EVOLUTION

The global rollout of biometric border control represents an evolution in transport security where speed, accuracy, and trust must coexist. The successes seen across Europe, the United States, the Middle East, and several Asian hubs highlight how intelligent system design and rigorous governance can deliver measurable benefits for both operators and travelers. However, sustainable progress depends on continued alignment with privacy frameworks such as the EU GDPR and emerging AI regulations. As biometrics become embedded in digital identity ecosystems, the challenge ahead lies not only in technological advancement, but in preserving public confidence through transparency, security, and respect for individual rights. 



India's DigiYatra initiative is a pioneer in offering biometric travel experiences at scale, according to Thales expert Françoise Bergasse. With DigiYatra, travelers pass through various checkpoints at the airport through paperless and contactless processing. The project is being implemented by the DigiYatra Foundation — a joint-venture company whose shareholders are the Airports Authority of India and airports around the nation. Ministry of Civil Aviation Government of India image.