



By James Careless



DEFINING TRANSPORTATION SECURITY:

The Biometric Trends That Will Shape the Next Five Years

Getty Images.



Ajay Amlani
Aware



Arif Mamedov
Regula Forensics



Jeff Lennon
Amadeus



Tim Ferris
IDEMIA

Transportation security has reached a critical tipping point. As cargo and passenger volumes surge globally, the industry can no longer endure the physical bottlenecks of the past.

This is why the next five years will be defined by a massive shift toward biometric identification. From facial recognition to continuous digital authentication, the traditional “show your papers” checkpoint is being systematically dismantled — fundamentally redefining how trust is established and maintained across land, air, and sea.

“The biggest shift will be from repeatedly proving identity to securely carrying trust through the journey,” said Ajay Amlani, president and CEO of Aware, a provider of biometric orchestration and identity solutions. “Instead of identity being a series of disconnected transactions, like check-in, bag drop, security, boarding, immigration, it becomes a trusted layer running across the journey.”

To understand exactly which biometric trends will dominate the next five years and how they will do it, Transport Security International consulted four of the leading voices in the digital identity sector. Their consensus is clear: the technology to create a seamless, touchless journey already exists. The challenge for the next half-decade is putting it in place.

“Ultimately, travelers should not have to prove their identity from scratch at every checkpoint,” noted Tim Ferris, global head of travel and transport at IDEMIA Public Security (IPS), a provider of government-grade biometric and identity verification systems.

Making this happen — and eliminating

current bottlenecks — requires looking beyond physical passports and anchoring security directly to the actual human being using biometric technology.

“What has remained constant is a basic principle: identity ultimately lives in people, not in the documents, devices or databases that represent them,” Amlani said. “Biometric technology gives us a way to anchor the person standing in front of us to a trusted identity with a very high degree of confidence.”

CARRYING TRUST, NOT CREDENTIALS

The foundation for this shift to faster border clearances began with the introduction of “Known Traveler” frameworks. The foundations for this shift can be seen in trusted-traveler programs such as NEXUS and Global Entry, alongside biometric identity services such as CLEAR.

“Known Traveler programs allow individuals who undergo pre-vetting to cross borders more efficiently, often without the need to show a passport, thanks to the use of biometric technology to verify their identity,” said Jeff Lennon, vice president, travel and governments at Amadeus, a travel technology provider. “These programs have operated successfully for many years and while they have scaled to cover frequent travelers, this represents only a minority of border crossing transactions.”

Under the Known Traveler approach, security screening shifts from inspecting physical booklets at every gate to validating pre-established digital trust, allowing passengers to clear customs quickly.

“Known traveler programs serve

different purposes and operate under different models, but they demonstrate a common principle: when a traveler’s identity and eligibility have been securely established in advance, subsequent controls can be faster, more targeted, and more convenient,” Ferris told Transport Security International. “This does not mean reducing security. It means establishing a higher level of trust earlier in the journey, enabling officers to focus their attention on exceptions and higher-risk cases.”

Historically, these fast-pass lanes came as part of a bargain with frequent flyers: if they were willing to undergo extensive background checks to qualify for the program, their reward would be faster border clearance.

“Known traveler programs demonstrated the value of establishing a higher-confidence identity relationship before a passenger reaches a checkpoint,” said Amlani. “Over the next five years, that concept will expand well beyond dedicated programs or expedited lanes. A traveler increasingly will be able to establish who they are before arriving at an airport or the border.”

The real driver of this expansion is the adoption of Digital Travel Credentials (DTCs), cryptographically secured digital representations of the identity information contained in an electronic passport.

“Digital Travel Credentials and wallet-based identities are critical to that evolution,” Amlani noted. “ICAO’s DTC framework is specifically designed to create a globally interoperable digital representation of passport identity information.”



Crucially, DTCs can allow travelers to securely provide verified identity information to authorities before arriving at the airport. This makes the passenger processing experience much faster and smoother once they reach the terminal.

"When equipped with the appropriate information in advance, border authorities can know who is scheduled to arrive in advance," Lennon noted. "This provides two benefits: background checks can take place ahead of time, and authorities can prepare a biometric gallery that enables travelers to be matched against their biometric information, removing the need to scan a passport."

Additionally, extending digital credentials to the broader public allows authorities to segment travelers based on actual intelligence, rather than subjecting everyone to the same rigid assessment process.

"Beyond traditional segmentation based primarily on nationality or travel document eligibility, authorities can distinguish between pre-vetted or previously enrolled travelers, first-time travelers requiring registration, passengers needing additional assistance, and individuals who warrant closer examination," Ferris said. "Directing each traveler to the most appropriate process improves both security outcomes and operational efficiency."

FROM STOP-AND-SCAN TO FREE-FLOW

The shift toward digital credentialing is just one of the trends reshaping transportation security over the next five years. Another is the transformation of the physical checkpoint, which currently relies on a "stop-and-scan" approach. Whether meeting a human officer or encountering an automated eGate, the traveler must step forward, halt their momentum, look into a lens, and wait for an algorithm to assess their face. It is a one-to-one interaction that inherently creates bottlenecks during peak travel hours.

Artificial intelligence (AI) is enabling systems to eliminate the need for passengers to stop at all as they approach the checkpoint.

"AI is allowing us to rethink the checkpoint itself," Ferris said. "Rather than requiring each traveler to stop and present themselves individually to a camera, the solution combines AI and facial recognition to identify and process multiple passengers in real time as they move naturally through a controlled area. Families and groups can remain together, while operators maintain real-time visibility."

Because it is efficient and contactless, facial recognition is emerging as a primary biometric identification system used in transportation. The downside is that relying on a single biometric modality creates vulnerabilities.

Generative AI tools have also made it easier for malicious actors to attempt spoofing attacks. Deepfakes, digital injection attacks, and high-quality synthetic masks have lowered the barrier to tricking facial recognition software. Consequently, systems must deploy advanced liveness detection to ensure the face captured by the camera belongs to a living person.

"AI and machine learning can help improve biometric accuracy, assess image quality, reduce friction for legitimate travelers, and enable systems to adapt more quickly to emerging fraud techniques, including presentation attacks, deepfakes, and digital injection attacks," warned Amlani.

Additionally, facial recognition algorithms can occasionally fail due to lighting, severe camera angles, or sensor limitations. In these situations, border authorities require alternative verification paths.

"Fingerprint, iris, or other biometric modalities can provide an additional layer of assurance, satisfy specific regulatory requirements, or help resolve cases where facial verification alone may not be sufficient," Ferris noted.

To maintain the highest level of security, digital and physical verification methods must operate in tandem.

"This is a double-edged sword," said Arif A. Mamedov, CEO of Regula Forensics, a document verification and forensic software developer. "On the

one hand, properly trained and securely deployed AI can streamline verification, reducing both passenger waiting times and the workload for security personnel... Facial recognition can make the journey faster, but it should not become the only source of trust."





Whether meeting a human officer or encountering an automated eGate, travelers must step forward, stop, look into a lens and wait for an algorithm to assess their face. Getty Images.

"Authenticated documents establish the identity claim, biometrics bind the credential to its holder, and additional signals help detect attacks or resolve cases in which automated verification is inconclusive," Mamedov added. "That means multimodal biometrics, as well as traditional document

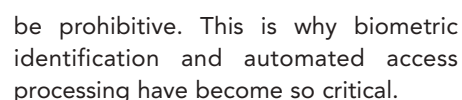
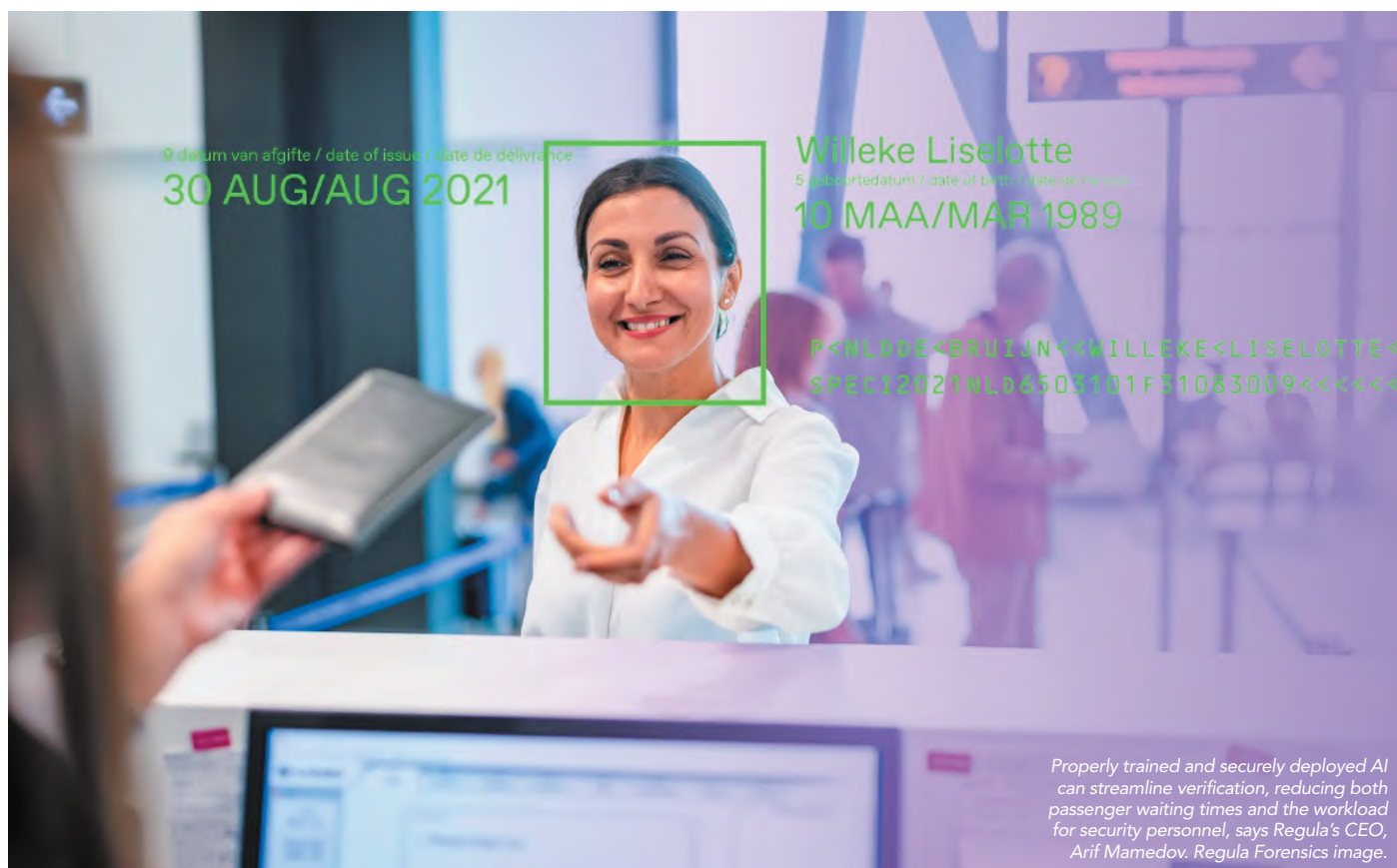
verification and authentication, will remain part of the equation."

SCALING BEYOND PHYSICAL LIMITS

There is a simple, stark physical reality driving the push toward biometric

automation. Across the globe, "passenger volumes are growing far faster than airports or governments can add physical infrastructure and trained personnel," Amlani said.

"Many airports and border crossings face physical infrastructure constraints



"Cost efficiency is another significant driver," Lennon said. "The U.K. Home Office estimates that processing travelers through eGates instead of staffed border checkpoints saves an average of £0.75 per crossing. With more than 100 million travelers using U.K. Border Force eGates in 2025 across more than 30 locations, this large-scale deployment demonstrates how biometrics can deliver meaningful cost savings."

However, the primary goal of using biometrics for access screening is to improve throughput without compromising security — not simply to push people through gates faster for its own sake.

"It depends on what we mean by 'basic efficiency,'" Mamedov cautioned. "If we measure it simply by how quickly someone passes through border control or security, the result can be misleading.

and challenges expanding their workforce,” Ferris agreed. “A model that relies primarily on repeated manual checks at the physical border cannot sustainably accommodate this growth.”

Transportation security officials must

process more people and vehicles in less time or face gridlock that threatens to cripple the entire transit system and supply chain. But even if authorities could address the bottleneck using traditional methods, the financial cost would

I have experienced '20-second border crossings' in two different countries. On paper, the efficiency was identical."

The difference, he explained, lies in what happens behind the scenes during those 20 seconds.

"In one case, within those 20 seconds, the border officer had access to a full set of information: advanced document and biometric verification results, checks from a third-party verification system, and information about the purpose, location, and duration of my stay," Mamedov noted. "So the real driver is not simply greater efficiency. It is increasing security without sacrificing efficiency. The meaningful metric is not processing time alone, but how much reliable information the system can evaluate within that time."

By allowing automation to handle routine verification, frontline staff can

be reserved for the cases that genuinely require human oversight, all while moving larger populations through terminals more effectively.

"The principal driver is the need to deliver stronger security assurance at scale," Ferris said. "They also support more effective traveler segmentation, allowing routine, low-risk travelers to move through automated or self-service channels while officers focus on exceptions, higher-risk cases, and decisions that require human judgment."

TESTING EUROPE'S DIGITAL BORDER

Europe has become the world's most ambitious large-scale proving ground for digital border management. The European Union's Entry/Exit System (EES) became fully operational across

Schengen external border crossings in April 2026, while ETIAS is scheduled to follow later this year.

"The EES and the European Travel Information and Authorization System (ETIAS) demonstrate how border management is shifting upstream," Lennon explained. "EES replaces manual passport stamping with digital registration of biometric and biographical data for third-country nationals entering the Schengen Area, while ETIAS will introduce pre-travel authorization for visa-exempt travelers."

Deploying a unified biometric framework across an entire continent requires linking central European IT infrastructure with the distinct systems of individual nations.

"EES is arguably one of the most ambitious and complex border-



THE SMART CHECKPOINT SOLUTION



 <http://www.nuctech.com/en>  avsec@nuctech.com



For the highest level of security, digital and physical verification methods must work together seamlessly. Getty Images.

transformation programs ever undertaken,” Ferris said. “That means connecting thousands of border-crossing points across air, land, and sea, each with distinct requirements and constraints. A major international airport handling high seasonal passenger volumes faces very different challenges than a remote land border crossing, seaport, or rail terminal.”

For the broader transportation industry, the European rollout illustrates that matching software is only one component of a functioning border environment.

“The lesson for the rest of the world is that identity transformation is an ecosystem project, not an algorithm deployment,” Amlani warned. “The biometric matching technology may be highly mature, but implementation also involves border infrastructure, carriers, government databases, network connectivity, enrollment processes, exception handling, traveler communication, privacy requirements, and thousands of frontline operational decisions.”

Beyond system integration, a primary operational hurdle involves passenger adaptation as travelers adjust to interactive kiosks, biometric scans, and digital pre-authorizations.

“Success depends on effective service design, traveler communication, operational readiness and appropriate safeguards,” Lennon noted. “Today’s challenges are typically less about technology and more about these additional factors. Many travelers still

lack awareness of what is required of them when entering Europe as third-country nationals.”

Because large-scale operational shifts require time for passengers and staff to adjust, digital deployments require ongoing optimization.

“What is already clear, however, is that deployments on this scale involve many moving parts that require continuous fine-tuning and optimization, so there is certainly room for improvement,” said Mamedov. “The broader lesson is that large-scale transformation takes time: technology, processes, infrastructure, and the organizations involved all need to work together.”

EARNING PUBLIC TRUST

As biometric security screening expands globally, its long-term success will be governed by how well systems and operators address public concerns regarding data privacy and surveillance.

“The winners will be systems that make that trust portable without making personal information unnecessarily portable,” Amlani explained. “Privacy-preserving biometrics therefore cannot be something we bolt onto the system after deployment. It has to be an architectural principle. That means minimizing the collection and retention of unnecessary information, protecting biometric templates, securing data in transit and at rest... There is a very important distinction between

knowing enough to trust a transaction and knowing everything about the individual making it.”

To address these concerns, some technology providers are developing decentralized approaches that give travelers greater control over their credentials.

“Amadeus has developed decentralized biometric workflows designed to give travelers greater control over their information,” said Lennon. “Relevant data can be stored locally on the traveler’s device, with only the information needed for each identity check shared at the relevant touchpoint. The information is then removed from that touchpoint in line with the solution’s applicable retention settings.”

Beyond public perception, regulatory differences between nations complicate global deployment.

“Ambiguous or inconsistent requirements across jurisdictions create legal uncertainty, consume resources, and make it more difficult to implement security measures consistently,” Mamedov said. “Clear regulation and transparent implementation are essential if these systems are to remain both secure and effective. Privacy-preserving biometrics are therefore not optional; they are fundamental to sustainable adoption.”

THE INVISIBLE BORDER

Over the next five years, transportation security will continue shifting toward a biometric model. However, national governance will remain the primary framework.

“International travel will remain an exercise in national sovereignty,” said Amlani. “Governments will continue to make their own decisions about admissibility, risk, visa policy, privacy and border control.”

“Complete global standardization is unlikely. Countries will continue to define their own eligibility rules, risk criteria, and immigration policies,” Ferris agreed. “The more realistic objective is therefore not to create one universal travel authorization, but to standardize

the underlying data, technical interfaces, and verification mechanisms.”

Consequently, industry efforts are focusing on global technical interoperability — establishing common data standards that allow different national systems to verify credentials securely.

“We can achieve much greater standardization around how credentials are created, signed, exchanged and verified,” said Amlani. “The real milestone won’t be when everyone uses the same system. It will be when different systems can trust each other.”

As these technical standards develop, physical border processing will continue shifting upstream.

“The next frontier will be the transformation of border security from a fixed physical checkpoint into a distributed security process that begins

well before a traveler arrives,” Ferris predicted. “The objective is not to remove border controls, but to perform them at the most appropriate time and location, supported by trusted identity, real-time intelligence, and a complete view of the traveler’s journey.”

Passenger verification, however, represents only one element of transport security.

“Passenger identity is only one part of transportation security. As passenger processing becomes more efficient, gaps elsewhere (particularly around luggage and cargo) become more visible,” said Mamedov. “So I believe the next major frontier will be bringing these elements together: connecting identity, document, risk, and operational signals across the journey.”

Managing these integrated data

streams will require automated processing systems, though industry experts emphasize that human oversight remains essential for final security decisions.

“Fully AI-based decision-making remains a sensitive subject,” Mamedov noted. “Our approach is to use AI as a powerful tool, but not as the ultimate decision-maker.”

By deploying biometric identification and automated data processing while maintaining human oversight for critical evaluations, transportation security can accommodate rising cross-border transit volumes without lowering operational standards.

“If we get that right, transportation security can become both stronger and less visible,” Amlani concluded. “Which is ultimately where this technology should take us.” 



ArchiteCT and SIMFOX CT deliver

FLEXIBLE & TARGETED SECURITY TRAINING

From customised 3D image creation to realistic screening simulation



+44 20 8457 9111 info@renful.co.uk www.renful.co.uk