WHITE PAPER

Unlocking Efficiency at Scale:

The Role of Digital Identity in Border Transformation

ENTRUST

SECURING A WORLD IN MOTION

Contents

Introduction

Global mobility has entered a new phase of scale and complexity. International travel volumes across air, land, and maritime borders have rebounded sharply and are now exceeding pre-pandemic levels in many regions.

Airports worldwide handled an estimated **9.4 billion passengers in 2024,** surpassing 2019 volumes, while international tourism reached approximately **1.52 billion arrivals in 2025,** nearly a full recovery to historic highs. At the same time, land borders continue to process tens of millions of vehicle and pedestrian crossings annually, while maritime borders continue to pose challenges for seamless border control amidst geo-political tensions.

This unprecedented scale places sustained pressure on border control authorities. Legacy, document-centric border processes, designed for much lower volumes and dependent on manual inspection are increasingly unable to deliver both **security** and **facilitation.** Inconsistent procedures, fragmented identity checks, and late-stage risk assessment introduce operational bottlenecks while expanding security exposure.

Digital border transformation addresses this challenge by shifting border decision-making earlier in the journey and anchoring it in high-assurance digital identity derived from ePassports. When traveller identity can be verified once, digitally, and reused securely across the journey, passenger data exchange becomes more accurate, border processes become more predictable, and traveller experiences become measurably smoother – without compromising national security.

Inconsistent Border Processes Create Both Risk and Friction

Traditional border control models rely heavily on physical document presentation at the point of arrival. Identity verification, eligibility checks, and risk assessment are often concentrated at the border itself, when time pressure is highest and options are limited.

This model creates three systemic challenges:

1. **Repeated identity checks with limited trust reuse**
   Traveller identity is assessed multiple times, during application for travel permissions, at check-in, boarding, and finally at arrival, with the same passport inspected repeatedly, adding friction, yet the chain of trust is never truly consolidated.

2. **Late risk discovery**
   When identity confidence is low or fragmented, risk assessment is delayed until arrival. This increases secondary inspections, manual interventions, and the likelihood of congestion or diversion.

3. **Uneven traveller experience**
   Low-risk travellers are treated the same as unknown travellers, leading to unnecessary queuing and frustration, while officers are forced to spend time on routine checks rather than targeted enforcement.

As traveller volumes grow, these inefficiencies scale non-linearly, creating pressure not just on throughput, but on security outcomes.

From Physical Documents to Trusted Digital Identity

Digital border transformation does not replace the passport; it **extends its trust digitally.**

Modern digital travel credentials can be **derived directly from the ePassport,** using the cryptographic integrity of the passport chip and biometric binding to create a secure digital representation of the traveller's identity. This digital identity can be verified remotely and reused securely across border processes, with the traveller remaining in control of when and how it is shared.

Rather than treating passenger data systems as standalone capabilities, forward-looking border strategies recognize that **identity assurance is the foundation on which all reliable data exchange depends.** When the traveller's identity is cryptographically verified and biometrically bound:

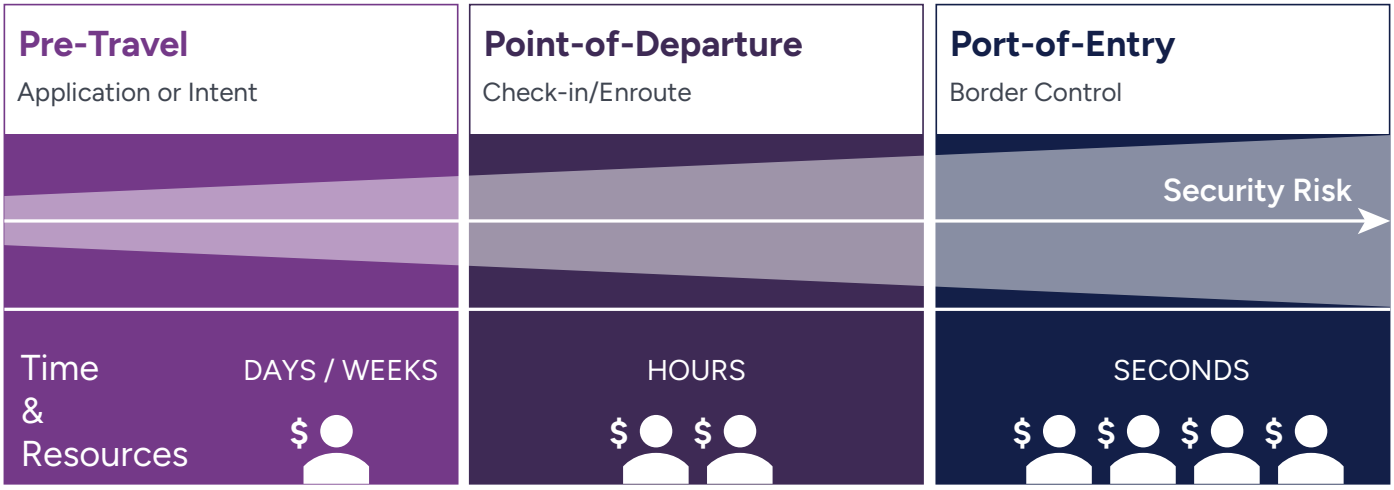
- Passenger data becomes more accurate and trustworthy
- Automated decision-making becomes more reliable
- Manual intervention is reserved for true exceptions

In effect, **digital identity turns passenger data from "information" into "evidence."**

Transforming the Travel Continuum With Digital Identity

Digital borders are most effective when designed across the entire travel continuum: from pre-travel to the point of departure (check-in), and finally to arrival at the port of entry, rather than as isolated checkpoints.

Improving National Security Using a Layered Border Management Approach



The effort and resources required to identify risky travelers increase as decisions are made closer to the physical border. When risk is assessed early, at the application or intent stage, border authorities have several days or weeks to automate checks and resolve issues with minimal disruption. As travelers move closer to departure, the same decisions require more coordination, manual intervention, and operational effort. At the port-of-entry, officers have only seconds to act, making risk identification far more resource intensive, disruptive, and costly. A layered border management approach shifts effort upstream, improving security while reducing pressure on frontline operations.

Pre-Travel: Establishing Trust Before the Journey Begins

The earliest opportunity to improve border security is **before the traveller departs**.

Digitally enabled pre-travel processes allow travellers to complete immigration formalities remotely, using mobile devices to verify their identity against their ePassport. Biographic and biometric data can be validated in advance, significantly reducing uncertainty later in the journey.

The UK Electronic Travel Authorization **(ETA)** program illustrates the impact of this approach at a global scale. Introduced to eligible travellers worldwide over the course of a year, the program is built to process millions of travellers annually. Robust identity verification is integrated as part of the ETA application process, that helps establish the traveller's identity at a high level of identity assurance. Automated decision-making, combined with robust facial biometric matching using ePassport data read via NFC, enables a majority of eligible travellers to receive an ETA decision within a day of application.

Since launch, digital identity technology has supported the issuance of **over 20 million ETAs**, demonstrating that the right technology powering high-assurance identity verification can operate reliably at scale.

Point-of-Departure: Reliable Data Depends on Reliable Identity

As travellers move closer to the border, multiple streams of passenger data are exchanged between carriers and governments. The value of this data depends directly on the **confidence in the underlying identity**. When passenger identity is verified digitally and consistently, rather than inferred from repeated visual document inspection, authorities can:

- Perform earlier and more accurate risk segmentation
- Reduce false positives caused by name variations or document errors
- Shift decision-making away from the physical border

Digital identity shared in advance of travel enables border agencies to arrive at the border **already knowing who is arriving, with high confidence**, allowing resources to be positioned proactively rather than reactively.

Arrival at the Border: From Inspection to Confirmation at Port-of-Entry

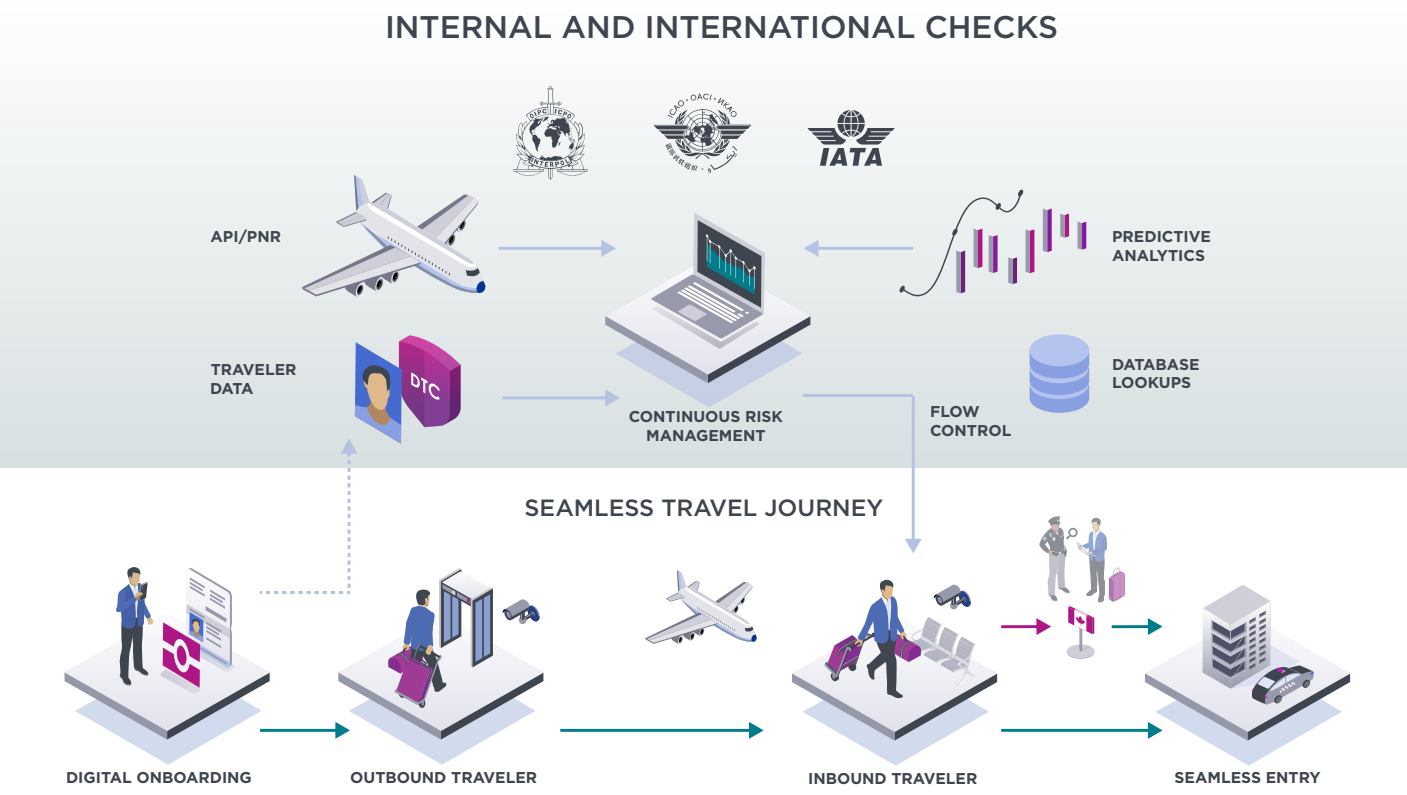
At the physical border, digital identity enables a fundamental shift in posture, **from inspection to confirmation**.

For eligible travellers, identity and eligibility have already been established. Arrival becomes a matter of confirming presence and liveness, rather than repeating full document checks. Automated gates, contactless flows, and biometric matching can be used confidently because the underlying identity has already been verified.

The Curaçao Express Pass program demonstrates this model in operation. Travellers complete a digital immigration process before travel, use their mobile device to share a secure digital credential derived from their passport, and are then able to enter through **contactless eGates** at the airport. The program was designed with a privacy-first, consent-based approach and without additional effort by airlines or airports.

Within six months of launch, **50,000+ travellers** had created and shared digital credentials, with transaction volumes exceeding **100,000** by late 2025 and adoption continuing to accelerate.

The Digital Chain of Trust



The Digital Chain of Trust: Verified digital identity forms the Chain of Trust across the travel continuum, from pre-travel and check-in to arrival at the physical border to enhance passenger facilitation and strengthen border security.

A Phased Approach to Digital Border Transformation

Modern border transformation progresses from upstream identity verification to fully orchestrated, real-time border operations.

Phase	Focus	Key Capabilities	Outcome
Phase 1	Digitalize Pre-Travel	• ETA / eVisa modernization • Remote identity verification (ePassport + biometrics)	Early risk detection and improved data quality
Phase 2	Introduce Digital Credentials	• ePassport-derived digital identity • Mobile wallet integration (consent-based sharing)	Reusable, high-assurance digital identity
Phase 3	Enable Biometric Flow at Border	• Facial recognition • Exception-based processing	Faster throughput and focused enforcement
Phase 4	Continuous Orchestration	• End-to-end journey orchestration • Real-time risk updates	Adaptive, data-driven border operations

Delivering Digital Identity at Scale

What to look for in a trusted partner

Successful digital border transformation requires integrated capabilities across identity, security, and operations. Entrust supports governments with:

- **Proven national-scale deployments**
  Experience supporting high-volume identity and travel authorization programs
- **End-to-end identity capabilities**
  From identity verification to credential lifecycle management and authentication
- **Privacy-first architecture**
  Designed around consent, data minimization, and decentralized identity models
- **Standards-based interoperability**
  Alignment with ICAO, ISO, and emerging digital identity frameworks

CONCLUSION

Security, Efficiency, and Experience Are No Longer Trade-Offs

A common misconception is that stronger security inevitably leads to more friction. Digital border programs demonstrate the opposite: **earlier, stronger identity verification reduces friction at the border**. The programs outlined here have demonstrated the following outcomes:

- **Improved security:** Higher confidence in traveller identity, earlier risk detection
- **Operational efficiency:** Fewer manual inspections, reduced queue volatility
- **Traveller satisfaction:** Predictable, transparent, and faster border experiences
- **Economic impact:** Smoother borders directly support tourism growth and trade

Digital Identity Is the New Border Infrastructure

By anchoring border processes in high-assurance digital identity and extending that trust seamlessly across the travel continuum, governments can transform border control from a bottleneck into a strategic capability: one that is secure, scalable, and traveller-centric.

The experiences of large-scale national programs and agile island states alike show that this transformation is not theoretical. It is achievable today, with the right combination of standards-based identity, privacy-first design, and proven digital technology, quietly powering borders that are both secure and seamless.

Next Steps for Government Agencies

Moving from strategy to implementation

As border modernization becomes a strategic priority, agencies can take practical steps today:

- **Assess current infrastructure**
  Identify gaps in identity assurance, data integration, and border processes
- **Define a phased roadmap**
  Align transformation with operational priorities and policy objectives
- **Pilot high-impact use cases**
  Start with pre-travel identity verification or automated border flows
- **Plan for ecosystem interoperability**
  Ensure systems can integrate across agencies and international partners
- **Engage experienced technology partners**
  Collaborate with providers who have deployed population-scale identity initiatives

Schedule a technical briefing or workshop to explore how a phased digital identity strategy can be applied to your border environment.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with comprehensive identity-centric security that protects people, devices, and data. Our solutions help enterprises and governments safeguard critical systems from every angle, enabling secure onboarding and issuance, providing everyday identity protection, and empowering them with 360-degree visibility and orchestration across keys, secrets, and certificates so they can transact and grow with confidence. Building on our decades as a pioneer and innovator in establishing trust, Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION