WHITE PAPER



European Digital Travel – Turning Policy Into Operational Reality

ENTRUST
SECURING A WORLD IN MOTION

Executive Summary

Europe is forging ahead with a raft of key policy initiatives aimed at securing its borders and enabling digital services for travellers and citizens. To achieve this, technology will play a pivotal role in mitigating security challenges and supporting continued free movement throughout the European Union.

In this paper, Entrust examines these initiatives, explores areas where questions remain, and sets out how and where key technologies – including mobile digital identity and pre-registration solutions – will turn policy into operational reality and enable hundreds of millions of people to travel safely, securely, and seamlessly on their journeys to, from, and throughout Europe.

Travellers and citizens rightfully expect seamless and secure digital experiences, whether at the border or when accessing e-government services. For over 50 years, Entrust has provided secure credential issuance solutions to enable these interactions for customers in more than 150 countries.

We welcome your comments and feedback on this paper and stand ready to support European institutions, agencies, and Member States in their ambition to digitalise migration and border management, turn policy into operational reality, and help Europe achieve its strategic aim of digital sovereignty.



Understanding the EU Digital Travel Ecosystem

Under the banner of its flagship policy package, Smart Borders[1], the European Commission Directorate-General for Migration and Home Affairs (DG HOME) has advanced a raft of initiatives on Migration, Asylum, Internal Security, Schengen, Visas, and Border Management.

To operationalise these policies, core pan-European systems have been deployed, with others in varying stages of design and development. Chief among these are the Schengen Information System (SIS), Visa Information System (VIS), shared Biometric Matching Service (sBMS), and the European Entry/Exit System (EES). These will be complemented by the European Travel Information and Authorisation System (ETIAS), scheduled for launch in early 2027.

Combined, these systems (and others) create an EU Digital Travel Ecosystem that will strengthen European border security at external borders for the efficient processing and risk assessment of non-EU travellers (i.e., third-country nationals (TCNs)).

Looking ahead, plans are underway to digitalise and centralise the Schengen Visa issuance process with the implementation of the EU Visa Application Platform (EU-VAP). To further digitalise border management processes, the Commission has proposed an EU Digital Travel Application (DTA) and the use of Digital Travel Credentials (DTCs) at external borders, with an expected delivery timeframe of 2030. The proposal has been well received by the European Parliament. The Committee on Civil Liberties, Justice and Home Affairs (LIBE) voted in December 2025[2] to endorse the proposal and commence negotiations with the Commission and Council, advocating for an accelerated implementation timeframe of 18 months after the regulation enters into force.

eu-LISA – The Digital Heart of Schengen

To deliver on these commitments, the European Parliament and the Council of the European Union adopted Regulation (EU) 1077/2011[3] and established the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. Better known as eu-LISA, the agency has been operational since 2012 and now has a well-established track record of delivering and managing core pan-European systems and a clear mission to support EU Member States in their digitalisation efforts and keep Europe safe through technology.

Strategically, the direction of travel for Europe is clear: The future of migration and border management is digital. However, the journey so far has not been without its difficulties, and further challenges lie ahead.



[1] Ref. European Commission – https://home-affairs.ec.europa.eu/policies/schengen/smart-borders_en

[2] Ref. European Parliament – https://www.europarl.europa.eu/news/en/press-room/20251201IPR31708/meps-endorse-digital-pre-clearance-system-to-speed-up-eu-border-crossings

[3] Ref. Official Journal of the European Union – https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R1077

European Entry/Exit System – Implementation Challenges

The European Entry/Exit System (EES) captures travel document information and biometric data of all non-EU nationals each time they cross an external border, creating a digital record of the date, time, and place of each crossing. EES replaces the manual stamping of passports, strengthens border security, mitigates illegal immigration, and improves the detection of overstayers, fake identities, and forged travel documents.

However, its implementation was mired in delays. The system finally entered into operation in April 2026 following a phased rollout that saw operational challenges, long queues, and significant delays at border crossing points. In the months prior to full implementation, EES came under harsh criticism from industry bodies including the International Air Transport Association (IATA), Airlines for Europe (A4E), and Airports Council International (ACI), who warned of severe disruptions and queues potentially reaching four hours or more.

Arguably, one of the principal reasons for EES' troubled implementation has been the lack of a viable mobile pre-registration solution. This will allow third-country nationals (TCNs) to submit biographic data, authenticate their travel document, and provide biometric information before arriving at the border, thereby drastically reducing queues and minimising the amount of data border systems and officers need to capture (and verify) upon arrival.

To address this, the European Border and Coast Guard Agency (Frontex) advocated adopting its *Travel to Europe*[4] app, but with limited success. Indeed, time and technology have moved on since Frontex first built the pilot app. Better alternatives are now commercially available and deployed in operational environments by other national governments.

At Entrust, we recognise the importance of adhering to well-established procurement rules and the value EU agencies derive from assessing a range of different solutions and approaches to deliver their requirements and ensure value for money for Member States.

We recommend the Commission, eu-LISA, Frontex (et al.) consult with industry to examine the functionality gaps of the pilot *Travel to Europe* app, capture lessons learned from the many recent DTC pilots implemented with Member States, and learn from the performance of the UK Electronic Travel Authorisation (ETA) and EU Settlement Scheme (EUSS) solutions – both of which are currently performing millions of transactions per year. These findings will inform – and derisk – the design of a mobile pre-registration solution for EES, ETIAS, EU-VAP, and the EU Digital Travel Application (DTA).

To mitigate future challenges, it will be vital to fully explore how processes and systems – both current and future – interoperate. The design of new services and capabilities must guarantee they are fit for purpose to enable eu-LISA, Frontex, and Member States to confidently comply with EU regulations, strengthen border security, enable digital travel, and build systems that are compliant, secure, scalable, interoperable, and future-proof.

[4] Ref. Frontex – https://www.frontex.europa.eu/what-we-do/etias-ees/travel-to-europe-app/

Current State of Play

At present, SIS, VIS, and sBMS are fully operational. EES is now fully operational, albeit without a viable mobile pre-registration solution.

While some believe they have a clear understanding of how digital travel policy and regulation will become operational reality – and how business processes, services, and capabilities will interoperate – not all stakeholders share that view. More work is needed to provide clarity. And more consultation and engagement are essential to ensure key stakeholders – including carriers, port operators, and technology providers – have a clear, shared understanding of the future shape and scope of the EU digital travel ecosystem and its potential implications for citizens and governments of non-Schengen EU Member States, i.e., Cyprus and Ireland.[5]

Key Questions and Gaps in Current Thinking

Questions and concerns remain. When exploring various scenarios as to how and when data will be captured and verified, gaps in the current thinking emerge:

- How will Member States configure arrivals and departures processes to differentiate between those who have and those who have not already registered in EES?
- How will Member States (and the systems that support them) manage variations in data retention periods, recognising that a traveller's ETIAS could have been issued many weeks or months prior to their arrival at the border and will therefore expire while their EES record remains active?
- How will Member States differentiate between those who are in possession of a government-issued Digital Travel Credential (i.e., Type 2) and one that is self-derived and self-verified (i.e., Type 1)?
- Assuming a viable mobile pre-registration solution is adopted by Member States, will travellers be able to proceed directly to an automated border control system (i.e., e-gate) to provide their fingerprints and complete the EES registration requirement?
- Once ETIAS and EU-VAP are implemented – and assuming travellers will be able to apply for each using a DTC (government-issued or self-derived) – will they be able to proceed directly to an automated border control system upon arrival to provide their fingerprints and complete the EES registration requirement?
- When EU stakeholders are satisfied that technology solutions can reliably capture and bind fingerprints to a person's identity, will this allow for all pre-registered travellers to use automated border controls, understanding that all requisite biographic and biometric data will have been captured, verified, and submitted in advance of their arrival?
- Will Member States be required to upgrade automated border control systems to allow travellers to use their DTC instead of their biometric passport; and for fingerprints to be captured (for TCNs pre-registered in EES) and/or randomly verified (for TCNs already registered in EES)?
- Will the European Commission advocate that the International Civil Aviation Organization (ICAO) allow for fingerprint data (where it is available) to be included in the DTC technical standards?
- Will the use of DTCs be available to non-Schengen EU Member States (i.e., Cyprus and Ireland)?

[5] NOTE: The European Commission has confirmed that Cyprus meets all technical requirements. A political decision from EU Member States on its full accession is anticipated in 2027.

Key Questions and Gaps in Current Thinking (continued)

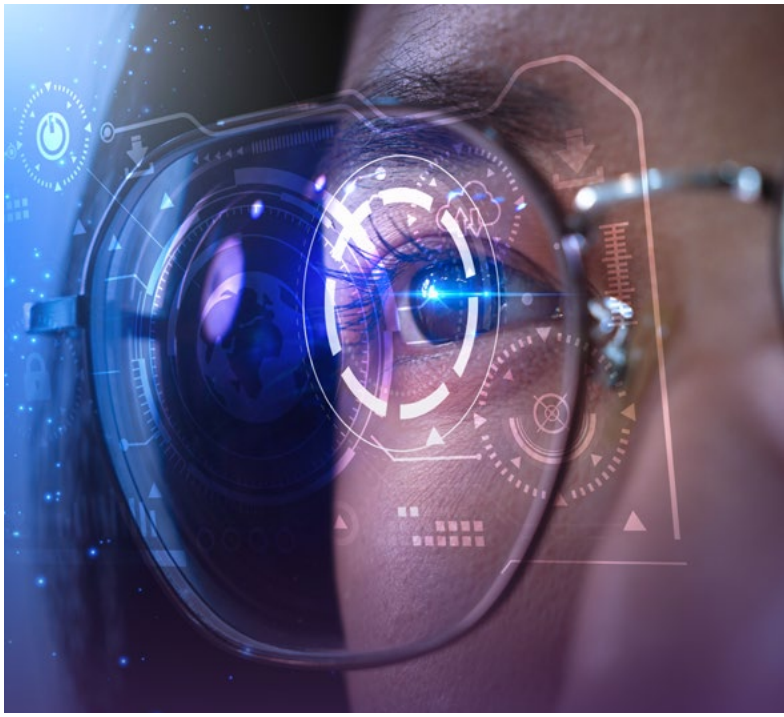
- Recognising that the EU has made significant progress on the design of European Digital Identity (EUDI)[6] Wallets and the supporting regulatory framework, eIDAS[7], what steps will the Commission take to address interoperability concerns regarding the use of other available wallets such as Apple, Google, GOV.UK, IATA One ID, and others?
- Understanding that EU Member States will ultimately be responsible for the issuance of Digital Travel Credentials (DTCs) to their citizens and, as such, be the guarantors of their security and the integrity of the issuance process, how will the Commission and its agencies ensure a common approach to the issuance, security, and usability of Member State-issued DTCs?
- What considerations have been made for dual-national EU citizens who legitimately hold more than one passport and may be in possession of multiple DTCs, including those issued by a third country?
- What considerations have been made to ensure citizens' identity data, stored in a European Digital Identity Wallet, is only made available, in part or in whole, to legitimate actors for legitimate purposes and securely stored and accessed in a manner consistent with GDPR?

These are just some of the questions arising from the current state of play regarding EU policy development and the planned regulatory environment.

From a safeguarding standpoint, it will be vital to ensure that future systems limit the amount of data required and the length of time it can be stored, and protect fundamental rights. Solutions must be engineered to guarantee Privacy by Design and Privacy by Default as set out in Regulation (EU) 2018/1725[8] and support the goals of the European Data Protection Supervisor (EDPS) by ensuring a consistent application (and enforcement) of data protection laws.

From a technology design and implementation standpoint, it will be essential to clarify (and differentiate) the roles of eu-LISA and Frontex, understand Member State obligations, determine the technical architecture of the EU digital travel ecosystem, and establish clear timelines to allow for consultation and engagement with industry stakeholders and specialist technology providers. Doing so will increase the readiness of industry and Member States to ensure implementation deadlines are achievable and new capabilities fully integrate with EES, ETIAS, EU-VAP, DTA, and future systems and processes.

More detailed technical questions regarding the detection of deepfakes and the ability to prevent presentation, morphing, and injection attacks – as well as the risks posed by the misuse of AI – will also need to be fully explored and answered to ensure future system designs can combat a significant rise in fraudulent attacks.



[6] Ref. European Commission EU Digital Identity Wallet – https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU+Digital+Identity+Wallet+Home

[7] Ref. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. Ref. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[8] Ref. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 – https://eur-lex.europa.eu/eli/reg/2018/1725/oj/eng

The Emerging EU Digital Travel Ecosystem

The emerging EU digital travel ecosystem follows a well-established principle adopted by countless governments around the world: **Risk-assess high-quality, verifiable data as early in the process and as far from the border as possible.**

As the future of migration and border management becomes increasingly digital, the principle of risk-assessing high-quality, verifiable data early in the process shall remain unchanged. In fact, with the right thinking and architecture, the principle becomes simpler to achieve for each of the many varied cohorts of travellers: visa holders, non-visa holders, first-time visitors, returning visitors, etc.

The Path to Convergence

To ensure convergence, technologies and knowledge systems must support one another in pursuit of a common goal: securing Europe's borders. At Entrust, we understand that this notion of convergence is the foundation of the Commission's proposal for a regulation establishing an application for the electronic submission of data (EU Digital Travel Application)[9] and the use of Digital Travel Credentials (DTCs).

A mobile pre-registration solution will enable third-country nationals to either submit their government-issued DTC or create one, establishing a secure, verifiable digital identity in advance of travel.

For those who do not require a Schengen Visa and only need an ETIAS, the same mobile pre-registration solution will enable them to share their DTC during the application process and, once issued, their data can be made available to EES prior to their arrival at the border. And for those who are not eligible to apply for an ETIAS and require a visa, they too will be able to share their DTC when making their applications via the EU Visa Application Platform (EU-VAP).

Crucially, pre-registration ensures compliance checks are conducted before the border and provides a higher level of assurance for carriers (e.g., airlines, cruise operators) that each passenger has the requisite documentation to travel to Europe and will not be deemed inadmissible upon arrival.

[9] Ref. European Commission (DG HOME) – https://home-affairs.ec.europa.eu/proposal-regulation-establishing-application-electronic-submission-data-eu-digital-travel_en



EU Digital Travel Ecosystem

CURRENT SYSTEMS · EU LEVEL · LIVE

SIS | Schengen Information System

Cross-border alerts on wanted persons, missing individuals, and stolen objects.

sBMS | shared Biometric Matching Service

Common biometric repository enabling fingerprint and facial recognition matching across SIS, VIS, EES, and Eurodac.

VIS | Visa Information System

Stores Schengen short-stay visa data and biometrics. Will remain the principal visa system behind the planned EU-VAP.

European Entry/Exit System (EES) — OPERATIONAL SINCE APRIL 2026

Records the entry and exit of all non-EU nationals (TCNs) at Schengen external borders, capturing travel document and biometric data. Replaces manual passport stamping and improves detection of overstayers, fake identities, and forged travel documents.

NUI · National Uniform Interface

NATIONAL LEVEL

National Border Management Systems

Member States operate national systems that interface with the central EES system via a National Uniform Interface (NUI), defined by Regulation (EU) 2017/2226 and based on common technical specifications, enabling secure connectivity between the central system and national border infrastructure and systems in each Member State.

FUTURE SYSTEMS · EU LEVEL

ETIAS | European Travel Information & Authorisation System — Early 2027

Pre-travel authorisation for visa-exempt non-EU nationals. Complements EES with advance risk screening before travel.

EU-VAP | EU Visa Application Platform — Front end to VIS

Single online platform to digitalise the Schengen visa application process.

EU Digital Travel Application & Digital Travel Credentials — Expected 2030

EU Digital Travel Application & Digital Travel Credentials – optional mobile pre-clearance for EU and non-EU travellers at Schengen external borders. Expected delivery 2030; LIBE advocates implementation 18 months after entry into force.

DEPLOYMENT ROADMAP

- **ACTIVE NOW: SIS · sBMS · VIS · EES**
  Deployed EU-level operational systems
- **FROM 2027: ETIAS**
  Pre-travel authorisation for visa-exempt TCNs
- **NEAR FUTURE: EU-VAP**
  Online Schengen visa applications; records held in VIS
- **EXPECTED 2030: EU DTA + DTCs**
  EU Digital Travel Application & Digital Travel Credentials

TRAVELLER ROUTES

Visa-exempt TCN	ETIAS → EES
Visa-required TCN	EU-VAP (records in VIS) → EES
All TCNs at the border	EES registration or check · SIS & sBMS
EU citizen	No ETIAS or EES · DTC optional

MOBILE PRE-REGISTRATION · BEFORE THE BORDER

TCNs submit biographic data, authenticate their travel document, and provide biometrics before arriving at the border. Data flows to ETIAS or VIS and to EES, enabling triage and the use of a verified DTC at border crossing points.

Operational management: eu-LISA · Policy: European Commission (DG HOME)
Frontex: European Border and Coast Guard Agency

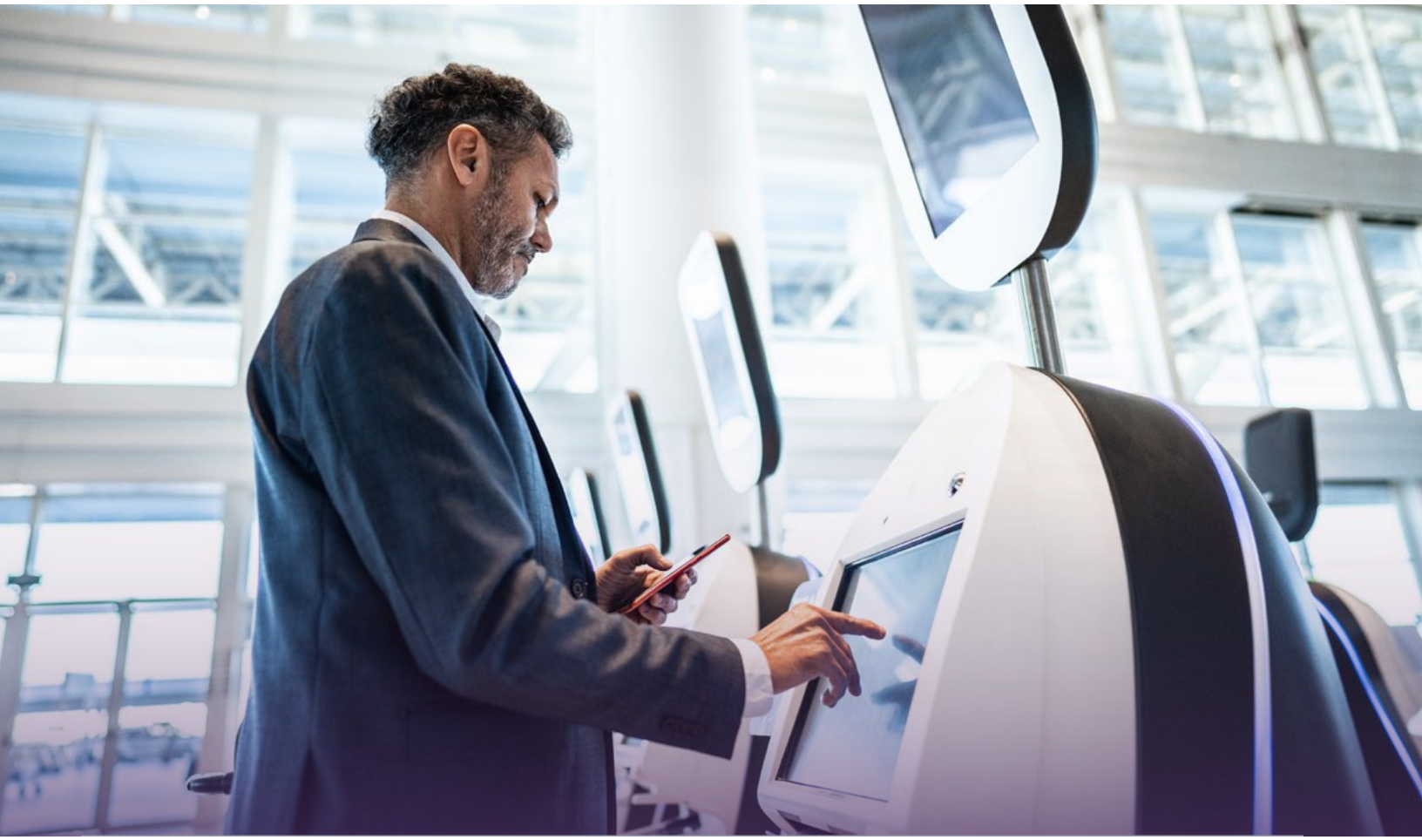
Critical Success Factors: Interoperability, Harmonisation, Industry Engagement

For this regulation to succeed and become an operational reality, interoperability is critical. This will ensure consistency of data formats, verification mechanisms, and document authentication. It will mitigate the risk of fragmentation – i.e., Member States adopting different approaches, creating additional costs, slowing adoption, and generating confusion and friction for travellers at EU ports and borders.

To achieve consistent security outcomes, it will be vital to continuously enhance the EU Digital Travel Application's ability to detect fakes, prevent increasingly sophisticated attempts to undermine the security of digital identity systems, and ensure the workloads of border guards are not adversely or negatively impacted.

In this regard, eu-LISA's role will be invaluable. The agency's role in designing the system architecture, defining technical and functional specifications, ensuring interoperability, coordinating testing, and supporting Member States in national-level integration and implementation is critical.

We recommend eu-LISA engage early and regularly with key stakeholders – particularly specialist technology providers of digital identity solutions, including Entrust – and solicit constructive challenge to ensure requirements and architectures are scalable and future-proof, and implementation timescales achievable.



Pre-Registration as a Triage Tool

The launch of EES, ETIAS, the EU Digital Travel Application (DTA), and the use of DTCs creates an unprecedented opportunity to rethink how travellers are processed at (and experience) EU borders.

Mobile pre-registration should not be viewed merely as an add-on "digital convenience feature." It is a core operational triage mechanism that enables border authorities to prioritise processing, reduce errors, and improve the overall traveller and border experience. It should be seen as a powerful tool to enhance operations and prioritise travellers who have completed key digital pre-clearance steps, differentiating those with an ETIAS, those with a Schengen Visa, those needing to complete their EES registration, and those who are already fully registered.

Crucially, from an operational perspective, this triage approach will reduce queues, wait times, and demand on border guard resources – especially during peak hours of operation. And for passengers, it will reduce friction and significantly enhance the experience of entering and exiting the European Union.

By translating system architecture into traveller journey scenarios, use cases help clarify how (and where) we bridge the gap between policy and operational reality. Scenarios, such as those on page 11, illustrate how diverse traveller profiles will use DTCs and interact with EES, ETIAS, EU-VAP, and DTA – demonstrating the importance of an effective triage tool.

To enable triage, a mobile pre-registration solution should include:

- Document authentication
- Travel status verification, visa, exceptions, etc.
- Passive authentication (i.e., validate document against Country Signing Certificate Authority)
- Biographic data capture
- Biometric data capture (face, liveness detection)
- Deepfake and fraud attack prevention
- Workflow routing to ETIAS, EU-VAP
- Secure data sharing with EES
- Creation and use of verified Digital Travel Credential (DTC) at border crossing points

The Importance of Triage at the Border

From conversations with senior leaders responsible for border management, including EU Member States, we sympathise with the challenges they experienced in implementing EES. Effecting change on this scale was always likely to encounter difficulties.

We do, however, firmly believe that much of this difficulty could have been minimised by implementing triage "before the border" and offering differentiated processing based on traveller profiles "at the border" – particularly between those already registered in EES and those presenting at the border for the first time.

Insights (to Date)

Through five decades of providing secure credential issuance solutions in more than 150 countries, we have gained truly unique insights into what works (and what doesn't) when it comes to operationalising digital pre-registration / pre-clearance solutions.

We have several operational systems, including two large-scale deployments at Europe's external border with the United Kingdom, that perform millions of transactions every year. We know that advance verification and risk-based processing can be seamlessly integrated into digital identity solutions, enabling operations to perform an effective triage of arriving/departing passengers on the day of travel – without compromising security.

Use Cases: Traveller Journey Scenarios

PRE-REGISTRATION AS A TRIAGE TOOL

TRIAGE DETERMINES

Traveller Type
EU citizen or third-country national (TCN)

Purpose and Length of Stay
Short or long stay

Authorisation
ETIAS, Schengen visa, long-stay visa, or none required

EES Status
First entry registration, already registered (subsequent entry), or N/A

Timing
Before the border or at the border

Requirements are set before travel; travellers are routed at the border.

Pre-Travel	En Route	At the Border	Repeat Travel
Travel Intent Purpose and length of stay: Tourism, business, or study 1 2 3 4	**Carrier Check** Travel authorisation and documents verified before boarding 1 2 3 4	**Document Presentation** Passport or DTC; long-stay visa shown by #4 1 2 3 4	**EES Record Reused** Verification instead of re-registration on subsequent border crossings 1 2 — —
Authorisation ETIAS (1) · Schengen visa via EU-VAP/VIS (2) · long-stay visa (4) · N/A for EU citizens (3) 1 2 — 4	**Advance Risk Assessment** Pre-submitted data assessed as early and as far from the border as possible 1 2 (3) 4	**Triage Routing** E-gate, kiosk, or manual lane, based on pre-clearance status 1 2 3 4	**Pre-Cleared Repeat Trips** Repeated subsequent crossings pre-cleared through mobile triage 1 2 (3) 4
Mobile Pre-Registration Document and passive authentication, biographic data, face capture with liveness, fraud and deepfake checks 1 2 (3) 4		**EES (Short-Stay TCNs)** Registration on first entry, or verification if already registered, via the national border system and its NUI 1 2 — —	**Less Friction** Faster processing and fewer manual interventions 1 2 3 4
DTC / EU DTA Create or share a Digital Travel Credential; submit travel data via the EU Digital Travel Application (1) (2) (3) (4)		**Entry Decision** Cleared, or referred to a border guard 1 2 3 4	

● Applies
○ Optional
— N/A

1 TCN Tourist (Visa-Exempt)
ETIAS from early 2027 + EES

2 TCN Visa Traveller
Schengen visa via EU-VAP/VIS + EES

3 EU Citizen
No ETIAS or EES; DTC optional

4 TCN Student (Long-Stay Visa)
No ETIAS; not registered in EES

Mobile pre-registration is a core operational triage mechanism that enables border authorities to prioritise processing, reduce errors, and improve the overall traveller and border experience.

Technology Evolution & Innovation Opportunities: Keeping Pace With Regulation

Technology continues to evolve at pace. And that presents both challenges and opportunities. Advances in technology routinely outpace regulations, resulting in solutions that are neither best of breed nor cost-effective. This can be further compounded by regulatory frameworks that do not provide sufficient flexibility to source new solutions (and/or replace outdated components and algorithms) mid-way through the contract or regulatory cycle. Regrettably, EES – based on regulations drafted a decade ago – did not fully anticipate the need for a mobile pre-registration solution. Its requirement to capture and verify data on the day of travel under the supervision of a border officer contradicts well-established global best practice.

On the Front Line: The Rise of Identity Fraud Attacks

While document fraud has declined sharply in recent years, identity fraud attacks continue to grow in both volume and sophistication. Systems that rely on "liveness only" checks are insufficient. Injection attacks – attacks in which attackers feed fake, pre-recorded, synthetic, or manipulated data directly into the camera or data stream – are increasing by approximately 40% each year. And systems that rely on a single vendor's solution create systemic vulnerabilities where, for example, new, better, faster, more performant algorithms exist but are not integrated into the solution, diluting its effectiveness and increasing its exposure to known risks and vulnerabilities.

As just one example, new liveness detection technologies have significantly evolved with solutions now capable of performing simultaneous biometric data capture (i.e., taking a selfie) and confirming liveness in less than a second.

We publish these insights (and more) every year to help our government customers understand the scope and scale of identity fraud and how it continues to evolve at an unprecedented rate. We recommend EU stakeholders examine the findings of the **Entrust 2026 Identity Fraud Report**[10]. It comprises insights from 195 countries, more than 30 separate industries, and an analysis of more than 1 billion identity verification attempts. Salient extracts from the report are included below:

Fraud and Security Considerations

Over the past year, Entrust has seen attacks evolve rapidly. They are leveraging artificial intelligence, automation, and organised fraud rings to exploit new vulnerabilities. Identity is now the front line of fraud. Protecting it requires a thorough understanding of the tactics fraudsters use and how threat patterns are changing.

By introducing the requirement for liveness and irregular elements, systems can more effectively distinguish between genuine users and synthetic media. This approach makes it harder for attackers to reuse static or pre-recorded content, which is often the case for deepfakes.

Injection attacks, which are increasing at approximately 40% per year, target verification systems at the technical layer rather than the user level. The main type of injection attack is via virtual camera injections, essentially fake video streams presented to the verification system as if they were captured in real time.

Of great concern for European digital travel, the report highlights 20% of biometric fraud attacks are now deepfakes.

[10] Ref. Entrust 2026 Identity Fraud Report – https://www.entrust.com/resources/reports/identity-fraud-report

Economic and Member State Considerations

In several countries, we have witnessed changes to entry requirements contributing to a decline in the country's tourism revenues, typically because of fewer international arrivals and a downturn in traveller confidence. Globally, government and industry ambition for seamless travel is not only to facilitate better, faster, more streamlined passenger experiences, but to strengthen identity verification and security controls at the border. This serves as a sobering reminder for Europe to ensure its new entry/exit requirements do not negatively impact tourism, a vital economic driver contributing approximately 10% of the bloc's GDP.

For systems to be procured and implemented cost-effectively, there must be transparency in the business model, how costs are structured, and how costs initially borne by an EU agency could ultimately be passed on to Member States or require them to invest more in integration and national-level implementations. Competitive, open procurements are essential to delivering value for money and ensuring the solutions are proven, scalable, and future-proof.

The advent of Dynamic Purchasing Systems (DPS) offers transparency and flexibility to both providers and buyers. However, the importance of engaging industry and technology suppliers on future procurement plans cannot be overstated. Time is needed to plan, prepare, and allocate resources to support public tender processes. With several DPSs in existence, along with the EU Funding & Tenders Portal, some providers could easily risk missing an opportunity to offer their services and capabilities.

Recommendations

- To inform and derisk the design and implementation of the EU Digital Travel Application (and the EU Visa Application Platform), we recommend the Commission, eu-LISA, Frontex (et al.) consult with industry to examine the functionality gaps of the pilot ***Travel to Europe*** app, capture lessons learned from recent DTC pilots, and evaluate the performance of the UK Electronic Travel Authorisation (ETA) and EU Settlement Scheme (EUSS) solutions.
- We recommend eu-LISA engage early and often with key stakeholders – particularly specialist technology providers of digital identity solutions – to ensure digital identity/travel requirements and architectures are scalable and future-proof, and implementation timescales achievable.
- We recommend Member States, particularly national subject matter experts, organise briefings with Entrust so we can share our findings from national implementations and jointly explore best practices to reduce cost and increase the operational effectiveness of digital identity solutions.
- We recommend concerned EU stakeholders examine the findings of the Entrust 2026 Identity Fraud Report[11] to learn more about the growing risk of identity fraud and new attack methods.

[11] Ref. Entrust 2026 Identity Fraud Report – https://www.entrust.com/resources/reports/identity-fraud-report

Conclusion

The direction of travel for Europe is clear: **The future of migration and border management is digital.**

Together, EES, ETIAS, the EU Digital Travel Application, and the use of Digital Travel Credentials present an unprecedented opportunity to rethink how travellers are processed at (and experience) EU borders.

To ensure lessons are learned and future services and capabilities can be implemented on time and on budget, engagement and consultation with industry stakeholders and specialist technology providers will be key.

As geopolitical tensions continue to rise, the security of Europe's borders is of paramount importance. Technology, designed and deployed across Europe, will be essential to ensuring security, scalability, and interoperability – and for travellers and citizens to continue to benefit from free movement and contribute to Europe's economic prosperity through the development of sustainable travel and tourism.

Entrust stands ready to support European institutions, agencies, and Member States in their ambition to digitalise migration and border management, turn policy into operational reality, and help Europe achieve its strategic aim of digital sovereignty.



ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organisations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

©2026 Entrust Corporation. All rights reserved. Entrust, Datacard, and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. IV27Q3-european-digital-travel-wp

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

ENTRUST
SECURING A WORLD IN MOTION