WHITE PAPER

ENHANCING SEAMLESS BORDER CROSSINGS WITH BEHAVIOURAL BIOMETRICS

ODYSSEUS

Unobtrusive Technologies for Secure and Seamless Border Crossing for Travel Facilitation

AUTHORS – LEONI CHONDROMATIDOU, NIKLAS PALAGHIAS

DATE – 06-06-2025

TABLE OF CONTENTS

Funded by the European Union

ODYSSEUS has received funding from European Union's Horizon Europe Innovation Programme under Grant Agreement N°101073910. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

ODYSSEUS

INTRODUCTION

Border management in the European Union is becoming smarter, with the first major step being the digitalisation of travel credentials through solutions such as Digital Travel Credentials (DTCs) and the upcoming European Digital Identity (EUDI) Wallet. These systems make use of mobile devices, which are now central to identity verification at borders. As these devices take on more responsibility, ensuring their security has become more important than ever. One promising solution is behavioural verification, which uses machine learning to analyse how users interact with their devices, such as how they type, swipe, hold, or move. This approach allows for identity checks that are passive, continuous, and seamless, removing the need to stop and take a selfie or remember passwords, both of which can be time consuming, requiring explicit action from the traveller or insecure. This white paper examines how behavioural verification is applied within the ODYSSEUS project as an additional security layer for the mobile wallet that stores the traveller's DTC. It presents the use case, highlights the benefits, and outlines how the system aligns with current EU legal frameworks, including the General Data Protection Regulation (GDPR) and the forthcoming Artificial Intelligence Act.

OVERVIEW

As global mobility increases and digitalization transforms how we travel, governments face growing pressure to modernize border management. The need to process rising volumes of travelers, respond to public health emergencies like COVID-19, and combat identity fraud is pushing countries to adopt `smarter` border systems. These systems aim to reduce manual checks, shorten wait times, and enhance security, without compromising individual freedom or privacy.

Across the world, automated border control technologies are rapidly being deployed. In the Netherlands, 78 e-Gates have been installed at Amsterdam Schiphol Airport to fast-track identity checks. The United Arab Emirates launched the Dubai Smart Tunnel, which allows registered travelers to pass through immigration in seconds, without the need of physical travel documents. From biometric passports to pre-arrival risk assessment software, the future of border crossing is increasingly contactless, data-driven, and integrated with artificial intelligence (AI).

One of the initial steps towards this digitalization is Digital Travel Credentials (DTCs), secure digital versions of passports stored on mobile devices, and the upcoming European Digital Identity (EUDI) Wallet, a mobile app that allows citizens to securely store and share their identity and official documents across the EU. These tools allow faster travel, give individuals more control over their digital identity, but they also demand robust, reliable ways to verify identity continuously and passively, without interrupting the user experience.

Funded by the European Union

ODYSSEUS has received funding from European Union's Horizon Europe Innovation Programme under Grant Agreement N°101073910. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

ODYSSEUS

This is where behavioral biometrics offer unique value. Unlike traditional biometrics like fingerprints or facial scans, behavioral biometrics uses machine learning algorithms to analyze how a traveler interacts with the digital wallet in their devices, how they type (keystroke dynamics), how they walk (gait), or how they hold and use their smartphone. These patterns are difficult to mimic and evolve naturally over time, offering continuous, real-time verification without requiring active input from the traveler. This offers a strong, continuous layer of security for the digital wallet, without requiring any extra verification steps from the traveler. Incorporating behavioral biometrics into mobile-based border technologies like DTCs can support seamless, secure identity verification throughout the use of the digital credentials. It can help detect unauthorized access to important travel credentials.

This white paper explores how behavioral biometrics can strengthen the next generation of digital border systems by enabling seamless, continuous, secure, and user-friendly identity verification during usage of digital credentials within the context of EU-Horizon project ODYSSEUS.

APPLICABLE LEGISLATION

Behavioral biometrics (ex. typing, device holding patterns) are used to verify identity based on how a person interacts with a device. While increasingly applied in sectors like finance and mobile security, this is relatively new and not yet widely adopted technology, particularly in emerging sectors such as smart border management. As a result, there is currently no specific legislation that directly regulates behavioral biometrics as a distinct category. Instead, their use is indirectly addressed through broader legal frameworks, primarily under the General Data Protection Regulation (GDPR). This section outlines the relevant legal instruments and key obligations and gaps that apply when deploying behavioral biometric verification in border control systems.

General Data Protection Regulation (GDPR)

The **General Data Protection Regulation (EU) 2016/679** is the primary legal instrument governing personal data in the EU. It does not provide a separate legal category for behavioral biometrics but treats them under the broader definition of biometric data in Article 4(14), provided they are used for the purpose of uniquely identifying a natural person[1,2].

When behavioral biometrics are used for identity verification, they fall under **Article 9** as special category data, requiring [3]:

[1] European Union. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[2] European Union. General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679. gdpr-info.eu, 2016, https://gdpr-info.eu/.

[3] Same as : European Union. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Funded by the European Union

ODYSSEUS has received funding from European Union's Horizon Europe Innovation Programme under Grant Agreement N°101073910. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

ODYSSEUS

- Explicit consent, or
- A legal basis such as substantial public interest
- A Data Protection Impact Assessment (DPIA) for high-risk processing, such as border management, to mitigate privacy risks.

AI Act (Upcoming Regulation)

The EU Artificial Intelligence Act, provisionally agreed in 2024, classifies biometric identification and verification systems, as high-risk AI systems[4]. While the act does not explicitly address behavioral biometrics, systems that use behavioral data for real-time identity verification may fall under this category[5]. High-risk AI systems must comply with[6,7]:

- **Transparency for users:** explicitly inform when interacting with biometric systems, including explanations of their capabilities and limitations.
- **Risk management and performance monitoring:** Ensure the system is tested before use and regularly monitored afterward to confirm it remains safe, accurate, and compliant.
- **Human Oversight:** High-risk systems must include human oversight mechanisms (Article 14) to allow intervention and override, ensuring accountability.
- **No Discrimination:** Systems must be tested for fairness and bias, maintaining equitable performance across all demographics.

Some uses, such as emotion detection or behavior-based profiling in public spaces, are prohibited outright[8].

Sector Exceptions

In the financial sector, the Revised Payment Services Directive (PSD2)enforced across the EU—requires strong protection for online payments and banking through a method called Strong Customer Authentication (SCA). To comply, service providers must use at least two of the following three types of security factors:

- Something the user knows (e.g., a password or PIN)
- Something the user has (e.g., a phone or token)

---

[4] European Commission. Artificial Intelligence Act (Provisional Agreement), COM/2021/206 final. https://artificialintelligenceact.eu/

[5] Özal, M. 'Behavioral Biometrics': A Brief Introduction from the Perspective of Data Protection Law. KU Leuven Centre for IT & IP Law (CiTiP). https://www.law.kuleuven.be/citip/blog/behavioral-biometrics-a-brief-introduction-from-the-perspective-of-data-protection-law/

[6] ISACA (2024). *Understanding the EU AI Act: Requirements and Next Steps. https://www.isaca.org/resources/white-papers/2024/understanding-the-eu-ai-act*

[7] AuditBoard. "Navigating New Regulations for AI in the EU – AuditBoard." *AuditBoard*, https://auditboard.com/blog/eu-ai-act.

[8] Same as: European Commission. Artificial Intelligence Act (Provisional Agreement), COM/2021/206 final. https://artificialintelligenceact.eu/

Funded by the European Union

ODYSSEUS has received funding from European Union's Horizon Europe Innovation Programme under Grant Agreement N°101073910. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

ODYSSEUS

- Something the user is (also called an inherence factor)

Under this third category, **behavioral biometrics** (such as how a person types or holds their phone) are officially recognized as valid inherence factors. This was confirmed by the **European Banking Authority (EBA)**, which clarified that these behavioral traits are acceptable as long as they can uniquely and reliably identify the user and meet a "very low probability of unauthorized access" [9].

The **UK's Information Commissioner's Office (ICO)** has also confirmed that **explicit consent is not always needed** for behavioral biometrics under PSD2, as long as the data is used lawfully and fairly under GDPR [10].

USE CASE - PASSIVE USER VERIFICATION DURING MOBILE CHECK-INS

The ODYSSEUS project is an EU-funded HORIZON EUROPE Innovation Action project focused on the design and development of the next generation of border security solutions, delivering seamless, non-intrusive inspection capabilities in a highly secure manner. Among others it provides a mobile Digital and Virtual Passport, stored in a traveler's mobile wallet app. To ensure that only the rightful owner can access and use this sensitive identity credential, ODYSSEUS incorporates AI-powered continuous behavioral verification.

A key element of the ODYSSEUS approach is the Digital and Virtual Passport, stored in a mobile wallet application. This digital identity is used to support seamless border verification, reducing the need for physical document checks and allowing for a smoother flow through border control points.

- ODYSSEUS combines several technologies to help ensure identity verification is both reliable and non-disruptive, including:
- Facial recognition (used only at the border gate for identity confirmation)
- Behavioral verification methods (security mechanism of DTC)
- Transparent decision-making through Explainable AI (X-AI)
- A Decision Support System (DSS) that integrates different signals into a confidence score
- Anonymous person-counting tools to help border staff manage queues effectively

What is Passive User Verification?

[9] European Banking Authority. Opinion on the elements of Strong Customer Authentication under PSD2. https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-opinion-elements-strong-customer-authentication

[10] Biger-Levin, A. ICO guidance on behavioural biometrics for PSD2 SCA is a step in the right direction. BioCatch. Retrieved June 9, 2025, from https://www.biocatch.com/blog/ico-guidance-step-in-right-direction

Funded by the European Union

ODYSSEUS has received funding from European Union's Horizon Europe Innovation Programme under Grant Agreement N°101073910. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

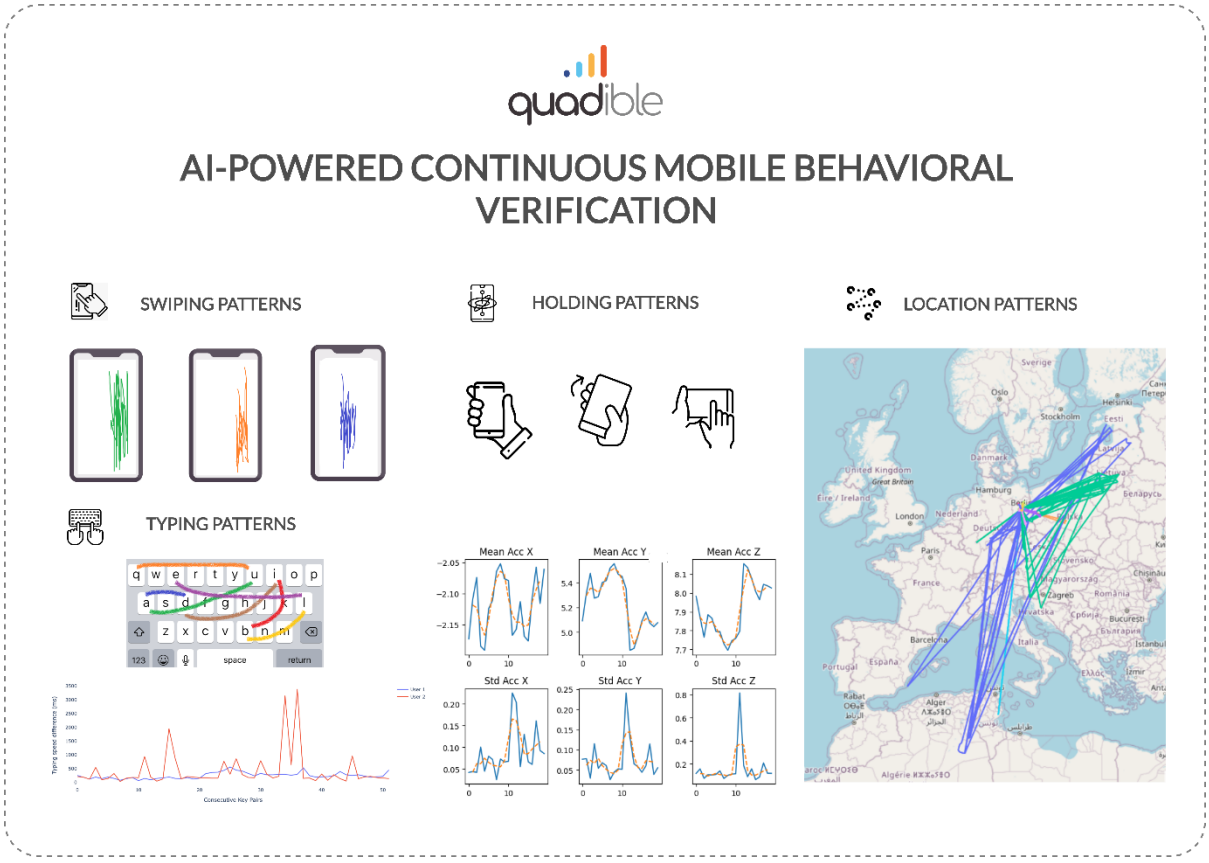
ODYSSEUS

One of the technologies integrated into ODYSSEUS is behavioral verification, which provides a supportive background layer of identity verification. It is not meant to replace other forms of verification but rather to offer an additional signal of trust, helping to strengthen access control to the mobile wallet app that holds the digital passport.

This verification works by identifying **general usage patterns** of the traveler's while using Digital Wallet to access the DTC. These patterns can include:

Before arriving at the border, the traveler opens their mobile wallet to access their Digital Passport. As they use the app, it collects signals in the background, such as:

- How the phone is held or moved
- How a person touches or interacts with the screen
- How a person types
- Movement patterns (e.g., way of walking)



When and How It is Used

Funded by the European Union

ODYSSEUS has received funding from European Union's Horizon Europe Innovation Programme under Grant Agreement N°101073910. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

ODYSSEUS

Behavioral verification becomes relevant when the traveler prepares to use their digital passport via the mobile wallet app, typically before reaching the actual border point. The goal is to gently enhance security by helping confirm that the person accessing the app is the one who enrolled in the passport.

This identity check is continuous but unobtrusive, helping to protect the credential from unauthorized use in case the phone is lost or accessed by someone else. If the system detects unusual behavior, it does not immediately deny access, instead, it can flag a risk level, which the broader ODYSSEUS platform may use to request additional verification or inform border authorities.

Step 1: User Registration and Consent

The process begins when a traveler voluntarily chooses to participate in ODYSSEUS and consents to his collected data for behavioral verification and downloads the official mobile wallet application on their personal device. As part of the onboarding process, the traveler registers their Digital Travel Credential (DTC) or passport by scanning the document and taking a selfie. This selfie serves two purposes: it links the traveler's facial biometric to their credential and provides an initial reference for the behavioral verification system to ensure that the patterns being collected are associated with the correct person.

Step 2: Initial Behavioral Data Collection

From this point, each time the traveler uses the digital wallet. the behavioral component collects necessary behavioral data. These include how they hold or move their phone, how they tap or swipe on the screen, how they type, and how they move while using the app. Behavioral data is primarily collected during normal app use, for example, when the traveler uses the app to pre-register an upcoming trip or review their travel details. These interactions allow the system to learn unique behavioral patterns of the rightful owner of the DTC, which acts as a digital signature unique to the individual. This process is passive and non-intrusive, requiring no additional action from the user. It is important to note that data is collected only after the traveler has given clear, informed consent, and the system is designed to operate in accordance with privacy-by-design principles. The app also offers controls for travelers to pause data collection, withdraw consent, or delete their information at any time.

Identity Verification at the Border

Later, when the traveler opens the app again, to verify their identity at the border using the digital passport, the behavioral verification system quietly compares their current interaction patterns to their stored profile. If the behavior matches the one of the legit owner of the device, access to the passport and identity functions proceed normally. If the system detects a significant deviation from the expected behavior, it notifies the ODYSSEUS platform, and the traveler may be prompted to complete an additional verification step.

Funded by the European Union

ODYSSEUS has received funding from European Union's Horizon Europe Innovation Programme under Grant Agreement N°101073910. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

ODYSSEUS

IMPLEMENTATION POLICY SUGGESTIONS

The ODYSSEUS platform is developed with strong adherence to EU legal frameworks and ethical principles. While behavioural biometrics are not yet regulated as a distinct category, their use is governed under broader instruments such as the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act). In addition, the system is designed to reflect key values such as fairness, transparency, user autonomy, and privacy-by-design.

General Data Protection Regulation (GDPR)

ODYSSEUS complies with GDPR through the following measures:

- **Explicit Consent:** Users must provide clear, informed consent before any behavioural data is collected. Consent is requested at the time of onboarding, and the process does not proceed without it.
- **Purpose Limitation:** Behavioural data is used solely to support access control for the Digital and Virtual Passport. It is never used for profiling, tracking, or unrelated purposes.
- **Anonymization and Data Minimization:** No personal identifiers such as names, passport numbers, or addresses are processed by the behavioural verification system. Each user is associated with an anonymous identifier provided by the ODYSSEUS platform. Only the data strictly necessary for verification is collected.
- **Data Security:** All data is encrypted on the device, during transmission, and in the backend databases. Encryption and secure data handling are enforced end-to-end.
- **User Control:** Travellers can withdraw consent, pause behavioural monitoring, or delete their data at any time through the app interface.
- **Data Protection Impact Assessment (DPIA):** A DPIA is conducted to assess and mitigate potential risks associated with processing behavioural data in border management, which is considered high-risk under GDPR.
- **Testing Without Personal Data:** During the system's development and testing phases, no personal data is used. Anonymous identifiers are employed to ensure that participants remain unidentifiable, even internally.

EU Artificial Intelligence Act (AI Act – Provisional Agreement, 2024)

ODYSSEUS complies with AI Act through the following measures:

- **Transparency:** Users are informed when behavioural verification is active, and the app clearly explains how the feature works, what data it collects, and how it supports identity verification.
- **Risk Management and Performance Monitoring:** The system is tested before deployment and continuously monitored post-deployment. Behavioural models are evaluated for reliability, and system performance is regularly reviewed to detect false positives or anomalies.

Funded by the European Union

ODYSSEUS has received funding from European Union's Horizon Europe Innovation Programme under Grant Agreement N°101073910. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

ODYSSEUS

- **Human Oversight:** The behavioural risk score is used as advisory input only. It cannot make final decisions. If a deviation is detected, the system may suggest additional verification, but the final judgment remains with border authorities. Human intervention is always possible, ensuring accountability.
- **Non-Discrimination and Fairness:** Each behavioural model is trained individually using only the data of the user it serves. This prevents cross-user generalization and ensures that gender, ethnicity, nationality, or other demographic traits do not influence verification outcomes. The system is also tested to ensure consistent performance across user groups.
- **Respect for Human Dignity:** The AI is designed not to manipulate, pressure, or profile users. It functions purely as a tool for secure access, with individuals remaining in control of their data and decisions.
- **No Prohibited Uses:** ODYSSEUS does not apply behavioural biometrics for emotion detection, psychological inference, or surveillance in public spaces—areas explicitly restricted under the AI Act.

CONCLUSION

Behavioural verification is a relatively new approach in border management, offering significant advantages in terms of security, convenience, and inclusivity, without imposing substantial privacy burdens on travellers. As implemented in the ODYSSEUS project, it enables continuous, passive identity verification that enhances security, prevents credential misuse, and improves the traveller experience, without requiring passwords, repeated scans, or manual checks. It offers strong privacy protection through anonymization, user-specific models, and full user control, while aligning with the GDPR and the forthcoming AI Act. Although behavioural biometrics are not yet explicitly addressed by a dedicated legislation, ODYSSEUS shows that they can be used responsibly and ethically within current legal frameworks. As the technology matures, clear regulatory guidance will be important, but its current application already demonstrates a well-balanced path forward: secure, inclusive, user-friendly, and privacy-conscious solution.

Funded by the European Union

ODYSSEUS has received funding from European Union's Horizon Europe Innovation Programme under Grant Agreement N°101073910. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

ODYSSEUS