Eurosmart Position Paper on the EU Digital Travel Application: Feedback on proposed amendments by LIBE Committee Shadow Rapporteurs and MEPs

June 2025

This position paper presents Eurosmart's detailed feedback on the proposed amendments to the European Commission's draft regulation on the EU Digital Travel Application, as submitted by Members of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE). Eurosmart, representing the voice of the digital security industry in Europe, welcomes the LIBE Committee's engagement but seeks to ensure that the final legislative text remains aligned with the goals of secure, user-friendly, and interoperable digital travel credentials, while fulfilling its potential as a secure, effective, inclusive, and trusted system that can benefit both travelers and authorities in the border-crossing process. In this context, Eurosmart offers constructive recommendations to enhance the proposed amendments focusing on maximizing the impact and usability of digital travel credentials, ensuring robust security and data protection, clarifying data governance responsibilities, supporting global interoperability, aligning with the eIDAS and EUDI Wallet framework, preserving the role of physical travel documents, and enabling practical and secure use at European and international borders.

Executive summary

Eurosmart welcomes the amendments proposed by the European Parliament's LIBE Committee and offers targeted recommendations to ensure that the EU Digital Travel Application delivers high security, data protection, and user-friendly innovation at European and international borders.

- Maximizing Impact: Eurosmart calls for digital travel credentials to be available to most citizens as quick as possible, and in particular urges reconsideration of the age restriction limiting digital travel credentials to individuals above 18, as this risks undermining uptake and overall efficiency. Eurosmart supports ensuring most citizens can obtain digital credentials free of charge.

- Enhancing Security: Eurosmart calls for stronger integrity and authenticity checks on travel document chips, the addition of validity verification, and cybersecurity measures including annual testing and mandatory high-level certification.

- Safeguarding Data Protection: Anonymization is unfeasible for uniquely identifying data; strong encryption is preferred. Eurosmart supports strict limitations on data transfers to third countries and clear encryption standards.

- Clarifying Data Governance: Amendments should clearly specify who has the data controller and processor roles, particularly regarding the EU Digital Travel Application and the Traveller Router.

- Supporting Global Interoperability: Digital travel credentials must align with ICAO standards to ensure global acceptance and functionality.

- Aligning with eIDAS and the EUDI Wallet: Eurosmart supports storing digital credentials in the EUDI Wallet and recommends treating them as electronic attestations of attributes issued by public authorities, while clarifying responsible entities.

- Preserving Physical Documents: Physical travel documents should remain the trust anchor and always be available as a fallback for identity verification.

- Enabling Practical Use: Eurosmart emphasizes that digital travel credentials must support facial recognition and allow optional use beyond border control, such as in financial services, while ensuring legal safeguards and traveler consent.

These recommendations aim to ensure that the EU Digital Travel Application delivers a secure, privacy-preserving, and interoperable solution that improves border crossing efficiency and trust for EU citizens and third-country nationals alike.

Eurosmart's key comments and recommendations on the proposed amendments:

1. Maximize impacts of digital travel credentials

Eurosmart believes that limiting the benefit of digital travel credentials to only individuals above 18 years old may substantially impede the expected impacts and benefits of border crossing in terms of (1) traveler experience, (2) increased throughput flow, and (3) improved inspection of documents and individuals. Individuals below 18 years are likely to travel with their parents or family. As a result, this restriction could discourage entire families from using digital travel credentials, prompting them to use the regular method of border crossing. This approach is likely to divert a large number of travelers from using digital travel credentials, resulting in reduced impacts in terms of (1) traveler experience, (2) increased throughput flow, and (3) improved inspection of documents and individuals. Instead, we suggest reconsidering this limitation, potentially by allowing an individual to use digital travel credentials as soon as they possess a travel document. Actually, Eurosmart recommends discarding amendments 5, 17, 26, 30 and 145. In addition, the approach proposed in amendments 62 and 155, whereby the age limitation would be defined by national laws, could be considered.

To ensure a widespread uptake of digital travel credentials among EU nationals and citizens, it is essential to have a large number of people who can enjoy them. For this reason, Eurosmart supports amendments 15, 44, 106, and 213, which guarantee that holders of a travel document can obtain a digital travel credential at any time (upon request if they already have one, or at the time of renewal). This position is further developed in Eurosmart's position paper on the EU Digital Travel Application, published on the 10th of April 2025, particularly in chapter 6.

Finally, Eurosmart recommends disregarding amendment 216, as the EU Digital Travel Application should be free of charge in all cases—whether during issuance or renewal.

2. Security of digital travel credentials

Eurosmart welcomes the clarification regarding the verification of integrity and authenticity of the data stored in the storage medium (whereas the original text was considering the verification of integrity and authenticity of the chip, which is unclear) as proposed in amendments 24 and 142. This item is further developed in Eurosmart's position paper on the EU Digital Travel Application, published on the 10th of April 2025, particularly in chapter 2.

Eurosmart welcomes the clarification introduced by amendment 28, which makes clear that the storage medium of the travel document is a chip. Accordingly, Eurosmart calls for consistent terminology throughout the final document, as three different terms are currently being used: 'chip', 'storage medium (chip)' and 'storage medium'. To ensure clarity and coherence, Eurosmart recommends using a single term across the text – preferably "chip".

However, amendment 28 lacks a clear description of the security controls to be carried out prior to the creation of digital travel credentials. Therefore, Eurosmart suggests modifying the following text:

"[…] verify the integrity and authenticity of the chip of the travel document " to as follows:

- Verify the integrity and authenticity of **the data on the storage medium (the 'chip');**
- Verify **the chip has not been cloned.**

This item is also further highlighted and developed in Eurosmart's position paper on the EU Digital Travel Application, published on the 10th of April 2025, particularly in chapter 2.

Eurosmart welcomes the clarification regarding the process to be applied to authenticate travel documents and digital travel credentials. The current proposal for a regulation only considers the verification of integrity and authenticity of the travel document and digital travel credentials and omits the verification of their validity. Eurosmart supports amendments 69, 71, 153, 225, 226, 230, and 231, which cover this gap. This point is further developed in Eurosmart's position paper on the EU Digital Travel Application, published on the 10th of April 2025, particularly in chapter 2.

Eurosmart welcomes amendment 27, which provides clarification on the technical criteria to be met by the travel documents hold by third-country nationals. It shall indeed have a chip but also have the technology preventing its cloning. As such, it guarantees that travel documents used to create digital travel credentials through the EU Digital Travel Application have not been cloned. This point is also highlighted in Eurosmart's position paper on the EU Digital Travel Application, published on the 10th of April 2025, particularly in chapter 2 (verification of authenticity of the chip).

Eurosmart supports amendments 50 and 54, which require traveler identification to be reliable and secure. Likewise, Eurosmart supports amendment 67, which provides for a user- and privacy-friendly mobile application. Having a reliable and secure traveler identification is key to ensure travelers trust the EU Digital Travel Application and agree to use it.

Eurosmart supports the following amendments aiming at guaranteeing a high level of security and data protection for the EU Digital Travel Application:

- Amendments 36 and 186, which require the mobile application to ensure privacy and data protection by design and meet a high level of security;
- Amendment 191 which requires the EU Digital Travel Application to meet the "state of the art" of security;
- Amendment 202, which provides for annual penetration testing and vulnerability assessment of the EU Digital Travel Application.

In addition, Eurosmart recommends:

- Linking these requirements for a high level of security and data protection to a mandatory cybersecurity certification of the EU Digital Travel Application at level 'High' as per Regulation (EU) 2019/881 (CSA);

- Enhancing the requirements for data protection by mandating that the EU Digital Travel Application and mobile application are designed in such a way that personal data are not available to (1) the mobile phone manufacturer, (2) the provider of the platform, or (3) the provider of the browser.

These amendments are instrumental in ensuring travelers trust the EU Digital Travel Application and agree to use it. This point is also further developed in Eurosmart's position paper on the EU Digital Travel Application, published on the 10th of April 2025, particularly in chapter 6.

3. Data protection

Eurosmart recommends discarding amendment 93, which provides that all communication between the Traveller Router and the competent authority should be protected using an anonymization method. However, it seems technically unfeasible to apply anonymization to data that – by nature – is meant to uniquely identify individuals. Strong encryption – already foreseen in the text – is the appropriate solution to prevent such data from being captured and processed by unauthorized parties.

Additionally, Eurosmart supports amendment 99 but recommends replacing "should" with "shall" to strengthen the requirement. The sentence should therefore read: *"…When designing and developing the router, eu-LISA **shall** ensure that data transmitted to competent border authorities are end-to-end encrypted in transit."* Similarly, Eurosmart supports amendment 186, while emphasizing that holder authentication shall be explicitly added alongside the requirement for the use of end-to-end encryption.

Eurosmart also strongly supports amendment 176, which prohibits the transfer of data to third countries or international organizations.

Finally, Eurosmart supports amendments 94, 95, 96, 97, 124, 199, and 241, as they promote and safeguard the use of anonymized and non-personal statistics.

4. Data governance

Eurosmart welcomes the clarifications introduced by amendments 174 and 175. However, they fall short of specifying who is the data controller for the processing of data required for the creation of digital travel credential, as highlighted in our position paper. Likewise, they do not clarify who is the data processor for the processing carried out by the Traveller Router. For further details, please refer to Eurosmart's position paper on the EU Digital Travel Application, published on the 10th of April 2025, particularly chapter 3.

5. Support of global interoperability of digital travel credentials

Eurosmart members have long been key contributors to the International Civil Aviation Organization (ICAO) technical works (e.g. ICAO NTWG, ISO SC17 WG3, SC 27 WG2, and others), particularly in the development of specifications aimed at supporting the implementation of digital travel credentials. Eurosmart members efforts focus on ensuring the highest levels of security and data protection for both digital travel credentials and (Schengen) border crossing. In addition, Eurosmart would like to emphasize the importance of leveraging on the international standards prepared by ICAO for digital travel digital travel credentials implementation, in order to facilitate the deployment and technical interoperability with other countries outside of the Schengen zone. As ICAO is the international organization responsible for ensuring worldwide interoperability of traveler identification in air travel, alignment and reliance of digital travel credentials with the work carried out by ICAO is essential.

In this context, Eurosmart supports amendment 111, which reinforces ICAO's role, and recommends discarding Amendment 56, which risks undermining global interoperability efforts.

6. Interplay with eIDAS and EUDI Wallet

Eurosmart welcomes amendment 8, which clarifies that digital travel credentials shall be stored not only within an EUDI Wallet that complies with the eIDAS Regulation, but also in accordance with the eIDAS regulation.

Eurosmart welcomes the clarifications regarding the technical nature of digital travel credentials within the EUDI Wallet framework, as proposed in amendments 106, 147, 215 (as QEAA). This is an item, Eurosmart highlighted in our position paper on the EU Digital Travel Application, published on the 10th of April 2025 (see chapter 5). Nevertheless, Eurosmart recommends that, in the specific case of digital travel credentials, they should be handled as "electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source" as defined in Article 3(46) of the eIDAS Regulation. This is appropriate, as digital travel credentials are intended to be issued by States themselves.

In addition, these amendments do not address the crucial question of which entity is effectively responsible for creating digital travel credentials or issuing them in the form of an attestation – an issue Eurosmart has also highlighted in its position paper on the EU Digital Travel Application, published on the 10th of April 2025 (see chapters 3 and 5).

Eurosmart recommends discarding amendments 70, 193 and 214 which would prevent digital travel credentials from being used within the EU Digital Identity Wallet framework. On the contrary, Eurosmart recommends that digital travel credentials should also be usable within this framework, so that other use cases – such as financial for KYC (verification of identity for financial operations) – can benefit from a digital representation of a travel document.

Nevertheless, Eurosmart emphasizes that the conditions under which digital travel credentials can be used within the EU Digital Identity Wallet framework are unclear and should be further clarified in the legal text. Key issues include:

- The nature of the digital travel credentials. Eurosmart reiterates its recommendation that they be handled as "electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source" in line with defined in article 3(46) of the eIDAS Regulation;
- Which entity is responsible for delivering these credentials?
- If eu-LISA is designated, is it subject to the eIDAS Regulation?

These points are also addressed and further developed in Eurosmart's position paper on the EU Digital Travel Application, published on the 10th of April 2025, particularly in chapter 5.

Finally, Eurosmart supports amendment 120, while recommending that the referred evaluation to the EU Digital Travel Application also include an assessment of the EUDI Wallet itself, as harmonization between the EU Digital Travel Application and the EUDI Wallet is essential.

7. Physical travel documents

Eurosmart recommends that the physical travel document remain the trust anchor for verifying the identity of individuals when crossing borders. Relying solely on digital solutions would make the process more vulnerable to cyberattacks and to issues such as the unavailability of a traveler's mobile phone. For this reason, Eurosmart recommends that physical travel documents continue to be issued to travelers, with digital travel credentials serving as a companion to the physical travel document – bringing added fluidity and convenience to the traveler. Therefore, Eurosmart supports amendments 90, 107 and 135.

In addition, for the very same reason, border authorities should retain the ability to request the physical travel document at any time in order to establish the traveler's identity with a high level of trust, if deemed necessary. Travelers should therefore still carry their physical travel documents. Hence, Eurosmart also supports amendment 89.

Furthermore, Eurosmart considers that the storage medium in travel documents (excluding fingerprints) should be available to relevant stakeholders involved in the border-crossing process – at minimum, air carriers – in accordance with national laws. This would help stakeholders fulfill their legal obligations regarding traveler identification (e.g. verification the presence of a valid visa or verifying that the traveler holds a boarding pass in their name prior to boarding). Such availability would support a streamlined process and help ensure a high level of border crossing security. Therefore, Eurosmart supports amendments 45 and 220, and recommends discarding amendments 219 and 221.

8. Use of digital travel credentials

Eurosmart supports amendment 60, which provides relevant clarifications regarding the benefits of digital travel credentials.

Nonetheless, Eurosmart recommends discarding amendment 55. The deleted original text from the European Commission's proposal on the EU Digital Travel Application shall be retained, as it clearly presents the advantages of digital travel credentials in comparison to a physical travel document.

Eurosmart strongly believes that digital travel credentials may serve purposes beyond proving one's identity for border crossing – such as proving identity for KYC procedures in financial operations. However, such use of digital travel credentials should remain voluntary, giving holders the possibility to use alternative methods, while being covered by applicable laws. Consequently, Eurosmart recommends discarding amendment 127.

A key principle of the proposed regulation is to streamline border crossings by sending ahead of border crossing the digital travel credentials, enabling checks to be carried out before the travel crosses the border. Through digital travel credentials, a high level of security and trust in the traveler's identity data can be achieved. As such, Eurosmart recommends discarding amendments 224 and 229.

In addition, it should be enshrined in the regulation that a Member State can request the presentation of a physical travel document – not just a digital travel credential – at border crossing, if an in-depth identity verification is deemed necessary. This point is also highlighted and further developed in Eurosmart's position paper on the EU Digital Travel Application, published on the 10th of April 2025, particularly in chapter 8.

Facial recognition is a mature technology that has been used for years in the border crossing processes. It is currently deployed in many countries worldwide for physical travel documents and has proven to be reliable, offering substantial benefits to both travelers (greater convenience and experience) and border authorities (improved accuracy, and flow facilitation and efficiency). Moreover, experience shows that facial recognition technology for border crossing can be implemented in ways that ensure privacy and respect for fundamental rights. Therefore, Eurosmart recommends discarding amendments 56, 57 and 152.

It is necessary that the back-end validation service carries out the facial recognition to verify the link between (1) the applicant and the presented travel document prior to the creation of digital travel credential, or (2) the traveler and the presented digital travel credential during the submission process of the digital travel credential. This binding stage of binding is necessary to ensure that (1) the digital travel credential is created by and delivered to the correct traveler, and (2) the digital travel credential is submitted by the rightful holder, with their consent. Hence, Eurosmart recommends discarding amendments 141, and 152.

Digital travel credentials which are created should contain the traveler's facial image, which is necessary to link the credential – submitted in advance – to the individual crossing the border, just as a physical travel document is linked to its holder through the printed portrait it contains. Removing the facial image from digital travel credentials would render them unusable for border crossing and

would make the EU Digital Travel Application inoperative. Subsequently, Eurosmart recommends discarding amendments 159, 217, and 218.

The creation of digital travel credentials requires data processing by the back-end validation service. This encompasses several steps such as (1) facial recognition, and (2) verification of validity and authenticity of the physical travel document used to create the digital travel credentials. Therefore, prohibiting any data processing by the back-end validation service would lead to prohibit the creation of digital travel credentials and once more render the EU Digital Travel Application inoperative. As a result, Eurosmart recommends discarding amendment 180.

Travel data includes the digital travel credential, which contains the traveler's identity and portrait. These data found in the digital travel credential should be stored until the traveler has crossed the border, to ensure a reliable link between the outcome of the processed travel data and the individual. Thus, the sentence "after the traveler has been granted entry" in item 1 of amendment 187 should be understood as the moment when the traveler crosses the border. However, Eurosmart suggests considering item 1 of amendment 188 instead, as it provides clearer language on this point than amendment 187.

Conclusion

Eurosmart endorses the development of the EU Digital Travel Application as a secure, interoperable, and user-centric solution designed to improve the border crossing experience. To unlock its full potential, the amendments proposed by the European Parliament's LIBE Committee rapporteur, shadow rapporteurs and MEPs on the EU Digital Travel Application, as well as the final regulation text, must ensure inclusive access by removing unnecessary age restrictions, preserve physical travel documents as the essential trust anchor, and incorporate robust security and data protection measures based on strong encryption and high-level certification.

Establishing clear data governance and aligning with international standards—including ICAO and the eIDAS/EUDI Wallet frameworks—are vital to building trust and enabling global interoperability. Furthermore, integrating practical functionalities such as facial recognition and allowing optional uses beyond border control, while strictly safeguarding privacy and user consent, will promote widespread adoption and operational effectiveness.

Through these recommendations, Eurosmart aims to foster a digital travel ecosystem that is resilient, reliable, and efficient—delivering meaningful benefits to travelers and border authorities across the EU and internationally.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART

The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 471 34 59 64 | mail Contact@eurosmart.com