EUROSMART
The Voice of the Digital Security Industry

Position Paper on the EU Digital Travel Application

April 2025

The European Commission's proposal for the EU Digital Travel Application aims to digitalize travel documents and identity cards, while streamlining the use of Digital Travel Credentials for Schengen border crossing. Eurosmart supports this initiative but highlights the need for a clear regulatory framework, robust security measures, and seamless interoperability with existing EU digital identity frameworks, for a successful implementation across the EU.

Key areas for improvement include clearer definitions, consistent security concepts, precise data governance, and better interplay with eIDAS and the EUDI Wallet. Eurosmart also stresses the importance of aligning with EU regulations and addressing technical challenges to ensure smooth implementation across Member States. A more realistic timeline for application, expert consultation and involvement are crucial for successful deployment.

This paper presents Eurosmart's recommendations to ensure that the Digital Travel Application fulfills its potential as a secure, effective, inclusive, and trusted system that can benefit both travelers and authorities in the border-crossing process.

Executive summary

The European Commission's proposal for a Digital Travel Application marks a significant move towards the digitalization of travel documents and identity cards within the EU. While Eurosmart acknowledges the potential benefits of digitalizing travel documents and identity cards and streamlining the use of Digital Travel Credentials for Schengen border crossings, it emphasizes that several critical issues must be addressed for an effective and secure implementation.

A primary concern is the need for clearer definitions between the "creation" and "issuance" of Digital Travel Credentials. The lack of clear definitions could create uncertainties regarding the security requirements and governance frameworks for these credentials. Likewise, the proposal is also ambiguous regarding the data governance, and in particular who would take over the roles of data controllers and processors for the creation of Digital Travel Credentials, and whether it should be exercise by eu-LISA.

In addition, Eurosmart calls for consistent verification processes requiring (1) validity verification alongside verification of integrity and authenticity of the chip data and (2) authenticity verification of the chip/storage medium of the travel document.

This text vests eu-LISA with a new role implying processing personal data from EU-citizens and EU-nationals to support the digital single market, which goes far beyond its original purpose focused on police and justice and processing data from criminals and non-EU citizens and nationals. This

substantial change requires supplemental protection and safeguard for personal data of EU-citizens and EU-nationals and thus reconsider the supervision of eu-LISA.

Interplay with eIDAS is another critical issue. The proposal should ensure that the EU Digital Travel Application functions effectively across various national EUDI Wallets (provisioning and presentation of Digital Travel Credentials). In addition, the exact interplay with eIDAS is still to be defined. First the shape of Digital Travel Credentials (PID or attestation) and the role of eu-LISA (Attestation provider or PID provider) within the eIDAS ecosystem should be clarified. Secondly, it shall be ensured that all the provisions of eIDAS are enforced and applied, even to eu-LISA. Also, Eurosmart highlights that the usage of Digital Travel Credentials from the EUDI Wallet raises many issues which should be clarified: how should it be bound to the EUDI Wallet? Which rules for provisioning and presenting it to third party? How to address privacy needs around the portrait – contained in the Digital Travel Credentials - when presenting it to third party?

The text contains several ambiguities or shortcomings regarding the Digital Travel Credentials. Despite the core of the text allows for issuance of Digital Travel Credentials linked to travel documents at any time, recital 19 is more restrictive. Yet to ensure a large and swift uptake of Digital Travel Credentials, the eligible population should be as large as possible. The text is unclear as to Member States shall set up national infrastructure for the creation of Digital Travel Credentials linked to travel documents and identity cards on top of the EU Digital Travel Application, and this aspect should be clarified. In addition, the security should be clearly considered for the issuance of Digital Travel Credentials. The content of the Digital Travel Credentials is also ambiguous. It could be understood in a restrictive way whereby it should contain exactly the same data as the original document. However, the issuance of Digital Travel Credentials is also an opportunity to refresh or update these data while not adding any new type of personal data (e.g. update of address or portrait). Therefore, clarifications should be added to ensure this use case is allowed.

In order to guarantee the successful uptake of the EU Digital Travel Application, Digital Travel Credentials and their integration with the EUDI Wallet, it is key that a dedicated expert group is established. This expert group should include all relevant stakeholders from the industry to prepare the required technical specifications of the Digital Travel Credentials in order to help ensure a well-coordinated and secure process.

There are also several ambiguities and shortcomings regarding the use of Digital Travel Credentials for border crossing. It should be clarified whether Digital Travel Credentials could be presented through a physical interaction – without online connection via the Traveller Router – in the course of border crossing to establish the traveler's identity. For security purposes, Member States should also be allowed to request the presentation of travel documents or identity cards to ascertain identity during border crossing.

To support a smooth roll-out, Eurosmart recommends a comprehensive review of the application timeline, advocating for an extension to 24 months. This would account for the complexities involved and to mitigate the risks related to public procurement processes, which may cause delays in deployment, testing, and operational readiness.

Additionally, Eurosmart advocates for the explicit inclusion of European Residence Permits so that their holder could also benefit from Digital Travel Credentials linked to their European Residence Permits.

By addressing the gaps in this position paper, the Digital Travel Application proposal could meet the operational needs of border authorities, while also protecting user privacy and fostering seamless digital integration across the EU.

Eurosmart's key comments and recommendations on the proposal:

1. Clarification of Definitions: "Creation" and "Issuance" of Digital Travel Credentials

The proposal distinguishes between the "creation" and "issuance" of Digital Travel Credentials but does not define either term, even in the recitals. The text suggests that Digital Travel Credentials can be both created and issued (Article 13(1), item 31), with each term used in specific contexts:

- The EU Digital Travel Application creates Digital Travel Credentials (recital 7, Article 1(a), Article 3(a), Articles 4.1, 4.5, 4.6, 4.7, and Article 7.4).
- Member States either issue or create Digital Travel Credentials (recital 19, Article 4.3(a), Article 12.1 item (d)).

This distinction implies differences which may impact several aspects such as the shape, the technical format, the process to obtain it or the nature of the link with the issuer but that are not explained in the text. Therefore, Eurosmart recommends that the proposal include clear definitions of "creation" and "issuance" of Digital Travel Credentials, particularly to clarify the differences between them.

2. Clarification of security concepts

The proposal's requirements for verifying the storage medium, chip data, physical travel document, or Digital Travel Credential are inconsistent. In several provisions—recital 6, recital 7, Article 3(b), Article 4.5, and Article 13.2(a) and (c) (first and second paragraphs)—only authenticity and integrity verification are required, while validity verification (i.e., ensuring the document has not been revoked) is missing.

To ensure a comprehensive and consistent verification process, validity checks should be explicitly included alongside authenticity and integrity in these provisions. Notably, Article 4.1(c) and Article 13.2(d) (first paragraph) already incorporate validity verification, underscoring the need for alignment across the text.

Additionally, the proposal should clearly distinguish between the storage medium (chip), and the data stored on it (chip data), particularly in Article 3(b) and Article 4.5.

- Article 3(b) requires confirming the authenticity and integrity of the chip data.
- Article 4.5 requires the verification of the integrity and authenticity of the storage medium of the travel document.

However, these provisions are insufficient, as both the chip data and the storage medium must be independently verified. Ensuring the integrity and authenticity of the chip data guarantees that the information is genuine, issued by an authorized entity, and unaltered. Meanwhile, verifying the authenticity of the storage medium ensures that the physical chip has not been tampered with or compromised.

To address these gaps, Eurosmart recommends updating Article 3(b) and Article 4.5 to explicitly require the verification of both the integrity and authenticity of the chip data, as well as the authenticity of the storage medium.

3. Clarification of data governance

Article 7 defines the roles of data processor and data controller for processing Digital Travel Credentials. However, it remains unclear who holds these roles when processing personal data for the creation of Digital Travel Credentials via the EU Digital Travel Application (e.g., biometric matching, document reading as per Article 4.5).

Key questions that require further clarification include:

- Should eu-LISA be the data controller for the creation of Digital Travel Credentials? If so, does this imply that eu-LISA or the European Union vouches for the identity of EU citizens and travelers?
- Should eu-LISA be the data processor for the creation of Digital Travel Credentials?
- Should Member States take on the role of data controller and/or data processor?

Moreover, Eurosmart recommends clarifying Article 7.2, particularly in relation to its distinction from Article 7.1, and specifying whether Member States are required to designate an additional competent authority—separate from the border authorities mentioned in Article 7.1—to act as the data controller.

4. Role of eu-LISA and Implications for Data Protection Supervision

Currently, eu-LISA is responsible for managing large IT projects aimed at supporting police and justice purposes, primarily targeting non-EU citizens or non-EU nationals (e.g., ECRIS-TCN, ETIAS, EES, VIS, Eurodac). A few exceptions, such as SIS and e-Codex, involve cross-border judiciary data exchange that can affect both EU citizens and nationals and non-EU citizens and non-EU nationals.

Under the new proposal, eu-LISA would take on a new major IT project: the EU Digital Travel Application. Unlike previous projects, this initiative:

1. Does not focus on police or justice purposes but goes beyond and seem to address the digital single market;

2. Primarily targets EU citizens and nationals, enabling the creation of Digital Travel Credentials from identity cards and travel documents and submit them ahead of border crossing.

This new paradigm represents a significant change in eu-LISA's role and responsibilities. Therefore, Eurosmart recommends reconsidering how Member States and national data protection authorities will effectively supervise and control the data processing carried out by eu-LISA in this new project, while ensuring that national data protection requirements are met.

5. Interplay between eIDAS and the EUDI Wallet

Ensuring interoperability of the EU Digital Travel Application with the EUDI Wallet is essential to leverage the efforts being made regarding the EU's goal of providing a digital wallet to all citizens. While Article 8.4 addresses this objective, the likelihood of multiple EUDI Wallets across the EU calls for clear specifications for testing the EU Digital Travel Application before it becomes operational. This includes testing the provisioning and reading of Digital Travel Credentials with all EUDI Wallets in use within each Member State, as referenced in recital 13, Article 8.5, Article 15.1, and Article 16.1(c). Additionally, testing should be conducted whenever a new EUDI Wallet is introduced, or an existing

wallet undergoes significant changes. To ensure thoroughness, Eurosmart recommends explicitly incorporating in Article 16.1(c) the test of provisioning and reading of Digital Travel Credentials with all EUDI Wallets in use in each Member State, as well as conducting supplementary tests for any newly introduced or substantially modified wallets.

Likewise, Article 8.4 requires eu-LISA to ensure the interoperability of the EU Digital Travel Application with the European Digital Identity Wallet under Regulation (EU) No 910/2014. However, this Article lacks sufficient details on this matter. Eurosmart identifies the following aspects as requiring clarification:

- What form should Digital Travel Credentials take within the eIDAS ecosystem: (Qualified) Electronic Attestation of Attributes (EAA) or Personal Identification Data (PID)?
- Which entity(ies) should act as:
  1. **Relying party,** as defined in the eIDAS Regulation, responsible for submitting Digital Travel Credentials and ensuring compliance with all applicable eIDAS requirements?
  2. **Provider of electronic attestation of attributes or PID provider,** as outlined in the eIDAS Regulation, responsible for providing Digital Travel Credentials and ensuring adherence to all applicable eIDAS requirements?
- Should eu-LISA operate such entity(ies)? If so, given that eu-LISA is not subject to the eIDAS Regulation (nor the NIS Directive, which applies to trust service providers if eu-LISA were to act as one), specific provisions should be added to the proposal to ensure that eu-LISA abides by the same requirements.
- Alternatively, should Member States take on the role of operating such entity(ies)?

Furthermore, Eurosmart considers clarifications are also needed regarding the technical integration of Digital Travel Credentials within the EUDI Wallet framework. Key considerations include:

- **Protocols for DTC Provisioning and Presentation:** While ICAO specifications are suitable for border-crossing scenarios in the context of the EU Digital Travel Application, other standards, such as ISO/IEC 23220-4, may be more appropriate for broader use cases within the EUDI Wallet ecosystem.
- **Security and Trust Requirements:** Clear standards must be established for the security, trust level, and binding quality (with the wallet and the user) of DTCs within the EUDI Wallet to ensure reliability and trust.
- **Privacy Considerations:** As DTCs include sensitive data, such as the holder's portrait, robust privacy measures should be available to user when presenting a DTC with an EUDI Wallet for uses cases other than border crossing. These could include mechanisms like selective disclosure of data contained in the DTC or the use of a lower-resolution portrait in certain use cases to safeguard privacy while maintaining functionality.

6. Clarification about the Digital Travel Credentials

To foster the uptake and use of Digital Travel Credentials, Eurosmart recommends that the holders be able to request their issuance at any time, rather than only during the application or renewal of a travel document. This flexibility would allow holders to have an issued Digital Travel Credential linked to their travel document without having to wait for the next renewal of their travel document (typically 10 years) and even if they did not request it at the time of application for a travel document. Additionally, this would significantly increase the number of eligible holders in the short term and would boost the uptake of Digital Travel Credentials associated to travel document.

While Article 12(1) 1a effectively supports this approach by enabling the issuance of a Digital Travel Document associated to a travel document at any time, recital 19 is more restrictive, stating that "[…] when applying for or renewing a travel document, applicants should be allowed to request that the

competent authority issues, together with the physical document, a corresponding digital travel credential. Holders of valid travel documents should also be able to create a digital travel credential based on their existing physical travel document". To eliminate confusion and facilitate broader uptake of Digital Travel Credentials, Eurosmart suggests aligning the content of recital 19 with Article 12(1) 1a, to describe the issuance of Digital Travel Credential corresponding to travel document at any time.

Eurosmart also considers that further clarification is needed regarding Member States' infrastructure for creating Digital Travel Credentials. Article 12(1) does not specify whether Member States are required to set up a separate infrastructure from the EU Digital Travel Application to enable the creation of Digital Travel Credentials based on passports and other travel documents they have issued. A similar ambiguity exists in Article 2.3 of COM(2024)671 final regarding identity cards. This issue should be clarified in both texts to ensure consistency.

Additionally, Eurosmart recommends explicitly addressing the security of Digital Travel Credentials in Article 12(2). Without clear security measures being ensured, the trust put by the users on Digital Travel Credentials may be undermined. Eurosmart recommends explicitly considering the security of (1) the issuance and disclosure process, (2) authentication and validation, and (3) revocation.

Clarifications are also needed regarding the content of Digital Travel Credentials. The text states that Digital Travel Credentials shall "[…] contain the same personal data, including facial image, as the passport or travel document based on which they are issued or created" (Article 12.1), or that "the digital representation of a person's identity issued or created pursuant to Article 4 of Regulation (EU) XXXX/XXXX [COM(2024) 670 final]*, Article 1(1a) of Regulation (EC) No 2252/2004**, or Article 2 of Regulation (EU) XXXX/XXXX [COM(2024) 671 final]" (Article 13.(1)). However, this wording could be interpreted narrowly, potentially preventing the inclusion in the Digital Travel Credentials of the same personal data as the passport or travel document based on which they are issued or created, but with an up-to-date value (e.g. recent portrait, current address). Allowing such possibility would enhance trust in the quality of data submitted through Digital Travel Credentials. Eurosmart, therefore, recommends clarifying this aspect in a dedicated recital.

7. Inclusion of Relevant Stakeholders in the Development of Technical Specifications

Eurosmart highlights that it could be beneficial to associate additional stakeholders in the development of the technical specifications and procedures for Digital Travel Credentials, as outlined in Article 12(2). Eurosmart proposes the creation of an expert group consisting of relevant stakeholders, such as industry representatives and carriers, to support the European Commission and Member States in preparing these documents. Eurosmart is ready to apply and join that expert group. This expert group could provide valuable insights on various aspects, including (1) technological choices, (2) technology readiness, (3) needs stemming from potential use cases, and (4) alignment with the EUDI Wallet.

8. Use of Digital Travel Credentials for border crossing

The EU Digital Travel Application enables travelers to submit Digital Travel Credentials to national border management systems ahead of the travel, allowing for pre-border checks or advance clearance. However, Eurosmart recommends clarifying whether the EU Digital Travel Application can also be used at the time of border crossing for presenting the Digital Travel Credential through a physical interaction – without online connection via the Traveller Router – to establish the traveler's identity. If so, it should be specified how this Digital Travel Credential is shared: either through the EU Digital Travel

Application and the Traveller Router or directly from the mobile application to the border control authority.

Article 13(2) (a) and (c) states that a Member State should be allowed to require checking at the border crossing point (1) the data received – through the Digital Travel Credential – against the data in the physical travel document and (2) the authenticity and integrity of the physical travel document when deemed necessary, in particular – but not only – for security reasons.

9. Recommended Timeline for Application of Digital Travel Credentials Provisions

Article 20 sets a 12-month period after the entry into force of the Implementing Act for adopting the relevant technical specifications for the application of the provisions in Article 12(1), which provides for (1) the issuance of Digital Travel Credentials alongside travel documents and (2) the creation of Digital Travel Credentials based on travel documents by Member States. However, this timeframe seems too short, particularly considering the complexities of public procurement processes, which can lead to delays in deployment, testing, and operational readiness. To mitigate these risks and ensure a smooth application, Eurosmart suggests considering extending the timeline to 24 months.

10. For the case of holders of European Residence Permits

The proposal is not clear regarding the case on Digital Travel Credentials based on European Residence Permits, as defined by Regulation (EC) No 1030/2002. Holders of European Residence Permits are likely required to present both their residence permit and travel document (e.g. passport from their country of origin or travel document issued by their residence country) when crossing external Schengen borders. However, the proposal appears to only cover the creation and issuance of Digital Travel Credentials from travel documents (Article 4.1(c)), and not also from European Residence Permits. This raises the question of whether such holders will still need to present their physical European Residence Permits at the border, or if the provision in Article 4.1(c) could also apply to European Residence Permits.

The proposal does not mention Council Regulation (EC) No 1030/2002, and Eurosmart strongly believes that the proposal should also provide for the issuance and creation of Digital Travel Credentials based on European Residence Permits (as defined by Regulation (EC) No 1030/2002) to enhance border facilitation and security for holders of such documents. Therefore, Eurosmart recommends including these documents in the scope of the proposal, potentially within Article 4.

Conclusion

In conclusion, while Eurosmart supports the European Commission's proposal for the EU Digital Travel Application, we believe that the successful and effective implementation of this initiative requires the following key actions from the European Commission:

1. **Clarify the interplay with the EUDI Wallet**: The legal text should clearly define which form the Digital Travel Credentials is to take and specify which entity related to Attestation provider or PID provider. Furthermore, it is essential to ensure that the applicable eIDAS requirements are met and that testing covers all EUDI Wallets deployed in the Member States. For more detailed information, please refer to Chapter 5.

2. **Strengthen and clarify data governance**: The legal text must clearly define the roles of data processors and data controllers for the creation of Digital Travel Credentials. A robust data protection framework should be established to safeguard personal data of EU citizens and EU nationals, in line with the expectations of Member States For more detailed information, please refer to Chapters 3 and 4.
3. **Clarify "Creation" and "Issuance" of Digital Travel Credentials**: The terms "creation" and "issuance" of Digital Travel Credentials need to be clarified and properly distinguished in the legal text to avoid confusion and ambiguities. For more detailed information, please refer to Chapter 1.
4. **Do not undermine the security of border crossing**: The legal text should explicitly authorize Member States to still require individuals to present physical documents at border crossings for security reasons (e.g. when particular risks bound to an individual are suspected). This ensures a layered security approach of border crossing, where individuals with no risks could cross borders without presenting their physical documents but only their Digital Travel Credentials, while risky profiles would still have to present their physical documents. For more detailed information, please refer to Chapters 2, 6 and 8.
5. **Include European Residence Permits in the legal framework**: The legal text should outline the creation and/or issuance of Digital Travel Credentials associated to European Residence Permits. For more detailed information, please refer to Chapter 10.
6. **Establish an Expert Group**: The legal text should provide for the creation of an expert group, involving relevant stakeholders, such as industry representatives and carriers. This group would provide support to the European Commission and Member States in preparing the necessary technical documents. By addressing key aspects, the expert group would contribute to ensuring the smooth and efficient implementation of the Digital Travel Application. Eurosmart is ready to apply and join this group. For more detailed information, please refer to Chapter 7.

Eurosmart, leveraging on its expertise in eIDAS, the EUDI Wallet, and other key areas, is committed to collaborating with relevant stakeholders and contributing to the successful and smooth implementation of the Digital Travel Application.

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