EUROSMART
The Voice of the Digital Security Industry

EU Digital Travel Application: Joint Analysis of the Council and European Parliament negotiating mandates

March 2026

Executive summary

Eurosmart welcomes the negotiating mandates from both the Council and the European Parliament, which introduce significant enhancements to the European Commission's original proposal for the EU Digital Travel Application. Drawing on industry expertise, Eurosmart's recommendations aim to contribute to the ongoing interinstitutional negotiations by helping to ensure a smoother, secure, and scalable implementation, anticipating potential obstacles that may arise.

Eurosmart particularly welcomes the Council's emphasis on better integrating the Digital Travel Credential with existing border management systems, notably ETIAS, EES, and VIS. This approach is expected to contribute to more efficient and streamlined border crossing procedures for all categories of travelers, including EU citizens and third-country nationals. In addition, Eurosmart welcomes the Council's efforts to further refine the definitions of "creation" and "issuance" of Digital Travel Credentials. However, Eurosmart notes that, as currently framed, the Council's position does not yet provide sufficient clarity and completeness, and that the resulting wording may be subject to differing interpretations. Eurosmart, therefore, considers that substantial clarifications and adjustments to these concepts, as well as the corresponding processes, will be required in the course of the interinstitutional negotiations with the European Parliament in order to reach an outcome that can be effectively implemented.

Similarly, Eurosmart supports the European Parliament's negotiating mandate measures aimed at preserving the central role of physical travel documents, clarifying data protection responsibilities, clarifying the nature of Digital Travel Credentials within the EUDI Wallet ecosystem, and reinforcing the security of the system through a closed architecture, high security standards, and regular testing.

While these negotiating mandates represent positive developments, Eurosmart has identified areas where further clarification and refinement during the trilogue negotiations would enhance legal certainty, technical feasibility, data protection, and security. The following sections provide a detailed analysis and recommendations intended to support the successful rollout of a secure, interoperable, robust, and user-friendly EU Digital Travel Application.

1. Negotiating mandate from the Council

1.1. Data processing

Compared to the proposal from the European Commission, the amended Article 7 of the negotiating mandate from the Council brings clarifications regarding which entities are data controller and data processor. However, there is still no clarification on who the data processor is for the processing of personal data in the backend validation service. **Eurosmart recommends clarifying which entity(ies) would have that responsibility.**

Article 7.1e clarifies that data processed in the backend validation service shall be deleted after the operations described in Article 3d have been carried out. Yet it seems that other processing may also be carried out in the backend validation service, such as the one relating to Article 4.5 (authentication or person's identity using and electronic identification means of level of assurance "High"). **Therefore, the scope of Article 7.1e should be extended to cover any processing which may take place in the backend validation service and not only the one described in Article 3d.**

1.2. Authentication of person's identity using an electronic identification of level of assurance "High" to obtain a Digital Travel Credential

According to Article 4.5 and recital (6), the authentication of person's identity using an electronic identification of level of assurance "High" is an alternative to the facial matching of the person with the facial image stored on the chip for the creation of a Digital Travel Credential. However, discrepancies and lack of clarity regarding this alternative are present in the text. As per recitals (6) and (7), the backend validation service is the component which carries out the authentication of person's identity using an electronic identification of level of assurance "High". Nevertheless, this responsibility is not foreseen in Articles 2(f) and Article 4.5.

It is also very likely that the backend validation service will have to rely on national systems for the authentication of person's identity using an electronic identification of level of assurance "High" to (1) interact with the electronic identification means and (2) carry out the authentication, as the electronic identification means is issued by Member States. Thus, the backend validation service is very likely to rely – partly or entirely – on national systems to carry out that operation.

Therefore, Eurosmart strongly recommends:

- **adding in Article 2(f) and Article 4.5 the parts – if any – of the authentication of person's identity using an electronic identification of level of assurance "High" carried out by the backend validation service;**
- **describing and clarifying in specific articles the interaction of the EU Digital Travel Application with the national systems when creating Digital Travel Credentials by authenticating person's identity using an electronic identification of level of assurance "High".**

1.3. Creation vs Issuance of Digital Travel Credentials

The negotiating mandate from the Council is ambiguous regarding the meaning of creation and issuance of Digital Travel Credentials. The creation of a Digital Travel Credential is the operation whereby the Digital Travel Credential is generated and stored in the mobile component for future use (recital (7a), Article 2(e), Article 3a.1 or the last sentence of Article 4.5). The issuance describes the operation whereby the Digital Travel Credential is generated to be stored in an EUDI Wallet for future use (recital (7a), Article 1.1, Article 4.2 or the last sentence of Article 4.5). Therefore, "creation" and "issuance" appear to be intended to be exclusive, as confirmed in various provisions of the text, namely Article 2(g), Article 4, Article 4.7, Article 13.1. However, some provisions use both the terms "creation" and "issuance", which can lead to confusion, as outlined below:

- "To promote the use of digital travel credentials, digital travel credentials created in the mobile component of the application should be able to be issued to the user's European Digital Identity Wallet following the format of electronic attestation of attributes." (recital 7a);
- "[…] Digital travel credentials created using the functionalities of the EU Digital Travel application may be issued following the format of electronic attestations of attributes to European Digital Identity wallets. […]" (Article 1.1);
- "[…] the issuance of digital travel credentials created in the EU Digital Travel application for use in the European Digital Identity Wallet following the format of electronic attestations of attributes […]" (Article 3.5(b)).

It raises the following points for clarification:

- Would it mean that the issuance of a Digital Travel Credential (in the EUDI Wallet) requires first its creation (in the mobile component)?
- If so, would it mean that it is not possible to issue directly a Digital Travel Credential without prior creation?

Eurosmart strongly recommends clarifying this aspect in Article 4.

1.4. Amendment to Regulation (EC) No 2252/2004

Article 12 amending Regulation (EC) No 2252/2004 gives rise to confusion, especially concerning the interpretation of the amending text 1a(a) which states:

> "1a Upon request from the applicant or holder of a passport or travel document, the Member State having issued the passport or travel document may issue a digital travel credential, which shall:
>
> (a) be capable of being used in the mobile component referred to in Article 3a of Regulation (EU) .../... COM(2024) 670 final and be based on the technical specifications adopted pursuant to Article 2, point (d);"

The use of the term "issue" (which implies that the Digital Travel Credential is stored in the EUDI Wallet) together with the sentence "shall be capable of being used in the mobile component" (which

implies that the Digital Travel Credential is stored in and used from the mobile component) can lead for this provision to be understood in two opposing ways:

- **Either** the Digital Travel Credential shall be issued, and thus stored and usable from an EUDI Wallet, **or**
- The Digital Travel Credential shall be created, and thus stored and usable from the mobile component.

Eurosmart strongly recommends clarifying this point and reviewing the wording of the provision. In addition, if the intention is for Member States to store Digital Travel Credentials in the mobile component, Eurosmart advises clarifying the interaction between the national systems and the EU Digital Travel Application.

1.5. Issuance of Digital Travel Credentials

Regarding the issuance of Digital Travel Credentials, some provisions suggest that both eu-LISA and Member States are entitled to issue Digital Travel Credentials (Article 1.1, Article 4.3(b) and Article 3d.1a). While recital (7a) suggests that eu-LISA only issues Digital Travel Credentials on behalf of Member States. **Eurosmart strongly recommends clarifying this aspect in the relevant Articles.**

If both eu-LISA and Member States are entitled to issue Digital Travel Credentials, the following issues arise:

- Regarding the provision of Article 3b.3 stating that the backend validation service "[…] shall enable the issuance of digital travel credentials to European Digital Identity Wallets […]", it is unclear whether it applies only to Digital Travel Credentials issued by eu-LISA or also to those issued by Member States. **Eurosmart strongly recommends clarifying this aspect in Article 3b.3. In addition, if the backend validation service shall also enable issuance of Digital Travel Credentials by Member States, Eurosmart recommends clarifying the interaction between the EU Digital Travel Application (backend validation service) and the national systems.**
- As per Article 4.3, only Digital Travel Credentials issued by Member States can be retrieved by the EU Digital Travel Application, meaning that those issued by eu-LISA could not be retrieved and thus could not be used for any of the uses described in Article 4a. **Eurosmart strongly recommends clarifying this interpretation.**

1.6. Process for the creation and issuance of Digital Travel Credentials

The process for the creation and issuance of Digital Travel Credentials described in Article 4.5 is unclear.

- The first sentence reads "Before the creation of a digital travel credential […]". Could you clarify whether the verification of integrity and authenticity of the chip of a travel document, passport or identity card is only applicable for the creation of Digital Travel Credentials but not for their issuance?

- Regarding the next sentence ("[…] The backend validation service shall, in accordance with Article 3b, compare the live facial image of the person seeking to create the digital travel credential with the facial image stored on the chip, unless the person's identity, in accordance with the implementing act referred to in Article 16(1) (a), can be authenticated using an electronic identification means conforming to assurance level high in accordance with the requirements of Regulation (EU) No 910/2014. If any of the verifications fail, the EU Digital Travel application shall not issue a digital travel credential to the European Digital Identity Wallet or create a digital travel credential in the mobile component"). Could you clarify whether:
    - The comparison of facial image is only applicable for the creation of Digital Travel Credentials as suggested by the wording "[…] of the person seeking to create […]"?
    - The alternative relying on the authentication of the person's identity using an electronic identification means of level of assurance "High" is applicable both for the creation and the issuance of Digital Travel Credentials?
- Considering the entirety of Article 4.5, could you clarify whether for the issuance of Digital Travel Credential:
    - no travel document, passport or identity card are required?
    - It requires only the authentication of the person's identity using an electronic identification means of level of assurance "High"?
- Assuming the above applies to the issuance of a Digital Travel Credential:
    - if the Digital Travel Credential is to contain the holder portrait, what would be the source of the holder's portrait as (1) it cannot come from the travel document, passport or identity card and (2) it may not be available in the electronic identification means or the Member States' database?
    - How to ensure that the holder's portrait included in the Digital Travel Credential is trusted, i.e. the one of the genuine holder to avoid impersonation?
    - It requires to (1) verify that the applicant holds a valid travel document, passport or identity card and (2) access some data (e.g. validity, type) which are only known by the Member State that has issued that document. Therefore, what are the interactions between the EU Digital Travel Application and the national systems providing such information?

Eurosmart strongly recommends clarifying these aspects.

1.7. Interaction between the EU Digital Travel Application and the carrier gateway

Article 4a.6 provides for the possibility of carriers to use the Digital Travel Credential to fulfill their obligations by submitting the Digital Travel Credential through the carrier gateway to (1) verify if the traveler holds a valid travel authorization or (2) transmit advance passenger information to the receiving State. However, it is unclear which component of the EU Digital Travel Application should interface with the carrier gateway. Article 3a (Mobile component), 3b (Backend validation service) and Article 3c (Traveller Router) do not describe such interaction.

Eurosmart recommends clarifying in Article 4a.6 which component carries out the interface with the carrier gateway.

2. Negotiating mandate from the European Parliament

2.1. Technical architecture and design of the EU Digital Travel Application

The use of facial recognition is a proven technology that is widely used for border crossing. It has demonstrated effectiveness in combating fraud and it has been shown to meet the highest level of data protection. Therefore, facial recognition should not be set aside. **In light of the above, Eurosmart recommends that Amendment 3 from the LIBE Committee not be taken forward.**

In the original proposal from the European Commission, data are transmitted from the mobile application to the competent authorities via the Traveller Router using encryption. As such, the Traveller Router can seamlessly interconnect the large number of mobile applications with the 27 national systems and competent authorities, while hiding the underlying complexity and ensuring scalability. In order to maintain confidentiality, the Traveller Router can implement transciphering, whereby it decrypts the received data and immediately encrypts it with the recipient's key (e.g. data received from the mobile application are decrypted and then encrypted with another key to send it to the competent authority). In this approach the Traveller Router manages transciphering between entities and securely manages all the relevant keys internally. This approach (1) makes the architecture of the EU Digital Travel Application simpler, (2) streamlines data exchange between any mobile application and any competent authorities, and (3) allows scaling up the number of mobile applications and competent authorities in a completely seamless manner. The Amendments 13, 20, 50, 77 (point 6), and 78 from the LIBE Committee, and Amendments 2 and 5 from the TRAN Committee require implementing end-to-end encryption between the mobile application and the competent authorities. Such end-to-end encryption is likely to have very substantial impacts on the overall architecture of the EU Digital Travel Application and in particular on the features, role, and design of the Traveller Router, which in turn will substantially impact the overall capacity and performance of the EU Digital Travel Application. **Accordingly, Eurosmart recommends that Amendments 13, 20, 50, 77 (point 6), and 78 from the LIBE Committee, as well as Amendments 2 and 5 from the TRAN Committee, not be taken forward.**

Likewise, Eurosmart highlights that it may be complex to design the EU Digital Travel Application and the mobile application in such a way that there is a direct and secure communication between the (1) carriers and the (2) mobile component. In particular this approach may not provide a scalable design and may raise security issues (e.g. if a new carrier allowed to retrieve a Digital Travel Credential is added, should all mobile applications be updated? How should the credentials that allow the carrier to interconnect with the mobile application be distributed and secured in the mobile application and in the carrier system?). Instead, a better approach could be to organize the interconnection through the Traveller Router so that all the complexity of interfacing the mobile application with carriers is managed by a single component (the Traveller Router). **Therefore, Eurosmart recommends that Amendment 77 (point 3) from the LIBE Committee not be taken forward.**

Amendments 24 and 90 from the LIBE Committee would prohibit innovative approaches and solutions in which travelers would be authenticated using one to several biometric comparison. For instance,

such approach could be used to allow all low-risk passengers of an aircraft that has landed to cross a border crossing point seamlessly without any actions (such as presenting a passport). These approaches and solutions could provide a better user experience while still being able to meet data protection and privacy expectations and requirements. **Hence, Eurosmart recommends that Amendments 24 and 90 from the LIBE Committee not be taken forward.**

Eurosmart strongly recommends that the Digital Travel Credential take the shape of an "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, as it is meant to be issued solely by public entities. On the other hand, the shape proposed in Amendments 28, 54 and 100 from the LIBE Committee – qualified electronic attestation of attributes – may be issued by the private sector, which is not acceptable for Digital Travel Credentials. **Therefore, Eurosmart recommends that Amendments 28, 54 and 100 from the LIBE Committee not be taken forward and that they be revised so that Digital Travel Credentials take the shape of an "electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source" (Article 3.46 of the eIDAS Regulation).**

Regarding Amendment 9 from the TRAN Committee, the meaning of "interoperable" is unclear. In addition, Eurosmart observes that the mobile application does not have to be interoperable, as it is one piece of the EU Digital Travel Application, which is intended to be used solely as part of the EU Digital Travel Application (closed system). **Accordingly, Eurosmart recommends that Amendment 9 from the TRAN Committee not be taken forward.**

Eurosmart highlights that the privacy of individuals cannot rely solely on the data model. Instead, the privacy of individuals shall be ensured by the EU Digital Travel Application as a whole. **Hence, Eurosmart recommends that Amendment 14 from the TRAN Committee not be taken forward.**

Eurosmart notes that Amendment 21 from the TRAN Committee, is unclear and ambiguous, and as such can be misunderstood. In addition, the only advanced digital identity solution to be integrated is the EUDI Wallet introduced by the eIDAS Regulation, which is already considered by the text. Allowing other digital identity solutions other than the EUDI Wallet to be integrated would undermine the objective of eIDAS Regulation and the EUDI Wallet by promoting fragmented approaches rather than a unified one (the EUDI Wallet). **Therefore, Eurosmart recommends that Amendment 21 from the TRAN Committee not be taken forward.**

2.2. Age limitation

The proposed amendments regarding age limitation to benefit from Digital Travel Credential may substantially limit their uptake, as it would deprive any family with a child below 16 of (1) enjoying and benefiting from Digital Travel Credential and ultimately (2) a smooth border crossing.

Currently, for the use of e-gates implementing automatic border crossing with facial recognition, the minimum age is left up to Member States and is lower than 16 years old. As the purpose for implementing Digital Travel Credential is the same as for e-gates implementing automatic border crossing with facial recognition, there is no reason to change the approach regarding the minimum age to enjoy this benefit. Instead we suggest leaving it up to Member States to define the minimum age to use and benefit from the Digital Travel Credential, in the same way as the minimum age to use e-gates implementing automatic border crossing with facial recognition is set by Member States.

Hence, Eurosmart recommends that Amendments 5, 32, 52, 55, 59, 99 and 102 from the LIBE Committee not be taken forward.

2.3. Maximizing impacts and benefits of Digital Travel Credentials

Eurosmart supports Amendments 28, 99 and 101 from the LIBE Committee which will foster a large-scale uptake of the Digital Travel Credential by ensuring that holders of previously issued travel documents and passports are also eligible to obtain a Digital Travel Credential and that the request can be made at any point in time. As such, it will ensure that quickly a large portion of EU citizens and nationals can use and enjoy the Digital Travel Credential without having to wait for the renewal of their passports or travel documents.

Digital Travel Credentials may also be very useful to individuals in the future in contexts other than border crossing. **Therefore, Eurosmart recommends that Amendment 34 from the LIBE Committee not be taken forward as it provides for the possibility to use the Digital Travel Credential for other purposes provided (1) it is allowed by Union or national law, and (2) that national law complies with Union law.**

2.4. Removing potential bottlenecks in the process of border crossing

It may be very useful to allow any stakeholders involved in the process of crossing the external borders to have access to the storage medium (chip) of the travel documents and passports, as provided for in the regulation proposal. It would (1) improve the user experience by streamlining the process, and (2) enhance security. The ambition of this regulation to streamline border crossing could fail if a single bottleneck remains in the overall process of crossing the external borders. Therefore, this provision as found in the proposal from the European Commission, is very important to address bottlenecks in the process of crossing the external borders which have not been explicitly foreseen. **Hence, in order to ensure the success of this regulation, Eurosmart recommends that Amendment 103 from the LIBE Committee not be taken forward and for Amendment 25 from the TRAN Committee be kept.**

2.5. Deadline for implementing the EU Digital Travel Application

The deadline for implementation of EU Digital Travel Application proposed in Amendments 82, 107, 108 and 109 from the LIBE Committee is challenging (1.5 years after the entry into force of this Regulation), as it may be too short for such a complex and ambitious system. A shorter implementation timeline could potentially affect the quality, security and overall functioning of the EU Digital Travel Application. **Therefore, Eurosmart recommends that Amendments 82, 107, 108 and 109 from the LIBE Committee not be taken forward.**

2.6. Keeping the physical passport and travel document at the core of border security

Eurosmart very much welcomes Amendments 16 and 94 from the LIBE Committee, whereby the possession of a physical travel document shall remain the rule for border crossing. It is important to ensure (1) a higher level of resilience in case the IT resources are not available (mobile phone, EU

Digital Travel Application, due to power outage or cyberattacks), and (2) support for advanced control at the border in case of doubt or for a high-risk profile passenger.

Likewise, **Eurosmart supports Amendments 53 and 55 from the LIBE Committee**, which better clarify the features that shall be supported by travel documents used by non-EU citizens to obtain a Digital Travel Credential. Such clarifications are important to ensure consistent security across travel documents used to obtain Digital Travel Credentials, whether they are issued by an EU Member State or a third country.

2.7. Clarification on data protection

Eurosmart welcomes Amendments 69 and 71 from the LIBE Committee, clarifying who is the data processor for the backend validation service and who are the data controllers.

Eurosmart also supports Amendment 72 from the LIBE Committee, as it will further strengthen data protection by ensuring that eu-LISA would not (1) engage another processor, or (2) transfer any personal data to a third country or international organization.

2.8. Ensuring a high level of security of the EU Digital Travel Application

Eurosmart welcomes Amendment 11 from the LIBE Committee, which will ensure that all components of the EU Digital Travel Application are controlled and that the EU Digital Travel Application is a closed system. It is essential to foster trust amongst travelers.

Eurosmart supports Amendment 77 (point 2), Amendment 80, Amendment 87, and Amendment 111, from the LIBE Committee, as well as Amendment 16 (points 2 and 5) from the TRAN Committee, which also support a high level of security for the EU Digital Travel Application by:

- requiring a state-of-the-art security and the application of the highest security standards;
- requiring regular penetration tests of the EU 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