

European Pirate Party

Response to the European Commission Public Consultation on the Draft Implementing Regulation Amending Regulations (EU) 2024/2979, 2024/2980 and 2024/2982 concerning Technical Standards and Specifications for the EU Digital Identity Wallet

Document Reference: Ares (2026)1286304

Submission deadline: March 5, 2026

The European Pirate Party (PPEU) is a pan-European political party representing Pirate Parties across EU Member States. Our movement is rooted in the defence of digital rights, civil liberties, and democratic participation. We view the internet and digital infrastructure as common goods and public utilities that must serve all citizens.

Our position on the EU Digital Identity Wallet flows directly from the core principles shared by the Pirate movement across Europe. Our manifesto commits us to the highest standards of civil rights, individual privacy and transparency of public institutions.

We believe that:

- *The privacy of the individual should be valued at all times and protected from being exploited by public and economic actors.*
- *Power resides with the people. Their rights and their dignity stand above all else.*
- *Transparency and accountability for public institutions are the counterpart of good data protection regulation to protect privacy.*

We believe that identity is among the most intimate things a state can ask of its citizens. How a government collects, stores, and shares proof of who you are, demonstrates the relationship between citizen and state, and shows whether that relationship is built on trust or on surveillance. Thus, a digital wallet that requires the inclusion of biometric attributes without providing a non-biometric alternative, enables tracking through publicly accessible revocation lists, and hands browser vendors privileged access to credential metadata is not a neutral infrastructure upgrade but a statement about what that relationship looks like.

We also believe that the gap between regulatory intent and technical reality is where we lose our rights. The eIDAS 2.0 framework promises citizen empowerment and selective disclosure. But implementing regulations that reference unpublished standards, exclude public interest actors through paywalled specifications, and embed platform dependencies into core infrastructure deliver something different in practice. Good intentions written into recitals do not survive bad architecture.

We affirm that concentration of power over identity infrastructure is a democratic risk regardless of who holds it. Whether that concentration sits with a government database, a dominant platform, or an opaque certification body, citizens lose when there is no meaningful

accountability, no route to challenge decisions, and no transparency about how the system works. The wallet framework must distribute power, not reorganise it.

Why We Are Responding

The EU Digital Identity Wallet is one of the most ambitious digital infrastructure projects in European history. Per eIDAS 2.0 ([Regulation \(EU\) 2024/1183](#)), by late 2026, every EU Member State must provide its citizens with a wallet capable of storing, managing, and sharing verified identity credentials across the Union. The implementing regulations in this initiative, will define the precise technical architecture, data formats, cryptographic standards, and governance mechanisms that will shape how hundreds of millions of Europeans interact with public and private services for years to come.

We welcome the ambition of a European digital identity framework that reduces fragmentation, improves cross-border interoperability, and gives citizens greater control over their credentials. However, the technical choices embedded in this initiative, are not neutral. They determine who can build wallets, what data is collected, how users can be tracked, and who holds power over critical infrastructure.

We believe that these choices require democratic scrutiny and so we are responding to ensure the wallet framework is designed around citizens, openness, and around accountability.

Opportunities and Risks

A well-designed framework for the EU Digital Identity Wallet, could reduce European dependence on commercial identity providers like Google and Apple, enable selective disclosure so citizens share only what is strictly necessary, and create portable, interoperable credentials that work across borders. These are outcomes worth pursuing, and we want to see them delivered.

But the wallet's value depends entirely on the choices made at the technical level. The same infrastructure that could empower citizens could just as easily surveil them, enable open competition and entrench monopolies. The difference lies in decisions that look like implementation detail but are in fact, political choices.

We see the following risks in the current draft that require revision before that potential can be realised.

The wallet mandates biometric data collection i.e., a facial portrait image for all users, with no non-biometric alternative. This is disproportionate and sets a dangerous precedent for identity infrastructure that will be used by hundreds of millions of people across the Union.

Multiple annexes reference technical standards that have not yet been published. They are either marked "tbc" or carrying draft version numbers such as "V0.0.12." Binding regulations should not be built on specifications that do not yet exist in final form. This creates legal uncertainty for Member States, developers, and citizens alike.

Additionally, the API-mediated request framework requires wallets to disclose the presence of stored credentials to browsers and operating systems by default. This grants platform vendors like Google, Apple and Microsoft, structural access to citizen identity metadata, with purpose limitations that have no enforcement mechanism behind them.

Also, the Trust Mark verification mechanism depends on Commission-controlled URLs with no fallback. The tool citizens would use to verify their wallet's own certification status, is listed as optional.

Finally, with high certification costs and complex compliance requirements, there is the risk of concentrating the ability to issue and manage credentials in a small number of large corporations, foreclosing the open-source and civil society participation that legitimate public infrastructure requires.

These risks are addressable so, we have set out where we believe revision is needed and what we are asking for, in the following sections:

1. Privacy and Data Protection

Under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, as well as Articles 5(1)(c) and 25 of Regulation (EU) 2016/679 (GDPR), any identity architecture must satisfy strict proportionality, data minimisation, and privacy-by-design requirements. Technical implementation must reflect these binding legal standards. This means that privacy is the foundation of legitimate identity infrastructure. Therefore, a wallet that normalises disproportionate data collection, enables tracking, or concentrates surveillance capability in platforms, undermines the civil liberties which this regulation claims to protect.

1.1 Disproportionate Data Collection and Surveillance Risks

Annex I, Table 1 mandates a facial portrait image as a mandatory person identification data attribute, compliant with ISO/IEC 19794-5 quality specifications. While facial images are already used in many national identity documents, the implementing regulation does not provide an explicit proportionality assessment for mandating their inclusion across all wallet implementations, nor does it require Member States to provide a non-biometric alternative for cross-border authentication purposes.

Biometrics are particularly risky in the sense that they are immutable, uniquely identifying, and capable of enabling surveillance at scale. Under Article 5(1)(c) GDPR and Article 52(1) of the Charter, such measures must be strictly necessary and the least intrusive means available. However, the regulation provides no alternative for citizens who cannot or do not wish to provide biometric data, nor any explanation of why this is necessary given the range of non-biometric identifiers already included.

Additionally, the optional field for `personal_administrative_number` (Annex I, Table 2) requires Member States to “describe in their electronic identification schemes... the policy that they apply to the values of this attribute.” In practice, this creates pressure towards inclusion as national schemes are designed around existing administrative identifiers. A national ID

number embedded in a digital wallet that is presented across services, creates a cross-service tracking identifier with significant surveillance potential.

Similarly, the “sex” field lacks any limitation on when it can be requested. People could be required to provide this information without the requesting party, demonstrating a clear legal basis for that specific use case. The regulation also specifies that where an attribute value “is not known for the person or cannot otherwise be issued,” Member States shall use “an attribute value appropriate to the situation instead.” This is dangerously vague. Who determines what is “appropriate”? This language opens the door to Member States inserting placeholder values without any standardised framework, potentially corrupting the integrity of the person identification data. Implementing regulations should not rely on undefined discretionary terminology in core identity attributes without harmonised criteria or interpretative guidance.

1.2 Surveillance Infrastructure Risks

The revocation mechanism specified in Annex Ib requires that status lists “shall, where appropriate, relate to at least 10,000 attestations” (R-WP-WUA-1.1). These lists are publicly accessible. While the 10,000-attestation minimum is designed to provide an anonymity set, we note that this threshold may be insufficient to prevent correlation attacks, particularly as wallet deployments grow and lists become more granular. As recognised in data protection jurisprudence, anonymisation requires that re-identification risk be reasonably unlikely in light of available means (see Recital 26 GDPR). Where revocation lists become segmented by issuer, credential type, or geography, effective anonymity sets may fall significantly below nominal thresholds.

The regulation mandates permanent, irreversible revocation of Mobile Security Objects (EAA-6.2.10.1-04 in Annex V), with no provision for temporary suspension. A citizen who loses their device, or whose credentials are revoked in error, has no recourse short of full reissuance. This is disproportionate and raises due process concerns under Article 41 of the Charter, that the regulation does not address.

The API-mediated request framework (Annex XIV, Section 6.3.4) requires wallet units to “by default disclose the presence of all stored electronic attestations of attributes to the mediating API” – that is, to the browser or operating system. While the regulation prohibits disclosure of attribute values, the disclosure of attestation “presence” is sufficient to create a detailed metadata profile: that a user holds a driver’s licence, a medical qualification, a social security credential. Combined with browser-level data, this constitutes a powerful fingerprinting capability. The parallel to Chat Control debates, where scanning metadata was argued to be less intrusive than content analysis, is instructive: metadata surveillance is surveillance. Indeed, the Court of Justice has repeatedly recognised that metadata may be highly revealing (see Joined Cases C-203/15 and C-698/15, *Tele2 Sverige*).

1.3 Enforcement Deficits and Coercive Privacy Trade-offs

The purpose limitation provisions (OIDFVP-HAIP-API_REQ-02 to 04) prohibit browsers and operating systems from using wallet metadata for “market analysis purposes.” However, no enforcement mechanism or audit requirement is specified. Given the documented history of platform data misuse under GDPR, where purpose limitation provisions have repeatedly

proven insufficient without independent technical enforcement, this prohibition is likely to be ineffective in practice.

A global opt-out from API disclosure is available to users (OIDFVP-HAIP-API_REQ-07), but the regulation states that where this is disabled, the wallet unit “shall not advertise or respond to API-mediated requests.” This is a coercive choice: privacy at the cost of functionality. Genuine data sovereignty requires that users can protect their metadata without being excluded from the wallet’s core capabilities.

In light of these privacy risks, we call on the commission to;

- Make biometric data (facial portrait) optional, with non-biometric alternatives required for all wallets.
- Increase the minimum status list anonymity set to at least 100,000 attestations, and prohibit metadata aggregation from status list monitoring.
- Introduce a temporary revocation mechanism with a defined appeals process before permanent revocation is applied.
- Replace the opt-out model for API-mediated disclosure with an opt-in model, with full functionality preserved where users decline.
- Require independent technical audits of browser and OS compliance with purpose limitation provisions.

2. Open Standards and Interoperability

The wallet framework’s legitimacy depends in part on whether its technical foundations are truly open. To be truly open, it has to be accessible to all developers, implementable without prohibitive cost, and free from monopolistic control. The current regulation raises significant concerns on each of these dimensions.

2.1 Standard Accessibility

The cryptographic mechanisms mandated by Annex Ia are defined exclusively by reference to ENISA’s “Agreed Cryptographic Mechanisms.” While ENISA is a credible body, this arrangement creates a single point of authority over cryptographic choices for an infrastructure used by 450 million Europeans. The governance process for updating this list, including stakeholder consultation and public input timelines, is not specified in the regulation.

A significant portion of the standards referenced in Annex V are ISO/IEC standards, including ISO/IEC 18013-5 and ISO/IEC 18013-7. These standards are sold commercially and are not freely accessible to developers, researchers, or civil society organisations. A regulation that mandates compliance with paywalled standards effectively excludes public interest actors from meaningful implementation and scrutiny. This is incompatible with the principle that technical infrastructure serving the public must be publicly auditable.

2.2 Unfinished Standards

Multiple provisions across Annexes VI, XIII, and XIV reference ETSI TS 119 472-3 described as “[tbc]” with version number V0.0.12 (2026-1). This is a draft standard that, as of the consultation period, has not been finalised or published. Implementing regulations should not reference unpublished specifications: doing so creates legal uncertainty for Member States and developers, and removes the specification from democratic oversight. If the standard changes after the regulation is adopted, there is no mechanism to reflect this without further legislative action.

Similarly, numerous requirements throughout Annex XIV are marked “void” without explanation. Retaining void provisions in a binding implementing regulation is confusing and may create interpretive conflicts between Member States.

2.3 Vendor Lock-in Risks

The API-mediated presentation framework in Annex XIV references CTAP 2.2 (Client to Authenticator Protocol) and ISO/IEC 18013-7 Annex C mechanisms that are primarily implemented by major browser and operating system vendors. Mandating these specific protocols without requiring vendor-neutral alternatives places significant structural power over wallet interactions in the hands of Apple, Google, and Microsoft. This directly contradicts the goal of European digital sovereignty.

The reliance on OpenID4VC-HAIP - while a technically sound choice - introduces dependency on the OpenID Foundation’s governance processes. The regulation does not specify how EU interests are represented in that governance, or what happens if the specification diverges from EU requirements.

In light of the risks regarding open standards and interoperability, we call on the commission to;

- Remove all references to unpublished or draft standards. Regulations must only reference finalized, published specifications.
- Require that all standards referenced in eIDAS implementing regulations be freely accessible to the public, with the Commission funding access where necessary.
- Require vendor-neutral API interfaces for wallet-browser/OS interaction, with open-source reference implementations provided.
- Remove or explain all “void” provisions, and provide a mechanism for fast-track regulatory alignment when referenced standards are updated.
- Specify ENISA’s cryptographic mechanism governance process, including consultation timelines and public comment periods.

3. Transparency and Governance

Accountability requires that citizens can verify the claims made by wallet providers, understand what certification means, and have recourse when things go wrong. The current Trust Mark and governance framework is a start, but has significant gaps.

3.1 Trust Mark Implementation

Article 14a mandates that wallet providers display the EU Digital Identity Wallet Trust Mark, with no provision for user opt-out. While we understand the regulatory logic of a visible certification signal, mandatory display without user control raises questions: a user seeking anonymity or testing a wallet in a private context cannot remove a government-mandated brand mark. The Trust Mark serves regulatory purposes; users should choose whether and how it is surfaced.

The verification mechanism for the Trust Mark depends on URLs “provided by the European Commission” (Article 14a (2)). This creates a critical dependency on Commission-controlled infrastructure. If these URLs are unavailable, users cannot verify certification status. There is no fallback mechanism, no decentralised verification option, and no requirement for mirror availability. The `WalletVerifierToolURL` field in Annex VIII (Trust Mark data) is listed as optional – we question why a tool for verifying the wallet’s own certification status is not mandatory.

3.2 Wallet Provider Accountability

The regulation introduces wallet instance attestations (WIA) and wallet unit attestations (WUA) as the primary mechanism for verifying wallet integrity. Wallet providers sign these attestations, and issuers of person identification data verify them against the trusted list of wallet providers. This architecture is sound in principle, but the regulation does not specify what happens when a wallet provider loses certification or ceases operations. Are existing credentials immediately invalidated? Is there a migration window? What are user data protection obligations during provider termination?

The certification information included in wallet unit attestations (C-claim-3, Annex Ib) includes “information on the conformity assessment body that certified the wallet solution, the certification number.” This information should be publicly queryable in a standardised format, not merely included as metadata in attestation tokens that most users cannot inspect.

3.3 User Rights and Informed Consent

Article 3 of the amendments to Implementing Regulation (EU) 2024/2982 requires wallet units to display information from relying party access certificates and wallet instance attestations before any disclosure. This is positive in principle. However, the volume and technical complexity of certificate metadata is not comprehensible to most users. Requirements to “display information” are not equivalent to requirements to enable informed decisions. The regulation should specify minimum comprehensibility standards for user-facing information.

The concept of “embedded disclosure policies” (Article 3(9)(b)) processed before user approval is also concerning. Who writes these policies? Under what public scrutiny? The regulation references their processing as a precondition for presentation without defining their content, scope, or accountability framework.

In light of these transparency and governance issues, we call on the commission to:

- Make `WalletVerifierToolURL` mandatory in Trust Mark data specifications.

- Require decentralised or mirrored verification infrastructure for Trust Mark status, removing single-point-of-failure dependency on Commission URLs.
- Establish a public, machine-readable registry of certified wallet solutions with certification history and status.
- Define minimum comprehensibility standards for user-facing disclosure information, with user testing requirements before certification.
- Require mandatory provider termination plans with minimum 12-month user migration windows and data portability obligations.
- Subject “embedded disclosure policies” to public consultation and parliamentary scrutiny before implementation.

Conclusion

The European Pirate Party supports the goal of a European digital identity framework that empowers citizens and reduces dependency on commercial identity providers. The EU Digital Identity Wallet has genuine potential to strengthen European digital sovereignty, protect privacy by enabling selective disclosure, and give citizens portable, interoperable credentials across the Union.

However, as currently specified, the implementing regulation contains provisions that risk undermining these goals. Mandatory biometric data collection, inadequate revocation privacy, platform surveillance via API-mediated disclosure, references to unpublished standards, paywalled specifications, and opaque governance structures are political choices with consequences for civil liberties.

We call on the Commission to revise the implementing regulation to:

- Embed privacy by design and data minimisation as non-negotiable foundations, not aspirational principles;
- Ensure all referenced technical standards are finalized, publicly accessible, and free to implement;
- Prevent platform capture of wallet infrastructure through genuinely open, vendor-neutral interfaces;
- Build accountable, transparent governance structures that give citizens real visibility into and control over the infrastructure that holds their identity.

Embedding privacy by design, ensuring legal certainty in technical references, preventing structural platform gatekeeping, and strengthening transparency mechanisms would enhance the legitimacy and durability of the European Digital Identity Wallet.

The EU Digital Identity wallet will be used by hundreds of millions of Europeans for decades. It deserves to be built on foundations that earn and sustain democratic trust.

European Pirate Party (PPEU)

europeanpirates.eu

References

- (GDPR), R. (. (2016). Retrieved from Regulation (EU) 2016/679 (GDPR): <https://gdpr-info.eu/>
- Commission, E. (2024). *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183>
- Court of Justice of the European Union (CJEU), G. C. (2016, December 21). *Tele2 Sverige and Watson (Joined Cases C-203/15 and C-698/15)*. Retrieved from https://infocuria.curia.europa.eu/tabs/affair?sort=AFF_NUM-DESC&searchTerm=%22C-203%2F15%22&publishedId=C-203%2F15
- Pirates, E. (n.d.). *European Pirate Party*. Retrieved from <https://europeanpirates.eu/manifesto/>
- Union, C. o. ((2000/C 364/01)). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf