

## European Pirate Party

### *Response to European Commission Public Consultation Implementing Regulation amending Implementing Regulation (EU) 2025/1569 Technical Specifications for Qualified Electronic Attestations of Attributes (QEAA)*

*Document Reference: Ares (2026)1286389*

*Submission Deadline: 5 March 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 Qualified Electronic Attestations of Attributes 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 institutional power determines who gets to issue official credentials such as degrees, professional qualifications, benefits entitlements, health records.

Under Article 16 of the Charter of Fundamental Rights (freedom to conduct a business) and Articles 7 and 8 (privacy and data protection), regulatory frameworks must ensure that security requirements do not produce disproportionate exclusion of lawful actors or unnecessary concentration of verification power.

When only a handful of corporations can afford the certification required to become trust service providers, the result is gatekeeping even though the goal originally, was security. In the same vein, when government databases log every verification request without accountability, this results in surveillance. Thus, the rules governing electronic attestations determine whether credential systems serve citizens or control them. Regulatory design must therefore satisfy the principle of proportionality under Article 52(1) of the Charter i.e., measures must be suitable, necessary, and the least restrictive means available.

We also believe that market structure is not separate from citizen rights. Certification requirements that cost hundreds of thousands of euros and take years to complete do not create a level playing field. They exclude universities, professional associations, civil society organisations, and open-source projects from participation in infrastructure that is meant to serve the public. When only large corporations can comply, the market serves corporate interests, not the public interest.

We affirm that transparency is not optional in public sector systems because, when the government databases that verify credentials operate without public accountability, when verification logs are collected without disclosure, and when citizens have no visibility into who accessed their data or why, trust cannot exist. Attestation systems built on opacity serve institutional convenience, not democratic legitimacy.

## **Why We Are Responding**

The framework for Qualified Electronic Attestations of Attributes, established under eIDAS 2.0 and detailed in the implementing regulations under consultation here, governs who can issue verifiable credentials in Europe and under what conditions. These credentials will include professional qualifications, educational degrees, social security entitlements, health records, and other attributes that determine access to employment, services, and rights across the Union.

We welcome the goal of cross-border credential recognition and the reduction of bureaucratic barriers. A system where a doctor certified in Portugal can have their qualifications instantly verified in Sweden, or where a university degree issued in Estonia is immediately recognised in Italy, is worth building.

But we are responding because the current implementing regulations make choices that concentrate power in ways that concern us. Under the general principle of legal certainty recognised by the Court of Justice, implementing regulations must provide clarity regarding governance responsibilities, cross-border applicability, and user rights. Where these are undefined, enforcement and accountability become inconsistent across Member States.

Certification requirements that effectively restrict trust service provision to a small number of corporations, authentic source verification mechanisms with no accountability for surveillance, and termination provisions that leave citizens vulnerable when providers fail are not incidental details. They are structural choices with consequences for who can participate in the attestation ecosystem and whether that ecosystem serves democratic ends.

We are also responding because this consultation is closely connected to the Digital Identity Wallet consultation. The wallet is the container; attestations are what go in it. Decisions made here about revocation, authentic sources, and trust service provider requirements will shape how the wallet works in practice. These consultations must be read together, and we intend to flag where they create contradictions or gaps.

## **Opportunities and Risks**

The attestation framework has genuine potential. A well-designed system could enable seamless cross-border recognition of qualifications, reduce administrative burden, and give citizens portable credentials they control. Professional mobility, access to services, and recognition of rights could all be improved if the technical architecture is built correctly.

But the value of the system depends entirely on who can participate in it, how verification works, and whether power is distributed or concentrated. The current draft raises significant concerns.

The trust service provider requirements demand secure cryptographic device certification to Common Criteria EAL 4+, EUCC EAL 4+, or FIPS 140-3 Level 3. These certifications cost between €100,000 and €500,000 and take 12 to 24 months to complete. This is a market barrier because, Universities, professional associations, and Member State agencies that could legitimately issue credentials are effectively excluded.

Additionally, the verification mechanism references authentic sources (government databases) but provides no framework for accountability. When a credential is verified, does the authentic source log who requested verification? Can that data be aggregated to profile credential holders? Under what legal basis? The regulation is silent.

Also, the termination requirements for trust service providers are minimal. Providers must notify supervisory bodies one month before changes and three months before cessation. There is no requirement for user migration tools, data portability, or service continuity planning. If a trust service provider goes bankrupt or loses certification, citizens holding credentials issued by that provider are left in legal limbo.

Finally, cross-border disputes lack clear resolution mechanisms. When an authentic source in one Member State refuses to verify a credential for a citizen from another, who adjudicates? The regulation does not say.

These risks are addressable, and the sections that follow set out where we believe revision is needed and recommendations for improvement.

## **1. Privacy and Data Protection**

The privacy risks in the attestation framework are not the same as those in the wallet framework, but they are no less serious. Article 5(1)(b) and (c) GDPR require purpose limitation and data minimisation. Verification mechanisms that permit logging or aggregation of credential checks must therefore be strictly limited to what is necessary for security and fraud prevention purposes. Where the wallet raises concerns about user tracking and platform surveillance, the attestation framework raises concerns about government database surveillance and the aggregation of verification data.

### **1.1 Authentic Source Surveillance**

Annex III specifies that attestations may be verified against authentic sources i.e., the authoritative government databases that hold the underlying data. The regulation describes the technical mechanism (clauses 6.1.1, 6.2.2, and 6.2.3 of ETSI TS 119 478) but provides no framework for what data is collected during verification, how long it is retained, or who can access it. Where authentic sources log verification requests, they process personal data concerning the credential holder and potentially the relying party. Under Article 6 GDPR, such processing requires a clear legal basis. The implementing regulation does not specify this.

When a citizen presents a credential such as a medical qualification, a professional license, or a degree, and a relying party verifies it against an authentic source, does the authentic source log that verification request? If so, that log records who verified the credential, when, and in what context. Aggregated over time, this creates a detailed profile of a citizen's professional activity, service access, and cross-border movement. The Court of Justice has recognised that metadata, taken as a whole, may allow very precise conclusions to be drawn about private life

(Joined Cases C-203/15 and C-698/15, Tele2 Sverige). Verification metadata should therefore be treated as sensitive from a fundamental rights perspective.

The regulation is silent on whether such logging is permitted, under what legal basis, and with what safeguards. To comply with Article 25 GDPR (data protection by design and by default), verification protocols should be designed to minimise or eliminate persistent logging unless explicitly required for security purposes and subject to independent oversight.

## **1.2 Cross-Border Data Flows**

When credentials are verified across borders for example, a German employer verifying a Polish medical degree, the verification request flows from the relying party to the authentic source in Poland. What data protection framework governs this exchange? Under which Member State's law is the data processed? Can Polish authorities access verification logs for German relying parties? Although GDPR provides a harmonised framework, the implementing regulation should clarify which authority exercises supervisory competence under Articles 55 and 56 GDPR in cases of cross-border verification disputes.

Without this clarification, citizens have no clear understanding of what data crosses borders, who controls it, or how they can exercise their rights over it. Legal clarity is particularly important in high-volume automated verification environments, where data processing occurs at scale without human intervention.

## **1.3 Revocation Privacy**

Annex II mandates that attestations use revocation techniques that are “privacy preserving and hindering traceability.” This is positive in principle, but the regulation provides no specificity. Recital 26 GDPR clarifies that anonymisation requires assessment of all means reasonably likely to be used for identification. Revocation lists that are publicly accessible and monitorable must therefore be assessed against realistic adversarial models.

The same status list and identifier list mechanisms described in the wallet consultation apply here, with the same privacy concerns: publicly accessible lists, potential for correlation, and no enforcement mechanism to prevent monitoring.

Revocation of professional credentials is not equivalent to revocation of wallet attestations. A revoked medical license, for example, carries reputational and legal consequences far beyond a technical credential failure. Under Article 41 of the Charter, EU institutions are bound by the right to good administration, including the right to be heard before adverse measures are taken. Where Member States implement Union law, Article 47 of the Charter guarantees the right to an effective remedy and procedural fairness. In the context of professional credential revocation, these safeguards require clear procedural guarantees prior to permanent withdrawal. Revocation mechanisms must therefore provide stronger due process and transparency than the current framework specifies.

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

- Prohibit authentic sources from logging verification requests unless explicitly authorized by the credential holder for a specific purpose.
- Require that verification protocols be designed for unlinkability, preventing authentic sources from correlating verification requests across relying parties.

- Mandate transparent data retention policies for authentic sources, with public disclosure of what data is collected, for how long, and under what legal basis.
- Clarify the legal framework for cross-border verification data flows, including which Member State’s law applies and how citizens can exercise GDPR rights.
- Specify revocation mechanisms in detail, with mandatory due process protections for professional credentials where revocation carries legal or reputational consequences.

## **2. Open Standards and Market Access**

The trust service provider requirements in Annex I will determine who can participate in the European attestation ecosystem. If only a small number of large corporations can afford compliance, the ecosystem will serve corporate interests regardless of what the regulation intends. Market structure is not separate from policy outcomes. Article 102 TFEU prohibits abuse of dominant market positions. While this regulation does not itself create dominance, structural certification barriers may entrench existing qualified trust service providers and reduce competitive entry. Regulatory design should therefore avoid reinforcing concentrated market structures.

### **2.1 Certification Cost as Market Barrier**

REQ-EAASP-7.5.3-02 mandates that secure cryptographic devices used by trust service providers be certified to Common Criteria EAL 4+, EUCC EAL 4+, or FIPS 140-3 Level 3. While high-assurance cryptographic certification enhances security, proportionality requires assessing whether identical requirements are necessary for all attestation categories, including low-risk academic or membership credentials. These certifications are not trivial. Common Criteria EAL 4+ certification typically costs between €100,000 and €500,000 and takes 12 to 24 months to complete. FIPS 140-3 Level 3 carries similar costs.

For a commercial trust service provider like DigiCert or GlobalSign, this is a manageable business expense. For a university issuing degrees, a professional association issuing certifications, or a Member State agency managing social security credentials, it may not be. The result is that credential issuance becomes concentrated in a small number of corporations with the resources to comply, while public interest actors are excluded.

The qualified trust service market is already reportedly dominated by fewer than 10 global providers for high-assurance services. These certification barriers will exclude precisely the diverse, localised issuers that the EU Digital Identity Wallet needs for genuine interoperability and citizen choice.

### **2.2 Who Can Become a Trust Service Provider?**

Beyond certification costs, the regulation imposes additional requirements: personnel with “expert knowledge, experience and qualifications” (REQ-EAASP-7.2-02), quarterly vulnerability scans (REQ-EAASP-7.8-05), and annual penetration testing (REQ-EAASP-7.8-06). Individually, these are reasonable security requirements. Together, they create an operational burden that many organizations cannot sustain.

Can a university IT department meet these requirements? Can a professional association? Can a Member State’s social services agency? The question is not whether these entities have the

technical capacity but whether they have the sustained administrative and financial resources to maintain compliance over time.

If the answer is no, then credential issuance will be outsourced to commercial providers. This creates dependency, not sovereignty.

### **2.3 Standard Accessibility**

Multiple standards referenced in the attestation framework are not freely accessible. ETSI TS 119 471 and ETSI TS 119 478 are available, but portions of the referenced ISO/IEC series are sold commercially. ETSI TS 119 478 is marked as “pending adoption” (V0.0.10), meaning it has not yet been finalized. Referencing unpublished or draft specifications risks violating the principle of legal certainty, which requires that binding obligations be clear and foreseeable (see Case C-17/03, VEMW).

A regulation that mandates compliance with paywalled or unpublished standards excludes civil society, researchers, and smaller developers from meaningful participation. Public infrastructure must be built on public standards.

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

- Introduce tiered certification requirements: lower-cost, faster certification for lower-risk attestations (e.g., non-QEAA), with the current EAL 4+ requirements reserved for high-risk credentials.
- Allow software-based hardware security modules (HSMs) for non-QEAA attestations, reducing dependency on expensive certified hardware.
- Provide EU funding for open-source trust service implementations with public audits, enabling civil society and academic participation.
- Remove all references to unpublished standards. Regulations must reference only finalized, published specifications.
- Require that all standards referenced in eIDAS implementing regulations be freely accessible, with the Commission funding access where necessary.

## **3. Governance, Accountability, and Public Sector Control**

Accountability in the attestation framework requires clarity about who controls authentic sources, what happens when trust service providers fail, and how cross-border disputes are resolved. The current regulation leaves significant gaps.

### **3.1 Authentic Source Power and Accountability**

Authentic sources are the government databases that hold the authoritative data used to verify credentials. The regulation assumes their existence but does not define their governance. To ensure compliance with Article 47 of the Charter (right to an effective remedy), individuals must have access to clear appeals mechanisms where authentic sources deny verification. Which public sector bodies are designated as authentic sources? Under what legal framework? What oversight exists? Can they deny access arbitrarily, and is there an appeals process?

If an authentic source refuses to verify a credential because of a bureaucratic error, a political dispute, or technical incompatibility, the credential holder is left without recourse. Cross-border disputes add another layer of complexity because, if a credential issued in one Member State is not recognized by an authentic source in another, who adjudicates?

This is a governance gap that will create real problems for citizens attempting to use credentials across borders.

### **3.2 Trust Service Provider Termination**

REQ-EAASP-6.3-02 requires trust service providers to notify supervisory bodies one month before implementing changes and three months before ceasing operations. This is inadequate. Three months is not enough time for citizens holding credentials issued by that provider to migrate to another provider, particularly if the credentials are professional qualifications or other high-value attestations. Article 20 GDPR establishes a right to data portability. Termination frameworks should explicitly require structured export formats and migration assistance to ensure continuity of legally significant credentials.

The regulation does not require user migration tools, data portability obligations, or service continuity planning. REQ-EAASP-7.12-04 references implementing acts under Article 24(5) of Regulation (EU) No 910/2014 for termination plans, but those acts are not yet defined. Until those acts are adopted, termination safeguards remain legally indeterminate. The present implementing regulation should include minimum continuity guarantees because in its current form, there is no enforceable framework.

If a trust service provider goes bankrupt or loses certification, what happens to the credentials it issued? Are they immediately invalid? Can they be transferred to another provider? Citizens deserve clarity, and the regulation does not provide it.

### **3.3 Transparency Requirements**

The regulation requires incident reporting (REQ-EAASP-7.9-02) but does not specify what incidents must be disclosed, to whom, or in what timeframe. Public disclosure of security incidents is a best practice in trust services; the regulation should mandate it. Transparency in trust services enhances systemic resilience and aligns with the Union's cybersecurity disclosure principles under Directive (EU) 2022/2555 (NIS2)

Similarly, there is no requirement for a public registry of trust service providers with certification history, status, and contact information. Citizens and relying parties have no standardized way to verify that a provider is legitimate or to check its certification status.

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

- Establish a public, machine-readable registry of authentic sources with governance frameworks, contact information, and dispute resolution mechanisms.
- Create an independent cross-border dispute resolution body to adjudicate conflicts between authentic sources and credential holders.
- Extend the termination notification period to 12 months, with mandatory user migration tools and data portability obligations.

- Require public disclosure of security incidents within 72 hours of discovery, with details published in a standardized format.
- Establish a public registry of trust service providers with real-time certification status, historical compliance records, and incident reports.

### **Conclusion**

The European Pirate Party supports the goal of cross-border credential recognition and the reduction of administrative barriers to professional mobility and service access. A well-designed attestation framework could deliver real benefits to European citizens and strengthen the Single Market.

But the current implementing regulation concentrates power in ways that undermine those goals. Certification barriers that exclude public interest actors, surveillance mechanisms with no accountability, and governance gaps that leave citizens vulnerable when providers fail are not technical details. They are structural choices with consequences for who can participate in the attestation ecosystem and whether that ecosystem serves democratic ends.

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

- Prevent authentic source surveillance through explicit prohibitions on verification logging and requirements for unlinkable verification protocols;
- Reduce certification barriers to enable participation by universities, professional associations, and public sector bodies;
- Ensure all referenced technical standards are finalized, publicly accessible, and free to implement;
- Build transparent governance structures with clear accountability for authentic sources, trust service providers, and cross-border disputes.

The attestation framework will determine who can issue official credentials in Europe and under what conditions. It deserves to be built on foundations that distribute power fairly and earn democratic trust.

**European Pirate Party (PPEU)**

[europeanpirates.eu](http://europeanpirates.eu)

## References

- CFR. (2000). *Charter of Fundamental Rights of the European Union*. Retrieved from [https://www.europarl.europa.eu/charter/pdf/text\\_en.pdf](https://www.europarl.europa.eu/charter/pdf/text_en.pdf)
- CJEU. (2005). *C-17/03 - VEMW and Others*. Retrieved from [https://infocuria.curia.europa.eu/tabs/affair?sort=AFF\\_NUM-DESC&searchTerm=%22C-17%2F03%22&publishedId=C-17%2F03](https://infocuria.curia.europa.eu/tabs/affair?sort=AFF_NUM-DESC&searchTerm=%22C-17%2F03%22&publishedId=C-17%2F03)
- CJEU. (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](https://infocuria.curia.europa.eu/tabs/affair?sort=AFF_NUM-DESC&searchTerm=%22C-203%2F15%22&publishedId=C-203%2F15)
- GDPR. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Retrieved from <https://gdpr-info.eu/>
- Manifesto, E. P. (n.d.). Retrieved from <https://european-pirateparty.eu/manifesto/>
- NIS2. (2022). *Directive (EU) 2022/2555*. Retrieved from <https://eur-lex.europa.eu/eli/dir/2022/2555>
- QEAA. (2025). *Ares(2026)1286389 – Qualified Electronic Attestations of Attributes (QEAA) Technical Specifications (Implementing Regulation (EU) 2025/1569)*. Retrieved from [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PI\\_COM:Ares\(2026\)1286389](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PI_COM:Ares(2026)1286389)
- TFEU. (2008). *Treaty on the Functioning of the European Union*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2008:115:TOC>