ENHANCING THE REGULATORY FRAMEWORK FOR W3C VERIFIABLE CREDENTIALS TO DRIVE INDUSTRY ADOPTION OF THE EUDI WALLET ECOSYSTEM

March 2026
Based on the draft amending Implementing Regulations
Ref. Ares(2026)1286304 – 05/02/2026

1. Introduction

Consorcio Red Alastria (hereinafter **Alastria**) warmly welcomes the opportunity provided by the European Commission to share its views on the **draft implementing acts and amendments to the eIDAS2 Regulation** published in February 2026.

Alastria is one of the largest public-permissioned, multi-sectoral blockchain platforms in the world. It has over 400 members of different sizes and from various sectors, compelling businesses (micro-enterprises, SMEs, and large companies), academia (universities, business schools, training centres, and technology and science research parks) and government. As a neutral meeting point, Alastria facilitates regulatory-aligned innovation and knowledge generation. We are committed to boosting the digital economy by promoting decentralized technologies and ensuring that blockchain development serves as a reliable foundation for trust services and digital sovereignty.

The reflections and recommendations presented in this document were gathered through a series of dedicated technical and legal sessions and working groups. These sessions brought together experts from various industries—including Financial Services, IT, Consulting, and Legal—as well as academic researchers. This collaborative approach ensures that our feedback reflects a holistic view of the challenges and opportunities that the eIDAS 2 framework presents for the European digital ecosystem.

In alignment with the findings of the **Draghi Report on the Future of European Competitiveness**, Alastria views the eIDAS2 framework as a strategic necessity to bridge the innovation gap and revitalize the EU's industrial landscape. We believe that a robust, interoperable, and decentralized digital identity is not merely a regulatory requirement, but a **critical driver for business productivity**. By reducing administrative friction in the Single Market and lowering operational costs for SMEs, eIDAS2 provides the foundation for European enterprises to thrive in an increasingly digital global economy.

Alastria emphasises the vital importance of leveraging the vast knowledge and strategic investments already made by the European Union through Large-Scale Projects (LSPs) and various funding initiatives. It is essential that the deployment of eIDAS 2 serves as the definitive mechanism to effectively transfer this technical expertise and innovation from pilot environments into real-world business practice. By integrating these proven advancements with the necessary legal and technical guarantees, Europe can ensure that public investment translates into tangible market solutions. This approach allows companies to adopt these technologies with confidence, transforming them into a sustainable global competitive advantage.

2. Regulatory Context

The draft amending Implementing Regulations published on 5 February 2026 has a direct impact on the EUDI Wallet adoption. This contribution aims at maximizing the EUDI wallet adoption by proposing changes to the regulation than will foster the acceptance and adoption of the EUDI wallet maximizing the number of use cases available for the public in the public and private areas. The draft amending Implementing Regulations published on 5 February 2026 replace the direct reference to W3C VCDM 1.1 in Implementing Regulation (EU) 2024/2979 with a reference to clauses 4, 5, 6 and 7 of ETSI TS 119 472-1 V1.1.1 (2025-12). Clause 5 covers SD-JWT VC, clause 6 covers ISO/IEC mdoc, and clause 7 covers JSON-LD W3C-VC based on VCDM v2.0. As a matter of regulatory text, W3C Verifiable Credentials have not been eliminated from the normative perimeter — the reference to clause 7 of ETSI TS 119 472-1 explicitly covers JSON-LD W3C-VC based on VCDM v2.0. The format has been absorbed into the ETSI reference layer, and indeed, upgraded from v1.1 to v2.0.

However, a systematic examination of the amending regulations reveals that whilst W3C-VC is formally referenced, it has not been given the regulatory scaffolding necessary to function within the EUDI Wallet ecosystem — that is, the ensemble of encoding tables, normative reference pins, revocation rules, schema options, presentation profiles and issuance protocol specifications that the Commission has defined for mdoc and SD-JWT VC (see section 7 for a detailed typology).

A systematic examination of the amending regulations has been contributed by Lluís Ariño[1], Alastria fully supports the detailed analysis and suggestions. This contribution focuses on the impact of not following such suggestions from an economic and social point of view.

3. Impact on industry and public investment

The Commission itself has already developed, funded and piloted W3C-VC based credentials at European scale through the EBSI infrastructure and the DC4EU Large Scale Pilot. Those projects are probably the best-known identity projects using W·C.VC based credentials, but they are not the only ones. There is a large number of initiatives and projects following the same approach and contributing to an already developed ecosystem in the public and private areas.

Those projects, in most cases partially funded by European and national programs, involving public and private partners, would suffer an important impact should the above-mentioned suggestions not followed. As a minimum the private and public investment would be lost, and the deployment of developed use cases would be delayed and reduced in capability.

As an alternative those projects will continue their development based on current W3C-VC producing a two-path evolution, qualified VC based on fully regulation supported VC and non-qualified VC with richer features, private supported project that will require cross European coordination effort and will obscure and delay EUDI wallet adoption.

[1] Ariño, L. (2026, February). Feedback on the *European Digital Identity Wallet – standards and technical specifications (update)* [Public comment]. European Commission. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16112-European-Digital-Identity-Wallet-standards-and-technical-specifications-update-/F33373595_en

Moreover, this situation could give an advantage to non-European identity initiatives that will provide a more complete and easier to understand identity proposal to European citizens impacting European technical sovereignty.

Estimated scale of exposure. The projects documented in Section 4 represent, in aggregate, European public funding exceeding €80 million (DC4EU, EBSI VECTOR, DALION/CAD, ISBE Next Generation EU funds), direct involvement of more than 200 organisations across more than 20 European countries, and a potential user base of over 30 million citizens and corporate clients. This is not a niche concern—it is the current W3C-VC ecosystem.

4. Industry use cases and projects

Several identity projects using W3C-VC are presented and the impact of lacking a full regulatory support analysed.

4.1 ISBE — Infraestructura de Servicios Blockchain de España

ISBE (Infraestructura de Servicios Blockchain de España) is Spain's first national public-permissioned blockchain network, promoted by the Community of Madrid, executed by Alastria — with direct participation of over 27 companies and 150 professionals — and financed through the Programme of Territorial Networks of Technological Specialisation under the Recovery, Transformation and Resilience Plan of the European Union (Next Generation EU). Built on Hyperledger Besu with QBFT consensus, ISBE is designed as compliance-by-design infrastructure, natively covering eIDAS 2, GDPR, MiCA, DORA and NIS2, and is positioned to become Europe's first Qualified Distributed Ledger (qDLT) under EU Implementing Regulation 2025/2531.

ISBE's digital identity architecture — developed by its Identity Digital Group, coordinated by Izertis — is built natively on W3C Verifiable Credentials (VCDM v2.0) and Decentralised Identifiers (DIDs). The credential catalogue covers corporate identity (legal entity identification, representation mandates and powers of attorney for the European Business Wallet), sector-specific attestations (sustainability certificates, professional qualifications), and public administration interactions. The dual-network architecture — a Bare Network (P-256/secp256r1, HSM-protected validator nodes) for the qualified electronic ledger function, and a Main Network (secp256k1, full EVM compatibility) for smart contracts and tokenisation — is designed precisely to accommodate the qualified trust services layer that eIDAS 2 requires. All W3C-VC credential specifications developed for ISBE are aligned with EBSI and designed for interoperability with the EUDI Wallet ecosystem.

> *Regulatory impact:* ISBE's entire credential architecture is built on W3C-VCDM. Without full regulatory scaffolding for W3C-VC in the EUDI Wallet — PID encoding tables, Bitstring Status List revocation (the only mechanism supporting both revocation and suspension as required by several Member States' legislation), schema validation via SHACL, and presentation profiles in HAIP — ISBE's credentials cannot achieve qualified status within the European framework regardless of the technical maturity of the infrastructure.
>
> The qDLT positioning of ISBE is contingent on regulatory completeness: a qualified electronic ledger whose native credential format is not fully supported within the EUDI Wallet ecosystem creates a structural contradiction at the heart of Europe's regulated digital identity architecture. The Next Generation EU investment in ISBE would be

architecturally disconnected from the European qualified identity ecosystem it was designed to anchor.

4.2 DC4EU — Digital Credentials for Europe

DC4EU was a Large-Scale Pilot funded under the Digital Europe Programme with a budget of €19 million, led by the Spanish Ministry of Economic Affairs and Digital Transformation, and bringing together more than 80 organisations from 23 European countries. Its objective was to validate the use of interoperable verifiable credentials for education, professional qualifications and related public services.

Work Package 5, dedicated to education and professional qualifications, developed a complete sectoral catalogue of Electronic Attestations of Attributes for lifelong learning, including the European Higher Education Diploma (EUHED), Diploma Supplement (EUHEDS), Transcript of Records (EUHETOR), Proof of Enrolment (EUHEPOE), Microcredential (EUHEMC) and Vocational Education and Training credentials. These pilots were executed with W3C Verifiable Credentials across 36 institutional scenarios in 10 European countries, validating three distinct trust architectures.

The European Learning Model (ELM)—the Commission's JSON-LD ontology underpinning Europass—was designed natively for W3C-VC. Without full regulatory support for W3C-VC in the Wallet, the ELM loses its deployment pathway and the promise of automatic cross-border credential recognition, the very capability that Spain invested in through DC4EU, is substantially diminished.

> *Regulatory impact:* DC4EU represents €19 millions of EU public investment specifically in W3C-VC-based educational credentials. A regulatory framework that leaves W3C-VC without operational scaffolding converts this investment into a pilot with no qualified deployment path. The 36 institutional scenarios validated across 10 countries cannot be deployed as QEAAs within the EUDI Wallet under the current draft Implementing Acts.

4.3 EBSI-VECTOR — Verifiable credentials and trusted registries for education, social security and business identity

EBSI-VECTOR (EBSI-enabled Verifiable Credentials and Trusted Organisations Registries), co-funded by the European Union under the Digital Europe Programme (Grant Agreement no. 101102512), ran from June 2023 to May 2025 and brought together 52 partners from 20 countries. The project's overarching objective was to move EBSI beyond the proof-of-concept stage and demonstrate production-ready deployment of verifiable credentials and trusted registries across three cross-border domains: education (student IDs, transcripts of records, learning outcomes, Erasmus+ participation, digital diploma issuance), social security (the European Health Insurance Card — EHIC — and the Portable Document A1 for posted workers), and business registries (verifiable identity of legal persons, powers of attorney, cross-border company verification).

The project consolidated existing EBSI capabilities on verifiable credentials and trusted registries, extending them with new functionality including decentralised identity of legal persons and revocation — all built on W3C-VC as the core credential format. Izertis led the project coordination and served as the host organisation, with its team centrally involved in the most technically complex deliverable of the initiative: designing and implementing the interoperability framework that enabled wallets and connectors developed independently by different organisations across different countries to communicate with each other. This meant establishing a common technical baseline across implementations built with different

assumptions, tooling stacks and national integration contexts. The result was the successful alignment of 16 wallet connectors and holder implementations — a significant achievement in a consortium of this scale and diversity, and a direct demonstration that W3C-VC can serve as the foundation for genuine multi-party, multi-country interoperability. Izertis also built the open-source reference implementation of the Enterprise Wallet, enabling organisations — as opposed to individual citizens — to manage, issue and verify verifiable credentials within the EBSI ecosystem. At the Final Event, Izertis presented the education use cases and co-presented the combined education and social security interoperability scenario, which demonstrated a Slovenian Erasmus student enrolling at a German university using educational and health credentials from different countries, confirmed to be interoperable across three distinct wallet implementations.

EBSI-VECTOR is the largest W3C-VC initiative referenced in this contribution: 52 organisations, 20 countries, public administrations, ministries, universities, social security bodies and standardisation organisations, all building on W3C-VC as the Commission-endorsed format for cross-border credentials. The interoperability work performed by Izertis — aligning 16 heterogeneous wallet implementations into a functioning cross-border system, spanning education and social security in production-ready scenarios — represents precisely the kind of structural technical investment that a coherent regulatory framework is supposed to protect.

> *Regulatory impact:* Without full regulatory scaffolding for W3C-VC in the EUDI Wallet, the interoperability results delivered by EBSI-VECTOR cannot be carried forward into the qualified European credential ecosystem: the 52-partner infrastructure built on this standard would be stranded outside the qualified framework that the Commission's own Digital Europe Programme funded it to prepare for.

4.4 DALION (Inetum – CAD): pioneer B2B and academic identity

The DALION project, launched in 2019 within the Alastria consortium, stands as one of the earliest large-scale European initiatives to implement a digital identity model fully aligned with the principles that the European Union would later consolidate under eIDAS 2.0. From its inception, DALION adopted the AlastriaID model, leveraging blockchain technology and data models and exchange formats based on the W3C Verifiable Credentials standard (W3C-VC) using JWT. This strategic choice positioned DALION years ahead of the regulatory curve.

The consortium brings together major Spanish companies with strong European reach: five large banks (Santander, BBVA, CaixaBank, Banca March and Unicaja), three major insurance companies (Mapfre, Generali and Línea Directa), an energy company (Repsol) and a leading public university (the Polytechnic University of Madrid). Collectively, these entities represent a potential user base of more than 18 million citizens.

As the project evolved, DALION expanded into the educational domain through the CAD (Digital Academic Credentials) pilot, fully aligned and interoperable with W3C-VC and European initiatives, namely EBSI, and financed with European funds via the UniDigital programme of the Spanish Ministry of Education and coordinated by the Polytechnic University of Madrid alongside ten other major universities. This extension opens the door for more than 10 million students and academic staff to benefit from verifiable credentials designed to be interoperable across Europe and compatible with EBSI.

From an economic perspective, DALION has received European funding support amounting to more than €0.7 million for the educational extension, and more recently nearly €1.8 million

through Recovery, Transformation and Resilience Funds to advance the project to TRL 7 for large-scale production.

Inetum, as the primary technology partner coordinating the CAD extension, has invested significant development effort in W3C-VC aligned credential architectures for the Spanish higher education ecosystem. This work represents both a technology investment and a commitment to European interoperability standards built on the W3C foundation.

> *Regulatory impact:* DALION/CAD represents over €2.5 millions of combined public investment in a W3C-VC-based identity and credential infrastructure involving major Spanish financial institutions, a large energy company, and eleven universities. Without qualified status for W3C-VC credentials within the EUDI Wallet framework, the 18 million citizens in the DALION user base and the 10 million students in the CAD ecosystem cannot benefit from the cross-border interoperability that the eIDAS 2.0 framework promises. The project has continuously adapted its architecture to remain aligned with the European digital identity landscape—a strategic approach that the current regulatory gap now penalises rather than rewards.

4.5 Telefónica – Izertis: anti-fraud credentials in supplier communications

Supplier impersonation fraud has become one of the most financially damaging threats in global supply chains, especially when attackers manipulate weakly authenticated communication channels to request fraudulent changes in bank account details. Criminals exploit vulnerabilities in email and supplier portals to redirect legitimate payments into accounts they control, often as part of sophisticated Business Email Compromise (BEC) schemes. The scale of the problem is staggering: BEC attacks caused $2.77 billion in losses, making them the second most costly fraud category worldwide, with 21,442 reported incidents, a volume that has remained persistently high year after year. This underscores the urgent need for stronger, verifiable mechanisms to authenticate supplier communications and protect payment processes from manipulation.

This use case, that will be launched in 2026, focuses on preventing fraud in supplier communications, in particular fraudulent instructions to change bank account details used for payments. In many supply chains, fraudsters exploit weakly authenticated communication channels—such as email or poorly secured portals—to impersonate suppliers and request changes to the bank accounts where invoices are to be paid. This type of attack, often related to business email compromise, leads to substantial financial losses when payments are redirected to accounts controlled by criminals.

The proposed solution uses verifiable credentials combining corporate representation and verified banking attributes, built on the W3C Verifiable Credentials standard. The core idea is that the supplier's legitimate representative holds, in a digital identity wallet, a credential attesting both that the person is authorised to act on behalf of a specific legal entity, and that certain bank account details are associated with that entity and have been verified. Whenever a supplier communicates about bank account details, the communication is accompanied by the presentation of this credential.

This use case illustrates how organisational Electronic Attestations of Attributes—including representation mandates and verified bank account data—can be used in routine supplier communications to create a more trustworthy and tamper-resistant channel for sensitive instructions. It is a concrete B2B example of the value proposition of the EUDI Wallet ecosystem beyond citizen identification.

Regulatory impact: The credential architecture for this use case—combining legal entity representation mandates with verified financial attributes—requires a format capable of carrying rich, linked semantic information about the organisational context. W3C-VCDM's JSON-LD serialisation is the only format among the three that natively supports this semantic depth. A regulatory framework that leaves W3C-VC without qualified status effectively precludes the development of this class of organisational EAA at qualified assurance level, limiting the anti-fraud capabilities that the EUDI Wallet ecosystem could otherwise provide.

4.6 SAFE ISLAND (Izertis) — Verifiable health credentials for tourism management

The Safe Island project, promoted by the Punta Cana Foundation in the Dominican Republic, addressed a concrete operational challenge: managing the secure entry of tourists into a destination through digital verification of health status — vaccination certificates and laboratory test results — without creating a centralised repository of sensitive personal health data. The solution required trustworthiness sufficient for health authorities, frictionless operation for travelers, and privacy compliance for applicable data protection requirements across multiple national jurisdictions. Izertis designed and implemented the core system: a W3C-VC issuance and verification infrastructure built on a decentralised identity model based on LACChain and Alastria, with cryptographic mechanisms for selective disclosure and anonymisation of sensitive traveler data, enabling verification of health status without exposing underlying personal information.

Safe Island is not a pilot. It is a production deployment, operating in a live environment managing real travelers and issuing credentials with legal significance for health border control. It validates W3C-VC as an operational format chosen for a production identity system in an international context — and it does so with a European company as the technology provider, using European-originated open standards.

Regulatory impact: Qualified status for W3C-VC within the EUDI Wallet framework would reinforce the competitive positioning of European technology exporters in precisely these markets; the regulatory ambiguity created by the current draft Implementing Acts signals institutional uncertainty about the standard on which those exporters are building.

4.7 PH4H (Izertis) — Verifiable health credentials for international interoperability

The secure and interoperable exchange of health information across national borders is a challenge that extends well beyond Europe. Citizens travelling internationally, healthcare professionals working across systems, and public health authorities managing cross-border events all depend on health documents — vaccination records, clinical summaries, laboratory test results — that can be trusted and digitally verified without requiring bilateral agreements between every pair of countries. The Pan-American Highway for Digital Health (PH4H) Connectathon 2025, organised by the Inter-American Development Bank (IDB) and the Pan American Health Organization (PAHO), brought together Ministries of Health from 17 countries to validate exactly this: cross-border continuity of care through international clinical summaries and interoperability of digital vaccination certificates. During the 2025 edition, more than 700 technical cross-border tests were executed between national systems. The credential architecture was built on W3C-VC.

Izertis participated as a core technological contributor, responsible for defining and validating the digital identity and verifiable credential architectures applied to the healthcare domain. This

included designing the mechanisms through which health certificates issued in one country's national system could be cryptographically verified in another's, without a centralised authority, using decentralised W3C-VC trust models.

The significance of PH4H for this contribution lies not only in its technical content but in its geography. It demonstrates W3C-VC adoption driven by European technical leadership in a non-European, intergovernmental context — 17 countries in Latin America and the Caribbean selecting this format precisely because of its interoperability properties and alignment with standards promoted by European institutions.

> *Regulatory impact:* A European regulatory framework that marginalises W3C-VC within the EUDI Wallet would directly damage the credibility and international competitiveness of European digital identity standards in the corridors where European companies are currently winning on the strength of those standards.

4.8 Sybol — Repsol: verifiable credentials for industrial B2B processes

Sybol is a European enterprise platform designed to improve the efficiency, security, and traceability of business processes that require the exchange and verification of organisational information between companies. The platform focuses particularly on scenarios where multiple organisations must share verified data in a reliable and automated way while preserving privacy and reducing administrative overhead.

The system leverages data models and exchange formats based on the W3C Verifiable Credentials (W3C-VC) standard, allowing organisations to issue, exchange, and verify digital attestations about operational attributes such as corporate representation, regulatory compliance, supplier qualifications, and other enterprise-level credentials.

Unlike many digital identity solutions primarily oriented toward citizen authentication, the Sybol platform targets business-to-business (B2B) interactions, where the absence of structured and verifiable data exchange mechanisms often results in significant operational friction. In many industries, organisations must repeatedly provide documentation to demonstrate compliance, authorization, or operational status. These processes typically rely on manual document exchange—PDF certificates, scanned documents, or emails—which introduces inefficiencies, delays, and opportunities for fraud.

The Sybol architecture addresses these challenges by enabling organisations to issue and manage Organisational Electronic Attestations of Attributes (EAA) in the form of verifiable credentials. These credentials may include, for example:

- proof of corporate representation
- supplier qualification or certification
- verified banking information
- regulatory compliance statements
- operational authorisations within supply chains

Through the use of W3C Verifiable Credentials, these attestations become machine-verifiable digital objects, allowing automated systems to validate their authenticity, issuer trust status, and semantic meaning without manual intervention.

A representative use case currently explored involves the automation of supplier communication and verification processes within large industrial organisations, including collaborations with companies such as Repsol. In complex industrial supply chains,

organisations interact with hundreds or thousands of suppliers across multiple jurisdictions. Routine administrative processes, such as onboarding suppliers, validating corporate documentation, or verifying operational credentials, often involve repeated manual checks of documents issued by third parties.

By representing these attributes as verifiable credentials issued by trusted authorities, Sybol enables organisations to verify supplier information automatically and continuously. This significantly reduces administrative costs, accelerates operational workflows, and improves fraud resilience by eliminating reliance on easily manipulated document formats.

From a technical perspective, the adoption of W3C-VC provides several advantages that are particularly relevant in enterprise contexts:

- semantic interoperability through linked data models, enabling machine interpretation of credential meaning across organisations
- portability across systems and jurisdictions without reliance on proprietary platforms
- compatibility with emerging European trust frameworks such as the EUDI Wallet ecosystem
- privacy-preserving verification mechanisms allowing selective disclosure of attributes

These characteristics are essential for enabling complex multi-party business ecosystems to exchange trusted data at scale. However, the absence of complete regulatory support for W3C-VC within the EUDI Wallet ecosystem have a direct impact on initiatives such as Sybol. Enterprise platforms that rely on semantically rich credentials would face increased uncertainty regarding interoperability with the regulated European identity infrastructure.

> *Regulatory impact:* The lack of harmonised regulatory specifications for W3C-VC issuance, presentation protocols, and credential lifecycle management could create fragmentation across Member States. Organisations deploying enterprise credential infrastructures may therefore need to maintain parallel mechanisms for interacting with the EUDI Wallet ecosystem, increasing complexity and potentially slowing adoption.
>
> At the same time, projects such as Sybol illustrate the economic and operational value of verifiable credentials beyond purely identity-centric use cases. While identity credentials enable citizens to authenticate themselves online, enterprise credentials enable organisations to automate trust processes that underpin the functioning of the digital single market.
>
> Supporting W3C-VC within the regulatory framework would therefore not only preserve the investments already made in European pilot projects but would also unlock a new generation of enterprise-level use cases capable of significantly reducing administrative friction across the European economy.

5. Cross-European convergence

The projects documented in Section 4 do not represent isolated Spanish choices. They reflect a convergence of technical judgment across European industrial ecosystems that has emerged independently and consistently. The WE BUILD consortium (European Business Wallet initiative, 41 partners), in its open architecture discussion process, has reached a parallel conclusion: W3C-VCDM with JSON-LD is the necessary credential format for B2B, industrial and machine-to-machine use cases because it is the only format that provides the linked data semantics,

credential chaining capabilities and graph-based reasoning that industrial credential flows require.

The same convergence is visible in Catena-X (European automotive data ecosystem, Digital Europe Programme), which uses W3C Verifiable Credentials for supply chain attestations; in Gaia-X, which incorporates verifiable credentials in its trust framework; and in the UN Transparency Protocol (UNTP), which mandates W3C-VCDM v2.0 for Digital Product Passports globally. These ecosystems have independently evaluated credential format options and converged on W3C-VCDM for industrial use cases.

The European Parliament resolution of 22 January 2026 on European technological sovereignty and digital infrastructure (P10_TA(2026)0022), adopted two weeks before the publication of the draft amending regulations, calls explicitly for digital public infrastructure to be "built on common and open standards", embracing "interoperability and interconnectedness", preventing "user and vendor lock-ins", and explicitly identifies the EU digital identity as an example of such infrastructure. The regulatory marginalisation of W3C-VC—the format whose governance most closely aligns with these principles—is in direct tension with this parliamentary mandate.

6. Conclusions and recommendations

Alastria submits this contribution to make a single, concrete point: the absence of regulatory scaffolding for W3C Verifiable Credentials in the EUDI Wallet ecosystem is not a technical abstraction. It is a decision with measurable consequences for Spanish and European companies, institutions and citizens that have invested in this standard on the basis of legitimate regulatory expectations.

The projects documented in this contribution share a common profile: they were built on W3C-VC because it is the standard best suited to their use case requirements; they were in many cases co-funded by European or national public programmes; and they are now in production or near-production, ready for qualified deployment within the EUDI Wallet ecosystem. The regulatory gap means they cannot achieve that qualified status under the current draft Implementing Acts, regardless of their technical maturity.

The Commission is not being asked to create something new. It is being asked not to discard what has already been built, funded and validated—with €19 million in DC4EU alone, plus the ISBE Next Generation EU investment, plus the DALION/CAD public funds, plus the production deployments already operating at industrial scale.

Alastria endorses the eight regulatory actions identified in the above referenced technical analysis: (1) PID encoding tables for W3C-VCDM v2.0; (2) pinning of W3C Recommendations of 15 May 2025 as normative references; (3) Bitstring Status List for W3C-VC QEAA/PuB-EAA supporting both revocation and suspension; (4) SHACL as preferred schema mechanism; (5) mandatory credentialStatus and short-lived credential exemption for W3C-VC; (6) bindings for credentialStatus with Bitstring Status List; (7) format identifier for embedded proofs in HAIP; and (8) W3C-VC format identifier in OID4VCI Credential Issuer Metadata.

Should the Commission prefer not to incorporate all these specific technical adaptations directly into this amendment cycle, the appropriate path is to issue a standardisation request to ETSI ESI to incorporate these adaptations into clause 7 of future versions of ETSI TS 119 472-1, without pinning normative references to versions that would architecturally preclude W3C-VC

support. This would respect the institutional role of the European standardisation body, ensure open expert consensus with Member State participation, and create a self-updating mechanism consistent with the Commission's existing approach to technical regulation.

What the Commission must avoid is any action that forecloses this path. Failing to act—leaving W3C-VC formally within the normative perimeter but excluded from PID issuance and without the harmonised profiles necessary for cross-border interoperability—**creates unjustified barriers to the single market**, strands legitimate investments, and contradicts both the Commission's own digital sovereignty objectives and the European Parliament's resolution of 22 January 2026.

The technology is proven. The investment has been made. The standards have been published. What remains is the political decision to complete the regulatory framework that European industry has built on.

Alastria remains available to contribute constructively to this work and looks forward to further dialogue. We can be reached at presidencia@alastria.io

Madrid, March 2026