



ESD POSITION PAPER

ESD Contribution to the Article 49 Review of eIDAS

Proposals for Targeted Amendments to Regulation (EU) No 910/2014

EUROPEAN SIGNATURE DIALOGUE

Hackhofergasse 5/16, A-1190 Vienna, Austria · Tel. +43 676 940 9309

office@european-signature-dialog.eu · ZVR-Nr. 579746942

European Transparency Register No. [994150833943-81](#)

CONTENTS

A. Purpose and Executive Summary	3
B. Overall Rationale for the Proposed Amendments	5
1. Legal certainty and the allocation of obligations	5
2. Provisions lacking the necessary infrastructure	5
3. A single-audit principle across EU frameworks	6
4. Effectiveness of EU-qualified status	6
5. Targeted amendments strengthen the framework	7
C. Proposed Amendments to the eIDAS Regulation	8
Suggestion 1 – Free-of-Charge Qualified Electronic Signatures	8
Suggestion 2 – Certification of Notified Identification Schemes	10
Suggestion 3 – Relationship with the Cyber Resilience Act	12
Suggestion 4 – Modular Compliance for Digital Identity Wallets	15
Suggestion 5 – Effective Recognition of QWACs	17
Suggestion 6 – Continuity of Signature and Seal Device Certification	21
Suggestion 7 – Interoperability of Attestations of Attributes	24
Suggestion 8 – Alignment of PubEAA and QEAA Requirements	25
D. Issues Concerning Implementing Acts, Standards and Supervisory Practice	27
E. About the European Signature Dialogue	30

A. Purpose and Executive Summary

Purpose of This Document

This working document sets out concrete proposals from the European Signature Dialogue (ESD)¹, the leading European platform for trust service providers, for targeted amendments to the eIDAS framework (Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183). The proposals are submitted in the context of the review provided for under Article 49 of the Regulation and are intended to contribute to the Commission's assessment of whether modifications to the Regulation or its specific provisions are appropriate.

Executive Summary

In the context of the review provided for under Article 49 of Regulation (EU) No 910/2014, ESD has identified a limited number of provisions of the eIDAS framework that, based on the operational experience of the qualified trust service providers and technology suppliers represented by ESD, warrant targeted amendment. These concern provisions whose current formulation has given rise to legal uncertainty, has proved incapable of effective application in the absence of the institutional or technical infrastructure it presupposes, or has produced effects at variance with the objectives pursued by the EU legislator.

The proposals build on the overall objectives and policy direction of Regulation (EU) 2024/1183 and seek to ensure their effective, coherent and proportionate implementation. They do not seek to reopen the overall policy choices underlying the revised eIDAS framework, but to address specific legal and practical obstacles identified in its implementation.

The paper addresses the following eight matters, which are summarised below and further developed in Section C ("Proposed Amendments to the eIDAS Regulation"), together with the corresponding proposals for amendment.

- (1) The first concerns the scope and the addressee of the obligation to make qualified electronic signatures available free of charge under Article 5a(5)(g), where the addressees of the obligation, the arrangements by which the service is to be financed, the delimitation of non-professional purposes and the technical means of applying that delimitation all remain unresolved.
- (2) The second concerns the certification of notified electronic identification schemes under Article 12a, which cannot presently be operated because neither the designated conformity assessment bodies nor a European cybersecurity certification scheme suited to services of that nature exists.
- (3) The third concerns the relationship between the eIDAS framework and Regulation (EU) 2024/2847, where the absence of any coordinating provision exposes the components of qualified trust services to a second, parallel conformity assessment regime.

¹ A more detailed description of the European Signature Dialogue (ESD) is provided at the end of this document.

- (4) The fourth concerns the certification of European Digital Identity Wallets under Article 5c, which does not require the recognition and reuse of valid assessment evidence already produced under the eIDAS framework in respect of the same components. This point is also applicable to electronic identification scheme, under Article 7.
- (5) The fifth concerns the effectiveness of the recognition obligation for qualified certificates for website authentication under Articles 45 and 45a, and the autonomy of the EU framework from technical governance exercised by private undertakings.
- (6) The sixth concerns the continuity of the certification of qualified electronic signature and seal creation devices, and more generally, of trustworthy systems that TSM must implement to provide trusted services, which is the necessary counterpart of the coordination with Regulation (EU) 2024/2847 addressed by the third matter.
- (7) The seventh concerns the interoperability of electronic attestations of attributes under Article 45d. Common syntactic formats alone do not ensure interoperability where identical attributes and values may be encoded differently by different providers. Common rules for the standardised encoding of attribute names and values are therefore needed to ensure consistent processing across attestation providers, wallets and relying parties.
- (8) The eighth concerns the different assurance and supervisory regimes applicable to qualified electronic attestations of attributes (QEAA) and attestations issued by or on behalf of public sector bodies responsible for authentic sources (PubEAA). Despite their comparable legal effect, PubEAA are not subject to the same recurring conformity assessment and supervisory requirements as QEAA. For attributes carrying elevated reliance risks, a higher and more closely aligned level of assurance should therefore be considered.

In addition to the eight proposed amendments to the eIDAS Regulation outlined above, ESD has identified a number of further issues concerning the implementing acts adopted under the Regulation, as well as related reference standards and supervisory practice.

These are addressed separately in Section D below. While they do not necessarily require amendments to the Regulation itself, they may affect the clarity, coherence and practical implementation of the eIDAS framework and are therefore submitted for consideration as part of the broader Article 49 review.

The matters identified in this document may accordingly require intervention at different levels of the eIDAS framework. The eight proposals set out in Section C concern targeted amendments to the Regulation itself, while the matters addressed in Section D may be more appropriately resolved through implementing acts, reference standards or supervisory practice. Together, they are intended to support the effective, coherent and proportionate application of the eIDAS framework.

B. Overall Rationale for the Proposed Amendments

Legal certainty requires clear allocation of obligations and means of implementation

The amendments introduced by Regulation (EU) 2024/1183 rest upon a distribution of responsibility among Member States, providers of European Digital Identity Wallets, qualified trust service providers and relying parties. Where that distribution is not expressed with the precision that the subject matter requires, the provision concerned does not merely lose clarity, rather it ceases to be capable of uniform application.

Article 5a(5)(g) illustrates the point. The obligation is attributed to the European Digital Identity Wallet - a technical instrument which cannot itself be the bearer of legal duties, with the consequence that the legal subjects upon whom the duty falls are not identified.

Divergent readings have followed at national level, and the arrangements by which the provision of free-of-charge signing is to be financed are addressed neither by the Regulation nor, in consequence of its silence, by any obligation resting upon the Member States.

The duty being one which the Member States are to discharge through the providers of the wallets they make available, it should be accompanied by a corresponding duty for the Member States to ensure that a proportionate and non-discriminatory financing or compensation arrangement is in place, the design of that arrangement remaining a matter for national frameworks.

The same imprecision affects the limitation which the second subparagraph permits, since the notion of non-professional purposes is neither defined nor made the object of any delimitation obligation. Clarity on these points is a condition of legal certainty for supervised undertakings, of the preservation of a level playing field between public and private wallet solutions, and of the coherent operation of the internal market in trust services.

Provisions cannot be effective where the infrastructure required for their application does not exist

A second and distinct difficulty arises where the Regulation confers a right or imposes a requirement whose exercise depends upon institutional or technical arrangements that do not exist and whose creation the Regulation does not secure.

Article 12a is the clearest instance: certification of notified electronic identification schemes is made conditional upon conformity assessment bodies designated by Member States, none of which has been designated or communicated at EU level, and upon a cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881, no such scheme covering electronic identification schemes having been adopted or being known to be in preparation.

The single scheme adopted to date is product-oriented and presupposes a delimited target of evaluation, a construct which cannot meaningfully be applied to an electronic identification scheme. The provision is inoperative, and the incentive which the EU legislator attached to it in the form of exemption from peer review is unavailable.

The limitation to non-professional purposes under Article 5a(5)(g) exhibits the same structure in a different field: its application presupposes knowledge of the purpose for which a signature is requested, which is apparent neither to the wallet provider nor to the qualified trust service provider and can be established only by reference to the relying party, yet no standardized means by which that information might be conveyed within the wallet ecosystem has been provided for. Where a provision cannot be applied, the objective which it pursues is not attained.

A single-audit principle to prevent duplicative conformity assessments across EU frameworks

Qualified trust services are subject to what is, by design, the most strict and demanding assurance regime within the EU digital market: recurring conformity assessments by accredited bodies under Article 20(1), covering both the requirements of the Regulation and the cybersecurity risk-management requirements of Article 21 of Directive (EU) 2022/2555, conducted on the basis of harmonized European standards and commonly supplemented by certification against ISO/IEC 27001.

That regime is now being overlaid by further horizontal and sectoral requirements addressed to the same subject matter. Regulation (EU) 2024/2847 stands to capture, as ordinary products with digital elements, the very software components with which qualified trust services are provided, the eIDAS Regulation containing no provision governing the relationship between the two instruments and thus offering no anchor for the coordination mechanism which Article 2(5) of that Regulation itself makes available.

Within the eIDAS framework, the certification of European Digital Identity Wallets under Article 5c treats the wallet as a monolithic object of assessment, although a wallet solution is in substance composed of elements - a substantial part of which has already been certified or audited under the same Regulation - and neither Article 5c nor the acts adopted thereunder require that such evidence be recognized and reused. The result in both cases is the repeated assessment of the same components against the same or lesser requirements, by different bodies and under different procedures, accompanied by parallel and potentially inconsistent reporting lines. No gain in security is obtained in such manner.

The burden falls with particular weight upon those undertakings that are already subject to the most demanding regime and operates as a structural disincentive to the participation of qualified trust service providers in the wallet ecosystem, at the very moment when their participation is most needed.

The appropriate response should be guided by a **single-audit and mutual-recognition principle**. Where compliance with a requirement has already been demonstrated through an accredited conformity assessment under eIDAS or another Union framework providing an equivalent or higher level of assurance, that assessment and the resulting evidence should be recognised and reused across overlapping regulatory regimes.

Presumption of conformity, modular assessment of composite solutions and the mandatory reuse of valid accredited evidence should also be applied systematically to prevent repeated assessment of the same requirements.

Where eIDAS already provides a comprehensive sector-specific framework achieving an equivalent or higher level of protection, duplicative horizontal requirements should, where appropriate, be limited or excluded altogether.

The objective should be that one substantive requirement is assessed once and that the resulting accredited evidence is recognised across the relevant Union frameworks, without any reduction in the level of assurance.

The effectiveness of EU-qualified status must not depend on discretionary recognition by private technical actors

Articles 45 and 45a embody a deliberate legislative choice, namely that qualified status conferred under EU law and attested by the trusted lists referred to in Article 22 is to be the condition of recognition, in place of the unilateral determinations of private undertakings. That choice is at present being displaced at the level of the technical standards through which compliance is evaluated.

Because Article 45(1) provides that the evaluation of compliance is to be carried out in accordance with the referenced standards, rather than establishing a presumption of compliance as is done for the other qualified trust services, those standards constitute the exclusive route to compliance; and said standards incorporate, for certificates used in the browser context, requirements adopted within a private forum and the additional conditions of the browser root store programmes.

The effective use of a qualified certificate for website authentication thus **remains conditional upon individual decisions of private undertakings, taken without procedural safeguards, without any duty to state reasons and without any avenue of objection or review.**

The same dependency now extends beyond the browser environment: certificates relied upon for the mutual authentication of supervised institutions in closed, machine-to-machine ecosystems under the EU payments framework are exposed to validity-period requirements conceived for the open web, whose application would multiply renewal operations across EU payment infrastructures without corresponding security benefit. The existence and the conditions of that category of certificates are, moreover, recognized only at the level of an implementing act.

It is a matter of legal certainty that the requirements applicable to qualified trust services be determined by EU law and by the standards to which EU law refers, and that a provider which has been granted qualified status and entered in a trusted list be placed in a position to bring its services into effective operation.

Targeted amendments can strengthen the effectiveness and coherence of the eIDAS framework

While the matters set out above differ in subject matter, they share a common objective: to ensure that the eIDAS framework can operate effectively, coherently and with legal certainty in practice. The legal uncertainty and practical difficulties identified above are borne principally by the undertakings that are most closely supervised and that must commit long-term investment on the basis of the framework as enacted.

In many cases, the remedies required are targeted and largely technical: clarifying the persons upon whom particular obligations fall and the arrangements by which those obligations are to be implemented and financed; providing a workable route to certification where the route presently contemplated is unavailable; expressly coordinating Union instruments where their cumulative application would result in duplicative requirements; and ensuring that qualified status conferred under EU law is given effect in practice.

The review provided for under Article 49 offers an appropriate opportunity to consider these matters together. Addressing them through targeted amendments, where necessary, would strengthen legal certainty and regulatory coherence and provide a more reliable basis for the continued deployment of the European Digital Identity ecosystem.

C. Proposed Amendments to the eIDAS Regulation *Suggestions 1–8*

Suggestion 1

Scope of the “free-of-charge” qualified electronic signature under Article 5a(5)(g)

Relevant provision:

Article 5a(5) provides, in its relevant part:

5. European Digital Identity Wallets shall, in particular:

[...]

(g) offer all natural persons the ability to sign by means of qualified electronic signatures by default and free of charge.

Notwithstanding point (g) of the first subparagraph, Member States may provide for proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to non-professional purposes.

Issues:

Issue 1. Article 5a(5)(g) is framed as an obligation of the European Digital Identity Wallet (EUDIW) itself, which is stated to offer natural persons the ability to sign free of charge.

A technical instrument of this kind cannot itself hold legal obligations, and the provision accordingly fails to identify with the necessary precision the **legal subjects upon whom the duty falls**.

The imprecision has produced divergent interpretations at national level, including interpretations under which the obligation is understood to extend to qualified trust service providers (QTSPs), engendering legal uncertainty and a risk of distortion of competition in the trust services market.

Issue 2. Article 5a(5)(g) provides that signing is to be offered to end users free of charge - but is silent as to how the provision of that service is to be financed and imposes no obligation on Member States to ensure that an appropriate financing arrangement is in place.

This omission gives rise to legal uncertainty as to the financing of free-of-charge signing and to a risk of divergent national approaches, with potential consequences for fair competition and for the proper functioning of the trust services market. Additionally, in the absence of such a rule, the cost of providing free signatures might fall unjustifiably on QTSPs, to the detriment of the sustainability of the trust services market.

Issue 3. The second subparagraph of Article 5a(5)(g) permits Member States to confine free-of-charge use to non-professional purposes, yet the notion is left undefined and its delimitation is not made the subject of any obligation.

The scope of free-of-charge signing is therefore uncertain and has already given rise to divergent approaches at national level, creating a risk of fragmentation of the internal market.

Issue 4. Where a Member State confines free-of-charge use to non-professional purposes, the application of that limitation presupposes knowledge of the purpose for which a given document is to be signed; that purpose, however, is not apparent to the wallet provider to

whom the obligation is addressed, nor to the qualified trust service provider, and can be established only by reference to the relying party.

Consequently, in the absence of a standardized technical means by which the **purpose of a signature** can be conveyed within the wallet ecosystem, the distinction between professional and non-professional use cannot be operated reliably, and the limitation permitted under the second subparagraph of Article 5a(5)(g) is rendered incapable of consistent and effective application.

Proposed modifications:

- 1. Addressee of the obligation.** The provision should be addressed to the Member States and to the providers of the EUDIW, the Member States being required to ensure that EUDIW providers make available to end users, through the wallet's features, the ability to sign by means of qualified electronic signatures (QES) by default and free of charge.
- 2. Compensation mechanism.** It should be expressly set out in the provision how the free-of-charge use by end users is to be compensated or, at a minimum, Member States shall be required to establish proportionate and non-discriminatory compensation or financing arrangements applying on equal terms to public and private wallets.
- 3. Definition of eligible non-professional use.** The Regulation should establish a **harmonized baseline for determining what constitutes non-professional use and the circumstances in which qualified electronic signatures must be provided free of charge.**

Within that framework, Member States would be able to introduce proportionate, objective and clearly defined conditions, such as limiting the benefit to specified categories of relying parties, setting an annual cap on the number of free signatures, or defining a list of eligible purposes, provided that such conditions do not undermine the effectiveness of the right.

- 4. Technical communication of the signing purpose.** Provision should be made for a standardized technical mechanism enabling the EUDIW to receive and process information indicating that a requested signature is intended for a non-professional purpose.

In particular, the mechanism should enable the wallet, through its interaction with the relying party, to identify the relying party and determine whether the requested transaction has been designated as falling within an eligible non-professional purpose. Such a mechanism should be standardized at Union level to ensure interoperability and consistent implementation across Member States.

Where no eligible non-professional purpose is communicated through that mechanism, the signature request should, by default, be treated as falling outside the scope of the free-of-charge regime.

Rationale:

Redirecting the obligation to Member States (which ensure delivery by wallet providers) reflects the structure of Article 5a and Recital 19 of Regulation (EU) 2024/1183 and confirms that the burden does not fall on QTSPs; an express compensation or financing duty prevents that burden from being shifted onto QTSPs; and harmonized boundaries for non-professional use, combined with a technical mechanism to communicate the signing purpose, make the non-professional limitation workable in practice while preventing fragmentation of the internal market and distortion of competition.

Suggested amendments:

5. European Digital Identity Wallets shall, in particular:

[...]

(g) ~~offer~~**enable** all natural persons ~~the ability~~ to sign by means of qualified electronic signatures by default and free of charge. **Member States shall ensure that providers of European Digital Identity Wallets make such functionality available to natural persons in accordance with this Regulation.**

Member States shall establish proportionate, transparent and non-discriminatory arrangements to ensure appropriate compensation or financing for the provision of qualified electronic signatures free of charge pursuant to point (g). Such arrangements shall apply on equal terms to public and private providers of European Digital Identity Wallets and qualified trust service providers.

Notwithstanding point (g) of the first subparagraph, Member States may provide for proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to non-professional purposes. **In determining non-professional purposes, Member States may take into account objective and clearly defined criteria, including the category of the relying party, the purpose of the transaction, or an annual maximum number of free qualified electronic signatures, provided that such measures are proportionate, non-discriminatory and do not undermine the effectiveness of the right established in point (g).**

The Commission shall establish, by means of implementing acts, a harmonized technical mechanism enabling the European Digital Identity Wallet to receive and process information indicating that a requested qualified electronic signature is intended for an eligible non-professional purpose.

Suggestion 2

Bodies competent to certify notified electronic identification schemes under Article 12a

Relevant provision:

Article 12a (Certification of electronic identification schemes) provides, in relevant part:

1. *The conformity of electronic identification schemes to be notified with the cybersecurity requirements laid down in this Regulation, including conformity with the cybersecurity relevant requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes, shall be certified by conformity assessment bodies designated by Member States.*

2. *Certification pursuant to paragraph 1 of this Article shall be carried out under a relevant cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 or parts thereof, insofar as the cybersecurity certificate or parts thereof cover those cybersecurity requirements.*

[...]

5. *The peer review of electronic identification schemes referred to in Article 12(5) shall not apply to electronic identification schemes or parts of such schemes certified in accordance with paragraph 1 of this Article. Member States may use a certificate or a statement of conformity, issued in accordance with a relevant certification scheme or parts of such schemes, with the non-*

cybersecurity-related requirements set out in Article 8(2) regarding the assurance level of electronic identification schemes.

6. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.

Issue:

Article 12a is at present inoperative, for two independent reasons.

First, it makes the certification of electronic identification schemes conditional on the existence of *conformity assessment bodies designated by Member States*. In practice, no such bodies have yet been designated by Member States, nor communicated to the Commission under Article 12a(6): the European Commission (DG DIGIT, Digital Building Blocks team) confirmed in writing in April 2026 that no notifications pursuant to Article 12a(6) have been received, that it is not aware of any Member State having indicated an intention to make such a notification, and that the Union-level publication facility for such notifications is not expected before September 2026. There is accordingly no available route for Member States to certify schemes in accordance with that provision.

Secondly, Article 12a(2) ties certification to a *relevant cybersecurity certification scheme pursuant to Regulation (EU) 2019/881*. No such scheme covering electronic identification schemes has been adopted, and none is known to be under preparation. The only European cybersecurity certification scheme adopted to date - the EUCC, established by Commission Implementing Regulation (EU) 2024/482 - is based on the Common Criteria (ISO/IEC 15408) and is inherently product-oriented: it presupposes a precisely delimited “target of evaluation”. An electronic identification scheme is, however, a composite operated service rather than a product: it encompasses enrolment and identity proofing, the issuance and lifecycle management of electronic identification means, authentication, and the surrounding organizational and management controls. For such a scheme, a Common Criteria-style target of evaluation cannot be meaningfully delimited, and reliance on EUCC-type product certification is structurally unsuited to the assessment task contemplated by Article 12a(1). For qualified trust service providers operating notified schemes, a product-oriented reading of Article 12a(2) would impose an assessment framework alien to the service-based conformity assessment model on which the eIDAS ecosystem otherwise rests.

Proposed modification:

Amend Article 12a so as to decouple the certification of notified electronic identification schemes from the cybersecurity certification scheme under Regulation (EU) 2019/881, which does not exist for schemes of this nature.

Specifically: (i) confine the certification under Article 12a(1) to conformity with the assurance-level requirements set out in Article 8(2), carried out by conformity assessment bodies designated by Member States; and (ii) repeal Article 12a(2), which makes certification conditional upon a cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 that has not been, and is not expected to be, adopted for electronic identification schemes.

Should a European cybersecurity certification scheme appropriate to electronic identification schemes be adopted in future, the linkage to that scheme may be reinstated at that time.

Rationale:

The only European cybersecurity certification scheme adopted to date, the EUCC established by Commission Implementing Regulation (EU) 2024/482, is based on the Common Criteria (ISO/IEC 15408) and is inherently product-oriented, presupposing a precisely delimited target of evaluation.

An electronic identification scheme is, however, a composite operated service rather than a product: it encompasses enrolment and identity proofing, the issuance and lifecycle management of electronic identification means, authentication, and the surrounding organisational and management controls.

For such a scheme a product-style target of evaluation cannot meaningfully be delimited, so that no scheme adopted under Regulation (EU) 2019/881 is presently capable of certifying it.

Conditioning certification upon a scheme that does not exist renders Article 12a inoperative and deprives schemes of the incentive attached to it, namely the exemption from peer review under Article 12a(5). Confining Article 12a(1) to conformity with the assurance-level requirements of Article 8(2), as technically specified by Implementing Regulation (EU) 2015/1502, allows the provision to operate on the basis of the very requirements to which it already refers, while leaving open the reinstatement of a cybersecurity-certification linkage if and when a scheme appropriate to services of this nature is adopted.

Suggested amendments:

Article 12a(1) and (2) could be amended as follows:

- 1. The conformity of electronic identification schemes to be notified with the requirements laid down in Article 8(2) regarding the assurance levels of electronic identification means, shall be certified by conformity assessment bodies designated by Member States.*
- 2. To be repealed*

Suggestion 3

Relationship between the eIDAS framework and the Cyber Resilience Act: an eIDAS-based presumption of conformity for qualified trust services and their software components

Relevant provision:

Article 20(1) of Regulation (EU) No 910/2014, as amended, provides:

- 1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555. [...]*

For context, Article 2(5) of Regulation (EU) 2024/2847 (Cyber Resilience Act - “CRA”) provides:

- 5. The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential cybersecurity requirements set out in this Regulation may be limited or excluded where such limitation or exclusion is consistent with the overall regulatory framework applying to those products and where the sectoral rules achieve at least the same level of protection as the one provided for by this Regulation. The Commission is empowered to adopt delegated acts [...] to supplement this Regulation by identifying such products and rules [...].*

Issue:

The eIDAS Regulation, in its current form, contains no provision governing its relationship with the CRA. In consequence, the software components with which qualified trust services are provided - background services, public key infrastructure and certificate issuance systems, authentication applications and signature-release applications, together with the associated “remote data processing” within the meaning of Article 3, point (2), CRA - stand to be captured by the CRA as ordinary products with digital elements.

The draft Commission Implementing Regulation on the technical description of the categories of important and critical products with digital elements expressly lists “public key infrastructure and digital certificate issuance software”, the core of any qualified trust service provider’s systems, among those categories.

These components are, however, integral parts of qualified trust services that are **already subject to a comprehensive, sector-specific cybersecurity regime**: recurring conformity assessment by accredited conformity assessment bodies under Article 20(1), which by its express terms covers both the requirements of the eIDAS Regulation and the cybersecurity risk-management requirements of Article 21 of Directive (EU) 2022/2555 (NIS2), on the basis of harmonized European standards - in particular ETSI EN 319 401, the ETSI EN 319 411 series and ETSI TS 119 461 - commonly supplemented by ISO/IEC 27001 certification.

The cumulative application of the CRA to the same components would produce duplicated requirements and audits, potentially conflicting obligations and reporting lines, and material additional cost, without a corresponding gain in cybersecurity.

The CRA is designed to remedy deficiencies in mass-market products, whereas qualified trust service providers operate in a narrowly defined, high-assurance segment whose “qualified” level of security by definition meets or exceeds baseline horizontal frameworks.

Article 2(5) CRA itself provides the mechanism for resolving such overlaps - a delegated act limiting or excluding the application of the CRA to products covered by sectoral Union rules achieving at least the same level of protection - but that mechanism has, to date, no anchor in the eIDAS Regulation on which the Commission could rely for trust services.

Proposed modification:

Amend the eIDAS Regulation, in the context of its revision, so as to: (i) insert an express provision (for instance, a new Article 20a) establishing that hardware and software components necessary for the provision of qualified trust services, insofar as they are subject to the requirements of the eIDAS Regulation and verified within the conformity assessment referred to in Article 20(1), shall be presumed to comply with the essential cybersecurity requirements set out in Annex I to the CRA and shall not be subject to separate conformity assessment obligations under the CRA; (ii) record, in the recitals and by way of a corresponding substantive provision, the legislator’s finding that the eIDAS framework - including the audits under Article 20(1), covering Article 21 of Directive (EU) 2022/2555, and the harmonized standards adopted thereunder - achieves at least the same level of protection as the CRA in respect of those components, including smart cards or similar devices with secure elements referred to in Annex IV, point 3, thereby establishing the substantive basis on which the Commission is to adopt the delegated act provided for in Article 2(5) CRA limiting or excluding the application of the CRA to them; and (iii) provide that incident notifications made by qualified trust service providers under the eIDAS and NIS2 frameworks are deemed to satisfy the corresponding reporting obligations under the CRA, so that a single, sector-specific reporting channel applies.

Rationale:

This approach keeps the legislative initiative entirely within the eIDAS revision - it amends eIDAS texts only - while producing the intended effect on the CRA and its implementing and delegated acts through the CRA's own coordination mechanism in Article 2(5), which presupposes precisely such sectoral rules and an equivalence finding. It is consistent with the position expressed by the European Signature Dialog in its comment of 13 April 2025 on the draft CRA implementing regulation, which requested that qualified trust service providers and the software components necessary for the provision of their services be excluded from the scope of the CRA. Anchoring the exclusion in eIDAS preserves the clarity of the Union's regulatory architecture - eIDAS remaining the *lex specialis* for trust services, the CRA applying to products not covered by specialized legislation - and avoids contradictory reporting lines, compliance duplication, fragmentation of supervision and cost inflation, none of which would improve security, while ensuring that the cybersecurity of qualified trust services continues to be guaranteed by the established sector-specific framework.

Suggested amendments:

A new Article 20a could be inserted as follows, accompanied by a recital recording the finding of equivalence on which paragraph 2 rests:

Article 20a - Cyber-resilience Compliance

- 1. Products with digital elements, including software or hardware components placed on the market separately, which are necessary for the provision of qualified trust services and which are subject to the requirements laid down in this Regulation, shall be presumed to be in conformity with the essential cybersecurity requirements set out in Annex I to Regulation (EU) 2024/2847, insofar as the fulfillment of those requirements is confirmed by the conformity assessment report referred to in Article 20(1) of this Regulation. Those products with digital elements shall not be subject to the conformity assessment procedures laid down in Article 32 of Regulation (EU) 2024/2847.***
- 2. The requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555, the fulfillment of which is confirmed by the audit referred to in Article 20(1) of this Regulation on the basis of the reference standards, specifications and procedures established pursuant to Article 20(4) thereof, shall be considered to achieve the same or a higher level of protection as that provided for by Regulation (EU) 2024/2847 in respect of the products with digital elements referred to in paragraph 1 of this Article, including smart cards or similar devices, including secure elements, referred to in point 3 of Annex IV to that Regulation. A limitation or exclusion of the application of that Regulation to those products with digital elements shall be considered consistent with the overall regulatory framework applicable to them. This Article shall constitute the basis for the adoption by the Commission of the delegated acts referred to in Article 2(5) of Regulation (EU) 2024/2847.***
- 3. Notifications made by qualified trust service providers pursuant to Article 24(2), point (fb), of this Regulation and pursuant to Article 23 of Directive (EU) 2022/2555 shall be deemed to fulfill the reporting obligations laid down in Article 14 of Regulation (EU) 2024/2847 in respect of the products with digital elements referred to in paragraph 1 of this Article.***

Suggestion 4

Modular compliance for the certification of European Digital Identity Wallets under Article 5c: recognition of existing QTSP certifications and audit evidence, avoidance of duplicative audits

Relevant provision:

Article 5c (Certification of European Digital Identity Wallets) provides, in relevant part:

1. The conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided with the requirements laid down in Article 5a(4), (5), (8), the requirement for logical separation laid down in Article 5a(14) and, where applicable, with the standards and technical specifications referred to in Article 5a(24), shall be certified by conformity assessment bodies designated by Member States.

3. For requirements referred to in paragraph 1 of this Article that are not relevant for cybersecurity, and, for requirements referred to in paragraph 1 of this Article that are relevant for cybersecurity, to the extent that cybersecurity certification schemes as referred to in paragraph 2 of this Article do not, or only partially, cover those cybersecurity requirements, also for those requirements, Member States shall establish national certification schemes following the requirements set out in the implementing acts referred to in paragraph 6 of this Article. [...]

Issue:

The certification framework of Article 5c treats the European Digital Identity Wallet as a monolithic object of assessment, although a wallet solution is in substance a composition of components and services a substantial part of which is already certified or audited within the eIDAS framework.

Wallets must enable signing by means of qualified electronic signatures (Article 5a(4), point (e), and Article 5a(5), point (a)(xi)), which rests on qualified certificates, qualified signature creation devices certified pursuant to Articles 30 and 39, and qualified trust services subject to recurring conformity assessment by accredited conformity assessment bodies under Article 20(1); wallets must meet the assurance-level-high requirements of Article 8 (Article 5a(5), point (d), and Article 5a(11)), which are technically specified by Implementing Regulation (EU) 2015/1502 and assessed in the context of the underlying electronic identification scheme; and Article 24(2), points (b) and (d) to (h), applies mutatis mutandis to wallet providers in any event (Article 5a(20)).

Neither Article 5c nor the implementing acts adopted under Article 5c(6) require the designated conformity assessment bodies, or the national certification schemes established under Article 5c(3), to recognize and reuse this existing, accredited assessment evidence.

The practical consequence - **of particular weight for wallet providers that are themselves qualified trust service providers, or that integrate qualified trust services of certified providers** - is that the same components, processes and requirements are assessed more than once, by different bodies, under different procedures.

Combined with the very large body of technical standards on which wallet certification depends, this duplication adds cost and delay without adding assurance, and burdens precisely those providers whose services are already subject to the most demanding regime in the framework.

Proposed modification:

Amend Article 5c, in the context of the eIDAS revision, so as to establish a modular (composite) compliance model:

- (i) insert a provision requiring that certification pursuant to Article 5c(1) recognize and reuse, without re-assessment, valid certificates, conformity assessment reports and audit evidence already issued in respect of components or services of the wallet solution under the eIDAS framework - in particular conformity assessment reports issued pursuant to Article 20(1), certifications of qualified signature and seal creation devices pursuant to Articles 30, 31 and 39, and assessments of the underlying electronic identification scheme against Implementing Regulation (EU) 2015/1502 - insofar as they cover the corresponding requirements referred to in Article 5c(1);
- (ii) provide that wallet functionalities which are provided by, or as, qualified trust services certified under Chapter III shall be presumed to conform with the corresponding requirements of Article 5a(4) and (5), the assessment under Article 5c being confined to the residual, wallet-specific requirements not already covered;
- (iii) require that the implementing acts referred to in Article 5c(6), and the national certification schemes established under Article 5c(3), give effect to this modular model, with the European Digital Identity Cooperation Group monitoring its consistent application; and
- (iv) state expressly that a provider shall not be required to undergo repeated assessment of the same requirements in respect of the same components by different conformity assessment bodies.

Rationale:

A modular compliance model reflects established certification practice, in which composite products and services are certified by reusing valid evaluation results for their certified constituents.

The evidence to be reused originates from accredited conformity assessment bodies applying the same or stricter requirements - qualified trust services and assurance level high representing the highest tiers of the eIDAS framework - so no reduction of assurance is involved; what is removed is only the repeated assessment of matter already assessed.

This directly reduces certification cost and time-to-market for wallet solutions, removes a structural disincentive for qualified trust service providers to act as wallet providers or component suppliers, and thereby **supports the deployment timeline and the emergence of competitive, market-driven wallet offerings.**

The proposal is consistent with the position expressed by the European Signature Dialog in its position paper on the Digital Omnibus of 13 October 2025, which called for a modular compliance model under which wallet providers demonstrate conformity via existing QTSP certifications without duplicative audits, and with the single-audit and mutual-recognition principle advocated in the same paper.

Suggested amendments:

Article 5c could be supplemented by new paragraphs 3a, 3b and 3c as follows:

3a. Certification pursuant to paragraph 1 of this Article shall recognize and reuse, without re-assessment, valid certificates, conformity assessment reports and audit evidence issued in

respect of components or services of the European Digital Identity Wallet under this Regulation, in particular conformity assessment reports issued pursuant to Article 20(1), certifications of qualified electronic signature creation devices and qualified electronic seal creation devices pursuant to Articles 30, 31 and 39, and assessments of the electronic identification scheme under which the European Digital Identity Wallet is provided against the requirements set out in the implementing acts referred to in Article 8(3), insofar as those certificates, reports or evidence cover the corresponding requirements referred to in paragraph 1 of this Article.

3b. Functionalities of the European Digital Identity Wallet which are provided by, or as, qualified trust services certified in accordance with Chapter III shall be presumed to conform with the corresponding requirements referred to in Article 5a(4) and (5). In such cases, the assessment pursuant to paragraph 1 of this Article shall be confined to those requirements which are not covered by that certification. A provider shall not be required to undergo repeated assessment of the same requirements in respect of the same components by different conformity assessment bodies.

3c. The implementing acts referred to in paragraph 6 of this Article and the national certification schemes referred to in paragraph 3 of this Article shall give effect to paragraphs 3a and 3b. The European Digital Identity Cooperation Group established pursuant to Article 46e shall monitor their consistent application.

Suggestion 5

Effective recognition of qualified certificates for website authentication and autonomy of the EU framework under Articles 45 and 45a

Relevant provision:

Article 45 (Requirements for qualified certificates for website authentication) provides, in its relevant part:

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. The evaluation of compliance with those requirements shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 2 of this Article.

1a. Qualified certificates for website authentication issued in accordance with paragraph 1 of this Article shall be recognized by providers of web-browsers. Providers of web-browsers shall ensure that the identity data attested in the certificate and additional attested attributes are displayed in a user-friendly manner. Providers of web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1 of this Article [...].

1b. Qualified certificates for website authentication shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for website authentication, referred to in paragraph 1 of this Article. [...]

Article 45a (Cybersecurity precautionary measures) provides, in its relevant part:

1. Providers of web-browsers shall not take any measures contrary to their obligations set out in Article 45, in particular the requirements to recognize qualified certificates for website authentication and to display the identity data provided in a user-friendly manner.

2. By way of derogation from paragraph 1 and only in the event of substantiated concerns related to security breaches or the loss of integrity of an identified certificate or set of certificates, providers of web-browsers may take precautionary measures in relation to that certificate or set of certificates.

Issues:

Issue 1. Although Article 45(1a) obliges providers of web-browsers to recognize qualified certificates for website authentication (QWACs), and Article 45(1b) provides that such certificates are not to be subject to any mandatory requirements other than those laid down in paragraph 1, the effective use of a QWAC for transport layer security authentication in the browser environment remains, in practice, conditional upon the inclusion of the issuing qualified trust service provider (QTSP) in the certificate trust programmes ("root store programmes") operated by the providers of the major web-browsers.

The standards by reference to which compliance is evaluated pursuant to Article 45(1), as listed in Commission Implementing Regulation (EU) 2025/2527 of 16 December 2025 adopted pursuant to Article 45(2) - in particular ETSI TS 119 411-5 - incorporate, for QWACs used as transport layer security certificates, the Baseline Requirements of the CA/Browser Forum and the additional requirements of the browsers' root store programmes.

Inclusion in a root store programme rests on **individual, non-transparent decisions** of private undertakings, taken without procedural safeguards, without an obligation to state reasons and **without any possibility of objection or legal review**. In consequence, the dependency on unilateral private gatekeeping which Article 45(1a) and (1b) were designed to remove is re-established at the technical level, and qualified trust service providers whose website authentication services have been granted qualified status and are included in the trusted lists referred to in Article 22 may nevertheless find themselves unable to bring those services into effective production, notwithstanding full compliance with the Regulation.

Issue 2. The Regulation provides no remedy against that state of affairs. Article 45a circumscribes the precautionary measures which browsers may take in relation to an identified certificate or set of certificates and subjects such measures to notification and supervisory investigation; it does not, however, reach the prior and more consequential conduct of a provider of web-browsers consisting in the refusal or omission to give effect to the recognition obligation vis-à-vis a given qualified trust service provider as such. The procedural protections of Article 45a(3) and (4) accordingly operate only downstream, while the **structural gatekeeping upstream remains outside the reach of the supervisory system**.

Issue 3. The exposure of the qualified framework to third-party private governance extends beyond the browser environment. QWACs are relied upon on a large scale outside web-browsers, most prominently in the Open Banking framework under Directive (EU) 2015/2366 (PSD2) and Commission Delegated Regulation (EU) 2018/389, in which payment service providers identify themselves and mutually authenticate their interfaces by means of QWACs issued in accordance with the certificate profile of ETSI TS 119 495 - a framework acknowledged by the European Banking Authority, embedded in the rulebooks of the European Payments Council payment schemes, and operating with certificates typically issued with a period of validity of up to two years.

The CA/Browser Forum adopted in April 2025 ballot SC-081v3, which progressively reduces the maximum validity of TLS certificates from 398 days to 200 days as of 15 March 2026, 100 days as of 15 March 2027 and ultimately 47 days as of 15 March 2029.

To the extent that the standards referenced in the implementing act adopted under Article 45(2) incorporate or defer to CA/Browser Forum requirements, those reductions - conceived for the open web ecosystem - cascade onto closed, supervised, machine-to-machine environments to which their rationale does not apply, and impose renewal cycles incompatible with the operational stability and resilience of Union payment infrastructures.

The Regulation itself is silent on this category of certificates: the distinction between QWACs used in and outside the browser context exists only in the structure of the Annex to Implementing Regulation (EU) 2025/2527, so that the existence, requirements and validity conditions of non-browser QWACs are governed exclusively at the level of an implementing act which may be amended at any time - although reliance on such certificates is set to expand under the forthcoming payments framework (PSD3/PSR) and the framework for financial data access.

Issue 4. The vulnerabilities described in Issues 1 and 3 share a common root in the drafting of Article 45(1), second sentence, under which the evaluation of compliance is to be "*carried out in accordance with*" the standards referred to in paragraph 2.

Unlike the corresponding provisions governing most other qualified trust services - for instance Article 24(5), Article 45j(2) and Article 45l(2), under which compliance is presumed where the referenced standards are met - that formulation makes the referenced standards the exclusive route to compliance and thereby elevates the private technical governance incorporated by those standards into de facto binding Union law.

Proposed modifications:

Amend Article 45 and Article 45a so as to:

- (i) prohibit expressly that the issuance, validity, recognition or effective use of QWACs be made conditional upon the inclusion of the issuing QTSP in, or its participation in, any root store programme or equivalent scheme operated by a provider of web-browsers or by any other private entity, and provide that, for the purposes of the recognition obligation under Article 45(1a), providers of web-browsers are to rely on the trusted lists referred to in Article 22 as the authoritative source of the qualified status of the provider and of the certificates issued by it;
- (ii) extend the procedural discipline of Article 45a to any refusal, restriction or omission by a provider of web-browsers which has the effect of preventing or limiting the recognition, display or effective use of QWACs, including a right for the QTSP concerned to refer the matter to the competent supervisory body and access to effective judicial remedies;
- (iii) recognize expressly the category of QWACs issued for use in transport layer security authentication outside the context of a web-browser, provide that the requirements applicable to such certificates, including their maximum period of validity, are governed exclusively by the Regulation and by the standards referred to in Article 45(2) - to the exclusion of rules adopted by private industry bodies - and direct that the implementing acts include reference standards appropriate to such uses, including sector-specific certificate profiles such as ETSI TS 119 495; and
- (iv) align Article 45(1) with the presumption-of-compliance model applied to the other qualified trust services.

Rationale:

The recognition and display obligations of Article 45(1a), together with the prohibition of additional mandatory requirements in Article 45(1b) and the strict confinement of browser measures in Article 45a, embody a deliberate legislative choice: the qualified status established under Union law, attested by the trusted lists, is to be the **sole condition of recognition**, in place of unilateral private gatekeeping (see also Recital 65 of Regulation (EU) 2024/1183).

Experience since adoption demonstrates that this choice is being circumvented at the level of technical standards: the European Signature Dialog, in its comments on the draft implementing regulation on reference standards for QWACs, requested an express proviso that qualified trust service providers "shall not have to be part of the dedicated browser root store program", as well as the express inclusion of ETSI TS 119 495 to safeguard the continuity of PSD2 certificates; the public statement issued by Mozilla on 23 December 2025 upon the publication of Implementing Regulation (EU) 2025/2527, presenting the outcome as the successful preservation of "browser root store independence", confirms that providers of web-browsers regard their gatekeeping function as intact notwithstanding Articles 45 and 45a.

Absent a Regulation-level prohibition and a redress mechanism, Article 45(1a) risks remaining a dead letter and the investments of QTSPs in qualified website authentication services are devalued.

As regards certificates used outside the browser context, the 47-day validity trajectory of the CA/Browser Forum responds to risks of the open web which have no equivalent in closed API ecosystems where both endpoints are supervised financial entities mutually authenticated by qualified certificates; applying it there would multiply renewal operations across the European payments infrastructure without any corresponding security gain, while each renewal cycle introduces operational risk.

Anchoring both safeguards in the Regulation itself provides legal certainty, preserves the level playing field between European supervised providers and non-European private gatekeepers, and confirms - consistently with Article 45(1b) - that the requirements applicable to qualified trust services are set by Union law and not by private governance bodies in which European qualified trust service providers have no guaranteed voice.

Suggested amendments:

Article 45(1) could be amended as follows:

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. ~~The evaluation of compliance with those requirements shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 2 of this Article.~~ Compliance with those requirements shall be presumed where a qualified certificate for website authentication complies with the standards, specifications and procedures referred to in paragraph 2 of this Article.

Article 45(1b) could be supplemented and a new paragraph 1c could be inserted as follows:

1b. Qualified certificates for website authentication shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1. In particular, the issuance, validity, recognition or effective use of qualified certificates for website authentication shall not be made conditional upon the inclusion of the issuing qualified trust service provider in, or its participation in, any certificate trust programme ('root store programme') or equivalent scheme operated by a provider of web-browsers or by any other private entity. For the purposes of the recognition obligation laid down in paragraph 1a, providers of web-browsers

shall rely on the trusted lists referred to in Article 22 as the authoritative source of the qualified status of the trust service provider and of the qualified certificates issued by it.

1c. Qualified certificates for website authentication may be issued for use in transport layer security authentication outside the context of a web-browser, including for the mutual authentication of automated systems in sectors regulated by Union law. The requirements applicable to such certificates, including their maximum period of validity, shall be governed exclusively by this Regulation and by the standards, specifications and procedures referred to in paragraph 2. The implementing acts referred to in paragraph 2 shall include reference standards appropriate to such uses, including sector-specific certificate profiles. Rules adopted by private industry bodies shall not affect the issuance, validity or use of such certificates.

A new paragraph 5 would be added to Article 45a:

5. Any refusal, restriction or omission by a provider of web-browsers, the effect of which is to prevent or limit the recognition, the display or the effective use of qualified certificates for website authentication issued by a qualified trust service provider, shall be deemed to constitute a precautionary measure within the meaning of paragraph 2. Paragraphs 3 and 4 shall apply accordingly. The qualified trust service provider concerned shall be entitled to refer the matter to the competent supervisory body and shall have access to effective judicial remedies.

Suggestion 6

Continuity of the certification of qualified electronic signature and seal creation devices

Relevant provision:

Article 31 (Publication of a list of certified qualified electronic signature creation devices) provides:

- 1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is completed, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified.*
- 2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices.*
- 3. The Commission may, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).*

Article 30(1) provides that conformity of qualified electronic signature creation devices with the requirements laid down in Annex II is to be certified by appropriate public or private bodies designated by Member States. Article 39(2) and (3) apply Articles 30 and 31 mutatis mutandis to the certification of qualified electronic seal creation devices and to the publication of the corresponding list.

Issues:

Issue 1. Articles 30 and 31 govern the certification of a device and the publication of its certification status, but does not address the period for which that certification is to be maintained. The information to be notified is confined to certifications completed and

certifications cancelled, with the result that the list published pursuant to Article 31(2) records the position as it stands at a given moment and discloses nothing as to its expected continuance.

Issue 2. The obligations laid down in Articles 30 and 31 are addressed to the Member States and to the designated bodies. The manufacturer of the device is not an addressee of those provisions, with the consequence that the information upon which the continuity of a qualified trust service depends is available only insofar as the manufacturer elects to disclose it, and no duty attaches to a manufacturer in respect of a change in its intentions.

Issue 3. Notification of a cancelled certification is required only after the cancellation has taken effect. The substitution of a qualified signature or seal creation device requires the adaptation of the procedures and processes of the qualified trust service provider, the integration of a device having different hardware and software characteristics and, as a rule, a further conformity assessment; a device certified in one Member State is, moreover, commonly relied upon by providers established in a number of others. No period of notice is prescribed within which such substitution may be prepared.

Issue 4. The obligations of manufacturers as regards the period of support of a product with digital elements, and the handling of vulnerabilities during that period, arise at present under Regulation (EU) 2024/2847. Were the application of that Regulation to be limited or excluded in respect of the devices referred to in point 3 of Annex IV thereto, as contemplated in Suggestion 3, no equivalent duty would subsist under this Regulation.

Proposed modifications:

1. **Content of the notification.** The information to be notified pursuant to Article 31(1) should be extended to include, for each certified device, the period for which the certification of the current configuration is to be maintained and the arrangements by which the manufacturer intends to maintain it, and that information should be reflected in the list published pursuant to Article 31(2).
2. **Addressee of the information duty.** Manufacturers should be required to provide that information to the body designated pursuant to Article 30(1) and to the notifying Member State, and to communicate any change to it without undue delay, the Member State being required to notify the change to the Commission.
3. **Period of notice.** A minimum period should be prescribed between the communication of an intention to discontinue the certification of a current configuration and the taking of effect of that discontinuation.
4. **Relationship with Regulation (EU) 2024/2847.** The finding of equivalence proposed in Suggestion 3 should be expressed as extending to the maintenance of the certification of the components concerned, by reference to the obligations laid down in Article 31.

Rationale:

The certification of a qualified signature or seal creation device is a condition of the qualified status of the services provided by means of it, and the planning horizon of a qualified trust service provider is accordingly governed by a decision taken by a third party over whom it has no contractual or regulatory hold.

Requiring that the intended duration of certification be disclosed at the point of notification, and that changes be communicated as they arise, places no substantive obligation upon manufacturers as to how long a device is to be supported; it renders visible a fact which the manufacturer already knows and upon which the market must rely.

A period of notice of twenty-four months corresponds to the interval between the conformity assessments required by Article 20(1), so that migration may be prepared, executed and assessed within a single audit cycle rather than across two.

The proposal is also the necessary counterpart of Suggestion 3: the limitation or exclusion of Regulation (EU) 2024/2847 in respect of secure elements and similar devices is defensible only where the sectoral framework achieves at least the same level of protection, and the support-period obligations of that Regulation must therefore find their equivalent in this one.

Questions of compensation for the cost of migration are left to the contractual relationship between the provider and the manufacturer, which the transparency proposed here places on a substantially better-informed footing.

Suggested amendments:

Article 31 could be amended as follows, the amendment applying to qualified electronic seal creation devices by virtue of Article 39(3):

*1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is completed, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified. **That information shall include, for each certified device, the period for which the certification of the current configuration of that device is to be maintained and the arrangements by which the manufacturer intends to maintain it.***

1a. Manufacturers of qualified electronic signature creation devices shall provide the information referred to in the third sentence of paragraph 1 to the body designated pursuant to Article 30(1) and to the Member State making the notification. Manufacturers shall inform that body and that Member State, without undue delay, of any change to that information, and the Member State concerned shall notify that change to the Commission in accordance with paragraph 1.

1b. Where a manufacturer intends to discontinue the certification of the current configuration of a certified device, it shall communicate that intention in accordance with paragraph 1a not less than 24 months before the discontinuation is to take effect.

*2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices. **That list shall indicate, for each device, the information referred to in the third sentence of paragraph 1 and any intention communicated pursuant to paragraph 1b.***

*3. The Commission may, by means of implementing acts, define formats and procedures applicable for the purpose of ~~paragraph 1~~ **paragraphs 1, 1a and 1b**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).*

Consequential addition to Suggestion 3:

Paragraph 2 of the Article 20a proposed under Suggestion 3 would be supplemented by the following sentence:

The requirements laid down in Article 31 as regards the maintenance of the certification of qualified electronic signature creation devices and qualified electronic seal creation devices

shall form part of that finding in respect of the devices referred to in point 3 of Annex IV to Regulation (EU) 2024/2847.

Suggestion 7

The interoperability of attributes

Relevant provision:

Article 45d (Requirements for qualified electronic attestation of attributes) provides:

(...)

5. *By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic attestations of attributes. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).*

Issue: Article 45d does not specify the exact expected scope of the specification and procedure needed for qualified electronic attestations of attributes.

Rationale

The interoperability of an attribute implies that the same attribute produced by any Provider of electronic attestations of attributes can be stored and managed to any wallet but also to any European Digital Identity Wallet-Relying Parties.

This can only be done if there is a common syntax, such as the one referred to in the implementing Act, but also if the information is encoded in the exact same way. As an example, the attribute 'Nationality or citizenship' can be encoded in a various way such as "FR", "FRA", "FRANCE", "France", "Française" "French". If provider, wallets and third parties are not agreeing on a common way to encode the attributes keys and values in the exact same way, interoperability will not be possible.

Suggested amendments:

Article 45d could be amended as follows,

(...)

6. By xx/xx/xxxx, the Commission shall, by means of implementing acts, establish a list of reference standards describing the interoperability syntax for qualified electronic attestations of attributes, such that the same attribute with the same value can only be encoded in a very limited number of attestations of attributes. The scope shall at least cover the list of attributes defined in Annex VI. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48.

Suggestion 8

Aligning PubEAA Requirements with QEAA Where Reliance Is High

Relevant provision:

Article 45d ("Requirements for qualified electronic attestation of attributes") subjects QEAA to the requirements laid down in Annex V, issued exclusively by qualified trust service providers ("QTSPs").

Article 45f ("Requirements for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source") subjects PubEAA to the distinct requirements of Annex VII, issued by a public sector body that Article 45f expressly does not treat as a QTSP. Article 45b(2) nonetheless provides that "a qualified electronic attestation of attributes and attestations of attributes issued by, or on behalf of, a public sector body responsible for an authentic source shall have the same legal effect as lawfully issued attestations in paper form."

Issues:

Issue 1. (*Institutional supervision gap*). A QTSP issuing QEAA is subject to the full QTSP supervisory regime: recurring conformity assessment audits at least every 24 months by a conformity assessment body (Article 20(1)), with withdrawal of qualified status on uncured failure (Article 20(3)), and the strict identity- and attribute-verification methods of Article 24(1a) and (1b).

A public sector body issuing PubEAA, by contrast, need only reach a level of reliability and trustworthiness "equivalent to" a QTSP (Article 45f(2)), confirmed once, at notification, by a single conformity assessment report (Article 45f(3)) — with **no recurring audit obligation comparable to Article 20(1), and no mechanism analogous to Article 20(3) for withdrawing that status if reliability later lapses**. The legal-effect equivalence established by Article 45b(2) is accordingly backed, on the PubEAA side, by a one-off assurance check rather than the ongoing supervisory cycle that underpins it on the QEAA side.

Issue 2. (*Attribute-risk mismatch*). The applicable regime — Annex V or Annex VII — turns exclusively on whether the authentic source is a public-sector body, not on the nature or consequences of the attested attribute or the reliance placed on it by relying parties, so that attributes with elevated consequences for relying parties (e.g. professional-qualification attestations tied to liability) can carry only the lighter Annex VII assurance.

Proposed modifications:

Amend Article 45f so as to:

- (i) introduce a recurring reassessment obligation for public sector bodies issuing PubEAA, modelled on Article 20(1): a conformity assessment report confirming continued compliance with Article 45f(2) submitted at a fixed interval (e.g. every 24 months), with a mechanism modelled on Article 20(3) for the competent authority to withdraw the body's inclusion in the list published under Article 45f(3) where the report is not provided or reveals non-compliance; and
- (ii) for the categories of attributes listed in Annex VI that the implementing acts identify as carrying elevated protection needs for relying parties, require either that the issuing public sector body meet the full supervisory regime of Articles 20, 21 and 24 as if it were a QTSP, or

that the PubEAA be co-signed or co-sealed by a QTSP, so that the institutional assurance gap identified in Issue 1 is closed precisely where Issue 2 shows it matters most, while leaving the lighter Article 45f(3) regime in place for attributes outside that category.

D. Issues Concerning Implementing Acts, Reference Standards and Supervisory Practice

A number of shortcomings have equally been identified within the implementing acts adopted under the Regulation, within the reference standards to which those acts refer and within supervisory practice.

It should be noted that the effectiveness of the Regulation depends in large measure upon the acts adopted under it. The identified points are recurrent rather than isolated, and they may be grouped as follows.

1. **Transitional arrangements and continuity of existing services.** The implementing framework contains transitional measures, but these are not uniform. Deferred dates of application have been provided in certain acts, including in respect of the verification of identity and attributes (Implementing Regulation (EU) 2025/1566) and the registration of wallet-relying parties (Implementing Regulation (EU) 2025/848). Other acts apply from their entry into force without an equivalent period (for example, Article 3 of Implementing Regulation (EU) 2025/1944).

A more comprehensive and harmonized approach to the continuity of existing certificates, services and processes would improve legal certainty during migration.

2. **Reuse of the qualified trust infrastructure within the wallet ecosystem.** The wallet framework establishes a dedicated registration, notification and certificate infrastructure distinct from the qualified trust service and trusted-list framework. The relevant roles are not reserved to qualified trust service providers, and existing qualified trust credentials are not generally recognized as substitutes for the wallet-specific credentials prescribed by the implementing acts (see, in particular, Implementing Regulations (EU) 2024/2980 and 2025/848, as amended respectively by Implementing Regulations (EU) 2026/1731 and 2026/1730).

Greater alignment between these infrastructures could reduce duplication and facilitate interoperability.

3. **Notification by authentic sources of changes in attribute content.** No general obligation has been established for authentic sources to notify attestation providers proactively where the underlying attribute information changes; verification is principally based on mechanisms made available at the request of the user (Article 9 of Implementing Regulation (EU) 2025/1569). Revocation requirements are, moreover, differentiated by reference to the validity period of the attestation, and no retention period is prescribed for revocation information (Article 4 of that Regulation).

Clarification of notification, revocation and retention mechanisms would improve the lifecycle management of electronic attestations of attributes.

4. **Non-professional use of the free-of-charge qualified electronic signature.** In relation to what is addressed in Suggestion 1 in Section C (“Proposed Amendments to the eIDAS Regulation”), the requirement to provide natural persons with free-of-charge access to qualified electronic signature functionality for non-professional purposes is not accompanied by a harmonized definition of those purposes (Article 11(3) of Implementing Regulation (EU) 2024/2979).

Further guidance would reduce the risk of divergent national interpretations.

5. **Interfaces for the creation of qualified electronic signatures within the wallet.** Where signature creation applications rely on remote qualified signature creation devices and are integrated into wallet instances, support for the prescribed application programming interface is mandatory (Article 12 and Annex IV to Implementing Regulation (EU) 2024/2979).

Greater flexibility in the evolution of interfaces, together with clear lifecycle arrangements for certified signature-creation devices, could reduce technical rigidity. Similar considerations arise from the treatment of device certification information in the applicable trust service practice statement (Implementing Regulation (EU) 2025/1567).

6. **Residual obligations on qualified trust service providers.** Certain notification, third-party and financial requirements applicable to qualified trust service providers remain broadly formulated, including as regards changes concerning third parties or relevant contractual arrangements and the maintenance of sufficient financial resources or appropriate insurance in connection with termination planning (Implementing Regulation (EU) 2025/2530). Certain technical requirements may also generate additional operational burden, such as the requirement for wallet units to request issuance in all supported formats in the circumstances specified in Article 4(3)(a) of Implementing Regulation (EU) 2024/2982.

Further clarification and proportionality could reduce divergent interpretations and unnecessary administrative burden.

7. **Institutional and terminological ambiguities.** Certain provisions rely on institutional or technical concepts whose meaning is not fully specified. Examples include the reference to a national competent authority in requirement VAL-8.3.3-21 of the Annex to Implementing Regulation (EU) 2025/1566 and the reference to an attribute defined in an analogue way in Article 8(3)(f) of Implementing Regulation (EU) 2025/1569.

In the wallet certification framework, no rule of priority has been established where the requirements of the Cyber Resilience Act and the security objectives of Article 51 of Regulation (EU) 2019/881 diverge, no channel or deadline has been established for reporting the fraudulent use of certification, and no time limit governs the opinions of the Cooperation Group (Articles 4(4)(e), 7(4), 8(3)(a) and 15 of Implementing Regulation (EU) 2024/2981).

Further clarification would be beneficial in each respect.

8. **Functional separation and the status of non-qualified attestations.** The requirement for functional separation in the provision of qualified electronic attestations of attributes is not accompanied by organizational or technical criteria specifying how that separation is to be achieved, and Implementing Regulation (EU) 2025/1569 does not provide an implementation model in this respect. The wallet framework does distinguish between categories of attestation provider through the applicable registration and access-certificate mechanisms (Article 4 of Implementing Regulation (EU) 2024/2982; Annex I to Implementing Regulation (EU) 2025/848).

Further guidance could nevertheless improve consistency in the treatment and identification of qualified and non-qualified providers.

9. **Accountability within the supply chain for creation devices.** The obligation to communicate changes affecting the notified information concerning certified qualified signature or seal creation devices, including changes in certification status, rests on the Member States (Article 1(2) of Implementing Regulation (EU) 2025/1570). Although the Annex requires information concerning certification, no direct lifecycle-notification mechanism has been established between manufacturers and the eIDAS supervisory ecosystem.

Greater clarity regarding manufacturer responsibilities, certification maintenance and lifecycle information could assist qualified trust service providers in managing continuity and migration risks.

E. About the European Signature Dialogue

The European Signature Dialogue (ESD) brings together leading companies servicing 250 million users in their everyday use of qualified trust services from across Europe, to foster secure and trustworthy digital interactions in line with the highest EU standards.

ESD acts as the main interlocutor for European and national institutions, providing expert advice and support, particularly for the European Commission, Parliament and Council. As the recognised voice for trust services across Europe, ESD members work together to develop common regulatory positions and shape the digital trust ecosystem. Beyond Europe, ESD and its members serve as ambassadors, promoting European excellence and standards in digital security around the world.