

Ref.: Commission Implementing Regulation proposal on Art. 24 for the verification of the identity and attributes of person in the context of issuance of a qualified certificate or a qualified electronic attestation of attributes

ESD feedback and proposal

The European Signature Dialog (ESD) is an initiative that represents the leading European Qualified Trust Service Providers (QTSPs), that play a crucial role in enabling secure digital interactions across Europe, facilitating communication and transactions between public entities, businesses, and individuals. The ESD is deeply involved in discussions and negotiations surrounding the eIDAS Regulation.

ESD expresses heartfelt appreciation to the European Commission for allowing to participate in the open consultation concerning the Commission Implementing Decisions on trust services, as regulated by Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, which pertains to electronic identification and trust services for electronic transactions within the internal market (eIDAS Regulation).

Qualified Trust Service Providers (QTSPs) play a pivotal role in the digital single market by ensuring trust and security in electronic transactions. Qualified Trust Services are essential for enabling mission-critical digital processes across various sectors; for instance, in the financial industry, QTSPs facilitate secure online banking and customer onboarding, ensuring that transactions are both authenticated and encrypted. In healthcare, they support the secure exchange of sensitive patient data and electronic health records, maintaining confidentiality and integrity. Additionally, in the public sector, QTSPs enable secure digital identification and electronic signatures for government services, streamlining administrative processes and enhancing citizen trust in digital interactions. By providing these crucial services, QTSPs help build a reliable and secure digital infrastructure that is fundamental for the smooth operation of the digital single market.

In this document, we offer comprehensive comments and feedback on the proposed Commission Implementing Decisions. Our feedback has been elaborate leveraging the deep knowledge of our members and experts, taking into consideration the technological and compliance impacts, as well as the user experience and the impacts on the business, to ensure the effective functioning of the Digital Single Market in Europe, safeguarding and enhancing the existing areas of excellence within the European market, preserving investments, and facilitating a seamless transition for QTSPs that currently provide Qualified Trust Services. We highlight the necessity of interoperability frameworks among various services and providers to promote a competitive, resilient, and innovative market.

Therefore, we request that the implementing acts mandating new standards, which introduce more stringent requirements and certifications, come into effect after a necessary adjustment period (24 to 30 months). This timeframe will allow the entire supply chain, including accredited laboratories, Conformity Assessment Bodies (CABs), Regulating Authorities, Supervisory Bodies, QTSPs, and their suppliers, to adapt accordingly. The introduction of new stringent requirements and certifications necessitates investments and adjustments to processes, technologies, and organizations, which require time. We urge the Commission to avoid decisions that could disrupt service provision, potentially causing severe consequences in mission-critical processes such as customer onboarding, digital health and telemedicine, public administration and justice, as well as the submission of annual financial statements to business registries.

1. ESD feedback

The implementation of the new requirements introduced by the Implementing Act will necessitate significant adjustments and investments across the trust services ecosystem, particularly for European QTSPs already managing identification and signing processes, including those operating remotely. These adjustments encompass the development, testing, and accreditation of updated laboratory procedures, the adaptation of Conformity Assessment Bodies (CABs) to new checklists, and, where applicable, amendments to national laws. Each of these steps requires considerable time and coordination. Additionally, given the current limited availability of accredited labs and CABs with the necessary expertise to perform audits on standards like ETSI TS 119 461 v 2.1.1, a surge in demand could overwhelm system capacity and create bottlenecks. This situation would unfairly disadvantage fully compliant QTSPs that simply lack access to timely audits. At present, it appears that only one laboratory in the entire EU is equipped to perform the required tests, making it practically impossible to comply with the requirements set out by the ETSI 119 461 standard. In the tables below, we highlight specific clauses, articles, or requirements in the Regulation, the annex, or the standard itself that could cause disruptions.

To ensure a level playing field and maintain the quality of audits and certifications, it is crucial to allow a realistic transition period. The sequence of activities required—starting with the publication of the Implementing Act in the Official Journal and extending through laboratory test planning, national accreditations, procedural adaptations by QTSPs, audits, and eventual rollout—demands adequate time for the ecosystem to adapt responsibly.

Based on this structured roadmap, **we recommend that the entry into force of the Implementing Act be postponed for no less than 30 months, providing sufficient time for the ecosystem to adapt without disrupting ongoing trust services.**

article	Comment	Proposed solution
Whereas (2) In order to ensure legal certainty and trustworthiness of the result of the verification process, verifications should be carried out in the same manner by all qualified trust service providers issuing a qualified certificate or a qualified electronic attestation of attributes. In accordance with the objectives of Regulation (EU) No 910/2014, a number of standards have been selected to meet these specific requirements. These standards reflect established practices, are widely recognised within the relevant sectors and ensure consistency, legal certainty and trust, while facilitating cross-border interoperability and the effective functioning of the internal market. Implementation of measures to comply with the requirements set out in the standards should take into account experiences from implementation and their effectiveness should be continuously improved.	The selected ETSI TS 119 461 v2.1.1 standard (that has been recently revised) is too young to be considered “established” and “widely recognized”, considering that no organization had already the time to fully apply it. The only similar and comparable existing standard is the French PVID that, despite having being issued in 2021, it is still concretely not widely used in the market because the designed identification process is too cumbersome and not user-friendly, in the current market context. ETSI 119 461 v2.1.1 is creating a similar process, with a high risk to be refused by the market: an immediate entry into force will imply that the relevant of the market players, that today are relying on processes based on Qualified Certificates, will choose to operate under a low level of trust and replace Qualified Signatures with other solutions, diminishing the level of protection of the citizens.	Entry into force of the IA not before 30 months from the publication, leaving time for an effective uptake of LoA high eIDs and EUDIW. In the meantime, national SBs should be allowed to approve national-specific identification processes, after presentation of a CAR and security assessment, to allow a smooth transition between the two regimes. The act should clarify that the new regime is applicable only to the certificates issued after its entry into force, and that the existing set of certificates used in the Single Market continues to be compliant and completely valid.

article	Comment	Proposed solution
Whereas (3) This Regulation is without prejudice to Article 51(4) of Regulation (EU) No 910/2014, clarifying that qualified trust service providers that were granted their qualified status under this Regulation before 20 May 2024 are to submit a conformity assessment report to the supervisory body proving compliance with Article 24(1), (1a) and (1b) of Regulation (EU) No 910/2014 as soon as possible and in any event by 21 May 2026. Article 2 This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	The process to adapt the identification processes for the QTSPs, especially those already operating with remote processes, will require several developments (and related investments), as well as the possibility to select and integrate third party components and solutions. In addition, more time is needed to get a full compliance, all the tests and certifications required and the approval from the Supervisory Body. It must be considered that in Europe there are not enough Conformity Assessment Bodies having all the skills (and the competent auditors) to carry on the audit on ETSI TS 119 461, as well as enough laboratories to carry on the security tests on the components (biometric, PADs, etc). This can cause a rush to the audit, overwhelming the effective capability of CABs to serve all the market, with negative impacts on the quality of the audit itself and creating unfair disadvantages to the QTSPs that won't be able to be audited, despite being <i>de facto</i> in full compliance. In addition, because not every QTSP will be in the position to undergo the audit on time, there can be serious impacts on the capability of existing QTSPs to carry on the current processes, especially when the issuance of a certificate is integrated into an onboarding process, typically for a Bank.	Entry into force of the IA shall be postponed not before 30 months from the publication, leaving time to CABs and laboratories to be prepared, and to QTSPs to adapt their processes and undergo the audit.

ANNEX



article	Comment	Proposed solution
(4) 8.3.3 Validation of physical identity document – VAL-8.3.3-21: The effectiveness of the measures for complying with the requirements VAL-8.3.3-02X, 4X, 4A, 4B, 4C, 5X, 5A, 5B, 5C, 7A and 12X, shall be tested by an accredited laboratory or a national competent authority, whenever they are designated, at the latest before 21 May 2026 and then be repeated every second year.	This requirement impacts on the standard and impose an obligation targeted only at QTSPs and excessively burdensome and disproportionate to the concrete risk, undermining the competitiveness and speed of innovation of eIDAS providers. It should be removed. The scope of testing by accredited laboratories should be limited to strictly technical aspects, such as certifications for IAD/PAD functionalities. Expanding laboratory certification to broader components would not be proportionate, especially considering the current limited capacity of accredited laboratories across Member States. Conformity Assessment Bodies (CABs) have consistently guaranteed high levels of assurance and compliance for over 270 QTSPs without additional certification layers. The testing process is long and cumbersome, taking more than 1 year time, in addition to the time needed by the QTSP to develop, or select and integrate, the necessary technologies. Moreover, in Europe there are not enough laboratories capable to carry on the tests, so there is a strong chance that the full testing process will not be completed before the deadline of 21 May 2026. In addition, shall be noted that VAL-8.3.3-02X relates to the requirements for validation of physical identity document. The examples provided in NOTE 2 thereto, of how these requirements shall be fulfilled, namely by certification under ISO/IEC 30107-1 and -3 (for PAD) and under TS 18099 (for IAD) shall not be mandatory, as these standards relate to biometrics. These standards settle injection and presentation attacks in the context of biometric identification and authentication process only. It is not meant to protect against presentation or injection of other streams, i.e. of an ID document. In this respect it is not possible to achieve certification by a laboratory for injection attacks under TS 18099 and thus the requirement under VAL-8.3.3-02X cannot be fulfilled.	The optimal choice is to erase this additional requirement to the standard. Alternatively, other means for satisfying VAL-8.3.3-02X shall be provided, such as penetration test reports, considering that the requirement is concretely not achievable. In any case, the entry into force of the entire IA, shall be postponed not before 30 months from the publication, leaving time to CABs and laboratories to be prepared, and to QTSPs to adapt their processes and undergo the audit and tests. It's necessary to clarify what "National Competent Authorities" refer to, if the eIDAS SBs, the NCA for NIS2 or the certification authority for CABs.

article	Comment	Proposed solution
(5) 8.4.2 Capture of face image of the applicant – [CONDITIONAL] BIN-8.4.2-04B: If the identity proofing targets Baseline LoIP, the biometric injection attack detection means shall be tested by an accredited laboratory according to TS 18099 [5] level Substantial (level 2) at the latest before 21 May 2026. – [CONDITIONAL] BIN-8.4.2-04C: If the identity proofing targets Extended LoIP, the biometric injection attack detection means shall be tested by an EN 2 EN accredited laboratory according to TS 18099 [5] level High (level 3) at the latest before 21 May 2026. – – BIN-8.4.2-07X: The PAD means shall be evaluated by an accredited laboratory according to ISO/IEC 19989-3 [6] at the latest before 21 May 2026.	Same as above	Same as above

article	Comment	Proposed solution
ETSI 119 461 v 2.1.1 standard, § 9.2.5. [CONDITIONAL] If the identity proofing is based on the use of a digital signature with a certificate, the following requirements apply. USE-9.2.5-01: Attribute collection shall be according to the requirements of clause 8.2.2.1 of the present document. USE-9.2.5-02: Collection of evidence shall be according to the requirements in clause 8.2.5 of the present document. [CONDITIONAL] USE-9.2.4-02A: If Baseline LoIP is targeted, requirement COL-8.2.5-03X shall apply. [CONDITIONAL] USE-9.2.4-02B: If Extended LoIP is targeted, requirement COL-8.2.5-03A shall apply.	The ETSI TS 119 461 standard recalled by the implementing act, introduces the requirement that the identity proofing based on a previous qualified certificate shall be restricted only to the certificates issued in compliance with the new Baseline level of identity proofing, set by the standard itself. This creates severe issues with the process of using the existing certificates, considering that only certificates issued after the entry into force of the IA itself could be used for a renewal process: this will impact millions of citizens, professionals, entrepreneurs, civil servants that every day rely on a certificate for their relationships.	The entry into force of the entire IA, including this additional requirement to the standard, shall be postponed not before 30 months from the publication, to permit the diffusion of new Qualified Certificates issued in compliance with the standard, and apply the requirement without harming the functioning of the digital single market. The act should clarify that the new regime is applicable only to the certificates issued after its entry into force, and that the existing set of certificates used in the Single Market continues to be compliant and completely valid.

In conclusion, we appreciate the opportunity to provide our detailed comments and feedback on the proposed Commission Implementing Decisions. We believe that our insights will contribute to the effective functioning of the Digital Single Market and support the continued excellence of European market.

For any further contributions or discussions, please feel free to contact us at:

European Signature Dialog (ESD) Email: office@european-signature-dialog.eu

We look forward to continued collaboration with the European Commission to ensure a secure, interoperable, and innovative trust services ecosystem.

Thank you for your attention and consideration.



Hackhofergasse 5/16

A-1190 Vienna

phone: +43 676 940 9309

office@european-signature-dialog.eu