



Hackhofergasse 5/16
A-1190 Vienna
phone: +43 676 940 9309

office@european-signature-dialog.eu

ZVR-nr: 579746942

Comments on AML CDD RTS Article 7 – Verification measures conducted on a non-face-to-face basis

The European Signature Dialog (ESD) brings together leading companies servicing over 250 million users in their everyday use of qualified trust services across Europe, fostering secure and trustworthy digital interactions in line with the highest EU standards. As the recognised interlocutor for European and national institutions — including the European Commission, Parliament, and Council — ESD contributes actively to shaping the European digital trust ecosystem.

Against this background, ESD welcomes the opportunity to provide comments on the Draft Regulatory Technical Standards (RTS) adopted under Article 28(1) of the AML Regulation concerning customer due diligence (CDD), in particular with regard to verification measures conducted on a non-face-to-face basis.

Given the increasing convergence between the EU's digital identity framework under Regulation (EU) No 910/2014 (eIDAS) and the AML/CFT framework, ESD considers it essential to contribute the perspective of Qualified Trust Service Providers. All ESD members are listed on the EU Trusted List and operate under strict compliance with EU legislation, in particular the eIDAS framework.

ESD members bring extensive operational experience in the deployment of secure remote identification and digital onboarding solutions across multiple Member States. This practical expertise underpins the observations set out below.

General Comment on Article 7(1)

We strongly support the explicit reference to electronic identification means meeting the requirements of Regulation (EU) No 910/2014 (eIDAS), at assurance levels "substantial" or "high", as well as to relevant qualified trust services.

It is important that the RTS fully recognise and promote the advantages associated with the use of recognised and evaluated eID schemes, European Digital Identity Wallets, and qualified trust services under eIDAS. These instruments provide:

1. Harmonised assurance levels across the Union;
2. Legal certainty and cross-border recognition;



3. High standards of security, integrity, and auditability;
4. Strong supervisory and conformity assessment frameworks.

Encouraging the use of these tools fosters interoperability, enhances trust in digital onboarding processes, and reduces fragmentation in supervisory expectations across Member States.

Comment on Article 7(4) in light of Article 7(3)

With specific reference to Article 7(4), and taking into account the detailed safeguards listed in Article 7(3), particularly in light of the continuously evolving technological landscape and the increasing sophistication of digital fraud techniques, we consider that further clarity could be beneficial regarding how obliged entities may demonstrate compliance with the prescribed requirements to their competent authorities. Ensuring robust, resilient and auditable identification mechanisms is essential to effectively mitigate emerging fraud risks with possible systemic risks while maintaining trust in non-face-to-face onboarding processes.

In particular, while the draft RTS appropriately sets functional and outcome-based requirements (e.g., integrity and confidentiality of communication, biometric consistency checks, quality of captured data, secure storage and time-stamping), obliged entities would benefit from wording that explicitly acknowledges the possibility of relying on recognised technical standards to evidence compliance.

In continuity with the EBA Guidelines on the use of Remote Customer Onboarding Solutions (EBA/GL/2022/15), which already provide an important supervisory benchmark in this area, ETSI TS 119 461 represents the most up-to-date European technical standard specifically addressing remote identity proofing and remote identification methods, and therefore constitutes an appropriate, technically robust and state-of-the-art reference framework and is already referenced in other European regulatory acts, while fully preserving the principle of technological neutrality.

In particular, ETSI TS 119 461:

1. Provides auditable requirements for remote identity proofing;
2. Aligns with eIDAS assurance principles;
3. Supports both a Baseline Level of Identity Proofing (LoIP) and an Extended LoIP, allowing obliged entities to calibrate controls in line with their risk assessment and risk appetite.

Recognising ETSI TS 119 461 (either at Baseline or Extended LoIP, depending on the risk analysis performed by the obliged entity) as an acceptable reference standard would ensure consistency with the 2022 EBA Guidelines and provide competent authorities with a clear and objective benchmark for ex-post supervisory assessment.



Such clarification would not limit technological neutrality, as the RTS would remain outcome-based, but would provide a structured and harmonised pathway for demonstrating compliance.

Proposed Amendment to Article 7(4)

We reiterate our support for the objective of strengthening secure non-face-to-face verification within the AML/CFT framework.

In particular, we respectfully propose that Article 7(4) be amended to explicitly recognise the possibility for obliged entities to demonstrate compliance with paragraphs 1 to 3 by relying on recognised European or international technical standards.

For instance, Article 7(4) could be reformulated as follows (additions in bold for ease of reference):

*"Obligated entities using remote solutions shall be able to demonstrate to their competent authority that the remote verification solutions they use comply with the requirements of this Article. **Such compliance may be demonstrated, inter alia, through adherence to recognised European technical standards that ensure equivalent safeguards and assurance levels, including where applicable the levels defined in Regulation (EU) 2024/1183 for trust services.** They shall also be able to justify why the customer could not be verified through the means referred to under Article 22(6) of Regulation (EU) 2024/1624."*

This amendment would:

1. Preserve technological neutrality and outcome-based regulation;
2. Strengthen legal certainty for obliged entities;
3. Facilitate supervisory convergence across Member States;
4. Ensure continuity with the EBA Guidelines on Remote Customer Onboarding (EBA/GL/2022/15), which already acknowledge structured and auditable frameworks for remote identity proofing.

For further information, please feel free to contact us: office@european-signature-dialog.eu