EBOOK

Guide to EU KYC Requirements

What Does the Future Look Like?

ENTRUST

SECURING A WORLD IN MOTION

Executive Summary

Evolving fraud and the increased expectation of digital access have resulted in a wealth of new identity verification technologies. These digital technologies enable businesses to identify customers anytime, and anywhere — creating better alignment with their customers' expectations and digital transformation initiatives.

European regulatory standards and directives are rapidly evolving to support these new methods of identity verification, but varying speeds of adoption and mixes of national and EU regulations have resulted in a notoriously complex and fragmented regulatory landscape.

Companies subject to EU anti-money laundering (AML) regulation, including those offering or aspiring to offer regulated products, such as credit cards or loans, urgently need to ensure their identity verification (IDV) vendor stays ahead of European identity standards and best practices. These new standards will be critical to protecting themselves and their customers against sophisticated fraud, retaining a competitive advantage, and pursuing growth ambitions in the EU.

For IDV vendors, the ETSI standard TS 119 461, “Policy and security requirements for trust service components providing identity proofing of trust service subjects,” is the lead standard.

For IDV vendors, the ETSI standard TS 119 461, “Policy and security requirements for trust service components providing identity proofing of trust service subjects,” is the lead standard. Although this standard was initially created for use in the context of eID and trust services, it is now used as a reference in other areas such as financial services.

AML regulation permits three approaches to identity verification for performing customer due diligence (CDD) as part of know your customer (KYC):

1. Electronic identification (eID)
2. Identity verification that conforms to ETSI technical standards
3. National accredited schemes

Each Member State accepts different variations of the above. We expect that when future AML regulation comes into force, national accredited schemes will be less prevalent as there is broader harmonization across Europe, which is why conforming to EU technical standards will be essential in enabling cross-border growth.

The “Brussels effect” will also likely influence the rest of the world. Similar to the global impact of the General Data Protection Regulation (GDPR), European standards, particularly those concerning consumer safety or data privacy, tend to set the bar with other markets looking to harmonize their standards or make them interoperable with those adopted by the EU. Partnering with a vendor that operates globally and adheres to EU standards is a way to help future-proof and protect your business.

Table of Contents

How Have Identity Verification Technologies Evolved?

Identity verification in Europe is undergoing a period of intense transformation. In 10 short years, it has evolved from face-to-face verification in stores and branches to live video calls, to identity document and biometric verification that can be conducted remotely and processed automatically.

But Member States have adopted different technologies at different paces, meaning there is a mix of national eID schemes in place (and each using different methods to onboard users) alongside local and global identity verification providers. Large pan-EU businesses frequently must use multiple local providers with varied performance to comply with a patchwork of national standards. Some markets are experiencing widespread adoption of eIDs, some have competing schemes, and others are limited to in-person verification.

In a political union where freedom of movement is guaranteed, the digital ecosystem is still playing catch-up. Institutions that serve these communities need to have confidence that they can have the same level of assurance no matter who they onboard and which Member State they come from. This is especially important for companies that must conduct customer due diligence to comply with KYC and AML requirements.

Which Regulations and Standards Impact KYC?

Identity verification is a critical component of KYC and is impacted at the EU level by various laws and standards.

Many of these are currently in various states of review or amendment, in a push to streamline and future-proof the way regulated businesses can verify customer identity across the EU. This section outlines the key laws and relevant developments.

EU AML Directives

Today

The EU AML Directives set out the basis for KYC by financial institutions. Article 13(1)(a) of the current EU AML Directive (2015/849) allows for remote KYC in three ways:

eID: A digital proof of identification.

Qualified Trust Services: Services issued by Qualified Trust Service Providers (QTSPs) that meet EU standards, including electronic signature with a qualified certificate, electronic seals with a qualified certificate, and electronic registered delivery services.

Nationally Accredited Identity Verification Solution: Identity verification solutions that are approved by local country-specific regulatory bodies, such as SEPBLAC in Spain.

In the future

The AML regulation is being updated, and changes are likely to come into force towards the end of 2026. The new package of measures will soon include a new Directive (AMLD6) and a new Regulation (AMLR).

AMLD6 builds upon AMLD5 and is the 6th Anti-Money Laundering Directive to prevent financial crime, including money laundering and terrorist financing. Among other things, it expands the scope of offences, gives greater transparency, and strengthens information sharing.

Although not finalized, AMLR aims to standardize requirements for KYC across the EU and increase the level of cross-border acceptance. While directives and regulations are both legal instruments, directives are transposed into national law, giving Member States discretion on how to implement them domestically, whereas regulations are directly applicable at a national level.

The EU institutions need to agree on the final measures, but it may limit acceptable forms of KYC to in-person, eIDs, or qualified trust services.

Electronic Identification, Authentication, and Trust Services (eIDAS)

Past

The eIDAS framework promotes harmonization of identity proofing and trust services across EU Member States to promote high levels of assurance, interoperability, and security. EU businesses and service providers engaging in services covered by eIDAS must comply with its standards.

Effectively, eIDAS is a framework for secure electronic transactions in the EU. It covers:

eID schemes: Ensuring that eID schemes in the EU are interoperable, secure, and accepted across Member States.

Trust services: Creating, verifying, and preserving electronic signatures, seals, electronic timestamps, electronic delivery services, and website authentication certificates.

Authentication: Promoting a high level of assurance and the use of strong authentication for eIDs, identity proofing methods, and trust services.

Mutual recognition: Ensuring that solutions meeting eIDAS standards are accepted across all Member States.

The wallet is designed to enable storage of digital credentials, eIDs, and qualified electronic signatures with a privacy-first approach.

Present and future

A new version of eIDAS came into effect in 2024. eIDAS 2.0 expands the original regulation's scope to:

1. Include a new type of electronic trust service: the issuance of **qualified electronic attestation of attributes**. Attributes are data related to an identity, such as tax rate or professional qualification, that could be used for digital transactions or access to government services.

2. Further harmonization of the existing regulation for qualified trust service providers.

3. Mandate that every EU citizen has access to a digital wallet and sets out a technical framework for Member States. The wallet is designed to enable storage of digital credentials, eIDs, and qualified electronic signatures with a privacy-first approach. It also requires all Member States to offer at least one eID to their citizens.

European Telecommunications Standards Institute (ETSI)

Today

ETSI is a non-profit organization, based in France, that sets technical standards for a wide range of ICT-related systems and services. The EU officially recognizes it as a European Standardization Organization and promotes best practices in assurance, interoperability, and security. While the specification is known for technical standards audits, it also assesses the maturity of the identity provider, ensuring it has robust processes in place to support its customers.

In 2021, ETSI released a technical standard for IDV (ETSI TS 119 461). It refers to another ETSI standard (ETSI EN 319 401) to support the eIDAS Regulation — in short, eIDAS sets the framework, and refers to ETSI standards to define the technical specifications that IDV solutions should adhere to.

In the future

ETSI standards are periodically reviewed and updated to better reflect the needs of businesses and their customers, considering the security context and industry needs. They are becoming increasingly integral to best practices in the IDV space.

European Banking Authority (EBA) Guidelines

Today

The EBA has produced several relevant guidelines for financial services on outsourcing. Most recently, the EBA issued guidance on remote customer onboarding solutions. These guidelines aim to provide a more harmonized framework across the EU on the implementation of AML rules on credit and financial institutions.

Increasingly, these guidelines reference external industry standards, in particular ETSI, as evidence of good practice, further highlighting the advantages of partnering with ETSI-compliant IDV providers.

In the future

The EBA updates its guidelines periodically.

What Does This Mean for Identity Verification?

Currently, a patchwork of different approaches to KYC is in place across the EU. Although the AML frameworks brought a degree of coordination, Members have transposed them differently at different speeds. In turn, there are several approaches to onboarding adopted across the EU. The onboarding approach deployed by various EU countries has evolved with each of the three following methods being used today:

Live video calls
(attended remote identity proofing)

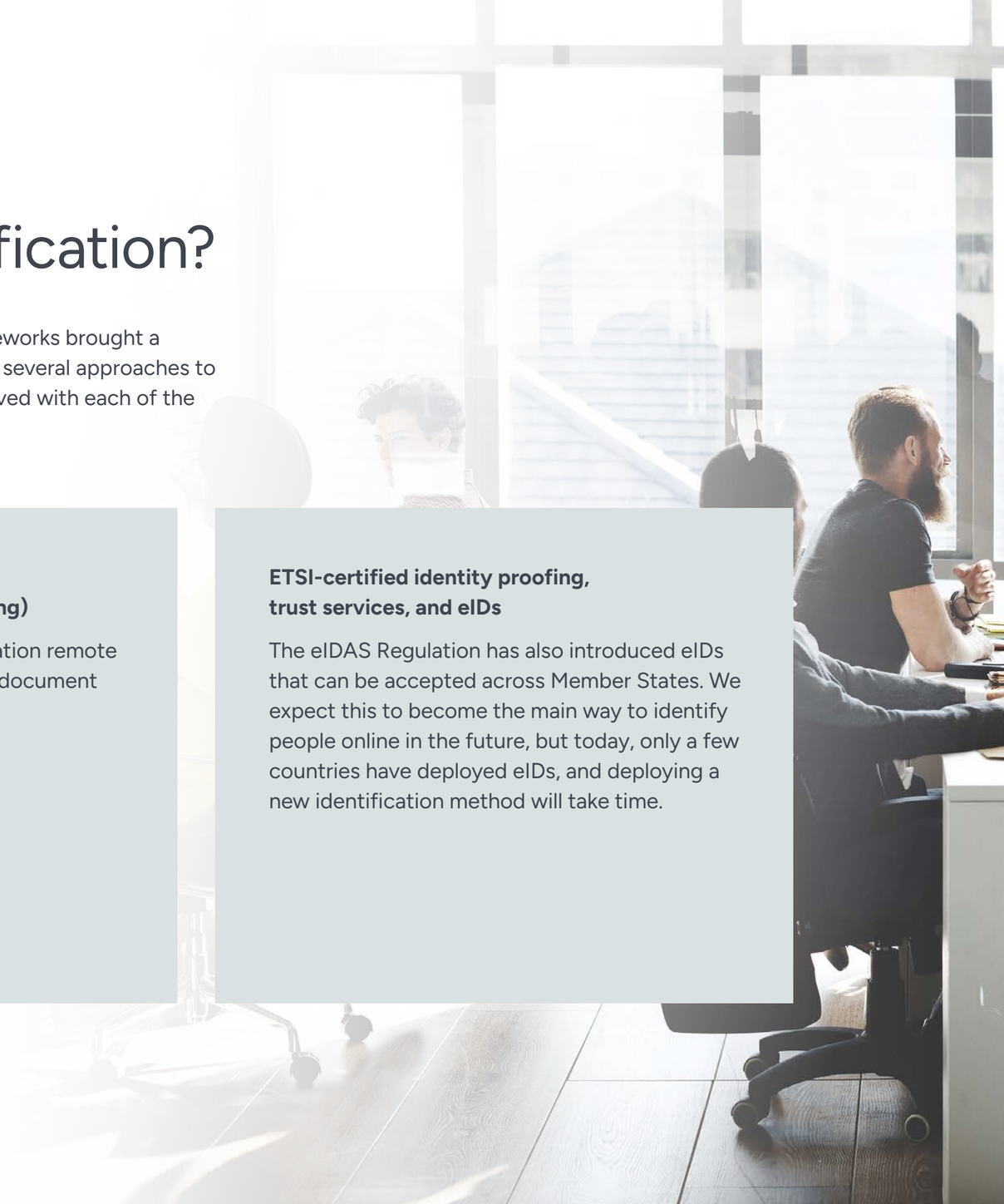
Member States started to adopt live video calls to verify customer identity, as it was the closest solution to the existing physical KYC that had happened in a store or branch. This is still a requirement by BaFin, the regulatory body in Germany, but we expect that an eIDAS-compliant alternative, such as eID or a solution based on a trust service such as QES, will be a more desirable and lower-friction alternative.

Remote IDV
(unattended remote identity proofing)

Member States adopted next-generation remote IDV, typically relying on AI-powered document and biometric verification.

ETSI-certified identity proofing, trust services, and eIDs

The eIDAS Regulation has also introduced eIDs that can be accepted across Member States. We expect this to become the main way to identify people online in the future, but today, only a few countries have deployed eIDs, and deploying a new identification method will take time.



While AML regulation means there are currently three options for approved identity proofing and trust services in the financially regulated space, in practice, at a national level, the rules can be more complex. For example:

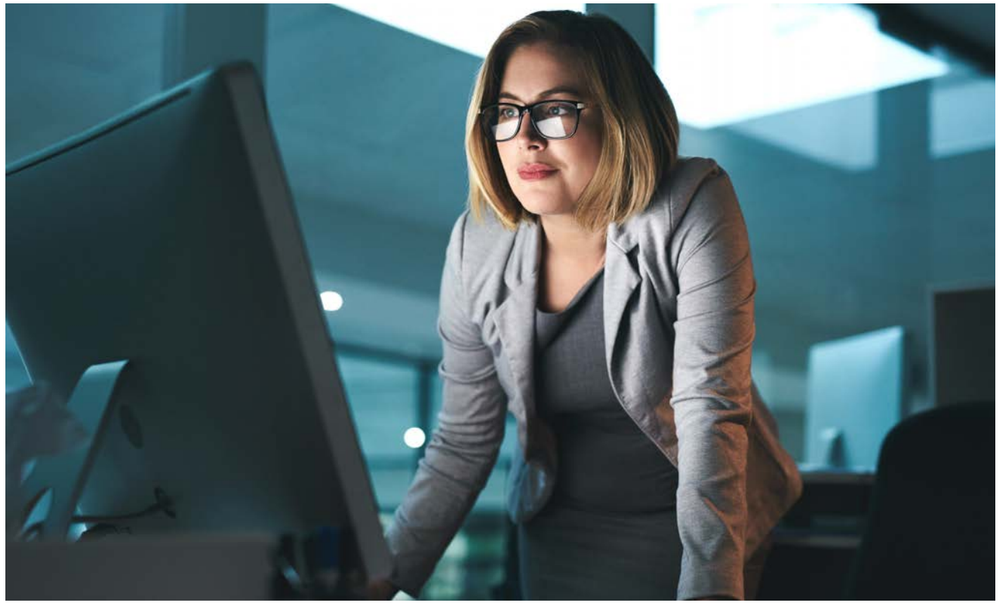
1. France created a nationally accredited IDV framework prior to the publication of ETSI TS 119 461. This meant France created its own remote IDV standard known as “PVID” by which to judge the technical standards of solutions.

2. Germany typically requires both real-time live video (which tends to be costly and inconvenient for both business and customer) or to adopt a micro-payment solution if using a qualified trust service.

The ETSI standard for identity proofing is not yet consistently adopted across countries, although it is frequently referenced as a best practice for identity standards. It is variously:

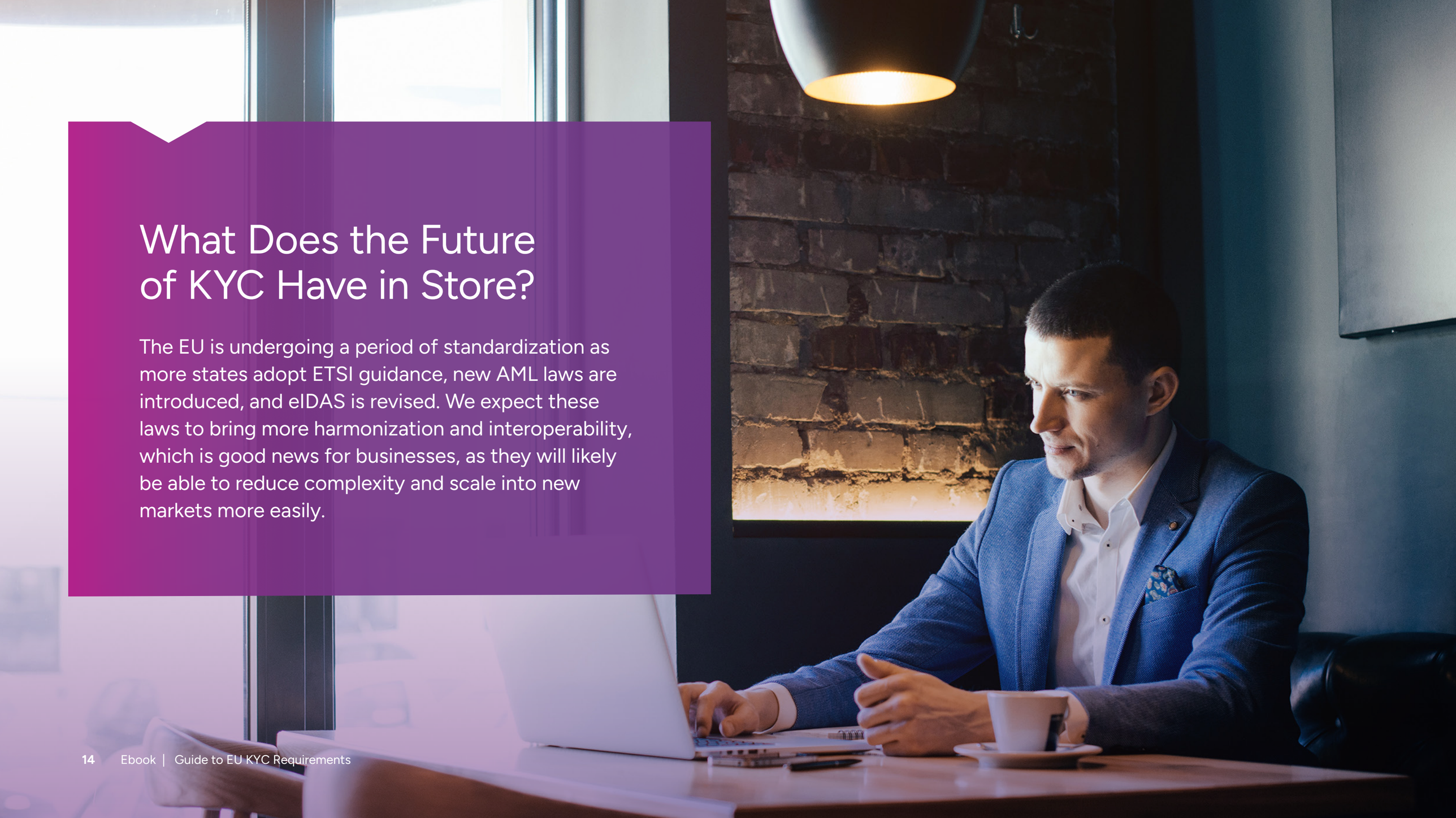
- Adopted in local regulation
- Adopted with additional local requirements
- Referred to as a best practice, but not required
- Not adopted at all (with other accredited ID schemes taking its place)

Even in states that have not adopted ETSI identity standards, businesses can and should consider it a prerequisite when choosing identity solutions — both because it is globally perceived as credible and seen as a gold standard, and it means they don’t risk needing additional partners when expanding into new markets. It also grants peace of mind that reputational and fraud risk is mitigated. Choosing a global partner that conforms to local standards allows for consolidation in a complex ecosystem.



What Does the Future of KYC Have in Store?

The EU is undergoing a period of standardization as more states adopt ETSI guidance, new AML laws are introduced, and eIDAS is revised. We expect these laws to bring more harmonization and interoperability, which is good news for businesses, as they will likely be able to reduce complexity and scale into new markets more easily.



AMLR Proposals

New AML laws currently being introduced will change how users can be onboarded for financial services. The Commission's draft AMLR proposal, published in the summer of 2021, Article 18(4), limits compliant KYC to the following:

- The submission of an identity document, passport, or equivalent, along with the acquisition of information from reliable and independent sources, whether accessed directly or provided by the customer.
- The use of electronic identification methods and relevant trust services as outlined in Regulation (EU) 910/2014.

Although not finalized, AMLR is expected to standardize KYC requirements across the EU and increase the level of cross-border acceptance. We're likely to see significant changes in how remote onboarding is conducted. In particular, the rules specify that eIDs and trust services will be valid methods for remote onboarding. The proposal is also intentionally aligned more closely with eIDAS requirements, which means that solutions built on these mechanisms will become increasingly prominent and important.

eIDAS 2.0

eIDAS 2.0 introduces a new framework focused on electronic IDs (eIDs), digital wallets, and qualified trust services. Among other mandates, it requires each EU Member State to offer eIDs and digital wallets to its citizens and mandates that all entities requiring Strong Customer Authentication — including banks and other financial institutions — accept them.

The regulation officially went into effect in the second half of 2024, following the publication of an Implementing Act that outlined the minimum technical specifications, standards, and procedures. Existing ETSI standards already cover many elements of eIDAS 2.0's requirements, and the Implementing Act is expected to formally incorporate these technical components to ensure consistency and interoperability.

What Are the Considerations for Business Conducting KYC?

Long Term

Businesses using KYC solutions will need to ensure their solutions comply with the rules and technical standards outlined in the latest EU-wide laws and regulations. There will likely be increased emphasis on the use of qualified trust services — such as qualified electronic signatures (QES) — as essential for achieving KYC compliance.

Short Term

However, once the new AML regulation is fully in effect — likely by the end of 2026 — national requirements are expected to align more closely with EU-wide standards. As a result, businesses will need to evaluate the available solutions and begin assessing identity partners that can support both their short-term needs and long-term compliance goals.

Businesses evaluating new providers should take a long-term view when selecting a partner. It's essential to choose one that is committed to meeting the new wave of regulatory requirements. Clear roadmap commitments and a proven track record of delivering solutions that align with leading industry standards will help avoid costly reintegration efforts down the road.

Businesses evaluating new providers should take a long-term view when selecting a partner. It's essential to choose one that is committed to meeting the new wave of regulatory requirements.

What To Look for in a Long-Term Identity Partner

The ideal partner needs to support compliance and offer effective fraud prevention, while also delivering on customer expectations related to the digital onboarding experience. Two key metrics that help inform that decision are:

1. **Product performance:** The ability of a solution to accurately verify a customer identity while providing an excellent user experience with high pass rates and quick turnaround times.

2. **Legal and standards compliance:** Ensuring that solutions comply with national and EU rules. ETSI technical standards for IDV are becoming increasingly integral to this and will likely become fundamental to compliance.

Future-Proofing With ETSI and QES

Businesses selling or wishing to start selling regulated products should partner with established global providers that conform to ETSI technical standards. Even now, an ETSI-compliant IDV and QES process is one cross-border criterion that is underpinned by the regulatory framework in every EU country. In the future, it will likely become a requirement across all Member States.

ETSI technical standards are designed to meet the highest levels of assurance, security, and interoperability — signifying premium performance and risk mitigation. ETSI-certified vendors are carefully scrutinized by auditors, who review not only the technology itself but also the operations and practices within the company.

The EU may be leading the way with respect to IDV standards, but we expect other markets will similarly level up regulations in the coming years.

How Can Entrust Identity Verification Help?

Entrust Identity Verification offers a suite of verifications, no-code orchestration, and AI-driven analysis to enable secure and compliant identity verification and access control.

Navigating EU KYC Compliance With Entrust

Entrust is certified to the following standards, which means institutions and businesses can use Entrust's ETSI-certified identity verification in any EU market in combination with other compliant products or trust services to help achieve local regulatory compliance:

- Remote identification service component (according to Regulation (EU) 910/2014 Art. 24.1d)
- UK Trust Framework (High Confidence Profile H1A)
- Navigate new compliance requirements

Additional applicable standards and regulations:

- ETSI TS 119 461 v.1.1.1
- ETSI EN 319 401 v2.3.1
- Commission Implementing Regulation (EU) 2015/1502
- Romanian-specific regulation (Decision no. 564/2021)

Please note that this paper does not constitute legal advice, and it should not be relied on as such. You are advised to seek independent legal advice where necessary.

Get in touch | Take our interactive tour

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION