eIDAS 2.0 — Executive Overview

eIDAS 2.0 is the 2024 update to the EU's digital identity and trust-services law, a.k.a. eIDAS (electronic Identification, Authentication and Trust Services).

It establishes the European Digital Identity (EUDI) Wallet so people and businesses can identify themselves, share verified information (attributes), and create legally-binding electronic signatures and seals across borders.

Beyond the Wallet, eIDAS 2.0 creates a common EU-wide trust layer so customers, suppliers, and staff can prove who they are and what they're entitled to.

For organisations, that means fewer manual checks, faster onboarding and procurement, legally reliable e-signatures and seals, and simpler compliance in regulated journeys.

It combines user control and data-minimisation with certified security, giving you a predictable, EU-wide way to cut friction and fraud while scaling digital services.

Mandatory acceptance

The regulation entered into force on 20 May 2024. The regulation mandates acceptance of at least one EUDI Wallet in all 27 European member states.

- When a **public-sector** online service requires eID/authentication, it must accept the EUDI Wallet and must accept the wallet no later than 36 months after the wallet Implementing Acts entered into force.

- **Very large online platforms** (like Amazon, AliExpress, Booking.com, Facebook, Instagram, TikTok, X, LinkedIn) that require user authentication under the EU Digital Services Act (DSA), must also accept the wallet on the user's request.

- The same is true for **Private relying parties** (except micro/small enterprises) in sectors where strong user authentication is required by law or contract (covering transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education and telecom) must accept the wallet no later than 36 months after the wallet Implementing Acts enter into force.

In short, the deadline for the public and semi-public sector is 31 December 2026 and for the private-sector 31 December 2027.

Business benefits

Although the EUDI wallet enforces mandatory acceptance by both public and private organizations, it also comes with significant business benefits.

Onboarding & KYC/AML

Accepting the EUDI Wallet streamlines onboarding and checkout by replacing scans and forms with verified information and built-in strong authentication.

- It reduces fraud and KYC/AML overhead by relying on certified wallets and qualified trust services, giving you audit-ready evidence.
- EU-wide, portable signatures and electronic attestations accelerate procurement, contracting, and cross-border service access.
- More about KYC/AML later, but bottom line: lower CAC and OPEX, lower abandonment, higher conversion, faster time-to-revenue.

Customer & workforce onboarding

Reusable, high-assurance identity and **selective disclosure** (e.g., “over-18”, “address verified”) cut form-filling and abandonment while improving KYC/AML assurance. Independent analysts expect lower drop-off and process costs as wallets standardise strong authentication and data-minimised proofs.

Cross-border signing & approvals

EUDI Wallets enable **qualified electronic signatures (QES)** and seals that carry legal effect EU-wide. The Commission also mandates **free QES for non-professional use**, useful for consumer-side flows and long-tail B2C agreements.

Procurement & supplier management

Harmonised **electronic attestations of attributes** (e.g., company registration, professional and business certifications, tax status) shorten vendor onboarding, tendering, and compliance checks, by replacing document uploads and manual verification with cryptographically verifiable proofs. Commission materials and independent briefings outline business-wallet scenarios for tendering and cross-border trade.

Payments & SCA

Wallet-based strong customer authentication (SCA) and verified attributes (e.g., ID, age, residency) reduce fraud and checkout friction. Payments experts tracking the pilots argue wallets could become an **additional SCA method** and streamline card/account flows: an emerging, but material, assumption to design against.

Risk, compliance & security posture

Wallets are subject to an **EU cybersecurity certification scheme** coordinated with ENISA. That gives CISOs and auditors a common baseline for acceptance decisions and vendor due-diligence.

KYC / AML / CTF and eIDAS 2.0

Regulatory acceptance of digital ID for CDD.
The new EU Anti-Money Laundering Regulation (AMLR, 2024/1624) explicitly tells obliged entities they may verify customers using electronic identification means meeting eIDAS “substantial” or “high” assurance, and, where eID isn’t available, via relevant qualified trust services. Recitals make clear these eIDAS tools should be “taken into account and accepted” in CDD, and Article-level text allows verification using such means, including for beneficial owners, with records retained accordingly. In short: using an eID/eIDAS wallet flow can satisfy CDD identity verification, provided you keep risk controls and evidence.

How the EUDI Wallet fits.
eIDAS 2.0 introduces the EUDI Wallet as a certified, high-assurance way to present verified attributes and create qualified signatures. The Commission’s materials position wallets as a reliable way to meet KYC needs, especially for cross-border onboarding, with user-controlled, selective disclosure of attributes. AMLR then dovetails by recognising eIDAS identification and qualified trust services as acceptable verification methods for obliged entities.

Practically, a wallet-based flow can deliver the required identifying data with auditability and lower friction. You remain responsible for validation and AML decisions, but under eIDAS 2.0 the accuracy liability for qualified electronic attestations has now shifted from you to the Qualified Electronic Attestation of Attributes (QEAA) issuer.

What you can rely on (and what you can’t).
A wallet or eIDAS credential proves authenticity and integrity of attributes from trusted issuers; it does not replace the risk-based AML program. You still need screening (sanctions/PEP), customer risk assessment, and ongoing monitoring. This is consistent with FATF guidance on digital ID, which encourages using assured digital identity within a risk-based framework for CDD.

Attributes and assurance for CDD.
AMLR mandates that AMLA will specify the attribute set electronic identification means/qualified trust services must expose for standard, simplified, and enhanced due diligence. Expect convergence on a predictable set (name, DoB, address; for legal entities: registration, legal form, representatives, UBOs), verifiable at eIDAS assurance levels and with revocation/status checks. Until AMLA issues the detailed list, map your flows to AMLR Article 20 CDD requirements and capture verification evidence from the wallet transaction.

KYB/KYS (business side).
For organisations, the same pattern applies: use authoritative electronic attestations of attributes (e.g., company registration, tax/VAT IDs, roles/mandates) and, where available, vLEI credentials, to bind legal entities and official roles. This shortens supplier onboarding and periodic reviews while keeping cryptographic proof trails. The Commission’s European Business Wallet initiative will formalise these patterns further.

Record-keeping and reliance.
AMLR requires you to retain CDD evidence, including data obtained through electronic identification means, and clarifies conditions for reliance on other obliged entities (with AMLA to issue additional guidelines). If you rely on a third party’s wallet-based verification, ensure you can obtain the underlying identification data and verification evidence within the required timeframes.

Remote onboarding controls.
EBA’s remote onboarding guidelines remain your operational blueprint: perform liveness/anti-spoofing, bind the identity to the user/device, capture logs and artefacts, and embed risk triggers for escalation. Wallet-based flows can simplify the evidence chain while meeting these controls.

Crypto/Travel Rule context.
For CASPs, AMLR extends full AML/CFT obligations and prohibits anonymous accounts; the EBA’s ‘Travel Rule‘ guidelines apply from 30 December 2024. Wallet-verified attributes can help populate originator/beneficiary information and mitigate self-hosted-wallet risks, but CASPs still need transfer-level checks and monitoring.

Signatures and consumer consent.
eIDAS 2.0 also makes qualified e-signatures free of charge for non-professional use via the wallet, which is useful for capturing consent and executing contracts during onboarding without extra signature fees on the customer side.

Some of the tech components

1. **Enable wallets for sharing.**
   Provide **EUDI Wallet support**, specifically the European Business Wallet to enable sharing of organisational credentials. If your customers or suppliers can't (or don't want to) run their own, consider offering a managed (custodial) business wallet yourself.

2. **Issuance endpoint for credentials.**
   Support **OpenID for Verifiable Credential Issuance (OID4VCI)** to issue/refresh credentials to EUDI and Business Wallets; implement Credential Offer, pre-authorized code / authorization code flows, and expose issuer metadata/JWKs plus a status/revocation mechanism.

3. **Protocol endpoint for presentations.**
   Support **OpenID for Verifiable Presentations (OID4VP)** for remote and cross-device data sharing flows; this is the ARF's profiled protocol for credential exchanges.

4. **Trust & certificate checks.**
   Support validating trust via the **EUDI trust model**: consult trust registries/trusted lists, verify issuer certificates, and check revocation; handle wallet attestation and device binding where required.

5. **Attestation formats.**
   Be ready to verify **W3C Verifiable Credentials** and **SD-JWT-VC** (optionally plus ISO 18013-5/-7 for mDL-style in-person flows) as profiled in the ARF.

6. **Signature/seal verification.**
   For signed documents and approvals, implement verification of **qualified e-signatures/e-seals** issued under eIDAS (ETSI-conformant), including timestamp and status checks.

Some reference sources

- **EUR-Lex** (law & definitions): Regulation (EU) 2024/1183 amending 910/2014; in force since 20 May 2024. EUR-Lex

- **EPRS briefing** (executive summary & timeline). European Parliament

- **European Commission** (EUDI overview, benefits, timelines; masterclass/use cases; QES note). European Commission European Commission Digital Strategy - European Commission

- **ENISA** (wallet cybersecurity certification context). EU Cybersecurity Cert ENISA

- **Independent analysis**: KuppingerCole (wallet impact & adoption); Wavestone (sector use cases); Edgar Dunn (payments implications). KuppingerCole RiskInsight edgardunn.com