eIDAS 2.0 Implementation Guide

A practical guide for organisations implementing eIDAS 2.0 qualified trust services – covering QTSP selection, integration, and legal certainty for qualified signatures.

eIDAS 2.0 Implementation Guide: QTSP Selection, Integration, and Legal Certainty for Qualified Signatures

Introduction

With Regulation (EU) 2024/1183 – better known as eIDAS 2.0 – the European Union has fundamentally upgraded its framework for digital identity and trust services. The revised regulation entered into force in May 2024 and obliges every member state to offer its citizens an EU Digital Identity Wallet, while expanding the family of qualified trust services and broadening the obligation to accept them. For organisations, this is both an opportunity and a deadline: qualified electronic signatures carry the same legal effect as handwritten signatures across all member states, wallets will soon arrive at your onboarding flows whether you are ready or not, and regulated sectors such as banking, telecom, and platforms face explicit acceptance obligations. Organisations that treat eIDAS 2.0 as a checkbox risk fragmented tooling, invalid signatures, and failed audits; organisations that implement it well gain faster onboarding, EU-wide legal certainty, and a durable trust infrastructure. This guide walks through what changes, how to select a Qualified Trust Service Provider (QTSP), and how to integrate qualified trust services into daily operations.

1. What Changes Under eIDAS 2.0

eIDAS 2.0 changes the trust landscape in three ways, making digital identity not only more widespread, but also more interoperable and legally binding:

1.1 The EU Digital Identity Wallet

Every member state must provide at least one EU Digital Identity Wallet (EUDI Wallet) to its citizens, residents, and businesses. The wallet holds a verified identity plus attestations of attributes – such as age, diplomas, mandates, or company roles – that users share selectively and free of charge. Crucially, the wallet also enables citizens to create qualified electronic signatures, turning every wallet holder into a potential signer with the highest legal assurance level.

1.2 An Expanded Family of Qualified Trust Services

Alongside the familiar qualified signatures, seals, timestamps, and website certificates, eIDAS 2.0 introduces new qualified services: electronic attestation of attributes, electronic archiving, electronic ledgers, and the management of remote signature creation devices. Providers of these services are audited and supervised, appear on the EU Trusted Lists, and may carry the EU trust mark – giving relying organisations a clear, verifiable standard for whom to trust.

1.3 Acceptance Obligations and a Hard Timeline

eIDAS 2.0 is not optional infrastructure. Very large online platforms and private relying parties in sectors such as banking, financial services, telecom, transport, energy, and healthcare must accept the EUDI Wallet for identification where strong customer authentication is required. With the implementing acts adopted at the end of 2024, the clock is running: wallets must be available by late 2026, and acceptance obligations follow shortly after. Organisations that map their signature and identification flows now avoid a forced migration later.

2. Qualified Trust Services in Practice

Which qualified trust services matter most in daily operations?

2.1 Qualified Electronic Signatures (QES)

A QES is the only electronic signature with the same legal effect as a handwritten signature in every EU member state, and the burden of disproving it lies with the challenger. Use QES for employment contracts, loan agreements, corporate resolutions, and any document where non-repudiation is essential. WeVerify delivers QES through identity verification via NFC-ID capture and selfie-matching, followed by remote qualified signing.

2.2 Qualified Electronic Seals

Where a signature binds a person, a seal binds an organisation. Qualified seals prove the origin and integrity of invoices, extracts, certificates, and system-generated documents – ideal for automated, high-volume document flows.

2.3 Qualified Timestamps

A qualified timestamp proves that a document existed, unaltered, at a specific moment. Combined with seals and signatures, timestamps anchor audit trails and protect evidence against later disputes.

2.4 Qualified Electronic Attestations of Attributes (QEAA)

New under eIDAS 2.0: qualified attestations let users prove a single attribute – over 18, authorised signatory, licensed professional – without revealing their full identity. This is data minimisation by design and will reshape onboarding, mandates, and age-restricted services.

2.5 Qualified Archiving and Electronic Ledgers

Signed documents must remain verifiable for years, often beyond the lifetime of the certificates used. Qualified electronic archiving preserves the legal validity of signatures over time, while qualified ledgers provide tamper-evident records of data and transactions.

2.6 Qualified Website Authentication and Registered Delivery

Qualified website authentication certificates (QWACs) prove who is behind a website, and qualified electronic registered delivery services (QERDS) prove that a message was sent, received, and unaltered – the digital equivalent of registered mail for formal notices and demand letters.

Industry-Specific Examples

Financial Services

Banks and lenders must combine strong identification under WWFT and EU-AML with legally binding contract signing. WeVerify's Qualified ID verifies the customer against the chip of their identity document, after which the loan or account agreement is signed with a QES – one flow, from KYC to binding signature (from the compliance documentation).

HR and Onboarding

Employment contracts signed with a simple click-to-sign are routinely challenged. A QES on the employment contract, created after a one-time identity verification stored in WeVerify's Identity Wallet, gives HR EU-wide legal certainty and cuts onboarding from weeks to minutes.

Public Sector and Regulated Professions

Permits, deeds, and professional attestations demand the highest assurance level. Qualified seals and timestamps make every issued document verifiable by any party in the EU, while QEAAs let professionals prove their authorisation without paperwork.

3. Checklist: Is Your Organisation Ready for eIDAS 2.0?

Use this checklist below to determine where you stand.

Legal & Compliance

- We do not know which of our documents legally require a qualified signature versus an advanced or simple one. *(Recommendation: Map signature levels per document type.)*
- Contracts are signed with click-to-sign or scanned signatures without identity verification.
- We have no policy for accepting the EU Digital Identity Wallet.

QTSP Selection

- Our signing provider is not on the EU Trusted Lists. (Recommendation: Verify QTSP status in the official trusted list before contracting.)
- Identity verification and signing are handled by different, unconnected vendors.
- We cannot verify signatures created by other parties or member states.

Integration & Processes

- Signing is a manual, standalone step outside our CRM or workflow systems. (Recommendation: Integrate qualified signing via API or no-code workflows.)
- Signed documents are stored without qualified timestamps or archiving, risking loss of validity over time.
- There is no audit-ready log of who signed what, when, and after which identity check.

Human Factor

- Legal, IT, and business teams each have a different understanding of eIDAS levels.
- There is no training around qualified signatures and wallet-based identification.

4. Implementation Roadmap for eIDAS 2.0

A pragmatic implementation consists of four steps, expanded with WeVerify's features from www.weverify.com (such as KYC via NFC and selfie, qualified signatures, and API integration).

4.1 Map Your Signature and Identification Flows

Inventory every process where identity is established or a document is signed: onboarding, contracting, mandates, approvals. Classify each flow by required assurance level – simple, advanced, or qualified – based on legal risk and sector rules. This map is the foundation of every decision that follows.

4.2 Select a Qualified Trust Service Provider

Choose a QTSP that appears on the EU Trusted Lists and covers the services you actually need: QES, seals, timestamps, and identity verification in one platform. Assess remote signing capability, supported identification methods (NFC-ID, wallet, selfie-matching), pricing model, and API quality. WeVerify combines qualified trust services with built-in identity verification, legally valid in the EU, Switzerland, UK, and US.

4.3 Integrate Signing Into Daily Operations

Qualified signing only delivers value when it lives inside your processes. Connect signing and verification to your CRM, HR system, or customer portal via API and no-code workflows, so every contract follows the same verified, logged path – and prepare the same endpoints to accept EUDI Wallet identification as it rolls out.

4.4 Preserve Validity and Prove Compliance

Documents must be verifiable, logged, and tamper-evident from the start – and stay that way. Apply qualified timestamps at signing, archive with validity preservation, and build audit-ready logs with timestamps so any regulator, auditor, or court can verify the full chain years later.

Review the map annually: implementing acts, wallet acceptance obligations, and national guidance under eIDAS 2.0 continue to evolve through 2026 and beyond.

5. Conclusion

eIDAS 2.0 is no longer a distant regulation, but an active deadline: wallets must be available across the EU by late 2026, acceptance obligations reach deep into the private sector, and qualified trust services have become the default standard for legally binding digital business. Organisations can no longer afford fragmented signing tools and unverified identities; the solution lies in a mapped signature landscape, a supervised QTSP, integrated qualified signing, and archiving that preserves validity for the long term.

WeVerify offers a proven, unified platform for KYC, KYB, qualified signatures, and secure e-signing – legally valid in the EU, Switzerland, UK, and US. Through PIN-protected data, NFC and selfie verification, no-code integrations, and timestamped audit trails, WeVerify reduces legal risk, accelerates contracting from weeks to minutes, increases conversion rates, and minimizes costs via a pay-as-you-go model without subscriptions. With €50 free credit upon registration, it is simple and cost-effective to start, aligned with eIDAS 2.0 and strict compliance standards.

By combining WeVerify with a clear implementation roadmap and guidance from your legal and compliance teams, organisations can adopt eIDAS 2.0 proactively and confidently. Do not wait until the acceptance obligations strike. Register today at www.weverify.com and build a future-proof trust infrastructure for legally certain, friction-free digital business that protects your organisation and stimulates growth.