European Business Wallets

A Conditional Roadmap for the Single Market, Cyber-Resilience and Accountable Automation

Research manuscript

Dr. Carsten Stöcker

Spherity GmbH

Prepared: 31 October 2026



Except where otherwise noted, this work is licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0). © 2026 Dr. Carsten Stöcker, Spherity GmbH.

Abstract

European businesses repeatedly supply the same evidence to customers and public authorities: that a company exists, that a licence is current, or that an employee may act for it. European Business Wallets are intended to make such evidence easier to exchange across borders. For example, a supplier responding to a public tender could present verified company information and its representative's authority; a receiving authority could check relevant evidence from another competent public body where legally permitted. This article asks when that infrastructure could become usable and how organisations can obtain value before its legal and technical arrangements are complete.

We compare official legislative texts, technical specifications and selected research available on 31 October 2026. The analysis identifies different implementation triggers in the Commission, Parliament and Council positions. Consequently, the updated roadmap distinguishes recorded developments from conditional planning scenarios: illustrative acceptance dates in 2029, 2030 and 2031 are calculations, not adopted deadlines. We propose six readiness gates covering legal requirements, technical compatibility, authoritative evidence, representation, receiving services and operational resilience.

The framework connects wallet deployment to completed transactions rather than to wallet ownership alone. It explains how reusable evidence could reduce repeated paperwork, support exchanges between authorities and lower barriers to cross-border business. For industrial software agents, verified organisational identity and bounded permissions can strengthen accountability, while separate controls remain necessary for correct decisions and safe physical actions. Post-quantum preparation requires its own risk-based migration plan. A practical implementation guide combines a simple use case, a minimum viable ecosystem and measurable business and resilience outcomes with adaptable technology. The contribution is a traceable policy comparison and an evaluation framework; economic and security benefits remain hypotheses requiring deployment evidence.

Keywords. European Business Wallet; eIDAS; Single Market; administrative burden; cyber-resilience; accountable AI; post-quantum cryptography; cross-border interoperability; macroeconomic impact; European USP

Article type: legal and technical policy analysis. Evidence cut-off: 31 October 2026. This manuscript has not been peer reviewed.

Contents

1 Introduction: from identity to completed transactions **3**

2 Concepts and a running transaction example **3**

3 Method, evidence and relationship to prior research **4**

4 Legislative position at the evidence cut-off **5**

5 Three proposed clocks for public-sector acceptance **6**

6 Calendar scenarios and sensitivity to dependencies **7**

7 Updated European Business Wallet roadmap **9**

8 Technical foundations and authoritative evidence **10**

9 Representation, delegation and accountable action **11**

10 Compliance automation in B2G and G2G workflows **11**

11 Cyber-resilience, privacy and continuity **12**

12 Post-quantum preparation and cryptographic agility **13**

13 Trusted, industrial and physical AI **14**

14 Economic value and the Single Market **15**

15 A transaction-level readiness framework **16**

16 Worked example: a cross-border tender submission **18**

17 Pilots, deployment priorities and governance **19**

18 Discussion: contribution and evaluation agenda **20**

19 Practical implementation guidance and conclusion **21**

19.1 Start with the transaction and the minimum ecosystem 21

19.2 Pilot, adapt and decide on evidence 21

19.3 Conclusion 22

References **23**

1 Introduction: from identity to completed transactions

A company may present a digitally signed register extract to a foreign authority and still be unable to complete a filing. The authority may not recognise the identifier, may require additional evidence, or may be unable to determine whether the submitting employee can bind the company. Equally, a recognised submission channel may be unavailable when a deadline approaches. These examples distinguish possession of a wallet, acceptance of its functions and successful completion of a legally meaningful transaction. An implementation roadmap must explain the dependencies between all three.

The Commission's proposal of 19 November 2025 establishes the starting point for European Business Wallets (EBWs). It addresses identification and authentication, attestations, signatures and seals, representation and registered delivery for economic operators and public sector bodies. Its scope extends beyond incorporated companies. It builds on the European Digital Identity (EUDI) Framework but follows a separate legislative procedure, 2025/0358(COD). The proposal is therefore a developing business infrastructure framework, with its own unresolved implementation rules. [1, 2]

The economic motivation is the repeated cost of establishing trustworthy relationships. Businesses reproduce identity information, commission documentary checks, reconcile incompatible records and ask staff to resolve exceptions. Public authorities also spend resources verifying information that another competent body already holds. A reusable evidentiary channel could lower these transaction costs, especially where entering another national market entails new administrative interfaces. Whether it does so depends on source coverage, receiving-service integration, pricing and the displacement of existing work. This causal pathway is more informative than treating the number of wallets issued as evidence of productivity growth. [3, 4]

The same infrastructure could support cyber-resilience and industrial automation. Verifiable organisational identity and restricted mandates can help a recipient distinguish an authorised request from an impersonation attempt. An industrial software agent could act within a documented permission rather than relying on a shared account. However, an authentic actor can still be compromised, an authorised request can still be unsafe, and a valid credential can contain a mistaken source fact. The analysis therefore treats identity as one component of a wider decision and control system.

The earlier Spherity roadmap correctly linked legislation, standards, authentic sources and adoption, but its chronology now requires revision. This article replaces a largely linear progression towards 2028–2029 with a comparison of negotiating texts and a conditional implementation model. It also extends the prior discussion of business credentials and shared evidence infrastructure to public-sector workflows, economic evaluation, AI accountability and cryptographic migration. [5, 6]

Three questions organise the study. Which events start the proposed acceptance clocks? Which legal and operational dependencies determine whether a transaction can actually succeed? How can investment produce economic and security value while the final legislation and technical profiles remain unsettled? The contribution is a source-traceable roadmap, a transaction-level readiness framework and a testable account of expected benefits. The paper reports documentary findings and analytical proposals, rather than deployment results.

2 Concepts and a running transaction example

An EBW is best understood through the organisational functions it is intended to support, rather than as a particular phone application. Under the proposal, an economic operator or

public body would use wallet services to establish identity, present attestations, demonstrate representation and perform supported interactions. The proposed EBW regime is a separate legislative initiative from the enacted EUDI framework. Reusing EUDI technical foundations does not make their legal obligations or deployment schedules identical. Mandatory acceptance also differs from earlier use under an existing lawful arrangement. [1, 7]

A credential is an attested claim, such as a company identifier or an employee's role. An issuer makes the claim, a holder presents it, and a verifier evaluates it for a purpose. These roles can be distributed across organisations and services. A mandate records permission to act for a principal, within a stated scope. A digitally signed company record and a current mandate answer different questions: which organisation is involved, and whether this actor may undertake this action. The terminology is functional; it does not assert that one credential format or mandate vocabulary has already been settled for all EBW uses. [1, 8]

Authentication provides evidence about an actor's identity; authorisation determines whether a requested action is permitted. Verification of a signature can establish integrity and an attributed issuer without establishing the truth, freshness or procedural sufficiency of every claim. A receiver therefore needs both technical checks and a decision about the source's competence, the applicable rule and the intended use. This distinction explains why a technically successful credential exchange may still lead to a legitimate rejection or a request for more information. [8]

Consider an illustrative manufacturer bidding for a public contract in another Member State. The manufacturer must identify itself, establish its representative's authority, provide the evidence required by the procedure and receive a meaningful submission outcome. The example assumes a receiving authority that is legally entitled to accept the selected evidence. It makes no claim that a particular national procurement procedure already accepts EBWs or that the evidence described exhausts its requirements. The transaction is used throughout the analysis to connect the legislative calendar with concrete dependencies.

A wallet could reduce repeated entry of the manufacturer's details and transmit a bounded procurement mandate. If a required company attribute changes, the receiver needs a rule for freshness and an authorised route to an updated source. If the mandate has been revoked, the submission should fail or move to a defined correction path even when the employee can still authenticate. If delivery succeeds but the receiving system does not associate the evidence with the tender, the business has not yet obtained the intended service outcome.

This running example sets the boundary of the argument. The unit of value is a completed, accountable transaction, including appropriate rejection and recovery, rather than a credential issued or a wallet installed. The following sections first establish the documentary basis and legal clocks, then analyse the dependencies that must be resolved, and finally turn the six readiness gates into an implementation and evaluation programme.

3 Method, evidence and relationship to prior research

We use comparative documentary analysis with a fixed evidence cut-off of 31 October 2026. The core corpus consists of the Commission proposal, the Council general approach, the report of Parliament's Committee on Industry, Research and Energy (ITRE), and official procedural records. Related enacted instruments, versioned standards, supervisory guidance and project announcements provide the implementation context. Documents are classified by legal and evidentiary status before their claims enter the roadmap: enacted requirement, negotiating position, recorded event, policy target, project plan or author-generated scenario. This

classification prevents an announced ambition from acquiring the appearance of a statutory deadline. [1, 2, 9, 10]

The legal corpus was assembled from EUR-Lex, the Council document register and Parliament's Legislative Observatory, report repository and event record. The Commission proposal, ST 9684/26 and the consolidated ITRE legislative text were read at article level; appended committee opinions were not substituted for that consolidated position. For each timing provision, the analysis records the operative event, interval, obligation and exceptions. Article-level wording takes precedence over summaries when calculating dates. Adoption, publication, entry into force and application are treated as separate events. Where texts differ, the differences are retained instead of selecting one preferred forecast. The two scenario rows in Table 2 use explicit assumptions and simple calendar addition; they do not estimate the probability or duration of negotiations. The same assumptions and labels appear in Figure 1.

Technical sources are assessed at the published-version level. A standard's existence is evidence of a specification baseline, rather than evidence that every deployment implements it. Project announcements establish planned scope or reported activity, rather than independently verified conformance. Economic statements are classified as modelled expectations, hypothetical calculations or observed results; no observed EBW savings are claimed here. The accompanying source register records identifiers, URLs, access date and available local source copies. This is a structured policy review, not an exhaustive systematic review or a formal legal opinion.

Earlier research clarifies why identity infrastructure requires more than credential exchange. Ferdous and colleagues distinguish authentication, authorisation and service provisioning within an identity lifecycle. Their conceptual treatment supplies useful categories without specifying an EBW implementation. Krul and colleagues show how application-specific trust assumptions generate requirements for issuers, holders and receivers; identifying an issuer does not alone establish its authority to attest a particular fact. These findings support analysis of institutional responsibilities and technical controls together. We apply that distinction to organisational representation and public procedures, without assuming that EBWs must reproduce a particular self-sovereign identity architecture. [11, 12]

Recent preprints add narrower evidence on disclosure decisions and verifier assurance. Zingg and colleagues find that decision support can reduce disclosure mistakes in a simulated credential-sharing study; their design does not establish effects in deployed business wallets or evaluate attribute-level selective disclosure. Sokolov distinguishes verifier evidence from wallet assurance using a bounded synthetic experiment; its results do not establish production conformance. We reviewed the relevant full-text methods, results and limitations and use these studies to formulate evaluation questions. Their preprint status remains explicit. The European Data Protection Supervisor (EDPS) opinion provides the official policy basis for examining personal-data risks in the business context. [13–15]

4 Legislative position at the evidence cut-off

The Commission published COM(2025) 838 on 19 November 2025. The Council adopted its negotiating position on 9 June 2026; the operative general-approach text used here is ST 9684/26, dated 2 June. Parliament's ITRE committee voted on 10 September, and report A10-0240/2026, with a cover date of 22 September, was tabled on 23 September. The Rule 72 negotiating mandate was announced on 5 October and confirmed on 7 October. An official Parliament event record identifies the first trilogue on 14 October 2026. These are procedural milestones, not dates of enactment. [1, 2, 9, 10, 16, 17]

At the cut-off, the reviewed official procedure remained at the stage preceding Parliament's first-reading position. The record did not establish an adopted final EBW regulation or its publication in the Official Journal. The European Council's request for agreement before the end of 2026 is a political target. Even achievement of that target would not make agreement, formal adoption, publication and entry into force simultaneous. Figure 1 therefore distinguishes recorded events from the target and leaves subsequent legal events conditional. [2, 18]

The negotiations concern substantive architecture as well as dates. The Commission and ITRE texts envisage public-sector wallet use for specified functions. The Council removes the corresponding wallet-ownership requirements while retaining functional acceptance and permitting directory participation by public bodies that do not own wallets. A receiving gateway and a wallet deployment are consequently different potential routes to public-service participation. Procurement that presumes one settled institutional architecture would run ahead of the legislative evidence. [1, Art. 16]; [9, Arts. 10, 16]; [10, Art. 16]

Representation also remains dependent on applicable law. The Council preserves national and Union requirements governing mandates and administrative procedures. A digital representation record can carry evidence of authority without creating authority that the underlying law does not recognise. The ITRE text adds more explicit provisions on auditable, revocable authorisation and automated interactions. Its proposed safeguards are relevant design inputs, but they should be identified as negotiating provisions rather than existing universal duties. [9, Arts. 2, 5, 6]; [10, Art. 6]

Several other matters remain open, including provider entry arrangements, data-location requirements and the relationship with registered delivery. The ITRE text contains proposed EU data-storage and third-country-control restrictions. The Council's provider assessment approach differs from a simple importation of EUDI wallet certification. The roadmap accordingly uses a provider-assurance workstream with no unconditional completion date. It does not label every provider a qualified trust service provider or assume that one certification scheme covers the entire service chain. [9, Arts. 7, 11]; [10, Arts. 6, 7]

Adjacent company-law initiatives are relevant but retain separate calendars. The Commission's EU Inc. initiative describes wallet-enabled company interactions, and the Council announced a position on that file on 23 October 2026. Those developments strengthen the policy case for reusable company evidence. They do not establish the EBW acceptance date. The paper treats policy alignment as a potential source of demand, while keeping each legal instrument's trigger, scope and implementation period distinct. [19, 20]

5 Three proposed clocks for public-sector acceptance

Let E denote entry into force of the EBW regulation. In the reviewed texts this follows Official Journal publication by twenty days. Let I denote the entry into force of the implementing acts referenced by ITRE Article 16, concerning Articles 5 and 6. Let A denote the application of the last implementing act listed in Council Article 22. These symbols describe different legal events; none is interchangeable with political agreement or pilot completion. Table 1 compares the public-sector acceptance obligation with general application. [1, 9, 10]

Table 1: Acceptance timing in the negotiating texts.

Baseline	General application	Public acceptance
Commission [1]	E + 12 months	E + 24 months; Art. 16
ITRE [10]	E + 12 months; Art. 20 exception	I + 24 months; Art. 16
Council [9]	A + 12 months; specified early provisions	A + 24 months; Art. 22(1c)

Under the Commission proposal, Article 16 sets acceptance at E plus twenty-four months. Article 22 provides general application at E plus twelve months. The Commission also proposes a conditional transitional alternative for specified registered-delivery functions until E plus thirty-six months. That transitional limit is neither a universal wallet go-live date nor a reason to add another twelve months to every acceptance obligation. Its conditions and scope require separate treatment. [1, Arts. 16, 22]

ITRE Article 16 instead uses I plus twenty-four months, with the corresponding conditional alternative-delivery period extending to I plus thirty-six months. The text requires adoption of the relevant Articles 5 and 6 implementing acts within twelve months of E. Adoption is not entry into force, so this requirement cannot mechanically fix I at E plus twelve months. If the two act streams take effect on different dates, interpretation of the final wording will matter. Our examples expressly assume a common date, without purporting to settle that question. [10, Arts. 5, 6, 16, 22]

The Council's Article 22(1c) sets acceptance at A plus twenty-four months. Article 22(1b) sets most other application at A plus twelve months, with specified early provisions applying from E. The acceptance period is measured directly from A: it is not added to the general-application period. Calculating A plus thirty-six months would therefore misread this text. The Council's trigger list covers acts under Articles 5(5), 6(5), 7(6c), 8(7), 9(4), 10(6) and 11(2c). A later application date in any listed stream can determine A. [9, Art. 22]

These differences have practical consequences. A Commission-based planning model depends primarily on the regulation's commencement; the two co-legislator models introduce implementing-act dependencies, but disagree on their breadth and operative event. A public explainer that says "two years after adoption" compresses distinctions that matter to programme delivery. The roadmap consequently retains three labelled clocks until the final legislation supplies one authoritative rule. It also keeps conditional registered-delivery transitions out of the main acceptance illustrations, because their scope and wording remain under negotiation.

6 Calendar scenarios and sensitivity to dependencies

Calendar examples make the legal differences inspectable. Assume that the EBW regulation enters into force on 1 April 2027. In the first example, assume that the relevant ITRE acts enter into force on 1 April 2028 and that the last Council-listed act applies on the same day. The Commission comparator yields acceptance on 1 April 2029. Both co-legislator calculations yield 1 April 2030, although I and A remain legally different triggers. Under the Council model, general application would fall on 1 April 2029. [1, 9, 10]

Table 2: Illustrative dates calculated from assumed triggers.

Assumed trigger	**Commission**	**ITRE / Council**
E = 1 Apr 2027; I and A = 1 Apr 2028	1 Apr 2029	1 Apr 2030
E = 1 Apr 2027; I and A = 1 Apr 2029	1 Apr 2029	1 Apr 2031

In the second example, E is unchanged but I and A move to 1 April 2029. The implementing-act-based acceptance calculations move to 1 April 2031, while the Commission comparator remains at 1 April 2029. These are transparent assumptions, not forecasts. The examples do not imply that an early legal date guarantees service readiness, that later acceptance is desirable, or that every voluntary deployment must wait for mandatory acceptance. Existing legal arrangements may support earlier, bounded use cases.

Sensitivity follows directly from the formulas. Moving A six months later moves the Council acceptance date six months later, all else equal; the same relation holds for I in the ITRE model. A delayed dependency outside the trigger list can instead leave the legal date unchanged while increasing operational risk. The programme must therefore monitor two dependency sets: those that set the legal clock and those that determine whether a transaction works. Credential-source coverage, staff capacity and recovery testing can be critical even where they do not themselves start or stop a statutory period.

No probability distribution is assigned to 2029, 2030 or 2031. The reviewed sources do not provide sufficient evidence to quantify negotiating duration, implementation lags or national integration capacity. The figure extends through 2031 to display the consequences of the stated assumptions, rather than implying that 2031 is a promised endpoint. Its workstream arrows denote continuing activity without a fixed completion commitment. A roadmap ending automatically in 2029 would conceal the implementing-act dependency introduced by the co-legislators.

Two other calendars belong in the same planning view but require distinct labels. Member States must provide at least one EUDI wallet by 24 December 2026. The specific authentic-source verification amendment in Article 1(3) of Regulation 2026/1735 applies from 1 January 2027. Separately, the coordinated EU post-quantum roadmap recommends initial transition measures by the end of 2026 and completion for high-risk use cases by the end of 2030. The former dates arise from enacted instruments; the latter are risk-based policy milestones. None supplies the missing final EBW acceptance date. [7, 21–25]

Updating the roadmap should therefore be event driven. A final compromise, new Official Journal publication, implementing-act application date or revised technical baseline should trigger a documented change. Programme owners should record which assumption changed and which downstream dates or tests it affects. This preserves the distinction between an actual legislative development and a revised internal planning assumption.

7 Updated European Business Wallet roadmap

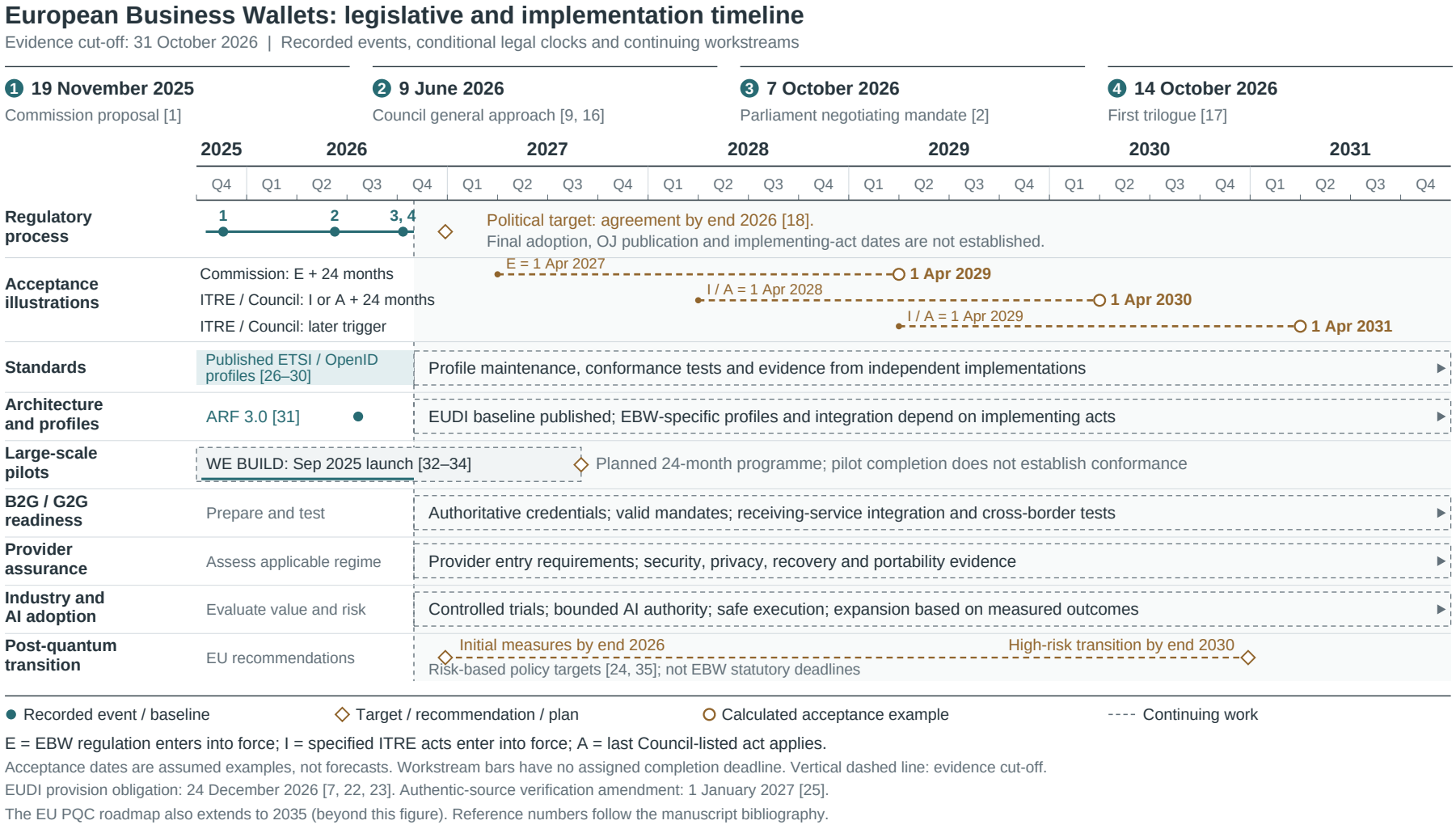


Figure 1: Legislative and implementation timeline at 31 October 2026. Filled markers record events or published baselines; open diamonds indicate political, programme or recommended policy milestones; open circles mark calculated acceptance examples. E, I and A are distinct legal triggers. Examples assume E = 1 April 2027 and the implementing-act dates shown. Continuing workstream bars do not assign completion deadlines. The EUDI and authentic-source dates are enacted milestones; PQC targets are coordinated recommendations, not EBW statutory deadlines. The EU PQC roadmap additionally extends to 2035, beyond the plotted horizon. Sources: [1, 2, 7, 9, 10, 16–18, 21–36]. Author synthesis.

8 Technical foundations and authoritative evidence

The official EUDI Architecture and Reference Framework identifies version 3.0.0 with a release date of 21 July 2026. It is a published EUDI baseline, not evidence of a final, separate EBW architecture. The earlier roadmap's expectation of ARF 3.0 around 2027 must therefore be replaced with the published version and a distinction between reusable foundations and pending business-specific requirements. The Member State obligation to provide at least one EUDI wallet by 24 December 2026 follows the twenty-four-month rule and the 2024 implementing baseline; it does not establish EBW acceptance or demonstrate completed deployment. [7, 22, 23, 31]

Published attribute specifications also need precise identification. ETSI TS 119 472-1 V1.2.1 covers general requirements; Part 2 V1.3.1 covers presentations; and Part 3 V1.1.1 covers issuance. OpenID for Verifiable Presentations 1.0 reached final status in July 2025, and OpenID for Verifiable Credential Issuance 1.0 on 16 September 2025. These specifications provide exchange building blocks. A working profile must additionally fix formats, schemas, identifiers, assurance requirements, trust anchors and status handling. Publication, legal incorporation and product implementation remain separate milestones. [26–30]

Implementing Regulation 2026/1731 amends four 2024 EUDI technical instruments. Attestation rules also evolved: Articles 6–9 of Regulation 2025/1569 apply from 19 August 2026, while Regulation 2026/1735 subsequently updates that instrument. Its Article 1(3), applying from 1 January 2027, adds specifications for authentic-source verification and requires identification of the source and at least an advanced electronic signature or seal based on a qualified certificate for the verification result. This minimum must not be confused with a requirement for a qualified signature or seal in every case. These enacted changes belong in procurement and source-integration plans. They do not require treating every authentic source as a qualified trust service provider. [21, 25, 36]

An authoritative fact, an attestation derived from it and a decision relying on the attestation are distinct objects. A registry can change after issuance; a credential can expire; a particular procedure can demand fresher evidence than another. A valid signature establishes integrity and an attributed issuer, rather than universal factual truth or sufficiency for every purpose. The receiver must establish the issuer's competence, the relevant identifier namespace, the meaning of each attribute and the applicable freshness rule. Name matching alone cannot resolve organisational identity. [8, 21]

We propose a deployment manifest that records the applicable legal provisions, specification versions, credential schemas, trust-list sources, algorithms, status policy, mandate forms and test-suite versions. It should identify which sources cover each required attribute and how a source change reaches the receiver. An upgrade must assess both technical compatibility and semantic changes. Older credentials may remain in circulation after a verifier changes, so rejection reasons and migration arrangements need explicit ownership.

This approach makes evidence availability measurable. Useful indicators include the share of required attributes obtainable through an authoritative path, the delay in reflecting a source change, identifier-matching errors and manual exceptions caused by unavailable evidence. The existence of a legal verification mechanism does not establish complete national endpoint coverage. The study proposes these measurements without claiming that any Member State or provider has achieved them.

9 Representation, delegation and accountable action

Business identity answers which organisation is involved. Representation answers which actor may perform a particular action for it. The distinction matters for directors, employees, external agents and automated services. A job title, employment credential or authenticated login is not a universal power to make commitments. The Council text preserves underlying representation rules, while ITRE Article 6 proposes more explicit auditable and revocable authorisation arrangements. A wallet can communicate evidence of authority; the receiver must still evaluate it against the procedure and applicable law. [9, Arts. 2, 5, 6]; [10, Art. 6]

A useful mandate record should identify the principal, acting party, permitted action, resource or procedure, limits, validity interval, issuer and revocation mechanism. Where onward delegation is allowed, each link should remain within the original grant. This is an analytical design schema, not a claim that a single harmonised mandate vocabulary has been adopted. The receiver must be able to reject an absent link, an exceeded amount, an expired permission or an action outside the stated purpose. An intelligible explanation of that decision is part of accountability.

Consider an illustrative supplier-payment workflow. A software assistant assembles an invoice and presents a delegated request. A policy service checks the company, the assistant's current authority, the permitted supplier and the transaction limit. Additional controls determine whether goods were delivered and whether payment approval is required. The wallet supplies evidence to these decisions. It cannot establish invoice legitimacy solely from the sender's identity, and it cannot transform a general credential into an unlimited authorisation to spend.

Delegation must remain controllable after issuance. Tests should cover an employee's departure, a delegate's attempted expansion of scope, replay of an earlier approval and stale revocation data during an outage. The correct fallback depends on consequence: a low-impact information request may tolerate a short cache period, while a high-value commitment may require fresh verification or human approval. A uniform permissive fallback would convert an availability problem into unauthorised action. Conversely, universal shutdown can create avoidable operational disruption.

ITRE Article 6(1)(d) expressly addresses automated interactions enabled by digital or AI systems, with verifiability, auditability and equivalent assurance and accountability, subject to applicable law. Its role–attribute provisions address revocation, over-delegation and expired authorisations. These proposals support a separate enforcement layer around automation. They do not create legal personality for an AI agent or establish that a model's output is substantively correct. Accountability remains with the organisations and persons responsible for the relevant decisions. [10, Art. 6]

The transaction record should permit reconstruction of who acted, under which authority, against which policy and with what result. Retention should be proportionate to the purpose and applicable requirements, rather than an indefinite collection of every disclosed attribute. Versioned policy decisions, timestamps and referenced evidence can support review while limiting unnecessary disclosure. This separation of identity, authority and execution is reusable before the final EBW settlement and remains valuable if the eventual exchange profile changes.

10 Compliance automation in B2G and G2G workflows

Business-to-government (B2G) burden reduction requires more than digital submission. A business should be able to reuse appropriate identity and attribute evidence, demonstrate a representative's authority, submit a complete case and obtain an explicit receipt or outcome. Automation can prefill fields, check document freshness and route exceptions. It reduces com-

pliance work only when these steps displace repeated collection, rekeying or validation. The substantive requirements of a tax, licensing or procurement procedure remain applicable; a wallet is an evidentiary and interaction mechanism, rather than a general exemption from compliance. [1, 9, 10]

Government-to-government (G2G) exchange offers a related opportunity. One authority may need confirmation of a fact held by another competent authority. Authenticated institutional endpoints, defined attribute meanings and verifiable responses could reduce correspondence and reconciliation. Such exchange requires a lawful purpose, access entitlement and appropriate record handling. Recognition of the requesting body is not itself permission to disclose every available record. A department's technical connection must therefore be coupled to its competence and the specific evidence request.

Existing public infrastructure provides important foundations. Article 14 of the Single Digital Gateway Regulation establishes a technical system for cross-border evidence exchange for specified procedures, commonly called the Once-Only Technical System (OOTS). Article 14 also includes user-request and preview safeguards, subject to its specified exceptions; it does not authorise unrestricted authority-to-authority queries. Article 10 of Regulation 2025/1569 permits reuse of relevant OOTS common services and national components for authentic-source verification. This supports complementary integration rather than the assumption that wallets should replace every sectoral channel. The Interoperable Europe Act also frames public-service interoperability in legal, organisational, semantic and technical terms. [21, Art. 10]; [37]; [38]

An illustrative licensing workflow begins with a company authorising a filing. The receiving authority verifies the actor and mandate, obtains or validates required evidence through an appropriate route and associates the submission with a case. Where a foreign source must confirm an attribute, the request identifies both the competent body and the permitted purpose. The process ends with a receipt, a reasoned request for correction or a decision. A successful login or transport acknowledgement alone does not demonstrate that the administrative obligation has been satisfied.

Compliance automation should separate stable source facts from rules and decisions. Identity and licence evidence can be reused where lawful, while the applicable rule version, jurisdiction, validity period and exception handling remain explicit. A change in law may require reassessment even when the underlying credential is unchanged. Human review remains necessary for contested facts, discretionary decisions and cases outside the automated policy. This design can make compliance more explainable while preserving the authority's responsibility for the outcome.

Evaluation should compare total staff time, elapsed completion time, duplicate requests, correction cycles, rejected submissions and unresolved cases before and after implementation. For G2G, it should also measure source-response latency and reconciliation effort. Savings for a business should not conceal extra work transferred to a public body or credential issuer. Parallel-channel costs, accessibility and support for smaller authorities belong in the same assessment. A shared gateway may reduce repeated integration work, but its resilience, responsibilities and exit arrangements must be demonstrated rather than assumed.

11 Cyber-resilience, privacy and continuity

EBWs could improve resistance to organisational impersonation by making identity, issuer provenance and delegated authority verifiable within a transaction. They could also shorten the period during which a revoked permission remains usable. These are mechanisms to test, not measured security gains in this study. An attacker may compromise a legitimate endpoint, mis-

use a valid mandate or induce an authorised person to approve a harmful action. Credential integrity is therefore one security control within a broader architecture that includes transaction policy, endpoint protection and incident response.

The zero-trust architecture of the US National Institute of Standards and Technology (NIST) is a useful design reference because it distinguishes authentication from authorisation and rejects implicit trust based on network location or ownership. Applied here, a wallet presentation should supply evidence to a resource-specific decision rather than grant blanket trust to a session. NIS2 Article 21 provides a complementary risk-management context for entities within its scope, including incident handling, continuity, supply-chain security, cryptography and access control. EBW participation alone does not make every business subject to every NIS2 obligation. [39,40]

Resilience requires anticipating concentrated dependencies. A directory, trust list, status service, issuer or hosting provider can become a common point of failure across many procedures. Redundancy without independent dependencies may provide less protection than its topology suggests. A receiving service should define what evidence can be cached, for how long, for which actions and under which revocation risk. High-impact operations may need to stop safely when essential evidence is unavailable; lower-impact services may support bounded degradation. Those choices require documented ownership and testing.

Recovery is as important as initial authentication. A lost key, compromised account or provider failure should lead to a controlled process for restoring access, invalidating affected authority and notifying relying parties. Recovery must not bypass the assurance of ordinary operation through a weaker support channel. Exercises should test key replacement, mandate reissuance, revocation propagation, disputed transactions and migration to another provider. Recovery time and the duration of potentially stale authority are more useful measures than an unsupported claim of uninterrupted service.

Business transactions can expose personal data about sole traders, representatives and employees. The EDPS opinion makes the business context no basis for ignoring data-protection duties. Selective disclosure and purpose-limited requests can reduce exposure, but identifiers, status queries, logs and network metadata may still enable correlation. A privacy assessment should therefore cover the full exchange and retention lifecycle. The disclosure experiment reviewed here motivates testing whether users understand requests and whether interfaces discourage unnecessary disclosure. Its simulated whole-credential decisions do not quantify effects for deployed EBWs. [13,15]

Security evaluation should include replay, maliciously expanded disclosure requests, compromised issuers, stale status data and fraudulent changes to payment or delivery endpoints. Results should report false acceptance, false rejection, incident detection, containment and recovery, together with the operating assumptions. A system that reduces impersonation but cannot recover from a provider outage may worsen overall business continuity. The readiness framework consequently treats security, privacy, continuity and provider exit as related operational requirements rather than separate marketing attributes.

12 Post-quantum preparation and cryptographic agility

Organisations need both confidential exchanges and durable confidence in who signed their evidence. Post-quantum cryptography (PQC) addresses the risk that sufficiently capable quantum computers could defeat widely used public-key mechanisms. Confidentiality and authenticity require separate analysis: intercepted encrypted data may be retained for later decryption, whereas vulnerable signatures create risks for future authentication and evidence validation. The relevant horizon depends on data sensitivity, required retention and system lifetime. A

wallet deployment is not automatically a high-risk use case in every respect; the classification should follow a documented assessment of the assets and consequences involved. [24, 35]

The coordinated EU roadmap recommends initial transition measures by 31 December 2026 and completion of the transition for high-risk use cases by 31 December 2030. It further recommends transitioning as many systems as feasible by the end of 2035, prioritising medium-risk use cases. These are coordinated policy milestones, not enacted EBW acceptance dates. Figure 1 places the 2026 and 2030 targets in a distinct lane. ITRE recital 30b also calls for EBW providers and qualified trust service providers to prepare for the quantum transition, but a negotiating recital does not establish an operative, adopted EBW deadline. [10, recital 30b]; [24]

Standards provide components rather than a complete migration solution. NIST FIPS 203 defines ML-KEM for key encapsulation; FIPS 204 and 205 define ML-DSA and SLH-DSA digital signatures. All three were finalised in August 2024. Their functions are different. Selecting a key-encapsulation mechanism does not replace credential signatures, and protecting a transport channel does not independently secure a long-lived signed record. A deployment must identify the relevant protocol, certificate, credential, hardware and archival dependencies. [41–43]

We propose beginning with a cryptographic inventory spanning issuers, wallets, verifiers, trust lists, certificates, hardware security modules, backups and software-update paths. Procurement should require documented algorithm support, migration interfaces and a tested exit path from obsolete components. Crypto-agility means the controlled ability to change algorithms and profiles while preserving security and interoperability; it does not mean accepting arbitrary algorithms advertised by a peer. Downgrade resistance and version negotiation are part of that control.

Hybrid classical and post-quantum deployment may support a transition, but the combination requires an agreed profile, sound composition and interoperability testing. NIST standardisation alone does not establish eIDAS qualified status or acceptance in a particular European wallet profile. Larger keys and signatures can affect payload sizes, constrained devices, verification latency and evidence storage; these impacts must be measured under the intended workload. The study reports no benchmark and does not claim a universal performance penalty or preferred algorithm for every use case. [24, 35, 41–43]

Long-lived industrial equipment makes upgrade planning particularly important. A device expected to remain operational beyond the migration horizon needs an authenticated update path that can itself evolve. For documentary evidence, preservation planning must distinguish a signature's validity at the time of a transaction from confidence in verification many years later. These dependencies justify PQC work before final EBW acceptance. The immediate outcome should be an inventory, risk classification and testable migration plan, followed by profile-specific implementation as the relevant standards and legal requirements permit.

13 Trusted, industrial and physical AI

Trusted AI requires more than identifying its operator. The NIST AI Risk Management Framework addresses validity, safety, security, accountability and other trustworthiness characteristics. EBWs could support a subset of these goals by connecting an automated interaction to an accountable organisation, verifiable evidence and bounded authority. They cannot certify the truth of a model output, establish an adequate training dataset or demonstrate safe behaviour in an unfamiliar situation. This boundary is central to a credible claim that identity infrastructure supports trustworthy AI. [44]

AI used in industrial operations and supply chains is termed industrial AI here; physical AI means AI whose outputs affect machines or physical processes. These are analytical descriptions rather than proposed legal classifications. An industrial procurement agent, for example, could prove the organisation for which it acts and present permission to request quotations within a specified category and budget. A separate policy service would enforce the limits, verify supplier evidence and require approval for exceptions. The model should not be able to expand its own authority merely by generating persuasive text.

A useful architecture separates the organisational principal, the software or machine actor, the mandate, the policy-enforcement point and the executed action. The wallet supports organisational evidence and controlled delegation; device or workload identity may require additional mechanisms. Policy enforcement should occur outside the generative model and should bind the authorisation to the actual action, resource and current context. ITRE's proposed provisions on verifiable automated interactions and revocable role–attribute mappings support this direction without settling every implementation detail. [10, Art. 6]

For physical operations, identity checks must coexist with local safety controls. An authorised maintenance agent might request a diagnostic operation on equipment, but the machine's operating state, safe limits and interlocks still determine whether execution is permissible. A wallet service should not be placed in a time-critical control loop without evidence that its latency and failure behaviour meet the process requirements. NIST's operational-technology guidance emphasises the distinctive safety, reliability and performance concerns of such systems. Remote credential validity cannot substitute for an engineered safety case. [45]

Digital Product Passports provide an adjacent example. A verifiable relationship between a producer, a product record and an authorised update can improve provenance and responsibility. It does not establish that a sensor reading is accurate, that an environmental claim is true or that the physical item matches its digital record. Those claims need their own measurement, assurance and anti-tampering arrangements. W3C discussions of DPPs and business wallets on 30 October 2026 show active consideration of shared semantics, not adoption of a complete cross-sector standard. [6, 46]

Evaluation should test revoked agent authority, malicious instructions embedded in business documents, compromised data sources and attempts to exceed spending or actuation limits. Outcomes should include unauthorised-action prevention, human intervention, traceability and safe recovery, alongside task completion. In a factory or logistics network, authentication failure and unavailable evidence need a predefined safe response. This keeps the economic promise of automated coordination connected to the cyber-resilience and physical consequences of actual operations.

14 Economic value and the Single Market

The main economic hypothesis is that reusable evidence reduces the cost of establishing and maintaining cross-organisational trust. Lower onboarding and verification costs could make entry into another Member State more attractive, particularly for firms facing substantial fixed administrative effort relative to turnover. Faster, more predictable processing could also reduce delays in procurement, licensing and supplier relationships. These are plausible mechanisms, not a quantified claim that wallets alone increase GDP or eliminate national differences. Substantive legal requirements, language, sectoral rules and enforcement remain relevant. [3, 4]

The Commission's policy page states an expectation of at least EUR 160 billion in annual business savings. This is a policy estimate, not an observed outcome. The supporting staff working document models several adoption and usage levels and distinguishes gross benefits,

one-off costs and recurring costs. The upper-benefit calculations in its Table 11 give second-year net direct benefits of EUR 19.49 billion at 10.43% usage and EUR 147.22 billion at 75% usage, across the modelled participants. Table 12 presents lower and upper bounds, including negative first-year outcomes in lower-benefit scenarios. These scenario results should not be presented as guaranteed savings or equated without qualification to the headline business-only figure. [3, 4]

A local evaluation can use a transparent accounting identity for annual net benefit:

$$B = N \times u \times (s - c) - F - X$$

Here N is annual eligible transaction volume, u the share completed through the new process, s the monetised manual effort avoided per completed transaction, and c its variable wallet-process cost. F is annual fixed cost, with implementation expenditure either charged in the evaluation year or annualised under an explicit rule. X is annual residual exception and parallel-channel cost not already counted in c or F. All terms must use the same evaluation period and cost boundary to avoid double counting. The expression is an author-proposed evaluation model, not a fitted estimate. Its value lies in exposing which assumptions determine the result.

Usage, rather than enrolment, is decisive. A company that holds a wallet but continues to rekey the same information receives little process benefit. Likewise, a receiving authority may incur integration and support costs before transaction volumes become material. Fees for issuance, verification and delivery, source-data maintenance and staff training can change who captures the value. Time released should be distinguished from cash expenditure actually avoided. Broader productivity effects require evidence about how resources are redeployed, rather than automatic conversion of hours into economic growth.

Distribution matters for the Single Market. Smaller firms and municipalities may benefit from common interfaces while struggling with fixed setup costs or specialised support. Provider concentration and proprietary extensions can recreate switching barriers inside a nominally interoperable system. Public procurement should therefore consider transparent pricing, portability, documented interfaces and support for non-wallet channels.

Credible evaluation should report completion rates, costs and error rates by procedure, firm size and cross-border status, with a documented pre-implementation baseline. Where feasible, phased rollout permits comparison with similar services not yet migrated. Changes in demand, staffing or procedural law must be considered before attributing effects to wallets. A common evidence framework could then distinguish genuine burden reduction from work shifted between businesses, authorities and intermediaries.

15 A transaction-level readiness framework

We propose six gates for assessing whether a defined transaction is ready for dependable wallet use. The unit of analysis is a procedure involving specified parties and evidence, rather than a country, product or ecosystem considered ready in the abstract. Table 3 records the evidence required at each gate. The gates can be developed concurrently, but a successful demonstration at one does not remove dependencies at the others. This is a prospective assessment framework derived from the preceding analysis, not a new certification scheme.

Table 3: Proposed transaction readiness gates and exit evidence.

Gate	Evidence required before claiming readiness
L Legal basis	Applicable rule, procedure and recognition scope identified
P Technical profile	Versioned manifest and cross-provider exchange tests
C Credentials	Authoritative source path, coverage and current status
M Mandates	Valid action-specific authority and revocation tests
S Receiving service	Complete submission and explicit outcome evidence
O Operations	Security, privacy, recovery, provider exit and PQC plan

Gate L establishes the applicable legal basis, recognition scope and procedural requirements. Gate P fixes a versioned exchange profile and tests independent implementations. Gate C establishes a complete path from a competent source to each necessary attribute. Gate M establishes current, action-specific authority, including delegation limits. Gate S demonstrates that the receiving service produces an explicit procedural outcome. Gate O covers security, privacy, continuity, recovery and provider exit, including an appropriate cryptographic migration plan.

For a particular transaction t, readiness can be expressed as:

$$R(t) = L(t) \wedge P(t) \wedge C(t) \wedge M(t) \wedge S(t) \wedge O(t)$$

This is an author-defined decision rule, not a validated theorem of necessary and sufficient conditions for every transaction. Each term is a documented judgement against stated criteria, with a defined scope and confidence limit, rather than an intrinsically binary property of the entire ecosystem. The logical conjunction makes a practical point: five successful components cannot compensate for an absent legal basis or an unusable receiving service. Where a gate is only partly satisfied, the permissible scope should be narrowed and the remaining risk made explicit.

An illustrative test of a foreign supplier filing would combine a company credential, a current mandate, required procedural evidence and a receiving endpoint. It should include a correct submission, a revoked mandate, missing evidence, an unsupported profile, interrupted delivery and a repeated request. Expected outcomes are specified before testing, including the evidence returned to the sender. A demonstration that uses one provider's issuer, wallet and verifier can establish internal functionality; it cannot by itself demonstrate independent cross-provider interoperability.

The evaluation should retain configuration, policy and specification versions so that a later change can be assessed. A source outage, algorithm migration or mandate-rule update may invalidate only part of the prior assurance case. Recording dependencies makes targeted retesting possible. For AI-assisted or physical workflows, the gate evidence must additionally connect permitted authority to the action actually executed and its safe failure behaviour. The framework therefore supplies a common structure while allowing the acceptance criteria to vary with consequence and context.

16 Worked example: a cross-border tender submission

The manufacturer example makes the readiness framework operational. Assume one business, its appointed representative, competent evidence issuers and a receiving procurement authority using an independent verification service. The illustrative pilot concerns the identity, representation and evidence-submission portion of a tender, not award evaluation or a claim of complete procurement-law compliance. Its success criterion is a correctly associated, reviewable submission outcome under the authority's published procedure. Table 4 assigns responsibility and observable evidence to each gate.

Table 4: Illustrative tender submission mapped to the six gates.

Step and gate	Responsible role	Observable evidence or failure
Define procedure (L)	Receiving authority	Required attributes, recognition scope and permitted source route
Exchange evidence (P)	Wallet and verifier operators	Independent implementations exchange the declared profile
Validate facts (C)	Issuer and receiver	Competent source, correct company identifier and freshness result
Check authority (M)	Principal and receiver	Current mandate for this tender; revoked mandate rejected
Complete submission (S)	Receiving service	Evidence linked to case; explicit receipt or correction request
Exercise recovery (O)	All service operators	Outage, retry and restoration preserve case integrity

The normal path starts with a procedure-specific evidence checklist and ends with a receipt that identifies the case and processing state. The manufacturer retains evidence of what was sent and the authority records the validation and authorisation decisions needed for review. Where the authority must obtain confirmation from another competent body, it uses an authorised channel with the applicable purpose and access controls. A G2G exchange may reduce repeated correspondence, but it is not assumed to bypass consent, request, preview or other safeguards that govern the selected route. [37]

Negative cases are equally informative. Revoke the representative's mandate before submission: the service should prevent the affected action and explain the correction path. Change a source attribute while a credential remains technically valid: the receiver should follow the declared freshness policy. Interrupt delivery after the sender transmits the evidence: a retry should not create a duplicate case or an unsupported assertion of timely filing. Unavailable evidence should produce the predefined pending, rejected or manually reviewed state appropriate to that procedure.

The pilot compares staff effort, elapsed time and correction cycles against the existing process, while recording which steps still require intervention. A shorter exchange time does not count as a complete saving if the authority's reconciliation work increases. The test also measures revocation propagation and recovery under stated conditions. No measured result is asserted here; the example specifies how the paper's value and resilience hypotheses could be examined by independent participants.

17 Pilots, deployment priorities and governance

WE BUILD is a relevant implementation setting for business, supply-chain and payment use cases. The consortium's 3 September 2025 announcement confirms its launch and describes a twenty-four-month programme. A July 2026 update reported preparation for the implementation phase. The roadmap therefore distinguishes the recorded September 2025 launch from the planned September 2027 endpoint. It does not infer that all use cases are already operational, that completion is independently verified or that participation confers conformity with final EBW requirements. [32–34]

Pilots should produce evidence that survives beyond a demonstration. Useful outputs include versioned profiles, semantic mappings, negative test cases, cross-provider results, incident exercises and documented exception handling. Tests should cover the entire transaction, including the business process at the receiver. A polished user interface can obscure an unimplemented source query or a manual step performed behind the scenes. Recording these dependencies helps identify whether the next investment should address credentials, representation, receiving services or operations.

Near-term priorities are capabilities with value under several legislative outcomes: authoritative-source inventories, mandate lifecycle management, documented integration interfaces, privacy controls and recovery exercises. Public bodies can map procedures and evidence needs while preserving the distinction between mandatory acceptance and optional architectures. Firms can identify recurring transactions where digital evidence might displace costly work. PQC inventories and risk assessments can begin alongside this activity, without waiting for the EBW acceptance clock to start. These are planning recommendations, not new statutory deadlines. [24, 35]

A subsequent stage should validate a small set of complete cross-border procedures with independent participants. Expansion should depend on measured completion, cost, error and recovery outcomes. Programmes should also test cases involving smaller firms and authorities, rather than extrapolating from well-resourced participants. Published pilot results should disclose the versions, assumptions, excluded cases and manual interventions needed to reproduce the findings. A failed test can be valuable evidence if it identifies a dependency that would otherwise remain hidden until production.

Governance must assign responsibility across sources, issuers, wallet providers, mandate administrators, receiving services and supervisory bodies. A shared component needs an accountable operator, funding model, change process and incident contact. Procurement should specify service evidence and portability requirements rather than relying on an "EBW-ready" label without a declared baseline. EUDI wallet certification under Regulation 2024/2981, trust-service qualification and the proposed EBW provider regime address different objects and must not be merged into one undifferentiated assurance claim. [1, 9, 10, 22]

The operational roadmap should be maintained together with the legal one. Each new act or profile version should prompt an assessment of affected contracts, credentials, verifiers and procedures. Readiness reporting should state which transactions passed which tests, with which participants and under which assumptions. This is more useful than a single percentage-complete figure that combines enacted obligations, software development and hoped-for adoption. It also creates the evidence needed to revise the economic case as actual use replaces modelling assumptions.

18 Discussion: contribution and evaluation agenda

The documentary findings answer the first research question: the reviewed institutions do not use one settled trigger for public-sector acceptance. The Commission's regulation-based period and the co-legislators' implementing-act dependencies produce materially different planning dates. Reporting the trigger and interval is therefore more informative than publishing a single expected year. The roadmap's contribution is a traceable comparison of these alternatives, with assumptions that can be revised when the final legal record changes.

The six-gate framework answers the second question by making the completed transaction the unit of readiness. It brings legal authority, exchange profiles, source evidence, mandates, receiver integration and operational resilience into one assessment. Its analytical contribution is their explicit connection, rather than the invention of any one component. A protocol-conformant exchange can fail on source competence; a lawful mandate can fail on revocation enforcement; and a timely legal obligation can meet an unprepared receiving service. Readiness claims should state the transaction and the supporting evidence.

Three propositions follow for empirical study. First, completed transaction volume and exception rates should explain realised process value better than wallet enrolment alone. Second, authoritative-source coverage and receiving-service integration should constrain automation even where exchange protocols interoperate. Third, bounded mandates and recovery processes should improve operational controllability only when their enforcement and failure paths are exercised. These are falsifiable expectations, not results established by the documentary analysis.

A suitable evaluation would begin with a defined procedure and pre-implementation measurements, then introduce the new process in phases while retaining comparable procedures as controls where feasible. Researchers should record changes in staffing, demand, law and case complexity that could explain observed effects. Completion costs should include all participating organisations, not merely the wallet holder. Security exercises can establish whether a particular revoked mandate is rejected under stated conditions; they cannot by themselves estimate the annual frequency or monetary cost of future attacks.

Alternative explanations and adverse outcomes deserve equal attention. Improvements may result from simplifying the underlying procedure rather than from the wallet channel. A low-volume process may not recover fixed integration costs. Proprietary extensions or concentrated infrastructure may increase switching costs or correlated outages. Strict freshness checks may improve control while harming continuity during source failures. These trade-offs require explicit decisions rather than an assumption that greater digitisation always improves welfare or resilience.

The study is limited by evolving law, selected rather than exhaustive literature coverage, uneven implementation visibility and the lack of an independent deployment dataset. National representation and procedural rules may constrain generalisation. The author's commercial affiliation creates a further risk of favourable use-case selection and is disclosed. The framework and accounting model require empirical validation. Within these limits, the third research question has a practical answer: early investment can be justified by a bounded, measurable value case and an adaptable design, without treating future acceptance or economic gains as certain.

19 Practical implementation guidance and conclusion

Organisations can begin with a business assessment and a bounded lawful use case while the final EBW requirements develop. The purpose is to remove a defined source of cost or operational weakness, not to accumulate wallet deployments. Investment should proceed when the participants, legal basis and expected value support it; inadequate evidence or a negative business case can justify postponement. The following sequence translates the readiness framework into management decisions, with milestones separate from the legal clocks in Figure 1.

19.1 Start with the transaction and the minimum ecosystem

1. Define a simple use case and business case. Select a recurring process with a named owner, such as reusing verified company information and a limited procurement mandate with one buyer. Specify the current manual steps, required evidence, transaction volume, delays and failure modes. State the business outcome in terms of a completed procedure. Establish an initial cost boundary and decision threshold before choosing technology; a process with little avoidable work may not justify a new channel.

2. Assemble a minimum viable ecosystem. This is the smallest set of independent roles capable of completing and supporting the selected transaction: a business, a competent source or issuer, a receiving counterparty and the necessary wallet, verification and operational services. Several roles may share an operator, but responsibilities must remain explicit. Include at least one real receiving counterparty; a single-vendor demonstration cannot establish ecosystem interoperability. Agree attribute meanings, evidence acceptance, lawful data use, support, incident handling and the route for disputed outcomes.

3. Establish a value-realisation plan. Assign a benefit owner, baseline, target, measurement method and review date. Separate time released from cash expenditure avoided, and tested control performance from hypothetical future loss reduction. Measure total cost across business, issuer and receiver, including support, parallel channels and migration. Table 5 provides the minimum decision record. Its targets should be chosen for the procedure and risk, not borrowed from a generic wallet adoption metric.

Table 5: Minimum decision record for early implementation.

Decision field	Record required
Transaction and ownership	Procedure, accountable process owner and benefit owner
Minimum participants	Source or issuer, holder, receiver and service responsibilities
Baseline and targets	Current volume, effort, cost, errors and recovery; measurable targets
Dependencies and change	Legal basis, profile, source coverage, migration owner and budget
Review and decision	Evidence date; pre-agreed expand, adjust or stop thresholds

19.2 Pilot, adapt and decide on evidence

4. Deliver and evaluate a controlled pilot. Apply all six readiness gates before bounded production use. Test correct submissions, revoked authority, missing or stale evidence, interrupted services, duplicate requests and recovery. An illustrative initial cycle could devote one month to design, one to integration and one to measurement; feasibility depends on procurement,

source availability and participant capacity. Agree the conditions for expansion, adjustment or stopping before the pilot starts. Record manual intervention so that a successful demonstration does not conceal an uneconomic operating process.

5. Design for changing standards. Separate the business workflow and value model from credential formats, protocols, trust-service interfaces and cryptographic components. Use documented interfaces, versioned profiles, portable records and replaceable adapters. Assign ownership and a budget for migration, including contract changes, retained evidence and regression tests. When European requirements change, identify the affected components, update mappings and rerun interoperability, authorisation and recovery checks. Modularity can reduce adjustment cost; it cannot make changes costless or guarantee that the original business case survives.

A numerical illustration makes the decision rule explicit. Suppose 1,200 eligible transactions occur annually, 60% complete through the new process, monetised effort avoided is EUR 18 per completion and variable cost is EUR 3. Assume annual fixed costs of EUR 7,000, including the chosen allocation of implementation cost, and additional annual exception and parallel-channel costs of EUR 1,500. The accounting identity yields EUR 2,300 annual net benefit. Under these assumptions, break-even usage is about 47.2%. These are invented management inputs, not market benchmarks or an EBW forecast; at 40% usage the same case loses EUR 1,300 annually.

The benefit owner should review both value and resilience. A pilot may release staff time without reducing payroll, or improve revocation performance while increasing support expenditure. Such outcomes can still be valuable if they meet the agreed objective and budget. Expansion requires a credible route to additional counterparties and sustained source coverage. An unsupported "EBW-ready" claim is insufficient; the decision record should state the tested versions, participants, exclusions and remaining dependencies.

19.3 Conclusion

The roadmap must remain conditional until the final legislative trigger is established. Operational readiness requires the six transaction gates in addition to the passage of a legal deadline. Early value is possible where a simple use case, a minimum viable ecosystem and a measured value-realisation plan justify action. Organisations should therefore begin the assessment and, where warranted, controlled implementation now, while reserving resources to adapt technology and process as standards develop. This approach connects Single Market ambitions with demonstrable burden reduction, accountable automation and tested cyber-resilience.

Declarations. The author, Dr. Carsten Stöcker, is affiliated with Spherity GmbH, which has commercial interests in digital identity and credential infrastructure. This perspective may influence use-case selection. No human-participant study or new empirical dataset is reported. The source register and editable roadmap accompany the manuscript. Automated research and drafting assistance was used; author approval is required before submission. Original text and figures are offered under CC BY 4.0; third-party source material retains its own terms.

References

[1] European Commission. Proposal for a Regulation on the establishment of European Business Wallets. COM(2025) 838 final, 19 November 2025. Especially Articles 5–11, 16 and 22.

Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0838

[2] European Parliament. Establishment of European Business Wallets. Legislative Observatory, procedure 2025/0358(COD). Status and key events reviewed at 31 October 2026.

Available at: https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2025%2F0358%28COD%29

[3] European Commission. European Business Wallets. Policy overview and economic expectations; describes the Commission proposal rather than final legislation.

Available at: https://digital-strategy.ec.europa.eu/en/policies/business-wallets

[4] European Commission. Staff Working Document accompanying the proposal on European Business Wallets. SWD(2025) 837 final, 19 November 2025. Sections 6–8, especially Tables 11–12; Annex 4.

Available at: https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2025)837&lang=en

[5] Stöcker C, Koenig R, Thiermann R, Westerkamp M. Legal and Operational EBW Roadmap Toward EU-Wide Acceptance. Spherity Research, updated 7 September 2026. Prior roadmap examined in this study.

Available at: https://spherity.github.io/spherity-research/ebw-roadmap.html

[6] Stöcker C. Global Digital Product Passports: Regulation, Interoperability and Shared Evidence Infrastructure. Spherity Research, version 1.0, 25 October 2026. Research manuscript; not peer reviewed.

Available at: https://spherity.github.io/spherity-research/global-digital-product-passport-regulation.html

[7] European Parliament and Council. Regulation (EU) 2024/1183 of 11 April 2024 establishing the European Digital Identity Framework through amendments to Regulation 910/2014. Article 5a(1) provides the twenty-four-month wallet provision rule.

Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32024R1183

[8] W3C. Verifiable Credentials Data Model v2.0. W3C Recommendation, 15 May 2025. Especially the ecosystem, trust model and validation distinctions.

Available at: https://www.w3.org/TR/2025/REC-vc-data-model-2.0-20250515/

[9] Council of the European Union. European Business Wallets — General approach. ST 9684/26, 2 June 2026; negotiating position adopted 9 June 2026. Especially Articles 11, 16 and 22.

Available at: https://data.consilium.europa.eu/doc/document/ST-9684-2026-INIT/en/pdf

[10] European Parliament, ITRE. Report on the establishment of European Business Wallets. A10-0240/2026, PE785.244v03-00. Cover dated 22 September 2026; tabled 23 September. Consolidated text, pp. 6–60, especially Articles 6, 7, 16 and 22.

Available at: https://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2026/0240/P10_A(2026)0240_EN.pdf

[11] Ferdous MS, Chowdhury F, Alassafi MO. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access. 2019;7:103059–103079. doi:10.1109/ACCESS.2019.2931173. Especially Section VI, pp. 103069–103070.

Available at: https://spiral.imperial.ac.uk/entities/publication/92a3a94e-e099-4aa9-9421-843eccf7aac4

[12] Krul E, Paik HY, Ruj S, Kanhere SS. SoK: Trusting Self-Sovereign Identity. Proceedings on Privacy Enhancing Technologies. 2024(3):297–313. doi:10.56553/popets-2024-0079. Especially Sections 2.1.4, 2.2.2 and 4.2.

Available at: https://petsymposium.org/popets/2024/popets-2024-0079.pdf

[13] Zingg S, Lain D, Nakatsuka Y, Kostiainen K, Bechtold S, Čapkun S. Credential Disclosure in (EU) Digital Identity Wallets: Privacy Risks and Practical Mitigations. arXiv:2606.06354v1, 2026. Preprint; especially Sections 4.2, 5.2 and 7.

Available at: https://arxiv.org/abs/2606.06354v1

[14] Sokolov A. Who Assures the Verifier? An Executable Assurance-Locus Audit of the European Digital Identity Wallet. arXiv:2609.26220v1, 2026. Technical pre-results preprint with a reported synthetic experiment; human fieldwork pending. Especially Sections 4.5, 5.2 and 7.

Available at: https://arxiv.org/abs/2609.26220v1

[15] European Data Protection Supervisor. Opinion 5/2026 on the Proposal for a Regulation on the establishment of European Business Wallets. 20 January 2026; especially executive summary and conclusions.

Available at: https://www.edps.europa.eu/system/files/2026-01/26-01-20_opinion_establishment_of_european_business_wallets_en.pdf

[16] Council of the European Union. European business wallets: Council adopts negotiating position. Press release, 9 June 2026.

Available at: https://www.consilium.europa.eu/en/press/press-releases/2026/06/09/european-business-wallets-council-adopts-negotiating-position/

[17] European Parliament. Interinstitutional negotiation event 2025-0358-MEET-TRI1-2026-10-14. Official ELI-DL open-data activity record, activity date 14 October 2026.

Available at: https://data.europarl.europa.eu/eli/dl/event/2025-0358-MEET-TRI1-2026-10-14

[18] European Council. Conclusions of 19 March 2026. Single-market agenda, point concerning agreement on European Business Wallets before the end of 2026.

Available at: https://www.consilium.europa.eu/media/lwhk3itd/en-20260319-european-council-conclusions.pdf

[19] European Commission. EU Inc.: a new digital company framework to simplify cross-border business in Europe. March 2026. Describes proposed wallet use for company documents.

Available at: https://digital-strategy.ec.europa.eu/en/news/eu-inc-new-digital-company-framework-simplify-cross-border-business-europe

[20] Council of the European Union. EU Inc: Council adopts position on a new EU corporate law for innovative companies. 23 October 2026. Separate legislative file and implementation calendar.

Available at: https://www.consilium.europa.eu/en/press/press-releases/2026/10/23/eu-inc-council-adopts-position-on-a-new-eu-corporate-law-for-innovative-companies/

[21] European Commission. Implementing Regulation (EU) 2025/1569 of 29 July 2025 on qualified attestations and authentic-source public-sector attestations. Especially Articles 4–11 and Annexes I–II; Articles 6–9 apply from 19 August 2026.

Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R1569

[22] European Commission. Implementing Regulation (EU) 2024/2981 of 28 November 2024 as regards the certification of European Digital Identity Wallets. OJ L, 4 December 2024.

Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32024R2981

[23] European Commission. Implementing Regulation (EU) 2024/2979 of 28 November 2024 on integrity and core functionalities of EUDI wallets. Original OJ publication 4 December 2024; Article 15, entry into force twenty days later.

Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2979

[24] NIS Cooperation Group. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. Published 23 June 2025. 2026, 2030 and 2035 timeline and risk-based migration guidance.

Available at: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[25] European Commission. Implementing Regulation (EU) 2026/1735 of 15 July 2026 amending Implementing Regulation 2025/1569 as regards applicable standards and specifications. Article 1(3) applies from 1 January 2027.

Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32026R1735

[26] OpenID Foundation. OpenID for Verifiable Presentations 1.0 Final Specification Approved. 10 July 2025.

Available at: https://openid.net/openid-for-verifiable-presentations-1-0-final-specification-approved/

[27] ETSI. TS 119 472-1 V1.2.1. Electronic Signatures and Trust Infrastructures; Profiles for Electronic Attestation of Attributes; Part 1: General requirements. February 2026.

Available at: https://etsi.org/deliver/etsi_ts/119400_119499/11947201/01.02.01_60/ts_11947201v010201p.pdf

[28] ETSI. TS 119 472-2 V1.3.1. Profiles for Electronic Attestation of Attributes; Part 2: Profiles for EAA/PID Presentations to Relying Party. July 2026.

Available at: https://etsi.org/deliver/etsi_ts/119400_119499/11947202/01.03.01_60/ts_11947202v010301p.pdf

[29] ETSI. TS 119 472-3 V1.1.1. Profiles for Electronic Attestation of Attributes; Part 3: Profiles for issuance of EAA or PID. March 2026.

Available at: https://etsi.org/deliver/etsi_ts/119400_119499/11947203/01.01.01_60/ts_11947203v010101p.pdf

[30] OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0. Final specification, 16 September 2025.

Available at: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-final.html

[31] European Commission. Architecture and Reference Framework for the EU Digital Identity Wallet. Version 3.0.0; official site release date 21 July 2026.

Available at: https://eudi.dev/3.0.0/

[32] WE BUILD Consortium. WE BUILD Consortium officially launched at General Assembly in Amsterdam. 3 September 2025. Reported launch and planned twenty-four-month programme.

Available at: https://www.webuildconsortium.eu/news/we-build-consortium-officially-launched-at-general-assembly-in-amsterdam

[33] WE BUILD Consortium. Project update: getting ready for the implementation phase. 1 July 2026.

Available at: https://www.webuildconsortium.eu/news/we-build-project-update-getting-ready-for-the-implementation-phase

[34] WE BUILD Consortium. About WE BUILD. Use-case scope, architecture, business identity and testing workstreams. Dated access snapshot.

Available at: https://www.webuildconsortium.eu/about-we-build

[35] NIS Cooperation Group. Frequently Asked Questions on the Transition to Post-Quantum Cryptography. 15 April 2026. Companion guidance to the coordinated implementation roadmap.

Available at: https://ec.europa.eu/newsroom/dae/redirection/document/132120

[36] European Commission. Implementing Regulation (EU) 2026/1731 of 15 July 2026 amending Implementing Regulations 2024/2977, 2024/2979, 2024/2980 and 2024/2982 as regards applicable standards and specifications. OJ L, 22 July 2026.

Available at: https://eur-lex.europa.eu/eli/reg_impl/2026/1731/oj/eng

[37] European Parliament and Council. Regulation (EU) 2018/1724 establishing a single digital gateway. 2 October 2018. Article 14: cross-border exchange of evidence through the once-only technical system.

Available at: https://eur-lex.europa.eu/eli/reg/2018/1724/oj/eng

[38] European Parliament and Council. Regulation (EU) 2024/903 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act). 13 March 2024. Articles 1–3.

Available at: https://eur-lex.europa.eu/eli/reg/2024/903/oj/eng

[39] European Parliament and Council. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). 14 December 2022. Especially Article 21.

Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[40] Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. NIST SP 800-207, August 2020. doi:10.6028/NIST.SP.800-207.

Available at: https://doi.org/10.6028/NIST.SP.800-207

[41] NIST. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. 13 August 2024. doi:10.6028/NIST.FIPS.203.

Available at: https://doi.org/10.6028/NIST.FIPS.203

[42] NIST. FIPS 204: Module-Lattice-Based Digital Signature Standard. 13 August 2024. doi:10.6028/NIST.FIPS.204.

Available at: https://doi.org/10.6028/NIST.FIPS.204

[43] NIST. FIPS 205: Stateless Hash-Based Digital Signature Standard. 13 August 2024. doi:10.6028/NIST.FIPS.205.

Available at: https://doi.org/10.6028/NIST.FIPS.205

[44] Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1, January 2023. doi:10.6028/NIST.AI.100-1.

Available at: https://doi.org/10.6028/NIST.AI.100-1

[45] Stouffer K et al. Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3, September 2023. doi:10.6028/NIST.SP.800-82r3.

Available at: https://doi.org/10.6028/NIST.SP.800-82r3

[46] W3C Verifiable Credentials Working Group. TPAC face-to-face meeting minutes, 30 October 2026. Section DPP and Business Wallets. Discussion record, not an adopted standard.

Available at: https://w3c.github.io/vc-wg/minutes/2026-10-30-f2f.html