QUANTUM CORE INSTITUTE

QCI-QS1-S8

EU Digital Identity Wallet Supplement

eIDAS 2.0 and EUDI Wallet Quantum Readiness Alignment

Document ID	QCI-QS1-S8
Version	1.1
Status	Published — For organizational adoption and external reference
Publisher	Quantum Core Institute (QCI)
Normative ref	QCI-QS1 Version 2.3 (September 23, 2026). Clause references are QCI requirement identifiers.
Applies to	EUDI Wallet providers, qualified and non-qualified trust service providers, WSCD and WSCA suppliers, and public and private relying parties in the EU Digital Identity ecosystem under eIDAS 2.0
Effective date	September 23, 2026
Companion docs	QCI-QS1-H Practitioner Handbook V2.3 (September 23, 2026) | QCI-QS1-S8-P Practitioner Supplement v1.0 (restricted)
Review cycle	Annual, or upon material eIDAS implementing act, EU PQC roadmap, or NIS2 developments, or a new edition of QCI-QS1

This supplement extends QCI-QS1 for providers and relying parties in the European Digital Identity (EUDI) Wallet ecosystem under eIDAS 2.0. It maps QCI-QS1 requirements to the wallet's cryptographic architecture, the EU Coordinated Post-Quantum Cryptography (PQC) Roadmap milestones, and the certification regime the wallet must pass. It does not replace QCI-QS1. It translates it for the digital identity context.

Foreword

The EU Digital Identity Wallet is being built and the post-quantum migration is being scheduled, and the two calendars were drawn in different rooms. Regulation (EU) 2024/1183, eIDAS 2.0, has been in force since May 20, 2024. It requires every Member State to offer at least one certified wallet by December 24, 2026. The EU Coordinated PQC Roadmap asks those same Member States to begin cryptographic migration by the end of 2026 and to finish high-risk systems by 2030. The wallet ships on classical cryptography in the same quarter the migration is supposed to start.

That would be a manageable overlap for an ordinary app. The wallet is not ordinary. It is built to Level of Assurance high, which means it must resist attackers with high attack potential, including state actors. It carries qualified electronic signatures that hold legal weight for years. Its trust anchors must stay verifiable long after the systems that issued them retire. A wallet is identity infrastructure with a long memory, and long memory is exactly what a harvest-now, decrypt-later attacker feeds on.

This supplement does not argue that the wallet should have waited for post-quantum standards. It should not have. It argues that the wallet must be crypto-agile from the first release, because the alternative is rebuilding a freshly deployed identity stack for hundreds of millions of people under deadline pressure. QCI-QS1 supplies the governance machinery to make that agility auditable rather than aspirational. This supplement maps it to the wallet.

What changed in version 1.1

Version 1.1 aligns this supplement to QCI-QS1 version 2.3. Clause references are now QCI requirement identifiers; the exception register citation in section 8 was corrected from a clause number that did not exist in the standard to QCI-7.3-01 and QCI-4.3-02. Section 5 is rebuilt around the identity records the standard now requires, separating the human identity the wallet holds from the workload identities the provider’s own infrastructure runs on (QCI-5.2-02). The band targets in section 6 are restated for the fixed Core profile: Defensible readiness begins at 81, coverage under gate G60 is fixed at 95 percent of validated critical systems and flows, and gate G70 is no longer satisfied by a documented exception — which, for a wallet on a native keystore, means the platform vendor holds the score (section 8). Hybrid signing and key exchange are stated as a profile decision under QCI-4.5-03 rather than a default. A new box in section 2.4 separates eIDAS certification from QCI-QS1 assessment, which is not a certification.

1. Scope and applicability

This supplement applies to the organizations that build, secure, certify, and rely on the EUDI Wallet:

- Wallet providers issuing a certified EUDI Wallet Solution under a Member State, whether public or delegated to the private sector.
- Qualified and non-qualified trust service providers issuing person identification data (PID) and electronic attestations of attributes that the wallet holds and presents.
- Suppliers of the Wallet Secure Cryptographic Device (WSCD), the tamper-resistant hardware that protects keys, and the Wallet Secure Cryptographic Application (WSCA), the software that drives it.
- Public and private relying parties that will accept wallet presentations, including the regulated sectors obliged to accept the wallet from December 2027.

Who this supplement is for

The people accountable for the wallet's cryptographic posture: wallet provider CISOs and security architects, PKI and key management leads, trust service provider technical directors, WSCD and WSCA product owners, and the compliance officers preparing for certification. It is written to be used before the wallet ships, not after the first finding.

Note on the AI-cryptographic provisions

QCI-QS1 carries conditional AI-cryptographic provisions. Where AI systems fall within the assessment scope, the organization also keeps linked AI artifact records with separate confidentiality and verification horizons (QCI-5.2-03), exercises the D7-AI incident scenarios (QCI-4.4-03), includes AI suppliers' posture in Pillar 5 (QCI-6.4-01), and issues Annex C section G, questions G1 to G5, to suppliers of AI platforms, ML infrastructure, model registries, or key management used with AI artifacts. Fraud, age-estimation, and identity-proofing models attached to wallet onboarding are the likely in-scope cases here. These provisions have no effect where AI systems are not in scope. They govern cryptographic risk arising from AI systems. They do not govern AI risk generally.

2. Regulatory context

2.1 eIDAS 2.0 and the wallet

eIDAS 2.0 is in force. Regulation (EU) 2024/1183 amended the 2014 eIDAS Regulation and created the European Digital Identity Framework. Article 5a fixes the headline obligation: each Member State shall provide at least one certified wallet, and the Commission's operational guidance sets that deadline at December 24, 2026. Public-sector relying parties must accept notified wallets from the same date. Regulated private-sector relying parties, including banks, telecoms, and very large online platforms, must accept it from December 2027.

The wallet's security rests on two anchors defined in the Architecture and Reference Framework. The WSCD is tamper-resistant hardware that stores keys and runs security-critical functions. The WSCA is the application that manages those cryptographic assets. The framework recognizes four ways to build the WSCD: a remote hardware security module, a local secure element such as an eSIM, a native keystore such as Android StrongBox or Apple Secure Enclave, and hybrids of these. The wallet presents credentials over OpenID for Verifiable Presentations for remote flows and ISO/IEC 18013-5 for proximity flows, and it can create qualified electronic signatures. Every one of those functions runs on cryptography today.

2.2 The EU Coordinated PQC Roadmap

The migration calendar is set by Commission Recommendation (EU) 2024/1101 and the NIS Cooperation Group's Coordinated Implementation Roadmap of June 2025 (QCI-QS1 Annex E, reference S17). It is a recommendation and a coordinated roadmap, not a binding regulation, and competent authorities treat it as the benchmark for whether an entity has taken appropriate technical measures. The milestones map cleanly onto wallet actions.

EU PQC milestone	What it requires	EUDI Wallet program action
By December 31, 2026	National PQC strategies initiated, inventories begun, pilots launched for high-risk use cases	QASI validated for wallet trust anchors, credential signing and presentation flows; first crypto-agility pilot underway on a signing pathway under QCI-4.7

EU PQC milestone	What it requires	EUDI Wallet program action
By December 31, 2030	High-risk systems, including critical identity infrastructure, migrated to PQC, quantum-safe by default for new products	Approved profile (QCI-4.5-01) selecting hybrid PQC signing and key exchange in production; trust anchor migration underway root-first (QCI-4.6-02); WSCD firmware on a PQC path
By December 31, 2035	Full transition complete for as many systems as practicable	Classical-only cryptography retired across the wallet stack; representative end-to-end tests passed across every critical trust pathway

Read against the December 2026 wallet deadline, the first two lines collide. The wallet must exist by end 2026. The migration must be underway by end 2026. An entity that treats these as sequential rather than simultaneous is planning to build the wallet twice.

2.3 NIS2 and the proposed COM(2026) 13

NIS2 is transposed into Member-State law and its cryptographic risk-management and supply-chain obligations already reach trust service providers. Wallet providers are not yet named in NIS2 as a distinct category. COM(2026) 13, a proposed amendment to NIS2 published January 20, 2026, would change that: it anchors to the June 2025 PQC roadmap, reaffirms the 2030 and 2035 targets, and would pull European Digital Identity Wallet providers into NIS2 scope. It is proposed, and it should be described that way in the obligations register (QCI-2.2-01), with its status verified at each review. It is also the direction of travel, and a wallet provider that waits for it to become binding has spent the intervening time not building the inventory that both regimes require first.

2.4 Certification, ENISA, ETSI, and NIST

The wallet reaches Level of Assurance high through certification against a scheme, and the cryptographic specifications sit in ETSI and CEN standards referenced by the implementing acts. ETSI's Quantum-Safe Cryptography group has produced transition guidance, including a three-stage framework of inventory, migration planning, and execution that mirrors the QCI-QS1 sequence. The destination algorithms are settled: NIST finalized ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) on August 13, 2024. The governance gap is not which algorithms to adopt. It is whether the certification scheme, the ARF, and the WSCD roadmaps require agility toward them before the classical stack is locked in.

Two different things called certification

The wallet is certified under the eIDAS scheme. A QCI-QS1 assessment is not a certification and does not claim to be one. Under QCI-1.2-03 an organization reports either a self-assessment or an independent assessment against the standard, with its conformance status stated beside the score (QCI-1.2-04). A wallet provider can present its QCI-QS1 evidence pack to a certification body as evidence of cryptographic governance, and this supplement is written to make that pack useful there. It does not substitute for the scheme, and the scheme does not substitute for it.

3. The quantum threat surface in the wallet

Almost every cryptographic mechanism the wallet standardizes on relies on asymmetric cryptography that a large quantum computer breaks with Shor's algorithm. Symmetric

encryption such as AES survives with adequate key sizes. The break is asymmetric, and the wallet is an asymmetric machine. It exists to prove who someone is and that an attestation is authentic, and proving identity is exactly what the vulnerable layer does. The exposure is not one thing. It is three, with different clocks and different owners.

Exposure	Mechanism at risk	Why it matters for the wallet
Forged signatures	ECDSA and EdDSA in credential attestations, PID, wallet unit attestations, and qualified electronic signatures	This is the dominant exposure. A forged attestation is a forged identity. Authentication failures are systemic and cannot be recovered retroactively. A signature honored in the past cannot be un-signed. In the standard's terms this is a verification horizon, and it is the longer of the two.
Harvested sessions	ECDH key exchange inside TLS and OpenID4VP presentation flows	Presented attributes and session data collected today can be decrypted later. For sensitive attributes with long confidentiality horizons, the harvest has already begun.
Long-lived trust anchors	Root and intermediate keys in the eIDAS PKI hierarchy	Trust anchors must stay verifiable for the legal life of the documents they underwrite, which runs to decades. A root that cannot migrate is technical debt with a statutory expiry it will outlive. QCI-4.6-02 requires its migration path to be recorded now.

The framing matters because attention drifts to the recoverable exposure. Confidentiality of a presented attribute is survivable. A forged qualified signature in a legal transaction is not. Pricing the wallet's quantum risk as a data-confidentiality problem understates it, because the catastrophic case is not someone reading a credential. It is someone issuing one.

4. The post-quantum gap and emerging solutions

The current standards are classical by design and quiet on post-quantum requirements. The gaps are specific.

- The ARF and the certification specifications standardize on classical algorithms and do not yet mandate PQC or hybrid modes. Agility is permitted, not required, which means it is optional, which means it is skipped under deadline.
- There is no settled mechanism for algorithm renewal in long-lived documents and signatures. Refreshing the cryptographic protection of a qualified signature without breaking its legal evidence chain is an unsolved governance and technical problem, not a configuration setting. QCI-4.6-03 makes the same point for stored data: re-wrapping does not remediate what has already been harvested.
- Anonymous and selective-disclosure credential schemes that are plausibly post-quantum secure are still immature. The privacy properties the wallet promises and the quantum resistance it needs are not yet available in the same primitive.
- WSCD hardware carries long certification cycles and limited field agility. A secure element certified in 2026 without a PQC upgrade path is a decade of technical debt cast in silicon.

The response is under construction. The POSEIDON project, funded under Horizon Europe and running from October 2025 to September 2028, is building crypto-agile, PQC-ready identity tools on a hybrid approach and feeding recommendations to the EUDI Cooperation Group. ETSI's quantum-safe work supplies the migration methodology. Several HSM and secure-element vendors now ship crypto-agile WSCD options with in-field ML-KEM and ML-DSA

upgrades, so the hardware path exists for providers who demand it in procurement. The EuroQCI and IRIS2 initiatives are longer-horizon enablers for quantum-safe communication infrastructure. For scale, the commercial internet has set its own clock: Cloudflare and Google both target post-quantum authentication by 2029, inside the wallet's own maturity window.

5. QASI record guidance for wallet components

The QASI record groups in QCI-QS1 Clause 5.2 satisfy the inventory expectation for wallet systems when completed for every component that holds a key or verifies a signature, and for every flow between them. Two record types matter more here than anywhere else in the supplement series. The wallet is a human identity system, so the credentials, attestations and signing keys bound to a natural person are human identity records under QCI-5.2-02. The provider's own infrastructure — the issuance services, the HSM clients, the trust-list fetchers, the CI/CD signing of the WSCA — authenticates with workload identities, and those are inventoried separately under the same requirement. A forged workload credential compromises the issuer; a forged human credential compromises the citizen. They have different owners, different horizons and different remediation paths, and the QASI must not blend them.

QASI field or record	EUDI Wallet guidance
Business criticality	Wallet unit attestation, PID issuance, and the QES signing pathway are always High. A single forged attestation compromises the assurance of the whole solution.
Confidentiality and verification horizons	Use the legal evidence horizon, not the session lifetime, and record it as a date. A qualified signature or an attestation tied to a long-lived entitlement can require verifiability for decades: that is the verification horizon, and it drives the signing-key record. Presented attributes carry the confidentiality horizon. Trust anchors inherit the longest horizon they underwrite.
Human identity records	PID, attestations, wallet unit attestations, and the signing keys bound to the holder. Record the signing scheme, the issuing trust anchor, the verification horizon, and the renewal path. These are the records a relying party ultimately depends on.
Workload identity records	Service credentials between the WSCA and the WSCD, between the issuer and the HSM, to the trust list, and in the build and signing pipeline for the WSCA itself. Record the credential type, the algorithm, the rotation method, and the owner. Firmware and application signing keys carry the QCI-4.6-01 safeguards, including signing-state controls for any stateful hash-based scheme.
Critical flows	Issuance, presentation (OpenID4VP and ISO 18013-5), trust-list retrieval, and WSCD firmware update are flows with protection and authentication at each hop (QCI-5.2-01). Coverage of flows is computed separately from systems (QCI-5.1-03).
Supplier dependencies	Name the WSCD vendor and form factor (remote HSM, local secure element, native keystore, or hybrid) and the WSCA supplier. The form factor determines how much crypto-agility the provider actually controls. Each is a critical supplier under QCI-7.1-01.
PQC support status	Expect None or Roadmap across the WSCD, the signing scheme, and the presentation protocols. Require a written, dated, product-specific roadmap that meets the adequacy criteria of QCI-7.2-02 before recording anything better.

QASI field or record	EUDI Wallet guidance
Crypto agility status	For WSCD hardware, agility means an in-field algorithm change without hardware replacement, demonstrated under a QCI-4.7 test. Native keystores and long-cycle secure elements will often be None. Document the constraint rather than leaving it blank.
Exposure flags	Raise the long-horizon flag (QCI-5.3-01) for any presentation flow carrying sensitive attributes and for any signing key whose signatures must remain valid beyond the migration window. Treatment status is recorded separately (QCI-5.3-02); a roadmap does not clear a flag.
Treatment and compensating controls	Data minimization and selective disclosure reduce what a harvested session exposes. Segmentation of the signing environment is a control where the algorithm cannot yet change. Document each as a decision with an owner and a review date, and count it as treatment only once verified.

6. Q-Risk Score guidance under the EU timeline

The Q-Risk Score gives a wallet provider a comparable readiness number against the same milestones a competent authority and a certification body will apply. The band targets below reflect what should be defensible at each review point, given that the wallet ships classical and migrates in parallel. They are planning guidance, not Core-profile thresholds (QCI-6.3-02). No score above 80 is possible unless gates G60, G70 and G80 have all passed, and Defensible readiness begins at 81.

Review point	Minimum defensible band	What assessors and certifiers look for
2026, wallet launch	Mobilizing (40 to 55)	Named ownership, validated QASI covering trust anchors, signing and presentation flows, at least one crypto-agility pilot on a signing pathway, governing-body briefing delivered
2027 to 2028	Mobilizing to Advancing (55 to 70)	Validated coverage at or near 95 percent for systems and flows; WSCD and WSCA supplier attestations received, with non-responses on the exception register and escalated; hybrid signing tested outside production
2029 to 2030	Advancing (70 to 80), Defensible readiness reachable once all three gates pass	Hybrid PQC in production for high-risk pathways under the approved profile; trust anchor migration underway root-first; every critical supplier attested (G70); representative end-to-end test passed on a critical path within 12 months (G80)
Post-2030	Defensible readiness (81 or above)	Classical-only pathways retired or on an active dated plan, full supplier attestation coverage, agility proven across every critical trust pathway, independent assessment where level 5 is claimed on any pillar

A low first score is a baseline, not a failure. A wallet provider that reports a Defensible readiness score in 2026 has either solved a problem the whole ecosystem is still working on or is not counting the WSCD. Certification bodies can tell the difference, and under v2.3 so can the gates.

7. Governance model for wallet providers

The governance requirements of QCI-4.1 map onto the wallet provider's existing accountability structure. Unassigned quantum risk does not get managed, and in an identity system the unmanaged risk is a forged signature nobody owned.

QCI-QS1 role	Wallet mapping	Note
Governing body (management body)	The wallet provider's governing body, or the Member State authority for a public wallet	Owns oversight and risk appetite. For a public wallet, the accountable authority sets the migration mandate. Accepted risk is approved explicitly (QCI-8.2-01).
Executive sponsor	CISO or CIO of the wallet provider	Owns the outcome. Accountable for whether agility is required or merely allowed.
Quantum Risk Owner	Wallet security architect or PKI lead	Runs the program. Needs access to both the WSCA software and the WSCD vendor relationship.
Procurement and vendor risk	Wallet and trust service procurement	Owns the WSCD and WSCA roadmap evidence and the QCI-7.1-02 contract terms. Procurement is where agility is bought or lost.
Legal and compliance	Trust service and eIDAS compliance	Owns the algorithm-renewal question for qualified signatures and the legal evidence chain that renewal must not break.

8. Vendor and supply-chain engagement

A wallet provider controls less of its own cryptography than it thinks. The WSCD vendor controls the hardware algorithms. The WSCA may be delivered by the wallet provider or by the WSCD vendor, and the split decides who can change what. The Annex C request pack converts that dependency from an assumption into a dated, signed position.

The four WSCD architectures carry different agility profiles, and the choice made for certification in 2026 constrains the migration for a decade:

- Remote HSM: highest agility. In-field ML-KEM and ML-DSA upgrades are available from several vendors today. Require them in the tender.
- Local secure element such as an eSIM: agility depends on the applet and the element's certified algorithm set. Confirm the PQC upgrade path in writing before selection.
- Native keystore such as StrongBox or Secure Enclave: agility is the platform vendor's decision, not the wallet provider's. Treat it as an external dependency with no local control and plan compensating controls.
- Hybrid: agility is only as good as the least agile component. Inventory each part separately.

Every supplier that cannot provide a dated PQC roadmap and an officer-signed attestation within the 60-day deadline of QCI-7.2-04 is handled under QCI-7.3-01 and goes on the exception register under QCI-4.3-02, with compensating controls, review triggers, an expiry and an exit path where feasible, and the top exceptions reach the governing body. Public procurement is the strongest lever available: a tender that requires PQC-ready, crypto-agile WSCD and WSCA hardware and software converts the whole roadmap from a hope into a contract term.

Gate G70 and the platform vendor

Under QCI-QS1 v2.3 an approved exception no longer satisfies gate G70. Every critical supplier must have provided an adequate, product-specific, officer-attested response before the score can exceed 70. For a wallet on a native keystore, the platform vendor is a critical supplier, and a published platform security statement does not meet the adequacy criteria of QCI-7.2-02 unless it is specific to the keystore release in use and attested. Most wallet providers on native keystores should therefore expect to be held at 70 until that attestation exists. That is the finding, reported honestly: the wallet's crypto-agility is in the platform vendor's hands. The record that makes it defensible is the request, the deadline, the escalation and the verified compensating controls — and, where the Member State procures, a coordinated request through the Cooperation Group so that the platform vendor attests once for every wallet.

9. The 90-day quick start

This sequence takes a wallet provider from nothing to a first Q-Risk Score snapshot and a certification-ready evidence pack in about 90 days. It adapts QCI-QS1 Clause 9.1 and is a planning aid, not a conformance grace period.

Weeks	Phase	Priority actions	Artifact produced
1 to 2	Establish	Name the executive sponsor and Quantum Risk Owner. Declare the assessment boundary (QCI-1.1-01) around the wallet's critical cryptographic components: trust anchors, signing, presentation, WSCD, WSCA. Note that coverage is fixed at 95 percent of critical systems and flows (G60). Seed the obligations register.	Signed scope statement. Named roles. Obligations register started.
3 to 6	Inventory	Build linked QASI records for trust anchors, PID and attestation signing, presentation flows, and the WSCD and WSCA. Separate human and workload identity records. Record form factor and agility per component. Flag every long-horizon signing key.	Validated QASI for critical wallet components and flows. Coverage figures for systems and flows.
7 to 9	Analyze	Map legal evidence horizons to signing keys and trust anchors. Raise exposure flags on presentation flows. Issue Annex C requests to the WSCD and WSCA vendors with the 60-day deadline.	Exposure flag count. Dated supplier requests. Flags active.
10	Score	Produce the first Q-Risk Score, labelled self-assessment (QCI-1.2-03), with gate results and evidence links. Be honest. The WSCD constraint will hold the number down, and that is the finding, not a failure.	Q-Risk Score snapshot with assessment type. Pillar and gate gaps identified.
11 to 12	Plan and report	Draft the migration roadmap with milestone types per QCI-4.2-02, root-first for trust anchors, and record the hybrid construction decision in the approved profile (QCI-4.5-03). Deliver the first governing-body briefing (QCI-8.1-01). Open the exception register. Assemble the certification evidence pack.	Roadmap draft. Profile decision recorded. Governing-body insert and evidence pack delivered.

10. Certification and supervision preparation checklist

The artifacts below are what a certification body and, under the proposed COM(2026) 13, a competent authority will expect a wallet provider to hold. Produce them before the review, not in response to it.

- Governance: a written quantum risk policy referencing eIDAS certification and the EU PQC roadmap, a named Quantum Risk Owner, and management-body minutes showing the Q-Risk Score was reviewed.
- Inventory: validated QASI records with named owners and evidence references for every trust anchor, signing key, WSCD, and WSCA, with human and workload identity records separated and horizon and agility fields completed.
- Cryptographic controls: an approved cryptographic profile (QCI-4.5-01) recording the hybrid construction and fallback decision per critical pathway, QCI-4.7 test records including the representative end-to-end test, and a documented compensating control for every component that cannot yet change algorithms.
- Vendor: dated requests to WSCD and WSCA suppliers with the 60-day deadline, officer-signed attestations refreshed annually, and an exception register for the non-responsive, with governing-body visibility.
- Reporting: quarterly Q-Risk Score snapshots with deltas, gate status and assessment type, archived, and a governing-body briefing insert each quarter.

Strategic priorities for wallet providers and Member States

Make crypto-agility a certification requirement, not a permitted option, for both WSCD and WSCA. Select the hybrid classical-plus-PQC construction for signing and key exchange in the approved profile for the transition, with the fallback behavior recorded (QCI-4.5-03), to keep interoperability while phasing PQC in. Plan trust-anchor migration root-first, and start now, because roots have the longest lead time and the longest horizon. Establish a governance framework for algorithm renewal that refreshes cryptographic protection without breaking legal evidence chains. Use public procurement to require PQC-ready hardware and software, and synchronize wallet milestones with the 2026, 2030, and 2035 PQC deadlines so the freshly deployed stack is not rebuilt under pressure.

11. Summary and engagement

The EUDI Wallet is critical identity infrastructure deployed on classical cryptography at the exact moment the EU has told everyone to start migrating off it. That is not a reason to delay the wallet. It is a reason to build it crypto-agile from the first release and to govern the migration as deliberately as the deployment. The providers that inventory their trust anchors, demand agility in the WSCD tender, and pilot hybrid signing before the 2026 launch will migrate on their own schedule. The providers that wait will migrate on the calendar’s schedule, at cost, across a stack already in citizens’ hands.

Europe can lead here. The wallet is being built once, for a continent, against a published migration calendar, with a research programme and a standards body already pointed at the problem. A quantum-safe digital identity is an achievable first, not a distant aspiration. The cost of inaction is a rebuild. The opportunity is a wallet that was right the first time.

QCI engagement support for the EUDI Wallet ecosystem

QCI works with wallet providers, trust service providers, and WSCD and WSCA suppliers to deliver

QCI-QS1 assessments calibrated to the wallet's cryptographic architecture, facilitate crypto-agility engagement across the hardware supply chain, and prepare certification and supervision evidence aligned to the EU PQC roadmap. Independent assessment under QCI-1.2-03 is available separately. Contact the Quantum Core Institute to discuss scope and timing.

Revision history

Version	Date	Changes
1.1	September 23, 2026	Aligned to QCI-QS1 v2.3: references by requirement identifier; exception register citation corrected to QCI-7.3-01 and QCI-4.3-02; section 5 rebuilt around human and workload identity records (QCI-5.2-02) with flows and verification horizons; band targets restated for the fixed Core profile (Defensible readiness at 81; G60 at 95 percent for systems and flows; G70 not satisfied by exceptions, with the platform-vendor consequence stated); hybrid construction stated as an approved-profile decision (QCI-4.5-03); eIDAS certification distinguished from QCI-QS1 assessment; EU roadmap cited as Annex E S17; COM(2026) 13 handling in the obligations register; 60-day deadline and annual refresh; governing body terminology; companion documents updated to QCI-QS1-H V2.3 and the restricted practitioner supplement, replacing the retired QCI-QS1-A v2.1.
1.0	September 10, 2026	First edition, aligned to QCI-QS1 v2.2.

Independent assessment against QCI-QS1 is performed by the Quantum Core Institute. Scope one at quantumcoreinstitute.com/independent-assessment. An independent assessment is not QCI certification (QCI-1.2-03).