Security Architecture Brief

How Sphereon functions as enterprise trust and control infrastructure

Executive takeaway

The core architectural shift

Sphereon's strategic strength is not simply issuing and verifying digital credentials. Its primary value lies in turning trust into an active, enterprise-grade control layer. The platform bridges the gap between raw external data and internal business logic by connecting proof creation, real-time trust resolution, and automated policy enforcement into a single, cohesive operating model.

From manual checks to verifiable evidence

Credentials, signed business facts, supplier attestations, and authorization evidence are presented using data minimization, verified against live status registries, pushed through business policy, and retained as cryptographically strong operational evidence. This shifts the organization away from "best-effort" reconstructions utilizing scattered PDFs, email chains, and manual approvals.

Real-world provenance and compliance readiness

Anchored in open standards (including eIDAS 2.0, ISO, and W3C specifications), the architecture is already being deployed in high-stakes, multi-stakeholder environments: securing global maritime certifications, powering EU-wide cross-border e-invoicing, and enforcing physical machine safety. For the modern security leader, this provides a defensible, continuous readiness posture for NIS2-era accountability, supplier assurance, and regulated data exchange.

1. Architecture as a verifiable control layer

For the modern CISO, "digital identity" is no longer just a checkbox or a standalone category: it is the foundation of a real-world control environment. The primary challenge today isn't just knowing *who* someone is, but whether the platform improves specific, high-stakes control points in real-time.

Sphereon's architecture is built to bridge the gap between "appearance-based" trust — relying on uploaded PDFs, email chains, and manual screenshots — and a truly cryptographically verifiable control path. By moving the focus from documents to data, we turn trust into a scalable operating layer.

Shifting the Focus: From Documents to Evidence

In a traditional security model, the "control object" is often a static file, like a scanned certificate or an HR record. Sphereon VDX transforms this business data into verifiable evidence. This ensures that every claim, whether it's a supplier's security certification or a contractor's authorization, is signed at the source and cryptographically bound to the holder. You are no longer managing files; you are managing proofs.

From Manual Checking to Policy-Controlled Decisions

Verification is only as valuable as the action it triggers. Sphereon frames the outcome as a policy-controlled decision, supported by robust workflow and operational tooling. This moves the organization away from ad-hoc, human-intensive checks and toward automated risk treatment.

- **Real-World Impact:** This isn't theoretical. This model is currently used to secure *physical machine safety*, where high-risk equipment only unlocks after the system verifies a user's specific cryptographic safety certification.

- **Operational Logistics:** In fields like *airline maintenance*, our architecture ensures that safety-critical skills are proven and recorded through an immutable audit trail before work begins.

Anchored in Global Open Standards

To eliminate the risk of vendor lock-in and ensure long-term ecosystem health, our technical stack is anchored in recognized global standards. This provides the transparency that security reviewers and regulators expect:

- **Core Protocols:** The stack is anchored in the eIDAS 2.0 ARF, W3C DID/VC, ISO 18013-5/7 mdoc, OID4VCI, OID4VP with DCQL, status lists, OpenID Federation, and common OpenID Connect integrations. That lowers ecosystem and lock-in risk.

- **Regulatory Alignment:** The architecture is built to the eIDAS 2.0 ARF and OpenID Federation specifications, ensuring your trust infrastructure is ready for cross-border and cross-sector requirements.

Flexible Operating Models for Enterprise Reality

We recognize that every enterprise has a different risk appetite and technical maturity. Sphereon offers three distinct deployment paths to align with your specific operating model:

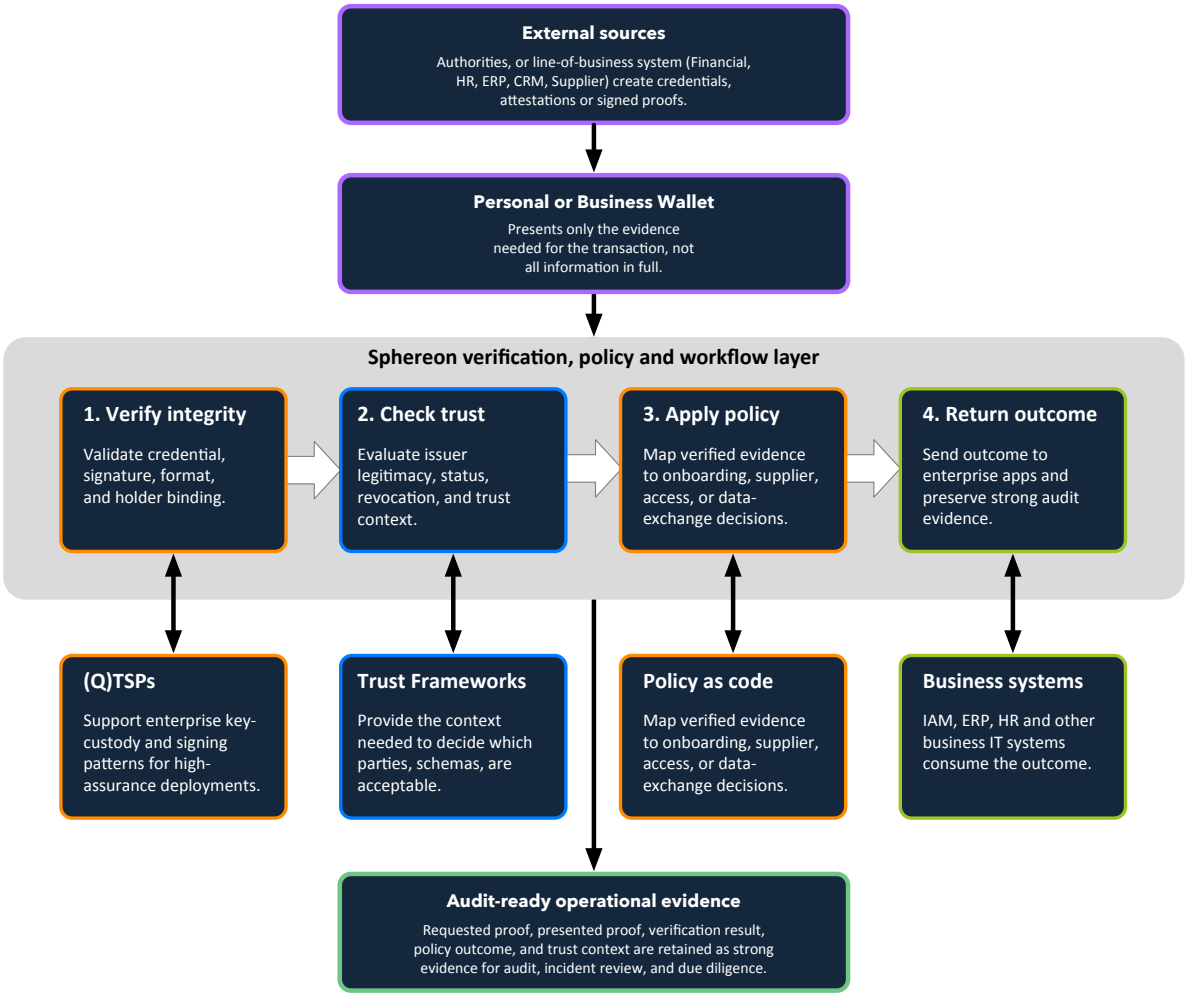
- **IDK (Developer Kit):** Best for teams that need protocol-level control and want to design their own surrounding service layer.
- **EDK (Enterprise Kit):** Designed for production environments that require enterprise runtimes, secure key integrations (HSM/QTSP), and compliance-oriented persistence.
- **VDX (Verifiable Data Exchange):** A complete, deployable trust platform with management UIs and APIs, optimized for rapid deployment and reusable solution patterns across the entire enterprise.

Ready for complex ecosystems

This is not theoretical software. Sphereon is already executing in multi-stakeholder environments where manual trust is no longer an option. By replacing appearance-based checks with verifiable cryptographic control, this architecture is built specifically for the complexity of the 2026 regulatory landscape and beyond.

2. Reference architecture: Sphereon as a trust control layer

The primary anchor of proof for any security infrastructure is the integrity of its control flow. Sphereon's architecture is designed to bridge the gap between raw data and business logic by connecting proof creation, trust resolution, and automated verification into a single, unified operating model.



The trust control plane: technical breakdown

While the control-flow schema traces the high-level movement of data, the following details explain how this architecture functions as a repeatable, standards-based control layer for the enterprise.

- **Protocols for evidence exchange:** The connection between **External sources** and **Wallets** is anchored in **OID4VCI**, while the presentation from the wallet to the **Sphereon verification layer** utilizes **OID4VP** and **DCQL**. This ensures that "what is presented" is limited to exactly what the verifier requires, supporting the core principle of data minimization.
- **Automated integrity and holder binding:** In step 1 (**Verify integrity**), the system performs more than a signature check. It validates the credential format, supporting **W3C VC** and **ISO mdoc**, and enforces cryptographic holder binding to ensure the evidence cannot be replayed or shared by an unauthorized party.

- **Real-time trust and status resolution**: Step 2 (**Check trust**) is the active bridge to external **Trust frameworks** and **Status/revocation checks**. The architecture resolves issuer metadata through registries or federations and performs real-time status checks, using **StatusList2021** or **Token Status List**, to ensure the evidence is valid at the moment of the transaction.
- **Bridging to existing enterprise systems**: Step 4 (**Return outcome**) is where the verifiable evidence is converted into an actionable decision for your **Business systems**. This is typically handled via **OpenID Connect (OIDC)** integration, direct **API-integration**, or (Managed) Enterprise Service Bus (ESB), allowing the platform to drive access, onboarding, or approval workflows within your current stack.
- **The verifiable audit path**: Every transaction terminates in the **Audit-ready operational evidence** layer. Unlike standard application logs, this captures the full context: the specific request, the trust source accepted, and the policy logic that produced the result. This creates a cryptographically verifiable trail designed specifically for **NIS2** and **eIDAS 2.0** regulatory scrutiny.

3. NIS2 & eIDAS 2.0: From static compliance to verifiable evidence

As we move through 2026, the European regulatory landscape is shifting from guidance to strict enforcement. With the *Dutch Cybersecurity Act* (Cbw) entering into force this quarter of 2026, organizations must transition from point-in-time compliance to continuous, verifiable control.

Under the NIS2 directive and the Cbw, the burden of proof rests on the ability to demonstrate that controls are repeatable and supplier-related risks are governed in real-time. Organizations can no longer rely on "best-effort" reconstructions of decisions from PDFs, email chains, and scattered application logs.

The architecture digitizes these high-friction, manual processes into a cryptographically verifiable proof trail. By capturing the requested proof, the trust context, and the policy outcome at the moment of the transaction, the architecture ensures that significant incidents can be investigated and reported within the mandatory 24-hour and 72-hour windows. This moves the organization from point-in-time compliance to a state of continuous, auditable readiness.

Indicative control mapping (NIS2 and regulatory readiness)

The following table demonstrates how the architecture converts high-level regulatory pressure points into specific, auditable technical outcomes.

NIS2 pressure point	Sphereon control contribution	Evidence retained
Supply chain security (Art. 21)	Replaces manual questionnaires with **cryptographic proofs** for suppliers, mandates, and certifications.	Requested proof, trust context, verification result, and policy outcome.
Incident reporting (Art. 23)	Enables **24/72-hour reporting** by preserving a verifiable chronology of authorizations and access events.	Timeline of proof requests, accepted/rejected evidence, and affected business decisions.
Risk management (Art. 21)	Shifts from ad-hoc exceptions to **repeatable, policy-driven decisions** that are easier to test and explain.	Consistent decision records and verifiable audit trails for internal or external review.
Cryptography (Art. 21)	Integrates with **QTSP and HSM providers** to ensure key custody is handled in regulated, high-assurance environments.	Signing context, key provider paths, and associated business event metadata.

Beyond generic logging: the verifiable proof trail

The architectural value here is not "logging" in the generic SIEM sense. Instead, Sphereon provides a cryptographically verifiable audit trail that captures the entire decision context: exactly what was requested, what was presented, which issuer and trust source were accepted, and which policy logic produced the final decision.

This level of detail is materially stronger under NIS2 scrutiny than any attempt to reconstruct a decision from email chains, static attachments, or scattered application logs after a significant incident has occurred. It transforms your compliance posture from a "best-effort" manual reconstruction into a state of continuous, machine-checkable readiness.

4. Proof of execution and operational deployment models

A strategic evaluator must determine whether an architecture exists outside of theory. Sphereon's maturity is evidenced by its active role in complex, multi-stakeholder environments where manual trust is no longer a viable option. Our software provides the underlying infrastructure for global certification, national tax pilots, and supply chain integrity.

Real-world provenance and ecosystem footprint

Sphereon provides the trust and control layer for high-stakes operational use cases across diverse, regulated sectors:

- **Global maritime certification:** Our software powers the Kiwa eLicense platform, providing digital certification for the maritime sector on a global scale. This ensures that safety-critical certifications are verifiable, tamper-proof, and accessible worldwide.

- **EU-wide cross-border e-invoicing:** As part of the WE BUILD EU Large Scale Pilot, we have transitioned direct e-invoicing pilots, originally conducted with the Dutch Tax Office and Chamber of Commerce, into a cross-border EU infrastructure. This utilizes OID4VP and DCQL to ensure invoice integrity and supplier identity across European borders.

- **Supply chain and product integrity:** GS1.nl utilizes our software to provide membership and product-code ownership proofs. Members share these cryptographic proofs with stakeholders like large-scale e-commerce platforms to verify they are the rightful manufacturer or supplier, securing the integrity of the retail supply chain.

- **Critical infrastructure and machine safety:** The architecture secures physical machine safety at KW1C, where industrial equipment only unlocks after the system verifies a user's cryptographic proof of certification.

- **Airline maintenance and services:** We provide the verifiable proof trails required for safety-critical skills and maintenance authorizations in a pilot at MBO college airport (ROC van Amsterdam), ensuring that every action is backed by an immutable record of competence.

- **Education and healthcare:** We power national eduwallet and micro-credential pilots with partners such as SURF, TU Delft, and KW1C, providing professionals with verifiable proofs of certified skills.

Operational deployment and integration choices

A meaningful strength of the Sphereon portfolio is that it does not force a "one-size-fits-all" model. Organizations can align both their engineering capacity and their sovereign hosting requirements with the models that fit their specific risk environment.

Architectural integration models

This determines how your teams integrate and interact with the Sphereon trust layer software.

Model	Best fit	Strategic implication
Identity Developer Kit (IDK)	Teams that require protocol-level control and want to design their own surrounding service layer.	Best for R&D or specialized product teams willing to engineer the foundational plumbing themselves.
Enterprise Developer Kit (EDK)	Environments requiring enterprise runtimes, secure key integrations (HSM/QTSP), and compliance-grade logging.	Stronger fit where auditability and production hardening are required from day one.
Verifiable Data Exchange platform (VDX)	Organizations seeking a deployable trust platform with management UIs, APIs, and workflow orchestration.	Best for rapid operational deployment and creating reusable solution patterns across the enterprise.

Hosting and sovereignty models

Because enterprise key-custody and data sovereignty are critical under NIS2, the platform supports flexible hosting models to ensure you maintain control over your trust infrastructure.

- **SaaS and MSP-hosted:** Optimized for rapid deployment and lower operational overhead, with infrastructure managed by Sphereon or a certified Managed Service Provider.
- **Private and sovereign cloud:** Customer-controlled cloud environments ensuring strict data residency, dedicated isolation, and compliance with your sovereignty requirements.
- **On-premises and edge:** For highly regulated, air-gapped, or physical safety use cases where local execution and direct hardware security module (HSM) integrations are mandatory.

The bottom line

Sphereon is strategically strong because it connects proof creation, trust resolution, policy execution, and evidence retention into a single, cohesive control plane.

This architecture gives you a clear path from pilot to production without forcing a single delivery model, and it provides defensible answers to NIS2-era accountability for 2026 and beyond.