ECHOWORX™

Technology Brief

Validated by AWS. Trusted by the World's Most Regulated Institutions.

FOR C-SUITE • ENTERPRISE ARCHITECTURE • COMPLIANCE • RFP EVALUATION

Echoworx is not hosted on AWS. It is validated by AWS.

EXECUTIVE SUMMARY

For the world's most regulated institutions, secure communication is no longer a technical upgrade. It is a compliance imperative and a cornerstone of operational resilience. Echoworx delivers that resilience as a fully managed, cloud-native encryption platform — **deployed 100% on Amazon Web Services (AWS)** and independently validated by AWS itself.

Echoworx is recognized as **AWS Qualified Software,** having completed the **AWS Foundational Technical Review (FTR)** against the AWS Well-Architected Framework for security, reliability, and operational excellence. That validation is reinforced by deep native integration across AWS Key Management Service (KMS), AWS Private CA, and the AWS Marketplace. This brief gives architecture, security, compliance, and procurement teams the evidence to evaluate Echoworx with confidence.

AT A GLANCE

- **100% AWS-deployed** — cloud-native from the ground up. No appliances to rack, patch, or maintain.
- **AWS Qualified Software** — reviewed and recognized against the AWS Well-Architected Framework.
- **Validated everywhere it runs** — Germany, Canada, US, UK, Ireland.
- **Deeply integrated** — native AWS KMS, AWS Private CA, and AWS Marketplace.
- **Control stays yours** — provider zero-access, always.

CONTEXT
Compliance Is the Catalyst

Evolving regulation, not cost, now sets the pace for encryption modernization. **DORA, NIS2, GDPR,** and **KRITIS** have moved secure communication from a background concern to a board-level mandate. Encryption must be auditable, governed, sovereign, and provable — across every cross-border, externally facing exchange.

Standard platform encryption rarely clears that bar. Regulated institutions need a solution that satisfies regulators, auditors, and architecture boards — and that scales globally without surrendering control. Echoworx is engineered for exactly that requirement.

Compliance is the catalyst.
Echoworx is the control.

VALIDATION
What AWS Confirmed

The FTR is a structured review against the AWS Well-Architected Framework, designed to identify and remediate risk **before** a solution earns qualified status. Echoworx passed on three foundational pillars.

FTR PILLAR	WHAT AWS VALIDATED
Security	Data protected by secure design, encryption at rest and in transit, disciplined identity management.
Reliabity	Recovers gracefully from faults. Holds performance through traffic spikes.
Operational Excellence	Deployment and scaling that is repeatable, predictable, and built to scale.

Every question your RFP asks —
answered, reviewed, and qualified by AWS.

INTEGRATION
Control That Stays Yours

Validation is one signal. Depth of integration is the proof that control, sovereignty, and governance are engineered in.

AWS KMS — Manage Your Own Keys (MYOK)

- **FIPS 140-3 validated HSMs** — hardware-backed key generation and storage (FIPS PUB 140-3 Level 3).
- **Bring Your Own Key (BYOK)** — generate, rotate, and automate keys under your own governance.
- **Provider zero-access** — your keys, your control. Even in a cloud-compromise scenario, data stays locked.

AWS Private CA — Automated S/MIME Lifecycle

- **Issue from your own CA** — Secure/Multipurpose Internet Mail Extensions (S/MIME) certificates from your managed authority, not an external provider.
- **Automated end to end** — issuance, renewal, and rollover, without manual workflows.
- **No expired certs** — regulated communication never stalls.

AWS Marketplace — Procurement Without Friction

- **Private Offers** aligned to your existing AWS agreement.
- **Consolidated billing**, automated tax handling, multi-currency support.
- **Pre-qualified adoption** — bypass lengthy vendor-vetting cycles.

Control stays yours.
The operational burden does not.

COMPLIANCE
Mapped to Concrete Controls

Each obligation maps to a specific control, so resilience is something you can **demonstrate, not just declare.** Echoworx logs key generation, certificate issuance, policy triggers, and delivery states across every encrypted communication — turninaudit readiness from a scramble into a standing posture.

REGULATION	HOW ECHOWORX ALIGNS
DORA (Digital Operational Resilience Act)	Audited recovery, high availability, full auditability, third-party oversight.
NIS2 (Network and Information Security Directive)	Policy-driven encryption, centralized governance, provable controls.
GDPR (General Data Protection Regulation)	Data-residency control, customer key custody, granular protection.
KRITIS (Critical Infrastructure Protection)	Sovereignty controls, hardware-backed keys, continuous availability.

The burden of proof matters as much as the control. Echoworx delivers both.

PROOF
Independently Validated, Repeatedly Recognized

AWS Qualified Software · SOC 2 · PCI DSS · OpenID Connect RP · FSQS-Registered

One consistent story: reviewed by the authorities that matter — and trusted by the world's most regulated institutions.

NEXT STEP
Validated by AWS. Engineered for your institution.

Modern encryption is no longer a technical upgrade — it is a compliance imperative and a cornerstone of operational resilience. Echoworx aligns auditability, key custody, certificate automation, and data sovereignty to the AWS foundation governing your transformation.

Bring your technical and compliance evaluation to our team. We'll walk your architects and risk stakeholders through:

- **FTR scope · AWS KMS key custody · AWS Private CA integration · Deployment models · Marketplace procurement** — against your environment.

powered by aws