

When Regulators Leave No Room for Error.

How a Major UK Bank Modernized PGP Encryption Across Three Countries — With Feature Parity Intact

Technical Proof Points

Architecture

- AWS-native SaaS, cloud-first Amazon KMS with dedicated Cloud HSM keys
- Hardware-backed key protection throughout
- Mirrored pre-production on separate database

Control

- Full feature parity from PGP-U
- Bulk key import via secure web APIs
- Akamai reverse proxy, customer-managed SSL keys
- Entra ID SSO (SAML); OpenID for multi-tenant
- Splunk SIEM via real-time API

Delivery

- PGP with automatic secure portal fallback
- Inbound PGP decryption using migrated keys
- Automated inbound public key harvesting
- Controlled Reply All with verification codes
- Optional S/MIME, restricted user group only

Executive Summary

For a large UK bank serving clients across the UK, Ireland, and Germany, secure communication carries a weight few outside the sector fully appreciate. Every encrypted message is a regulatory commitment, a safeguard for client data, and a quiet proof that the institution can be trusted with what matters most. In banking, that trust is not decorative. It is the foundation everything else stands on.

Yet the bank's encryption sat on aging ground. A legacy Symantec PGP-U appliance carried a vast library of public and private keys — built across years of trusted client exchange — but it was becoming harder to maintain, harder to scale, and harder to defend under the intense regulatory scrutiny this institution faces every day. The bank needed to modernize without losing a single key, a single flow, or a single day of confidence.

The bank turned to Echoworx for a true one-to-one migration: a SaaS platform running entirely on AWS, built to preserve every capability the legacy appliance provided, satisfy a process-heavy regulator-led review, and give the institution a cloud-native foundation with room to grow. The requirement was clear from the start — feature parity, no compromise, and hardware-backed key protection that regulators could scrutinize and accept.

The result: a modern, auditable, standards-based encryption platform that carried every legacy capability forward, cleared exhaustive compliance review, and gave the bank a resilient foundation ready for whatever regulators demand next.

The Challenge

01 | A compliance environment that leaves no room for error.

This bank operates where regulators watch closely and negotiation is not an option. Any new platform had to survive extensive, process-oriented scrutiny — detailed documentation, security evidence, certifications, and proof of every architectural claim. The Symantec PGP-U appliance, dependable in its day, was tethered to on-premises infrastructure that had grown harder to justify under modern resilience expectations. For an institution accountable across three countries, encryption that could not clearly demonstrate hardware-backed key protection and auditable governance was a regulatory exposure waiting to surface.

02 | A migration that couldn't lose a thing.

The bank held a vast library of PGP public and private keys, established communication flows, and long-standing client relationships built on all of it. Losing any of that during migration was not an acceptable outcome. The institution needed feature parity in the truest sense — the same encryption behavior, the same delivery patterns, the same trusted experience for thousands of external contacts — carried across without disruption. Every key had to move. Every flow had to work from day one.

03 | A modernization program that couldn't stall.

Encryption didn't exist in isolation. The bank was already advancing a broader infrastructure transformation, including a gateway migration from Cisco IronPort to Proofpoint, and it needed an encryption platform that would process messages seamlessly before, during, and after that change. A tool that fought the wider program — or imposed its own timeline on it — would have slowed everything down. The bank needed a partner able to hold pace with heavy regulatory overhead, extensive stakeholder engagement, and a large, complex onboarding, all at once.

The Solution

The bank chose Echoworx precisely because the platform could match its legacy Symantec appliance capability for capability — then extend it onto a modern, cloud-native, hardware-protected foundation. What made the partnership work was both depth and flexibility: the ability to accommodate exacting requirements, engage directly with the institution's change-management and compliance processes, adapt where the project demanded it, and prove every step to the people whose approval mattered.

“This bank came to us with one of the most demanding requirements we’ve seen — a true one-to-one migration under intense regulator engagement, with no room for anything to slip,” says Derek Christian, Echoworx Engagement Manager. “Our job was to carry every key, every flow, and every capability across without disruption, prove it all with evidence to the regulators, and stay responsive as the project evolved. Feature parity was the starting point. What we built together goes much further.”

Hardware-backed key management, built into the platform.

Cloud HSM was a non-negotiable for this institution. Because Echoworx is a SaaS platform running entirely on AWS, Amazon KMS and native Cloud HSM are integrated by design — not bolted on. All encryption keys are generated, stored, and managed in hardware-protected infrastructure through a dedicated managed key, satisfying the bank's most stringent compliance mandates without requiring a separate solution. Alongside that, integration with the bank's Akamai reverse proxy gave the institution complete control over the SSL keys used for web and portal access, routing all traffic through the bank's own controlled channels. Together, these capabilities gave the bank cryptographic command end to end — keys, traffic, and access, fully under institutional governance.

PGP encryption, preserved and modernized.

At the heart of the migration was the bank's PGP requirement. Echoworx carried it forward in full — using PGP encryption wherever recipient keys were available, and automatically routing to a secure portal whenever they were not. That design decision guaranteed the outcome the bank valued most: every message reaches its recipient, and every message stays secure. Inbound PGP decryption operated on the same keys migrated from the Symantec appliance, preserving every existing relationship. Automatic PGP public key harvesting from new inbound messages kept the library growing without manual effort.

Bulk key migration, handled at scale.

Moving thousands of public and private PGP keys by hand was never realistic. Echoworx's secure web APIs allowed the bank to import them in bulk through automated scripts — an effectively seamless migration for a key library built across years of operation. The keys the bank depended on carried over cleanly, ready to work from day one.

Mandatory verification, without day-one friction.

Security starts at registration. Echoworx enforced automated secure user verification for every new recipient: a system-generated code, shared out of band by phone or SMS, ties portal registration directly to the bank's own identity-proofing standards. From that point, users self-serve and manage their own credentials. But onboarding thousands of already-trusted contacts on migration day couldn't mean thousands of simultaneous verification hurdles. So the bank leveraged its incumbent platform to send welcome messages, and Echoworx made a controlled, deliberate exception for those existing, already-verified users. New users from that point forward meet the full, fixed verification standard. High security where it counts; smooth onboarding where it made sense.

continued...

Secure collaboration, governed by the bank.

The bank needed Reply All flows that let external parties communicate securely with the bank and with one another through the portal — while keeping every exchange initiated and governed by the bank's own processes. Echoworx delivered exactly that: multi-party secure conversation with controls that keep the institution firmly in charge of who participates and how. Additional Reply All use cases with verification codes were delivered as onboarding enhancements, reinforcing the bank's governance posture without adding complexity for external parties.

S/MIME support, scoped and controlled.

S/MIME represented a small but important slice of the bank's message flows, and the bank wanted tight governance over it. Echoworx provided S/MIME support scoped to a strictly defined group of individuals — giving the institution precise control over a specialized capability without extending access beyond what the compliance framework permitted.

A modern security stack, integrated without disruption.

Echoworx's gateway-agnostic design let the platform process messages to and from any DLP stack, so the bank's parallel migration advanced in step rather than in conflict. Secure web APIs fed real-time security event data into the bank's Splunk SIEM — configured largely by the bank

itself from shared instructions — turning every encrypted communication event into live, reviewable compliance data. SSO through Entra ID via SAML streamlined secure authentication across the platform, with OpenID now available as a modern option for multi-tenant customers.

A public directory that kept the bank's identity intact.

To mirror the bank's existing public presence, Echoworx published PGP keys to its public LDAP directory with aliasing — so the bank could preserve its own public identity and established client expectations while the Echoworx directory worked behind the scenes. Familiar to every client. Modern in every layer.

A pre-production environment, and a partner that responds.

Given the scale and regulatory intensity of this project, the bank required a full pre-production environment to manage, validate, and approve every change before it reached production. Echoworx built a mirrored environment with a completely separate database instance — including matching schema — keeping the project on schedule through rigorous, evidence-based change control. When the bank asked for enhanced audit telemetry, real-time session change monitoring, and additional security hardening around session integrity, those refinements were incorporated directly into the platform. Large enough to serve an institution this demanding. Nimble enough to respond when it mattered.

The Results

The migration delivered on the promise that mattered most: everything the bank relied on carried forward, now modern, hardware-protected, auditable, and resilient.

Full feature parity, achieved.

Every capability of the legacy Symantec PGP-U appliance moved to the cloud intact — PGP encryption, inbound decryption with migrated keys, automatic key harvesting, controlled Reply All, and scoped S/MIME — so nothing the bank depended on was left behind.

Compliance proven under regulator scrutiny.

The platform cleared an exhaustive, process-oriented regulatory review with the certifications, security evidence, and documentation the bank needed to demonstrate it meets every obligation across three jurisdictions.

Hardware-backed key sovereignty.

Amazon KMS and native Cloud HSM delivered hardware-protected key generation, storage, and management — through a dedicated managed key — satisfying the bank's most demanding compliance mandates by design, not by workaround.

Full control over SSL keys and web traffic.

Akamai reverse proxy integration gave the bank complete ownership of its SSL keys and portal traffic, ensuring no public access path fell outside institutional control.

Secure delivery, guaranteed.

PGP with automatic secure portal fallback ensured every recipient could be reached securely, so a missing key never became a message sent in the clear.

Mandatory verification, tied to identity proofing.

Out-of-band verification codes anchored new-user registration to the bank's own standards, while a controlled exception moved thousands of existing, trusted contacts through migration without friction.

Bulk key migration at scale.

Thousands of public and private keys imported via secure web APIs — a near-seamless move that preserved years of accumulated cryptographic trust.

Real-time audit visibility into Splunk.

SIEM integration, configured by the bank from shared instructions, turned every secure communication event into live, reviewable compliance data.

A modernization program that never stalled.

Gateway-agnostic processing carried the bank through its infrastructure migration without interruption, while a mirrored pre-production environment kept every change validated and on schedule.

Enhancements delivered during onboarding.

Enhanced audit telemetry, real-time session change monitoring, and additional Reply All verification use cases were folded into the platform during onboarding — proof that the relationship was built to evolve, not just to deliver.

The Bigger Picture

This bank set out to replace an aging appliance. What it built was something far more durable: a cloud-native, hardware-protected encryption platform that preserved everything it valued and stands ready for the next wave of regulatory demand across three countries.

That is the real lesson here. In a highly regulated, process-heavy institution, the hardest part of modernization is rarely adding something new — it is carrying everything forward without losing a step, while proving it all under regulator review. By choosing a partner able to match its legacy capability precisely, satisfy exhaustive compliance requirements, and adapt throughout a large and complex onboarding, the bank turned a high-stakes migration into a relationship built to last. Feature parity was the floor. Resilience, sovereignty, and a foundation ready for what comes next — that was the ceiling.

Echoworx makes that possible: compliant by design, resilient at scale, and faithful to every flow the people who depend on it already know.

Is your secure communication ready for what's next?

If a legacy PGP appliance is straining under regulatory scrutiny, holding back your cloud strategy, or standing between your institution and its next compliance milestone, there is a better path forward.

[Talk to an Echoworx expert today.](#)