

When Client Trust Cannot Be Compromised

How a Leading Magic Circle Law Firm Modernized Secure Communication — With Every Client Process Intact

Technical Proof Points

Architecture

- AWS-native SaaS, cloud-first throughout
- Integrates with existing Mimecast environment
- No rip-and-replace of the current stack
- Full feature parity with legacy PGP Universal appliance

Control

- Outbound S/MIME with automatic key selection
- Optional PGP via subject-line keyword trigger
- Signing applied to all outbound messages
- LDAP key publishing for firm-wide sharing
- External lookups via Global TrustPoint aggregator

Delivery

- Inbound S/MIME and PGP decryption at the gateway
- Automatic public key harvesting from signed messages
- Post-harvest key stripping keeps inboxes clean
- Aligned with Mimecast inbound policies
- Portal delivery under evaluation for broader use cases

Executive Summary

For a firm that sits at the center of some of the world's most consequential legal matters — cross-border transactions, high-stakes disputes, global investigations, and complex regulatory engagements spanning multiple jurisdictions — secure communication is not a support function. It is part of the practice itself. With clients who bring the most sensitive and commercially critical matters imaginable, this firm's reputation for discretion is as foundational as its legal expertise, and every encrypted message carries the full weight of that standing — a quiet but non-negotiable assurance that what is shared stays protected, handled with the precision and confidentiality the firm's global standing demands.

But the firm's encryption sat on aging ground. A legacy PGP Universal appliance still carried the certificate-based workflows its most demanding clients relied on, yet it was growing harder to maintain and increasingly difficult to align with a modern, cloud-first security posture. For a firm whose partners exchange the most confidential communications imaginable, an encryption layer that couldn't keep pace represented a quiet but serious risk to the one thing that cannot be recovered once lost.

The firm turned to Echoworx for a verified feature-parity replacement — a cloud-native platform that preserved every PGP and S/MIME workflow its clients expected, integrated cleanly with its existing secure email environment, and honored the strict, non-negotiable processes that define high-stakes legal communication.

The outcome: a modern, standards-based encryption foundation that advanced every workflow without disruption, strengthened governance across every exchange, and kept the firm's promise of digital trust secure — message after message, client after client.

The Challenge

01 | A reputation that leaves no room for compromise.

In elite legal practice, trust is the operating currency, and a single mishandled communication can unravel a client relationship built over years. The firm's most important partners and contacts insisted on specific, established encryption processes — precise PGP and S/MIME steps with little room to negotiate. Any replacement platform had to honor those expectations exactly, because for this firm, protecting confidential communication is not an added feature. It is the practice itself.

02 | Legacy encryption that couldn't keep up.

The firm's PGP Universal appliance had served its purpose, but it was becoming harder to maintain and increasingly at odds with a modern, cloud-first approach to security. As a Mimecast customer, the firm needed an encryption layer that would fit cleanly into the environment it already trusted — not a disruptive overhaul that forced its people to relearn how they work. The requirement was precise: preserve every workflow that works, modernize the infrastructure beneath it.

03 | Governance across a complex web of external contacts.

This firm exchanges sensitive matters with partners, clients, and counsel across the globe, each with their own keys, their own directories, and their own expectations. Managing that complexity through aging infrastructure introduced friction and left room for inconsistency. What was needed was a single, governed, standards-based foundation capable of locating the right keys, applying the right protection, and proving control over every message that leaves the firm's perimeter.

The Solution

The firm selected Echoworx following a full proof-of-concept evaluation — one that exercised every workflow and returned a clean result across the board. What made the decision straightforward was this: Echoworx could match the legacy appliance capability for capability, then move it onto a resilient, cloud-native foundation, all while fitting cleanly into the firm's existing secure email environment.

"This firm came to us needing something specific: every PGP and S/MIME workflow their most important clients depend on, preserved without compromise," an Echoworx engagement lead explains. **"We verified every use case in the proof of concept, moved each one across cleanly, and integrated with the secure email environment they already trust. That's what a genuine like-for-like migration looks like in practice — and it's the foundation that lets the relationship keep growing."**

Feature-parity PGP and S/MIME, carried forward with precision.

At the center of the migration was an exact replacement of the firm's certificate encryption. Outbound messages now use S/MIME with automatic key selection based on available recipient keys, with optional PGP triggered by a subject-line keyword — so the people who depend on secure communication kept the exact steps they already knew. Nothing to relearn, nothing to renegotiate. The workflows the firm's clients expect continued without interruption; only the platform beneath them changed.

Signing on every outbound message, trust made visible.

Because S/MIME and PGP sit at the core of how this firm communicates, all outbound mail is routed through Echoworx to sign every message. That signature is more than a technical detail — it is a mark of authenticity on every exchange, giving recipients assurance that a message genuinely originates from the firm and arrives exactly as sent. For an institution whose name carries considerable weight, that provable authenticity is digital trust made tangible.

Inbound decryption and clean, effortless key handling.

Echoworx manages inbound S/MIME and PGP decryption at the gateway, working alongside the firm's email security policies to ensure every incoming message is readable and secure. The platform also harvests public keys from signed messages automatically — and strips those keys

once captured, so they never surface in inboxes or create confusion for end users. Everything happens invisibly at the gateway, keeping the experience clean for the people who rely on it every day.

Global key discovery through trusted directories.

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 text, 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.

Room to grow, at the firm's own pace.

With its certificate encryption now on a modern foundation, the firm is evaluating Echoworx portal delivery as an additional channel — a practical way to extend secure communication to wider use cases and build natural adoption across its people and offices. The infrastructure is in place; the firm can expand on its own terms and timeline.

The Results

The migration delivered on its central promise: every workflow the firm's clients counted on was carried forward, now governed, modernized, and built to endure.

Full workflow continuity, confirmed.

Every certificate encryption capability — outbound S/MIME with auto-select, optional keyword-triggered PGP, inbound decryption, and key harvesting — moved to the cloud without missing a step, so no client relationship felt the transition.

Reputation protected, exchange by exchange.

Signing on all outbound mail gives every communication provable authenticity, reinforcing the trust the firm's name has earned over decades.

Client processes honored without exception.

The exact PGP and S/MIME steps the firm's most demanding partners rely on remained unchanged, so high-profile relationships continued without a break in the chain.

Seamless integration with the existing stack.

Echoworx works directly alongside the firm's email security policies, strengthening the secure communication layer without disrupting the environment already in use.

Global reach, precisely governed.

Integration with external directories — including the Global TrustPoint aggregator — enables the firm to locate the right keys worldwide while keeping key handling automatic and clean at the gateway.

A platform built to expand.

With portal delivery under evaluation, the firm has a clear, low-friction path to extend secure communication to new use cases on its own schedule.

The Bigger Picture

This firm came to Echoworx to replace an aging appliance. What it took away was something far more enduring: a cloud-native encryption foundation where every trusted workflow survived the transition intact — and a platform built to scale alongside a practice that operates at the very edge of international legal complexity, where the matters are unprecedented, the clients are global, and the margin for error is zero.

The real takeaway runs deeper than technology. For a firm whose standing is built on handling the matters that cannot afford to go wrong — the cross-border transactions, the international disputes, the regulatory engagements that set precedent — discretion is not a principle. It is the practice. The hardest measure of a successful modernization is not what was added; it is what was never put at risk. By choosing a platform that could replicate its legacy capabilities precisely, honor the exact processes its most demanding clients insist on, and integrate cleanly into the tools already in use across its global offices, the firm completed one of the most sensitive migrations possible without a single concession to continuity. Exact parity was not the ambition — it was the non-negotiable condition. What it achieved was something rarer: a complete transition that the firm's clients never had reason to notice.

Echoworx makes that possible: secure by design, resilient at scale, and faithful to the workflows the people who rely on it already know.

Is your secure communication ready for what's next?

If a legacy encryption appliance is straining to keep pace with a modern, cloud-first practice — or standing between your firm and the trusted processes your clients insist on — there is a way to move forward without leaving anything behind.

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