CUSTOMER STORY

When Compliance Meets Convenience

How a Leading Irish Commercial Bank Transformed Secure Customer Communication

Technical Proof Points

Architecture

- AWS-native SaaS, cloud-first throughout
- Ireland/EU data residency aligned to DORA & GDPR
- PCI DSS and SOC 2 audited annually, FSQS-registered
- No appliances to rack, patch, or maintain

Control

- Secure sending from shared mailboxes with optional reply routing
- Multi-brand support across parent and affiliate business units
- Shared licensing and infrastructure with no duplicated administration
- Policy-driven delivery and authorization across all channels

Delivery

- Secure portal delivery, PDF, Attachment encryption, TLS with fallback
- Portal self-provisioning — no initial push email required
- Published URL for inbound secure messaging
- Multiple authentication options across every delivery channel

Executive Summary

For a leading Irish commercial bank — ranked among the Top 1000 World Banks and recognized as a digital-first institution serving personal, business, and corporate customers — secure communication is not a back-office concern. It is a regulatory mandate and a promise to every customer.

Under the Digital Operational Resilience Act (DORA) and GDPR, the bank needed encryption that was auditable, resilient, and sovereign. But its existing built-in tooling could not keep pace with the bank's real-world workflows. The result was friction: for staff, for customers, and for the compliance teams accountable when secure communication falls short.

By partnering with Echoworx, the bank transformed customer document handling into a streamlined, secure, and scalable process. The outcome was measurable and immediate — **a 63% increase in encryption adoption**, a simpler experience for customers, and a resilient, cloud-native foundation built to satisfy Europe's most demanding regulatory frameworks.

The Challenge

For a bank of this standing, secure communication is not a background concern. It is a regulatory obligation and a daily promise to every customer.

The bank had been managing secure customer documentation through a built-in encryption tool. On paper, it met a basic bar. In practice, it created friction at every level — for staff, for customers, and for the compliance teams responsible when something falls short.

The obstacles were specific and serious:

01 | No shared mailbox support.
Team-based workflows run through shared email addresses are the backbone of the bank's customer service model and SLA commitments. The existing tool could not accommodate them.

02 | Multi-step manual workflows.
Securing a single customer document required multiple manual steps and staff coordination — draining time and complicating already-stretched rostering.

03 | Forced customer registration.
Customers had to register with an encrypted email service just to access and return their own documents — an unnecessary barrier that undermined the bank's digital-first promise.

04 | Operational drag.
Inefficient processes created resourcing challenges that pulled teams away from higher-value work.

These were not minor inconveniences. For a digitally-led institution with aggressive modernization targets, they were compliance risks and customer experience failures happening simultaneously.

The Evaluation

The bank had done its homework. It arrived at its evaluation with a clear picture of what competing tools could not do.

It came with sharp, specific questions — the most important being: **How do you handle a shared mailbox?**

A rigorous proof of concept followed. The bank was not looking for promises. It wanted every critical workflow demonstrated, under the scrutiny of its own business, regulatory, and regional requirements — including data residency, multi-brand architecture, and the certifications its compliance and security review teams would require.

Echoworx answered every question. The proof of concept confirmed what the bank needed to see: a platform flexible enough to match its exact processes, and a compliance foundation strong enough to satisfy its regulators.

The Solution

Echoworx delivered a cloud-native encryption platform that resolved the bank's operational challenges while placing regulatory compliance at its core.

"This bank came to us with a compliance mandate and a very specific operational problem — and those two things had to be solved together, not separately," says Derek Christian, Echoworx Engagement Manager. "The shared mailbox question told us everything. They knew exactly what they needed, they'd already seen what other tools couldn't do, and they wanted proof — workflow by workflow, under their own regulatory and regional requirements. What we built together didn't just clear their compliance bar. It gave them a foundation that will hold up as DORA and GDPR obligations evolve, and a platform that keeps expanding without adding complexity."

Workflows that match how the bank actually operate

Shared mailbox and reply routing — The collaborative flows that the previous tool could not support now run without friction. Staff send securely from shared mailboxes and route replies to a different address than the sender, enabling true team-based secure communication aligned to the bank's SLA requirements.

Device-agnostic secure composition — Staff compose secure messages and attach files on any device, without organizational prompts or unnecessary interruptions to existing processes.

Portal self-provisioning and inbound secure messaging — Customers access secure communication without requiring an initial outbound push email. The registration barrier is gone. When the bank later needed to extend this further — allowing contacts to initiate secure communication entirely on their own terms — Echoworx enabled inbound secure messaging through a published URL, activated through simple configuration with no new procurement cycle required.

Multi-brand delivery under a single platform.

The bank's mortgage group operates under its own well-recognized affiliate brand — distinct from the parent, but closely connected to it. Echoworx supports multi-brand delivery across business units using shared licensing and shared infrastructure, so the bank never duplicates administration across environments.

continued...

A compliance foundation built to satisfy regulators, auditors, and architecture boards.

This is where the platform's depth matters most.

Echoworx is deployed 100% on AWS and independently recognized as AWS Qualified Software — reviewed against the AWS Well-Architected Framework across security, reliability, and operational excellence. That validation is not a marketing credential. It is the structured, independent evidence that compliance teams, security architects, and procurement reviewers need before they can say yes.

Every encrypted communication is logged across key generation, policy triggers, and delivery states. Audit readiness is not a scramble — it is a standing posture.

DORA demands audited recovery, high availability, and full auditability of third-party communication infrastructure. GDPR demands data-residency control, granular protection, and demonstrable sovereignty. Echoworx maps to both — backed by annual PCI DSS and SOC 2 certification, and documented processes that moved the bank through its security and approval review with speed and confidence.

Regional deployment aligned to Irish and GDPR requirements ensures the bank's data stays exactly where it must — not as an assumption, but as a provable fact backed by AWS-native infrastructure validated across EMEA, including Ireland.

The Results

The impact was measurable, immediate, and lasting — across compliance posture, operational efficiency, and customer experience alike.

Compliance moved from a pressure point to a provable standing posture.

With every encrypted message logged, every policy trigger recorded, and every delivery state captured, the bank can demonstrate compliance under audit rather than scramble for it. DORA and GDPR obligations are not managed reactively — they are met continuously, by design.

63% increase in encryption adoption — driven by trust, not mandate.

The bank uses encryption discretionarily, letting senders decide what to encrypt and when. Adoption grew organically. Usage, volume, and active senders climbed substantially in a short period and kept growing. That trajectory reflects what happens when the underlying platform is resilient, compliant, and genuinely trusted by the people depending on it every day.

Operational friction eliminated.

Manual steps were removed, staff coordination simplified, and the customer registration barrier lifted entirely. Teams recovered time and capacity previously consumed by workarounds — freeing resources for higher-value work.

Seamless, branded customer experience.

Customers gained a secure, frictionless way to exchange sensitive documents — no unnecessary registration, no unfamiliar experience. Encrypted communication now feels like a natural, trusted extension of the bank's service.

A platform that grows with the business.

Because the bank licensed the full Echoworx platform, every new requirement activates through configuration rather than a new contract negotiation. The relationship continues to expand — secure communication stays agile enough to move at the speed of the business.

The Bigger Picture

This bank set out to replace a tool that couldn't keep pace. What it built was something far more durable: a cloud-native, DORA- and GDPR-aligned secure communication platform that eliminated operational friction, turned compliance into a standing posture, and made encrypted communication something employees and customers actually want to use.

That is the real lesson here. For a digitally-led institution, the hardest part of modernization is rarely adding something new — it is replacing what's broken without disrupting what works, while proving every step of it to regulators and auditors. By choosing a partner able to meet its operational requirements precisely, satisfy exhaustive compliance scrutiny, and expand over time without renegotiation, the bank turned a painful tooling problem into a resilient, future-ready foundation.

Echoworx makes that possible: compliant by design, resilient at scale, and built to grow alongside the institutions that depend on it.

Is your secure communication ready for what's next?
If built-in encryption is holding back your compliance posture, creating friction for staff and customers, or standing between your institution and its next modernization milestone, there is a better path forward.
Talk to an Echoworx expert today.