

Two Banks. One Platform. Zero Compromise.

How a Major German Institution Centralized Encryption Across Sovereign Business Units

Technical Proof Points

Deployment model

AWS-native, multi-region:
Ireland + Germany.

Data residency

Data held in-jurisdiction

Key management

FIPS 140-3 validated key
management

Certificate lifecycle handling

DigiCert-automated S/MIME
lifecycle

DLP integration

Mimecast DLP integration

Encryption point

Gateway encryption replaces
desktop ZIP

Standards-based formats

Native PDF, Microsoft Office,
and ZIP

Portal-less delivery

Shared passphrase delivery

Microsoft 365 add-ins

Multi-option menu + single-button

Executive Summary

In the DACH region, few things are watched as closely as how a bank protects the data it moves. Germany, Austria, and Switzerland carry some of the deepest, longest-standing security expectations in the world — expectations written into regulation, reinforced by governance, and felt across every partner and customer relationship. For one major German financial institution, meeting those expectations was not a project. It was a standing obligation.

Yet the bank's encryption ran in the wrong place. A desktop-based Totemo system handled secure ZIP encryption at the endpoint, which meant sensitive files slipped past the hygiene scanning and backup controls the region demands. Worse, the institution wasn't one buyer with one need. Its main bank and its investment arm operated as distinct organizations, each with its own strategy, its own data residency requirements, and its own vision for the cloud.

The bank turned to Echoworx to resolve both problems at once — moving encryption off the desktop and into the cloud, and giving two very different business units the tailored environments they each required, without splintering into two disconnected tools.

The outcome: a single, standards-based encryption platform that pulled fragmented control back to the center, honored strict data sovereignty across separate AWS regions, and let each business unit operate on its own terms — all under one roof.

The Challenge

01 | Encryption happening in the wrong place.

The bank's endpoint approach to secure ZIP encryption looked convenient, but it carried a hidden fault line. When files are encrypted desktop-to-desktop, they never pass through the corporate hygiene scanning and backup processes that DACH compliance treats as non-negotiable. Every ZIP that left an employee's machine left the bank's governance behind with it. For an institution operating under this level of regulatory scrutiny, secure communication that bypasses its own controls isn't secure at all — it's a gap waiting to be found.

02 | A manual habit that didn't fit a modern bank.

Employees were doing the work by hand: bundling files into ZIP packages, setting passwords, and passing those passwords along one exchange at a time. Popular though the pattern still is, even in large organizations, it leaned on people to get every step right and on IT to keep desktop encryption software running across the business. It was effort spent maintaining a workflow, rather than advancing the bank's move to the cloud.

03 | One institution, two very different mandates.

The real complexity ran deeper than any single tool. Inside the same bank, separate stakeholders and business units had charted separate courses. The main bank wanted encryption tied cleanly into its existing DLP and hygiene processes, delivered in a way its external contacts would find effortless. Its investment arm — the financial services division — had an entirely different outlook: cloud-first, cloud-only, built around S/MIME, and bound by strict data residency inside Germany. Each unit was right for its own reasons. The challenge was serving both without fracturing encryption control back into the silos the bank was trying to escape.

The Solution

The bank chose Echoworx precisely because the platform could hold two strategies at once — standardizing security while respecting the sovereignty of each business unit. What tied the whole approach together was breadth of delivery: the same platform offered enough encryption methods to replace legacy tools for both divisions, each on its own terms.

“Two business units, two very different visions — one wanted shared passphrases and ZIP encryption, the other S/MIME through their own DigiCert,” Derek Christian, Echoworx Engagement Manager explains. “Our job was to honor both, keep each unit’s data in its own region, and pull fragmented encryption back under one roof — without either team losing the way they already worked.”

Digital sovereignty, drawn along regional lines.

Data residency in the DACH region is not a checkbox — it’s a mandate, and it can differ from one business unit to the next. Echoworx met that head-on with region-specific AWS deployments. The main bank operated from an Ireland-based AWS region suited to its needs, while the investment arm, which required data to stay inside Germany, deployed in a separate Germany-based region. Using AWS regions and availability zones to anchor each footprint, the platform kept every institution’s data exactly where its governance demanded. Sovereignty, in practice, meant each unit kept command of its own data, in its own jurisdiction.

Encryption pulled back to the gateway.

The single most important shift was moving encryption off the desktop and up to the cloud gateway. There, it slotted directly into the workflows it had been skirting — DLP, hygiene scanning, backup — so every secure message now travels through the controls meant to govern it. For the investment arm, that discipline extended through Echoworx’s long-standing alliance with Mimecast for DLP, aligning cloud-first security with cloud-first strategy. The gap closed not by adding more oversight, but by putting encryption back where oversight already lived.

Standards-based encryption, familiar to everyone who receives it.

Echoworx secured files using the formats external contacts already know and trust — PDF, Microsoft Office, and ZIP. Nothing proprietary sat between the bank and its partners, so recipients could keep working through the same flows they already expected. For an institution whose

reputation rides on frictionless, trustworthy exchanges, standards-based wasn’t a technical footnote. It was the point.

A tailored path for the main bank.

The main bank wanted employees to choose the right protection for each message. Echoworx delivered a custom Microsoft 365 add-in with a purpose-built menu offering two paths: attachment-only encryption, where the email travels in the clear but the files inside are secured, or full message encryption, protecting the body and attachments together as a password-secured PDF. And because the delivery used shared passphrases exchanged out of band, the bank met a requirement its partners quietly value most — portal-less delivery. External contacts open protected messages straight from their inbox, with no account to register and no new password to memorize.

A tailored path for the investment arm.

The investment arm wanted something different, and got it. Its priority was S/MIME, delivered through the division’s own DigiCert subscription. Echoworx automated the full certificate lifecycle — generating, managing, and applying public-private key pairs, harvesting inbound certificates, verifying signatures, and ensuring outbound messages were signed. That automation preserved feature parity with the Totemo environment the arm was leaving, making the migration feel less like a change and more like a continuation. When a recipient held no key, a secure portal stepped in as automatic fallback, so no message ever went out unprotected. And where the main bank offered choice, the investment arm chose simplicity: a single-button add-in — encrypt or don’t — with every routing decision handled quietly on the back end.

The Results

Encryption returned to governed ground.

By moving secure ZIP and attachment encryption from the desktop to the cloud gateway, every message now flows through the hygiene scanning and DLP controls DACH compliance requires — closing a gap the endpoint approach had left wide open.

Sovereignty honored, unit by unit.

Separate AWS deployments in Ireland and Germany kept each business unit's data inside its required jurisdiction, satisfying strict residency mandates without forcing one division's rules onto the other.

Two strategies, one platform.

The main bank and its investment arm each ran the encryption model that fit them — shared passphrase portal-less delivery for one, automated S/MIME for the other — while the institution regained centralized, standards-based control over both.

A hands-off S/MIME lifecycle.

DigiCert integration automated key generation, certificate harvesting, and signature verification for the investment arm, replacing manual key management and preserving full feature parity with its previous solution.

Effortless for the people on the receiving end.

Shared passphrases let the main bank's external contacts open secure messages directly in their inbox — no portal, no registration — while standards-based formats kept every recipient working in tools they already trust.

Nothing left exposed.

Automatic portal fallback guaranteed secure delivery even when a recipient had no key, so a missing certificate never became a security compromise.

A migration that met each unit where it stood.

Both divisions moved off Totemo without abandoning the habits and capabilities their people relied on — feature parity for the investment arm, method-of-choice flexibility for the main bank.

The Bigger Picture

This institution began with a placement problem — encryption running where governance couldn't reach it. What it built was something more durable: a centralized, standards-based foundation that respects, rather than erases, the differences between its business units.

That distinction is the heart of the story. In a large, regulated organization, the hardest part of modernization is rarely the technology — it's serving genuinely different mandates without fragmenting into a patchwork of disconnected tools. By choosing a platform broad enough to deliver S/MIME to one arm and portal-less shared-passphrase encryption to another, deployed in the regions each required, the bank turned that complexity into an advantage. Decentralized control became centralized governance, without a single unit losing the autonomy it needed.

Echoworx makes that possible for organizations of any structure: unified where it matters, sovereign where it counts, and standards-based throughout.

Ready to unify encryption without flattening what makes your business units different?

If desktop-bound encryption is slipping past your controls, or if separate divisions are pulling your security strategy in different directions, there is a way to centralize governance while honoring each unit's mandate.

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