KUNDENGESCHICHTE

Wenn Regulierungsbehörden keinen Spielraum für Fehler lassen.

Wie eine große britische Bank die PGP-Verschlüsselung in drei Ländern modernisierte — bei erhaltener Funktionsparität

Technische Nachweise

Architektur

- AWS-native SaaS, Cloud-first
- Amazon KMS mit dedizierten Cloud-HSM-Schlüsseln
- Hardwaregestützter Schlüsselschutz durchgängig
- Gespiegelte Vorproduktionsumgebung auf separater Datenbank

Kontrolle

- Vollständige Funktionsparität zu PGP-U
- Massenhafter Schlüsselimport über sichere Web-APIs
- Akamai-Reverse-Proxy, kundenseitig verwaltete SSL-Schlüssel
- Entra ID SSO (SAML); OpenID für Multi-Tenant-Umgebungen
- Splunk SIEM über Echtzeit-API

Zustellung

- PGP mit automatischem Fallback auf ein sicheres Portal
- Eingehende PGP-Entschlüsselung mit migrierten Schlüsseln
- Automatisierte Erfassung eingehender öffentlicher Schlüssel
- Kontrolliertes „Allen antworten“ mit Verifizierungscodes
- Optionales S/MIME, nur für eingeschränkte Benutzergruppen

Kurzfassung

Für eine große britische Bank mit Kunden in Großbritannien, Irland und Deutschland ist sichere Kommunikation weit mehr als eine technische Funktion. Jede verschlüsselte Nachricht ist ein regulatorisches Versprechen, ein Schutz für Kundendaten und ein Beleg dafür, dass die Institution mit hochsensiblen Informationen vertrauenswürdig umgeht.

Doch die Verschlüsselungsinfrastruktur der Bank basierte auf einer alternden Symantec-PGP-U-Appliance. Über Jahre hinweg hatte sie eine umfangreiche Bibliothek öffentlicher und privater Schlüssel getragen, wurde jedoch zunehmend schwerer wartbar, schwerer skalierbar und unter intensiver regulatorischer Prüfung immer schwieriger zu vertreten. Die Bank musste modernisieren, ohne Schlüssel, Kommunikationsflüsse oder Vertrauen zu verlieren.

Deshalb entschied sie sich für Echoworx: eine vollständig auf AWS betriebene SaaS-Plattform, die eine echte Eins-zu-eins-Migration ermöglichen sollte — mit vollständiger Funktionsparität, hardwaregestütztem Schlüsselschutz und einer cloudnativen Grundlage für weiteres Wachstum.

Das Ergebnis war eine moderne, auditierbare und standardbasierte Verschlüsselungsplattform, die bestehende Funktionen vollständig übernahm, eine umfassende Compliance-Prüfung bestand und die Bank belastbar auf künftige regulatorische Anforderungen vorbereitete.

Die Herausforderung

01 | Ein Compliance-Umfeld ohne Fehlerspielraum.
Diese Bank agiert in einem Umfeld, in dem Aufsichtsbehörden genau hinschauen und Verhandlungsspielraum nicht besteht. Jede neue Plattform musste eine umfangreiche, prozessorientierte Prüfung bestehen — mit detaillierter Dokumentation, Sicherheitsnachweisen, Zertifizierungen und belastbaren Belegen für jede architektonische Aussage. Die Symantec-PGP-U-Appliance war zwar lange verlässlich, blieb jedoch an eine On-Premises-Infrastruktur gebunden, die sich unter heutigen Anforderungen an Resilienz immer schwerer rechtfertigen ließ. Für ein Institut mit Verantwortung in drei Ländern bedeutete eine Verschlüsselungslösung ohne klar nachweisbaren hardwaregestützten Schlüsselschutz und auditierbare Governance ein regulatorisches Risiko.

02 | Eine Migration, bei der nichts verloren gehen durfte.
Die Bank verfügte über eine umfangreiche Bibliothek öffentlicher und privater PGP-Schlüssel, etablierte Kommunikationsflüsse und langjährige Mandanten- bzw. Kundenbeziehungen, die darauf aufbauten. Dass bei der Migration irgendetwas davon verloren gehen könnte, war ausgeschlossen. Gefordert war echte Funktionsparität — dasselbe Verschlüsselungsverhalten, dieselben Zustellungsmuster und dieselbe vertraute Erfahrung für Tausende externer Kontakte, nur ohne Unterbrechung. Jeder Schlüssel musste migriert werden. Jeder Ablauf musste ab dem ersten Tag funktionieren.

03 | Ein Modernisierungsprogramm, das nicht ins Stocken geraten durfte.
Die Verschlüsselung stand nicht für sich allein. Die Bank trieb bereits eine umfassendere Infrastrukturmodernisierung voran, darunter die Migration ihres Gateways von Cisco IronPort zu Proofpoint, und brauchte deshalb eine Verschlüsselungsplattform, die Nachrichten vor, während und nach dieser Umstellung nahtlos verarbeiten konnte. Ein Werkzeug, das dem Gesamtprogramm im Weg stand oder ihm einen eigenen Zeitplan aufzwang, hätte das gesamte Vorhaben gebremst. Gesucht war ein Partner, der gleichzeitig mit hoher regulatorischer Komplexität, intensiver Abstimmung mit Stakeholdern und einem großen, anspruchsvollen Onboarding Schritt halten konnte.

Die Lösung

Die Bank entschied sich für Echoworx, weil die Plattform die Funktionen ihrer bisherigen Symantec-Appliance vollständig abbilden konnte — und diese zugleich auf eine moderne, cloudnative und hardwaregeschützte Grundlage überführte. Entscheidend für den Erfolg der Partnerschaft waren dabei sowohl technische Tiefe als auch Flexibilität: die Fähigkeit, präzise Anforderungen zu erfüllen, sich direkt in Change-Management- und Compliance-Prozesse der Institution einzubringen, sich an neue Projektanforderungen anzupassen und jeden Schritt gegenüber den entscheidenden Prüfinstanzen belastbar nachzuweisen.

„Diese Bank kam mit einer der anspruchsvollsten Anforderungen auf uns zu, die wir je gesehen haben — eine echte Eins-zu-eins-Migration unter intensiver Einbindung der Aufsicht, ohne Spielraum für Fehler", sagt Derek Christian, Engagement Manager bei Echoworx. „Unsere Aufgabe war es, jeden Schlüssel, jeden Ablauf und jede Funktion ohne Unterbrechung zu übertragen, alles mit belastbaren Nachweisen für die Regulierungsbehörden zu belegen und während des gesamten Projektverlaufs reaktionsfähig zu bleiben. Funktionsparität war dabei nur der Ausgangspunkt. Was wir gemeinsam aufgebaut haben, geht weit darüber hinaus."

Hardwaregestütztes Schlüsselmanagement — direkt in die Plattform integriert

Cloud HSM war für dieses Institut nicht verhandelbar. Da Echoworx eine vollständig auf AWS betriebene SaaS-Plattform ist, sind Amazon KMS und natives Cloud HSM von Grund auf integriert — nicht nachträglich angebunden. Sämtliche Verschlüsselungsschlüssel werden in hardwaregeschützter Infrastruktur über einen dedizierten Managed Key erzeugt, gespeichert und verwaltet.
So konnten selbst die strengsten Compliance-Anforderungen der Bank erfüllt werden, ohne dass eine separate Zusatzlösung erforderlich war. Darüber hinaus gab die Integration mit dem Akamai-Reverse-Proxy der Bank dem Institut die volle Kontrolle über die für Web- und Portalzugriffe verwendeten SSL-Schlüssel und leitete den gesamten Datenverkehr über die eigenen kontrollierten Kanäle der Bank. Zusammen verschafften diese Fähigkeiten der Bank durchgängige kryptografische Kontrolle — über Schlüssel, Datenverkehr und Zugriffe, vollständig unter institutioneller Governance.

PGP-Verschlüsselung — erhalten und modernisiert

Im Zentrum der Migration stand die PGP-Anforderung der Bank. Echoworx führte sie vollständig weiter — mit PGP-Verschlüsselung überall dort, wo Empfängerschlüssel verfügbar waren, und mit automatischer Weiterleitung an ein sicheres Portal, wenn dies nicht der Fall war. Diese Architektur sicherte genau das Ergebnis, das für die Bank am wichtigsten war: Jede Nachricht erreicht ihren Empfänger, und jede Nachricht bleibt geschützt.

Die eingehende PGP-Entschlüsselung arbeitete mit denselben aus der Symantec-Appliance migrierten Schlüsseln weiter und bewahrte so sämtliche bestehenden Kommunikationsbeziehungen. Die automatische Erfassung öffentlicher PGP-Schlüssel aus neuen eingehenden Nachrichten ließ die Schlüsseldatenbank zudem ohne manuellen Aufwand weiter wachsen.

Massenmigration von Schlüsseln — in großem Maßstab bewältigt

Tausende öffentliche und private PGP-Schlüssel manuell zu übertragen, war nie realistisch. Die sicheren Web-APIs von Echoworx ermöglichten es der Bank, diese per automatisierten Skripten gesammelt zu importieren — eine praktisch nahtlose Migration für eine über Jahre gewachsene Schlüsselinfrastruktur. Die Schlüssel, auf die die Bank angewiesen war, wurden sauber übernommen und waren vom ersten Tag an einsatzbereit. das Echoworx-Verzeichnis im Hintergrund arbeitete. Für jeden Kunden vertraut. In jeder Schicht modern.

Fortsetzung..

Verpflichtende Verifizierung — ohne Reibung am ersten Tag

Sicherheit beginnt bei der Registrierung. Echoworx setzte für jeden neuen Empfänger eine automatisierte sichere Benutzerverifizierung durch: Ein systemgenerierter Code, der außerhalb des eigentlichen Kanals per Telefon oder SMS übermittelt wird, verknüpft die Portalregistrierung direkt mit den eigenen Standards der Bank zur Identitätsprüfung. Ab diesem Zeitpunkt verwalten die Nutzer ihre Zugangsdaten selbst im Self-Service. Gleichzeitig durfte das Onboarding Tausender bereits vertrauter Kontakte am Tag der Migration nicht zu Tausenden gleichzeitigen Verifizierungshürden führen. Deshalb nutzte die Bank ihre bestehende Plattform, um Willkommensnachrichten zu versenden, und Echoworx ermöglichte für diese bereits verifizierten Bestandsnutzer eine kontrollierte, bewusst gesetzte Ausnahme. Für alle neuen Nutzer ab diesem Zeitpunkt galt dann der vollständige, verbindliche Verifizierungsstandard. Hohe Sicherheit dort, wo sie entscheidend ist — und ein reibungsloses Onboarding dort, wo es sinnvoll war.

Sichere Zusammenarbeit — unter der Governance der Bank

Die Bank benötigte Reply-all-Abläufe, mit denen externe Parteien sicher mit der Bank und untereinander über das Portal kommunizieren konnten — wobei jede Interaktion weiterhin von den Prozessen der Bank ausgehen und durch diese gesteuert werden musste. Genau das lieferte Echoworx: sichere Mehrparteien-Kommunikation mit Kontrollen, die der Institution die volle Hoheit darüber geben, wer teilnimmt und auf welche Weise. Zusätzliche Reply-all-Anwendungsfälle mit Verifizierungscodes wurden als Erweiterungen im Onboarding umgesetzt und stärkten die Governance-Position der Bank, ohne die Komplexität für externe Parteien zu erhöhen.

S/MIME-Unterstützung — klar begrenzt und kontrolliert

S/MIME machte nur einen kleinen, aber wichtigen Teil der Nachrichtenflüsse der Bank aus, und die Bank wollte diesen Bereich eng steuern. Echoworx stellte S/MIME-Unterstützung bereit, die auf eine klar definierte Gruppe von Personen beschränkt war. So erhielt die Institution präzise Kontrolle über eine spezialisierte Funktion, ohne den Zugriff über den durch das Compliance-Rahmenwerk erlaubten Kreis hinaus auszuweiten.

Ein moderner Security-Stack — ohne Unterbrechung integriert

Dank des gateway-agnostischen Designs von Echoworx konnte die Plattform Nachrichten zu und von jedem DLP-Stack verarbeiten, sodass die parallele Migration der Bank nicht ausgebremst, sondern nahtlos unterstützt wurde. Sichere Web-APIs speisten Sicherheitsereignisse in Echtzeit in das Splunk-SIEM der Bank ein — weitgehend von der Bank selbst auf Basis gemeinsamer Vorgaben konfiguriert — und machten damit jedes Ereignis verschlüsselter Kommunikation zu live auswertbaren Compliance-Daten. SSO über Entra ID via SAML vereinfachte die sichere Authentifizierung über die gesamte Plattform hinweg; zusätzlich steht OpenID inzwischen als moderne Option für Multi-Tenant-Kunden zur Verfügung.

Ein öffentliches Verzeichnis, das die Identität der Bank wahrte

Um die bestehende öffentliche Präsenz der Bank abzubilden, veröffentlichte Echoworx PGP-Schlüssel in seinem öffentlichen LDAP-Verzeichnis — mit Alias-Funktion. So konnte die Bank ihre eigene öffentliche Identität und die etablierten Erwartungen ihrer Kunden bewahren, während durch rigorose, nachweisbasierte Change-Control-Prozesse im Zeitplan. Als die Bank erweiterte Audit-Telemetrie, Echtzeit-Monitoring von Sitzungsänderungen und zusätzliche Security-Härtung rund um die Sitzungsintegrität verlangte, wurden diese Anpassungen direkt in die Plattform aufgenommen. Groß genug für ein Institut mit diesen Anforderungen. Beweglich genug, um dann zu reagieren, wenn es darauf ankam.

Eine Vorproduktionsumgebung — und ein Partner, der reagiert

Angesichts von Umfang und regulatorischer Komplexität des Projekts benötigte die Bank eine vollständige Vorproduktionsumgebung, um Änderungen vor dem Go-live zu prüfen und freizugeben. Echoworx stellte dafür eine gespiegelte Umgebung mit separater Datenbankinstanz und identischem Schema bereit und hielt das Projekt durch belastbare Change-Control-Prozesse im Zeitplan. Erweiterte Audit-Telemetrie, Echtzeit-Monitoring von Sitzungsänderungen und zusätzliche Härtung der Sitzungsintegrität wurden direkt in die Plattform integriert. Groß genug für diese Anforderungen. Beweglich genug, um zu reagieren, wenn es darauf ankam

Die Ergebnisse

Die Migration hielt genau das Versprechen, auf das es der Bank am meisten ankam: Alles, worauf sie sich verlassen hatte, wurde nahtlos übernommen — jetzt modern, hardwaregeschützt, auditierbar und resilient.

Vollständige Funktionsparität — erreicht.

Sämtliche Funktionen der bisherigen Symantec-PGP-U-Appliance wurden vollständig in die Cloud überführt — darunter PGP-Verschlüsselung, eingehende Entschlüsselung mit migrierten Schlüsseln, automatische Schlüsselerfassung, kontrolliertes Reply All und gezielt bereitgestelltes S/MIME. Nichts von dem, worauf die Bank angewiesen war, blieb zurück.

Compliance — unter regulatorischer Prüfung nachgewiesen.

Die Plattform bestand eine umfassende, prozessorientierte aufsichtsrechtliche Prüfung mit genau den Zertifizierungen, Sicherheitsnachweisen und der Dokumentation, die die Bank benötigte, um ihre Anforderungen in allen drei Rechtsräumen belastbar zu erfüllen.

Hardwaregestützte Schlüsselsouveränität.

Amazon KMS und natives Cloud HSM ermöglichten hardwaregeschützte Generierung, Speicherung und Verwaltung von Schlüsseln — über einen dedizierten Managed Key. Damit wurden selbst die anspruchsvollsten Compliance-Vorgaben der Bank von Grund auf erfüllt, nicht über Umwege.

Volle Kontrolle über SSL-Schlüssel und Web-Traffic.

Die Integration des Akamai-Reverse-Proxys gab der Bank die vollständige Hoheit über ihre SSL-Schlüssel und den Portal-Traffic und stellte sicher, dass kein öffentlicher Zugriffspfad außerhalb der institutionellen Kontrolle lag.

Sichere Zustellung — garantiert.

PGP mit automatischem Fallback auf ein sicheres Portal stellte sicher, dass jeder Empfänger sicher erreicht werden konnte, sodass ein fehlender Schlüssel nie dazu führte, dass eine Nachricht unverschlüsselt versendet wurde.

Verpflichtende Verifizierung — an die Identitätsprüfung gekoppelt.

Out-of-Band-Verifizierungscodes verankerten die Registrierung neuer Nutzer in den bankeigenen Standards zur Identitätsprüfung, während eine kontrollierte Ausnahme Tausende bestehende, bereits vertrauenswürdige Kontakte nahezu reibungslos durch die Migration führte.

Massenmigration von Schlüsseln — in großem Maßstab.

Tausende öffentliche und private Schlüssel wurden über sichere Web-APIs importiert — ein nahezu nahtloser Übergang, der über Jahre gewachsenes kryptografisches Vertrauen bewahrte.

Echtzeit-Audit-Transparenz in Splunk.

Die SIEM-Integration, von der Bank auf Basis gemeinsamer Vorgaben konfiguriert, machte jedes Ereignis sicherer Kommunikation zu live auswertbaren Compliance-Daten.

Ein Modernisierungsprogramm, das nie ins Stocken geriet.

Das gateway-agnostische Processing trug die Bank ohne Unterbrechung durch ihre Infrastrukturmigration, während eine gespiegelte Vorproduktionsumgebung dafür sorgte, dass jede Änderung validiert wurde und das Projekt im Zeitplan blieb.

Erweiterungen bereits während des Onboardings umgesetzt.

Erweiterte Audit-Telemetrie, Echtzeit-Monitoring von Sitzungsänderungen und zusätzliche Reply-all-Anwendungsfälle mit Verifizierung wurden bereits während des Onboardings in die Plattform integriert — ein Beleg dafür, dass diese Partnerschaft auf Weiterentwicklung ausgelegt war, nicht nur auf reine Lieferung.

Das große Ganze

Diese Bank wollte ursprünglich eine veraltete Appliance ersetzen. Was sie stattdessen aufgebaut hat, ist weit tragfähiger: eine cloudnative, hardwaregeschützte Verschlüsselungsplattform, die alles bewahrt, was für sie wichtig war, und zugleich bereit ist für die nächste Welle regulatorischer Anforderungen in drei Ländern.

Genau darin liegt die eigentliche Erkenntnis. In einem hochregulierten, prozessintensiven Institut besteht die größte Herausforderung der Modernisierung nur selten darin, etwas Neues hinzuzufügen — sondern darin, alles Bestehende ohne Bruch weiterzuführen und dies zugleich unter regulatorischer Prüfung belastbar nachzuweisen. Indem die Bank einen Partner gewählt hat, der ihre bestehende Funktionalität präzise abbilden, umfassende Compliance-Anforderungen erfüllen und sich während eines großen, komplexen Onboardings flexibel anpassen konnte, wurde aus einer Migration mit hohem Einsatz eine Partnerschaft mit langfristiger Perspektive.

Funktionsparität war die Basis. Resilienz, Souveränität und ein Fundament für das, was als Nächstes kommt — das war das eigentliche Ziel.

Echoworx macht genau das möglich: Compliance by Design, Resilienz im großen Maßstab und Verlässlichkeit für jeden Ablauf, den die Menschen, die täglich darauf angewiesen sind, bereits kennen.

Ist Ihre sichere Kommunikation bereit für das, was als Nächstes kommt?
Wenn eine veraltete PGP-Appliance unter regulatorischem Druck an ihre Grenzen stößt, Ihre Cloud-Strategie ausbremst oder zwischen Ihrem Institut und dem nächsten Compliance-Meilenstein steht, gibt es einen besseren Weg nach vorn.
Sprechen Sie noch heute mit einem Echoworx-Experten.