

Quand les régulateurs ne laissent aucune place à l'erreur.

Comment une grande banque britannique a modernisé le chiffrement PGP dans trois pays — à parité fonctionnelle constante

Éléments techniques clés

Architecture

- SaaS cloud native sur AWS
- Amazon KMS avec clés CloudHSM dédiées
- Protection des clés adossée à du matériel sécurisé de bout en bout
- Préproduction miroir sur base de données distincte

Contrôle

- Parité fonctionnelle complète avec PGP-U
- Importation massive des clés via des API web sécurisées
- Reverse proxy Akamai avec clés SSL gérées par le client
- SSO Entra ID (SAML) ; OpenID pour l'environnement multi-tenant
- Intégration Splunk SIEM via API en temps réel

Remise

- PGP avec bascule automatique vers un portail sécurisé
- Déchiffrement PGP entrant à l'aide des clés migrées
- Collecte automatisée des clés publiques entrantes
- Fonction Répondre à tous contrôlée avec codes de vérification
- S/MIME en option, réservé à un groupe restreint d'utilisateurs

Résumé de direction

Pour une grande banque britannique au service de clients au Royaume-Uni, en Irlande et en Allemagne, la communication sécurisée revêt une importance que peu de secteurs mesurent pleinement. Chaque message chiffré représente un engagement réglementaire, une protection des données clients et une preuve discrète que l'institution mérite la confiance qu'on lui accorde. Dans la banque, cette confiance n'est pas accessoire. Elle est le socle de tout le reste.

Pourtant, son chiffrement reposait sur une base vieillissante. Une appliance Symantec PGP-U héritée prenait en charge une vaste bibliothèque de clés publiques et privées — constituée au fil d'années d'échanges de confiance avec les clients — mais devenait de plus en plus difficile à maintenir, à faire évoluer et à défendre face au niveau d'examen réglementaire que l'institution subit chaque jour. La banque devait se moderniser sans perdre une seule clé, un seul flux ni un seul jour de confiance.

La banque s'est tournée vers Echoworx pour une migration véritablement à l'identique : une plateforme SaaS entièrement opérée sur AWS, conçue pour préserver chaque capacité fournie par l'appliance historique, satisfaire un processus d'évaluation rigoureux mené sous l'impulsion des régulateurs, et offrir à l'institution une base cloud native capable d'évoluer. L'exigence était claire dès le départ : parité fonctionnelle, aucun compromis, et une protection des clés adossée à du matériel sécurisé que les régulateurs pourraient examiner et valider.

Le résultat : une plateforme de chiffrement moderne et auditable, qui a préservé les capacités historiques, satisfait aux exigences de conformité et donné à la banque une base résiliente pour la suite.

Le défi

01 | Un environnement de conformité qui ne laisse aucune place à l'erreur

Cette banque évolue dans un contexte où les régulateurs exercent une surveillance étroite et où la négociation n'est pas une option. Toute nouvelle plateforme devait résister à un examen approfondi, centré sur les processus : documentation détaillée, preuves de sécurité, certifications et validation de chaque choix d'architecture. L'apppliance Symantec PGP-U, fiable en son temps, restait liée à une infrastructure sur site devenue de plus en plus difficile à justifier au regard des exigences modernes de résilience. Pour une institution responsable dans trois pays, un chiffrement incapable de démontrer clairement une protection des clés adossée à du matériel sécurisé et une gouvernance auditable constituait une exposition réglementaire en attente de se matérialiser.

02 | Une migration qui ne pouvait rien perdre

La banque disposait d'une vaste bibliothèque de clés PGP publiques et privées, de flux de communication établis et de relations clients de longue date construites sur cet ensemble. En perdre une partie pendant la migration n'était pas envisageable. L'institution avait besoin d'une véritable parité fonctionnelle : le même comportement de chiffrement, les mêmes schémas de remise, la même expérience de confiance pour des milliers de contacts externes — le tout sans interruption. Chaque clé devait être migrée. Chaque flux devait fonctionner dès le premier jour.

03 | Un programme de modernisation qui ne pouvait pas ralentir

Le chiffrement n'existait pas en vase clos. La banque menait déjà une transformation plus large de son infrastructure, notamment une migration de passerelle de Cisco IronPort vers Proofpoint, et elle avait besoin d'une plateforme de chiffrement capable de traiter les messages de manière fluide avant, pendant et après ce changement. Un outil qui serait entré en conflit avec ce programme global — ou aurait imposé son propre calendrier — aurait ralenti l'ensemble. La banque avait besoin d'un partenaire capable d'avancer au même rythme malgré de fortes contraintes réglementaires, une mobilisation étendue des parties prenantes et un onboarding vaste et complexe.

La solution

La banque a choisi Echoworx précisément parce que la plateforme était capable d'égaliser, fonctionnalité pour fonctionnalité, les capacités de son appliance Symantec historique, puis de les prolonger sur une base moderne, cloud native et protégée par du matériel sécurisé. Ce qui a rendu ce partenariat efficace, c'est à la fois sa profondeur et sa flexibilité : la capacité à répondre à des exigences extrêmement strictes, à s'intégrer directement aux processus de gestion du changement et de conformité de l'institution, à s'adapter lorsque le projet l'exigeait, et à démontrer chaque étape aux personnes dont l'approbation était indispensable.

« Cette banque est venue vers nous avec l'une des exigences les plus exigeantes que nous ayons rencontrées : une véritable migration un pour un dans un contexte d'implication réglementaire intense, sans aucune marge d'erreur », explique Derek Christian, Engagement Manager chez Echoworx. « Notre mission était de transférer chaque clé, chaque flux et chaque capacité sans interruption, d'en apporter la preuve aux régulateurs, et de rester réactifs à mesure que le projet évoluait. La parité fonctionnelle n'était que le point de départ. Ce que nous avons construit ensemble va bien au-delà. »

Une gestion des clés adossée à du matériel sécurisé, intégrée nativement à la plateforme

CloudHSM était une exigence non négociable pour cette institution. Parce qu'Echoworx est une plateforme SaaS entièrement opérée sur AWS, Amazon KMS et CloudHSM natif y sont intégrés par conception — et non ajoutés après coup. Toutes les clés de chiffrement sont générées, stockées et administrées dans une infrastructure protégée par du matériel sécurisé, au moyen d'une clé dédiée gérée, répondant ainsi aux exigences de conformité les plus strictes de la banque sans nécessiter de solution distincte. En parallèle, l'intégration avec le reverse proxy Akamai de la banque a donné à l'institution un contrôle total sur les clés SSL utilisées pour l'accès web et portail, en faisant transiter l'ensemble du trafic par ses propres canaux maîtrisés. Ensemble, ces capacités ont offert à la banque une maîtrise cryptographique de bout en bout — clés, trafic et accès, entièrement sous gouvernance institutionnelle.

Un chiffrement PGP préservé et modernisé

Au cœur de la migration se trouvait l'exigence PGP de la banque. Echoworx l'a intégralement maintenue — en utilisant le chiffrement PGP partout où des clés destinataires étaient disponibles, et en basculant automatiquement vers un portail sécurisé lorsqu'elles ne l'étaient pas. Ce choix de conception garantissait le résultat le plus important pour la banque : chaque message parvient à son destinataire, et chaque message reste sécurisé. Le déchiffrement PGP entrant reposait sur les mêmes clés migrées depuis l'appliance Symantec, préservant ainsi chaque relation

existante. La collecte automatique des clés publiques PGP à partir des nouveaux messages entrants a, quant à elle, permis d'enrichir la bibliothèque en continu, sans effort manuel.

Migration massive des clés, à grande échelle

Migrer manuellement des milliers de clés PGP publiques et privées n'était tout simplement pas réaliste. Les API web sécurisées d'Echoworx ont permis à la banque de les importer en masse via des scripts automatisés — une migration pratiquement fluide pour une bibliothèque de clés constituée au fil des années. Les clés sur lesquelles la banque s'appuyait ont été transférées proprement, prêtes à fonctionner dès le premier jour.

Un environnement de préproduction — et un partenaire réactif

Compte tenu de l'ampleur du projet et de son intensité réglementaire, la banque exigeait un environnement complet de préproduction afin de gérer, valider et approuver chaque changement avant son passage en production. Echoworx a mis en place un environnement miroir avec une instance de base de données entièrement distincte — y compris un schéma identique — afin de maintenir le projet sur les rails grâce à un contrôle des changements rigoureux et fondé sur des preuves. Lorsque la banque a demandé un renforcement de la télémétrie d'audit, une surveillance en temps réel des changements de session, ainsi que des mesures supplémentaires de durcissement de la sécurité

autour de l'intégrité des sessions, ces améliorations ont été directement intégrées à la plateforme. Suffisamment solide pour répondre aux exigences d'une institution de cette envergure. Suffisamment agile pour s'adapter quand cela comptait vraiment.

Vérification obligatoire, sans friction au démarrage

La sécurité commence dès l'inscription. Echoworx a imposé une vérification sécurisée automatisée pour chaque nouveau destinataire : un code généré par le système, transmis hors bande par téléphone ou SMS, relie directement l'inscription au portail aux propres standards de vérification d'identité de la banque. À partir de là, les utilisateurs gèrent eux-mêmes leurs identifiants en libre-service. Mais, le jour de la migration, l'intégration de milliers de contacts déjà approuvés ne pouvait pas se traduire par des milliers d'étapes de vérification simultanées. La banque a donc utilisé sa plateforme existante pour envoyer les messages de bienvenue, et Echoworx a prévu une exception contrôlée et délibérée pour ces utilisateurs existants, déjà vérifiés. Tous les nouveaux utilisateurs ensuite ont été soumis au standard complet et permanent de vérification. Une sécurité renforcée là où elle compte, et une intégration fluide là où elle était nécessaire.

Une collaboration sécurisée, sous gouvernance bancaire

La banque avait besoin de flux Répondre à tous permettant aux parties externes de communiquer en toute sécurité avec la banque et entre elles via le portail, tout en veillant à ce que chaque échange soit initié et encadré par ses propres processus. Echoworx a répondu précisément à ce besoin : une conversation sécurisée multipartite, avec des contrôles qui permettent à l'institution de garder une maîtrise complète des participants et des modalités d'échange. Des cas d'usage supplémentaires autour de Répondre à tous, avec codes de vérification, ont également été mis en place dans le cadre des améliorations d'onboarding, renforçant la posture de gouvernance de la banque sans ajouter de complexité pour les parties externes.

Une prise en charge S/MIME ciblée et maîtrisée

S/MIME représentait une part réduite mais importante des flux de messagerie de la banque, qui souhaitait en conserver une gouvernance étroite. Echoworx a fourni une prise en charge S/MIME limitée à un groupe strictement défini d'utilisateurs, offrant ainsi à l'institution un contrôle précis sur cette capacité spécialisée, sans élargir l'accès au-delà de ce qu'autorisait son cadre de conformité.

Une pile de sécurité moderne, intégrée sans perturbation

Grâce à sa conception indépendante des passerelles, Echoworx a permis à la plateforme de traiter les messages entrants et sortants avec n'importe quelle pile DLP, de sorte que la migration parallèle de la banque a pu avancer en cohérence plutôt qu'en conflit. Des API web sécurisées ont alimenté le SIEM Splunk de la banque en données de sécurité en temps réel — une configuration largement mise en place par la banque elle-même à partir d'instructions partagées — transformant chaque événement de communication chiffrée en donnée de conformité exploitable et vérifiable en continu. L'authentification unique via Entra ID avec SAML a simplifié l'accès sécurisé à l'ensemble de la plateforme, tandis qu'OpenID est désormais disponible comme option moderne pour les clients multi-tenant.

Un annuaire public qui a préservé l'identité de la banque

Pour refléter la présence publique existante de la banque, Echoworx a publié les clés PGP dans son annuaire LDAP public avec un système d'alias. La banque a ainsi pu conserver sa propre identité publique et les attentes établies de ses clients, tandis que l'annuaire Echoworx opérait en arrière-plan. Une expérience familière pour chaque client. Une modernisation à tous les niveaux. autour de l'intégrité des sessions, ces améliorations ont été directement intégrées à la plateforme. Suffisamment solide pour répondre aux exigences d'une institution de cette envergure. Suffisamment agile pour s'adapter quand cela comptait vraiment.

Résultats

La migration a tenu la promesse la plus essentielle : tout ce sur quoi la banque s'appuyait a été préservé, désormais sur une base moderne, protégée par du matériel sécurisé, auditable et résiliente.

Full feature parity, achieved.

Chaque capacité de l'appliance historique Symantec PGP-U a été intégralement portée vers le cloud — chiffrement PGP, déchiffrement entrant à partir des clés migrées, collecte automatique des clés, Répondre à tous contrôlé et S/MIME à périmètre restreint — de sorte qu'aucune fonctionnalité essentielle pour la banque n'a été laissée de côté.

Conformité démontrée sous examen réglementaire

La plateforme a franchi avec succès un examen réglementaire exhaustif et fortement centré sur les processus, avec l'ensemble des certifications, preuves de sécurité et documents nécessaires pour permettre à la banque de démontrer qu'elle satisfait à toutes ses obligations dans trois juridictions.

Souveraineté des clés adossée à du matériel sécurisé

Amazon KMS et CloudHSM natif ont permis la génération, le stockage et l'administration des clés dans une infrastructure protégée par du matériel sécurisé — au moyen d'une clé dédiée gérée — répondant par conception, et non par contournement, aux exigences de conformité les plus strictes de la banque.

Full control over SSL keys and web traffic.

L'intégration avec le reverse proxy Akamai a donné à la banque une maîtrise complète de ses clés SSL et du trafic de son portail, garantissant qu'aucun point d'accès public n'échappe au contrôle institutionnel.

Remise sécurisée, garantie

Le chiffrement PGP, associé à une bascule automatique vers un portail sécurisé, a garanti que chaque destinataire puisse être joint de manière sécurisée, de sorte qu'une clé manquante ne se transforme jamais en message envoyé en clair.

Vérification obligatoire, alignée sur la preuve d'identité

Des codes de vérification hors bande ont ancré l'inscription des nouveaux utilisateurs dans les propres standards de vérification d'identité de la banque, tandis qu'une exception contrôlée a permis de faire passer des milliers de contacts existants et déjà approuvés à travers la migration sans friction.

Migration massive des clés à grande échelle

Des milliers de clés publiques et privées ont été importées via des API web sécurisées — une transition quasi transparente qui a préservé des années de confiance cryptographique accumulée.

Visibilité d'audit en temps réel dans Splunk

L'intégration au SIEM Splunk, configurée par la banque à partir d'instructions partagées, a transformé chaque événement de communication sécurisée en donnée de conformité en temps réel, exploitable et vérifiable.

Un programme de modernisation qui n'a jamais ralenti

Le traitement indépendant des passerelles a permis à la banque de poursuivre sa migration d'infrastructure sans interruption, tandis qu'un environnement miroir de préproduction a garanti que chaque changement soit validé et maintenu dans le calendrier prévu.

Des améliorations livrées dès l'onboarding

Le renforcement de la télémétrie d'audit, la surveillance en temps réel des changements de session et des cas d'usage supplémentaires de vérification pour Répondre à tous ont été intégrés à la plateforme dès la phase d'onboarding — preuve d'une relation pensée pour évoluer, et pas seulement pour livrer.

Une vision plus large

Cette banque avait entrepris de remplacer une appliance vieillissante. Ce qu'elle a construit est bien plus durable : une plateforme de chiffrement cloud native, protégée par du matériel sécurisé, qui a préservé tout ce à quoi elle tenait et qui est prête à faire face à la prochaine vague d'exigences réglementaires dans trois pays.

C'est là la véritable leçon. Dans une institution fortement réglementée et très structurée par les processus, la partie la plus difficile de la modernisation n'est que rarement l'ajout de quelque chose de nouveau — c'est la capacité à tout faire évoluer sans perdre le rythme, tout en démontrant chaque élément sous examen réglementaire. En choisissant un partenaire capable de reproduire avec précision ses capacités historiques, de satisfaire à des exigences de conformité exhaustives et de s'adapter tout au long d'un onboarding vaste et complexe, la banque a transformé une migration à forts enjeux en une relation conçue pour durer.

La parité fonctionnelle était le point de départ. La résilience, la souveraineté et une base prête pour ce qui vient ensuite — voilà ce qui représentait l'objectif ultime.

Echoworx rend cela possible : une conformité intégrée dès la conception, une résilience à grande échelle et une fidélité absolue à chaque flux déjà maîtrisé par les personnes qui en dépendent.

Votre communication sécurisée est-elle prête pour la suite ?

Si une appliance PGP héritée peine à répondre aux exigences réglementaires, freine votre stratégie cloud ou se dresse entre votre institution et sa prochaine étape de conformité, il existe une meilleure voie à suivre.

[Échangez dès aujourd'hui avec un expert Echoworx.](#)