PrimeFactors™
APPLIED DATA PROTECTION

One of the World's Largest Banks Deploys EncryptRIGHT to Simplify Protecting Sensitive Data in Wire Transfer Application

Modernizing Encryption and Replacing Manual Wire Transfer Key Processes with Automated Cryptographic Key Management

One of the top five banking institutions in the world aimed to enhance the security of their payments infrastructure by reducing complex, manual processes for securing wire transfer data at the application layer. EncryptRIGHT simplified the integration work needed to improve their security posture and implement automated key rotations to better secure data in their payment applications.

Securing Wire Transfer Data at the Application Layer

Wire transfers are an integral part of international banking. However, given the abundance of financial and personal information at stake, wire transfer fraud ranks as a prominent target for hackers in today's digital landscape, especially as wire transfers are executed in applications, where data is exposed and more susceptible to breaches. One of the world's largest banks had developed custom encryption code to address this vulnerability, but it required manual key rotation, which involved a meticulous logbook system that wasn't particularly secure and was prone to human error, along with complex upkeep when changes to algorithms, keys, or applications were required. The bank knew they needed a better encryption solution with automated key management and integrated access controls, but wanted to avoid extensive re-architecture costs and timelines.

Improving Security and Control, While Reducing Complexity

EncryptRIGHT offered the bank a turnkey application-level data security solution that deployed in only a few lines of code. The bank was not only able to improve its security posture but also save significant application re-architecture costs and time. Because EncryptRIGHT centralizes both data protection policy management and robust cryptographic key management, the bank could easily control how sensitive data in applications is secured. Leveraging built-in access controls, the bank easily set up user permissions for securing and revealing sensitive data and managing cryptographic keys, which can be set to automatically rotate. Rotated keys can then be automatically deleted upon expiration, retained indefinitely for archiving purposes, or scheduled for deletion after a specified expiration period, providing the bank with enhanced security, operational efficiency, and the flexibility to tailor key lifecycle policies to their specific needs. Integrated audit logs now natively track and report security infrastructure changes, assuring the bank's audit team of no unexpected security posture changes.

The bank was not only able to improve its security posture but also save significant application re-architecture costs and time.

Centralized EncryptRIGHT data protection policies automatically apply all the correct security to data without being prone to manual error. Policies can be easily changed without re-integration or complex application architecture changes. This allows the bank's wire transfer application to update data protection methods, access permissions, and data formats without incurring huge redevelopment costs. This bank can secure its most sensitive data at the application layer in an environment where every second counts – future-proofing data security without breaking the budget.

Interested in learning more about how to simplify data protection at the application layer?

Click here to request a free proof of concept