Global Bank Tokenizes Payment Cards Across Internal and Third-Party Payment Applications

Centralizing Control While Reducing Implementation Time from Months to Days

One of the top 10 banks in the Western Hemisphere, serving tens of millions of customers worldwide, needed to implement tokenization to protect their customers' payment card numbers during transaction processing in compliance with the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS compliance, which emphasizes the importance of tokenization, particularly for cardholder data, is not optional for financial services institutions. However, the third-party, off-the-shelf payment application that the bank had been using to process payments from point-of-sale terminals across the Americas did not natively support tokenization. To complicate things further, the Bank was also using an internal banking application that received payment card information from teller windows and ATMs that required the same level of compliance. Both applications needed to be able to seamlessly tokenize and de-tokenize the same data in real time, without locking the other application out.

Challenges Centralizing Data Security Between Internal and External Applications

Tokenizing the bank's data in a vendor's payment application running across multiple geographical locations is hardly trivial, but coordinating a data security scheme that the bank could centrally control, across both their own bespoke payment application as well as an off-the-shelf software product presented quite the challenge. Traditionally, application owners would need to re-architect their applications to interweave data security functionality into their programs, which can be extremely expensive and time-consuming undertakings. Any effort from either the bank's internal development team or their third-party application vendor to implement tokenization, along with access controls, encryption, and masking, in their respective applications would risk paralyzing the other application's access to the real data, not to mention risking potential 'token collisions' caused by the same token being inadvertently used for different card numbers. Instead, they would both need to deploy the exact same data security techniques using the exact same security policies with perfectly consistent user access controls to truly share secured data. This presented quite the technical challenge, since the traditional approach to re-architecting these applications to change how they manage and secure sensitive data would require work that could take months, if not years, which the bank simply could not afford. They needed to find a better way.

> *...The traditional approach to re-architecting these applications to change how they manage and secure sensitive data would require work that could take months, if not years, which the bank simply could not afford.*

©2024 Prime Factors All Rights Reserved

Simplifying Data Security

The bank turned to EncryptRIGHT, which turns conventional application-level data protection on its head. Instead of re-architecting applications to protect data better, EncryptRIGHT allows an application to simply present a piece of data to EncryptRIGHT and ask that the data be secured with a centralized data protection policy by name. The data is instantly transformed into its secure state using whatever security techniques (tokenization, encryption, hashing, masking, digital signing, etc.) that are defined in the policy. The policy, which also defines what level of data access is granted to each user group, can instantly govern what pieces of the original data a given user or application can see when they 'unsecure' the data. It is the policy, not the application itself, that contains all of the definitions for how data is protected, who can access it, and what form the data takes when access is granted. This means there is no longer a need for security functionality to be interwoven into or managed by applications. Everything is centralized, and application-native data protection can be implemented in as little as 3 lines of code.

After completing a Proof-of-Concept (POC), the bank quickly proved to themselves that EncryptRIGHT could deliver the robust data security they needed while seamlessly bridging the gap between their third-party card processing system and their internal banking applications. The bank deployed EncryptRIGHT, defined a central policy that could protect their payment card data wherever it was used, moved, or stored, and pointed their applications to EncryptRIGHT. Rather than taking months or years to redesign their applications, the entire process was done in a matter of days. When the bank's payment application receives a payment card number from an ATM, teller window, or point-of-sale device, it immediately leverages the EncryptRIGHT policy to replace each card number with unique tokens that obfuscate the real payment card information, preventing the exposure of actual card numbers during the transaction. Not only is EncryptRIGHT enforcing a centralized data protection policy to secure and unsecure the payment card data, but these policies also deliver the crypto-agility needed to future-proof data security. The bank can instantly change how the data is secured or who can unlock the secured data by simply updating the policy, without additional integration work. This gives them the flexibility and control they need to easily share and collaborate on secure data across their various applications.

*Rather than taking months or years to redesign their applications, the entire process was done in **a matter of days**.*

When a bank uses outsourced payment applications, especially for smaller transaction processers, there are often limitations that make it challenging to accommodate necessary data protection techniques, like tokenization, masking, and encryption. Using traditional application-level data protection approaches, it can take considerable time, resources, and developer hours to secure the vast volumes of customer data passing through ATMs, processing systems, and banking environments. EncryptRIGHT simplifies everything, centralizing control and significantly reducing the efforts, costs, and complexities of securing sensitive payments-related data.

--

Interested in learning more about tokenization to secure your sensitive data? We're ready to demonstrate how easy it can be. Request a free proof of concept today.

CS-ER-FINSVCS-20240306

©2024 Prime Factors All Rights Reserved