Protecting Card Processors' Data from Cyber Threats

Xpress Bill Pay gets more robust security and faster key management with EncryptRIGHT

In the wake of the largest bank card security breaches in history, transaction processors like Xpress Bill Pay have been under mounting pressure to shore up their service infrastructure to stay ahead of hackers. The chief challenge for companies like this has been how to eliminate manual key generation while maintaining high processing speeds without needing a lot of new hardware.

The Need for Speed

Xpress Bill Pay, located in Lindon, UT, facilitates online bill payments to municipalities and utilities, which carries the added pressure of government and local regulatory commission oversight. As they considered upgrading their data security, the company needed to find a solution that would allow it to maintain its current performance standards, including daily data updates, zero-day settlement, real-time information synchronization, and the elimination of manual data entry. Xpress Bill Pay needed a solution that would be secure, reliable, and most importantly, fast.

In the electronic payments industry, most clients have service level agreements that define requirements for the speed of transactions in milliseconds. Any time encryption computation time is added, it slows performance and increases overhead. Fortunately, EncryptRIGHT works in local memory, so a payment processor does not experience the latency associated with disk retrieval or cross network communication, which is a pitfall of other solutions.

Test Driving the Key Management Tool

Under Payment Card Industry (PCI) rules, bank card processors are required to rotate their keys at least annually. However, Xpress Bill Pay President and CEO Keith Jenkins explained that his team wanted to increase the frequency of their key rotation to monthly. Their hope was to significantly strengthen consumer data protection while limiting the exposure of any possible breach.

> *"WE WANTED TO BE ABLE TO DO THINGS SIMPLER AND QUICKER…WITH ENCRYPTRIGHT, WE CAN PRE-DEFINE KEYS AND PRE-SET START AND STOP DATES SO ROTATION IS FULLY AUTOMATED."*
>
> — Keith Jenkins, President and CEO, Xpress Bill Pay

Xpress Bill Pay
Innovative Internet Payment Systems

Jenkins shared that Xpress Bill Pay's primary focus throughout their search for a data protection solution was on the overall efficiencies of the security product. "We wanted to be able to do things simpler and quicker," he said. In the face of current cyber threats and the resulting market and regulatory demands, Jenkins said they needed to find a partner that would facilitate their mounting security needs yet expedite the implementation time to satisfy their clients' expectations. After a broad solution search, they found that EncryptRIGHT by Prime Factors best met their data protection needs and helped them

©2024 Prime Factors All Rights Reserved

drastically improve their encryption key management. "In the past, we had to manually rotate keys, which was time consuming and cumbersome, but with EncryptRIGHT we can predefine keys and pre-set start and stop dates, so the rotation is fully automated."

Jenkins was impressed that Prime Factors offered a live test drive of EncryptRIGHT that not only included a fully loaded version but also permitted full service technical support and system consulting. His team was able to download the product, install it and immediately start the configurations, while the team at Prime Factors provided guidance and advised on specific problems or workarounds.

"With Prime Factors' development environment we were able to go in there and practice with the system," said Jenkins. "We were able to migrate our existing data policies and create new ones, and then we were able to export and import them. It was not difficult."

Jenkins said that his team spent most of their time deciding which data and what keys were necessary, however once these were defined, the implementation was very quick. EncryptRIGHT makes it easy to define what data to protect and how to protect it, user permissions for accessing data, and changing security and key management policies.

All of the definitions for how data is protected, what cryptographic keys are used to secure and unsecure data, and the permissions associated with how data can be accessed by user group can all be performed by a security administrator, using an administrative user interface instead of custom code. Application programmers simply configure their application to call EncryptRIGHT and reference a data protection policy (DPP) to protect sensitive data in the appropriate manner. Since all of the data protection decisions are made within a DPP, programmers do not need to be encryption or tokenization experts in order to appropriately apply application-native data protection.

When considering the overall costs of deploying a data protection solution, many companies emphasize the upfront cash, time and resources required, which can be considerable, to write custom code. However, once application integration is complete, the efforts associated with changing data protection options, such as implementing new algorithms or key types, can be equally costly. EncryptRIGHT allows for changes to a data protection policy on the fly through a simple administrative interface, without making any changes to the applications using EncryptRIGHT to protect their sensitive data. This allows customers like Xpress Bill Pay to have a more a nimble data security posture that can react more quickly and efficiently to changes in the data protection landscape, while also saving significant costs over time.

> *"[using EncryptRIGHT]... translates into saving a lot of time and money on the back end."*

The Key (Rotation Differential)

One thing that differentiated EncryptRIGHT for Jenkins was its ability to develop multiple versions of a cryptographic key in advance and schedule the automatic rotation of the keys at desired intervals. This meant that Xpress Bill Pay could achieve its top priority of implementing monthly key rotation, without requiring complex manual effort each month.

When it comes to encrypting personal consumer data and credit card numbers, if a single key is used, and it gets compromised, all of the data associated with that key over a number of years will be a risk. However, if keys are rotated monthly, then only 30 days' worth of data would be at risk if a key is compromised. Using a frequent key rotation strategy, EncryptRIGHT significantly reduced Xpress Bill Pay's data vulnerability.

One of the key areas where EncryptRIGHT stood out was in how it manages permissions and key versioning. With most other encryption products, permissions must be established to manage each separate encryption key, however, EncryptRIGHT can apply a specific set of permissions to many different versions of an encryption key. This allows pre-

©2024 Prime Factors All Rights Reserved

generated key versions to be scheduled to rotate monthly, so if a key expires and a network goes down, a processor can still implement the rotation without skipping a beat.

Xpress Bill Pay now has the confidence of knowing that they won't suffer prolonged delays or service interruptions, because they already have the new version of each key. Their encryption operations are now able to automatically flip over to the scheduled encryption key and continue encrypting and decrypting data.

Equally important, Xpress Bill Pay has the assurance that archived copies of previously used keys are secure and easily accessible when the company needs to decrypt historical encrypted data.

Scalability

Jenkins said that he was aware that Prime Factors' services are often deployed in large-scale environments consisting of IBM mainframes and AS400s, but he was impressed to learn that there was an option to install EncryptRIGHT in distributed environments running Linux, Unix, and PCs. This meant Xpress Bill Pay could install EncryptRIGHT on a standard Windows® server, satisfying their need for a package that would not require extra hardware. It also meant that EncryptRIGHT could easily and swiftly scale as Xpress Bill Pay's processing demands grew with each new client and operating environment.

EncryptRIGHT can also be deployed to protect sensitive information in various cloud computing environments, including Amazon® Web Services.

Since EncryptRIGHT supports both software key operations as well as hardware key operations, it is perfectly suited to allow customers to decide how they would like to prioritize performance and security to meet their unique business needs.

Pricing, Service, and Support

Jenkins' other concerns when vetting various encryption solutions were related to price and the ease of making the transition. "There were some other solutions that were less expensive, but in the end, I think the value is there with Prime Factors," he said. "One of the things I was concerned about with some of the lower cost providers was the possibility of more rip and replace." Jenkins confirmed that he was impressed that EncryptRIGHT offered simple installation with the opportunity to upgrade as new conditions arose or as new features became available. This ensured that as data protection requirements change over time, EncryptRIGHT can change with them, without the need to rip and replace hardware and software. "That translates into saving a lot of time and money on the back end," said Jenkins.

He also pointed out how the high-touch service, support and consulting from Prime Factors has been just as robust after implementation as it was in the test drive phase. "We've been able to get ahold of anybody at any time. It was even easy to find someone on a weekend which assured us that we could also be more available to our customers in the event of a service outage," he said.

PrimeFactors™
APPLIED DATA PROTECTION

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

Click here to request a free proof of concept today.

©2024 PRIME FACTORS ALL RIGHTS RESERVED