Arroweye Solutions: Taking the Risk Out of Data Protection Change

Stronger Encryption & Better Cryptographic Key Management, Without the Pain

As stringent data protection requirements in the payment card industry continued to evolve, Arroweye Solutions found that they needed to replace their data encryption capabilities with stronger encryption algorithms than their in-house software solution could handle. This was not a nominal undertaking. However, the company turned to EncryptRIGHT® by Prime Factors to complete the necessary data protection upgrades to their innovative payment card personalization system in significantly less time – and with much less risk – than re-architecting their in-house system.

Challenges

Arroweye Solutions burst into the payment card market in 2004, introducing an innovative digital on-demand payment card production platform that allowed real-time payment card provisioning and manufacturing for several different card-vendors at the same time. The solution leveraged a home-grown discrete, reusable encryption module that the Arroweye team had built from the ground up to protect data. However, during this same period, the rapid evolution of data privacy threats forced regulators in the payments market to elevate the degree of protection required for payment card data. As the company built a large client base, it was forced to address these new data protection requirements.

Arroweye CIO and co-founder, Brian Huse, found that having more customers meant more data and more regulatory compliance requirements, which incrementally increased both the need for data protection as well as its complexity. More data protection also spelled the need for more encryption keys and advanced data protection algorithms. Arroweye needed a replacement for their legacy encryption module used in a large number of discrete applications throughout the organization, as well as the ability to keep up with evolving regulatory requirements. Huse began to realize that if this work was to be done in-house, someone from his team would need to become a cryptographic expert.

In addition to regulatory developments, new customers began requiring Arroweye to unconditionally commit that their customers' data would be destroyed at specific time periods, such as at the end of a contract. By using a different encryption key, or set of encryption keys, for each customer, Huse saw that Arroweye could secure all of a given customer's data independently from others', even on backup tapes that commingle customers'

> *"With EncryptRIGHT we leverage best-in-class cryptographic capabilities without the expense of recoding all our applications and systems."*
>
> — Brian Huse, CIO Arroweye Solutions, Inc.

©2024 Prime Factors All Rights Reserved

data. By simply deleting a customer's cryptographic keys (a procedure sometimes referred to as "data shredding"), Arroweye could guarantee that their specified data was completely irretrievable upon demand.

To the extent that he could, Huse wanted to automate the cryptographic key management – functions such as key creation, setting expiration and rotation dates, delivery of replacement keys, and secure storage. Equally important to him was the ability to minimize key handling and demonstrate the absolute highest level of key protection. Huse phrased it as "…making sure that keys do not need to be handled by, and are not visible to, developers, users, or anyone, even the key managers."

Huse understood that building the technology in-house would take resources away from the company's core focus: leading the industry in on-demand card fulfillment. He wanted to keep the team focused on their primary mission, but updating their proprietary systems to stronger encryption algorithms and securely automating cryptokey life cycle management was necessary.

Arroweye CIO Selects EncryptRIGHT

Huse and the team began their search by evaluating offerings from global vendors, including Safenet® KeySecure®, HP® OpenView®, and IBM® Tivoli®. In all cases, it became apparent that integrating the needed capabilities would require rebuilding Arroweye's on-demand card production system to fit the key manager – something Huse wanted to avoid.

Realizing that he needed a packaged offering with a simpler integration profile than those products but built by cryptography experts, Huse turned to Prime Factors. He knew that the company had focused exclusively on addressing the cryptographic needs of global customers since the early 1980's and had developed deep expertise in the area of data protection, including cryptographic key management. Prime Factors introduced the Arroweye team to EncryptRIGHT, a data protection middleware that implemented strong encryption algorithms needed to satisfy regulations and fully automated cryptographic key management. EncryptRIGHT integrated into Arroweye's existing systems with ease via a simplified API that greatly reduced the amount of coding, QA, and acceptance testing required to replace their legacy encryption module.

> *"EncryptRIGHT brings asymmetric key security to symmetric key exchange."*

A Short Path to Enhanced Data Protection

The Arroweye development team was able to quickly install the EncryptRIGHT components and begin work, finding the product "…exceeded their expectations." The middleware abstracted all the complexities of encryption algorithms and crypto key management outside of Arroweye's application code, requiring only a single API call to protect, or to unprotect data. Managing keys was completely isolated outside the application code as well, administrated through a graphical interface designed for the data protection professional. The developers were not required to learn any of the arcane aspects of cryptography, while the company addressed all its needs for regulatory compliance and automated means to address its customers' data destruction requirements.

Retrofitting the on-demand card production system to use the EncryptRIGHT API was quick, easy, and successful. As Huse recounted it, one of the developers commented in a private email, "You install it and it just works." The team also found that the use of EncryptRIGHT improved encryption performance by 30-35%, a boon to bulk encryption activity such as scheduled backups of their customers' data.

Arroweye was able to migrate from their legacy encryption module to a new iteration based on EncryptRIGHT in far less time than any of the other alternatives they had considered, thereby reducing both the cost of the effort as well as the time-to-market.

See real data security in action.

Click here to request a free proof of concept.

CS-ER-ARROW-20240807

© Prime Factors All Rights Reserved