Mercury Insurance Ensures Clients’ Security with SafeNet KeySecure

The Organization
For more than 50 years, Mercury Insurance Group has provided comprehensive coverage options ranging from personal auto insurance to homeowners insurance to mechanical breakdown protection. It is the leading independent broker and agency writer of automobile insurance in California, and has been one of the fastest-growing automobile insurers in the United States.

The Business Need
From the beginning, Mercury has implemented various encryption methods to secure sensitive information, originally utilizing the native encryption on various databases and business applications. But as the company grew it became clear that the company needed to invest in a centralized data encryption and key management solution.

“Our core systems are heavily accessed and relied on to carry out critical business activities. So any security functionality we add to it cannot negatively impact system performance which in turn can decrease the productivity of the business,” explained Art Coble, Director of Information Security at the Mercury Insurance Group.

Challenge
Mercury needed to implement encryption on legacy and proprietary systems, as well as install a FIPS-certified centralized encryption and key management solution that would interoperate with a variety of existing databases.

Solution
SafeNet KeySecure with Crypto Pack enabled Mercury to encrypt and tokenize high-value data and centrally manage encryption keys with a high-assurance hardware appliance.

Benefit
Mercury is able to secure sensitive data on a variety of systems, all without impacting end-user performance.
Mercury began searching for a solution that would enable centralized key management of encryption keys across all databases—regardless of native encryption platform—as well as a high-speed encryption appliance. It also needed to be built on industry standard algorithms (AES) and have FIPS certification.

The Solution

Mercury evaluated several encryption and key management solutions, and quickly became interested in the ability to not just encrypt but also tokenize data, which preserves the data’s format and can remove it from the scope of compliance. Gemalto is one of the only security providers that offers encryption, tokenization, and centralized key management, and SafeNet KeySecure is FIPS certified, supporting encryption solutions for data at rest and in motion. Mercury was able to implement SafeNet KeySecure in conjunction with several features of the Crypto Pack—including SafeNet ProtectApp and SafeNet Tokenization Manager—to encrypt, tokenize, and manage keys for various databases throughout the company.

SafeNet KeySecure is the industry’s leading centralized key management platform. By utilizing KeySecure, organizations benefit from its flexible options for secure and centralized key management—deployed in physical, virtualized infrastructures, and public cloud environments.

SafeNet Tokenization Manager protects sensitive information in databases by replacing it with a surrogate value that preserves the length and format of the data, making it a highly scalable and cost-effective solution to implement. Through its integration with KeySecure, Tokenization Manager provides a single, centralized interface for logging, auditing, and reporting access to protected data, keys, and tokens.

The Benefits

With SafeNet KeySecure, Mercury was able to meet all their encryption and key management objectives without impacting performance or overhauling their legacy systems. Users are able to quickly and easily access business-critical data, while the company rests assured that their clients’ information remains protected.

KeySecure provided Mercury with:

Centralized Key Management: Instead of manually managing individual encryption systems, Mercury is now able to manage all systems in one simple console, enforce separation of duties, and even set up automatic processes.

IBM i (AS/400) Integration: SafeNet KeySecure is one of the only solutions to manage encryption keys for IBM i, including AS/400, which was a significant concern for Mercury. KeySecure and ProtectApp can encrypt applications written in COBOL, RPG, and Java, along with other languages running on IBM i, through a comprehensive set of encryption and decryption APIs.

Redundancy and Failover: Mercury installed two KeySecure appliances in each data center—one primary, one secondary. The failover process is seamless, so users don’t even know when it happens.

About Thales Cloud Protection & Licensing

Today’s enterprises depend on the cloud, data and software in order to make decisive decisions. That’s why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored—from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

“Getting the right solution that managed keys and encrypted or tokenized data on our core systems without impacting our users and business processes was like open heart surgery—a complex operation at the heart of business-critical processes. Gemalto provided us the ability to implement the security we needed without negatively impacting performance. With KeySecure, we have a world-class enterprise encryption key management solution.”

— Art Coble, Director of Information Security, Mercury Insurance Group.