BM.I

gemalto
security to be free

CASE STUDY

A Matter of National Security: BM.I Relies on Gemalto Encryption to Secure Storage

The Austrian Federal Ministry of the Interior (BM.I) needed robust encryption of its stored data, and key management capabilities, in order to fulfill its charter for safeguarding public security. Gemalto delivered the solutions that met their stringent requirements.

Background

With more than 30,000 employees, the Austrian Federal Ministry of the Interior (Bundesministerium für Inneres, or BM.I) is the top government agency responsible for domestic security—fighting crime and terrorism, handling asylum and immigration, mounting disaster and crisis response, and overseeing elections.

> "With the implementation of the Gemalto storage solution, we established significant organizational changes in the BM.I. For the first time, we introduced separation of duties so that an administrator can manage the data without viewing the actual content. By employing a "four-eyes" principle, the IT administrator and department staff now jointly grant access to data. The administrators especially see this as an advantage to prevent breaches of trust and ensure data integrity. Now we can see who has accessed what data, and this information is stored in tamper-proof logs on the system."
>
> Roman D'Alessio, Communication and Information Technology Lead, BM.I

Challenge

A public institution, the BM.I required robust encryption and key management to secure sensitive data, and wanted a solution that seamlessly integrated with their storage environment.

Solution

Gemalto SafeNet StorageSecure and KeySecure are interoperable with a variety of storage and encryption vendors, making them the ideal security solutions for the BM.I.

Results

Through the seamless integration and robust security capabilities of Gemalto solutions, BM.I was able to quickly and cost-effectively address its critical security requirements.

The Challenge: Ensuring the Security of BM.I Data

The BM.I stores highly sensitive information and is constantly in the public eye. Therefore, the infrastructure and operations group wanted to find an encryption solution that would help ensure that confidential information could only be read by authorized personnel. At the same time, they needed a solution that streamlined administration and fit into their tight budget.

The Solution

BM.I has both regional and centralized storage servers. In each regional police command is a clustered system that includes core applications, file services, databases, and Microsoft Exchange servers. These systems are replicated to the headquarters in Vienna, with disk-based backup to ensure rapid data recovery. This unified system enables them to automate various administrative tasks.

The BM.I team appreciated the uninterrupted user environment between their storage and Microsoft applications. They wanted an encryption solution that would have a similar level of integration. This led them to select Gemalto's SafeNet StorageSecure for storage encryption, and KeySecure for centralized encryption key management.

StorageSecure is a hardware-based encryption appliance that protects sensitive data in Ethernet-based network-attached storage (NAS). It provides seamless, advanced encryption services based on high-speed, 256-bit AES encryption, and featuring redundant components and clustered failover for high reliability. Through its granular encryption capabilities, StorageSecure ensures data is protected at all times and can only be accessed by authorized personnel.

BM.I also uses KeySecure for centralized management of cryptographic keys. KeySecure is built on Key Management Interoperability Protocol (KMIP), which enables out-of-the-box integration with not just SafeNet's solutions, but any encryption solution built on the KMIP platform. This makes it ideal for organizations seeking to consolidate key management across several departments or legacy encryption solutions.

The Benefits

BM.I uses KeySecure to generate and manage keys in a dedicated hardware appliance. As a result, keys are separated from storage applications and databases, and stored in a FIPS-certified, tamper-resistant appliance. It also provides BM.I with centralized management and backup of cryptographic key material.

In cooperation with CoreTEC, a company specializing in computer and information security, BM.I was able to develop a pilot project that implemented not just hardware but new organizational policies. For the first time, BM.I was able to implement a "four-eyes" approach in which access to data was strictly separated from data administration, and changes must always be reviewed by at least two people. Through this method, the organization separated duties between those essential to the operation and maintenance of systems, and those relating to data access.

To enforce the "four-eyes" policy, administrators work with the department leads to determine which users can access which key material (and thus what data), and then assign granular permissions accordingly. Existing authorization structures, from such directory services as Microsoft Active Directory or LDAP, can be integrated. Adherence to compliance rules at the BM.I can now be controlled from a central interface, and it is easy to generate a detailed report for auditing and logging.

At the BM.I, the introduction of StorageSecure was a seamless, non-disruptive process. The solution was integrated in the network, between the client and storage servers attached to two 10GB Ethernet connections. With StorageSecure, nothing changes in users' daily activities - they can continue to work with the usual drives and do not even realize that their data is being encrypted in the background. Further, their storage system is not changed. All the encryption and decryption work is done on the processors running on the StorageSecure appliance.

Solution Highlights

- Secure Regulated Data - Implement data security mandates across their storage infrastructure
- Secure Archived Data - Enforce data isolation and protection throughout its lifecycle regardless of the storage tier
- Enable Separation of Duties - Allow storage administrators to manage resources without gaining access to sensitive data
- Enable Multi-Tenant Data Isolation - Leverage shared resources while securing data by business policy to segregate data for multiple departments

About Gemalto's SafeNet Identity and Data Protection Solutions

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com
Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free