thalescpl.com

THALES

Securing IBM's XIV and A9000/ A9000R Storage:

Enterprise Key Management with SafeNet KeySecure

In the era of Big Data, organizations collect more data points than ever before. Often, organizations will store these data points because of regulatory concerns or because they hope to mine them in a way that is useful to business operations. To complicate the matter, as data breaches become more common, customers and regulators demand that this data stay secure at all times. Organizations build large-scale, complex storage deployments (in many cases, a combination of on-premises, virtualized, and remote data centers) to meet their needs, but the complexity can make adequate security difficult. Who should access the data? How do you protect against security breaches? How do you manage the encryption and decryption of data on an ongoing basis? SafeNet and IBM offer a solution to address these challenges.

The solution

IBM's XIV and A9000/A9000R storage systems have several features built specifically for the needs of big data. Built into XIVand A9000/A9000R is AES-256 encryption that secures the entire drive. SafeNet KeySecure integrates with these IBM platforms to store and centrally manage the keys for the system's self-encrypting drives.

IBM XIV and A9000/A9000R storage systems

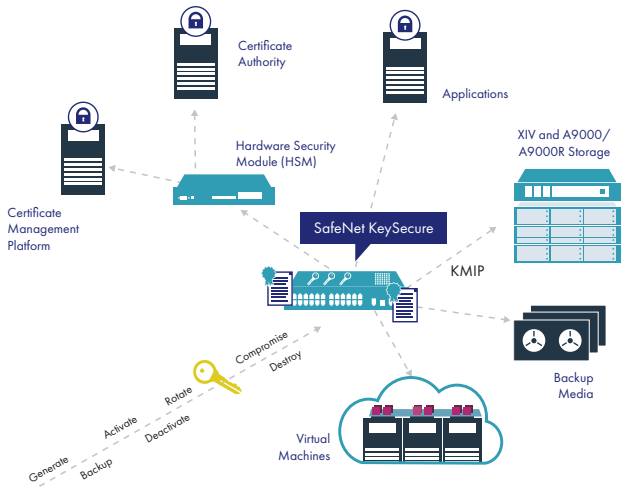
IIBM XIV and A9000/A9000R are flash-based storage systems. They are built on grid architecture for large-scale parallelism to allocate system resources uniformly at all times. Administrators can add modules to increase capacity, and automatically redistribute resources throughout the system, including the new capacity. Encryption security is a base feature for both storage systems, available in the form of self-encrypting drives.

Key benefits

- **Infrastructure and encryption management simplified:** XIV and A9000/A9000R is built for efficient growth with easy capacity planning. SafeNet KeySecure makes it easy to manage additional encryption keys as more encryption is deployed to secure growing storage.
- **Resiliency and high availability:** Both the XIV and A9000/ A9000R storage systems have a grid architecture that reduces risk of downtime. SafeNet KeySecure supports high-availability deployments that ensure encryption keys—and therefore secured data—are always accessible.
- **Cost-effective management solution:** SafeNet KeySecure's ability to manage keys for multiple, disparate cryptographic solutions makes it a small capital investment with a big impact. Additionally, instead of purchasing additional appliances as the security infrastructure expands, administrators can use their existing deployment with additional licenses to manage growing deployments.

SafeNet KeySecure

SafeNet KeySecure is a key management server that allows security teams to centrally manage encryption keys across their storage deployments. SafeNet KeySecure can manage not only the keys for IBM self-encrypting drives but also any KMIP-compatible encryption keys across the enterprise. Keys managed by the server are stored in SafeNet's FIPS 140-2 Level 3 tamper-proof hardware security modules (HSMs), where they are protected from unauthorized users. In addition, SafeNet KeySecure supports the OASIS Key Management Interoperability Protocol (KMIP) standard for easy deployment. KMIP support allows SafeNet KeySecure to centrally manage the keys for a broad range of encryption products heterogeneously deployed across a number of departments.



Use cases

- **Key management**—Centralize key management from across departments and disparate encryption solutions.
- **Logging and auditing**—Record all key state changes to monitor security administrator activity.
- **Multi-tenant security**—Secure data as it is stored in environments with data from other tenants.
- **Key availability**—Ensure that encryption keys are always available to decrypt secured data.
- **Manage multiple key types**—Centrally manages symmetric, asymmetric, secret data, and X.509 certificates, along with their associated polices.

Key features

Centralized encryption key management

When encryption is deployed in different departments around an organization, it is easy to end up with a variety of key management silos, each with its own set of enforcement policies. For security administrators, the keys to IBM's self-encrypting drives may be just one set among many from across the storage and security infrastructure. SafeNet KeySecure consolidates the management of encryption keys for disparate deployments into one easy-to-use console. Once centralized, administrators can efficiently maintain and manage the organization's disparate security solutions on an ongoing basis. In addition, with important key log information recorded and stored in one location, reporting for security audits requires less time and effort.

Ensure key integrity

Ensuring the integrity of cryptographic materials is a by-product of centralizing key storage and management in KeySecure. Irrespective of whether the data resides locally, remotely, or virtually, keys and their policies can be stored in an appliance that remains in full control of security teams (and not storage administrators). KeySecure delivers these benefits to IBM customers, allowing them to address regulatory requirements concerning their sensitive data. Without access to the appropriate encryption key, stolen data remains unreadable to the thief—the integrity of the key management system underpins the entire encryption deployment.

Strengthens multi-tenant data isolation

SafeNet KeySecure facilitates encryption in multi-tenant or cloud deployments of XIV and A9000/A9000R. Since different sets of encryption keys can be controlled in one appliance, SafeNet KeySecure's management console provides enough flexibility to encrypt tenant data co-mingled across storage environments. SafeNet KeySecure allows administrators to tailor user authorizations for specific sets of encrypted data according to defined access and usage policies by automatically retrieving access control information from existing LDAP or Active Directory services.

High-availability configurations for persistent access

Administrators can deploy SafeNet KeySecure in high-availability configurations within a single operation center or across multiple, geographically dispersed centers using an active-active mode of clustering. Such high-availability configurations mean that authorized users will always have access to their data by continually having access to the keys that unlock that data. When these configurations are spread across multiple data centers in different geographic zones, enterprises reduce the risks of technical issues in one data center, affecting global operations.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

For more information

IBM and SafeNet KeySecure combine to form a cost-effective, powerful, secured storage solution that is easy to manage and deploy.To learn more, visit safenet.gemalto.com/partners/ibm/

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com