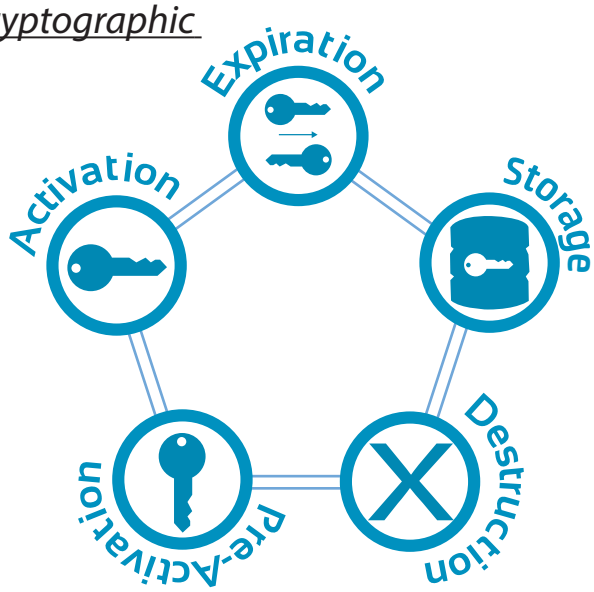
Alliance Key Management

Improves the security and administration of cryptographic keys.

Once the data is encrypted, to maintain optimal data security within your company your private information depends on the administration of cryptographic keys. Key Management provides an effective administration of cryptographic keys of the company based on standards for a wide range of applications and databases. Key Management is a FIPS 140-2 encrypted key manager that helps organizations comply with the requirements and regulations to protect private information.

Life cycle of the keys cryptographic



EXSYSTEM

Alliance Key Management

CHARACTERISTICS:

Easy management, adjusted to standards and standards.
The symmetric encryption cryptographic key management solution creates, manages and distributes 128-bit, 192-bit and 256-bit AES cryptographic keys for any application or database that runs on any operating system. It supports applications for Microsoft SQL Server with transparent data encryption (TDE) and level encryption (CLE), Microsoft SharePoint encryption and other applications.

Meets PCI DSS requirements for cryptographic key management.
For VMware users who need to comply with regulations, Alliance Key Manager has been validated by a qualified QSA PCI evaluator by an independent audit firm. Businesses in all sectors, regardless of where VMware deploys, are subject to PCI DSS compliance if electronic payments are processed with credit cards.

Complies with OASIS KMIP standards.
Complying with the OASIS standard KMIP allows operational communication between cryptographic environments and the management of encrypted keys, which reduces training and infrastructure operating costs for companies. Applications and databases that support KMIP can deploy Alliance Key Manager to easily initiate the protection of cryptographic keys.

Management of cryptographic keys for your platform.
Customers can deploy Alliance Key Manager from a VMware, cloud (AWS, Azure, IBM Cloud, or as traditional hardware (HSM) in their data center.

Compatibility with other platforms.
It works with the main technological platforms (IBM i, IBM z, Windows and Linux) and its encryption applications in the devices owned by the company.

ADVANTAGE:

Reliable and safe.
Key Management reflects keys between multiple cryptographic key management devices through a secure and authenticated TLS connection for real-time backup and support for high availability environments.

Capacity to manage audit records.
It allows administrators to track all recovery of cryptographic keys, management of cryptographic keys and system activity. The reports can be sent automatically to the system administrators, or to the SIEM system for a timely and permanent record of the activity.

Meets the PCI-DSS Requirements for Access Control Key
Cryptographic keys can be restricted based on several criteria. The most permissive level requires a secure and authenticated TLS session with the key server. Individual cryptographic keys can be restricted to specific users, groups or users in a group. Groups across the company can be defined and cryptographic keys can be restricted to super users.

Change and rotation of cryptographic keys.
Automatic or manually cryptographic keys are changed. Security administrators can define the frequency of key rotation based on internal security policies. When a cryptographic key change occurs, the new version is created and the old version is moved to a historical database and available for cryptographic operations.

GUI system administration.
Alliance Key Manager provides a Java GUI application to create and manage cryptographic keys and access policies. All access to security administration is authenticated by the TLS client and authentication by server. The system allows multiple logins of the security administrator to be required to comply with the Dual Control regulations.

Encryption and decryption services.
For applications that require a high level of security, you can use the encryption and decryption services. The cryptographic key never leaves the Key Management cryptographic key manager when consuming these services from any application, system or external device.

Integration of ISV and OEM.
ISV and OEM customers can quickly deploy integrated cryptographic key management solutions through the use of Alliance Key Manager binary APIs.

contact@exsystemusa.com
+1 (786) 352-8109
3785 NW 82 Ave Suite 309
Miami, FL 33166. USA.