Alliance Key Manager Helps Meet PCI DSS Section 3 Requirements

This document is designed to help security administrators understand how the Alliance Key Manager solution helps meet PCI Data Security Standards Section 3 requirements for key management. This document is not intended to replace guidance you might receive from a qualified QSA auditor.

Alliance Key Manager is a FIPS-140-2 certified encryption key management solution that implements NIST recommendations for encryption key management (NIST SP-800-57).

Each section below provides a reference to the relevant PCI DSS section and sub-section, guidance for the section, and recommended testing steps.
Section 3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse

Note: This requirement also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.

Testing: Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:

3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary

Testing: Examine user access lists to verify that access to keys is restricted to very few custodians.

Guidance: There should be very few who have access to cryptographic keys, usually only those who have key custodian responsibilities.

Alliance Key Manager isolates data encryption keys to a separate hardware appliance to minimize risks of data loss on protected platforms, and to enable separation of duties between key management and processing of cardholder data. Key management functions are restricted to security administrators who have PKI credentials for key management. There is no use of operating system user IDs or accounts for access authentication. Access controls can be configured to require two different administrators to authenticate for any key management function, with a defined lease time for key management operations. This meets PCI requirements for dual knowledge. All key management activity is logged to system logs with real time transmission to a separate log collection server or SIEM solution. All key management communications are secured by authenticated TLS communications.

3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.

Testing: Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys. And, identify key storage locations to verify that keys are stored in the fewest possible locations and forms.

Guidance: Cryptographic keys must be stored securely, usually encrypted with key-encrypting keys, and stored in very few locations. It is not intended that the key-encrypting keys be encrypted, however they are to be protected against disclosure and misuse as defined in Requirement 3.5. Storing key-encrypting keys in physically and/or logically separate locations from data-encrypting keys reduces the risk of unauthorized access to both keys.

Alliance Key Manager isolates data encryption keys to an isolated server platform with secure and authenticated access. For redundancy and failure protection, keys may be mirrored to one or more backup key management servers using secure and authenticated TLS communications.

Data encryption keys (DEK) are protected by key-encrypting keys (KEK) and key authentication keys (AK) which are stored separately. KEK and AK are further protected with RSA 2048-bit encryption. Key management backup routines perform additional encryption of backup images, and separate the data encryption keys (DEK) from key-encrypting keys (KEK) and Authentication Keys (AK) keys for proper off-site storage. Key encryption keys are never smaller than the data encryption keys they protect.

Alliance Key Manager is FIPS-140-2 certified and meets NIST requirements to store keys in encrypted format and to prevent key corruption.

Section 3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following

Note: Numerous industry standards for key management are available from various resources including NIST.

Testing: Verify the existence of key-management procedures for keys used for encryption of cardholder data. For service providers only: If the service provider shares keys with their customers for transmission or storage of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely transmit, store and update customer’s keys, in accordance with Requirements 3.6.1 through 3.6.8 below.

Guidance: The manner in which cryptographic keys are managed is a critical part of the continued security of the
A good key management process, whether it is manual or automated as part of the encryption product, is based on industry standards and addresses all key elements at 3.6.1 through 3.6.8.

Examine the key-management procedures and perform the following:

**Alliance Key Manager:** User documentation for key management procedures and application use are provided on the product documentation distribution. Alliance Key Manager conforms to NIST guidelines for key life cycle management, and is FIPS-140-2 certified.

### 3.6.1 Generation of strong cryptographic keys

**Testing:** Verify that key-management procedures are implemented to require the generation of strong keys.

**Guidance:** The encryption solution must generate strong keys, as defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms under “strong cryptography.”

Alliance Key Manager: All data-encryption keys, key-encryption keys, and authentication keys, are generated using NIST approved and certified random number generation procedures, and meet NIST recommendations for strong encryption key generation and establishment. See NIST RNG certificate reference below.

### 3.6.2 Secure cryptographic key Distribution

**Testing:** Verify that key-management procedures are implemented to require secure key distribution.

**Guidance:** The encryption solution must distribute keys securely, meaning the keys are not distributed in the clear, and only to custodians identified in 3.5.1.

Key management functions are only available via a secure and mutually authenticated TLS communications session. The key server implements two layers of authentication during TLS negotiation. The first layer is provided by the TLS negotiation itself where a known certificate must be presented and authenticated by the server. The second layer of authentication by the server uses X509v3 certificate information to validate the user name (CN) and organizational unit name (OU) to validate access. Dual control may be implemented to require two separate administrators to authenticate before any key management activity is allowed. Key import and export functions can be restricted to only allow RSA encrypted (2048-bit or higher) transfer of cryptographic material. Key material is never distributed in the clear.

Alliance Key Manager is FIPS-140-2 certified which requires that no key material be transferred in the clear.

### 3.6.3 Secure cryptographic key storage

**Testing:** Verify that key-management procedures are implemented to require secure key storage.

**Guidance:** The encryption solution must store keys securely, meaning the keys are not stored in the clear (encrypt them with a key-encryption key).

Alliance Key Manager: Data encryption keys (DEK) are protected by key-encrypting keys (KEK) and key authentication keys (AK) which are stored separately per NIST guidelines and the FIPS-140-2 standard for cryptographic modules. KEK and AK are further protected with RSA 2048-bit encryption. Key management backup routines maintain the separation of DEK from KEK and AK keys so that separation can be maintained off-site.

Alliance Key Manager is FIPS-140-2 certified and meets NIST requirements to store keys in encrypted format, detect key corruption, and separate data encryption keys from key encryption keys.

### 3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod

**Testing:** Verify that key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod.

**Guidance:** A cryptoperiod is the time span during which a particular cryptographic key can be used for its defined purpose. Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted. Periodic changing of encryption keys when the keys have reached the end of their cryptoperiod is imperative to minimize the risk of someone’s obtaining the encryption keys, and being able to decrypt data. If provided by encryption application...
vendor, follow the vendor’s documented processes or recommendations for periodic changing of keys. The designated key owner or custodian can also refer to industry best practices on cryptographic algorithms and key management, for example NIST Special Publication 800-57, for guidance on the appropriate cryptoperiod for different algorithms and key lengths. The intent of this requirement applies to keys used to encrypt stored cardholder data, and any respective key-encrypting keys.

Alliance Key Manager allows specifying automatic key change at a user-defined interval, or manual key change as needed. The key server will generate new keys at a specified interval, and immediately make new keys available for use. Keys can be expired and retired from user based on security administrator policy. All key generation is done through NIST approved random number generation routines which are certified by NIST.

3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised.

Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.

Testing: Verify that key-management procedures are implemented to require the retirement of keys when the integrity of the key has been weakened.

Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.

If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations.

Guidance: Old keys that are no longer used or needed should be retired and destroyed to ensure that the keys can no longer be used. If old keys need to be kept (to support archived, encrypted data, for example) they should be strongly protected. (See 3.6.6 below.) The encryption solution should also allow for and facilitate a process to replace keys that are known to be, or suspected of being, compromised.

Alliance Key Manager: Security administrators can revoke encryption keys at any time to prevent further use of retired or compromised keys. Additionally, encryption keys can be changed to generate new keys and old keys can be deleted (destroyed). Archived keys are protected through the use of strong encryption, and KEK and AK keys are archived separately from DEK. If retention of keys is needed to support decryption of stored data, the backup of the keys are further encrypted on backup media.

3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key).

Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.

Testing: Verify that manual clear-text key-management procedures require split knowledge and dual control of keys.

Guidance: Split knowledge and dual control of keys are used to eliminate the possibility of one person’s having access to the whole key. This control is applicable for manual key management operations, or where key management is not implemented by the encryption product.

Alliance Key Manager: The key server can be configured to require two separate security administrators to authenticate before key management processes can be used (dual control). No generation of split knowledge keys or reconstruction of keys is implemented. Keys are automatically generated using NIST FIPS-140-2 certified random number generation. No manual establishment of keys in the clear is supported.

3.6.7 Prevention of unauthorized substitution of cryptographic keys

Testing: Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.

Guidance: The encryption solution should not allow for or accept substitution of keys coming from unauthorized sources or unexpected processes.

Encryption key retrieval is secure and authenticated by a TLS session. Mutual authentication is required before keys
can be retrieved. Additionally, key access controls are implemented on the key server to prevent unauthorized use of encryption keys. Access control is unique for each data-encrypting key (DEK). Data-encrypting keys are protected by key-encrypting keys and substitution is prevented through the use of NIST certified HMAC validation and the use of key-authentication keys.

3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.

Testing: Verify that key-management procedures are implemented to require key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.

Guidance: This process will ensure individuals that act as key custodians commit to the key custodian role and understand the responsibilities.

Alliance Key Manager: This is a user procedure and is not implemented by the key server.

Townsend Security

Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Companies worldwide trust Townsend Security’s NIST and FIPS 140-2 compliant solutions to meet encryption and key management requirements in PCI DSS, GDPR, CCPA, HIPAA/HITECH, FISMA, and other regulatory compliance requirements. Learn more at www.townsendsecurity.com.
References


Glossary

AK – Authentication Key. An encryption key used by the key management system to detect and prevent the corruption or substitution of data encryption keys (DEK).

DEK – Data Encryption Key. An encryption key used to protect Primary Account Numbers (PAN) and other PCI information requiring encryption.

FIPS-140-2 – Federal Information Processing Standard 140, version 2. This is a NIST standard for evaluating and certifying cryptographic modules such as key management systems.

KEK – Key Encryption Key. An encryption key used to protect Data Encryption Keys (DEK). Key encryption keys are stored separately from the data encryption keys.

NIST – National Institute of Standards and Technology. This US government agency establishes the standards for encryption and cryptographic processes such as key management system. NIST charters independent testing laboratories through the NVLAP program to conduct testing of encryption and cryptographic systems. On the Internet at www.nist.gov

NVLAP – National Voluntary Laboratory Accreditation Program. This is a NIST program to accredit and certify independent testing laboratories. An NVLAP organization tests and coordinates certification for NIST encryption and cryptographic modules.

Certifications

NIST FIPS-140-2 Level 1 - Certificate number 1449

NIST AES Validation (AESAVS), certificate numbers 1245, 1486

NIST Random Number Generation (RNGVS) Validation to ANSI X9.31, certificate number 692, 810.

NIST Keyed-Hash Message Authentication Code (HMAC) Validation (HMACVS), certificate numbers 728, 875.

NIST Secure Hash Algorithm (SHAVSI) validation number 1144, 1342.