ISO Information Security Office

The University of Texas at El Paso

Payment Card Industry Cryptographic Keys

PCI Cryptographic Keys

1.0 Protection of Cryptographic Keys

Cryptographic keys used for encryption of cardholder data must be protected against both disclosure and misuse.

1.1 Custodian Access to Cryptographic Keys

Access to cryptographic / decryption keys must be restricted to the fewest number of custodians necessary and only those with a need to know.

1.2 Storage of Cryptographic Keys

Access to cryptographic keys must be stored securely, and in the fewest possible locations and forms. The data encryption key (DEK) must be stored encrypted and the key used to encrypt the DEK (the key encryption key or KEK) must be stored separately from the DEK.

2.0 Cryptographic Key Management

The following are key-management procedures for keys used for encryption of cardholder data utilizing industry-accepted standards for purposes of complying with the PCI DSS initiatives. The list of industry-leading security standards, benchmarks and frameworks to utilize includes, but is not limited to the following:

- NIST Special Publication 800-57: Recommendation for Key Management Part I, II and III

http://csrc.nist.gov/publications/PubsSPs.html

Additionally, key management procedures used for encryption of cardholder data address the following requirements in order to ensure further compliance with the PCI DSS initiatives (Security Standards Council):

- Key-management procedures are implemented to require the generation of strong keys
- Key-management procedures are implemented to require secure key distribution
- Key-management procedures are implemented to require secure key storage
- Key-management procedures are implemented to require periodic key changes, no less than once per annum
- Key-management procedures are implemented to require the retirement of old keys
  - Example: archiving, destruction and revocation (as applicable)
- Key-management procedures are implemented to require the replacement of known or suspected compromised keys
- Key-management procedures are implemented to require split knowledge and dual control of keys
  - Example: requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key

- Key-management procedures are implemented to require the prevention of unauthorized substitution of keys
- Key-management procedures are implemented to require key custodians to sign a form confirming their understanding and acceptance of their key custodial responsibilities

2.1 Generation of Strong Keys

Generation and distribution of asymmetric key pairs shall be executed in accordance with the mathematical specifications of the appropriate, approved standard.

A static key pair shall be generated by the entity that owns the key pair (i.e., the entity that uses the private key in the cryptographic computations), by a facility that distributes the key pair or by the user and facility in cooperation. When generated by the entity that owns the key pair, a signing private key shall not be distributed to other entities. In the case of a signature verification public key and its associated private key, the owner should generate the keying material rather than any other entity generating the keying material for that owner; this will facilitate non-repudiation.

2.3 Secure Key Distribution

Generation and distribution of symmetric keys for the symmetric keys used for the encryption and decryption of data or other keys shall be determined by an approved method and shall be provided with appropriate protection.

Thus, symmetric keys shall be either:

- Generated and subsequently distributed manually, using a public key transport mechanism or using a previously distributed or agreed-upon key encrypting key
- Established using a key agreement scheme
- Determined by a key update process
- Derived from a master key

Symmetric keys determined by key generation methods shall be generated by an approved random number generation method, created from the previous key during a key update procedure or derived from a master key using an approved key derivation function.

When split knowledge procedures are used, the key shall exist as multiple key components. The keying material may be created and then split into components, or may be created as separate components. Each key component shall provide no knowledge of the key value (i.e., each key component must appear to be randomly generated). If knowledge of k (where $k \leq n$) components is required to construct the original key, then knowledge of any k-1 key components shall provide no information about the original key other than, possibly, its length.

2.4 Secure Key Storage

From a scope perspective, secure key storage encompasses operational storage, backup storage and archival storage. Each of the three respective components plays a vital role in secure key storage for PCI DSS compliance.

UTEP's operational secure key storage elements consist of the following:

- For system components that require immediate access and availability to the keys for specific applications within the boundaries of system components as defined by the PCI DSS. These keys, which may be stored locally, must have strong physical security controls and logical security controls. Such controls preclude the writing of key values in the startup instructions or in the policy and procedures manual.
- Additionally, the use of root or a single authentication and authorization right that could be utilized by multiple users should also be prohibited.
- For users that *do* have access to keys within the operational storage environment, the system components must have acceptable audit and logging trails enabled and various dual controls as needed.
- If the keys are stored in a database repository, the Database Administrator (DBA) or any other individual with system administrative, super user or privileged rights to the database should not have access to the respective keys in a clear text format.

UTEP's backup storage secure key storage elements consist of the following:

- Keys should be backed up to a secure and physical source of media, which is independent from the keys used in the operational storage environment.
- This allows for the retrieval of keys in the event of the operational storage environment being compromised.

UTEP's archive storage secure key storage elements consist of the following (NIST, n.d.):

- An archive for keying material shall provide both integrity and access control.
- Integrity is required in order to protect the archived material from unauthorized modification, deletion or insertion. Access control is needed to prevent unauthorized disclosure.
- The cryptographic information may be stored so as to be immediately available to an application (i.e., on a local hard disk or a server); this would be typical for keying material stored within the cryptographic module or in immediately accessible storage (e.g., on a local hard drive).
- The keying material may also be stored in electronic form on a removable media (e.g., a CD-ROM) in a remotely accessible location, or perhaps in hardcopy form and placed in a safe; this would be typical for backup or archive storage.

2.5 Periodic Key Changes at Least Annually

It is the policy of UTEP that keys must be changed on a periodic basis, with the frequency of key changes depending on our business needs in conjunction with our overall security need to protect the keys and associated system components within the cardholder data environment.

During the key generation phase, the duration of the keys' use will be determined. Additionally, when the keys are retired, they shall no longer be in use unless needed for encryption functions related to historical data recovery. For any data retention requirements for compliance, UTEP will archive the keys as necessary.

2.6 Retirement or Replacement of Old or Suspected Compromised Keys

The end of the key life will ultimately result in key deregistration, which is the scheduled process initiated when there is no compelling business requirement (legal or compliance) for retaining the keys.

When copies of cryptographic keys are made, care should be taken to provide for their eventual replacement. All copies of the private or symmetric keys shall be destroyed once they are no longer required (i.e., for archival or reconstruction activity) in order to minimize the risk of a compromise. Any media, on which unencrypted keying material requiring confidentiality protection is stored, shall be erased in a manner that removes all traces of the keying material to preclude its recovery by either physical or electronic means. Public keys may be retained or destroyed as desired.

If a key or keys have been compromised, they must expeditiously and properly be revoked in a manner that will mitigate or eliminate the impact on the cardholder environment or any supporting system components.

The process for compromised keys includes the following steps:

- Immediately remove all instances of keys that have been affected. This includes keys used in operational storage and usage.
- Immediately replace affected keys with a new set of keys that allows business operations to continue as normal.

Additionally, these procedures and accompanying steps are supported by the Key Management Compromise Plan (KMCP) and must be filled out and provided to the Information Security Office. Examples of these forms are illustrated below.

Key Management Compromise Plan (KMCP): Systems Components Impact

Impacted System Components	Owners of System Components	Other parties Affected Outside of Organization

Key Management Compromise Plan (KMCP): Personnel

Name and Title	Contact Information	Role and Responsibility

Key Management Compromise Plan (KMCP): Notification Process for External Vendors

Name and Title	Contact Information	Role and Responsibility
UTEP Information Security Office	(915) 747-6324 or (915) 490-3203	Centralized Point of Contact

2.7 Split Knowledge and Dual Control of Keys

UTEP adheres to the concept of split knowledge and dual controlling by ensuring that multiple personnel are required to undertake specific actions and respond to requests regarding effective key management procedures. Thus, it is a standard practice within our organization to ensure that a single individual or person does not have full control of the key-management lifecycle. Various persons are involved in different stages of the following key-management lifecycle activities (NIST, n.d.):

- Key Generation
- Key Distribution
- Key Archiving
- Key Renewal
- Key Retirement
- Key Revocation
- Key Deletion/Destruction
- Key Recovery

Responsibility for activities above will fall on the department. The keys will be provided to Information Security Office for secure storage.

2.8 Prevention of Unauthorized Substitution of Keys

The substitution of keys will not be permitted unless keys have been compromised, which may affect the integrity and overall security of keys utilized in conjunction with system components in the cardholder environment. Due care will be administered throughout the key-management lifecycle to ensure the substitution of keys is prohibited. Split knowledge and dual control of keys will be considered a primary control for verifying the safety of keys throughout the key-management lifecycle. Additionally, logical and physical controls will also play a critical role in enforcing this policy.

2.9 Key Custodians to Sign Form Confirming the Understanding and Acceptance of their Key Custodian Responsibilities

The individuals referenced below are responsible for performing various duties and tasks in relation to the key-management process. As such, they have read the aforementioned policies and procedures concerning the key-management process, and have acknowledged their responsibilities by signing a form similar to the table/form illustrated below.

It is the responsibility of the Security/System Administrators to provide the signed, acknowledged forms to the Information Security Office.

Key Management Lifecycle Stage	Name	Title	Signature	Date
Key Generation				
Key Distribution				
Key Archiving				
Key Renewal				
Key Retirement				
Key Revocation				
Key Deletion/Destruction				

3.0 REFERENCES

Please refer to the following for addition information:

- *The University of Texas at El Paso Information Resources Use and Security Policy*
  - UTEP Standard 1: Information Resources Security Requirements Accountability Information Security Administrator (also referred to as Information Resources Custodian) Responsibilities.
  - UTEP Standard 4: Access Management
  - UTEP Standard 9: Data Classification
  - UTEP Standard 11: Safeguarding Data
  - UTEP Standard 19: Server and Device Configuration and Management
  - UTEP Standard 23: Security Control Exceptions
- Acceptable Encryption

4.0 REVISION HISTORY

Created:	September 28, 2007
Revised:	April 01, 2011
Revised:	July 01, 2013
Revised:	October 16, 2013
Approved:	October 16, 2013 by Gerard D. Cochrane Jr., Chief Information Security Officer
Revised:	June 30, 2017 (minor formatting changes made; added 4.0 Revision History as a section; clarification on definition to and references to Security Administrator; addition of links to current Policy and Standards)
Approved:	July 5, 2017 by Gerard D. Cochrane Jr., Chief Information Security Officer