Cryptographic Key Management Standard

Issued Date: 14 May 2015
Effective Date: 14 May 2015

Purpose

This document establishes cryptographic key management requirements to meet annual PCI compliance efforts.

Scope

This standard applies to all employees and information assets in scope for PCI's Self-Assessment Questionnaire D.

Definitions

In the context of this document, the following terms are used as indicated here:

Cardholder data – Full magnetic stripe or payment card number (credit or debit) plus any of the following: cardholder name, expiration date, or service code.

Cryptoperiod – The cryptoperiod (or key lifetime) is the time span during which a specific cryptographic key is authorized for use.

Dual control – No single person is permitted to access or use the materials.

Encryption – Process of converting information into an unintelligible form except to holders of a specific cryptographic key.

Key Custodian – The role responsible for performing key management duties, such as creating and distributing encryption keys.

Split knowledge – Key components are under the control of at least two people who only have knowledge of their own key components.

PCI System Administrator – Any employee, affiliate, contractor, or vendor of the university who has administrative or operational responsibility over cardholder data or technical systems.

Standards

Encryption Key Generation

Use only strong encryption methods to protect cardholder data. Examples that meet the intent of strong cryptography are AES (128 bits and higher), TDES (two or three independent keys), and RSA (2048 bits).

(continued)

Cryptoperiod

Keys must be rotated at one-year intervals.

Responsibilities

Key Custodians and PCI System Administrators must:

- Protect keys from unauthorized access and modification on all systems where the keys reside; and
- Acknowledge and accept responsibilities of their role by use of a formal signature (in writing or electronically).

Documentation Requirements

Key Custodians must maintain procedures for:

- Key generation using strong encryption methods,
- Secure key distribution and storage, and
- Destruction of cryptographic keys.

PCI System Administrators must maintain procedures for:

- Changing keys at the end of the defined cryptoperiod,
- Destroying or replacing keys when the integrity of the key has been weakened, and
- Replacing known or suspected compromised keys.

Where manual unencrypted key management operations are required, procedures must exist to:

- Demonstrate split knowledge and dual control of keys, and
- Prohibit any one custodian from having access to all components of a single secret key.

An example of unencrypted key management operations is manual key loading that involves the use of media such as paper or specially designed key-loading hardware devices.

Revision History

Author	Date	Comments
Jeremy Parrott	10 April 2015	Initial Draft
Kyle S. Brown	23 April 2015	Formatting
Jeremy Parrott	5 May 2015	Updates based on feedback

(continued)

Appendix A

Encryption Key Responsibility Form

Employees must protect access to all encryption keys in their custody.

I, _____, as an employee of _____ hereby agree that I:

1. Have read and understood the policies and procedures associated with key management and agree to comply with them to the best of my ability.
2. Agree to never compromise the security of the keys in my custody by divulging any information about key management practices, related security systems, passwords, or other private information associated with the company's systems to any unauthorized persons.
3. Agree to immediately report any suspicious activity that may compromise key security.

Printed Name:
Title:
Date:
Signature: