Example
Tech Documentation

Cryptographic Key Custodian Policy

Updated: 2011.01.10 | Security classification: **Unclassified**

Key Custodian Responsibilities - General Information

Purpose

This document defines Example's policy for the responsibilities of Key Custodians (KC) as required by the Payment Card Industry's Data Security Standard (PCI-DSS).

Applicability

This policy applies to all Employees, Contractors, Consultants, Outsourcers and Service Providers, of Example, who are designated and required to perform in the capacity of a KC.

Background

The Payment Card Industry Data Security Standard (PCI-DSS) is an industry regulation for the protection of sensitive credit-card data. Amongst many security requirements, it mandates the encryption of Personal Account Numbers (PAN) when stored on a computerized device. Cryptographic encryption keys used for protecting the information are required to be managed with "appropriate key-management" operations as defined in the PCI-DSS Key Management (KM) section of the Requirements and Security Assessment Procedures, Version 3.2, dated April 2016. Reference: PCI Security Standards .org *(https://www.pcisecuritystandards.org/)*

Policy Owner

The creation, implementation and any subsequent changes to this policy is the responsibility of the Chief Security Officer (CSO). This policy and any subsequent changes must be approved by two or more of the following officers of the company:

- Chief Executive Officer
- Chief Technology Officer
- Chief Financial Officer
- Chief Legal Officer
- Internal Auditor

Sensitive Data

Confidential personal information (to be hereinafter called Sensitive Data) is currently defined by the company to be any one of the following:

- Cardholder Data as defined by PCI-SSC
- Government issued IDs
- Behavioral Data
- Account number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Roles

Chief Security Officer

The Chief Security Officer (CSO) is the owner of this policy.

Key Custodian

The Key Custodian (KC) is a part owner of the cryptographic keys established by Example to protect Sensitive Data.

Encryption Domain Administrator

The Encryption Domain Administrator (EDA or DA) is the technical administrator of the cryptographic keys and data created and maintained by Example.

Authorized Users

Any human user or software application executing on any device that needs to access Sensitive Data is an Authorized User (AU). AU's must be explicitly permitted to perform any function within the cryptographic systems established by Example.

Resources

StrongAuth KeyAppliance (SAKA)

Example has purchased and deployed the StrongAuth KeyAppliance (SAKA) to comply with PCI-DSS requirements for encryption and key-management (EKM). While many of the statements in this policy document are technology-independent, some statements are specific to the implementation chosen by Example and how they are carried out within the SAKA.

In the event the SAKA conflicts with this policy, Example will work with the vendor to resolve the differences. Where the SAKA goes above and beyond this policy, all Roles are required to adhere to the requirements of the SAKA implementation.

Processes

Requesting Access to the SAKA

Access to the SAKA is handled through Example's standard SDLC process.

During design phase, development will consult with InfoSec and determine if a new encryption domain should be created, or if the requested use requires access to an existing encryption domain.

Once approved by InfoSec and the CTO, a Jira ticket will be created. Creation of the domain will be accomplished by the Domain Administrator, a role currently assigned to the Sr. Director of Operations, or the back-up Domain Administrator, also a member of the Operations team.

The Domain administrator is also responsible for securely distributing the access credentials and making any additional modifications to the domain. The Domain Administrator will follow all standard Example change control procedures.

Revoking Access to the SAKA

Revoking access to the SAKA also occurs via the standard Example change control system. The Domain Administrator implements the revocation

Responsibilities

All Employees

All Employees, Contractors, and Consultants employed by Example are required to comply with this policy, without exception.

Chief Security Officer (CSO)

The CSO is responsible for:

- Implementing this policy and ensuring it stays current i.e., it must conform to PCI-DSS and other regulations which cover Example's business operations.
- Ensuring that people in Roles related to this policy are trained to comply with this policy.
- Providing annual reports to Example's Audit Committee on compliance to this policy.

Key Custodians

The KC is responsible for:

- Maintaining strict control over the credential/token they are entrusted with to activate the cryptographic module on the SAKA.
- Selecting a complex password – alphabet, numeral and special character – for their credential, of a minimum length of eight (8) characters.
- Never revealing their credential password to anyone.
- Never handling more than one KC credential at any time.
    - Note: There are three (3) KC credentials, denoted by the Red, Green and Blue colored tokens.
    - A KC must never be responsible for more than one colored token credential at any time.
- Never copying anything on the token intended for their credential.
- Never copying their credential file to any computer.
- Notifying the CSO of any loss of or compromise to the credential as soon as feasible.

Encryption Domain Administrator

The EDA/DA is responsible for:

- Maintaining strict control over the credential/token they are entrusted with to manage an Encryption Domain on the SAKA.
- Selecting a complex password (alphabet, numeral and special character) for their credential of a minimum length of eight (8) characters.
- Never revealing their credential password to anyone.
- Never handling a KC credential at any time.
- Never copying anything on the token intended for their credential.
- Never copying their credential file to any computer.
- Notifying the CSO of any loss of or compromise to the credential as soon as feasible.
- Never granting, revoking, or modifying privileges to the SAKA without complying with the Processes described in this policy.

Internal Auditor

The IA is responsible for:

- Periodically reviewing the SAKA environment for compliance to this policy.
- Notifying the CSO of violations and/or deficiencies in compliance to this policy.
    - In the absence of the CSO not rectifying the violation/deficiency within 60 days, the IA will notify Example's Audit Committee of the violation and/or deficiency.

Related Policies

See: Example Information Classification Scheme.

Other Resources

See: Payment Card Industry Data Security Standard *(https://www.pcisecuritystandards.org/pci_security/)*
See: SAKA Documentation
(https://www.researchgate.net/publication/259532997_SAKA_A_Secure_Authentication_and_Key_Agreement_Protocol_for_GSM_Networks)

Document Information

Version	1.0
Date	Month Day, Year
Notes	Template of Cryptographic Key Custodian Policy
Author	*Name*
Reviewed by	*Name*
Approved by	*Name*