|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Changes** |
| 0.01 | 30th April 2017 | Bondhan Novandy | * Main objective of this project |

# Introduction

The idea of this project is to develop a Key Management System software on the scale of desktop application, Open source, robust and PCI compliant to some degree. This document will note whatever the idea which came from my mind in order to produce the objective of the KMS.

1. Desktop Application

As its title, the software will be developed for desktop application. At first it will be targeted on Windows environment

1. Open Source

Obviously

1. Robust

Should be designed very well that any state it came to when error occurred due to unexpected input or behavior it should be very well managed and does not sacrifice its secureness.

1. PCI Compliant

To some degree – if not all, it will be developed by incorporating the PCI requirements or how it will tackle all the requirement mandated by the PCI.

# Benefits

Why develop this application? Some ideas of application usage:

* KMS

Serving key management, requests and cryptographic functions

* As a dongle – and open source
* Distributed KMS

Application 🡨🡪 KMS Messaging API 🡨🡪KMS 🡨🡪 Smart Card

# Objects

List of objects to be managed:

1. Keys
   1. Type of Keys:
      1. Symmetric Key
      2. Asymmetric Key
   2. Key Life Cycle
   3. Key Encryption Key
   4. Key Residence
   5. Key Export-Import
   6. Key Usage
   7. Key Generation
   8. Key Destruction
   9. Key Compromise
2. Roles
3. Database