|  |  |
| --- | --- |
|  | Vision Document |
|  |  |
| November 1, 2014 | Project Name |
|  | Note: Text written in the blue comments of this document is intended as an aid to the author and should be deleted before this document is released. Update the title and project name by updating the Word DocProperties. The purpose of the vision document is to ensure all stakeholders agree on what problem they are attempting to solve. |

# Introduction

The main goal of this project is to allow any user, whatever their technology savviness to create secure passwords, enter those passwords easily and keep them private.

A secondary goal is to create a PKI that anybody can easily use and in so doing allow everyone to communicate securely.

The primary goal is achieved by storing an encrypted form of the data on a server but keeping the encryption key private on a user’s mobile device and creating plug-ins for all browsers and a USB dongle which allows the phone to act as a keyboard on any computer.

# Purpose

## Business Opportunity

Recent events with privacy breaches by governments but also the rising fear of identity theft have elevated the awareness of security but no novel solutions has been proposed.

SmartPass relies on the smart phone for 2 level authentication: the thing you own is the phone and the thing you know it the PIN to your SIM. Everything comes back to the phone for managing the passwords.

Money can be earned by operating the exchange which allows all the user’s devices to communicate with the phone and get unencrypted versions of the passwords.

## Problem Statement

Most password lockers (OnePass, Keyper, ) rely on a master password to lock the data vault. They usually distribute the vault onto different devices or computers with the assumption that the data is secured by the master password.

This assumption seems flawed to us. An attacker will usually get the vault open within an acceptable amount of time as user entered passwords are usually easy to guess. Furthermore the security of the data can be compromised without the knowledge of the user.

## Market

Anyone who needs an easier way to enter their passwords on computers, tablets and smart phones and keep the information private is a potential customer.

## Product Position

SmartPass offers more security but firstly it offers more convenience in managing passwords and one’s certificate. The main feature being “your phone is your password”.

Existing solutions will allow you to create a digital vault in which you can store your password securely. The key to the vault is a master password which you have to enter every time you want to open it. Entering secure passwords on a physical keyboard is strenuous on mobile devices it’s a pain. But the mobile devices are the means to access information these days and a new solution for managing passwords is needed.

# Stakeholders

Summarize the important non-user stakeholders for the system. Besides the users of the system, there are other non-users such as the funding authority, the project manager, testers, etc. who will each have their own unique interests in the system.

## Stakeholder Goals

Summarize the goals of each stakeholder. If the system were a success, what would they achieve?

# Product Overview

What is the context of the system? Where and how is it used? This section should summarize the context diagram of the system and describe all major external entities that will interact with the system.

## Features and Benefits

Include a terse list of the major features in the system (e.g. Sales capture, payment authorization) and the benefits each feature provides.

• Feature

# External Requirements and Constraints

Describe any requirements or constraints the external environment places on the system. For example, are there any time constraints that must be met?