Password Safe (Coding Hand in 3)

Introduction

A few weeks ago a fresh start-up company “easy coders” developed a password safe tool for their very first customer. Time to market was very close and so developers created a quick solution. Nonetheless, the customer accepted the solution and business started. Impressed by the first success, they decided to throw the application on other markets as well. Therefore, some quality requirements have to be improved or even fulfilled.

Overview of the current application

The current application supports following use cases:

- Set a new/initial master password
- Display a list of stored passwords
- Delete a stored password
- Create a new password
- Reveal a stored password

What the new markets need?

After long discussions in several workshops with stakeholders, architects summarized the outcome in bullet points below:

- Users with access to the file system on the installation should not be able to read the master password.
- By setting a new password, it should be entered twice and checked for equality before writing to file.
- As the solution was specifically developed for the very first customer, it cannot be installed on other machines. Seems that a more flexible configuration for locations of “master.pw” file and password.pw folder is required.
- The encryption method for the passwords should be exchangeable. Right now, the app supports only AES and there is no easy/foreseen way to introduce another algorithm. It would be great to switch between already implemented methods by proper configuration settings.
- Right now, each password is stored in a separate file. As figured out by some marketing surveys, some customers prefer storing all passwords in a single file or maybe use more advanced storage types (e.g.: databases). Introducing and exchanging storage technologies/ concepts is necessary.

Your mission

Refactor the already existing solution to a system that fulfils the quality requirements listed by the “What the new markets need?” section.