

Morik Password Manager

Programmentwurf

von

Moritz Gutfleisch

und

Erik Zimmermann

Abgabedatum:	01. Februar 2018
Bearbeitungszeitraum:	01.10.2017 - 31.01.2018
Matrikelnummer, Student:	0000000, Moritz Gutfleisch
Matrikelnummer, Student:	0000000, Erik Zimmermann
Kurs:	TINF19B1
Gutachter der Dualen Hochschule:	Daniel Lindner

Abstract

- English -

This is the starting point of the Abstract. For the final bachelor thesis, there must be an abstract included in your document. So, start now writing it in German and English. The abstract is a short summary with around 200 to 250 words.

Try to include in this abstract the main question of your work, the methods you used or the main results of your work.

Abstract

- *Deutsch* -

Dies ist der Beginn des Abstracts. Für die finale Bachelorarbeit musst du ein Abstract in deinem Dokument mit einbauen. So, schreibe es am besten jetzt in Deutsch und Englisch. Das Abstract ist eine kurze Zusammenfassung mit ca. 200 bis 250 Wörtern.

Versuche in das Abstract folgende Punkte aufzunehmen: Fragestellung der Arbeit, methodische Vorgehensweise oder die Hauptergebnisse deiner Arbeit.

Inhaltsverzeichnis

Abkürzungsverzeichnis	IV
Abbildungsverzeichnis	V
Tabellenverzeichnis	VI
Quellcodeverzeichnis	VII
1 Einleitung	1
2 Clean Architecture	2
2.1 Plugins	2
2.2 Adapter	3
3 Programming Principles	4
4 Domain Driven Design	5
4.1 Ubiquitous Language	5
4.2 Value Objects	6
4.3 Entities	7
4.4 Aggregate	7
4.5 Repositories	8
4.6 Domain Services	8
5 Unit Tests	9
6 Entwurfsmuster	10
7 Refactoring	11

Abkürzungsverzeichnis

SQL Structured Query Language

Abbildungsverzeichnis

4.1 Datenbank-Spaltennamen nach Ubiquitous Language	6
---	---

Tabellenverzeichnis

4.1 Ubiquitous Language Gegenüberstellung	6
---	---

Quellcodeverzeichnis

1 Einleitung

2 Clean Architecture

2.1 Plugins

2.1.1 Datenbank

Die Datenbank stellt eines der Plugins dar. Als Technologie wurde hier eine SQLite3 Datenbank verwendet. Die konkrete Implementierung der Schnittstelle zur SQLite-Datenbank befindet sich in der Klasse *SQLiteDatabase*. Diese Klasse erbt von der abstrakten Klasse *AbstractDatabase*, die sich in der Applikationsschicht befindet. Hierdurch wird eine Dependency Inversion erreicht, da nun eine *AbstractDatabase* von anderen Klassen verwendet werden kann, um SQL-Befehle auf der Datenbank auszuführen, statt eine konkrete *SQLiteDatabase* zu verwenden, was die Abhängigkeit von innen nach außen laufen lassen würde.

2.1.2 Verschlüsselung

Ein weiteres Plugin ist die Verschlüsselungsbibliothek. Als solche wurde Cryptopp¹ verwendet. Die abstrakte Klasse *Cipher* definiert die Schnittstelle in der Applikationsschicht, die das Plugin implementieren muss. Eine konkrete Implementierung dieser Schnittstelle befindet sich in der Klasse *CBC_Cipher*. Dadurch findet auch hier eine Dependency Inversion statt, da *Cipher* verwendet werden kann, um Verschlüsselung zu verwenden, statt eine Dependency auf eine konkrete Klasse der Pluginschicht zu brauchen. Die Schnittstelle muss lediglich einen String ver- und entschlüsseln können unter Angabe des Klar- bzw. Geheimtextes und eines Schlüssels. *CBC_Cipher* implementiert dies für die Chiffren, die im *BLOCK* enum aufgezählt sind. Momentan handelt es sich dabei um AES und Serpent, neue Chiffren können allerdings leicht hinzugefügt werden, solange sie von Cryptopp unterstützt werden. Diese werden als Block-Chiffren mit Cipher Block Chaining (CBC) als Betriebsmodus verwendet. Um andere Betriebsmodi, oder Nicht-Blockchiffren zu

¹<https://cryptopp.com/>

verwenden, müssten weitere Implementierungen des *Cipher* Interfaces hinzugefügt werden. Dies ist ohne Weiteres möglich, solange ein *String* zur Schlüsselherleitung hinreichend ist.

2.2 Adapter

2.2.1 Datenbank

Die Klasse *DbInterface* implementiert die eigentliche Funktionalität in Form der SQL-Anweisungen und führt diese über eine konkrete Implementierung der *AbstractDatabase* in der Datenbank aus. Somit geht keine Funktionalität verloren, wenn das Plugin durch eine andere Datenbanktechnologie ausgetauscht wird. Die Umsetzung der Funktionalität als SQL-Anweisungen bedeutet jedoch, dass ein Austausch des Plugins nur ohne Weiteres möglich ist, wenn die neue Datenbank ebenfalls eine SQL-Datenbank ist. Handelt es sich bei der neuen Datenbank jedoch beispielsweise um eine noSQL-Datenbank, so muss die Funktionalität, also die Abfragen, angepasst werden. Der Klasse *DbInterface* wird im Konstruktor eine *AbstractDatabase* übergeben, was die Dependency Injection umsetzt. Auf die Benutzung von Prepared Statements wurde innerhalb des Adapters verzichtet, da die Datenbank lokal ist und nur der Benutzer Befehle auf ihr ausführt. Würde die Datenbank über eine öffentliche Schnittstelle angesteuert werden, so wäre dies nicht zu vernachlässigen.

3 Programming Principles

4 Domain Driven Design

4.1 Ubiquitous Language

Die Analyse der Ubiquitous Language ergab die zuvor genannten Programmteile, deren Bezeichnungen mit denen anderer Passwortmanager verglichen werden. KeePass unterscheidet in der Ubiquitous Language nicht zwischen den zwei von uns identifizierten Arten von Passwörtern, nämlich PlaintextPassword und EncryptedPassword. Stattdessen werden diese zwei Umstände meist mit Adverbien beschrieben ("sensitive data is stored encryptedly", "make sensitive data available unencryptedly") oder mithilfe mehrerer Substantive ("passwords as plain-text"). Da wir im Source Code weder mit Adverbien noch mit unnötig langen Konstrukten aus mehreren Substantiven arbeiten wollen, wir jedoch trotzdem eine Unterscheidung der beiden Zustände eines Passworts benötigen, haben wir uns für die beiden genannten Varianten entschieden. Was das Entry angeht, so verwenden wir den gleichen Begriff wie KeePass (1Password zieht hier Item vor). Was die EntryId angeht, so verwenden wir keine UUID, da wir nur Entries verwalten und demnach keine eindeutige Kennung über mehrere Tabellen hinweg benötigen. Das Präfix "Entry" vor der Id dient dem besseren Nachvollziehen von was es die Id ist. Das Gleiche gilt für das Präfix des EntryName. Hier haben wir uns für Name statt wie KeePass für Title entschieden, da wir dies für eindeutiger halten. Außerdem haben wir uns gegen User Name entschieden und haben stattdessen Login gewählt als Begriff, da unser Passwort Manager darauf abzielt dem Benutzer beim Anmelden zu helfen. Aus diesem Grund kann im Feld Login die konkrete Zeichenkette gespeichert werden, die der Benutzer zum Anmelden braucht, sei es tatsächlich der Benutzername oder aber die Email Adresse. Entsprechend uneingeschränkt sollte auch die Bezeichnung dieses Feldes sein, was bei User Name nicht der Fall ist. 1Password nennt den Ort, an dem die Passwörter gespeichert werden den Vault. Wir haben uns stattdessen für EntryRepository entschieden, um zum einen klar zu machen, dass es sich um einen Aufbewahrungsort handelt und zum anderen eindeutig festzulegen, dass dies der Aufbewahrungsort speziell für Entries ist. Dies beseitigt sämtliche Fragen, was genau dort aufbewahrt wird. Beim PasswordGenerator jedoch sind wir uns einig mit der Bezeichnung von KeePass. Weder KeePass noch 1Password benennen

Domänenexperte (KeePass/1Password)	Implementierung (Morik)
Password	PlaintextPassword
Password	EncryptedPassword
Entry/Item	Entry
UUID	EntryId
Title	EntryName
User Name	Login
Vault	EntryRepository
Password Generator	PasswordGenerator
?	PasswordEncrypter
?	PasswordDecrypter

Tabelle 4.1: Ubiquitous Language Gegenüberstellung

die Teile ihrer Software, die die Daten ver- und entschlüsseln. Stattdessen ist die Rede von encrypted data und "decrypted data". Da Passwörter die einzigen Felder sind, die von uns ver- und entschlüsselt werden, haben wir uns dafür entschieden die dafür zuständigen Programmteile mit PasswordEncryptor und PasswordDecryptor zu bezeichnen, sodass wir trotzdem die von KeePass und 1Password verwendeten Wortstämme verwenden, daraus jedoch Substantive machen.

Um die Ubiquitous Language des Programms auch außerhalb des Source Codes zu verwenden, haben wir ebenfalls die Spalten der Datenbank an die festgelegten Begriffe angepasst. Dies kann in [Abbildung 4.1](#) beobachtet werden.

EntryId	EntryName	Login	EncryptedPassword
1	TestEntry	max.mustermann@beispiel.de	SafeAndEncryptedPassword

Abbildung 4.1: Datenbank-Spaltennamen nach Ubiquitous Language

4.2 Value Objects

Das erste Value Object ist das PlaintextPassword, welches das vom Benutzer eingegebene abzulegende Passwort beinhaltet bevor es verschlüsselt wird beziehungsweise nachdem es entschlüsselt wird. Es handelt sich dabei um ein Value Object, da es sich um das gleiche PlaintextPassword handelt wenn der Benutzer zwei mal die gleiche Zeichenkette eingibt. Das EncryptedPassword, das das Passwort beinhaltet nachdem es verschlüsselt ist, gilt

ebenfalls als Value Object. Dies gilt aus dem gleichen Grund wie beim PlaintextPassword, also dass die gleiche Zeichenkette auch die Gleichheit des Objekts impliziert. Außerdem gilt der EntryName als Value Object, der den Namen, welchen der Benutzer für den Eintrag vergibt, speichert. Hierbei handelt es sich ebenfalls um ein Value Object, da die gleiche eingegebene Zeichenkette bedeutet, dass es sich um den gleichen Namen für den Eintrag handelt. Auch der vom Benutzer optional hinzugefügte Login eines Entrys gilt als Value Object, ebenfalls aus dem Grund dass die gleiche Zeichenkette bedeutet, dass das Objekt das Gleiche ist. Zu guter Letzt gilt auch die EntryId als Value Object, die die ID des Entrys speichert. Hier gilt, dass der gleiche Integer Wert schlussfolgern lässt, dass es das gleiche Objekt der Klasse EntryId ist.

4.3 Entities

Ein Entry beschreibt einen konkreten Eintrag in der Datenbank. Der Entry beinhaltet die ID des Eintrags, den Namen des Eintrags, einen optionalen Login und das verschlüsselte Passwort. Man stelle sich Folgendes vor. Der Benutzer löscht einen Entry und erstellt danach einen neuen. Bei dem neuen Entry vergibt er den gleichen Namen, Login und das gleiche Passwort wie bei dem zuvor gelöschten Entry. Handelt es sich darum um den selben Entry? Nein, denn der wurde gelöscht. Darum ist der Entry eine Entity und kein Value Object.

4.4 Aggregate

Es gibt genau ein Aggregat. Dieses Aggregat beinhaltet ein Entry, eine EntryId, einen EntryName, einen Login und ein EncryptedPassword. Diese Teile sind als Aggregat zu betrachten, da sie immer gemeinsam von Interesse sind. Ein Benutzer möchte nicht einfach irgend ein Passwort wissen ohne den zugehörigen Namen des Eintrags zu kennen. Die Aggregat-Root ist dabei der Entry, wobei über die EntryId des Entrys auf das jeweilige Aggregat zugegriffen wird.

4.5 Repositories

Da es nur ein Aggregat gibt, gibt es ebenfalls genau eine Repository. Diese Repository ist die EntryRepository und stellt den Zugriff auf die Datenbank dar, die die Einträge des Benutzers persistiert. Die EntryRepository liefert demnach vorhandene Entries zurück, speichert neue Entries, löscht nicht mehr benötigte und passt Werte eines Entrys an neue Werte an.

4.6 Domain Services

Der Generator für neue Passwörter (PasswordGenerator), sowie die Verschlüsselung eines PlaintextPasswords (PasswordEncryptor) und die Entschlüsselung eines EncryptedPasswords (PasswordDecryptor) werden als Domain Services realisiert.

5 Unit Tests

6 Entwurfsmuster

7 Refactoring