

Neuentwicklung einer Android-App zur Passwortverwaltung

Grundlegende Anforderungen – Lastenheft

Letzte Bearbeitung: 13. November 2014

Inhaltsverzeichnis

1. Überblick	3
1.1. Hintergrund	3
1.2. Zielsetzung	3
2. Anforderungen und Architektur.....	4
2.1. Grundlegende Anforderungen	4
3. Nutzen	5
4. Zeitplan.....	5



1. Überblick

1.1. Hintergrund

Mit der fortschreitenden Technisierung des Alltags und der Zunahme an anwendungsbasierten Services haben Benutzer immer mehr Passwörter zu verwalten. Aus Sicherheitsgründen sollten die Passwörter immer komplexer gestaltet werden. Gleichzeitig sollte optimaler Weise pro Zugang ein individuelles Passwort verwendet werden, um das Sicherheitsrisiko im Falle eines Passwortdiebstahls zu minimieren.

Durch diese Situation ergibt sich die Frage, wie man seine Passwörter für den Fall des Vergessens festhält. Die Passwörter auf Papier zu schreiben ist nur bedingt praktisch, da ein Zettel beispielsweise sehr leicht verloren gehen kann und ein unverschlüsselt aufgeschriebenes Passwort ein großes Sicherheitsrisiko darstellt. Denkbar wäre eine Anwendung, die auf dem Computer installiert wird. Da man seinen Computer aber nicht überall griffbereit hat, scheint eine Passwortverwaltung direkt auf dem tragbaren Gerät – wie einem Smartphone oder Tablet – auf dem die Passwörter auch benutzt werden, am effizientesten.

Diese Problemstellung und ein Interesse an der Android App-Entwicklung bilden die Motivation für die im Folgenden beschriebene Projektarbeit.

1.2. Zielsetzung

Ziel dieses Projektes ist die Entwicklung einer Android-App, die dem Nutzer das Verwalten und Nutzen seiner Passwörter erheblich erleichtern soll. Dabei wird der Fokus auf die Sicherheit der gespeicherten Passwörter gelegt: Einerseits in der Hinsicht, dass niemand anders unbefugt Zugriff auf die Passwörter erlangen soll und andererseits so, dass der Anwender möglichst komplexe und damit sichere Passwörter nutzen kann. Der Komfort der Anwendung soll dadurch erhöht werden, dass sie auf mobilen Geräten wie Smartphones und Tablets immer zur Hand ist. Des Weiteren soll der Nutzer durch eine intuitive und übersichtliche Benutzeroberfläche unterstützt werden.


Ein weiteres persönliches Ziel bei der Entwicklung der App ist das Kennenlernen und Verstehen der Entwicklung einer App für das Android-Betriebssystem.


2. Anforderungen und Architektur

2.1. Grundlegende Anforderungen

Die Anwendung soll zunächst Passwortmanagement im Allgemeinen komfortabel ermöglichen. Sie soll stabil auf einem Android-Smartphone oder Tablet betrieben werden können und eine intuitive, übersichtliche Oberfläche besitzen. Die folgenden Bausteine sollen enthalten sein:

1. das Generieren sicherer Passwörter
2. das Ver- und Entschlüsseln der gespeicherten Passwörter
3. das Speichern und Lesen von Passwörtern

Beim Generieren neuer Passwörter soll der Nutzer die zu verwendende Zeichenmenge (Groß- & Kleinbuchstaben, Sonderzeichen, Zahlen etc.) und die gewünschte Länge des Passworts angeben können. Des Weiteren soll es möglich sein, die Sicherheit bereits erstellter Passwörter anzeigen zu lassen. Die Bewertung soll anhand der Länge und verwendeten Zeichen  erfolgen und direkt visualisiert werden.

Beim Speichern eines neuen Passworts wird dieses mit dem **Master-Passwort**  verschlüsselt und abgespeichert. Dieses Master-Passwort wird beim Ersten Start der Anwendung durch den Benutzer vergeben und lässt sich später beliebig ändern. Bei Änderung des Master-Passworts werden alle gespeicherten Passwörter neu verschlüsselt. Das Master-Passwort wird beim Öffnen der App abgefragt. Nach der Eingabe des Benutzers wird – unabhängig von der Korrektheit der Eingabe – eine Liste der Dienste angezeigt, für die Passwörter gespeichert sind. Diese Passwörter werden mit dem eingegebenen Masterpasswort entschlüsselt, daher werden nur bei korrekter Eingabe die tatsächlichen Passwörter berechnet. In der Liste kann auf einen Dienst getippt werden, wodurch das entschlüsselte Passwort dazu angezeigt wird. Es soll eine Möglichkeit geben, das Passwort für eine beschränkte Zeit in die Zwischenablage zu übernehmen.

Um Passwörter ändern oder löschen zu können, muss man ein Bearbeitungspasswort eingeben. Dies muss ebenfalls beim ersten Anwendungsstart festgelegt werden. Im Gegensatz zum Master-Passwort wird hier zurückgemeldet, ob die Eingabe richtig oder falsch war. Nur mit einem korrekten Bearbeitungspasswort ist ein Ändern oder Löschen möglich.

Neben durch die Anwendung generierten Passwörtern soll es außerdem möglich sein, manuell erstellte Passwörter zu speichern.

3. Nutzen

Die Vorteile dieser Anwendung liegen auf Hand:

- eine intuitive Oberfläche
- eine portable Lösung, die auf dem Smartphone oder Tablet immer zur Hand ist
- ein hohes Maß an Komfort durch die Speicherung in die Zwischenablage per Knopfdruck
- eine zentrale Passwortverwaltung
- ein hohes Maß an Sicherheit bei der Erstellung und Verwaltung der Passwörter

4. Zeitplan

Der Ablauf und die Inhalte der Vorstudie werden in der folgenden Tabelle gezeigt.

Zeitraum	Aktivität
14.11.14 – 21.11.14	Einlesen in die Android-App-Entwicklung
22.11.14 – 21.12.14	Einrichtung der Entwicklungsumgebung & Entwickeln des ersten Entwurfs
22.12.14 – 02.01.15	Weihnachtspause
03.01.15 – 14.01.15	Testen, Erfassen von Bugs
15.01.15 – 31.01.15	Bugfixing/ Fertigstellung der App
01.02.15 – 06.02.15	Erstellen der Dokumentation
07.02.15	Abgabe der Projektarbeit
13.02.15	Abschlusspräsentation

