
Vorname	Nachname	Beruf	Dauer
Marten	Meißner	Fachinformatiker AE	07.22-07.24

Wochenbericht KW 19. (2023.05.08. - 14.)

Nach gemeinschaftlicher Diskussion über unsere IK_Inventory App, haben wir festgestellt das ein kommerzieller Nutzen momentan nicht absehbar ist. Da einige aus unserem Team feststellten das es im Play-Store keine Kalender App gibt, die auf Termine hinweist. Da es außerdem sehr Reizvoll ist eine funktionsfähige App im Play-Store hochzuladen, haben wir uns entschieden eine Kalender App die Termine verwaltet und benachrichtig zu entwickeln. Das hat verschiedene Vorteile, zum einen ist es die Erfahrung eine Lauffähige App zu veröffentlichen, welche Pflichten und Anforderung an eine App gestellt werden um sie zu veröffentlichen und zum anderen ist es eine gute Präferenz im Lebenslauf. Und zu guter Letzt kennt es jeder selber mal einen Termin verpasst zu haben und ein netter reminder wäre dabei sehr hilfreich gewesen. Jedoch sollte die IK_Inventory App mit einer Lauffähigen Version unterbrochen werden, so das alle wichtigen Funktionen enthalten sind und ein sauberen Abschluss hat, um später weiter entwickelt werden kann. Dafür kontrollierte ich alle unbearbeiteten Issues in Jira und sortierte diese nach "müssen erledigt werden für eine stabile Version" und " Feature für nächste Version".

Das war schnell erledigt, da unser Fokus von Anfang an auf den wichtigsten Funktionen der App lag. Jedoch blieb eine letztes Feature übrig damit die Version 0.5 Abgeschlossen werden kann. deswegen übernahm ich die Letzte Aufgabe während sich meine Mitschüler schon mit den neuen Projekt begonnen haben.

Das Letzte Feature war dann die Passwort abfrage mit der Datenbank zu koordinieren, so das ein Nutzer sein Passwort erneuern kann und sich über ein One-Time-Password verifizieren kann. Nachdem Frank und ich uns die API Dokumentation von Supabase durch lasen und uns im Dialog über Lösungsmöglichkeiten die uns Supabase bietet am besten nutzen kann. Des weiteren unterhielten wir uns darüber, warum in der Programmiersprache Dart es so viel Komplizierter ist, als zb. in Javascript. Wir kamen dann zu Überlegung das Javascript eventuell Server seitig ausgeführt wird und nur das Ergebnis zum Nutzer gesendet wird und deswegen nicht über den Browser einsehbar ist und damit die Anwendung zu hacken erschwert wird und weil wir mit Dart ein Programm programmieren welches auf unseren System läuft kann von Angreifern jeder Befehl eingesehen werden. Damit aber auch hier eine hohe Sicherheit ein gehalten werden kann, können wir nur beschränkt auf Nutzer Daten zugreifen oder auslesen. So zum Beispiel kann ich nicht auf Passwort oder andere Eigenschaften eines Nutzer zugreifen um diese zu vergleichen, jedoch habe ich fertige Methoden mit denen ein Passwort geändert werden kann oder ein Nutzer kann sich alternativ mit einem OTP anmelden. Nachdem wir also wussten was Supabase uns erlaubt, haben wir uns entschieden den Prozess wie folgt abzuarbeiten: Zuerst muss der Nutzer seine Emailadresse eingeben, diese wird dann verglichen mit den Emailadressen der Registrierten Nutzer wenn die Emailadresse zu einem Account gehört wird eine Email verschickt mit einem OTP und der Nutzer wird auf eine andere Seite Navigiert wo er dann sein OTP aus der Email eingeben kann und zusätzlich ein Neues Passwort vergeben wird. Nachdem der Nutzer sein Korrektes OTP eingeben hat und ein sicheres neues Passwort gewählt hat, wird zuerst der Nutzer mit der API Funktion von Supabase verifiziert und wenn dies geschehen ist wird in einem Zweiten schritt das Passwort geändert.

Kontrolliert am: _____ Unterschrift : _____