**<שם הפרויקט>**

מסמך אפיון

<עדי בלייר>

<גרסה 0.1>

<11.12.18>

**היסטוריית גרסאות המסמך**

|  |  |  |
| --- | --- | --- |
| **תאריך** | גרסה | **תקציר השינויים** |
| 11.12.18 | 0.1 | התחלת כתיבה על פרוטוקולי תקשורת |
|  |  |  |
|  |  |  |
|  |  |  |



1. **הקדמה**

החלק הזה ישמש להצגה כללית של מסמך האפיון - הוא נועד לאפשר לקורא להבין במה מדובר - מה זה בכלל הפרויקט הזה ומה מופיע בהמשך המסמך.

* 1. מטרה

*מה המטרה של המסמך ומי קהל היעד שלו*

* 1. המוצר

*חלק זה צריך להכיל את הדברים הבאים:*

* *שם המוצר אותו מפתחים (ובאמצעותו נתייחס למוצר בהמשך המסמך)*
* *הסבר כללי של מה המוצר עושה (ואם צריך- מה הוא לא עושה)*
* *תיאור של מטרות המוצר ויתרונותיו העיקריים. נסו להיות מדויקים וספציפיים כמה שניתן.*

*המוצר שואף לעשות בצורה אוטומטית ככל הניתן את ההרשמה וההתחברות שאפליקציות שונות.*

*המוצר ייתן מעלה לכל אפליקציית וינדוס, ולא רק לאתרי אינטרנט.*

* 1. הגדרות

*בחלק זה יש לציין את כל ההגדרות, המושגים וראשי התיבות בהם תשתמשו בהמשך המסמך.*

* 1. תקציר

*הסבר מה מופיע בהמשך המסמך ופירוט כיצד זה מסודר לאורך המסמך*

1. תיאור כללי
   1. פונקציונליות

*המערכת בנויה משני חלקים, צד שרת וצד לקוח*

* 1. *צד לקוח:*
     1. התחברות למערכת (מסך התחברות\ התחברות אוטומטית בזמן עליית ווינדוס)
     2. בכל עלייה של תוכנה שפרטי ההתחברות עבורה נשמרו תתבצע התחברות אוטומטית
     3. בכל מסך הרשמה ניתן לבקש מהתוכנה למלא את המסך, התוכנה תמלא סיסמא רנדומלית, ופרטים נוספים עם היא מזהה (אימייל, טלפון וכולי)
     4. אופציונאלי: אפשרות להצפנה כפולה של הסיסמאות עם מפתח שיינתן למשתמש.
  2. צד שרת:
     1. שרת זיהוי משתמשים:
        1. שומר בסיס נתונים של שמות משתמש וסיסמאות
        2. מנפיק אישורי JWT למתחברים
     2. שרת שמירת המידע
        1. שומר את כל סיסמאות המשתמשים
        2. מאפשר קבלה, עדכון, הוספה ומחיקה של סיסמאות
     3. שרת הרשאות (על אותו המחשב כמו שרת שמירת מידע)
        1. מחזיק בסיס נתונים על ההרשאות של כל משתמש
        2. מאפשר קבלה של מספר רשומה ומשתמש ואומר האם למשתמש יש גישה לרשומה.
  3. קהל היעד

*תיאור כללי של קהל היעד של המערכת - מה תפקידם, ניסיונם, יכולתם ללמוד את ממשק המערכת וכל דבר אחר שישפיע על דרישות המערכת. יתכן יותר מפרופיל אחד של משתמש במערכת, ולכן יש לפרט את כל הסוגים וההשלכות/משמעויות שלהם מבחינת אופי ורקע טכנולוגי או פונקציונלי.* ("מי הולך להשתמש במערכת?")

* 1. אילוצים עיקריים
     1. המערכת דורשת חיבור לאינטרנט.
     2. המערכת תומכת בריבוי משתמשים.
  2. הנחות ותלויות
     1. *הלקוח ירוץ רק בסביבת וינדוס*

1. דרישות מפורטות
   1. צד שרת
      1. *כניסת משתמש*

*עדיפות: חיוני*

*קלט: שם משתמש וסיסמא*

*תהליך: בדיקה האם השם משתמש והסיסמא קיימים, ומחזיר ללקוח עם קיים או לא.*

*פלט: דף סיסמא שגויה או התחברות לתוכנה*

*טיפול בשגיאות: ניתוק הקשר*

* + 1. *הוספת סיסמא*

*עדיפות: חיוני*

*קלט: מזהה התוכנה, שם משתמש וסיסמא*

*מהו מזהה התוכנה???*

*תהליך: הוספת הרשומה לממסד הנתונים*

*פלט: הסיסמא נוספה לממסד*

*טיפול בשגיאות: ??? (ניסוי חוזר)*

* + 1. *מחיקת סיסמא*

*עדיפות: חיוני*

*קלט: מזהה התוכנה, שם משתמש וסיסמא*

*מהו מזהה התוכנה???*

*תהליך: מחיקת הרשומה מממסד הנתונים*

*טיפול בשגיאות: החזרת הודעה שהרשומה לא קיימת*

* + 1. *שינוי סיסמא*

*עדיפות: חשוב*

*קלט: מזהה התוכנה, שם משתמש וסיסמא חדשה*

*מהו מזהה התוכנה???*

*תהליך: עדכון הרשומה מממסד הנתונים*

*טיפול בשגיאות: החזרת הודעה שהרשומה לא קיימת.*

*אופציונאלי: הלקוח ישנה סיסמא אוטומטית כל זמן קבוע.*

* + 1. *קבלת סיסמא*

*עדיפות: חיוני*

*קלט: מזהה התוכנה,*

*מהו מזהה התוכנה???*

*תהליך: הוצאת הרשומה ממסד הנתונים*

*פלט: החזרת הרשומה*

*טיפול בשגיאות: החזרת הודעה שהרשומה לא קיימת.*

*צד לקוח*

* + 1. *קבלת כל הסיסמאות*

*עדיפות: חשוב*

*פלט: כל הסיסמאות שנשמרו בשרת*

*טבלת ה REST API*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Action | HTTP Verb | URL Path | Action number | Description |
| Create | POST | ??? | 2 | Defines a unique URL to create a new password |
| Read password | GET | ??? | 5 | Defines a unique URL to read a password |
| Read passwords | GET | ??? | 6 | Defines a unique URL to read all the passwords |
| Update | PUT/PATCH | ??? | 4 | Defines a unique URL to update an existing password |
| Delete | DELETE | ??? | 3 | Defines a unique URL to delete an existing password |

* 1. צד לקוח
     1. *יצירת סיסמא*

*עדיפות: חיוני*

*פלט: סיסמא רנדומלית.*

* + 1. *הרשמה אוטומטית*

*עדיפות: חיוני*

*קלט: מזהה התוכנה*

*תהליך: נרשם לתוכנה על ידי מילוי כל השדות הידועים לו, לאחר אישור המשתמש מוסיף את הסיסמא למערכת*

*פלט: אין*

*טיפול בשגיאות: לא לוחץ אף פעם על אישור ונותן למשתמש לשנות את הפרטים.*

* + 1. *החלפת סיסמא אוטומטית*

*עדיפות: חשוב*

*קלט: אין*

*תהליך: מחליף את הסיסמא של שירות מסוים (תלוי מספר 4 בצד שרת)*

*פלט: אין*

*טיפול בשגיאות:*

*שגיאת מקום החלפת סיסמא לא נמצא – מבקש מהמשתמש להחליף סיסמא בעצמו*

* + 1. *שינוי הגדרות*

*עדיפות: חשוב*

*קלט: הגדרות חדשות*

*תהליך: שינוי קובץ הגדרות*

* + 1. *עלייה אוטומטית*

*עדיפות: אופציונאלי*

*תהליך: התוכנה תעלה כל פעם שהמחשב ירוץ*

* + 1. *הכנסת סיסמאות אוטומטית*

*עדיפות: אופציונאלי*

*תהליך: התוכנה תרוץ ברקע וכל פעם שתהיה כניסה לאתר מזוהה היא תכניס אוטומטית את הסיסמא ותתחבר*

* + 1. *כפתור זכור אותי*

*עדיפות: אופציונאלי*

*תהליך: התוכנה תשמור את השם משתמש והסיסמא ווינדוס ותתחבר אוטומטית כל עלייה של המחשב*

* + 1. *הגדרות:*
* *עלייה אוטומטית – דלוק*
* *הכנסת סיסמאות אוטומטית – דלוק*
* *אבטחה כפולה – כבוי*
* *Remind me - דלוק*
  1. דרישות הבטחה

*כל התקשורת המפורטת להעיל תהייה בhttps*

*שרת זיהוי משתמשים:*

*מאמת את המשתמש באמצעות שם וסיסמא ומספק אישורי JWT.*

*כל משתמש עם הרשאות master יוכל להנפיק אישורים למשתמשים שלו באיזו דרך שיבחר לפי מדיניות המפתחות(3.6).*

*שרת משאבים:*

*מקבל בקשות מהלקוח ומעדכן את ממסד הנתונים.*

*לכל בקשה שנשלחת לAPI יצורף האישור. האישור ייבדק ואם הוא הונפק על ידי גורם מאושר יינתנו ההרשאות למשתמש על פי רישומו בממסד הנתונים.*

*לכל משתמש יש שתי רמות הבטחה:*

*רגילה – דורשת זיהוי*

*גבוהה - דורשת זיהוי מחדש ומפתח. מידע ברמת הבטחה גבוהה תוצפן על ידי הלקוח לפני השליחה לשרת. פתיחה של מידע זה ושימוש בו יוסג על ידי קבלת המידע מהשרת ופתיחתו עם המפתח שקיים צל הלקוח.*

*את המפתח ניתן לשמור במשתמש שלך בווינדוס(win32crypt.CryptProtectData) או בקובץ.*

* 1. מדיניות מפתחות JWT

|  |  |
| --- | --- |
| HEADER  {  "alg": "HS256",  "typ": "JWT"  } | Alg- the algoritem to decrept the signature, only HS256 supported  Type- the type of the token, only JWT supported |
| PAYLOAD  {  "sub": "1234567890",  "ip": "185.125.1240",  "exp" : 1516239082  } | Sub- user ID  ip- the ip thet get the token, just this ip can use the token. Maby use ijt instead?  Exp- time of token expansion |
| HMACSHA256(  base64UrlEncode(header) + "." +  base64UrlEncode(payload), secret  ) | Secret- the secret key that used by the initiator of the token |