< KeyPass>

מסמך אפיון

<עדי בלייר>

<גרסה 0.2>

<13.12.18>

**היסטוריית גרסאות המסמך**

|  |  |  |
| --- | --- | --- |
| **תאריך** | גרסה | **תקציר השינויים** |
| 4.12.18 | 0.1 | התחלת כתיבה על פרוטוקולי תקשורת |
| 13.12.18 | 0.2 | הוספת פונקציונאליות של אדמיין ומדיניות מפתחות. |
|  |  |  |
|  |  |  |



1. **הקדמה**
   1. מטרה

מסמך תכנון ראשוני, מוגדר בשפה פשוטה ככל הניתן לתת סיקרה על הפרויקט לאנשים שאינם בעלי ידע מקצועי בנושא.

* 1. המוצר

*המוצר שומר את הסיסמאות של המשתמש בשירותים השונים ומאפשר התחברות קלה.*

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

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

* 1. הגדרות

*מזהה התוכנה- מחרוזת כלשהי שמזהה את סוג השירות (שם התוכנה או הURI של האתר).*

1. תיאור כללי

*המערכת בנויה משני חלקים, צד שרת ,צד לקוח וצד לקוח מנהל מערכת.*

* 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. זיהוי משתמשים:
        1. שומר בסיס נתונים של שמות משתמש וסיסמאות
        2. מנפיק טוקן למתחברים ומעדכן את ממסד הנתונים בהתאם.
     2. שמירת המידע
        1. שומר את כל סיסמאות המשתמשים
        2. מאפשר קבלה, עדכון, הוספה ומחיקה של סיסמאות
     3. 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.
     4. ניהול
        1. בסיס נתונים של הלוגים של כל המודולים האחרים.
        2. אתר לוקאלי של ניתוח הלוגים ונתונים אחרים.
           1. גודל התעבורה וסוגה (הצלחת הבקשות, סוג הבקשות, מיקום)
           2. גודל ממסד נתונים
           3. מהירות התגובה של השרת לכל בקשה.
           4. מספר הרשומות בכל סוג אבטחה.
  3. צד לקוח מנהל מערכת
     1. מסך סטטוס מערכת
     2. מסך הגדרות מערכת
  4. קהל היעד

*הלקוחות שעומדים להשתמש במערכת מתחלקים שלני סוגים:*

* לקוח רגיל- משתמש בגרסה הבסיסית של התוכנה, לא משנה את ההגדרות ברירית המחדל.
* לקוח מתקדם- אדם בעל הבנה מסוימת ברשת, ובעל מודעות להבטחת מידע. משתמש בהגדרות מתקדמות כגון רמת הבטחה גבוהה(ראה 3.4).
  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.*

*פלט: מפתח הזדהות או הודעת שגיאה.*

*סוג שגיאות: שם משתמש וסיסמא לא נכונים.*

* + 1. *הגשת שאלת הבטחה*

*עדיפות: חיוני*

*קלט: התשובה לשאלת ההבטחה.*

*תהליך: הכנסת המשתמש וכל הטוקנים שנוצרו לפני לblacklist (לפי userid ,iat). בקשה לשם משתמש וסיסמא חדשים, ולאחר קבלה עדכון בממסד נתונים.*

*פלט: אין*

*סוג שגיאות: ??*

* + 1. *קבלת שאלת ההבטחה*

*עדיפות: חיוני*

*קלט: אין*

*תהליך: החזרת שאלת ההבטחה למשתמש. לאחר שמקבל תשובה נכונה, הכנסת המשתמש וכל הטוקנים שנוצרו לפני לblacklist (לפי userid ,iat) ואיפוס הסיסמא.*

*פלט: החזרת שאלת ההבטחה.*

*סוג שגיאות: ??*

*בכל התהליכים הבאים מפתח הזדהות יהיה קלט של התכונה. לפני ביצוע הפעולה הנדרשת ייבדק המפתח, ורק עם הוא תקף הפעולה תתבצע. עם לא תוחזר שגיאה שהמפתח לא תקף.*

* + 1. *הוספת סיסמא*

*עדיפות: חיוני*

*קלט: מזהה התוכנה, שם משתמש וסיסמא.*

*תהליך: הוספת הרשומה לממסד הנתונים.*

*פלט: הרשומה שנוספה או הודעת שגיאה.*

*סוג שגיאות: מזהה תוכנה כבר קיים.*

* + 1. *מחיקת סיסמא*

*עדיפות: חיוני*

*קלט: מזהה התוכנה, שם משתמש וסיסמא.*

*תהליך: מחיקת הרשומה מממסד הנתונים.*

*סוג שגיאות: הרשומה לא קיימת.*

* + 1. *שינוי סיסמא*

*עדיפות: חשוב*

*קלט: מזהה התוכנה, שם משתמש וסיסמא חדשה.*

*תהליך: עדכון הרשומה מממסד הנתונים.*

*סוג שגיאות: מזהה התוכנה לא בממסד נתונים.*

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

* + 1. *קבלת סיסמא*

*עדיפות: חיוני*

*קלט: אין*

*תהליך: הוצאת הרשומה ממסד הנתונים*

*פלט: החזרת הרשומה*

*סוג שגיאות: הרשומה לא קיימת.*

* + 1. *קבלת כל האתרים*

*עדיפות: חשוב*

*תהליך: הוצאת כל מזהה התוכנות של המשתמש.*

*פלט: כל שמות המשתמש והאתרים שלהם. אין דרך לקבל את כל הסיסמאות בבקשה אחת משיקולי אבטחה.*

* 1. צד לקוח
     1. *יצירת מפתח הצפנה*

*עדיפות: חיוני*

*פלט: מסך שמירת מפתח. ניתן לייבא לקובץ או לשמור לוקאלית בצורה מוגנת תחת משתמש הwindows.*

* + 1. *יצירת סיסמא*

*עדיפות: חיוני*

*קלט אופציונאלי: מפתח הצפנה*

* + 1. *הרשמה אוטומטית*

*פלט: סיסמא רנדומלית.*

*עדיפות: חשוב*

*קלט: מזהה התוכנה*

*תהליך: נרשם לתוכנה על ידי מילוי כל השדות הידועים לו, לאחר אישור המשתמש מוסיף את הסיסמא למערכת. לא לוחץ על אישור ונותן למשתמש לשנות/להוסיף פרטים.*

*פלט: אין*

*סוגי בשגיאות: אין.*

* + 1. *החלפת סיסמא אוטומטית*

*עדיפות: חשוב תלוי 3.1.4,3.2.1,3.2.6*

*קלט: אין*

*תהליך: מחליף את הסיסמא של שירות מסוים בצורה אוטומטית ומעדכן את השרת.*

*פלט: אין*

*סוגי בשגיאות:*

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

* + 1. *שינוי הגדרות*

*עדיפות: חשוב*

*קלט: הגדרות חדשות*

*תהליך: שינוי קובץ הגדרות או שליחת ההגדרות לשרת.*

* + 1. *עלייה אוטומטית*

*עדיפות: אופציונאלי*

*תהליך: התוכנה תעלה כל פעם שהמחשב ירוץ.*

* + 1. *הכנסת סיסמאות אוטומטית*

*עדיפות: חיוני*

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

* + 1. *כפתור זכור אותי*

*עדיפות: אופציונאלי תלוי 3.4.6*

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

* + 1. *הגדרות ברירית מחדל:*
* *עלייה אוטומטית – פעיל*
* *הכנסת סיסמאות אוטומטית – פעיל*
* *אבטחה כפולה – כבוי*
* *Remind me – פעיל*
  1. לקוח מנהל מערכת:
     1. **התחברות**
        1. **שם משתמש וסיסמא או מפתח** SSH
     2. **דף סטטוס מערכת**
        1. **מצב סרבר (פעיל\כבוי)**
        2. **רוחב פס או מספר בקשות**
        3. **מהירות תגובה ממוצעת של כל בקשה.**
        4. **אחוז בקשות נכשלות וסוג כישלון.**
     3. **דף הגדרות מערכת**
        1. **זמן תפוגה של אישורים.**
        2. **הקפאת משתמש לפי מזהה משתמש.**
  2. דרישות הבטחה

*כל התקשורת המפורטת להעיל תהייה בhttps*

*שרת זיהוי משתמשים:*

*מאמת את המשתמש באמצעות שם וסיסמא ומספק מפתחות התחברות.*

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

*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 שחזור חשבון

הקפאת חשבון תעשה על ידי מענה על שאלת הבטחה. ההקפאה תמנע גישה לחשבון עד איפוס סיסמא. קישור לאיפוס סיסמא ישלח לטלפון או לאימייל המוגדר כאימייל איפוס. קישור השחזור יהיה תקף לחצי שעה בלבד.

* 1. מדיניות מפתחות JWT – להזיז למסמך שני
  2. OTP,HSM

אימות מפתח:

1. בדיקת החתימה
2. בדיקה ברשימת המבוטלים
3. בדיקת הexp
4. בדיקת הip???
5. בדיקת הiat
6. בדיקת רמת ההרשאות על מול הבקשה

|  |  |
| --- | --- |
| HEADER  {  "alg": "HS256",  "typ": "JWT"  } | Alg- the algorithm to decrepit 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 that 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 |