**תכנון פרוטוקול לשרת לקוח מוצפן**

\* בסוף יש הערה ממני לפרוטוקול ולקוד

1. **המטרה** – לבצע חיבור מאובטח בין השרת ללקוח שכולל הירשמות התחברות TFA ושינוי סיסמה

2. **סוגי הודעות**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **קוד הודעה 4 בתים** | **כיוון** | **תיאור** |
| 1 | SNGU | מהלקוח | בקשה להירשם, יש לשלוח שם משתמש, אימייל, סיסמה, את אותה סיסמה וכל אחד בשדה אחר. |
| 2 | SNGR | מהשרת | Reply מהשרת שמאשר את ההירשמות או מסביר בעיה בלקוח |
| 3 | LOGI | מהלקוח | בקשת להתחבר למשתמש קיים, יש לשלוח שם משתמש וסיסמה בשדות שונים |
| 4 | LOGR | מהשרת | Reply מהשרת שמאשר התחברות סופית או מסביר בעיה בלקוח |
| 5 | 2FAR | מהשרת | בקשת מהלקוח לשלוח את הקוד שנשלח לו במייל, ללא שדות |
| 6 | 2FAC | מהלקוח | בקשת לאמת קוד שנשלח במייל ע"י השרת, לשלוח קוד בשדה יחיד |
| 7 | 2FAV | מהשרת | שולח האם הקוד מהלקוח נכון או שגוי |
| 8 | FGPS | מהלקוח | בקשה לשנות סיסמא למשתמש, לשלוח שם משתמש בשדה יחיד |
| 9 | FGPR | מהשרת | Reply מהשרת עם הבקשה שגויה (לא קיים שם משתמש כזה) |
| 10 | CHPS | מהלקוח | בקשה לשנות סיסמא, לשלוח את אותה הסיסמה החדשה ב2 שדות שונים |
| 11 | CHPR | מהשרת | Reply מהשרת אם שינוי הסיסמה צלח או לא |
| 12 | CNCL | מהלקוח | בקשה לצאת מהמצב הנוכחי למצב אנונימי |
| 13 | CNCR | מהשרת | Reply מהשרת שהלקוח במצב אנונימי וקודים קדומים לא רלוונטים |
| 14 | EXIT | מהלקוח | לקוח מבקש מהשרת לנתק אותו כי סיים לבקש שרות (רק קוד הודעה) |
| 15 | EXTR | מהשרת | שרת עונה ללקוח שקיבל את בקשתו לצאת ולאחר ששלח EXTR יחכה שנייה ויסגור ערוץ תקשורת |
| 16 | ERRR | מהשרת | שגיאה כולל קוד שגיאה והסבר באנגלית |

3. **מבנה ההודעות**

* כל ההודעות מחרוזתיות
* מפריד בין כל שדה ~ . (ללא מפריד בסוף ההודעה)
* כל ההודעות יכילו שדה גודל ההודעה ראשון בגודל קבוע של 4 בתים (int) בBIG INDIAN, ערך השדה לא יחשיב את עצמו וגם לא את המפריד הראשון. דוגמא  
  P\x00\x00\x00~SNGU~omri~aaaaaaaaaaaaaaaaaaaaaa@gmail.com~12345678~12345678
* כל שדה שנוסף לשדה האורך וסוג ההודעה יעבור BASE64 ENCOED בשביל לשמור על המפרידים
* השרת שומר את המצב של הלקוח ולכן לא מאשר לו הודעות מסוימות (מפורט בשגיאה 3)
* כאשר השרת מחזיר את מצבו של הלקוח לאנונימי הקוד האחרון שנשלח נמחק אצל השרת
* אם אותו משתמש מנסה להיכנס מ2 מחשבים שונים לTFA השרת יחסום אחד
* הודעות 5,12,13,14,15 - הודעות ללא שדות נוספים פרט לקוד ההודעה
* הודעה 15 תכיל 2 שדות נוספים (קוד שגיאה והסבר ראה סעיף 5 )

27~ERRR~002~code not supported

4. **צורת מענה** – סינכרוני ,

**תלות בין הודעות** -   
בכל מצב שליחת הודעה 14 תענה עם 15 ותנתק את הלקוח.  
בכל מצב שליחת הודעה 12 תענה על 13 ותחזיר את הלקוח למצב אנונימי  
 הלקוח מתחיל במצב אנונימי:  
 הוא יכול לשלוח את הודעה 1 ולקבל בתשובה את הודעה 2.   
 הוא יכול לשלוח את הודע 3 ולקבל בתשובה את הודעה 4 אם כשל ו5 אם צלח בצירוף עם   
 שינוי מצבו למצב התחברות.  
 הוא יכול לשלוח את הודעה 8 ולקבל את הודעה 9 אם כשל ו5 אם צלח בצירוף עם   
 שינוי מצבו למצב שיכחון סיסמה.

כל הודעה אחרת, תוביל לשגיאה

הלקוח במצב התחברות:

הוא יכול לשלוח את הודעה 6 ולקבל את הודעה7. אם כשל יישאר במצב התחברות אחרת  
יעבור למצב מחובר בו הוא במסך הבית  
כל הודעה אחרת, תוביל לשגיאה

הלקוח במצב שיכחון סיסמה:

הוא יכול לשלוח את הודעה 6 ולקבל את הודעה7. אם כשל יישאר במצב שיכחון סיסמה אחרת יעבור למצב שינוי סיסמה.  
כל הודעה אחרת, תוביל לשגיאה

הלקוח במצב שינוי סיסמה:

הוא יכול לשלוח את הודעה 10 ולקבל את הודעה11. אם כשל יישאר במצב שינוי סיסמה אחרת יחזור למצב אנונימי  
כל הודעה אחרת, תוביל לשגיאה

5. **שגיאות** – רק מהשרת ללקוח  
001 – שגיאה כללית General error

002- קוד הודעה לא נתמך code not supported קורא כשהלקוח שולח הודעה שאסור לו במצבו הנוכחי (לדוגמה לשלוח קוד TFA כאשר הוא אנונימי)

003 – מצבו של הלקוח לא ידוע (האם הוא לא אנונימי, מנסה לשנות סיסמא וכו') unknown state

004 – הודעה מכילה כמות לא נכונה של שדות wrong amount of fields