**מסמך פרוטוקול שרת לקוח מוצפן – איתמר דלל י"א3**

1. **המטרה** – תקשורת מוצפנת בין השרת לבין הלקוח. בשרת יש מסד נתונים והוא מנהל את ההרשמה ואת ההתחברות של הלקוחות.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **קוד הודעה 4 בתים** | **כיוון** | **תיאור** |
| 1 | REGS | מהלקוח | בקשת הירשמות. |
| 2 | LOGN | מהלקוח | בקשת התחברות. |
| 3 | VERC | מהלקוח | בקשה לשלוח קוד אימות לאימייל. |
| 4 | CODE | מהלקוח | בקשה לאישור קוד האימות. |
| 5 | PWUP | מהלקוח | בקשה לבצע עדכון סיסמה למשתמש. |
| 6 | CSOK | מהשרת | להודיע ללקוח שהשרת תומך בשיטת ההצפנה שהוא בחר. |
| 7 | PKEY | מהשרת | לשלוח ללקוח את המפתח הציבורי. |
| 8 | KEYK | מהשרת | מודיע ללקוח שהמפתח הסודי של AES תקין. |
| 9 | CSNK | מהשרת | מודיע ללקוח שהשרת אינו תומך בשיטת ההצפנה שהוא בחר. |
| 10 | REGK | מהשרת | מודיע ללקוח שהרישום התבצע בהצלחה. |
| 11 | LOGK | מהשרת | מודיע ללקוח שההתחברות התבצעה בהצלחה. |
| 12 | SNTC | מהשרת | מודיע ללקוח שקוד האימות נשלח אל האימייל שלו. |
| 13 | CDEK | מהשרת | מודיע ללקוח שקוד האימות שהוא שלח לשרת הוא תקין. |
| 14 | CDEW | מהשרת | מודיע ללקוח שקוד האימות שהוא שלח לשרת הוא לא תקין. |
| 15 | PWUK | מהשרת | מודיע ללקוח שעדכון הסיסמה התבצע בהצלחה. |
| 20 | EROR | מהשרת | מודיע על שגיאה בתקשורת בין הלקוח לשרת. |

2. **סוגי הודעות**

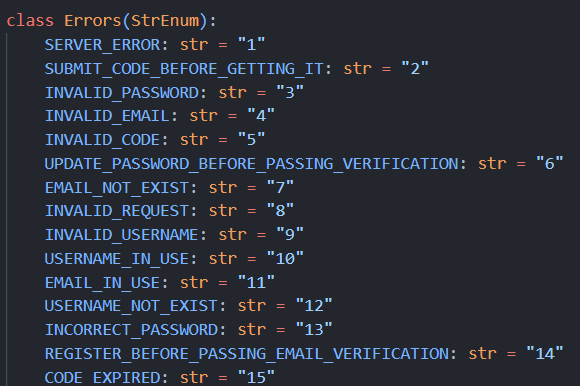
3. **מבנה ההודעות**

* כל ההודעות מחרוזתיות
* מפריד בין כל שדה | . (ללא מפריד בסוף ההודעה)
* כל ההודעות יכילו שדה גודל ההודעה ראשון בגודל קבוע של 8 בתים, ערך השדה לא יחשיב את עצמו וגם לא את המפריד הראשון.

4. **צורת מענה** – סינכרוני.

5. **שגיאות**

מחלקה של שגיאות וה-opcode של כל שגיאה:

****