**תכנון פרוטוקול: שרת לקוח מוצפן – אופיר הופמן יא3**

1. מטרה: מערכת שרת-לקוח המאפשרת הרשמה והתחברות באמצעות תקשורת מוצפנת.
2. סוגי הודעות: קוד הודעה בשדה השני:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | קוד | כיוון | מהות | שדות נוספים | הערות ותיאור |
| 1. | RSAA | מהלקוח | שאילתה את השרת האם תומך בהחלפת מפתחות RSA | אין | שרת מחזיר תשובה כן או שגיאה |
| 2. | RSAR | מהשרת | תגובה חיובית מהשרת לשאלה האם תומך בRSA להעברת מפתח | אין | אין |
| 3. | DHAA | מהלקוח | שאילתת השרת האם תומך בהחלפת מפתחות Diffie-Helman | אין | שרת לא תומך לכן אין תגובה חיובית לשאילתה זו |
| 4. | GKEY | מהלקוח | בקשה מהשרת למפתח ציבורי RSA | אין | אין |
| 5. | KEYR | מהשרת | שליחת מפתח RSA | המפתח | משומש לשם העברת מפתח AES לתעבורה "שוטפת" |
| 6. | INIT | מהלקוח | הלקוח שולח לשרת את מפתח AES | מפתח AES | אין |
| 7. | INOK | מהשרת | אישור מהשרת על קבלת מפתח AES | אין | אין |
| 8. | LOGN | מהלקוח | לקוח שולח בקשה להתחברות | 1. שם משתמש  2. סיסמה | אין |
| 9. | LOGR | מהשרת | אישור התחברות מהשרת (שם משתמש קיים+סיסמה מתאימה) | אין | אם אין התאמה באחד מהשניים מוחזרת הודעת שגיאה (בהמשך הטבלה) |
| 10. | REGI | מהלקוח | בקשת לקוח להרשמה | 1. שם משתמש  2. סיסמה | אין |
| 11. | REGR | מהשרת | אישור הרשמה | אין | רק אם אין שם משתמש קיים כבר בשם זה (אחרת שגיאה)  לאחר מכן נשלחת הודעה באימייל למשתמש עם קוד אימות |
| 12. | VERR | מהלקוח | בקשת לקוח לאישור קוד אימות | 1. אימייל  2. קוד | שרת מאמת קוד בצד שלו (לקוד זמן תפוגה, בזמן הזה השם משתמש שמור) |
| 13. | VERF | מהשרת | אישור אימות קוד הירשמות בצד השרת | אין | רק אם קוד תקף ונכון – אחרת מוחזרת שגיאה |
| 14. | RSND | מהלקוח | בקשת לקוח לשליחה חוזרת של הקוד אימות | אימייל לקוח | מתלווה בהודעת VERF מהשרת |
| 15. | FORG | מהלקוח | בקשת לקוח לאיפוס סיסמה | אימייל לקוח | אין |
| 16. | REST | מהשרת | אישור לבקשת איפוס סיסמה מלקוח | אין | שרת שולח קוד אימות לאימייל לקוח |
| 17. | RSTR | מהלקוח | סיסמה חדשה מלקוח | 1. קוד 2. סיסמה חדשה | אין |
| 18. | RSOK | מהשרת | אישור שרת על איפוס סיסמה בהצלחה | אין | מתקיים רק אם הקוד שהתקבל נכון ותקף אחרת מוחזרת שגיאה |
| 19. | EXIT | מהלקוח | בקשה לקוח להתנתקות | אין | אין |
| 20. | EXTR | מהשרת | אישור התנתקות לקוח | אין | שרת סוגר חיבור (וסוגר thread) |
| 21. | ERRR | מהשרת | הודעת שגיאה מהשרת | 1. מס' שגיאה | משמעות מספרי שגיאה למטה. |

1. מבנה ההודעות:

* הודעות מחרוזתיות – מוצפנות AES (או בינארי לפני העברת מפתח)
* שדה אורך בגודל קבוע של 8 תווים
* מפריד בין שדות: '~' (ללא הפרדה בין שדה אורך לקוד הודעה)

לדוגמה:

“00000004LOGN~ophir@gmail.com~ophir123”

“00000004REGI~ophir@gmail.com~ophir123”

“00000004VERR~ ophir@gmail.com~4d90669e”

1. צורת מענה: סינכרוני, **תלות בין הודעות:** כל הודעה 1,3,4,6,8,10,12,14,15,17,19 תלווה בהודעת תגובה 2, 5,7,9,11,13,16, 18,20,21
2. שגיאות: 501 – שגיאת התחברות (שם משתמש ו\או סיסמה)

502 – שגיאת הירשמות

503 – שגיאה עקב קוד אימות שגוי \ לא תקף (עברה מגבלת הזמן) או משתמש לא קיים

504 – שרת לא תומך בשיטת העברת מפתחות שנתבקשה מהלקוח