**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**   
לכל לקוח יש מצב שבו הוא נמצא, את המצב השרת זוכר ולפיו מסנן אילו הודעות הלקוח יכול לשלוח.  
מצב ראשון: מצב אנונימי בו כל לקוח חדש מתחיל

|  |  |  |  |
| --- | --- | --- | --- |
| OPP | צד | שדות | הסבר |
| SNGU | לקוח | username, email, password, renter | בקשה להירשם לפלטפורמה |
| SNGR | שרת | username,  UsernameUsed  InvalidEmail  WrongRenter  SingedUp | שולח את שם המשתמש והאם נרשם בהצלחה או את סיבת הכישלון |
| LOGI | לקוח | username, password | בקשה להתחבר |
| LOGR | שרת | FailToLogin | נשלח אם שם פרטי החיבור שגויים |
| FGPS | לקוח | username | הצהרת שיכחון סיסמה (בשביל שחזור עתידי) |
| FGPR | שרת | WrongUsername | נשלח אם שם המשתמש בשיכחון הסיסמה לא קיים |
| 2FAR | שרת | NONE | נשלח לאחר התחברות או שיכחון סיסמה מוצלח, משנה את מצב הלקוח למתחבר או שוכח סיסמה בהתאמה ושולח קוד במייל |

מצב שני: מצב החברות בו לאחר LOGI מוצלח נשלח קוד במייל של המשתמש והודעת 2FAR שמחכה לקבלת הקוד.

|  |  |  |  |
| --- | --- | --- | --- |
| OPP | צד | שדות | הסבר |
| 2FAC | לקוח | code | שליחת הקוד לשרת בשביל בדיקה דו שלבית |
| 2FAV | שרת | Verified  NotVerified | מודיע ללקוח אם הבדיקה הדו שלבית עבדה ומשנה את מצבו למצב בית במידה וכן |

מצב שלישי: מצב שיכחון סיסמה בו לאחר FGPS מוצלח נשלח קוד במייל של המשתמש והודעת 2FAR שמחכה לקבלת הקוד.

|  |  |  |  |
| --- | --- | --- | --- |
| OPP | צד | שדות | הסבר |
| 2FAC | לקוח | code | שליחת הקוד לשרת בשביל בדיקה דו שלבית |
| 2FAV | שרת | Verified  NotVerified | מודיע ללקוח אם הבדיקה הדו שלבית עבדה ומשנה את מצבו למצב שינוי סיסמה במידה וכן |

מצב רביעי: מצב שינוי סיסמה בו שם משתמש של הלקוח כבר אושר וניתן לשנות את סיסמתו

|  |  |  |  |
| --- | --- | --- | --- |
| OPP | צד | שדות | הסבר |
| CHPS | לקוח | password, renter | בקשה לשנות סיסמה, שולח את הסיסמה פעמיים בכדי לוודא שאין שגיאת הקלדה |
| CHPR | שרת | ChangedPassword  WrongRenter | מודיע ללקוח האם השינוי היה מוצלח ובמידה וכן משנה את מצבו לאנונימי |

מצב חמישי: מצב בית בו זהותו של המשתמש ידוע וכעת הוא יכול לבצע בקשות שונות בפלטפורמה

|  |  |  |  |
| --- | --- | --- | --- |
| OPP | צד | שדות | הסבר |
| GTUD | לקוח | username | מבקש מידע על משתמש מסוים |
| GUDR | שרת | Description, icon, status, followers, following | מחזיר מידע על אותו משתמש שכולל את כל השדות הנ"ל |
| GTUL | לקוח | NONE | מבקש רשימה של כל שמות המשתמשים |
| GTUR | שרת | UsernamesList | מחזיר רשימה של כל שמות המשתמשים במערכת |
| CHPI | לקוח | icon | מבקש לשנות תמונת פרופיל |
| CPIR | שרת | IconSet | משנה תמונת הפרופיל בשרת ומודיע על הצלחה |
| CHDS | לקוח | description | מבקש לשנות את תיאור הפרופיל |
| CHDR | שרת | not a valid description  description changed | מודיע האם שונה התיאור בשרת ואם לא אז למה |
| FOLL | לקוח | username | בקשה לעקוב אחר משתמש |
| FOLR | שרת | Already followed  Followed | מודיע האם המעקב התבצעה או שהלקוח כבר עקב אחר משתמש זה |
| UFOL | לקוח | username | בקשה להסיר עוקב ממשתמש |
| UFOR | שרת | Already unfollowed  Unfollowed | מודיע האם הסרת המעקב התבצעה או שהלקוח אינו עוקב אחר משתמש זה |
| STRM | לקוח | Title, ip | בקשה לעלות לשידור ממחשב מסויים ועם כותרת |
| STMR | שרת | Already streaming  video\_sock,  audio\_sock | מעלה את הלקוח לשידור ומחזיר לו אל אילו PORTS עליו לשלוח מידע בכדי שיעבור לצופים שלו ויעביר אותו למצב שידור. אלה אם הוא כבר בשידור (לא אמור לקרות) ואז השרת לא יעשה כלום |
| WSTM | לקוח | Streamer, ip | בקשה לצפות במשתמש ממחשב מסויים |
| WTSR | שרת | Not streaming  audio\_port, title | משנה את מצב הלקוח לצופה במשתמש זה ושולח לו את PORT שדרכו הוא יקבל שמע ואת כותרת השידור. אלה אם כן המשתמש לא בשידור |

מצב שישי: מצב משדר בו הלקוח מעביר UDP VIDEO ו TCP AUDIO אל השרת והשרת מפיץ את המידע ללקוחות אחרים

|  |  |  |  |
| --- | --- | --- | --- |
| OPP | צד | שדות | הסבר |
| STOP | לקוח | NONE | מבקש לסיים את השידור |
| STOR | שרת | Not streaming  Stopped | מספיק את השידור אלה אם כן הוא לא בשידור (לא אמור לקרות) ומעבר את הלקוח למצב בית. |
| GETV | לקוח | NONE | מבקש את מספר הצופים בשידור |
| GTVR | שרת | viwers | מחזיר את מספר הצופים בשידור |

מצב שביעי: מצב צופה בו הלקוח מקבל מידע UDP VIDEO ו TCP AUDIO על לקוח באמצעות מעבר המידע דרך השרת

|  |  |  |  |
| --- | --- | --- | --- |
| OPP | צד | שדות | הסבר |
| STWS | לקוח | NONE | מבקש לסיים את השידור |
| STWR | שרת | Not watching  Stopped watching | מספיק את הצפייה בלקוח אלה אם כן הוא לא צופה באף אחד (לא אמור לקרות) ומעבר את הלקוח למצב בית. |
| GETV | לקוח | NONE | מבקש את מספר הצופים בשידור בו הלקוח צופה |
| GTVR | שרת | viwers | מחזיר את מספר הצופים בשידור בו הלקוח צופה |

\*בכל מצב הלקוח יכול לשלוח OOP CNCL והשרת יחזיר OPP CNCR ויעביר אותו למצב אנונימי ויסגור את שידורו או יפסיק את צפייתו אם נדרש.

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