עקרונות יישום האימות המוגבר

ועדת כרטיסי חיוב

תוכן עניינים

[פרק 1 : רקע ומטרות 2](#_Toc108505577)

[פרק 2 : אימות מוגבר באירופה 3](#_Toc108505578)

[פרק 3 : מאפיינים לאימות מוגבר בישראל 4](#_Toc108505579)

[פרק 4 : פרוטוקול D Secure3 6](#_Toc108505580)

[פרק 5 : אימות מוגבר בעסקה טלפונית ובהרשאה לחיוב חשבון 8](#_Toc108505581)

## פרק 1 : רקע ומטרות

בשנים האחרונות חלה התפתחות משמעותית בתחום התשלומים בישראל אשר הביאה לפיתוח מגוון של אמצעי תשלום חדשניים. לצד היתרונות בשימוש באמצעי התשלום המתקדמים, ישנם גם סיכונים שאליהם הלקוח ובית העסק עשויים להיות חשופים כגון הונאות, גניבת זהויות, זיופים, שימוש לרעה וכו'. על מנת לצמצם סיכונים אלו ולהגביר את התחרות והחדשנות יש צורך לקבוע סטנדרטים ועקרונות ברורים לגבי האופן שבו ניתן יהיה לאמת את זהותו של הלקוח ברמת וודאות גבוהה.

חוק שירותי תשלום, תשע"ט-2019 (להלן: "**החוק**") הבחין בין "פרט אימות", שהינו פרט **ייחודי למשלם** שנועד לאמת את זהותו ולהבטיח כי אכן הוא שנתן את הוראת התשלום, לבין "פרט אימות מוגבר", שהינו פרט אימות המאמת את זהותו של המשלם **ברמת ודאות גבוהה.** כאשר נותני שרותי תשלום באים ליישם את החובות האמורות עליהם לפעול בהתאם להגדרות אלה ולתכליות שלהן.

נייר עמדה זה, גובש בוועדת כרטיסי חיוב[[1]](#footnote-1) (להלן: "**הוועדה**") בעבודה משותפת של השחקנים השונים בשוק כרטיסי החיוב במסגרת הוועדה, במטרה לקבוע סטנדרטים אחידים בין נותני שירותי התשלום וליצור וודאות בשוק בנוגע למרכיבים אשר יכולים להיחשב כאימות מוגבר.

אגף הפיקוח על מערכות תשלומים יעקוב אחרי השיטות שהשוק יבחר ליישם בפועל.

## פרק 2 : אימות מוגבר באירופה

בשנת 2019 פרסם ה-EBA נייר עמדה הנוגע למרכיבים ולתהליך שייחשבו כאימות מוגבר (Strong Customer Authentication) באיחוד האירופאי[[2]](#footnote-2). ה-EBA קבע כי יישום האימות המוגבר יתבסס על שני מרכיבים או יותר מתוך הקטגוריות הבאות:

1. ידע (Something You Know – משהו שאתה יודע) – מידע שרק המשתמש יודע.
2. החזקה (Something You Have – משהו שיש לך) – משהו שרק למשתמש יש. החזקה אינה מתייחסת רק להחזקה פיזית, אלא יכולה גם להתייחס להחזקה שאינה פיזית.
3. משהו מובנה (Something You Are – משהו שהוא אתה) – בקטגוריה זו נכללים מאפיינים ביולוגיים, התנהגותיים וביומטריים.

כלומר, על מנת שיתבצע אימות מוגבר, יש צורך לזהות את המשתמש על ידי 2 מרכיבים או יותר, כאשר כל מרכיב הינו מקטגוריה אחרת. נוסף על כך, חלה החובה שמרכיבים אלו יהיו בלתי תלויים אחד בשני כך שפגיעה באחד לא תפגע במהימנות השני וסודיות המידע תישמר.

## פרק 3 : מאפיינים לאימות מוגבר בישראל

במסגרת הוועדה נערכו דיונים הנוגעים למצב המשפטי הקיים בישראל, מורכבויות וצורכי השוק, החלת האימות המוגבר באירופה, כללים ומרכיבים אפשריים ל-"פרט אימות מוגבר" ופתרונות אפשריים לאימות מוגבר בעסקה טלפונית והרשאה לחיוב חשבון.

במסגרת הדיונים הוסכם בין השחקנים לאמץ את העיקרון שנקבע על ידי ה-EBA שלצורך אימות מוגבר יש צורך בזיהוי המשלם על ידי 2 מרכיבים או יותר מתוך הקטגוריות: משהו שיש לך, משהו שאתה יודע ומשהו שהוא אתה, כאשר לא ניתן יהיה להסיק מתוך פרט אימות מוגבר אחד על האחר.

הוועדה בחנה, בכל קטגוריה כאמור, את הכללים והמרכיבים שנקבעו באירופה ואלו אשר הוצעו על ידי השחקנים השונים ואת התאמתם להיכלל כפרט אימות מוגבר בהתאם למאפיינים ולצרכי השוק הישראלי.

כללים ומרכיבים מוסכמים אלו המשקפים את המצב המקובל היום, הינם מרכיבים אפשריים שניתן לעשות בהם שימוש לצורך האימות המוגבר וכל נותן שירותי תשלום יכול לבחור את המרכיבים הרלוונטיים מבחינתו (בהתאם לניהול הסיכונים שלו), זאת בהתאם לעיקרון שיש לעשות שימוש בלפחות 2 מרכיבים או יותר מתוך 3 הקטגוריות.

כללים ומרכיבים אלו אינם מהווים רשימה סגורה וצפויים להתעדכן מפעם לפעם, בהתאם לשינויים בטכנולוגיה, שינויים בסוגי ההונאות ושינויים בצרכי השוק. משכך:

* מרכיב ששימש לאימות בקטגוריה אחת אינו יכול לשמש כמרכיב בקטגוריה אחרת. כך למשל, OTP יכול להיחשב כמרכיב ידע או החזקה אך לא כשניהם באותה עסקה.
* השימוש בשני המרכיבים בתהליך האימות יכול להתבצע באותו מכשיר שבו החלה העסקה. כלומר, אין חובה להשתמש בשני מכשירים שונים מתחילת התהליך ועד סופו.
* תהליכי האימות אינם חייבים להיות חשופים למבצע התשלום ויכולים להתבצע מ"אחורי הקלעים" ובלבד שהעסקה תירשם כעסקה שבוצעה באימות מוגבר.

להלן המרכיבים בכל קטגוריה שיכולים להיחשב כפרט אימות מוגבר:

**ידע** (Something You Know) – משהו שאתה יודע[[3]](#footnote-3):

|  |  |  |
| --- | --- | --- |
| מספר | המרכיב | פרט אימות מוגבר  |
| 1 | סיסמה | **כן** |
| 2 | PIN | **כן** |
| 3 | תבנית זיכרון | **כן** |
| 4 | OTP | **כן** |
| 5 | כתובת דואר אלקטרוני | לא |
| 6 | שם משתמש | לא |
| 7 | פרטי כרטיס האשראי המודפסים עליו | לא |
| 8 | מספר תעודת זהות[[4]](#footnote-4) | לא |

**החזקה** (Something You Have) – משהו שיש לך[[5]](#footnote-5):

|  |  |  |
| --- | --- | --- |
| מספר | המרכיב | פרט אימות מוגבר  |
| 1 | החזקת מכשיר שאומת באמצעות יצירה או קליטה של One-Time Password  | **כן** |
| 2 | החזקת מכשיר שאומת באמצעות חתימה (חומרה או טוקן תוכנה) | **כן** |
| 3 | החזקת מכשיר או כרטיס שאומת באמצעות QR[[6]](#footnote-6) | **כן** |
| 4 | אפליקציה או דפדפן שאומת על ידי קישור המכשיר[[7]](#footnote-7) | **כן** |
| 5 | החזקת כרטיס חיוב שאומת באמצעות Point Of Sale | **כן** |
| 6 | החזקת כרטיס חיוב המאומת בקוד דינאמי | **כן** |
| 7 | החזקת איי מייל שאומת באמצעות One-Time Password | **כן** |
| 8 | החזקת קו נייח שאומת באמצעות One-Time Password | **כן** |
| 9 | אפליקציה המותקנת במכשיר | לא |
| 10 | החזקת כרטיס חיוב המאומת על ידי הפרטים המודפסים עליו | לא |
| 11 | החזקת כרטיס חיוב המאומת על ידי פרט מודפס אחר  | לא |

משהו **שהוא אתה** (Something You Are)[[8]](#footnote-8):

|  |  |  |
| --- | --- | --- |
| מספר | המרכיב | פרט אימות מוגבר  |
| 1 | טביעת אצבע | **כן** |
| 2 | זיהוי קול | **כן** |
| 3 | זיהוי של יד ופנים | **כן** |
| 4 | סריקה של רשתית העין | **כן** |
| 5 | זיהוי לפי תבנית הקלדה[[9]](#footnote-9) | **כן** |
| 6 | קצב לב או תבנית תנועת גוף אחרת | **כן** |
| 7 | הזווית בה המכשיר מוחזק | לא |
| 8 | מידע המשודר באמצעות פרוטוקול תקשורת  | לא |
| 9 | תבנית זיכרון | לא |

## פרק 4 : פרוטוקול D Secure3

3-D Secure הינו פרוטוקול אשר מספק שכבת אימות נוספת ללקוח וזאת במטרה להפוך עסקאות מסחר דיגיטלי למאובטחות יותר בזמן אמת[[10]](#footnote-10). הפרוטוקול מאפשר להחליף נתונים בין המנפיק, בית העסק, ובעת הצורך גם הלקוח, כדי לאשר כי הבעלים החוקי של החשבון יזם את העסקה.

פרוטוקול 3-D Secure הינו טכנולוגיה התומכת באפשרות לבצע, בהתאם לפרופיל וניהול הסיכונים של כל מנפיק, תהליך אימות מוגבר של מבצע התשלום העומד בסטנדרטים שנקבעו על ידי ה-EBA (Strong Customer Authentication).

פרוטוקול 3D Secure גרסה 2.2 ומעלה הינו דור חדש של הפרוטוקול התומך בתהליך זה וכולל מגוון פרמטרים ושיטות של אימות מוגבר, כגון: מיקום המשתמש בעת ביצוע העסקה, אופי העסקאות הקודמות שביצע, גובה התשלום בעסקאות קודמות, סוג המטבע שבו נעשה שימוש, מידע ספציפי אודות המכשיר שממנו בוצעה העסקה, מידע אודות הדפדפן לרבות כתובת ה-IP ועוד. לאור שקלול הנתונים מעריך הפרוטוקול את הסיכון בעסקה ובהתאם לכך יכול לבקש ממבצע התשלום פרטים ותהליכי אימות נוספים (לדוגמה: OTP) על מנת לאמת את זהותו.

תהליכים אלו בפרוטוקול יכולים למעשה לזהות את המשלם ולאמת את זהותו, ברקע, מבלי שהמשלם ידע שהאימות מתבצע (לדוגמה: זיהוי המכשיר הספציפי שממנו מתבצע התשלום ושהמשלם הוא זה שביצע את הכניסה לאותו מכשיר באמצעות קוד או זיהוי ביומטרי אחר).

לאור המנגנונים ותהליכי האימות שנקבעו בפרוטוקול ה- 3-D Secure, במסגרת דיוני הוועדה, הוסכם כי עסקה המאומתת באמצעות פרוטוקול 3-D Secure גרסה 2.2 ומעלה יכולה להיחשב כעסקה שבוצעה בתהליך של אימות מוגבר של מבצע התשלום[[11]](#footnote-11), זאת בהתאם למקובל בעולם.

בתהליך אימות המבוסס 3-D Secure מסר האימות יהיה דינאמי כך שסכום העסקה ובית העסק יוצגו למשלם.

יובהר כי מדובר בהסכמות בין השחקנים בשוק ואין בפרסום העקרונות כדי להעיד על עמדת המאסדרים של השחקנים, לרבות הפיקוח על הבנקים, או כדי לפגוע או לצמצם את סמכויות הפיקוח והאכיפה שלהם.

## פרק 5 : אימות מוגבר בעסקה טלפונית ובהרשאה לחיוב חשבון

הוועדה דנה באופן ספציפי גם בפתרונות אימות מוגבר בעסקאות טלפוניות ובהרשאות לחיוב חשבון שגובשו על ידי עמותת הפרוטוקול ובחנה את עמידת הפתרונות שהוצעו על ידי העמותה בעקרונות האימות מוגבר.

**עסקאות טלפוניות:**

הפתרון המוצע לאימות עסקאות טלפונית עושה שימוש בפרוטוקול 3-D Secure לביצוע האימות המוגבר. מכיוון שכך, השחקנים סבורים כי יישום פתרון העמותה לאימות בעסקאות טלפוניות עשוי להיחשב כעסקה שבוצעה בתהליך של אימות מוגבר.

יובהר כי ההחלטה לביצוע אימות מוגבר בעסקאות אלו נתונה לשיקול דעתו של בית העסק.

**הרשאה לחיוב חשבון:**

הפתרון המוצע לאימות הרשאות לחיוב חשבון משתנה בהתאם לערוץ הקמת ההרשאה לחיוב חשבון (הוראת הקבע):

1. **באמצעות דף אינטרנט או מוקד טלפוני** – האימות יבוצע במנגנון 3D Secure.
2. **בנוכחות הלקוח** – האימות יבוצע באמצעות שני רכיבים כאשר אחד מהם הינו PIN code. (כרכיב של משהוא שאתה יודע).
3. **קבצי אצווה – Batch** – האימות המוגבר יבוצע על ידי המנפיק במועד הקמת ההרשאה בהתאם לעקרונות האימות המוגבר ולכן בעת דרישת התשלום באצווה מכוח הוראות הקבע לא נדרש לבצע אימות נוסף.

במקרים שבהם מבוצעת החלפה של כרטיס, בין אם ישירות על ידי הלקוח מול בית העסק ובין אם בתהליך אוטומטי של העברת הרשאות לחיוב חשבון על ידי המנפיק החדש, נדרש לבצע תהליך אימות מוגבר מחדש בהתאם לעקרונות שנקבעו בנייר זה. נציין כי ניתן לבצע תהליך אימות מוגבר אחד עבור מספר הרשאות לחיוב חשבון.

יובהר כי החוק קובע שיש לאמת את המשלם בפרט אימות מוגבר כאשר מוגשת בקשה למתן הרשאה לחיוב, בין אם הבקשה הוגשה על ידי המשלם ובין אם הוגשה באמצעות המוטב.

**נדגיש כי האימות המוגבר בעסקאות אלו יכול להתבצע גם בדרכים נוספות אחרות העומדות בעקרונות האימות המוגבר וכי מרכיבים אלו יעודכנו מעת לעת בהתאם לשינויים ולהתפתחויות בתחום.**

1. ועדת כרטיסי חיוב הוקמה על מנת להוות פלטפורמה לקידום נושאים מקצועיים וטכנולוגיים הנוגעים לדרך הפעילות ולכללי ביצוע העסקאות במערך כרטיסי החיוב. הוועדה משמשת כגורם מייעץ לפיקוח על מערכות תשלומים בבנק ישראל בתפקידו לוודא את יעילותן ויציבותן של מערכות התשלומים במשק ומורכבת מנציגים של שחקנים שונים בשוק כרטיסי החיוב – בהם שב"א, תאגידים בנקאיים, מפיצים, יצרנים, סולקים ומנפיקים. [↑](#footnote-ref-1)
2. <https://www.eba.europa.eu/file/104475/> [↑](#footnote-ref-2)
3. יישום מרכיבים אלו צריך לכלול אמצעים לצמצום החשיפה שלהם לגורם לא מורשה. [↑](#footnote-ref-3)
4. ביטול השימוש במספר ת"ז כחלק מתהליך אימות פרטי המשלם בעסקאות כרטיסי חיוב צפוי לידון בעמותת הפרוטוקול לשם הוצאת רכיב זה מהפרוטוקול. [↑](#footnote-ref-4)
5. יישום מרכיבים אלו צריך לכלול אמצעים למניעת שימוש לא מורשה במרכיב או ביכולת לשכפלו. [↑](#footnote-ref-5)
6. מקור חיצוני הקורא את קוד ה-QR מהכרטיס או מהמכשיר המאומת – זיהוי ייחודי. [↑](#footnote-ref-6)
7. קישור ייחודי בין המכשיר לאפליקציה\דפדפן. [↑](#footnote-ref-7)
8. יישום מרכיבים אלו צריך להתבצע באופן שיוביל לסבירות נמוכה כי גורם לא מורשה יאומת כמשלם. [↑](#footnote-ref-8)
9. הכוונה לאופן ההקלדה (קצב, עוצמה וכו') לא לתבנית עצמה (אשר יכולה להיחשב כאלמנט ידע). [↑](#footnote-ref-9)
10. <https://www.emvco.com/emv-technologies/3d-secure/> [↑](#footnote-ref-10)
11. נדגיש כי ביישום המנגנון נדרש ליישם מנגנונים העומדים ב-Strong Customer Authentication, כלומר שימוש בשני מרכיבים מקבוצות שונות לפחות. [↑](#footnote-ref-11)