



מדיניות לאומית להזדהות בטוחה

תוצר ג' –

"קווים מנחים" לאמצעי הזדהות

טבלת מסמכי המדיניות

(הערה: שם המסמך הנוכחי מודגש **בצהוב**)

שם המסמך
עיקרי המדיניות הלאומית להזדהות בטוחה
תוצר א' - "קווים מנחים" לרמות הבטחת אימות ולסיווג שירותים
תוצר ב' - "קווים מנחים" לשלב ההרשמה
תוצר ג' - "קווים מנחים" לאמצעי הזדהות



טבלת ניהול מהדורות

מהדורה	תאריך	סטטוס	פרק/סעיף	תקציר השינוי
0.1	25.12.15	טיוטה	כל המסמך	מהדורה ראשונה
0.2	18.1.16	טיוטה	כל המסמך	עדכון בעקבות הערות רוחביות של הממונה לתוצר ב'
0.3	10.2.16	טיוטה	כל המסמך	טיוטה פנימית לדיון ביחידה
0.4	15.2.16	טיוטה	כל המסמך	טיוטה פנימית לדיון ביחידה
1.0	7.3.16	טיוטה	כל המסמך	טיוטה לאישור הממונה, לאחר הטמעת ההערות בסבב הפנימי
1.1	30.3.16	טיוטה	כל המסמך	נוסח מאושר ע"י הממונה להפצה לסבב היועצות שני
1.2	7.4.16	טיוטה	סעיף 1.1	נוסח מאושר ע"י הממונה להפצה לסבב היועצות שני
1.2.1	21.4.16	טיוטה	סעיפים שונים	נוסח לאישור הממונה
1.3	26.5.16	טיוטה	סעיפים שונים	עדכון לאחר הערות הממונה בפגישה ב- 9.5.16
1.4	15.6.16	טיוטה	סעיפים שונים	הטמעת מהדורה 1.3
2.0	26.6.16	טיוטה להיוועצות	עדכון	
3.0	15.9.2016	מהדורה סופית		
4.0	8.9.2020	מהדורה מעודכנת	כל המסמך	ר' מכתב סימוכין - 0939

סיווג : בלמ"ס



תוכן עניינים¹

תוכן

4	תוצר ג' - "קווים מנחים" לאמצעי הזדהות: דוגמאות מעשיות למימוש
4	1. כללי
4	2. דוגמאות למאתמתיים נפוצים בישראל
5	3. דוגמאות למנגנוני אימות משולבים של מספר מאמתים
5	4. סוגי מאמתים מרכזיים
6	תוצר ג' - "קווים מנחים" לאמצעי הזדהות
6	1. רקע
6	2. הנחייה למשרדי הממשלה למימוש הזדהות בטוחה ברב"א 3
6	3. מטרות המסמך
7	4. מתודולוגיה ומבנה המסמך
7	5. תפישה והגדרות לגבי סיווג אמצעי הזדהות
11	6. עמידת אמצעי הזדהות ברב"א
13	7. היבטים ארגוניים וניהוליים
14	נספח א' - שלבי משנה של הנפקת אמצעי הזדהות וניהולם
17	נספח ב' - ניתוח איומים ובקורות עבור שלב הנפקת אמצעי ההזדהות וניהולם
22	נספח ג' - ניתוח איומים ובקורות עבור שלב האימות המקוון

¹ ביעור המושגים והמונחים בפרק זה ניתן לקרוא במסמך [עיקרי המדיניות](#), בנספח 3, מונחים והגדרות, עמ' 39

תוצר ג' - "קווים מנחים" לאמצעי הזדהות: דוגמאות מעשיות למימוש

1. כללי

- 1.1 תוצר זה מפרט את אמצעי ההזדהות² העונים על דרישות הרב"א השונות. התוצר כולל גם הנחיות טכניות ספציפיות על פי מסמך הנחיות שפרסם NIST³.
- 1.2 במסגרת תוצר זה, ולצורך הצגת תהליך האימות, שולב המונח "מאמת" (authenticator). מונח זה, בהקשר של תהליך האימות, משמעותו כלי אחסון של "סוד" הנשלט על ידי גורם אימות אחד או יותר. זוהי למעשה "המעטפת" השומרת על "הסוד", לצורך הזדהות מול מערכת מקוונת⁵. מקור המונח "מאמת" הוא במסמך הטכני של NIST כאמור לעיל, בו מתוארות רמות הבטחת האימות לאמצעים טכנולוגיים שונים. זאת, בעוד שהתקן⁶ עליו מתבססת המדיניות, אינו מפרט אמצעים כאלו, שכן הוא "נייטרלי" מבחינה טכנולוגית.

2. דוגמאות למאמתים נפוצים בישראל

להלן מספר דוגמאות של "מאמתים" נפוצים ונגישים בישראל, והרב"א שהם עומדים בה בפני עצמם (ללא שילוב עם מאמתים אחרים):

ספ'	סוג המאמת	רב"א	דוגמאות
1	סוד זכור ⁷	2 / 1	סיסמה או PIN Code.
2	ידע רשום מראש (יר"מ) ⁸	2 / 1	שאלות אימות על בסיס ידע רשום מראש. היר"מ לא יכול לכלול פרטים המודפסים על גבי הכרטיס המשמש לאימות כגון מידע המודפס על ת.ז, רשיון, ספרות כרטיס אשראי, וכן מידע המודפס לצד אמצעי האימות. בנוסף כתובת אי מייל לא תחשב ביר"מ. או מידע שיש לו פוטנציאל שיהיה חשוף לכלל, כגון : כתובת מגורים וכו'.
3	מאמת בערוץ נפרד (מב"ן) ⁹	2	משלוח מסרון (SMS) ובו קוד אימות המועבר בערוץ נפרד, אם כי שני הערוצים יכולים להתקיים באותו מכשיר נייד פיזי.
4	מודול תוכנה קריפטוגרפית ר"ג ¹⁰	3	אפליקציית חילול סיסמה חד-פעמית ¹¹ מאובטחת, במכשיר נייד.
5	התקן קריפטוגרפי/ ביומטרי ר"ג	4	תעודת הזהות החכמה, שעליה תעודה דיגיטלית לאימות, או מידע ביומטרי לצורך אימות.

² Credentials

³ NIST.SP.800.63.3

⁴ NIST.SP.800.63.3

⁵ בטיטות מהדורת NIST הנמצאת בהיוועצות הוחלף המונח token - authenticator שהוא מונח מתאים יותר. המינוח הקודם גרם לאי-הבנות שכן token מתייחס כיום לאמצעי חומרה מאובטח המשמש לאימות מקוון.

⁶ ISO/IEC 29115 – First Edition, Information technology – Security techniques – Entity authentication assurance Framework

⁷ Memorized secret

⁸ Knowledge Based Verification

⁹ Out-of-Band token

¹⁰ ר"ג – רב-גורמי, MF / Multi-Factor

¹¹ One-Time-Password

3. דוגמאות למנגנוני אימות משולבים של מספר מאמתיים

המטריצה להלן מתייחסת לשילוב בין מספר מאמתיים, והרב"א המתקבלת כתוצאה משילוב זה¹²:

התקן קריפטוגרפי/ ביומטרי ר"ג ¹⁴	מודול תוכנה קריפטוגרפית ר"ג	מאמת בערוץ נפרד (מב"ן)	ידע רשום מראש (יר"מ)	סוד זכור	רב"א כמאמת בודד ¹³	
4	3	3	2	2	2	סוד זכור
4	3	3	2	2	2	ידע רשום מראש (יר"מ)
4	3	2	3	3	2	מאמת בערוץ נפרד (מב"ן)
4	3	3	3	3	3	מודול תוכנה קריפטוגרפית ר"ג
4	4	4	4	4	4	התקן קריפטוגרפי/ ביומטרי ר"ג

4. סוגי מאמתיים מרכזיים

- 4.1 ניתן לעשות שימוש בתעודת הזהות החכמה ו/או בתעודה אלקטרונית בין אם על ידי התעודה הדיגיטלית לאימות (שימוש ב PIN CODE) ובין אם על ידי המידע הביומטרי שעל תעודת הזהות, ברב"א 4.
- 4.2 ניתן לעשות שימוש במערכת ניהול זהויות מרכזית כגון מערכת ההזדהות, תוך שימוש בסיסמה (סוד זכור) ובקוד אימות הנשלח לטלפון הנייד בצורה מאובטחת (מאמת בערוץ נפרד), ברב"א 3.
- 4.3 ניתן לעשות שימוש במודול תוכנה קריפטוגרפי רב גורמי, כגון – מודול מאושר להפקת סיסמה חד-פעמית (OTP) באפליקציה מאובטחת על מכשיר נייד, ברב"א 3.
- 4.4 במקביל נבחנים אמצעי הזדהות נוספים לרבות שימוש עם מכשירים ניידים, אשר לאחר הגדרתם וההחלטה לגביהם, ישולבו בהמשך במסמך זה (כגון – שימוש בטכנולוגיה לזיהוי חזותי או באמצעים אחרים).

¹² הטבלה מתרכזת באמצעי הזדהות הרלבנטיים לשימוש בממשלה

¹³ עמודה זאת מציגה שוב לצורך התזכורת את הרב"א המושג כמאמת יחיד, בהתאם לטבלה הקודמת בסעיף 2

¹⁴ מתייחס לתעודת הזהות החכמה עם התעודה האלקטרונית לאימות שעליה

תוצר ג' - "קווים מנחים" לאמצעי הזדהות**1. רקע**

- 1.1 לאחר שספק השירותים¹⁵ סיווג את השירות בהתאם לר"ב"א, כמפורט בתוצר א' - "קווים מנחים לקביעת רמת הבטחת אימות ולסיווג שירותים", יש לקבל החלטות נוספות הקשורות במימוש המעשי של תהליך האימות הכולל¹⁶ לשם מתן השירות.
- 1.2 בהתאם לסעיף 11 במסמך המדיניות, יש לתת מענה לשלבים הבאים:
- 1.2.1 שלב ההרשמה (Enrolment).
- 1.2.2 שלב הנפקת אמצעי הזדהות וניהולם (Credential Management) - כמפורט במסמך זה.
- 1.2.3 שלב האימות (Authentication) - כמפורט במסמך זה.

2. הנחייה למשרדי הממשלה למימוש הזדהות בטוחה בר"ב"א 3

- 2.1 בהתאם להחלטת ממשלה 2960, ועל פי סעיף 1 ח, החל בחודש ינואר 2018 תהליך עבודה אל מול מנכ"לי משרדי הממשלה, בו דיווחו לראש היחידה (להלן: "הממונה") על אופן ביצוע הזיהוי בפרייקטים ממשלתיים, זאת כדי לוודא את תאימותם למדיניות הלאומית.
- 2.2 בהתבסס על המגמות הבינלאומיות¹⁷ בתחום רמות הבטחת האימות, לצד קצב התפתחות הטכנולוגיה והאיומים בתחום ההזדהות, המליץ הממונה כי **הר"ב"א להזדהות לקבלת שירותי ממשלה דיגיטליים (מזוהים) לא תפחת מר"ב"א 3** אלא במקרים חריגים, בתיאום ובאישור הממונה.
- 2.3 יוזכר, כי סיווג של ר"ב"א 3 אינו עומד באיום מדינתי, ולכן לעמדת הממונה, שירותים מסוג מסוים יידרשו לעמוד בר"ב"א 4, כמפורט בתוצר א' לסיווג שירותים.

3. מטרת המסמך

- 3.1 מטרת מסמך זה הינן:
- 3.1.1 סיווג אמצעי הזדהות עיקריים בהתאם לר"ב"א בתהליך האימות החוזר לקבלת שירותים מקוונים.
- 3.1.2 הצגת שיטה לסיווג אמצעי הזדהות בהתאם לרמות הבטחת האימות למתן שירותי הממשלה.
- 3.1.3 הצגת דרישות עבור שלב הנפקת אמצעי הזדהות וניהולם.
- 3.1.4 הצגת דרישות עבור שלב האימות המקוון.
- 3.2 **קהל היעד:** מסמך זה מיועד עבור ארבע אוכלוסיות:
- 3.2.1 **תושבי המדינה**, אשר יוכלו ללמוד על מדיניות הממשלה המוסמכת בהקשר להזדהות בטוחה;
- 3.2.2 **ספקי שירותים**, אשר מעוניינים להתאים את רמת הבטחת האימות שקבעו לשירותים, לדרישות שלב הנפקת אמצעי ההזדהות וניהולם;
- 3.2.3 **ספקי זהויות**¹⁸ העוסקים בביצוע שלב ההרשמה.
- 3.2.4 **ספקי אמצעי הזדהות**¹⁹ העוסקים בהנפקת אמצעי הזדהות.

¹⁵ Service Provider

¹⁶ במונח "תהליך האימות הכולל" הכוונה ל- Authentication Framework. חלק ממסגרת תהליך האימות הכולל הוא שלב האימות

המקוון שמתבצע בעת קבלת השירות. לפיכך, השימוש במונח "אימות" במסמך זה, מתייחס להקשר המתאים.

¹⁷ המגמות בעולם ביניהן: צו נשיאותי בחתימות נשיא ארה"ב, הקובע כי גישה לשירותי ממשלה, הכוללים מידע אישי, תתבצע תוך שימוש בשני גורמי אימות והליכי הרכשת זהות תואמים, כלומר, גישה לשירותים בר"ב"א 3 ומעלה. ארגון ה-NIST הפיץ נוסח עדכני של הנחיות להזדהות דיגיטלית, אשר נותן מענה טכנולוגי מפורט, בהלימה לצו הנשיאותי, להעלאת רמת ההזדהות עם שני גורמי אימות. בנוסף, באיחוד האירופי, בהתאם למסגרת ה-eIDAS, קיימות שלוש רמות הבטחת אימות. המסגרת מגדירה כי הסתמכות של מדינה על זיהוי שבוצע במדינה אחרת באיחוד תהיה מחייבת רק מהרמה המקבילה לר"ב"א 3 ומעלה.

¹⁸ Identity Providers

¹⁹ Credential Service Providers

- 4.1 מסמך זה מתבסס על התפישה הכוללת שהוגדרה במסמך "עיקרי המדיניות הלאומית להזדהות בטוחה", ובפרט על תקן ISO/IEC 29115²⁰ עליו מתבססת המדיניות. כמו כן ישנה התייחסות לשני מסמכים נוספים:
- 4.1.1 מסמך ה-NIST לעניין אימות²¹.
- 4.1.2 מסמכי האיחוד האירופי לעניין מסגרת eIDAS²².
- 4.2 מסמך זה כולל את התכנים הבאים:
- 4.2.1 בסעיף 4 מוצגות תפישת והגדרות לגבי סיווג אמצעי הזדהות.
- 4.2.2 בסעיף 5 מוצגת עמידת אמצעי ההזדהות בהתאם לר"א, כולל דוגמאות עבור אמצעי ההזדהות המרכזיים המוצעים כיום על ידי הממשלה.
- 4.2.3 בסעיף 6 מתוארים **היבטים ארגוניים וניהוליים**.
- 4.2.4 בנספח א' מוגדרים **שלבי המשנה** של הנפקת אמצעי ההזדהות וניהולם.
- 4.2.5 בנספח ב' מוצג נושא **ניתוח הסיכונים והבקורות** הכרוכים בהנפקת אמצעי ההזדהות וניהולם.
- 4.2.6 בנספח ג' מוצג ניתוח איומים ובקורות עבור **שלב האימות המקוון**.

5. תפישה והגדרות לגבי סיווג אמצעי הזדהות

.5

- 5.1 **עקרונות**
- 5.1.1 אמצעי הזדהות (Credential) הינו **מידע** שמאפשר לצד המסתמך, לאמת את מחזיקו.
- 5.1.2 **המידע** יכול להיות **מסוגים שונים** ולהיות מיוצר/ מחולל בצורות שונות. עצם הצורה הבסיסית של המידע מעניקה לו חוסן שונה בפני גילוי וחשיפה.
- 5.1.3 **המידע** יכול להיות שמור **בכלי איחסון שונים**, אשר מעניקים לו חוסן נוסף.
- 5.1.4 ניתן להשתמש בתהליך אימות מקוון בו-זמנית במספר אמצעי הזדהות שונים, מסוגים שונים. השילוב של **מספר גורמי אימות**²³ מעניקים לתהליך חוסן חזק יותר מאשר שימוש **בגורם אימות אחד בלבד** ועל כן יש לעשות שימוש בשני גורמי אימות לפחות בתהליך האימות- רב"א³.
- 5.1.5 להלן יפורטו ויוסברו העקרונות דלעיל.
- 5.2 **סוגי אמצעי הזדהות**
- 5.2.1 לצורך הצגת מודל האימות, ישולב בדיון המונח "**מאמת**". מונח זה, בהקשר של תהליך האימות, משמעותו כלי אחסון של "סוד" הנשלט על ידי גורם אימות אחד או יותר. זוהי למעשה "המעטפת" השומרת על "הסוד", לצורך הזדהות מול מערכת מקוונת.
- 5.2.2 המעטפת החיצונית של המאמת, יכולה להיות מיושמת על ידי חומרה²⁴, על ידי תוכנה²⁵ או אף בזיכרון האנושי²⁶.

²⁰ ISO/IEC 29115 – First Edition, Information technology – Security techniques – Entity authentication assurance Framework

²¹ NIST.SP.800.63.3. וכן טיוטת NIST.SP.800.63.3.

²² ר' בפרט את תקנות EIDAS - <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN>

²³ סעיף 3 - הגדרות, הגדרה (2).

²⁴ Multi-factor authentication

²⁵ כגון ע"י כרטיס חכם

²⁶ כגון מודול תוכנה קריפטוגרפי

²⁶ במקרה של סיסמה, לדוגמה, אשר אמורים לזכור אותה בזיכרון, לאחר שהודפס על פלט מתאים, נמסר לאדם ושונן על ידי האדם

- 5.2.3 פלט המאמת הוא **"מידע אימות"** לאימות טענת הזהות של אדם על ידי הצד המסתמך. מידע זה יכול להיות הסוד עצמו²⁷ או התמרה²⁸ כלשהי של הסוד.
- 5.2.4 ישנם שני מקורות קלט אופציונליים למאמת: האחד – קלט לצורך חילול "מידע אימות", והשני – קלט לצורך הפעלת²⁹ המאמת.
- 5.2.5 קלט לשם חילול מידע לאימות, יכול להיות "אתגר" שיבקש לקבל "תגובה" (מנגנוני Challenge-Response)³⁰ או מספר חד-פעמי³¹. מידע זה יכול להיות מסופק על ידי המשתמש עצמו או שהוא קיים במאמת הספציפית³².
- 5.2.6 קלט לשם הפעלת מאמת מסוג "משהו שיש לך", מיושם כאשר בקרת ההפעלה היא על ידי גורם אימות של "משהו שאתה יודע" או על ידי "משהו שאתה". אם המאמת עצמו הינו מסוג של "משהו שאתה יודע" (כגון – סיסמה), אזי "ההפעלה" מובנית כבר במאמת עצמו.
- 5.2.7 "אמצעי הזדהות" ספציפי משמעותו – **קשירה של מאמת מסויים לזהות מסוימת**.

5.3 סוגי מאמותים בהתאם לגורמי האימות

- 5.3.1 מאמת יכול להיות מסוג של **חד-גורמי (ח"ג)**³³ אם הוא עושה שימוש בגורם אימות אחד בלבד. לדוגמה – סיסמה היא מסוג ח"ג שכן היא עושה שימוש רק ב"משהו שאתה יודע" ואין צורך בגורם נוסף להפעלה.
- 5.3.2 מאמת יכול להיות מסוג **רב-גורמי (ר"ג)**³⁴ אם הוא עושה שימוש במספר גורמי אימות. לדוגמה, כרטיס חכם הכולל מפתח פרטי שלשם הפעלתו לביצוע פעולת אימות נדרשת סיסמה (PIN Code). הכרטיס עצמו הוא "משהו שיש לך" (something you have), ה-PIN Code³⁵ הוא "משהו שאתה יודע" (something you know). אם ייעשה שימוש בביומטריה לשם הפעלת המפתח הפרטי, שוב מדובר במאמת ר"ג כאשר הגורם הנוסף הוא "משהו שאתה" (something you are).
- 5.3.3 ככלל לא נדרש שימוש ביותר משני גורמים גם להגעה לר"ג 4. ואולם, ייתכנו מתארים בהם יידרשו כל שלושת גורמי האימות.

5.4 סוגי מאמותים

- 5.4.1 בסעיף זה יוצגו מספר סוגי מאמותים, אשר רלבנטיים למימוש במסגרת המדיניות.
- 5.4.2 הטבלה הבאה מציגה את הרכיבים הבאים:
- 5.4.2.1 סוג המאמת.
 - 5.4.2.2 סוג גורם האימות.
 - 5.4.2.3 האם המאמת הוא ח"ג או ר"ג.
 - 5.4.2.4 דוגמאות.
 - 5.4.2.5 מידע האימות.

²⁷ כגון הסיסמה

²⁸ טרנספורמציה

²⁹ activation

³⁰ מנגנון "אתגר-מענה" הינו מנגנון לאימות זהויות, שבו הישות ה-"טוענת", מציגה את זהותה לישויות אחרת "מאמתת", באמצעות "ידיעת סוד" המשוך לאותה ישות, מבלי לחשוף את הסוד עצמו (מקשה/אינ מאפשר ל-"מצותת" לחשוף את הסוד או לבצע אימות חוזר). מנגנון "אתגר-מענה", עושה שימוש באמצעים קריפטוגרפיים ומוגדר "מאמת חזק".

³¹ nonce

³² כגון התקן חומרה של OTP אשר ייעשה שימוש בשעון שנמצא בו

SF - Single-Factor

MF - Multi-Factor

³⁵ ולכן אסור שה PIN Code יהיה מוטבע על גבי התעודה



ספ'	שם המאמת	סוג גורם האימות	ח"ג / ר"ג	דוגמאות	"מידע אימות"
1	סוד זכור ³⁶	משהו שאתה יודע	ח"ג	מילת סיסמה, הכוללת רצף של אותיות ו/או מספרים; או - רצף מספרי בלבד, כגון PIN Code –	הסוד עצמו, בין אם זאת מילת הסיסמה או ה-PIN Code
2	ידע רשום מראש – יר"מ ³⁷	משהו שאתה יודע	ח"ג	שאלות של ידע אישי, אשר נרשמות מראש במערכת בשלב ההרשמה, כולל התשובות אליהן, ואמורות להיות ידועות רק לבעל הסוד	תשובות האימות הצפויות לשאלות המתאימות
3	מאמת בערוץ נפרד - מב"ן ³⁸	משהו שיש לך	ח"ג	שימוש בהתקן/ מכשיר ³⁹ בערוץ תקשורת נפרד (קרי יישום שונה) מאשר ערוץ התקשורת הראשי שבו נעשה שימוש לצורך האימות. לדוגמה, הערוץ הראשי הינו תקשורת לאתר אינטרנט מסוים. הערוץ השני הינו מכשיר נייד שיש לאדם המבקש להיכנס לאתר. הערוץ השני יכול להיות למכשיר הנייד אשר נרשם בהקשר למשתמש, בתהליך הרישום. המשתמש מקבל את הנתון ומקליד אותו במקום המתאים בכניסה לאתר.	הגורם המאמת שולח מסר עם סוד חד-פעמי (קוד אימות), שיכול להיות אלפאנומרי או עם ספרות בלבד. יובהר שניתן להשתמש גם באותו התקן/ מכשיר, לדוגמה – גלישה ממכשיר סלולארי וקבלת מסרון באותו מכשיר סלולארי אך בערוץ אחר.
4	התקן חילול סיסמה חד-פעמית ח"ג ⁴⁰	משהו שיש לך	ח"ג	התקן שנועד לחולל בצורה אקראית/ ספונטנית, סיסמה חד-פעמית על בסיס מידע גרעיני כלשהו שנשמר בו. אין צורך בגורם אימות נוסף לצורך הפעלתו. לדוגמה, הצג שעל המכשיר יציג סיסמה של 6 ספרות.	מסירת הסיסמה החד-פעמית שחוללה על ידי המכשיר, שנבדקה ונמצאת כסיסמה מקובלת, ומראה כי המשתמש שולט בהתקן

³⁶ Memorized secret. התרגום הוא על בסיס המונח "לשנן" – ללמוד ולזכור על ידי חזרה

³⁷ Pre-Registered Knowledge או Knowledge Based Verification - KBV

³⁸ Out of Band Token

³⁹ device

⁴⁰ Single Factor One-Time-Password

ספ'	שם המאמת	סוג גורם האימות	ח"ג/ר"ג	דוגמאות	"מידע אימות"
5	התקן חילול סיסמה חד-פעמית ר"ג	משהו שיש לך, וכן – משהו שאתה יודע או משהו שאתה	ר"ג	כמו סעיף 4, כאשר לצורך ההפעלה נדרש גורם אימות נוסף , כגון PIN Code או ביומטריה.	כמו 4, בתוספת גורם אימות נוסף
6	מודול תוכנה קריפטוגרפית ר"ג	מודול התוכנה הוא משהו שיש לך, כאשר ההפעלה נעשית על ידי משהו שאתה יודע או משהו שאתה	ר"ג	המפתח נשמר על גבי דיסק או מדיה אחרת שאינה התקן חומרה מיוחד ומחייבת הפעלה על ידי גורם אימות נוסף.	מותנה בפרוטוקול הספציפי
7	התקן קריפטוגרפי ר"ג	משהו שיש לך, וכן – משהו שאתה יודע או משהו שאתה	ר"ג	התקן חומרה הכולל רכיב קריפטוגרפי שמחייב הפעלתו על ידי גורם אימות נוסף. לדוגמה – תעודת הזהות החכמה.	הוכחת בעלות על ההתקן ושליטה על המפתח
8	התקן ביומטרי ר"ג	משהו שיש לך ומשהו שאתה	ר"ג	התקן חומרה הכולל מידע ביומטרי עליו, כאשר נדרש מידע נוסף להפעלה לצורך הגישה למידע הביומטרי. לדוגמה, תעודת הזהות החכמה כאשר יידרש מנגנון מיוחד לשליפת המידע הביומטרי שעל התעודה.	המידע הביומטרי, לצורך השוואה ביומטרית, או מחוץ להתקן או על ההתקן

5.5 שימוש במאמתים בתהליך האימות

- 5.5.1 תהליך האימות יכול לעשות שימוש במאמת אחד בלבד, או במספר מאמתים בו-זמנית.
- 5.5.2 לגבי שימוש במאמת אחד, הרב"א אליה ניתן להגיע הינה כמפורט בסעיף 5.1 להלן.
- 5.5.3 שימוש במספר מאמתים: אדם/ משתמש המבקש להזדהות, מציג מידע אימות משני מאמתים, או יותר. שילוב המאמתים מאופיין על ידי מספר גורמי האימות, הן אלו שהם אינהרנטיים בכל מאמת, והן אלו המשמשים כאמצעי בקרה להפעלתו של המאמת. הרב"א אליה ניתן להגיע הינה כמפורט בסעיף 5.2 להלן.
- 5.5.4 לדוגמה, ניתן לעשות שימוש בסיסמה קבועה ("משהו שאתה יודע") ובנוסף במב"ן (מאמת בערוץ נפרד, שהוא "משהו שיש לך"). ביחד מושגת תוצאה של מאמת ר"ג.
- 5.6 ניתוח וניהול סיכונים עבור שלבים שונים בתהליך: ר' נספחים א', ב', ג'⁴¹ במסמך זה.

⁴¹ ר' לידיעה גם סעיף 6.2 ב- במסמך NIST.SP.800-63-2



6.1 סעיף זה מציג את עמידתם של מאמתים שונים ברב"א, בהתאם לדרישות העיקריות לכל רב"א:

6.2

ספ'	סוג המאמת	רב"א	דרישות עיקריות
1	סוד זכור	1	סיסמה שנבחרה על ידי המשתמש באורך 6 ספרות/ תווים לפחות מתוך מבחר של 90 תווים לפחות; או - PIN Code מחולל בצורה אקראית של 4 ספרות לפחות; או - אמצעי שווה ערך מבחינת אנטרופיה ⁴² .
2	סוד זכור	2	סיסמה שנבחרה על ידי המשתמש, אשר תהווה "סיסמה חזקה", המכילה שילוב של אותיות, ספרות ותווים מיוחדים, בכלל זה שימוש באורך 8 ספרות/ תווים לפחות מתוך מבחר של 90 לפחות; או - PIN Code המחולל בצורה אקראית של 6 ספרות לפחות; או - אמצעי שווה ערך מבחינת אנטרופיה; וכמו כן, ספק הזהות (ה- IdP) מפעיל אמצעי לבדיקת חוזק הסיסמאות.
3	ידע רשום מראש (יר"מ)	1	אם השאלות אינן נקבעות על ידי המשתמש, יש לאפשר לו בחירת שאלה (prompt) מתוך קבוצה של 5 שאלות לכל הפחות. אין לאפשר מענה "ריק" על שאלה.
4	ידע רשום מראש (יר"מ)	2	אם השאלות אינן נקבעות על ידי המשתמש, יש לאפשר לו בחירת שאלה (prompt) מתוך 7 שאלות לכל הפחות. אין לאפשר מענה "ריק" על שאלה.
5	מאמת בערוץ נפרד (מב"ן)	2	המסר נשלח למאמת שניתן לזהות את כתובתו באופן חד-ערכי, ובערוץ שאינו משמש כערוץ התקשורת הראשי לצורת האימות. המסר המחולל הוא ברמת אנטרופיה של 64 ביט לפחות. רמה זו תקשה על התוקף לשבש את תהליך העברת המאמת.
6	התקן חילול סיסמה חד-פעמית ר"ג	2	ייעשה שימוש בפונקציית הצפנת בלוק מאושרת או פונקציית מיצוי ⁴³ , תוך שילוב מפתח סימטרי המצוי על המכשיר יחד עם nonce ליצירת הסיסמה החד-פעמית. ה- nonce יכול להיות תאריך וזמן, או מונה (counter) המחולל על ידי ההתקן.
7	מודול תוכנה קריפטוגרפית ר"ג	3	המודול הקריפטוגרפי ייבדק ויאומת לפי FIPS 140-2 רמה 1 ומעלה. כל הפעלה תחייב הכנסת הסיסמה או מידע הפעלה אחר, וההעתק הבלתי מוצפן של המפתח יימחק לאחר כל אימות.

⁴² אנטרופיה- מדד לכמות חוסר הוודאות המצויה בפני התוקף, כדי לקבוע את הערך של המאמת (הסוד) המועבר. העברה של המאמת דרך ערוץ נאמדת במקטעים, ומקטעים אלו מהווים את יחידות המדידה של האנטרופיה.
⁴³ Hash function



ספ'	סוג המאמת	רב"א	דרישות עיקריות
8	התקן חילול סיסמה חד-פעמית ר"ג	4	המודול הקריפטוגרפי ייבדק ויאומת לפי FIPS 140-2 רמה 2 ומעלה, עם בדיקת אבטחה פיזית לפי FIPS 140-2 רמה 3 ומעלה. ייעשה שימוש בפונקציית הצפנת בלוק מאושרת או פונקציית מיצוי⁴⁴, תוך שילוב מפתח סימטרי המצוי על התקן אישי יחד עם nonce ליצירת הסיסמה החד-פעמית. ה- nonce יכול להיות תאריך וזמן, או מונה (counter) המחולל על ידי ההתקן. כל הפעלה תחייב הכנסת הסיסמה או מידע הפעלה אחר, באמצעות מנגנון קלט אינטגרלי בהתקן.
9	התקן קריפטוגרפי / ביומטרי ר"ג	4	המודול הקריפטוגרפי ייבדק ויאומת לפי FIPS 140-2 רמה 2 ומעלה, עם בדיקת אבטחה פיזית לפי FIPS 140-2 רמה 3 ומעלה. יחייב את הכנת הסיסמה, ה- PIN Code או המידע הביומטרי, לצורך הפעלת מפתח האימות. לא יאפשר ייצוא של מפתחות האימות מתוך ההתקן. לדוגמה: תעודת הזהות החכמה שעליה תעודה דיגיטלית לאימות. במקרה של מידע ביומטרי, האזור המוגן לשמירת המידע הביומטרי, יעמוד לפחות בדרישות ה- ICAO לדרכון הביומטרי. יתאפשר ייצוא של המידע הביומטרי, באמצעות מנגנון קריפטוגרפי שיאושר על ידי הגורמים המוסמכים. דוגמה: שימוש בביומטריה שעל תעודת הזהות החכמה.

6.3 מנגנוני אימות משולבים של מספר מאמטים

6.3.1 הטבלה להלן, מתייחסת לשילוב בין מספר מאמטים, על מנת להנחות את ספקי השירות באשר לאמצעים המרכזיים הנפוצים והרלבנטיים לשימושם⁴⁵:

התקן קריפטוגרפי/ ביומטרי ר"ג ⁴⁷	מודול תוכנה קריפטוגרפית ר"ג	מאמת בערוץ נפרד (מב"ן)	ידע רשום מראש (יר"מ)	סוד זכור	רב"א כמאמת בודד ⁴⁶	
4	3	3	2	2	2	סוד זכור
4	3	3	2	2	2	ידע רשום מראש (יר"מ)
4	3	2	3	3	2	מאמת בערוץ נפרד (מב"ן)
4	3	3	3	3	3	מודול תוכנה קריפטוגרפית ר"ג
4	4	4	4	4	4	התקן קריפטוגרפי/ ביומטרי ר"ג

7. היבטים ארגוניים וניהוליים

7.1 "מסמך הצהרת מדיניות" וקובץ הנחיות מפורט: באחריות ספק זהות, העוסק בהנפקת אמצעי הזדהות למשתמשים, לפרסם "מסמך הצהרת מדיניות" (Policy Statement - PS) המפרט את המבנה הארגוני, תהליכי העבודה, נהלי העבודה והבקורות, שמיושמים בתהליך הנפקת אמצעי הזדהות, בהתאם לרב"א.

7.2 ביקורת חיצונית: נדרש שיהיה תיעוד מסודר של תהליך הנפקת אמצעי הזדהות לצורך ביקורת חיצונית על פי הצורך. ביצוע ביקורת על ידי גורם בלתי תלוי עשויה להידרש בהתאם לדין התקף.

7.3 במטרה לתת מענה הולם בנושא אבטחת המידע/ הגנת הסייבר יש לעמוד בדרישות תורת ההגנה בסייבר (להלן: "תוה"ג")⁴⁸, ובפרט פרק 4- "בקרת גישה" או על פי דין. שימוש במידע אישי והגנת הפרטיות:

7.3.1 תהליך הנפקת אמצעי ההזדהות כרוך במסירת מידע אישי על ידי המבקש לצורך אימות זהותו, בין היתר במערכות מידע חיצוניות רגישות. מסירת מידע כזה תהיה רק מתוך הסכמת המבקש, בכפוף לכל דין.

7.3.2 על הגורם המקבל את המידע לפעול כמתחייב לגבי מידע אישי בהתאם להנחיות.

7.3.3 יש לתכנן את מערכת המידע בתפישה של "עיצוב לפרטיות"⁴⁹ ולהציב בקורות ארגוניות מתאימות בהקשר לאבטחת המידע והגנה עליו, אי-שמירת מידע רגיש לאחר תהליך הנפקת אמצעי ההזדהות וטיפול בחריגים.

7.3.4 יש למנוע חשיפת מידע רגיש לעובדים, בארגון המבצע את הנפקת אמצעי הזדהות, על בסיס העיקרון של Need to Know.

⁴⁵ הטבלה מתרכזת באמצעי הזדהות הרלבנטיים לשימוש בממשלה
⁴⁶ עמודה זאת מציגה שוב לצורך התזכורת את הרב"א המושג כמאמת יחיד, בהתאם לטבלה הקודמת בסעיף 5.1
⁴⁷ מתייחס לתעודת הזהות החכמה עם התעודה האלקטרונית לאימות שעליה
⁴⁸ תורת הגנה בסייבר 1.0
⁴⁹ privacy by design



נספח א' - שלבי משנה של הנפקת אמצעי הזדהות וניהולם

1. **חלוקה לשלבי משנה**
 - 1.1 הנפקת אמצעי הזדהות וניהולם, כוללים שלבי משנה רלוונטיים לניהול מחזור החיים של אמצעי ההזדהות (שלב ההרשמה, המפורט בתוצר ב' של המדיניות הלאומית להזדהות בטוחה, הינו שלב מקדים לשלבי המשנה להלן, להנפקת אמצעי הזדהות וניהולם), מהנפקתם ועד לביטולם הסופי. חלק משלבי משנה אלו תלוי בכך, אם אמצעי ההזדהות מותקן על התקן חומרה מאובטח (hardware token).
 - 1.2 להלן רשימת שלבי המשנה:
 - 1.2.1 א' - יצירת אמצעי הזדהות.
 - 1.2.2 ב' - עיבוד מוקדם⁵⁰, הכולל:
 - 1.2.2.1 ב'1 - איתחול⁵¹.
 - 1.2.2.2 ב'2 - צימוד⁵².
 - 1.2.3 ג' - הנפקת⁵³ אמצעי הזדהות.
 - 1.2.4 ד' - הפעלת⁵⁴ אמצעי הזדהות.
 - 1.2.5 ה' - איחסון⁵⁵ אמצעי הזדהות.
 - 1.2.6 ו' - השעיה⁵⁶, ביטול⁵⁷ ו/או השמדת⁵⁸ אמצעי הזדהות.
 - 1.2.7 ז' - חידוש⁵⁹ או החלפת⁶⁰ אמצעי הזדהות.
 - 1.2.8 ח' - ניהול רשומות⁶¹.
 - 1.3 מימוש השלבים נעשה בהתאם לרב"א.
 - 1.4 פירוט לשלבי המשנה קיים בתקן ISO 29115, ובצורה תמציתית יותר, בהמשך נספח זה.
2. **יצירה**: יצירת אמצעי ההזדהות⁶² בפעם הראשונה.
3. **עיבוד מוקדם**
 - 3.1 אמצעי הזדהות מסוימים מחייבים לעיתים עיבוד מראש לפני ההנפקה, כגון - התאמה אישית לזהות הישות.
 - 3.2 התאמה אישית יכולה להיות, כדוגמה, פרסונליזציה של כרטיס חכם, שעליו נרשמת תעודה דיגיטלית שמשמשת כאמצעי ההזדהות אלקטרוני, כולל הדפסה על הצד החיצוני של הכרטיס ו/או כתיבה לשבב של הכרטיס, של פרטים אישיים נוספים של הישות שעבורה יונפק הכרטיס.
 - 3.3 מאידך, יש גם סוגי אמצעי הזדהות שאינם מחייבים התאמה אישית ועיבוד מראש, כגון - סיסמאות.
 - 3.4 שלבי המשנה של העיבוד המוקדם הם:
 - 3.4.1 אתחול – ר' סעיף 3.5 להלן.
 - 3.4.2 צימוד – ר' סעיף 3.6 להלן.

Pre-Processing⁵⁰
 Initialization⁵¹
 Binding⁵²
 Issuance⁵³
 Activation⁵⁴
 Storage⁵⁵
 Suspension⁵⁶
 Revocation⁵⁷
 Destruction⁵⁸
 Renewal⁵⁹
 Replacement⁶⁰
 Record-Keeping⁶¹

⁶² הכוונה לאמצעי ההזדהות, או אמצעי להפקת אמצעי ההזדהות – כגון, מחולל סיסמאות. לצורך נוחות הקריאה, לא נחזור בכל פעם על שני המונחים, ומכאן - המונח "אמצעי הזדהות" כולל גם "אמצעי להפקת אמצעי הזדהות", אלא אם כן ייאמר אחרת במפורש.



3.5 אתחול

3.5.1 אתחול אמצעי הזדהות כולל את כל הצעדים שמתבקשים כדי להבטיח שאמצעי ההזדהות יוכל לתמוך בהמשך בפונקציות נדרשות שונות.

3.5.2 דוגמה: כרטיס חכם עשוי להיות מונפק על ידי היצרן במצב של "נעילה" שמחייב הצגת סיסמה מיוחדת לשחרור ואתחול הכרטיס.

3.6 צימוד

3.6.1 המונח "צימוד" מתייחס ליצירת קשר בין אמצעי ההזדהות לבין הישות שעבורה הוא יונפק.

3.6.2 דוגמה: כאשר מקשרים בין אמצעי ההזדהות שנוצר בתהליך מקוון לבין רשומת המשתמש, ייעשה שימוש בקוד הפעלה חד פעמי⁶³ שיאושר על ידי המשתמש, וכך יקשור בין המשתמש לבין רשומתו.

4. הנפקה

4.1 הנפקת אמצעי ההזדהות כוללת את אספקתו למשתמש, או קשירה בדרך אחרת בין ישות לבין אמצעי ההזדהות המסויים שהונפק עבורה.

4.2 ככל שהרב"א גבוהה יותר, התהליך עשוי להיות כרוך בהנפקה פיזית של התקן חומרה כלשהו, כגון – כרטיס חכם או token פיזי, ומסירתו בתהליך של "פנים אל פנים"⁶⁴.

4.3 במקרה של רב"א נמוכה, תהליך ההנפקה עשוי להיות פשוט יותר, לדוגמה – שליחת הסיסמה או הקוד אישי בדואר למענו של המבקש, או לחלופין – משלוח סיסמה או קוד לדואר האלקטרוני שסופק על ידי הישות בתהליך ההרשמה. חשוב לוודא, שמאמתיים שיכולים לשמש גם עבור רב"א גבוהה (רב"א 3 ו-4), יימסרו באופן מאובטח.

5. הפעלה

5.1 בשלב הפעלת אמצעי ההזדהות מבוצעות פעולות הכנה שונות, כדי שאמצעי ההזדהות יהיה מוכן לשימוש מעשי על ידי המשתמש.

5.2 לדוגמה, במקרה של חילול מפתחות דיגיטליים על גבי שבב כרטיס חכם, השבב יכול להיות במצב "נעול" לאחר שלב האתחול, כדי למנוע שימוש לרעה בתקופת הביניים שבה אמצעי ההזדהות מאוחסן במפעל ובהמשך בתהליך העברתו הפיזית למשתמש, כאשר למשתמש אין עדיין שליטה באמצעי ההזדהות. במקרה כזה, תידרש פעולת "שחרור נעילה" על ידי המשתמש, לדוגמה – באמצעות שימוש בסיסמה או ב-PIN Code במועד ההנפקה לישות.

5.3 כדוגמה נוספת, ניתן להנפיק תעודה דיגיטלית במצב "מושעה", כך שלא תהייה בתוקף באופן זמני, ולהפעילה רק לאחר תהליך "ביטול השעיה".

5.4 לצורך שימוש בסיסמה, לא נדרש שלב של הפעלה.

6. אחסון: אחסון אמצעי ההזדהות נעשה באופן מאובטח, בתהליך ההנפקה, באופן שמגן עליו מפני חשיפה, שימוש לרעה, שינוי פרטים, או אף הרס, על ידי גישה בלתי מורשית אליו.

7. ביטול, השעיה והשמדה

7.1 "ביטול" הוא מצב שבו תוקף אמצעי הזדהות מסתיים באופן קבוע.

7.2 "השעיה" הוא מצב שבו תוקף אמצעי הזדהות מופסק באופן זמני (ר' גם סעיף 5.3 לעיל לגבי שלב ההפעלה).

7.3 להלן מספר דוגמאות לביצוע "ביטול" אמצעי הזדהות:

7.3.1 אמצעי הזדהות דווח כ"אבד", "נגנב", או שנפגע בדרך אחרת;

7.3.2 פג תוקפו של אמצעי הזדהות;

⁶³ לדוגמה – משלוח קוד אימות במסרון – OUT OF BAND

⁶⁴ בין אם זה במצב שבו המשתמש מגיע למשרדי המנפיק, או שנציג המנפיק מגיע פיזית למשתמש



- 7.3.3 הבסיס להנפקת אמצעי הזדהות אינו קיים עוד. לדוגמה, כאשר עובד עוזב את מעסיקו, אשר הנפיק לו את אמצעי ההזדהות לאור היותו מועסק באותו ארגון ;
- 7.3.4 נעשה שימוש באמצעי הזדהות שלא עבור המטרות המורשות ;
- 7.3.5 הונפק אמצעי הזדהות חדש שמחליף את אמצעי ההזדהות הקודם.
- 7.3.6 משך הזמן בין קבלת ההודעה על אירוע שהתרחש, שמחייב את ביטול אמצעי ההזדהות, לבין הביטול עצמו, נקבע על ידי מדיניות ספק אמצעי ההזדהות. ככל שהרב"א גבוהה יותר, פרק הזמן הנדרש עד לביטול הוא בדרך כלל קצר יותר.
- 7.4 במקרה של אמצעי הזדהות מסוימים, כגון - תעודות דיגיטליות שנשמרות על גבי כרטיסים חכמים, או התקני חומרה אחרים, ניתן לעיתים להשמיד פיזית את הכרטיס החכם או את ההתקן התקול. מאידך, המידע הקשור לאמצעי ההזדהות, אינו ניתן בהכרח להשמדה.

8. **חידוש והחלפה**

- 8.1 "חידוש" הוא תהליך שבו משך תוקפו של אמצעי ההזדהות, מוארך מעבר לתקופה הראשונה שלגביה הונפק.
- 8.2 "החלפה" הוא תהליך שבו מונפק אמצעי הזדהות חדש עבור הישות במקום אמצעי הזדהות שהונפק בעבר ובוטל.
- 8.3 דוגמה להחלפה: ספק אמצעי הזדהות שולח סיסמה זמנית לכתובת הדוא"ל של הישות, המאפשרת ליצור סיסמה חדשה לאחר מסירת הסיסמה הזמנית, אשר תחליף את הסיסמה הקודמת שהייתה לו.
- 8.4 דוגמא נוספת: שימוש ב"סיסמת קוד שחרור" של כרטיס חכם⁶⁵, במקרה שהכרטיס ננעל לאחר שימוש בסיסמה לא נכונה לאחר מספר ניסיונות שהוגדרה, ובעקבות זאת - חידוש האפשרות לשימוש בכרטיס החכם.
- 8.5 רמת הקושי של תהליכי חידוש או החלפה, משתנה בהתאם לרב"א.

9. **ניהול רשומות**

- 9.1 הרשומות המשמשות את תהליך הנפקת אמצעי ההזדהות, יישמרו לאורך כל מחזור החיים שלו, ובכל שלב בתהליך, היכן שהדבר ישים.
- 9.2 הרשומות יתעדו את המידע הבא, לכל הפחות, והיכן שהדבר ישים :
- 9.2.1 עצם העובדה שנוצר אמצעי הזדהות ;
- 9.2.2 מספר מזהה חד-ערכי של אמצעי ההזדהות. לדוגמה – מספר תעודה דיגיטלית ;
- 9.2.3 הישות שעבורה הונפק אמצעי ההזדהות ;
- 9.2.4 מצב (סטטוס) אמצעי ההזדהות.
- 9.3 בעת הנפקת אמצעי הזדהות לאנשים, ניהול הרשומות עשוי להיות כרוך בעיבוד של מידע אישי רגיש (PII).

⁶⁵ PUK – PIN Unlock Key. לאור תפקידו, לפיכך יש להתייחס ל- PUK כאל PIN לכל דבר.

נספח ב' - ניתוח איומים ובקורות עבור שלב הנפקת אמצעי ההזדהות וניהולם

1. רקע

- 1.1 סעיף זה מגדיר "קווים מנחים" לבקורות הנדרשות להתמודדות עם האיומים המזוהים בשלב הנפקת אמצעי ההזדהות כחלק מתהליך האימות הכולל, על מנת לצמצם⁶⁶ סיכונים אלו.
- 1.2 בסעיף 2 מוגדרים האיומים המיוחסים לשלב הנפקת אמצעי ההזדהות.
- 1.3 בסעיף 3.1 מוצגת טבלה אשר מרכזת את הבקורות הנדרשות לכל רב"א. עבור האיום המוגדר בעמודה הראשונה, מוגדרות בעמודה השנייה סוגי הבקורות הרלבנטיות. בהמשך, בארבע העמודות השמאליות, מופיעים מספרים המשקפים את אופן מימוש הבקרה לכל רב"א, כאשר לעיתים דרישה מסוימת אחידה לכל הרב"א, ומאידך – בבקורות אחרות ישנה התייחסות לכל רב"א בנפרד.
- 1.4 בסעיף 3.2 מוצג פירוט של כל בקרה, בהתאם למספר הבקרה.

2. האיומים

שלב משנה ⁶⁷	האיום	דוגמאות
יצירה	שיבוש ⁶⁸	תוקף משנה את המידע המועבר מתהליך ההרשמה לתהליך יצירת אמצעי ההזדהות.
	יצירה בלתי מורשית	תוקף גורם ל"ספק" המנפיק את אמצעי ההזדהות (CSP ⁶⁹) ליצור אמצעי הזדהות המבוסס על ישות שאינה קיימת בפועל.
הנפקה	חשיפה וגילוי ⁷⁰	אמצעי הזדהות שנוצר על ידי CSP עבור ישות מסוימת, מועתק על ידי תוקף כאשר הוא מועבר לישות בעת ההנפקה.
הפעלה	החזקה בלתי מורשית	התוקף משיג אמצעי הזדהות שאינו שייך לו, ועל ידי התחזות לישות האמיתית, גורם ל- CSP להפעיל את אמצעי ההזדהות.
	אי-זמינות	1. הישות הקשורה עם אמצעי ההזדהות, אינה נמצאת במיקומה הרגיל ואינה יכולה לאמת את זהותה ל- CSP. 2. משלוח אמצעי ההזדהות מעוכב, וההפעלה בתוך פרק הזמן שנקבע מראש, אינה אפשרית.
אחסון	חשיפה וגילוי	אמצעי ההזדהות המאוחסן במערכת קבצים כלשהי, נחשפים. לדוגמה, רשומת שם משתמש וסיסמה נחשפים לגישה לתוקף.
	שיבוש	הקובץ שממפה את הסיסמאות לאמצעי ההזדהות, נתקף ומשובש, כך שהמיפוי משתנה, ואמצעי הזדהות קיימים מוחלפים על ידי אמצעי הזדהות שלתוקף יש גישה אליהם.
	שכפול	התוקף משתמש במידע שנאגר במערכת על מנת לשכפל את אמצעי ההזדהות (לדוגמה – על ידי שכפול כרטיס חכם שמחולל את אמצעי ההזדהות), ואשר ניתן לעשות בו שימוש על ידי ישות בלתי מורשית.
	חשיפה וגילוי על ידי המשתמש	הישות מחזיקה העתק כתוב של שם המשתמש והסיסמה במקום שיכול להיות נגיש על ידי אחרים.
ביטול	עיכוב הביטול	הפצת המידע על אמצעי הזדהות מבוטלים אינו נעשה במועד שנקבע, באופן שמוביל לאיום על הישויות אשר אמצעי ההזדהות שלהם היו אמורים להיות מבוטלים – אך הם עדיין מאומתים כתקפים – עד שרשימת הביטולים העדכנית תתפרסם.

⁶⁶ לצמצום סיכונים במובן של mitigation

⁶⁷ בהתאם להגדרות שלבי המשנה בסעיף 1 בנספח א'

⁶⁸ tampering

⁶⁹ Credential Service Providers – CSP

⁷⁰ disclosure



שלב משנה ⁶⁷	האיום	דוגמאות
	שימוש לאחר סיום סיבת ההנפקה/ עזיבה/ פרישה ⁷¹	חשבונות משתמש אינם מבוטלים במועד כאשר עובד עוזב את החברה, ובכך עלול לגרום לשימוש לרעה אפשרי בחשבונות ישנים על ידי אנשים בלתי מורשים.
חידוש	חשיפה וגילוי	אמצעי הזדהות אשר מחודש על ידי CSP עבור ישות מסוימת, מועתק כאשר הוא מועבר לישות.
	שיבוש	אמצעי הזדהות חדש שנוצר על ידי ישות, משתנה ⁷² על ידי תוקף כאשר הוא נמסר ל- CSP לצורך החלפת אמצעי ההזדהות שפג תוקפו.
	חידוש בלתי מוסמך	התוקף מצליח לנצל לרעה פרוטוקול חידוש אמצעי הזדהות על מנת להאריך את תקופת התוקף של אמצעי ההזדהות עבור ישות קיימת. התוקף מצליח להונות את ה- CSP ולגרום לו להנפיק אמצעי הזדהות לישות קיימת, ואמצעי הזדהות חדש זה מוצמד לאמצעי הזדהות אשר מסופק על ידי התוקף.
ניהול רשומות	התכחשות	ישות טוענת שאמצעי הזדהות שנופק באופן תקין, הינו מזויף, או כולל מידע לא נכון, וזאת במטרה להכחיש במרמה שנעשה שימוש באמצעי ההזדהות על ידי הישות.

3. הבקורות הנדרשות ביחס לאיום בכל רב"א

3.1 טבלת בקורות בהתאמה לכל רב"א

בקורות נדרשות לכל רב"א				סוגי הבקורות	האיום
רב"א 4	רב"א 3	רב"א 2	רב"א 1		
2#	2#	1#	1#	יצירה תקינה	יצירה – שיבוש
3#	-	-	-	חומרה בלבד	
4#	-	-	-	נעילת מצב ⁷³	
5#	5#	5#	5#	מעקב אינוונטר	יצירה בלתי מורשית
8#	7#	7#	6#	הנפקה תקינה	הנפקה - חשיפה וגילוי
11#	10#	9#	9#	הפעלה על ידי הישות	הפעלה - החזקה בלתי מורשית
					הפעלה – אי זמינות
15#	14#	13#	12#	איחסון בטוח	אחסון - חשיפה וגילוי
					אחסון - שיבוש
					אחסון - שכפול
					אחסון - חשיפה וגילוי על ידי המשתמש
16#	16#	16#	16#	תהליך ביטול בטוח והשמדה	ביטול - עיכוב הביטול
					ביטול - שימוש לאחר סיום סיבת ההנפקה/ עזיבה/ פרישה

⁷¹ decommissioning

⁷² modified

⁷³ State-Locked



האיוס				סוגי הבקורות	בקורות נדרשות לכל רב"א			
					רב"א 1	רב"א 2	רב"א 3	רב"א 4
חידוש - חשיפה וגילוי חידוש - שיבוש חידוש - חידוש בלתי מוסמך				חידוש בטוח	17#	17#	18#	19#
ניהול רשומות - התכחשות				שימור נתונים ורשומות ⁷⁴	20#	20#	21#	21#



סוג בקרה	מס' בקרה	תיאור הבקרה
	11#	יתקיים הליך שיבטיח שאמצעי ההזדהות יופעל רק אם הוא יהיה תחת שליטת הישות המיועדת. הליך זה: - יספק הוכחה שהישות צמודה, או קשורה, להפעלת אמצעי ההזדהות (לדוגמה – על ידי פרוטוקול אתגר-תגובה); - יאפשר הפעלה רק במשך פרק זמן מסוים שיוגדר בהתאם לעניין.
איחסון בטוח	12#	- אמצעי הזדהות אשר מבוססים על "סודות משותפים"⁷⁷ יהיו מוגנים על ידי בקרות גישה אשר יגבילו את הגישה אליהם רק למנהלי מערכת וליישומים שנזקקים לגישה זאת; ובנוסף- - מדיניות ההגנה על אמצעי ההזדהות תתועד בתיעוד שיקושר לשימוש באמצעי הזדהות אלו, ושתהיה זמינה לישויות הרלבנטיות.
	13#	- כל הבקרות של 12#; ובנוסף- - קבצים מסוג זה המכילים "סודות משותפים", לא יכללו את הסודות המשותפים או את הסיסמאות בטקסט פתוח⁷⁸; שיטה שונה עשויה להיות בשימוש כדי להגן על הסודות המשותפים.
	14#	- כל הבקרות של 13#; וגם – - אמצעי הזדהות אשר מבוססים על "סודות משותפים" יהיו מוגנים על ידי בקרות גישה אשר יגבילו את הגישה אליהם רק למנהלי מערכת וליישומים שנזקקים לגישה זאת. סודות משותפים כאלו יהיו מוצפנים. מפתח ההצפנה עבור הסוד המשותף יהיה מוצפן בעצמו ויישמר במודול קריפטוגרפי (במודול חומרה או במודול תוכנה). מפתח ההצפנה עבור הסוד המשותף, יפוענח רק כאשר יידרש באופן מיידי לפעולת אימות מקוון; וגם – - ישויות או מיופי כוח מוסמכים של הישויות, יידרשו לאשר שהם מבינים את הדרישות הללו ומסכימים להגן על אמצעי ההזדהות שלהם בהתאם לדרישות אלו.
	15#	- כל הבקרות של 14#; וגם – - הישויות או מיופי כוח מוסמכים של הישויות, יידרשו לחתום על מסמך המאשר שהם מבינים את הדרישות לאיחסון אמצעי ההזדהות, ומסכימים להגן על אמצעי ההזדהות בהתאם.
תהליך ביטול בטוח והשמדה	16#	ה-CSP יבטל, ואם אפשרי – גם ישמידו – אמצעי הזדהות (כולל כאלו שמבוססים על סודות משותפים), בתוך פרק זמן מוגדר לכל רב"א, כמוגדר במסמך המדיניות הארגוני.
חידוש בטוח	17#	- ה-CSP יבסס מדיניות מתאימה עבור הליך החידוש וההחלפה של אמצעי הזדהות. - הוכחת החזקה⁷⁹ באמצעי ההזדהות הנוכחי שטרם פג תוקפו יוצג על ידי הישות טרם שה-CSP יאפשר חידוש ו/או החלפה; וגם – - הסיסמאות יעמדו בדרישות המזעריות לפי מדיניות ה-CSP לגבי חוזק הסיסמאות, ושימוש חוזר בסיסמאות; וגם – - לאחר שפג תוקפו של אמצעי ההזדהות הנוכחי, לא יתאפשר חידושו; וגם – - כל התקשורת והאינטראקציה בין הישות ולבין ה-CSP, יתבצעו על גבי ערוץ מאובטח, כגון SSL/TLS.

Shared Secrets ⁷⁷

Plain text ⁷⁸

Proof of Possession ⁷⁹



סוג בקרה	מס' בקרה	תיאור הבקרה
	18#	- כל הבקורות של #17 ; וגם – - תבוצע בדיקת הוכחת זיהוי⁸⁰ ברב"א 2 ובהתאם לבקורות של פעולה זאת⁸¹.
	19#	- כל הבקורות של #17 ; וגם – - תבוצע בדיקת הוכחת זיהוי ברב"א 3 ובהתאם לבקורות של פעולה זאת⁸².
שימור נתונים ורשומות	20#	יבוצע תיעוד מסודר של תהליך הרישום, ההיסטוריה והסטטוס של כל אמצעי הזדהות (כולל ביטול), והוא יתוחזק על ידי ה-CSP. משך זמן שימור הנתונים ייקבע על פי מדיניות ה-CSP.
	21#	- כל הבקורות של #20 ; וגם – - יפותחו הליכים מתועדים ורשמיים, לגבי "Chain of Custody" עבור כל רשומה.

⁸⁰ Identity Proofing

⁸¹ ר' תוצר ב' - "קווים מנחים לשלב ההרשמה", בסעיף המתייחס לבקורות אלו.

⁸² ר' תוצר ב' - מסמך "קווים מנחים לשלב ההרשמה", בסעיף המתייחס לבקורות אלו.

נספח ג' - ניתוח איומים ובקורות עבור שלב האיומים המקוון

1. רקע

- 1.1 סעיף זה מתייחס לבקורות שיש להשתמש בהן על מנת להתמודד עם האיומים המזוהים בשלב האיומים המקוון. הכוונה הן לאיומים הקשורים בשימוש באמצעי ההזדהות בתהליך האיומים המקוון, והן לאיומים כלליים הקשורים לתהליך זה.
- 1.2 האיומים הכלליים לאיומים מקוון כוללים, אך אינם מוגבלים רק, לתוכנות זדוניות (כגון – וירוסים, סוסים טרויאנים, רושמי הקשות מקלדת⁸³); אמצעי הנדסה חברתית (כגון – "גלישת כתפיים"⁸⁴; גניבת התקני חומרה וגניבת סיסמאות אישיות – PINS); שגיאות משתמש (כגון – סיסמאות חלשות; אי שמירה מספקת על מידע המשמש לאיומים); הכחשה שגויה; יירוט ו/או שינוי מידע בלתי מורשים של מידע המשמש לאיומים תוך כדי שידור; מניעת שירות⁸⁵; וחולשה בהליכי העבודה.
- 1.3 **למעט השימוש באיומים רב-גורמים⁸⁶, כל הבקורות הנוגעות לאיומים כלליים על תהליך האיומים, אינם חלק מהתקן וממסמכי המדיניות.** הטיפול בהם ייעשה במסגרת בחינת היבטי אבטחת מידע והגנה כנגד איומי סייבר בהתאם לתוה"ג, ולא דווקא בהקשר לאמצעי ההזדהות.
- 1.4 סעיף זה יתמקד באיומים הקשורים לשימוש באמצעי הזדהות לאיומים מקוון.
- 1.5 למעט הדרישה לשימוש באיומים רב-גורמים, עבור רב"א 3 ורב"א 4, לא יוגדרו הבקורות במונחי רב"א, עבור שלב האיומים המקוון. בפרט, יש בקורות שאינן מתאימות לכל ההקשרים שבהם מופעל תהליך האיומים המקוון. לכן, ההמלצה עבור התנהלות מיטבית⁸⁷ היא, שכלל שהסיכונים וההשלכות משמעותיים יותר, יש לשקול את שיקולי האבטחה לעומקם, בהתאם לרב"א ולסביבה התפעולית. קביעת הבקורות בסביבות השונות, הינה באחריות מתכנן המערכת והגורם שמפעיל אותה.
- 1.6 ישנם סיכונים רבים לאמצעי ההזדהות במהלך האיומים, כמפורט בסעיף 10 בתקן. הפירוט להלן יתייחס רק לבקורות הרלבנטיות לאבחנה בין רב"א שונות.
- 1.7 בסעיף 2 מוגדרים האיומים הכלליים לשלב האיומים המקוון בהזדהות.
- 1.8 בסעיף 3.1 מוצגת טבלה אשר מרכזת את הבקורות הנדרשות לכל רב"א. עבור האיום המוגדר בעמודה הראשונה, מוגדרות בעמודה השניה סוגי הבקורות הרלבנטיות. בהמשך, בארבע העמודות השמאליות, מופיעים מספרים המשקפים את אופן מימוש הבקרה לכל רב"א, כאשר לעיתים דרישה מסוימת אחידה לכל הרב"א, ומאידך – בבקורות אחרות ישנה התייחסות לכל רב"א בנפרד.
- 1.9 בסעיף 3.2 מוצג פירוט של כל בקרה, בהתאם למספר הבקרה.

2. האיום

האיום	דוגמאות
איומים כלליים	איומים כלליים לשלב האיומים המקוון כוללים קטגוריות רבות, המשותפות לכל סוגי מערכות התקשוב. הדוגמאות כוללות "רושמי הקשות מקלדת"; אמצעי הנדסה חברתית; ושגיאות משתמש. למעט השימוש באיומים רב-גורמים⁸⁸, כל הבקורות הנוגעות לאיומים כלליים על תהליך האיומים, אינם חלק מהתקן וממסמכי המדיניות. כמו כן, יש לשים לב שאיומים רב-גורמים בפני עצמו, אינו מגן כנגד כל סוגי האיומים.

Key stroke logger⁸³
Shoulder surfing⁸⁴
Denial of service⁸⁵
Multi-factor authentication⁸⁶
Best Practice⁸⁷
Multi-factor authentication⁸⁸

האיום	דוגמאות
"ניחוש" מקוון	תוקף מבצע ניסיונות כניסה חוזרים ונשנים על ידי ניחוש ערכים אפשריים של האישורים.
"ניחוש" לא מקוון	"סודות" הקשורים לייצירת האישורים ניתנים לחשיפה באמצעות שיטות אנליטיות בנפרד מתהליך אימות האישורים. פיצוח סיסמאות, מסתמך לרוב על תקיפת "מעבר שיטתי על כל הסיסמאות האפשריות", כגון שימוש ב- "מתקפות מילון". ב-"התקפות מילון", התוקף משתמש בכלים ייעודיים כדי "לחשב" את כל המילים במילון (או מילונים מרובים בשפות שונות), מחשב את ערך ה- "ערבול" (גיבוב) עבור כל מילה ובודק את ערך ה- "ערבול" המתקבל מול מסד הנתונים. שימוש בטבלאות "מעורבלות" (מגובבות), הינה שיטת תקיפה (פיצוח סיסמא) נוספת. טבלאות "מעורבלות" הם טבלאות מחושבות מראש של צמדי ערכים טקסט רגיל / מגובב. תקיפה בשיטת טבלאות "מעורבלות" מהירה יותר מתקיפת "מעבר שיטתי על כל הסיסמאות האפשריות", מכיוון שהם משתמשים בפונקציות ייעודיות לצמצום זמן החיפוש. תוקף יכול לעשות שימוש חוזר בתקיפה מסוג טבלאות "מעורבלות" לאחר יצירתן.
שכפול אישורים	ישות האישורים, או האמצעים ליצירת האישורים, הועתקו באופן לא לגיטימי. דוגמא לכך היא העתקה בלתי מורשית של מפתח פרטי.
"דיוג"	ניסיון לגניבת מידע רגיש (שם משתמש, סיסמא וכו') ברשת האינטרנט. דוגמה לכך הפנייה בעורמה של משתמש תמים להיכנס לאתר "מזויף" (אתר הונאה) וחשיפת פרטי משתמש רגישים, כתוצאה מהקלדת הפרטים על-ידי המשתמש התמים באתר ה-"מזויף".
ציתות	תוקף מאזין (לקו התקשורת) לתהליך האימות באופן פסיבי, במטרה להשיג את המידע הנדרש לביצוע האימות, כדי לבצע התחזות בשלב מאוחר יותר.
אימות מתחזה	תוקף מבצע אימות (מתחזה) באמצעות מידע שהושג בשלב קודם למול נותן השירות (גורם נסמך).
"חטיפת" תקשורת	תוקף "משלב" את עצמו בתהליך האימות בין המשתמש (יישות) לבין הגורם המאמת ומשיג את פרטי האימות הנדרשים. התוקף מסוגל להתחזות מצד אחד ליישות ומצד שני לנותן השירות (גורם נסמך) ולשלוט במידע העובר בין שני הצדדים. דוגמה לכך היא כאשר תוקף עושה שימוש בפרטי אימות מאושרים, על-ידי ציתות או חיזוי הערך של פרטי האימות המשמשים לסימון בקשות שנשלחו על ידי הישות כחוקיות.
תקיפת באמצע (MITM) "האיש"	התוקף "משלב" את עצמו בין הישות לבין נותן השירות (גורם נסמך), המאפשר לו ל-"יירט" ולשנות את התוכן הודעות פרוטוקול האימות. בדרך כלל, התוקף מתחזה כלפי הישות כנותן השירות (גורם נסמך) ובמקביל מתחזה כלפי הגורם המאמת כיישות. התהליך הנ"ל המתבצע במקביל עם שני הצדדים, מאפשר לתוקף לעשות שימוש בפרטי האימות שנשלחו בין שני הצדדים.
גניבת אישורים	התוקף מצליח לשים את ידו על מכשיר המייצר או מכיל אישורים.
זיוף והתחזות	התוקף מתחזה ליישות אחרת באמצעות פעולות זיוף והתחזות, במטרה לבצע פעולות שאין לו אישורים לבצע (למשל, קבלת גישה לנכס). הנ"ל ניתן לביצוע באמצעות שימוש באישורים של הישות או להתחזות ליישות (למשל, זיוף אישורים). דוגמאות לכך הן כאשר תוקף המתחזה ליישות מזויף מאפיין ביומטרי אחד או יותר על ידי יצירת אצבע "גומי" התואמת את הנתונים הביומטריים של הישות; תוקף מזויף כתובת MAC (כתובת MAC היא מספר מזהה עבור התקני תקשורת והשימוש המוכר ביותר נעשה בכרטיסי רשת. כתובת MAC היא כתובת פיזית. כתובת MAC זהה בשימושה לתעודת זהות עבור בני אדם) בכך שהמכשיר שלו משדר כתובת MAC השייכת למכשיר אחר שיש לו הרשאות ברשת מסוימת; או שתוקף מתחזה כמפרסם תוכנה לגיטימי האחראי על הורדת יישומי תוכנה מקוונת ו / או עדכונים.



בקורות נדרשות לכל רב"א					סוגי הבקורות	האיום
רב"א 4	רב"א 3	רב"א 2	רב"א 1	רב"א *		
1#	1#	-	-		אימות רב-גורמים	כללי**
-	-	-	-	2#	סיסמא חזקה	"ניחוש" מקוון
-	-	-	-	3#	בקרת אישורים	
-	-	-	-	4#	שימוש "בחשבון" ברירת מחדל	
-	-	-	-	5#	ביקורת וניתוח	
-	-	-	-	6#	שימוש בסיסמא מגובבת בתוספת מידע מוכמן ("salt")	"ניחוש" לא מקוון
-	-	-	-	7#	שימוש באמצעים נגד זיוף	שכפול אישורים
-	-	-	-	8#	שימוש באמצעים לזיהוי "דיוג"	"דיוג"
-	-	-	-	9#	אימוץ שיטות נגד "דיוג"	
-	-	-	-	10#	ביצוע אימות הדדי	
-	-	-	-	11#	המנעות משליחת סיסמא בתקשורת	ציתות
-	-	-	-	12#	שימוש באימות מוצפן	
-	-	-	-	13#	שימוש בפרמטר אימות שונה בכל אימות (OTP)	
-	-	-	-	13#	שימוש בפרמטר אימות שונה בכל אימות (OTP)	אימות מתחזה
-	-	-	-	14#	שימוש ב-"חתימת זמן"	
-	-	-	-	15#	שימוש באבטחה פיזית	
-	-	-	-	16#	הצפנת התקשורת	"חטיפת" תקשורת
-	-	-	-	17#	עדכון "טלאי" אבטחה בפרוטוקולים	
-	-	-	-	18#	ביצוע "תיאום תקשורת" מוצפן	
-	-	-	-	10#	ביצוע אימות הדדי	תקיפת "האיש באמצע" (MITM)
-	-	-	-	16#	הצפנת התקשורת	
-	-	-	-	19#	שפעול של האישורים	גניבת אישורים
-	-	-	-	20#	שימוש בחתימה אלקטרונית	זיוף והתחזות
-	-	-	-	21#	בדיקת "חיות"	
					יישום בקורות אלו, יבוצע בהמשך לביצוע סקר סיכונים.	
					לא ניתן למנוע את כל האיומים הכלליים רק באמצעות שימוש באימות רב-גורמי.	

⁸⁹ המזהים המצויינים בטבלה 3.1, תואמים את הבקורות הייעודיות הנדרשות לטובת מתן ההגנה הנדרשת לכל אחד מ-הרב"א. תיאור הבקורות בטבלה 3.2 להלן



סוג בקרה	מס' בקרה	תיאור הבקרה
אימות רב-גורמים	1#	ייעשה שימוש באמצעי הזדהות, אשר מיישמים לפחות שני גורמי אימות שונים (לדוגמה, "משהו שיש לך" משולב עם "משהו שאתה יודע", או "משהו שיש לך" משולב עם "משהו שאתה").
סיסמא חזקה	2#	יעשה שימוש בסיסמאות חזקות (לדוגמה, מחרוזות מורכבות שאינן מילים בעלות משמעות ומכילות אותיות "גדולות" אותיות "קטנות", ספרות ותווים מיוחדים).
בקרת אישורים	3#	יעשה שימוש במנגון "נעילה" או "הגבלה", לאחר מספר מסוים של ניסיונות כושלים להזדהות באמצעות סיסמא.
שימוש "בחשבון" ברירת מחדל	4#	לא יעשה שימוש בשמות משתמשים וסיסמאות המוגדרים כברירת מחדל (למשל, הגדרות יצרן).
ביקורת וניתוח	5#	יבוצע ניתוח של נסיונות כניסה כושלים, במטרה לזהות דפוס של ניסיונות ניחוש סיסמא מקוונים.
שימוש בסיסמא מגובבת בתוספת מידע מוכמן ("salt")	6#	יעשה שימוש בטבלאות גיבוב בשילוב עם מידע מוכמן ("salt") במטרה למנוע תקיפות "מעבר שיטתי על כל הסיסמאות האפשריות" ותקיפות טבלאות "מעורבלות".
שימוש באמצעים נגד זיוף	7#	יעשה שימוש באמצעים נגד זיוף (לדוגמה, הולוגרמות, מיקרופרינט וכו') במכשירים בהם מאוחסנים אישורים.
שימוש באמצעים לזיהוי "דיוג"	8#	יעשה שימוש בבקורות ייעודיות לזיהוי תקיפות "דיוג" (לדוגמה, פילטרים של שיטות סטטיסטיות המבוססות על תאוריית באייס, כתובות IP חשודות, פילטרים מבוססי כתובות אתרים חשודים, היוריסטיקה ו- "טביעות אצבע" של תקיפות מוכרות).
אימוץ שיטות נגד "דיוג"	9#	יעשה שימוש ביכולות כגון: "השבתת" יכולת להסתעף לתמונות, "השבתת" קישורים ממקורות לא מהימנים ושילוב סימנים "חזותיים" במיילים, במטרה להגן על משתמשי הקצה בפני התקפות "דיוג".
ביצוע אימות הדדי	10#	יעשה שימוש באימות הדדי (אימות בו זמנית על-ידי שני הצדדים).
המנעות משליחת סיסמא בתקשורת	11#	יעשה שימוש במנגנוני אימות שאינם מעבירים סיסמאות ברשת (למשל, פרוטוקול קרברוס - Kerberos).
שימוש באימות מוצפן	12#	במקרים בהם נדרש לבצע העברת פרטי אימות ברשת התקשורת, נדרש להצפין את נתוני האימות טרם ביצוע פעולת האימות.
שימוש בפרמטר אימות שונה בכל אימות (OTP)	13#	יעשה שימוש בפרמטרי אימות שונים בכל פעולת אימות (לדוגמה, סיסמא חד פעמית, סיסמא, אישורי "שיחה בתקשורת" וכו').
שימוש ב-"חתימת זמן"	14#	יעשה שימוש ביכולת "חתימת זמן" ללא יכולת שינוי לכל הודעה בתקשורת.
שימוש באבטחה פיזית	15#	יעשה שימוש באמצעי אבטחה פיזית (לדוגמה, ראיות לפגיעה/חבלה פיזית, לאבטחה גופניים (כלומר, ראיות לחבלה, אמצעי גילוי, אמצעי תגובה וכו').
הצפנת התקשורת	16#	יעשה שימוש בהצפנת "שיחות בתקשורת".
עדכון "טלאי" אבטחה בפרוטוקולים	17#	יבוצע עדכון שוטף של "טלאי" אבטחה, לטובת תיקון פגיעויות בפרוטוקולים (לדוגמה, פרוטוקול TCP / IP).
ביצוע "תיאום תקשורת" מוצפן	18#	יעשה שימוש במנגנוני "תיאום תקשורת" הדדי המבוססים על קריפטוגרפיה (לדוגמה, פרוטוקולי SSL / TLS).
שפעול של האישורים	19#	נדרשת יכולת לשפעול עתידי של האישורים (לדוגמה, הכנסת PIC CODE או נתון ביומטרי לאמצעי החומרה המכיל את האישורים).
שימוש בחתימה אלקטרונית	20#	יעשה שימוש ביכולות "חתימה דיגיטלית", בכדי לאמת למול מקורות מהימנים ולאפשר "הורדה" רק של אפליקציות/יישומים מאושרים בלבד, במטרה להימנע מ-"הורדת" אפליקציות/יישומים שנוצרו/עודכנו על-ידי גורמים לא מורשים.
בדיקת "חיות"	21#	יעשה שימוש במנגנוני "גילוי חיות", כדי לזהות את השימוש במאפיינים ביומטריים מלאכותיים (למשל, תמונות של אדם, טביעות אצבעות מזויפות וכו').

**** סוף מסמך ****

עמוד 25 מתוך 25