

המדיניות הלאומית להזדהות בטוחה

קווים מנחים – כרך כללי

2025

טבלת ניהול מהדורות

מהדורה	תאריך	סטטוס	פרק/סעיף	תקציר השינוי
1.2	6.8.15	הפצה	כל המסמך	מהדורה שהופצה לצורך היוועצות
1.3	25.1.16	טיוטה	כל המסמך	עדכון בעקבות תהליך ההיוועצות
1.3	6.3.16	טיוטה	כל המסמך	עדכון פנימי
1.4	7.3.16	טיוטה	כל המסמך	עדכון פנימי להגשה לממונה
1.5	31.3.16	טיוטה	כל המסמך	עדכון לאחר הערות הממונה והכנת תקציר מעודכן
1.6	8.4.16	טיוטה	תקציר המנהלים	קבלת סימני שינוי בתקציר ועדכון מספר הערות
1.7	16.4.16	טיוטה	כל המסמך	עדכון המסמך לקראת אישור הממונה
1.8	9.5.16	טיוטה	כל המסמך	עדכון לפי הערות הממונה לאישור
1.9	26.5.16	טיוטה	כל המסמך	עדכון לפי הערות הממונה בדיון ב-9.5.16
1.9.1	5.6.16	טיוטה	כל המסמך	הערות רועי פרידמן
1.9.2	5.6.16	טיוטה	כל המסמך	עדכון הערות רועי פרידמן
1.10	13.6.16	טיוטה	כל המסמך	עדכון הערות למהדורה 1.9.2
1.11	19.6.16	טיוטה	כל המסמך	עדכון הערות למהדורה 1.10
2.0	26.6.16	טיוטה להיוועצות	כל המסמך	עדכון הערות למהדורה 1.11
2.1	1.8.16	טיוטה לאחר היוועצות	כל המסמך	הטמעת הערות לאחר ההיוועצות עם הציבור
2.1.1	15.8.16	טיוטה	כל המסמך	הטמעת משוב צוות בינמשרדי
2.2	17.8.16	טיוטה	כל המסמך	הטמעת הערות צוות בינמשרדי
3.0	21.8.16	מהדורה לאישור	כל המסמך	הטמעת הערות עריכה
3.1	15.9.16	מהדורה סופית	כל המסמך	מהדורה סופית שאושרה בצוות הבין-משרדי
3.2	2025	מהדורה מעודכנת	כל המסמך	מהדורה סופית שאושרה לאחר היוועצות בין משרדית ועם הציבור

סיווג: בלמ"ס

תוכן עניינים

1. תקציר מנהלים	4
1.1. מבוא	4
1.2. המדיניות כארגז כלים	4
1.3. וקטורי איום ושיקולי אבטחה	4
1.4. דיווח ותאימות שנתי	5
1.5. דרישות לשימוש בביומטריה	5
1.6. שימוש במנגנונים בשליטת נותן השירות	5
1.7. הגבלת מספר ניסיונות גישה	5
1.8. בדיקות חוסן וחדירות	5
1.9. הזדהות פדרטיבית	5
2. מבוא	6
2.1. ייסוד המדיניות, תהליך עבודת הכתיבה ומקור הסמכות	6
2.2. בין זהות להזדהות	6
2.3. איזון בין דרישות אבטחה מחמירות לבין חוויית המשתמש	7
2.4. מתן שירות דיגיטלי (מקוון) - שלבים בהזדהות	7
2.5. הנגשת שירותים דיגיטליים על ידי גופים ציבוריים	8
3. מסמך המדיניות כארגז כלים לזהות דיגיטלית והזדהות דיגיטלית	10
4. סיכומי וקטור ההזדהות במרחב הדיגיטלי	10
5. וקטורי איום ושיקולי אבטחה	10
6. תהליך דיווח ותאימות שנתי	11
6.1. מטרות פעילות דיווח והכוונה	11
6.2. מקור סמכות	11
6.3. תהליך הדיווח	11
7. דרישות לשימוש בביומטריה	12
8. בדיקת מהימנות ותקפות מסמכי זיהוי	15
9. הגבלת מספר ניסיונות גישה	15
10. ביצוע בדיקות חוסן וחדירות במערכות הזדהות מקוונות	16
11. הזדהות פדרטיבית ומערכות הזדהות פדרטיביות בתהליכי הזדהות לשירותים ציבוריים וממשלתיים	17
11.1. מהי הזדהות פדרטיבית	17
11.2. תהליך פדרטיבי אופייני	18
11.3. דוגמא למערכת פדרטיבית בישראל	18
נספח 1 - עיקרי העדכונים במסמכי המדיניות והקווים המנחים	19
נספח 2 - עקרונות המדיניות להזדהות בטוחה	21
נספח 3 - טבלת סוגי איומים/ תקיפות עיקריים בתחום ההזדהות	23
נספח 4 - הזדהות פדרטיבית	26

1. תקציר מנהלים

1.1. מבוא

בעידן בו הזדהות דיגיטלית מהווה שער לשירותים חיוניים, מסמך זה של המדיניות הלאומית להזדהות בטוחה (להלן: "המדיניות") מהווה יסוד חשוב ליצירת בטחון ואמון הציבור. המדיניות גובשה בתהליך היועצות עם גופים מרכזיים בממשלה ובמגזר העסקי, בשיתוף יועצים מחו"ל ובקבלת הערות מהציבור. גרסה זו מעדכנת את גרסת המדיניות הקודמת בהתאם להתפתחויות טכנולוגיות, עדכוני תקינה בינלאומיים והשתנות וקטורי האיום (ר' נספח 1). החלטת ממשלה 2960¹ אישרה את המדיניות, שעקרונותיה מפורטים בנספח 2, וקבעה כי יש לפרסם "קווים מנחים" מכוח המדיניות ולעדכןם ככל שיידרש. מסמך המדיניות נשען על תקנים בין-לאומיים, ומותאם למציאות הישראלית תוך ראייה ארוכת טווח. המסמך משלב בין הנחיות טכניות, שיקולים של אבטחה ושירותיות.

1.2. המדיניות כארגז כלים

מסמך זה ותוצריו מהווים את "ארגז הכלים" ליישום הנגשת השירותים הדיגיטליים בהתאם לתקינה הבינלאומית. המדיניות כוללת שלושה תוצרים עיקריים העומדים בבסיס ההזדהות הדיגיטלית ומגדירים את הדרישות הטכניות עבור:

1. תוצר א' - סיווג רגישות השירות

התוצר נועד לספק כלי מעשי לספקי (נותני) השירותים המקוונים, לסיווג רגישות השירות לפי רמות הבטחת הוכחת הזהות. סיווג רגישות השירות מאפשר התאמת רמת ההזדהות לנוף הסיכון של השירות – לרבות קביעת רמת זהות (1 עד 4), הקצאת משאבים יעילה ושמירה על חוויית משתמש מיטבית.

2. תוצר ב' - תהליך הרשמה (רב"ה)

התוצר נועד להציג את הדרישות וההנחיות לביצוע שלב ההרשמה (רב"ה), בהתאם לסיווג רגישות השירות כפי שנמצא בתהליך ניהול סיכונים כמפורט בתוצר א'. התוצר מתאר תהליך המבוסס על הצגת "ראיות" מסמכי זיהוי (פיזיים/אלקטרוניים/דיגיטליים).

3. תוצר ג' - תהליך אימות (רב"א)

התוצר נועד להציג את הדרישות וההנחיות לביצוע שלב האימות (רב"א), בהתאם לסיווג רגישות השירות כפי שנמצא בתהליך ניהול סיכונים כמפורט בתוצר א' למדיניות - קווים מנחים לתהליך סיווג רגישות שירותים מקוונים. התוצר מדגיש את חשיבות השימוש בגורמי אימות מאובטחים (קריפטוגרפיים, זיהוי ביומטריה ושימוש בתהליך אימות רב גורמי).

1.3. וקטורי איום ושיקולי אבטחה

קיימות שלוש קטגוריות כלליות של איומים על תהליך הוכחת הזהות: התחזות, מצג שווא/הונאה ותשתית התחזות – כאשר תוקף מנסה להתחזות לזהות לגיטימית. מצג שווא/הונאה – יצירת זהות בדויה. תשתית – פגיעה בשלמות, זמינות או סודיות של התשתית או הנתונים. טבלת סוגי תקיפות ומנגנונים להפחתת

¹ https://www.gov.il/he/pages/2017_dec2960

איומים מפורטת **בנספח 3**. נספח זה מספק טבלה סדורה של איומים נפוצים (כגון: גניבת זהות, התחזות, זיוף ראיות) ואמצעים מתאימים להפחתת סיכון בהתאם למדיניות.

1.4. דיווח ותאימות שנת

בהתאם להחלטת הממשלה, נדרשים משרדי הממשלה לדווח ליחידה, בכל שנה, על תהליכי ההזדהות במתן שירותים דיגיטליים. מטרת הדיווח היא לבחון את תאימות הנגשת השירותים המקוונים הדורשים הזדהות, הניתנים על ידי המשרדים ויחידות הסמך למדיניות, ולספק בעת הצורך הנחיה לשיפור הישום.

1.5. דרישות לשימוש בביומטריה

ביומטריה הינה תהליך לזיהוי אוטומטי של בני אדם על סמך מאפיינים ביולוגיים ו/או התנהגותיים. יש לעשות שימוש זהיר בביומטריה ובהתאם לעקרונות המדיניות הלאומית. יש להשתמש במנגנון מבוקר, ובאופן שמבטיח כי הדגימה נלקחה ממבקש השירות עצמו. נדרשים ספי ביצועים לאימות ביומטרי (1:1): FMR של 1:10,000 או טוב יותר, FNMR של 1:100 או טוב יותר. יש להפעיל מנגנוני גילוי מצג שווא (PAD) בהתאם לדרישות התקן ISO/IEC 30107, וכן לפעול באופן מיטבי לגילוי הזרקה (Injection) וגילוי זיוף עמוק (Deep Fake).

1.6. שימוש במנגנונים בשליטת נותן השירות

בעל מערכת ההזדהות יפעל במטרה לעשות שימוש באמצעי הזיהוי ולוודא שליטה בפעולתם. עליו ליישם אמצעי בקרה ובדיקות עתיות על כל אמצעי זיהוי.

1.7. הגבלת מספר ניסיונות גישה

ספק השירות יפעל ליישום בקרות להגנה מפני תקיפות לניסיונות ניחוש. לדוגמה, הגבלות על ניסיונות התחברות כושלים (5 ניסיונות או 10 ניסיונות עם הטמעת מערכת למניעת מצג שווא) והשהיית זמן בין ניסיונות התחברות.

1.8. בדיקות חוסן וחזירות

בדיקות אלו חיוניות לאיתור חולשות לוגיות וטכניות. כל נותן שירות מחזיק/מתפעל מערכת הזדהות חייב בביצוע מבדקי חוסן אחת ל-18 חודשים, כולל תרחישים מותאמים, בהתאם להתפתחות המערכת או אירועים נקודתיים, והטמעת לקחים.

1.9. הזדהות פדרטיבית

הזדהות פדרטיבית היא מנגנון המאפשר למשתמשים לגשת לשירותים באמצעות ספק זהות אחד, ללא צורך ביצירת זהויות נפרדות. נדרשת עמידה בפרוטוקולים מאובטחים (למשל: SAML). הדוגמא המרכזית בישראל היא מערכת ההזדהות הלאומית המספקת אימות זהות ברמת סמך 3 או 4, בכפוף לסיווג השירות ובכפוף למדיניות זו. ככל שמערכת זו אינה מספקת את רמת הסמך הנדרשת לשירות, לא ניתן להשתמש בה. הארנק הדיגיטלי הלאומי, הנמצא בשלבי תכנון, מהווה אף הוא דוגמה למערכת פדרטיבית.

2. מבוא

2.1 ייסוד המדיניות, תהליך עבודת הכתיבה ומקור הסמכות

זיהוי אמין ובטוח הוא הבסיס למתן שירותים ציבוריים מקוונים "מרחוק". החלטת הממשלה מספר 2097 מיום 10.10.2014, הטילה על היחידה להזדהות ויישומים ביומטריים (להלן: "היחידה"), להוביל את התוויית מדיניות ההזדהות (להלן: "המדיניות") הנחוצה למימוש המיזם הלאומי "ישראל דיגיטלית" ויישומה של מדיניות זאת, תוך היועצות עם הגורמים הרלבנטיים בממשלה.

בהתאם, הוקם צוות בין-משרדי אשר עבודתו כללה בין היתר את לימוד המצב הקיים במדינות מובילות בהקשר זה. הצוות בחן תקנים בינלאומיים רלוונטיים המתפרסמים על ידי ארגוני התקינה הבינלאומיים ISO² ו-NIST³. כחלק מהכנת כתיבת המדיניות, בוצע הליך היועצות עם גופים מרכזיים בממשלה ובמגזר העסקי. כמו כן, מסמכי המדיניות נמסרו להערות יועצים בכירים מחו"ל בעלי ניסיון רב בנושא, והערותיהם שולבו בהם. טרם סיכום המדיניות והבאתה לאישור סופי, פורסמו מסמכי המדיניות לציבור הרחב, לצורך קבלת הערות, השגות והצעות. החלטת ממשלה 2960 אישרה את המדיניות, שעקרונותיה מפורטים בנספח 2, וקבעה כי יש לפרסם "קווים מנחים" מכוח המדיניות ולעדכןם ככל שיידרש.

עד כה הקווים המנחים למדיניות, לביצוע הרשמה ולאומיות במערכות הזדהות דיגיטליות התבססו בעיקר על תקן ISO29115. בעדכון המדיניות הנוכחי, לשנת 2025, בוצע הליך עדכון המתבסס בעיקרו על תקן ה-NIST SP800-63-4, לאור זאת שתקן ה-NIST מהווה תקן טכנולוגי, ומעודכן (לשנת 2025) למציאות בעולם "פוסט קורונה" לצד התאוצה הטכנולוגית והתרחבות השימוש בהזדהות דיגיטלית, בעוד שתקן ISO הנו משנת 2013, ומהווה תקן של רגולציה ומדיניות. נדגיש כי עדכון הקווים המנחים מותאם למציאות הישראלית.

המדיניות גובשה בראייה ארוכת טווח, תוך מתן מענה שיעניק תועלות מרביות למשק, ולפיכך מתייחסת לאוכלוסיות היעד להלן:

1. ממשלת ישראל, המאשרת את המדיניות.
2. הדרג הניהולי במשרדי הממשלה ובגופים רלבנטיים אחרים, האמורים ליישם את המדיניות הלכה למעשה.
3. היחידה במערך הסייבר הלאומי, כמסמך מנחה לפעילותה של היחידה.
4. הציבור הרחב, כמסמך המשקף את השיקולים המנחים את מדיניות ממשלת ישראל בהקשר להזדהות דיגיטלית בטוחה.

2.2 בין זהות, זיהוי והזדהות דיגיטלית

במדינת ישראל, בשונה ממרבית העולם, משרד הפנים מהווה עוגן אמון בתשתית הזיהוי – מרגע לידתו, באמצעות רשות האוכלוסין וההגירה, אשר מקצה לנו מספר זיהוי חד ערכי, והוא משמש מקור סמכותי ואמין לפרטי הזיהוי של אדם, שעל בסיסם נבנים מנגנוני אימות במרחב הדיגיטלי. כאשר בעת הגיענו לגיל

² ISO –for Standardization the International Organization ; IEC – The International Electrotechnical Commission - ISO29115

³ NIST -National Institute of Standards and Technology. SP800-63-4

16 או לחילופין כאשר אנו מבקשים ממשרד הפנים להעניק לנו "מסמך נסיעה" (דרכון), אנו נדרשים להגיע למשרדי רשות האוכלוסין וההגירה, על מנת שיטלו מאיתנו תמונת פנים וטביעות אצבע לצורך הפקת המסמכים הפיזיים, כאשר הם נשמרים, תוך אבטחה ובהתאם לחוק הכללת יישומים ביומטריים על ידי רשות המאגר הביומטרית. כך בעצם, נוצרת זהותנו במרחב.

כאשר אדם נרשם לשירות מקוון (ממשלתי, פיננסי או חברתי), הוא יוצר לעצמו זהות **דיגיטלית הקשרית**, שמטרתה לאפשר זיהוי והזדהות לצורך קבלת שירות, בהתאם לעקרונות של הזדהות פדרטיבית ומדיניות זהות דיגיטלית מאובטחת.

2.3 איזון בין דרישות אבטחה מחמירות לבין חוויית המשתמש

המדיניות מדגישה את החשיבות של איזון בין דרישות אבטחה מחמירות לבין חוויית המשתמש, ופועלת להבטיח כי תהליכי ההזדהות יהיו פשוטים וידידותיים ככל האפשר, תוך שמירה על פרטיות התושבים ויישום עקרונות של Privacy-by-Design ושל Security-by-Design.

למרות שטכנולוגיות זיהוי ביומטריות, כגון צילום פנים וטביעות אצבע, הינן טכנולוגיות איכותיות שמומלץ לעשות בהן שימוש, שילובן במערכות הזדהות יבוצע באופן מושכל וזהיר ותחת פיקוח ובקרה הדוקים, בהתחשב בפגיעותה של הטכנולוגיה למצגי שווא ולהונאות מתוחכמות וכן בהתחשב באופי הסטטיסטי הכרוך בשימוש בהשוואות ביומטריות. במקביל לשימוש בביומטריה מומלץ לעשות שימוש מושכל בטכנולוגיות קריפטוגרפית להצפנה ולחתימה על פירטי מידע בתהליכי הזדהות בטוחה. יש לעשות שימוש במנועי השוואה לזיהוי ביומטרי שעברו מבדק במעבדה מוסמכת, וקיבלו אישור לעמידה בדרישות בהתאם למדיניות.

לצד הדרישות המפורטות במסמכי המדיניות, מספקת המדיניות גמישות מסוימת, ומתירה חריגות ברורות ומנומקות, בכפוף לאישור מוקדם ובכתב של היחידה. מטרת הגמישות היא לאפשר מתן מענה למצבים חריגים, תוך בקרה, הנחיה והתאמת תהליכי ההזדהות לעקרונות וליעדי המדיניות.

שלושת מסמכי המדיניות (תוצרים א', ב', ג') משקפים תפיסה אחודה ורב-שכבתית שנועדה להבטיח כי כלל הגורמים במרחב הדיגיטלי (המקוון) בישראל – ציבוריים, עסקיים ואזרחיים – יוכלו להעניק ולצרוך שירותים דיגיטליים בביטחון מלא, תוך מתן מענה לסיכונים המתפתחים ומתן גמישות במענה לצרכים הייחודיים של השירותים השונים.

2.4 מתן שירות דיגיטלי (מקוון) - שלבים בהזדהות

מתן שירות דיגיטלי (מקוון) מחייב ביצוע שלושה שלבים עיקריים: סיווג רגישות השירות, הרשמה ואימות. סיווג רגישות השירות מהווה את שלב היסוד, ונעשה באמצעות תהליך ניתוח סיכונים, שמטרתו לקבוע את רמת הבטחת הזהות הנדרשת (רמות 1 עד 4), בהתאם לסוג השירות ולסיכונים הכרוכים בו. לאחר סיווג השירות, מתבצע שלב ההרשמה שנועד לבסס את הזהות הדיגיטלית של המשתמש. בשלב זה נאספות ראיות, פיזיות או דיגיטליות, בהתאם לרמת ההבטחה שנקבעה בתהליך הסיווג (רב"ה – רמת בטחון

בתהליך הרשמה). לאחר שלב ההרשמה ניתן לצרוך את השירות באופן שוטף, תוך ביצוע תהליך אימות בהתאם לרמת הסיווג ולרמת הבטחון הנדרשת (רב"א – רמת בטחון בתהליך אימות).

בהתאם להנחיית היחידה, ולצד קצב התפתחות הטכנולוגיה והאימונים הגוברים בתחום ההזדהות, רמת הביטחון הנדרשת להזדהות עבור שירותי ממשלה דיגיטליים, הן בהרשמה והן באימות לא תפחת **מרמה 3**. חריגה מהנחיה זו הנה אפשרית במקרים חריגים, בהם יפנה הנציג ליחידה **מראש ובכתב בבקשה לאישור ההחריגה**, ויצוין את הסיבה להנגשת השירות שלא בתאימות למדיניות, לתוצריה ו/או להנחיות, וכן יצוין תאריך יעד להשלמת ההתאמה למדיניות.

ככל שסבור נותן השירות הדיגיטלי, כי בהתאם לתהליך סיווג השירות נמצא כי השירות הדיגיטלי דורש רמת ביטחון גבוהה מאוד בזהות המשתמש (רמה 4), עליו לוודא כי **ההרשמה לשירות הדיגיטלי תתבצע באופן פיזי**, על ידי הגעה של המשתמש לחצרות נותן השירות, וזיהוי המשתמש באופן וודאי על ידי פקיד, או לחלופין זיהוי המשתמש בקיוסק מפוקח בחצרות נותן השירות, דהיינו קיוסק המוצב בחצרות נותן השירות והמפוקח באופן צמוד ורצוף על ידי נציג אנושי מוסמך של הגוף נותן השירות, באופן פיזי או בפיקוח רצוף באמצעות מצלמה. בנוסף, על מנגיש השירות הדיגיטלי לעמוד בהנחיות לאימות ברמה זהה (ראה תוצר ג' – קווים מנחים – ביצוע אימות לשירותים דיגיטליים מרחוק). חריגה מדרישה זו אפשרית, ואולם דורשת נימוקים ואת אישור היחידה מראש ובכתב.

שלבי ההרשמה והאימות יכולים להתבצע על ידי ספק הזדהות/שירות יחיד, או לחלופין באמצעות מערכות הזדהות פדרטיביות (לדוגמא, מערכת ההזדהות הלאומית). מערכות אלו מאפשרות ניהול מרכזי של השירותים המקוונים ומציעות חוויית משתמש נוחה ופשוטה, תוך שמירה על סטנדרטים גבוהים של אבטחת מידע ופרטיות.

תהליכי ההרשמה והאימות מתבססים על ראיות וגורמי אימות מגוונים, הכוללים בין היתר תיעוד ביומטרי, מסמכים מאובטחים המכילים מידע קריפטוגרפי ומאמתים רב-גורמים (MFA). התהליך כולל דרישות ברורות לאיסוף ואימות ראיות פיזיות, אלקטרוניות או דיגיטליות, הקפדה על אותנטיות ושלמות המידע, והנחיות מפורטות להפעלת מאמתים – כגון : סיסמאות מורכבות, קודים חד-פעמיים (OTP) ומפתחות קריפטוגרפים, בהתאם לרמת הבטחת הזהות שנקבעה.

חשוב להדגיש, בהינתן שנותן השירות ו/או בעל מערכת ההזדהות אינו עומד בעקרונות המפורטים לשימוש בגורמי הזיהוי, במסמך המדיניות ותוצריו, בתהליך ההרשמה והאימות, יפעיל ראש היחידה את סמכותו להתלות את אישור רמת הסמך שניתן לנותן השירות, וזאת עד לבירור וביצוע ההתאמות הנדרשות לעמידה בדרישות המדיניות ותוצריה.

2.5 הנגשת שירותים דיגיטליים על ידי גופים ציבוריים

חוק תקשורת דיגיטלית⁴, עוסק בחובת הנגשת שירותים נפוצים על ידי גופים ציבוריים שונים, באופן דיגיטלי. מטבע הדברים הנגשת שירותים באופן דיגיטלי כולל את הצורך ביישומים שיאפשרו הזדהות דיגיטלית, באופן אמין ובטוח.

⁴ https://www.nevo.co.il/law_html/law01/501_921.htm

החוק קובע כי קיימת חובת הנגשה דיגיטלית של שירותים נפוצים, אלא אם נקבע אחרת בדין (למשל ביחס להנפקת תעודת זהות ודרכונים) ואלא אם כן נקבע חריג בתוספת השביעית לחוק או נקבע חריג בהתאם לתהליך הנדרש בחוק הכולל ועדת חריגים בה חבר נציג המערך.

החוק קובע כי הנגשת השירות תעשה בהתאם להוראות הבאות (בנושאי הזדהות, הגנת סייבר ופרטיות):

1. לעניין שירות נפוץ אשר בשל אופיו מתחייבת הזדהות של מקבל השירות – מקבל השירות יזוהה באמצעי דיגיטלי שמאפשר הזדהות **ברמת ודאות התואמת את סוג השירות המבוקש ואת רגישותו**, בנסיבות העניין;

2. הגוף הציבורי ישקול שיקולים הנוגעים להגנה על פרטיותו של מקבל השירות, ובכלל זה שמירה על סודיות רפואית ואבטחת מידע;

3. העברת מידע בעל רגישות מיוחדת כהגדרתו בחוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד-2024, מאת מקבל השירות אל הגוף הציבורי, תתאפשר בדרך מאובטחת ובאופן שמתחשב בשיקולי הגנה על הפרטיות, והכול בהתאם למידת רגישות המידע בנסיבות העניין;

4. הגוף הציבורי ישקול שיקולי הגנת הסייבר לעניין תקיפות על המערכות והממשקים הנוגעים לשירות או תקיפות באמצעותם, וינקוט אמצעי הגנה לשם כך, לרבות אמצעים לזיהוי תקיפות סייבר ולהתמודדות עימן.

עוד קובע החוק כי גוף ציבורי המנוי בתוספת החמישית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, כלומר גוף המונחה על ידי מערך הסייבר הלאומי, בשל היותו גוף תמ"ק⁵, יגיש שירות נפוץ, בכפוף להנחיות קצין מוסמך⁶.

כמו כן, נקבע כי הוראות החוק אינן גורעות מדין אחר, ובאופן ספציפי הובהר כי הוראות הסעיף באות להוסיף על כל הוראה בעניין הגנת הסייבר או הזדהות בטוחה שנקבעה בהחלטת הממשלה או לפיה, ולא לגרוע מהן; ואולם, במקרה של סתירה, יגברו הוראות החוק.

⁵ תמ"ק- תשתית מדינה קריטית

⁶ גופים שאינם מוגדרים כתמ"ק יפעלו בכפוף להנחיות הרגולטור בתחום הגנת הסייבר ו/או המדיניות להזדהות בטוחה

3. מסמך המדיניות כארגז כלים לזהות דיגיטלית והזדהות דיגיטלית

הזהות הדיגיטלית (כפי שהוסבר בפרק 2.2) היא זו המאפשרת לנו להתנהל במרחב המקוון. מסמך זה ותוצריו⁷ מהווים את "ארגז הכלים" ליישום התהליך לביסוס זהות דיגיטלית, בכל אחת מהפלטפורמות הממשלתיות / ציבוריות – כאשר לכל אחת יש לנו זהות דיגיטלית נפרדת, או זהות דיגיטלית אחת מול שירותים ממשלתיים (מערכת ההזדהות הלאומית) ובכלל זאת מגדירים את הדרישות הטכניות עבור:

1. אופן סיווג רגישות השירות- תוצר א'.
2. הוכחת הזהות בתהליך ההרשמה- תוצר ב'.
3. הוכחת הזהות בתהליך האימות – תוצר ג'.
4. עקרונות לדרישות במערכות דיגיטליות פדרטיביות – [סעיף 11](#)

4. סיכוני וקטור ההזדהות במרחב הדיגיטלי

תהליך ההזדהות במרחב הדיגיטלי יכול להיות נקודת תורפה מרכזית במערכות הזדהות בכלל במשק ועבור מערכות הזדהות לשירותים ממשלתיים בפרט, ומהווה יעד מועדף לתוקפים. באמצעות התחזות למשתמשים לגיטימיים, תוקפים יכולים לחדור למערכות, לבצע פעולות זדוניות בשם גורמים מורשים ולנצל את הגישה שהושגה לצרכים שונים - החל מפגיעה במוניטין או באמינות הארגון, דרך גרימת נזק כלכלי לגוף הממשלתי או לאזרחים (משתמשי המערכת), ועד לחשיפת מידע רגיש ואף פגיעה ממשית בביטחון המדינה. התחזות זו, לעיתים בלתי ניתנת לזיהוי בזמן אמת, ממחישה את הצורך בהגנה הדוקה ומרובת שכבות על תהליך ההזדהות במערכות הדיגיטליות של הממשלה.

5. וקטורי איום ושיקולי אבטחה

הגנה יעילה על הזהות, במעבר לצריכת שירותים מקוונים מרחוק, מחייבת שימוש בשכבות אבטחה תוך שימוש בבקורות לתהליכים לאורך ביצוע האינטראקציה עם מבקש השירות. כדי להשיג זאת יש צורך בהבנה היכן וכיצד יכולים להיווצר איומים ופגיעה בתהליך ההרשמה והוכחת הזהות, אשר יובילו ליצירת זהות דיגיטלית בטוחה/ מאובטחת.

קיימות שלוש קטגוריות כלליות של איומים⁸ על תהליך הוכחת הזהות; התחזות, מצג שווא/ הונאה ותשתית. להלן הסבר;

התחזות: כאשר תוקף מנסה להתחזות לזהות "לגיטימית" קיימת בתהליך רישום לשירות דיגיטלי שיחשב (גניבת זהות) ולייצר זהות דיגיטלית "מתחזה" (ניתן לביצוע או בשלב ההרשמה לשירות, או בשלב האימות)

מצג שווא/ הונאה: כאשר תוקף מייצר "יש מאין" זהות בדויה (למשל, הונאת זהות סינתטית⁹).

תשתית: כאשר תוקף עשוי לפגוע/ לסכן את שלמות, זמינות או סודיות התשתית, הנתונים או האנשים התומכים בתהליך הוכחת הזהות במערכת של ספק השירות.

טבלת סוגי תקיפות ומנגנונים הקשורים לסיוע בהפחתת איומים, מפורטים [בנספח 3](#).

⁷ תוצר א'- סיווג שירותים, תוצר ב' - קווים מנחים להרשמה, ותוצר ג' - קווים מנחים לאימות.

⁸ טבלת סוגי איומים/ תקיפות מפורטות [בנספח 2](#).

⁹ יצירת זהות/ ישות של אדם שאינו קיים.

6. תהליך דיווח ותאימות שנתי

6.1. מטרות פעילות דיווח והכוונה

1. לשקף את פעילות משרדי הממשלה בהנגשת שירותים מקוונים הניתנים לתושב ובכלל זאת את היקף השירותים המקוונים וטיבם.
2. לשקף את עבודת היחידה במתן משוב ולהכווין את משרדי הממשלה למימוש הסטנדרט שנקבע להזדהות דיגיטלית בטוחה בעת מתן שירותים מקוונים, על פי רגישות השירות ובהתאם למדיניות.
3. לבחון את תאימות הנגשת השירותים למדיניות¹⁰.

6.2. מקור סמכות

בהתאם להחלטת הממשלה, נדרשים משרדי הממשלה לדווח ליחידה על תהליכי ההזדהות במתן שירותים דיגיטליים לתושבים. היחידה מרכזת את הדיווחים אחת לשנה, מנתחת אותם, מבצעת בקרה ומנחה את המשרדים באופן מקצועי לשם קידום התאמתם למדיניות, בשיתוף פעולה ובכפוף לדין.

6.3. תהליך הדיווח

תהליך הדיווח כולל חמישה שלבים כמפורט להלן:

שלב א' - פנייה למשרדי הממשלה ויחידות הסמך

שלב זה כולל שליחת מכתב פנייה וטופס דיווח דיגיטלי למנמ"רים, מנהלי אבטחת מידע ומנהלי יישומים של משרדי הממשלה ויחידות הסמך, אשר הונחו על ידי מנכ"לי משרדם לבצע את הדיווח בהתאם לסעיף 1ח להחלטת הממשלה בנושא. במסגרת הפנייה מתבקשים נציגי המשרד לדווח ליחידה באופן מפורט על אותם שירותים דיגיטליים לתושב המחייבים תהליך הזדהות ועל אופן ההזדהות עבורם.

שלב ב' - קבלת הדיווחים

איסוף אוטומטי של דיווחים שהתקבלו ממשרדי ממשלה ויחידות הסמך ובדיקתם.

שלב ג' - ניתוח הנתונים

ביצוע ניתוח מעמיק של הדיווחים שהתקבלו ובחינה לתאימות למדיניות.

שלב ד' - שליחת משוב והמלצות

שליחת משוב פרטני לכל אחד מהמשרדים בהתאם לדיווח שנשלח והמלצות מקצועיות להנגשת שירותים דיגיטליים בהתאם למדיניות, ופתיחת תהליך הכוונה למשרדים שאינם מנגישים שירותים בהתאם למדיניות.

שלב ה' - גיבוש דוח סיכום

גיבוש דוח סיכום של פעילות הדיווח במטרה לייצר הסתכלות רחבה על דיווחי המשרדים ומתן מענה בתהליך הכוונה סדור לתאימות למדיניות.

¹⁰ בהתאם לרמת רגישות השירות ובאופן שלא פוחת מרמת סמך 3, בהתאם להנחיית היחידה

7. דרישות לשימוש בביومترית

7.1. ביומטריה הינה מונח המשמש לחלופין לתיאור תכונה או תהליך. **כתכונה** : מאפיין ביולוגי (אנטומי או פיזיולוגי) והתנהגותי הניתן למדידה, אשר ניתן לעשות בו שימוש לזיהוי אוטומטי. **כתהליך** : שיטות אוטומטיות של זיהוי אדם בהתבסס על מאפיינים ביולוגיים (אנטומיים ופיזיולוגיים) והתנהגותיים הניתנים למדידה.¹¹

7.2. השוואה ביומטרית היא תהליך לאימות או לזיהוי בני אדם, באופן אוטומטי, על סמך מאפיינים ביולוגיים והתנהגותיים (המודלים הביומטריים). הנתונים הביומטריים ("תבניות" או "טמפלטים") הם ייצוגים ממוחשבים של המודלים הביומטריים הנוצרים עם הרכשתם או עיבודם.

7.3. מערכת ההזדהות הדיגיטלית עשויה להשתמש בביומרית במטרה לוודא את חוקיות הראיות/ ההוכחות לזהותו של המשתמש/ מבקש השירות. זיהוי פנים וטביעת אצבע הם המודלים המשמשים בצורה הנפוצה ביותר לטובת תהליכי הזדהות במערכות דיגיטליות.

7.4. ככלל, יש לעשות שימוש זהיר בביומרית ובהתאם לעקרונות למדיניות הלאומית ליישומים ביומטריים¹², ולקווים המנחים המפורטים במסמך זה.

7.5. בעולם הזהות נוהגים להתייחס ל- 3 "משפחות" של סוגי מאמתים :

7.5.1. **ידע (Something You Know)**.

7.5.2. **בעלות (Something You Have)**.

7.5.3. **משהו שאתה (Something You Are)**.

הביומטריה השייכת ל"משפחה" של משהו שאתה (Something You Are), כאשר השוואה ביומטרית בתהליך אימות זהות היא בעלת אופי סטטיסטי (איננו מוחלט), בעוד שגורמי אימות אחרים, כגון : סיסמה, קוד חד פעמי, הם מוחלטים. לפיכך, **נהוג** לשלב מאמתים ממשפחות שונות, כדי לחזק את תהליך אימות הזהות.

7.6. בעת שימוש ביישומים ביומטריים, לטובת תהליך הזדהות, יש להקפיד על כיוול המערכת לעמידה בדרישות הביצועים המפורטות להלן, כדי לשמור על שעורי שגיאה בהיקף סביר למול רגישות השירות, לרבות ביחס לנושא ההתמודדות עם הונאות וזיופים (ביומטריה חשופה לפגיעויות של התחזות והונאות של מצג שווא, זיופים, הזרקה ו Deep Fake).

7.7. ככלל, מומלץ לבצע אימות ביומטרי אל מול קובץ דיגיטלי חתום (כגון שבב מסמך/ תיעוד אלקטרוני¹³ או קובץ ממסמך/ תיעוד דיגיטלי¹⁴ או מול מאגר ביומטרי מוסמך ככל שהדבר אפשרי), ולהימנע מביצוע השוואה לצורך אימות זהות אל מול תמונה מודפסת/ סרוקה, לאור הקלות היחסית בזיוף התעודה באמצעות החלפת תמונה ולאור איכותה.

7.8. אפליקציות (יישומונים) להזדהות רבות עושות שימוש במנגנון הביומטרי שבמכשיר הקצה, כגורם אימות. ככלל, יש להעדיף מנגנון ביומטרי עצמאי שאינו נשען על מכשיר הקצה, ככל הניתן, בפרט לצורך הרישום לאפליקציה. העדפה זו נובעת משליטה טובה יותר במנגנון הביומטרי ובשעורי השגיאה שלו.

¹¹ בהתאם להגדרה **במדיניות הלאומית ליישומים ביומטריים**

¹² מסמכי המדיניות ליישומים ביומטריים - https://www.gov.il/he/pages/_2bio_biopolicy_app?chapterIndex=3

¹³ **מסמך/תיעוד אלקטרוני** – מסמך פיזי הכולל גם שבב אלקטרוני אשר גם בו כלולים הפרטים האישיים ולעיתים גם תמונה של בעל המסמך, וזאת באופן מאובטח ומוצפן והניתן לאימות באיכות גבוהה (כגון : באמצעות חתימה אלקטרונית).

¹⁴ **מסמך/תיעוד דיגיטלי** – מסמך וירטואלי (קובץ) בו כלולים הפרטים האישיים ולעיתים גם תמונה של בעל המסמך, וזאת באופן מאובטח ומוצפן והניתן לאימות באיכות גבוהה (כגון : באמצעות חתימה דיגיטלית).

7.9. ככל שנעשה שימוש במנגנון הביומטרי במכשיר הקצה, חשוב להקפיד על הפרדה בין פעולת "פתיחת" מכשיר הקצה באמצעות המנגנון הביומטרי שלו, ובין שימוש במנגנון זה כגורם אימות עבור פתיחת האפליקציה להזדהות דיגיטלית ולבצע במנגנון שימוש נוסף בעת הגישה לאפליקציה.

7.10. להלן הדרישות הטכניות לשימוש במנגנונים ביומטריים כחלק מתהליך הוכחת הזהות:

7.10.1. נותן השירות יוודא כי האלגוריתמים הביומטריים נבדקו באמצעות גורם עצמאי (מעבדה מוסמכת/ מוסד מחקר) לחקר ביצועים, בהתבסס על תקני ISO/IEC.

7.10.2. נותן השירות ישאף לעמוד בספי הביצועים המינימליים הבאים לאימות ביומטרי בתרחיש אימות פנים 1:1 ;

7.10.2.1. שיעור התאמה שגויה (FMR) : 1:10,000 או טוב יותר.

7.10.2.2. שיעור אי התאמה שגויה (מניעת שירות) (FNMR) : 1:100 או טוב יותר.

7.10.3. המדדים הנוגעים לזיהוי פנים 1:M תלויים בגודל המאגר, ובדרך כלל פעולה זו אינה נפוצה במערכות להזדהות דיגיטליות. באם נותן השירות עושה שימוש בפעולת השוואה זו, יש לבחון את שעורי השגיאה באופן המתאים לתרחיש ולהיקף המאגר.

7.10.4. נותן השירות ישאף להשתמש בטכנולוגיות ביומטריות מוכחות המספקות ביצועים דומים עבור אוכלוסיות דמוגרפיות שונות (על רקע גזע, מגדר, צבע עור, מוצא אתני, גיל וכו'). ככל שישנם פערים בביצועים, יש לשאוף לצמצם אותם למינימום האפשרי, באמצעות כלים מתאימים (ספים דינמיים, טיוב מערכת הצילום ועוד)¹⁵.

7.10.5. נותן השירות יגיש את תוצאות הביצועים והבדיקות התפעוליות לזמינות לציבור, ככל הניתן, כדי לקדם שקיפות ואמון.

7.10.6. נותן השירות ייטול את הדגימה/ מאפיין הביומטרי באופן שיצמצם את הסיכון לכך שהביומטריה נלקחה ממישהו אחר ולא ממבקש השירות עצמו שנרשם למערכת.

7.10.7. התמודדות עם הונאות - בעת ביצוע האיסוף והשוואה של הביומטריה מרחוק, נותן השירות יישם יכולות של גילוי ניסיונות זיוף והתחזות ובהן גילוי מצגי שווא (PAD¹⁶), וכן יפעל לבצע באופן מיטבי גילוי הזרקה (Injection) וגילוי זיוף עמוק (Deep Fake).

7.11. פירוט הדרישות לשימוש בגילוי התקפות מצג שווא (PAD)

7.11.1. יש לוודא כי הזהות הנטענת היא של אדם חי המספק את טענת/ ראיית הזהות בזמן אמת.

7.11.2. יש להשתמש באימות ביומטרי תוך ביצוע בדיקת "חיות", וליישם מנגנון גילוי התקפות מצג שווא מסוגים שונים בשיעורי הצלחה גבוהים ובהתאם למפורט להלן:

7.11.2.1. המערכת תכלול רכיב לגילוי חיות ולגילוי התקפות מצג שווא ברמות התקפה שונות,

ותיבדק בהתאם לתקן ISO/IEC 30107 ובכלל זאת **תשאף** לביצועים של עמידה ב

¹⁵ בהתאם לתקן NIST ישאף ספק שירות ההזדהות לוודא ששיעורי השגיאה אינם חורגים ביותר מ 25% ביחס לכלל האוכלוסייה.

¹⁶ Presentation Attack Detection

IAPAR¹⁷ של לא יותר מ 2% לרמת התקפה 1, ועד 185% לרמות התקפה 2 ו-193. עבור

מדד BPCER²⁰ - לא יותר מ 2%.

7.11.2.2. במסגרת הוכחת העמידה בביצועי PAD, נדרש להציג אישור ממעבדה מוסמכת²¹.

7.11.3. בנוסף, בהתאם לאופן מימוש/ יישום השירות, מומלץ לעשות שימוש במנגנון אימות "חיות

אקטיבי רנדומלי", דהיינו תוך הנחיית המשתמש לפעולות אקראיות, שלא ניתנות לחיזוי מראש,

באופן שיוכל למנוע זיוף עמוק (Deep Fake).

7.12. **הגנה מפני איום הזרקה (Injection) ביישום ביומטרי:** בהתקפה זו התוקף מנסה להחדיר מידע

ביומטרי (כמו תמונה או וידאו מזויף) לתוך המערכת כדי להערים עליה כי מדובר במשתמש לגיטימי.

משכך יש להטמיע את הבקורות להלן:

7.12.1. **חובה** ליישם בקורות טכניות על מנת לוודא שהמדיה הדיגיטלית המיוצרת בתהליך הוכחת הזהות

בוצעה באמצעות חיישן אמיתי ולא באמצעות מצלמה וירטואלית, מכשיר שעבר פריצה, תוכנה או

מערכת חומרה המדמה את פעולת המערכת המקורית (לוודא שלא מדובר באמולטור).

7.12.2. **חובה** לוודא שהמידע (התמונה/ הווידאו) מגיע מהחיישן עצמו (חיישן מקורי ומזוהה).

7.12.3. **חובה** להשתמש בערוץ מוגן בין החיישן (או נקודת הקצה) לבין המאמת. קרי, התקשורת בין

החיישן לבין מנגנון האימות תהיה מוגנת, מוצפנת וחתומה.

7.12.4. **חובה** לבצע בדיקה לזיהוי מניפולציה או זיוף של המדיה הדיגיטלית:

7.12.4.1. יש לעשות שימוש באלגוריתמים (שעברו בדיקת מעבדה מוסמכת) לניתוח תמונות²² ולוודא

כי רמת הביצועים (לזיהוי שיעור שגיאות קבלה ודחייה שגויה) הם בהתאם לסעיף 7.10

לעיל.

7.12.4.2. בתהליך בדיקת המערכת טרם הפעלתה, חובה לתעד סוגי דוגמאות של התקפות שנבדקו

ואת שיעורי השגיאות ולהעמידם לרשות הגורמים המסתמכים על המערכת לטובת מתן

שירותים באמצעותה, לפי דרישה.

7.12.4.3. **מומלץ**, לבצע ביקורת ידנית, באופן מדגמי, על ידי גורם אנושי במטרה לספק רובד נוסף

של דיוק.

7.12.5. להגדיר הגבלת ניסיונות גישה- כמפורט [בסעיף 9.2](#).

7.13. **ככלל, לטובת הגנה מפני איומי מצג שווא והזרקה, מומלץ:**

7.13.1. פתיחת מצלמה בזמן אמת (לא לאפשר העלאת תמונות או סרטונים מתוך מאגר אישי כגון "גלריית

התמונות").

7.13.2. לעשות שימוש במנגנון אימות זהות אקטיבי ורנדומלי כאמור בסעיף 7.11.3 לעיל.

¹⁷ IAPAR - impostor Attack Presentation Accept Rate - שיעור הצלחת התחזות במצג שווא.

¹⁸ תנאפשר חריגה של עד 10% באישור היחידה.

¹⁹ שלוש רמות התקפות: רמת התקפה 1- התקפה באמצעים הדורשים מאמץ/ מיומנות קלה כגון: תמונה מודפסת/סרטון דו מימדי באמצעות מכשיר. רמת התקפה 2 - באמצעים הדורשים מאמץ/מיומנות בינונית כגון: מסיכת נייר/ לטקס. רמת התקפה 3 - התקפה באמצעים מתקדמים/ מיומנות מקצועית/גבוהה כגון: מסיכת סילקון/מסכות תלת מימד היפר ריאליסטיות. בהתאם לתקן ISO/IEC 30107-3.

²⁰ BPCER - Bonafide Presentation Classification Error Rate - שיעור התראות שווא.

²¹ קיימות מספר מעבדות כגון: Ingenium, BixeLab, iBETA.

²² ניתוח תמונות/ וידאו כגון: ניתוח "מטא-דאטה", ניתוח הבעות לא טבעיות, גילוי "רעשים סינטטיים" (ריצודים), "חוסר סינכרון בין התמונה לקול וכדומה.

8. בדיקת מהימנות ותקפות מסמכי זיהוי

בעת שימוש במסמכי זיהוי לטובת תהליך הרשמה ו/או אימות במערכות הזדהות מקוונות, נדרשת בדיקת תקפות (Validation) ומהימנות/ אמיתות (Authentication) של מסמך מזהה²³ לצורך הוכחת בעלות על הזהות²⁴. לבדיקת המסמך נדרש לבצע את הפעולות הבאות :

- 8.1. בדיקת תקפות המסמך עצמו – האם הוא בפורמט תקני לדוגמה : סימני אבטחה, שדות פרטי מידע ומיקומם במסמך, לוגיקה²⁵, ושאינו מזויף ; כאשר עבור **מסמכים אלקטרוניים** יש להוסיף בדיקות כגון : חתימה אלקטרונית, השוואת בין המידע המודפס למידע בשבב, בדיקה מול CRL²⁶.
- 8.2. ניתוח פורנזי הכולל לדוגמה : סוג פונט, עובי הפונט, מרחק בין אותיות ומספרים.
- 8.3. בדיקת מהימנות – השוואת "ביומטרית" בין תמונת המשתמש לבין זו שבמסמך (דיגיטציה), תוך שימוש בבדיקת "חיות" (Liveness Detection), ובהצלבה מול מאגרי מידע ממשלתיים/ מוסמכים, בהתאם לרמות הזהות הנדרשות (רב"ה/ רב"א).
- 8.4. לביצוע תהליך בדיקות זה, נהוג להשתמש בטכנולוגיות OCR מתקדמות וכלים לזיהוי זיופים (במסמכי זיהוי פיזיים) ושירותי אימות חיצוניים (API) ובדיקות קריפטוגרפיות (במסמכי זיהוי אלקטרוניים ודיגיטליים), המספקים תשתית מלאה לזיהוי מאובטח ומדויק של מסמכי זיהוי.

9. הגבלת מספר ניסיונות גישה

- 9.1. ספק השירות יפעל ליישום בקרות להגנה מפני תקיפות לניסיונות ניחוש גורמי האימות המקוונים. תיושם מגבלה לכמות הניסיונות לכל משתמש בהתאם לרמת רגישות השירות²⁷. טכניקות אפשריות נוספות, במטרה להגביל את הסבירות לתקיפה יכללו ;
 - 9.1.1. ספק השירות ידרוש מהמשתמש לבצע "אתגר זיהוי"²⁸ (סימון מעברי חצייה/ רמזורים מתוך תמונה או פעולה פיזית אקראית אחרת, כגון : לחיצה על מקש מסוים) במטרה להפחית את האפשרות לתקיפה באמצעות "בוט" המנסה לבצע אימות זהות.
 - 9.1.2. דרישה מהמשתמש להמתין פרק זמן מסוים בעקבות ניסיון אימות כושל.
 - 9.1.3. הגבלת כמות הניסיונות המותרות לניסיונות כושלים (כמפורט בתהליכי ההרשמה והאימות בהתאם לרמת הסיכון).
 - 9.1.4. הגבלת משך זמן ביצוע הניסיונות (כמפורט בתהליכי ההרשמה והאימות בהתאם לרמת הסיכון).
 - 9.1.5. יכולת קבלת שירות וביצוע אימות המגיע מרשימת כתובות IP שממנו המנוי אושר לביצוע השירות.
 - 9.1.6. מינוף טכניקות אימות המבוססות על דפוסי התנהגות של המשתמש.

²³ מסמך מזהה יכול להיות מסמך פיזי לא אלקטרוני, מסמך פיזי אלקטרוני (הכולל שבב, ויכול לכלול גם דגימה ביומטרית) או מסמך דיגיטלי (ר' פירוט סוגי מסמכים - בכרך ב', סעיף 6.4, עמ' 9)

²⁴ ר' פירוט בכרך ב' - הרשמה

²⁵ לדוגמה : חישוב ספרת הביקורת בת.ז.

²⁶ CRL – Certificate Revocation List – רשימת מסמכים/ תעודות מבוטלים.

²⁷ פירוט מספר ניסיונות בתהליך אימות- ר' תוצר ג'.

²⁸ challenge

9.2. במערכת הכוללת רכיב אימות/זיהוי ביומטרי בעל המערכת ישאף לביצועים הבאים:

- 9.2.1. לאפשר לא יותר מ 5 ניסיונות אימות כושלים רצופים או 10 ניסיונות כושלים רצופים באם יש מערכת PAD העומדת בדרישות כמפורט בסעיף 7.10 לעיל, המוטמעת במערכת ההזדהות. כאשר לאחר מכן המערכת תטיל עיכוב של 30 שניות לפחות לפני סדרת ניסיונות נוספת, עם מגבלה כוללת של לא יותר מ 10 ניסיונות אימות כושלים רצופים (ו - 20 ניסיונות אם מוטמע PAD).
- 9.2.2. לאחר הגעה לתקרת הניסיונות, המערכת תשבית את יכולת האימות הביומטרי של המשתמש, ויוצע למשתמש שימוש בגורם אימות אחר.

10. ביצוע בדיקות חוסן וחזירות במערכות הזדהות מקוונות

- 10.1. בדיקות חוסן וחזירות הן מרכיב קריטי בהגנה על מערכות מידע, במיוחד כשמדובר במערכות להזדהות דיגיטלית. מערכות אלו מהוות שער גישה לשירותים אישיים ונתונים שיכולים להיות רגישים ואף מסווגים – מה שהופך אותן ליעד מועדף על תוקפים. ביצוע בדיקות חוסן וחזירות מאפשרות לזהות חולשות, שגיאות, פגיעויות וכשלים לוגיים, שעלולים לאפשר לתוקפים לעקוף מנגנוני אימות, לגנוב זהויות או להשתלט על מערכות. ביצוע תקופתי של בדיקות אלו מסייע לארגונים להיות ערוכים לאיומים, להבין את רמת החשיפה לסיכונים ולתקן נקודות תורפה לפני שהן מנוצלות בפועל על ידי תוקפים.
- 10.2. מעבר לאיתור חולשות, בדיקות חוסן וחזירות משמשות גם כלי אסטרטגי להעלאת המודעות הארגונית ולחיזוק מדיניות אבטחת המידע. הן מאפשרות לארגון לבחון את מוכנותו לתרחישי תקיפה בזמן אמת, ולחדד נהלים ותהליכים קיימים. במערכות להזדהות דיגיטלית – בהן חוויית המשתמש והאבטחה חייבות ללכת יד ביד – בדיקות אלו חיוניות לאיזון נכון בין נוחות לבין הגנה מיטבית על נתוני המשתמש והארגון.
- 10.3. כל נותן שירות דיגיטלי, המחזיק / מתפעל מערכת הזדהות, חייב בביצוע בדיקות חוסן/חזירות, עבור תרחישים בתחום ההזדהות מחד והיבטי אבטחת סייבר מאידך. יש לבצע מבדקי חוסן/חזירה (PT) באופן עיתי, אחת ל 18 חודשים, ובהתאם להתפתחות הטכנולוגית של המערכת, משטחי התקיפה המתרחבים ואירועים נקודתיים שהתרחשו במערכת. תרחישי המבדק, נדרשים להיות ייעודיים לתחום ההזדהות (ולא תרחישי בדיקת סייבר כללית). בעל / מתפעל מערכת הזדהות, יעביר את תרחישי הבדיקה לאישור היחידה טרם ביצועה, יקבל משוב לגבי התרחישים שנבחרו, וידווח על תוצאותיה ליחידה.
- 10.4. הבדיקה יכולה להיערך במתכונת "קופסא אפורה" או "קופסא שחורה", כדי לדמות תוקף חיצוני או פנימי ולהעריך את האפקטיביות של אמצעי ההגנה מכל זווית אפשרית. ובלבד שתבוצע על מערכת הייצור, או על מערכת זהה למערכת הייצור (על כל רכיביה). ככל הנדרש תתוכנן "השבתה" של המערכות לפרק זמן מוגדר לביצוע הבדיקות.

11. הזדהות פדרטיבית ומערכות הזדהות פדרטיביות בתהליכי הזדהות לשירותים ציבוריים וממשלתיים²⁹

11.1 מהי הזדהות פדרטיבית

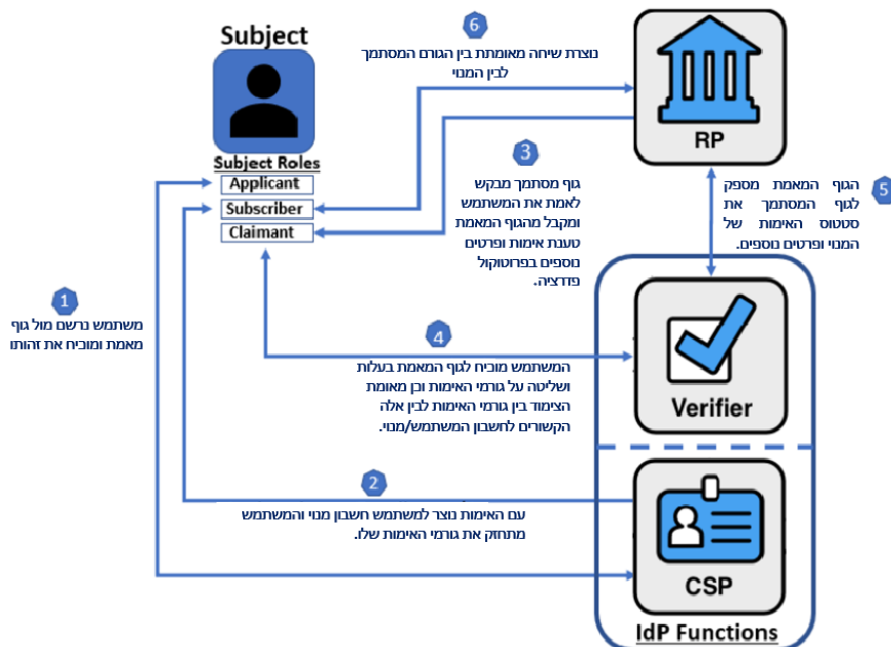
- 11.1.1. הזדהות פדרטיבית היא מנגנון המאפשר למשתמשים לגשת למספר שירותים דיגיטליים שונים באמצעות אישורי זהות דיגיטלית (Credentials) ושירותי אימות שוטף מספק זהות דיגיטלי אחד או יותר (Identity Digital Provider, IdP), במקום ליצור ולנהל חשבונות נפרדים וכפועל יוצא, קיום זהויות דיגיטליות נפרדות, עבור כל שירות. פירוט מפרט הנחיות טכניות למימוש שירותי הזדהות דיגיטלית פדרטיביים מפורטים מעבר לפרק זה **בנספח 4**.
- 11.1.2. במודל זה, המשתמש נרשם למערכת הפדרטיבית, אשר מאמתת את זהותו מול ספק הזהות העיקרי (Identity Provider). בסיום שלב הרישום נקבעים גורמי האימות בהם יעשה שימוש לטובת אימות זהות המשתמש, לקבלת שירותים המשויכים למערכת הפדרטיבית וניתנים באמצעותה.
- 11.1.3. כיוון שמדובר במספר נותני שירות במערכת הפדרטיבית, הפרוטוקולים מורכבים ומחייבים עמידה בתנאי אבטחה ושמירה על פרטיות וחייבת לספק את האישורים בפרוטוקולים מאובטחים כגון SAML³⁰.
- 11.1.4. נוסף ונציין כי לצורך ניהול תהליכים "פדרטיביים" כמו ארנק זהויות דיגיטלי (כלומר- מערכת מרכזית הנותנת שירות הזדהות כ HUB או מערכת של ספק השירות), יש צורך בהקמה של **מערכת ניתוח הונאות (Fraud Analysis System)** מתקדמת (יכולות איסוף, ניתוח ותגובה בזמן אמת לאירועים חריגים וא-נומליות).

²⁹ ככל שמדובר בתהליכי הזדהות בממשלה (מערכת הזדהות שהוקמה על ידי הממשלה). משכך יש להוציא את השירותים לגופים בחברות הפרטיות (שאינן שייכות למגזר הממשלתי/ ציבורי) ממסגרת ההתייחסות במסמך זה.

³⁰ SAML - Security Assertion Markup Language - "שפת סימון לאישורי אבטחה". זהו פרוטוקול תקשורת מבוסס XML שמאפשר החלפת מידע על אימות (Authentication) והרשאות (Authorization) בין שני צדדים עיקריים: ספק זהות (Identity Provider – IdP) וספק שירות (Service Provider – SP). מטרת SAML היא לאפשר Single Sign-On (SSO) - התחברות אחת למספר מערכות. הפרוטוקול נכתב ופותח ע"י ארגון OASIS - ראשי תיבות של Organization for the Advancement of Structured Information Standards מדובר בארגון תקינה בינלאומי שמתמחה בפרוטוקולי מידע פתוחים. הגרסה הנפוצה כיום היא SAML 2.0, שפורסמה בשנת 2005 והיא הבסיס לרוב פתרונות ה SSO-הארגוניים הקיימים

11.2 תהליך פדרטיבי אופייני

תהליך פדרטיבי אופייני מתואר בתרשים שלהלן :



11.3 דוגמא למערכת פדרטיבית בישראל

מערכת ההזדהות הלאומית

בישראל, ככל והשירותים המקוונים למשתמש ניתנים באמצעות שירות הזדהות במערכת פדרטיבית - מערכת ההזדהות הלאומית, על הבעלים / הגורם המתפעל של מערכת ההזדהות (קרי, מערך הדיגיטל הלאומי) לעמוד בכללי המדיניות הלאומית להזדהות בטוחה, לוודא שהמערכת מאובטחת ומוגנת, למלא אחר כלל הוראות האבטחה, וכן לוודא כי בעל השירות "המתארח" במערכת ביצע תהליך של סיווג רגישות השירות, בהתאם למדיניות, ומצא כי המערכת הפדרטיבית הספציפית, מעניקה לו את רמת הסמך הנדרשת לו להנגשת השירות.

נספח 1 - עיקרי העדכונים במסמכי המדיניות והקווים המנחים

לאור התפתחות האיומים והטכנולוגיה בתחום ההזדהות הדיגיטלית, לצד עדכוני תקינה בינלאומיים עליהם מבוססת המדיניות, ובהתאם להחלטת הממשלה, בוצעו במהלך השנים 2021 ו- 2023 מספר עדכונים למסמכי המדיניות, תוך תהליך היועצות עם הצוות הבין-משרדי, כאשר עדכון הגרסה הנוכחית מחליף את הגרסה הקודמת שפורסמה בשנת 2023. להלן עיקרי העדכונים שבוצעו:

1. עדכונים בכרך הכללי

- 1.1. **הבחנה בין מושג רמת הבטחת זהות - בתהליך הרשמה (רב"ה) לרמת הוודאות בזהות בתהליך האימות (רב"א).**
- 1.2. **חשיבות איזון בין דרישות אבטחה מחמירות לבין חווית משתמש - תפיסה אחודה לאופן הנגשת שירותים דיגיטליים במענה לסיכונים מתפתחים לצד נוחות וחווית משתמש בתחום ההזדהות הדיגיטלית.**
- 1.3. **חוק תקשורת דיגיטלית - הכנסת תת פרק המתייחס לתיקון החוק, והחשיבות להנגשת שירותים נפוצים הדורשים הזדהות באופן דיגיטלי שמאפשר הזדהות ברמת ודאות התואמת את סוג השירות המבוקש ורגישותו.**
- 1.4. **וקטור איום ושיקולי אבטחה - עדכון סוגי התקיפה ומנגנונים להפחתת איומים.**
- 1.5. **תהליך דיווח ותאימות שנתית - התייחסות לתהליך עבודת ההכוונה מכוח החלטת הממשלה, לתאימות משרדי הממשלה למדיניות לאופן הנגשת השירותים הדיגיטליים הדורשים הזדהות.**
- 1.6. **דרישות לשימוש בביומטריה - העברת הדרישות לשימוש בביומטריה בכרך הכללי, ובכלל זאת עדכון הדרישות בהתאם לעדכוני התקנה, כולל דרישות טכניות ושיעורי שגיאה, והתייחסות לשימוש במנגנוני גילוי התקפות מצג שווא (PAD), והזרקות (Injection).**
- 1.7. **הגבלת מספר ניסיונות גישה - חידוד הדרישות להגבלת ניסיונות גישה מתוך ראייה של הגבלת סבירות לתקיפה.**
- 1.8. **ביצוע בדיקות חוסן וחזירות - הוספת פרק המתייחס לצורך והחובה בביצוע בדיקות חוסן וחזירות עתירות, לתרחישים שונים בתחום ההזדהות.**
- 1.9. **הזדהות פדרטיבית - הוספת פרק המתייחס לתהליכי ההזדהות לשירותים ציבוריים וממשלתיים במערכות פדרטיביות, ובו דרישות ביצוע.**

2. עדכונים בכרך א' - סיווג שירותים

הכרך עבר טיוב, תוך תמצות ודיוק של דרישות התהליך הנדרשות לביצוע תהליך הסיווג, וכן הפנייה למחשבון המקוון.

3. עדכונים בכרך ב' - הרשמה

- 3.1. **אימות זהות ואיסוף ראיות לטובת הוכחת זהות בשלב ההרשמה - הסבר על תהליך הצגת הראיות לטובת תהליך ההרשמה, והתייחסות לחוזק ראיות שונות ומאפיינים, על מנת לבצע את ההרשמה בהתאם לרגישות השירות.**
- 3.2. **דרישות לראיות בהתאם לרמת רגישות - עדכון הטבלה לשילוב הראיות הנדרשות בתהליך ההרשמה, והוספת דוגמאות ליישום בישראל.**

4. עדכונים בכרך ג' - אימות

- 4.1. **איומים המזוהים בשלב האימות** - עדכון טבלת האיומים הקיימים לשלב האימות.
- 4.2. **סוגי מאמתיים** - עדכון גורמי האימות הקיימים לטובת תהליכי אימות במערכות הזדהות דיגיטליות, ודרישות לשימוש.
- 4.3. **דרישות למימוש תהליך אימות בהתאם לרמת רגישות** - עדכון הטבלה לשילוב גורמי האימות הנדרשות בתהליך האימות, והוספת דוגמאות ליישום בישראל.
- 4.4. **גורמי אימות הניתנים לסנכרון** - הוספת פרק לגורמי אימות הניתנים לסנכרון (מפתח גישה, PASSKEY), והסבר על הדרישות הכלליות בעת מימוש.

נספח 2 – עקרונות המדיניות להזדהות בטוחה

עקרונות המדיניות נקבעו בהחלטת הממשלה 2960 :

1.1 עיקרון השימושיות והפשטות :

- אמצעי ההזדהות שיינתנו בידי התושבים, ותהליכי העבודה לצורך השימוש בהם, כחלק מאספקת שירותים דיגיטליים, יהיו פשוטים, קלים ונוחים לתפעול ככל שניתן.
- יש לאפשר פתרונות הזדהות פשוטים ונגישים, מתוך הבנה שפשטות הפתרונות תורמת לשימושים.

1.2 הגנת סייבר ובכלל זה אבטחת המידע

- תשתית ההזדהות תהיה מאובטחת ועדכנית באופן התואם את האיומים המשתנים.
- תהליכי ההזדהות יבטיחו הגנה על כל הגורמים המעורבים, ויפעלו בהתאם לבקורות הנדרשות בכל שלבי התהליך.
- תידרש עמידה בתקני אבטחת מידע מקובלים³¹ בהתאם לטכנולוגיה הרלוונטית.
- יבוצע תכנון מוקדם בראיית אבטחה (Security-by-Design)

1.3 עיקרון הגנת הפרטיות:

- תשתיות ההזדהות הבטוחה יבטיחו הגנה על פרטיות התושבים.
- ייושמו עקרונות הגנה על הפרטיות, על פי הדין בישראל.
- יבוצע תכנון מוקדם בראיית הפרטיות (Privacy-by-Design).
- תתבצע הפרדה ככל שניתן בין מידע על הזדהות התושב מול ספקי ההזדהות, לבין מידע על שירותים שהתושב צורך מספקי השירות השונים.
- לא ייווצר מידע עודף בתהליכי ההזדהות באופן שעלול לפגוע בפרטיות התושבים : עיצוב תשתיות המערכות יתבסס על עיקרון צמצום המידע הנשמר, ככל שניתן, הן לעניין היקף המידע, סוג המידע והן לעניין משך זמן שמירתו. בצד עקרון זה, יהיה צורך לאפשר לגורמים שונים במערכות ההזדהות, אשר יחויבו במעקב ובקרה אחר תהליכי ההזדהות, שמירה של מידע בהיקפים מסוימים.
- ניהול הרשאות הגישה למערכות ולמידע יתבצע, ככל הניתן, לפי "הצורך שלהם לדעת" (Need To Know).
- עקרון הכללת המידע³² : צמצום והכללת מידע ככל הניתן, כגון : אי שמירת תאריך לידה מדויק, אלא רק אינדיקציה לגבי "מעל/ מתחת גיל 18".
- ככל ונשמר מידע ביומטרי, יש לקבל את הסכמת המשתמש ולתעד את הסכמתו.
- שקיפות : לתושב יהיה מידע באשר לשמירת נתוניו האישיים והשימושים שיעשו בהם. ככל שניתן, תתאפשר שליטה של התושב על המידע השמור לגביו ועל החלטתו מי רשאי לגשת למידע זה, בכפוף לכל דין.

1.4 עיקרון התאימות הטכנולוגית ומערכות פתוחות:

- אמצעי ההזדהות והשימוש בהם, יהיו תואמים במידת האפשר ובשינויים המחויבים לתקנים בינלאומיים.

³¹ כדוגמה – תקני ISO רלבנטיים, Common Criteria, או תקני FIPS של ה-NIST.

³² Generalization

- תוקם תשתית של "מערכת פתוחה" עם קישוריות בין הרכיבים השונים שבה (Inter-Operable), כדי להבטיח תחליפיות בין אמצעים וספקים שונים, ועל מנת לאפשר מודולריות במימוש ופיתוח בשלבים, תוך התאמה לדרישות הביצועים הנגזרים.

1.5 עיקרון השימוש באמצעי ההזדהות:

- אמצעי ההזדהות הבסיסי המונפק לתושבי ישראל על ידי המדינה, הוא תעודת הזהות החכמה, המכילה מידע ביומטרי וקריפטוגרפי לצורך אימות זהות.
- ימומשו אמצעי הזדהות שיאפשרו הזדהות בטוחה, נגישה ופשוטה ממכשירים ניידים, כנגזרת של תעודת הזהות החכמה, בכפוף לעקרונות המדיניות בכלל, ועקרון השימוש והפשטות בפרט.

1.6 עיקרון סיווג השירותים:

- הבנייה אחידה של תחום ההזדהות הבטוחה מחייבת סיווג השירותים לרמות הבטחת האימות המתאימות להם. הסיווג יבוצע בהתבסס על ניתוח והערכת הסיכונים הקשורים בתהליך ההזדהות לקבלת שירותים אלו.
- האחריות להגדרת רמות הבטחת האימות עבור השירותים והעמידה בהן, הינה של בעל השירות. במידה ורמת הבטחת האימות אשר נקבעה על ידי מנכ"ל בעל השירות אינה תואמת את הקווים המנחים, יציין את הסיבות להחלטתו במסגרת הדיווח השנתי ליחידה.

1.7 היעדר קישור ל"מאגר הביומטרי":

- יובהר, כי במסגרת החקיקה הקיימת, נכון ליום כתיבת מסמך זה, לא ניתן לבצע קישור למאגר הביומטרי (המנוהל על ידי משרד הפנים) לצורך אימות זהות, וזאת בהתאם לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009.³³

³³ נושא זה נבחן בימים אלו, ובהיעדר שינוי עקרון זה ישאר.

נספח 3- טבלת סוגי איומים/ תקיפות עיקריים בתחום ההזדהות

תקיפה/ איום	הסבר	דוגמא
ניסיונות הרשמה אוטומטיים	תוקפים ממנפים "סקריפטים" ותהליכים אוטומטיים במטרה לייצר במהירות כמויות גדולות של "נרשמים פיקטיביים".	באמצעות "בוט" מבצעים הרשמה ע"י מסד נתונים גנוב, ובאמצעותו מייצרים חשבון לגישה לקבלת הטבות.
זיוף ראיות	התוקף יוצר או משנה "ראיות" על מנת לתבוע זהות.	זיוף רישיון נהיגה המשמש כהוכחת זהות.
יצירת סינטטית זהות	התוקף בודה ראייה על זהות שאינה מקושרת לאדם אמיתי.	פתיחת כרטיס אשראי בשם בדוי, במטרה לייצר קובץ חיוב אשראי.
שימוש בזהות בדויה (גניבת זהות)	התוקף משתמש במרמה בזהותו של אדם אחר או בראיות המוכיחות את זהותו.	תוקף משתמש בדרכון/ תעודה גנובה.
הנדסה חברתית	תוקף משכנע את המשתמש למסור פרטים אודות זהותו במטרה להשתמש בהם לצורך הוכחת זהות תחת טענת שווא.	אדם מוסר פרטים אישיים לתוקף, אשר עושה בהם שימוש לצורך התחזות וקבלת שירות.
טענת שווא	תוקף מציג מידע כוזב תחת זהות לגיטימית.	קבלת הטבות סוציאליות שלא כדין.
דליפה של גורמי אימות בשימוש במערכת ההזדהות	תוקף עושה שימוש בגורמי אימות שדלפו "לרשת", רוכש מידע המכיל גורמי אימות שדלף "לרשת" או מבצע בעצמו תקיפה להשגת גורמי אימות לטובת תהליך ההזדהות. או שימוש בסיסמאות "חלשות", שניתן "לפצח" אותן בקלות יחסית או שימוש במאמטים, החשופים לקהל הרחב.	שימוש בסיסמאות של תאריך לידה או שימוש בתאריכי יציאה/כניסה לארץ מחו"ל כמאמת. ברשת האינטרנט "הגלויה" או ברשת האינטרנט "העמוקה", ניתן להשיג/לרכוש גורמי אימות המשמשים בתהליך ההזדהות (מספרי כרטיסי אשראי, תאריכי הנפקת מסמכים, תאריכי כניסה/ יציאה מחו"ל וכו')
חשיפת מידע בעת החזרת הודעות שגיאה שונות	מתן מידע עודף למשתמשים בעת שליחת מסכי תגובה לשגיאה בעת התחברות למערכת.	במסך המכיל מספר שדות (ערכים) להזנה. ציון מפורש של הערך השגוי הנדרש טיפול.
איום הזרקת תמונה או סרטון וידאו	התוקף יוצר סרטון וידאו או תמונה מזוייפים שמקושר לאדם אמיתי.	התחזות באמצעות תמונה/ סרטון Deepfake. שימוש בתמונה/ סרטון לגיטימיים בהזרקה (Replay Attack)

דוגמאות תמציתיות להתמודדות עם איומים / תקיפות בהתאם למפורט לעיל

להלן מנגנונים הקשורים לסיוע בהפחתת איומים, כפי שהוצגו לעיל, אין לראות בטבלה זו כסיכום מקיף, אלא כסיכום תמציתי של הפחתות עבור האיומים שפורטו לעיל;

תקיפה/ איום	אסטרטגיית הפחתת האיום
ניסיונות הרשמה אוטומטיים	1. ספק השירות יטמיע אפליקציית WEB של "חומות אש", לבקרה ואיתור של בוטים (WAF). 2. ספק השירות מיישם אימות בערוץ נפרד. 3. ספק השירות יישם אימות ביומטרי הכולל "זיהוי חיים", במטרה לקבוע נוכחות אמיתית של מבקש השירות. 4. ספק השירות יישם יכולות תעבורת נתונים ברשת במטרה לזהות תעבורה זדונית. 5. ספק השירות יישם מנגנון למניעת בוטים כגון: CPATCHA בשילוב סינון טכני.
זיוף ראיות	1. ספק השירות יאמת את תכונות הליבה (תכונות עיקריות) באמצעות מקורות סמכותיים/ אמינים. 2. ספק השירות יבדוק תכונות אבטחה פיזיות או דיגיטליות של הראיות שהוצגו.
יצירת זהות סינתטית	1. ספק השירות יאסוף מספר ראיות (MFA) על מנת לתמוך בתהליך הוכחת הזהות. 2. ספק השירות יאמת את סט התכונות/ מסמכים/ תיעוד מול מקורות מוסמכים/ אמינים. 3. ספק השירות יאמת את הזהות באמצעות השוואה ביומטרית של המבקש אשר סופקו ממקור מוסמך/ אמין.
שימוש בזהות בדויה (גניבת זהות)	1. ספק השירות יאמת את הזהות באמצעות השוואה ביומטרית מול שבב בתיעוד הלאומי החכם או למול גורם ייחוס אחר, מאושר על ידי היחידה. 2. ספק השירות לא יעשה שימוש במנגנוני זיהוי שאינם בשליטתו (כגון מכשירים סלולאריים חשבונות cloud וכדומה). 3. ספק השירות יטמיע אמצעי זיהוי התקפות מצג שווא. 4. ספק השירות יישם אימות באמצעות ערוץ נפרד. 5. ספק השירות יבצע בדיקות סטטיסטיות של חיוניות המאגרים. 6. ספק השירות יישם איתור יכולות הונאה וניתוח התנהגות כדי לזהות אינדיקטורים של חשבון העלול להיות זדוני.
הנדסה חברתית	1. ספק השירות יטמיע כלים לאיתור סימני מצוקה או כפייה, בתהליך האימות. 2. ספק השירות יספק יכולת הזדהות בערוץ נפרד במטרה לאמת את מיקומו של המשתמש. 3. ספק השירות יספק מידע ודרכי התקשרות למשתמשי הקצה עבור איומים נפוצים להנדסה חברתית.
טענת שווא	1. ספק השירות יישם הגבלות גאוגרפיות להרשאות גישה בתעבורת נתונים. 2. ספק השירות יאמת את סט התכונות/ מסמכי התיעוד אל מול מקורות מוסמכים ומהימנים.
דליפה גורמי אימות במערכת ההזדהות	1. ספק השירות יודא שימוש במאמתים "חזקים" בלבד. 2. ספק השירות יודא שימוש במאמתים מוכמנים בלבד. 3. ספק השירות לא יעשה שימוש במנגנוני זיהוי שאינם בשליטתו (כגון מכשירים סלולאריים חשבונות cloud וכדומה). 4. ספק השירות יבצע בקרה שוטפת לוודא את "חוזק" ואי חשיפת המאמתים. 5. ספק השירות יבצע בדיקת חדירות (PT), בתדירות הנדרשת לבדיקת "חוזק" המאמתים ואי חשיפתם. 6. ספק השירות ירכז דיווחים של משתמשים בנושא "חולשת" מאמתים. 7. שימוש ב-2FA הכולל גורמי אימות "ממשפחות" שונות. 8. צמצום שימוש בגורמי אימות סטטיים (סיסמאות, pin code וכו'). 9. עדכון גורמי אימות על-ידי המשתמשים אחת ל-24 עד 18 חודשים.

תקיפה / איום	אסטרטגיית הפחתת האיום
	10. ספק השירות יבצע מעקב אחד דיווחים בנושא דליפת מאמנים ויעדכן את תהליך אימות הזהות בהתאם. 11. ספק השירות יבצע "קמפיינים" להעלאת מודעות המשתמשים לנושא אפשרות לדליפת גורמי אימות ודרכי התמודדות בנושא.
חשיפת מידע בעת החזרת הודעות שגיאה שונות	1. ספק השירות יוודא, שהמידע המוחזר בהודעות השגיאה לא יחשוף את המאמנים (הרכב, מבנה וכו') בהם נעשה שימוש. 2. ספק השירות יוודא, קיום של השהייה בביצוע פעולות אימות לאחר מספר שגיאות, בהתאם להגדרה במדיניות. 3. ספק השירות יבצע בדיקת חדירות (PT), בתדירות הנדרשת לבדיקת אי "חשיפת" מידע בעת החזרת הודעות שגיאה.
איום הזרקת תמונה או סרטון ידאו	1. ביצוע בקורות טכניות לזיהוי חיישנים אמיתיים. 2. ניתוח המדיה הדיגיטלית על מנת לוודא שלא בוצעו מניפולציות, זיוף או שינוי. 3. ניתוח מדיה לזיהוי כלים של בינה מלאכותית ו Deep Fake 4. שימוש בערוצים מוגנים ומאומתים בעת העברת הנתונים. 5. ביצוע זיהוי אקטיבי רנדומלי מצד המשתמש לטובת הגדלת חשיפת מדיה מזויפת/ מעובדת. ר' פירוט בפרק 7, בסעיף 7.11 לעיל.

נספח 4 – הזדהות פדרטיבית

1. רב"א פדרטיבית (Federated Assurance Level – FAL)

- א. FAL מגדיר את הרב"א הנדרשת בפדרציה בתעבורה בין גופים מאמתים לגופים מסתמכים ואת אופן ההנגשה וההגנה על טענות אימות. על מנת לעמוד בדרישות עבור הרב"א הנדרשת בפדרציה (FAL), טרנזקציית הפדרציה תהיה תואמת לכל הדרישות המפורטות עבור אותה רב"א (FAL). כל רב"א (FAL) מאופיינת בסט של דרישות, המתגברות בהיבט האבטחה והמורכבות ככל שהרב"א (FAL) "עולה".
- ב. להלן ריכוז הדרישות בהתאם לרמות הרב"א :

דרישה	רב"א 2 (FAL1)	רב"א 3 (FAL2)	רב"א 4 (FAL3)
הגבלת משתמשים	ריבוי RP מותרים לכל טענה, מומלץ RP בודד לכל טענה	RP בודד לכל טענה	RP בודד לכל טענה
הגנת הזרקה	מומלץ לכל הטרנזקציות	נדרש, הטרנזקציה מתחילה ב-RP	נדרש, הטרנזקציה מתחילה ב-RP
הסכם אמון	"מובל" על-ידי המנוי או מוגדר מראש	מוגדר מראש	מוגדר מראש
מזהה ויצירת מפתח	דינמי או סטטי	דינמי או סטטי	סטטי
הצגת המידע	טענת הזדהות אישית ³⁴	טענת הזדהות אישית	טענת בעל הראייה או מאמת "מצומד" ³⁵

על טענות האימות לעבור בפרוטוקול פדרציה מאובטח כגון TOKEN ID בפרוטוקול OpenID Connect או SAML (Security Assertion Markup Language).
בכל רב"א (FAL) על גוף מאמת לעמוד בבקורות בטחון בינוניות ומעלה עפ"י SP800-53 או תקן רגולטורי מחייב דומה. כל רמה עוקבת מכילה וממלאת את כל הדרישות של רמות נמוכות יותר [למשל : תהליך פדרציה ברב"א 4 (FAL3) יכול להתקבל ברב"א 3 (FAL2) או ברב"א 2 (FAL1) מאחר שרב"א 4 (FAL3) עונה על כל הדרישות של רמות נמוכות אלה]. שילובים שאינם נמצאים בטבלה 1 אפשריים, וגופים שונים יכולות לבחור ליישם הגנות חזקות יותר באחד או יותר מתחומי הדרישות ברב"א הנדרשת בפדרציה (FAL).

2. פרוטוקול פדרציה

פרוטוקול פדרציה מתנהל בין משתמשים, גופים מאמתים וגופים מסתמכים, בתהליך הבא :

א. **הסכם אמון** - גוף מאמת וגוף מסתמך מסכימים על הסכם אמון שבו נקבעים פירטי ההרשאה, מטרת כל נתון המועבר ביניהם, אופן דיווח למשתמש, חלוקת אחריות, רמות הבטחה זמינות בגוף המאמת ורמות הבטחה נדרשות לגוף המסתמך, הכול בהבחנה בין מדיניות סטטית בה הפרטים

³⁴ טענת הזדהות אישית- הטענה להוכחת הזהות האישית המוצגת על ידי המשתמש עצמו כהוכחה לזהות המשתמש.
³⁵ טענת הזדהות המנוהלת על ידי ספק הזהות (IdP) או באמצעות גורמים מאמתים המוצמדים למשתמש (כגון : תעודה+קוד).

נקבעים מראש, לבין מדיניות דינמית בה הפרטים משתנים בזמן ריצה על פי החלטת המשתמש והגופים.

ב. **הרשמה** - הגופים מבצעים הרשמה הדדית כדי לאפשר העברת מסרי פדריציה מאובטחת, וזאת תוך קביעת מפתחות קריפטוגרפיים, מזהי מערכת, כתובות והרשאות גישה הדדיים. תהליך הרשמה יכול להיות ידני בהתערבות מנהלי המערכות, או אוטומטי, אך בכל מקרה עליו להתבצע בערוץ מאובטח הנפרד מערוץ הפדריציה.

ג. **אופן אימות** - בניסיון גישה של משתמש לגוף מסתמך מחליטים הגוף המאמת והגוף המסתמך על אופן העברת נתוני המשתמש ועל פירטי המשתמש לצורך אימותו, תוך יידוע המשתמש או תוך אישורו, בהתאם להרשאות שנקבעו בשלבים הקודמים, באופן סטטי בתחילת התהליך או באופן דינמי בזמן ריצה במידה וכך נקבע בשלבים קודמים. בכל מקרה נתוני משתמש יהיו לצורכי אימות בלבד.

ד. **אימות** - המשתמש מאמת מול הגוף המאמת וטענת האימות מועברת לגוף המסתמך. הן הגוף המאמת והן הגוף המסתמך מנהלים באופן מאובטח חשבונות למשתמשים, הכוללים הרשאות ופירטי אימות והנגישים למשתמשים פעילים. שמירת פירטי חשבון יכולה להיות קבועה או זמנית למהלך השיחה בלבד. הגוף העיקרי בניהול חשבונות משתמשים הוא הגוף המאמת, אשר מעדכן את הגופים המסתמכים בכל עדכון או ביטול של חשבון משתמש המנוהל על ידו. עדכונים וביטולים יכולים לעבור באופן דו צדדי באמצעות API במסגרת מגבלות הסכם האמון. במידה והגוף המסתמך מנהל פרטי משתמש שנאספו על ידו מגופים אחרים (מחוץ לפדריציה) לצורך אימות, עליו לעשות זאת בשקיפות הן כלפי המשתמש והן כלפי גופים מאמתים בפדריציה.

ה. **החלטה** - הגוף המסתמך מעבד את הטענה ופירטי חשבון אחרים בהתאם לצורך, ומחליט על פיהם האם לאפשר למשתמש גישה לשרות.

סוף המסמך