מערך הסייבר הלאומי

מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

משרד האוצר

רשות האוכלוסין וההגירה



אסטרטגיה לאומית להזדהות דיגיטלית

נובמבר 2026

דבר וועדת ההיגוי
(מבוא)

בעשור האחרון עובר העולם טרנספורמציה דיגיטלית, המשנה מן היסוד את האופן שבו מדינות, מוסדות, עסקים ותושבים מתקשרים, צורכים שירותים ומנהלים פעילות כלכלית ואזרחית. מגמה זו הואצה באופן משמעותי בעקבות משבר הקורונה, אשר המחיש את חשיבותם של שירותים דיגיטליים רציפים, זמינים ובטוחים, וזירז את המעבר מערוצים פיזיים לערוצים מקוונים. שירותים שבעבר חייבו התייצבות פיזית, ותהליכי זיהוי ואימות שאינם דיגיטליים, ניתנים היום לביצוע באופן מקוון, במהירות ובזמינות גבוהה.

התפתחות זו הפכה את אמצעי ההזדהות מכלי טכנולוגי תפעולי לתשתית חיונית לכלכלה, "עשיית עסקים" והחברה הדיגיטלית. יצירת "מערכת אקולוגית", אקוסיסטם, לתהליכי הזדהות מהימנים, יעילים ובטוחים, בה לכל תושב/ת יהיה ייצוג דיגיטלי אמין ומוגן, באמצעותו יתקבל שירותים ברמה גבוהה, הפכה להיות יעד מובהק עבור מדינות רבות בעולם. זהו תנאי למתן שירותים דיגיטליים מתקדמים, להפחתת הנטל הבירוקרטי, לחיזוק אמון הציבור ולהאצת הצמיחה הכלכלית[1].

היכולת להעמיד ולנהל אקוסיסטם להזדהות דיגיטלית בישראל, תלויה בגיבוש אסטרטגיה מתאימה ברמה הלאומית. ביוני 2025 פנתה ראש היחידה להזדהות ויישומים ביומטריים במערך הסייבר הלאומי אל מערך הדיגיטל, רשות האוכלוסין וההגירה, אגף התקציבים במשרד האוצר, החשב הכללי ולבנק ישראל, כדי להקים וועדת היגוי אשר תגבש תכנית לאומית עבור ישראל, לאחר סקירת המגמות הבינ"ל והמודלים הקיימים במדינות שונות בעולם.

עבודת ועדת ההיגוי התבצעה במהלך השנה החולפת (2025-2026). במסגרת עבודה זו נבחנו, בין היתר, תפיסות ואסטרטגיות של מדינות שונות, כאשר נעשתה התמקדות במדינות הבאות: בלגיה, אסטוניה, אוסטרליה, בריטניה, סינגפור וכן התפיסה הכוללת של האיחוד האירופאי; בחינת האקוסיסטם הקיים בישראל, נכסיו, התפתחותו לאורך השנים ותפקיד המדינה בהקשרים אלה למול המשק; הכשלים והפערים במערך הקיים; חלופות ומודלים אפשריים עבור ישראל; ההיבטים הכלכליים והרגולטוריים הכרוכים בהם; והצורך באיזון בין אינטרסים ציבוריים שונים, ובהם פרטיות, מהימנות, הגנת הסייבר, נוחות המשתמש והגנה על התושב, תוך העמדת צרכי התושב/ת במרכז.

לצורך גיבוש כיווני הפעולה המרכזיים התקיימו גם שולחנות עגולים והתייעצויות עם מגוון רחב של גורמים בממשלה ובמשק. במסגרת זו השתתפו גופים מהמגזר הפיננסי, ובהם בנקים, חברות אשראי וחברות ביטוח; גופים ממגזר הבריאות בהם בתי חולים וקופות חולים; וכן מומחים ונציגים משירות המדינה, מהתעשייה וממגזר התקשורת. השיח אפשר לבחון את האתגרים, הצרכים וההזדמנויות מנקודת מבטם של כלל השחקנים הרלוונטיים לאקוסיסטם.

אנו שמחים לפרסם את האסטרטגיה שגובשה על ידי חברי וועדת ההיגוי להערות הציבור.

[1] OECD, The OECD Digital Government Policy Framework (2020); World Bank, Identification for Development (ID4D).

דבר וועדת ההיגוי

בבסיס האסטרטגיה עומדת תפיסה לחיזוק הייצוג הדיגיטלי של התושב/ת בישראל ושל מערכת ההזדהות הלאומית, תוך שמירה על תאימות לזהות היסודית (הבסיסית) המנוהלת על ידי רשות האוכלוסין וההגירה, והסדרת ממשקי העבודה והאחריות בין הגופים הממשלתיים הרלוונטיים. לצד זאת, האסטרטגיה מבקשת להציג את המהלכים המרכזיים למינוף נכס הלאומי זה עבור כלל המשק, לשם העלאת חוסן וחיזוק תהליכי הזיהוי הדיגיטליים של הגופים המסתמכים במגזרים השונים, ולמתן שירות יעיל ובטוח עבור התושב/ת.

לאחר בחינת החלופות והמודלים השונים, ועדת ההיגוי סברה כי עבור ישראל נכון להמשיך ולחזק את תפקידה של המדינה ביצירת ובניהול התשתית הלאומית לזהות דיגיטלית, ולפעול להנגשת נכס זה לגופים נוספים במשק באופן מתקדם ולטובת התושבים. גישה זו מחייבת גידור וניהול סיכונים הנוגעים לפרטיות התושבים, לשקיפות, להיבטים הנוגעים להגנת הסייבר, היבטים כלכליים, היבטים רגולטוריים ועוד.

חשוב להדגיש כי נקודת המוצא בהנגשת יכולת זיהוי חזקה יותר בהתבסס על תשתית ממשלתית, עבור גופים מסתמכים במשק, ביחס לתהליכים/שירותים שהממשלה אינה צד להם, תעשה באופן וולונטרי. הדבר יבוצע בהתאם לקריטריונים מתאימים, כאפשרות נוספת בסל הכלים שיהיה בידי הגופים המסתמכים לחיזוק התהליכים שהם מנהלים, וללא חשיפת פרטי השירות. המגזרים העיקריים בהם התמקדנו היו המגזר הפיננסי ומגזר הבריאות, כאשר גופים אחרים או תרחישים ספציפיים ייבחנו באופן פרטני על ידי הגורמים המוסמכים לכך בהמשך הדרך.

אחד הכלים המרכזיים באמצעותו תמומש התפיסה המוצעת, ואשר יש חשיבות רבה בקידומו, הוא ארנק הזהויות הדיגיטלי של ישראל, בעניינו גובש מסמך עקרונות עבודה על ידי מערך הדיגיטל הלאומי, אשר יוביל את פיתוחו והנגשתו לציבור הרחב.

לצד אסטרטגיה זו תגובש תכנית יישום לחמש השנים הבאות, אשר תפרט את המהלכים הנדרשים למימוש עקרונותיה ויעדיה. ועדת ההיגוי תמשיך ללוות את יישום האסטרטגיה, במטרה להבטיח את מימושה באופן מיטבי, תוך בחינה ועדכון תקופתיים והתאמתה להתפתחויות הטכנולוגיות, הרגולטוריות והכלכליות ולשינויים המהירים המאפיינים מרחב חדשני ודינמי זה.

נבקש להודות לכל הגורמים אשר היו שותפים בגיבוש האסטרטגיה, ובפרט לנציגי בנק ישראל בראשותה של גב' ליאורה נבון, אשר סייעו באיגום עמדות גופי המגזר הפיננסי, השתתפו בישיבות וועדת ההיגוי ותרמו רבות בהבנת הפערים והאתגרים בתחום זה. כמו כן נודה לעוסקים הרבים במלאכה: לגב' ענבר פז, ראש תחום הזדהות דיגיטלית וגב' מירי זילברשטיין, ראש תחום אסטרטגיה במערך הסייבר הלאומי על ריכוז עבודת הוועדה, שותפותן לתהליך החשיבה והגיבוש המקצועי של האסטרטגיה, למר יהוד מרסיאנו, מר רפי דבוש ומר אלון זרגרי ממערך הדיגיטל, למר חן קסנטיני מרשות האוכלוסין וההגירה, לגב' עדי שיינבך מחטיבת החדשנות וטכנולוגיה בחשב הכללי, מר שלומי רוט מאגף התקציבים במשרד האוצר ולחברת Deloitte אשר ליוו תהליך זה.

נעמה בן צבי
ראש היחידה להזדהות וליישומים ביומטריים

יוגב שמני
מנהל חטיבת הטכנולוגיות והשירותים הדיגיטליים

שירה אייזנטל
ראש אגף טכנולוגיות דיגיטליות ומידע

אביתר פרץ
סגן בכיר לחשב הכללי

עופרי אשל
רכזת צוות, ממשל ומיוחדים אגף תקציבים

תוכן עניינים

הקדמה 5

הזדהות לאומית - האקו-סיסטם הישראלי 6

מגמות בין-לאומיות 8

פערים ואתגרים באקו-סיסטם הישראלי 10

חזון לאומי והעקרונות למימושו 13

ליבת האסטרטגיה:

1. פרק ראשון: זהות אחת בטוחה 15

1.1 יעד ראשון: כתובת אחת בממשלה להנגשת הייצוג הדיגיטלי למשתמשים ולגופים המסתמכים 16

1.2 יעד שני: הגנת סייבר והזדהות בטוחה 16

1.3 יעד שלישי: תאימות בין הזהות היסודית לייצוג הדיגיטלי 18

1.4 יעד רביעי: היערכות לעידן הפוסט קוואנטום 19

2. פרק שני: אופטימיזציה של ניהול הייצוג הדיגיטלי 19

2.1 יעד ראשון: ארנק זהות דיגיטלי לאומי 19

2.2 יעד שני: שקילות מלאה בין התעודה הפיזית לתעודה הדיגיטלית 23

2.3 יעד שלישי: מודרניזציה לתשתיות ההזדהות הלאומיות 23

2.4 יעד רביעי: זהויות אוטונומיות הפועלות בשם המשתמשים - AI Agents 24

3. פרק שלישי: הרחבת השימוש במערכת ההזדהות הלאומית עבור גופים מסתמכים שאינם ממשלתיים 25

3.1 יעד ראשון: הנגשת מערכת ההזדהות למגזר הפרטי וקביעת מנגנון מתאים 27

3.2 יעד שני: עקרונות הגנת הפרטיות (Privacy by Design) 29

3.3 יעד שלישי: חלוקת אחריות 30

3.4 יעד רביעי: התאמת המסגרת הרגולטורית עבור גופים פרטיים במשק 31

נספחים

נספח א' – הגדרות ומושגים 33

נספח ב' – מעגלי ההיוועצות 37

הקדמה

הזדהות דיגיטלית היא מנוע צמיחה כלכלי משמעותי. מחקרים בין-לאומיים[2] מצביעים על כך שכלכלה דיגיטלית מתקדמת נשענת על תשתיות אמון המאפשרות ביצוע עסקאות ושירותים באופן מאובטח, פשוט ורציף. אימוץ מערכות זהות דיגיטלית מהימנות צפוי לתרום להגדלת הפריון הכלכלי, להפחתת עלויות תפעול, להרחבת הפעילות העסקית ולשיפור הנגישות לשירותים ציבוריים ופרטיים כאחד. חשיבות הנגשת שירותים דיגיטליים קיבלה ביטוי גם בחקיקה בישראל, בה ניתן דגש לתקשורת הדיגיטלית עם גופים ציבוריים והחובה של גופים אלה בהנגשה של שירותים דיגיטליים, לרבות חובת הזיהוי הנדרשת בהתאם לרמת השירות המקוון[3].

בד בבד, הפכה הזהות הדיגיטלית לאחד הנכסים האסטרטגיים במרחב הדיגיטלי, ובהתאם גם לאחד מיעדי התקיפה המרכזיים של גורמי איום[4]. בשנים האחרונות מתרחב היקף הונאות הזהות, גניבת אמצעי הזדהות והשימוש בזהויות מזויפות או סינתטיות, לצד התפתחות מהירה של טכנולוגיות בינה מלאכותית יוצרת, (Generative AI), המאפשרות יצירת אמצעי התחזות מתוחכמים, ובהם זיופים עמוקים (Deep Fakes), יצירת זהויות סינתטיות (Synthetic Identity Fraud) ותקיפות מצג שווא (Presentation Attacks). מגמות אלו מעבירות את מוקד הסיכון מהגנה על מערכות בלבד אל הצורך להבטיח את מהימנות הזהות הדיגיטלית ואת יכולת ההסתמכות עליה לאורך כל מחזור החיים שלה[5].

התפתחויות אלו ממחישות כי זהות דיגיטלית אינה עוד רכיב טכנולוגי נקודתי, אלא תשתית אמון לאומית, המהווה תנאי לקיומה של כלכלה דיגיטלית מתקדמת ולמתן שירותים ציבוריים ופרטיים ברמת אמון גבוהה. בהתאם לכך, מדינות רבות מקדמות בשנים האחרונות אסטרטגיות לאומיות המשלבות בין ניהול זהות, אבטחת מידע, פרטיות, רגולציה וחדשנות, מתוך תפיסה מערכתית הרואה בזהות הדיגיטלית רכיב מרכזי בתשתיות הציבוריות הדיגיטליות (Digital Public Infrastructure)[6].

---

[2] World Bank, ID4D Practitioner's Guide; McKinsey Global Institute, Digital Identification: A Key to Inclusive Growth.(2019)

[3] 2018 סעיף 3יא לחוק תקשורת דיגיטלית עם גופים ציבוריים , תשע"ח

[4] ENISA Threat Landscape .2024 tropeR snoitagitsevnI hcaerB ataD nozireV ;2024

[5] NIST SP (2025) senilediuG ytitnedI latigiD ,800-63-4

[6] United Nations Development Programme (UNDP), Digital Public Infrastructure Safeguards Framework (2024); Regulation (EU) 2024/1183 (eIDAS 2); European Digital Identity Wallet Architecture and Reference Framework.

הזדהות לאומית – האקו-סיסטם הישראלי

היכולת להעניק לתושב ייצוג דיגיטלי מהימן נשענת בראש ובראשונה על קיומה של **זהות יסודית** (Foundational Identity), ועל היכולת לקשור באופן מהימן בין זהות זו לבין הייצוג הדיגיטלי המשמש את התושב במרחב המקוון. קשר זה נבנה לאורך מחזור החיים של הזהות - החל משלב הרישום והוכחת הזהות (Identity Proofing) דרך הנפקת אמצעי הזיהוי וההזדהות, ועד לאימות הזהות בעת קבלת שירותים דיגיטליים[7].

בנקודת מוצא זו נהנית מדינת ישראל מיתרון אסטרטגי משמעותי ביחס למדינות רבות בעולם.

מפקד האוכלוסין הראשון נערך בישראל ב-8 לנובמבר 1948. החל ממועד זה ועם אישור פקודת מרשם התושבים, התש"ט-1949, על ידי מועצת המדינה הזמנית, נקבעה מסגרת רישום האוכלוסין והחלה להבנות בישראל תשתית מרכזית לניהול זהויות, אשר ממשיכה לשמש כבסיס למימוש זכויות ולהנגשת שירותים ציבוריים עד היום. תשתית זו כוללת מספר נכסי זהות לאומיים חשובים.

נכסי הזהות הלאומיים של ישראל



בליבת תשתית זו ניצב **מרשם האוכלוסין**, המשמש כמקור המוסמך לנתוני הזהות של תושבי המדינה. המרשם מנהל את מחזור החיים של הזהות - מלידה ועד פטירה - ומספק את הבסיס המשפטי והמנהלי לייצוגו של התושב במדינת ישראל[8].

על בסיס מרשם האוכלוסין פועלת **מערכת לק"ח** (לקוחות חיצוניים), היא מערכת טכנולוגית המאפשרת לגופים ממשלתיים, ציבוריים וגורמים פרטיים מורשים נוספים לאמת בזמן אמת נתוני מרשם בסיסיים מול המרשם, ובכך מספקת שירות לאומי להנגשת מידע מאומת לצורך מתן שירותים. חיבור למערכת מותר רק למי שעומד בתנאים הקבועים בסעיף 29א לחוק מרשם אוכלוסין, התשכ"ה-1965, ולתקנות מכוחו.

[7] ISO/IEC 24760-1:2019

[8] חוק מרשם האוכלוסין, התשכ"ה-1965

הזדהות לאומית – האקו-סיסטם הישראלי

נדבך נוסף בתשתית הוא **מערך התיעוד הביומטרי הלאומי**, המבוסס על **מאגר ביומטרי מרכזי**, במסגרתו מונפקים תעודות זהות ודרכונים חכמים. תשתית זו מחזקת את מהימנות תהליך הוכחת הזהות, מצמצמת את הסיכון לזיוף ולהתחזות ומאפשרת להעניק רמת אמון גבוהה לזהות היסודית של התושב[9].

את החיבור בין הזהות היסודית לבין המרחב הדיגיטלי משלימה **מערכת ההזדהות הלאומית**[10], זוהי מערכת פדרטיבית המאפשרת לתושב להזדהות באופן מאובטח לשירותים ממשלתיים וציבוריים באמצעות ייצוג דיגיטלי הנשען על זהותו היסודית, ולקבל שירותים בהתבסס על תהליכי אימות מול המערכת.

מערכות אלה נחשבות תשתיות מדינה קריטיות. **אבטחתן וחוסנן מהווים רכיב מרכזי בביטחון הדיגיטלי של מדינת ישראל, ועל כן הן נהנות ממעטפת הגנה מתקדמת והנחיה וליווי מקצועיים של הגופים הממשלתיים האמונים על אבטחתן**[11].

ניהולן של התשתיות הלאומיות מבוצע בידי מספר גופים ממשלתיים, ובהם רשות האוכלוסין וההגירה, הרשות לניהול המאגר הביומטרי, מערך הדיגיטל הלאומי ומערך הסייבר הלאומי, הפועלים בהתאם לאחריותם הסטטוטורית ובממשקי עבודה מורכבים.

ציוני דרך בתשתית הזהות הלאומית



שילובם של נכסי זהות לאומיים אלה מעניק לישראל בסיס מוסדי וטכנולוגי מתקדם, אשר מדינות רבות בעולם אינן מחזיקות במלואו. במדינות רבות אין מרשם אוכלוסין מרכזי, אין תשתית תיעוד לאומית אחודה או שאין מערכת הזדהות לאומית מרכזית. שונות זו נובעת מגודל המדינה והיקף האוכלוסייה (שטח והיקף קטן של האוכלוסייה הוא יתרון) וכן מהבדלים היסטוריים, משפטיים וחברתיים בתפיסת היחסים שבין המדינה לבין הפרט.

[9] חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009.

[10] מערכת ההזדהות הלאומית הוקמה על ידי מערך הדיגיטל בשנת 2020 בהתאם להחלטת ממשלה 2097 מיום 10/10/2014

[11] חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן: "החוק להסדרת הבטחון").

עם זאת, קיומם של נכסי יסוד אלה אינו מבטיח, כשלעצמו, מיצוי מלא של הפוטנציאל הגלום בהם. **האתגר העומד כיום בפני מדינת ישראל אינו הקמת תשתית זהות יסודית חדשה, אלא חיבורם של הנכסים הקיימים למערכת אחת, אחודה ומתואמת, וקידום כלים דיגיטליים מתקדמים, שיאפשרו לתושב ולמשק להסתמך על ייצוג דיגיטלי אחיד, מהימן ומאובטח לאורך כל מחזור החיים של הזהות.**

מודלים בעולם - מגמות בין-לאומיות במודלים של זהות דיגיטלית

במבט כלל עולמי, ניכרת מגמה ברורה של מעבר ממנגנוני הזדהות נקודתיים לתשתיות זהות דיגיטליות רחבות ואחודות, המאפשרות צריכת שירותים ציבוריים ופרטיים כאחד. אף על פי שקיימת שונות במימוש, ניתן לאפיין את התפיסה ה"מבנית" להזדהות הדיגיטליות בעולם כיום באמצעות שלושה מודלים מרכזיים:

מודל 1

מודל זהות ממשלתי מרכזי

המדינה משמשת כגורם המרכזי לניהול, הנפקה ואימות של הזהות הדיגיטלית, באמצעות תשתית לאומית אחודה עבור כלל המשק.

- אסטוניה • eID
- סינגפור • Singapass

יתרונות

- עוגן זהות לאומי ברמת אמון גבוהה
- זיקה ישירה למערכת המדינה ולמקורות זהות מוסמכים

אתגרים

- מחייב יכולות ממשלתיות משמעותיות לניהול, פיתוח והרחבת השירותים.
- נדרשים מנגנונים שיאפשרו אימוץ רחב גם מחוץ למגזר הציבורי

מודל 2

מודל ריכוזי בהובלת השוק הפרטי

ספקי זהות פרטיים, כגון בנקים או חברות טכנולוגיה, מספקים פתרונות הזדהות דיגיטליים המשמשים לצריכת שירותים ציבוריים ולעיתים אף ממשלתיים

בלגיה • itsme

הוקמה על ידי המערכת הפיננסית ומשמשת היום כפלטפורמה המרכזית (כמעט בלעדית) להזדהות דיגיטלית במדינה, עליה נשענת גם הממשלה.

אוסטרליה • ConnectID

הוקם על ידי הגופים הפיננסים עבור גופים פיננסיים ומספק היום שירות הזדהות דיגיטלי גם עבור גופים נוספים במשק.

יתרונות

- מינוף תשתיות קיימות במגזר הפרטי
- חוויית משתמש גבוהה ואימוץ מהיר יחסית

אתגרים

- מורכבות ביחס למודל העסקי
- ניהול סיכוני תלות בספקים פרטיים והבטחת קיימות ארוכת טווח של המערכת

מודל 3

מודל משולב - תשתית ממשלתית עם שכבה מבוזרת

על פי מודל זה מוגדרים כללי האמון, התקינה והרגולציה, והמדינה יכולה להחליט האם להקים את הפלטפורמה בעצמה או להפעיל מודל רישוי של גופים מוסמכים להקמת פלטפורמה כזו, אשר כפופים לאותם כללים ותהליכי פיקוח

איחוד אירופי • eIDAS

רגולצייה העוסקת בזיהוי אלקטרוני ושירותי אמון לזיהוי וחתימה באירופה ומקדמת את הארנק האירופי לזהות דיגיטלית (European Digital Identity Wallet[12])

יתרונות

- פרטיות, מזעור מידע, שיתוף מידע סלקטיבי ושקיפות גבוהה עבור המשתמש
- רשת אמון בין מדינות אירופה והכרה הדדית, לרבות ע"י גופים ציבוריים ופרטיים מסוימים
- שירות טוב יותר לתושב

אתגרים

- אתגרים מורכבים של הקמת רשת אמון רחבה מבוזרת וממשל רב-משתתפים
- מורכבות רבה בתהליכי הפיקוח וניהול סיכוני סייבר

הבחינה הבין לאומית מלמדת כי אין מודל אחיד המתאים לכל המדינות, וכי בחירת המודל מושפעת מנקודת הפתיחה הלאומית, מהנכסים הקיימים ומהיעדים האסטרטגיים. נקודת הפתיחה של מדינת ישראל, כאמור, היא מודל ריכוזי שנשען על זהות יסודית חזקה ונכסי זהות לאומיים המונגשים היום דיגיטלית בדרכים שונות, כאשר נדרש שיפור בתהליכים אלה.

[12] רגולציה זו קודמה על ידי האיחוד האירופי ב 2014, ובשנת 2024 הוסיפה את נושא ארנק הזהויות הדיגיטלי (eIDAS2) המחייבת את מדינות אירופה לספק לפחות ארנק אחד, בהתאם לפרמטרים שנקבעו ברגולציה, בשנים 2026-2027.

פערים ואתגרים באקו-סיסטם הישראלי

למרות בסיס הנכסים הלאומי הייחודי של מדינת ישראל, מיצוי מלוא הפוטנציאל של הזהות הדיגיטלית אינו מתאפשר כיום באופן מלא. לאורך השנים התפתחו בישראל מספר תשתיות ומנגנונים שנועדו לתת מענה לצרכים שונים: ניהול זהות יסודית, הנפקת תיעוד, אימות נתונים ומתן גישה לשירותים דיגיטליים. עם זאת, בהיעדר תפיסה אסטרטגית אחודה המגדירה את יחסי הגומלין בין רכיבים אלה, נוצרו פערים מבניים המגבילים את יכולת המדינה לספק לתושב ייצוג דיגיטלי אחיד, מהימן ונגיש.

פער במשילות והגדרת אחריות

לאורך השנים התפתחו מרכיבי הזהות הדיגיטלית תחת אחריותם של מספר גופים ממשלתיים, בהתאם לתפקידיהם ולסמכויותיהם. מבנה זה אפשר את פיתוחן של יכולות משמעותיות, אך לצד זאת יצר מורכבות בניהול הממשקים בין הגופים, בקביעת מדיניות אחידה ובהגדרת אחריות כוללת למרחב הזהות הדיגיטלית.

היעדר מסגרת משילות לאומית כוללת הקשתה על יצירת תפיסה אחודה ביחס למינוף נכסי הזהות הלאומיים, לקביעת סדרי עדיפויות ולהרחבת השימוש בתשתיות הקיימות עבור כלל מגזרי המשק.

פער במימוש הקשר בין הזהות היסודית לייצוג הדיגיטלי

כאמור, אחד התהליכים המורכבים הוא החיבור בין הזהות היסודית לזהות הדיגיטלית. לאורך השנים, חסמים טכנולוגיים, משפטיים, ארגוניים ותפעוליים, הכבידו על היכולת לייצר קשר הדוק יותר בין זהויות אלה, עבור הממשלה עצמה ועבור המשק. אף שמערכת ההזדהות הדיגיטלית נשענת על מרשם האוכלוסין, קיים פער מסוים ביחס לרישום ותוקף הזהות, הנובע בעיקר מקשיים תפעוליים, זמינות והקשר בין המערכות.

חסמים אחרים עיכבו את היכולת לעשות שימוש רחב יותר בתיעוד הביומטרי הלאומי לצורך אימות זהות דיגיטלי חזק, לתהליכי ההרשמה הדיגיטליים, בפרט במערכת ההזדהות הלאומית. מערכת זו אינה מקבלת כיום את החיזוק מתהליך האימות מול התיעוד הלאומי, כלי חשוב לחיזוק תהליכי הרישום שהיא מנהלת.

כתוצאה מכך, השירותים הדיגיטליים נשענים כיום על פתרונות הזדהות שאינם אחידים, אינם מבוססים תמיד על אותה רמת אמון ואינם מאפשרים הסתמכות מלאה על הזהות היסודית של התושב.

פער בניהול הייצוג הדיגיטלי ובחוויית משתמש

בהיעדר ייצוג דיגיטלי לאומי אחוד ונגיש, התפתחו לאורך השנים ריבוי חשבונות משתמש, תהליכי הרשמה נפרדים ומנגנוני הזדהות שונים מול גופים ציבוריים ופרטיים.

מציאות זו יוצרת עומס על התושב, מגדילה את הצורך בניהול פרטי התחברות רבים ומרחיבה את משטח התקיפה האפשרי. בנוסף, היא מגבילה את היכולת של התושב לשלוט במידע האישי שלו ולנהל באופן פשוט ומאובטח את האישורים והמסמכים הדיגיטליים שלו.

העדר תפיסה ביחס לתפקיד הממשלה ביצירת תשתית אמון למשק

הממשלה היום מחצינה את נכסיה הלאומיים באמצעות שתי מערכות הפועלות באופן מקוון, אשר נותנות יכולת הסתמכות לגופים מסוימים. בדיקת אימות פרטים מול מערכת לק"ח (של רשות האוכלוסין), הנותנת שירות לכ-408 גופים, כולל גופים פרטיים ובפרט המגזר הפיננסי[13], אך אינה מבצעת "אימות זהות" כפעולה אקטיבית הקושרת את המשתמש הדיגיטלי לזהותו במרשם.

מערכת ההזדהות הלאומית (המופעלת ע"י מערך הדיגיטל הלאומי) מבצעת תהליכי אימות זהות ובדיקת פרטים, אך נשענים עליה בעיקר גופים ממשלתיים וציבוריים.

כלומר, קיימת כפילות מסוימת כאשר שני גופים ממשלתיים פועלים במקביל למול המשק על מנת לבסס אמינות זהותו של אדם (בין אם על ידי אימות פרטי מרשם או על ידי זהות דיגיטלית אמינה), בצורות שונות, ללא תפיסה סדורה בנושא זה והאמצעים בהם נעשה שימוש אינם מתקדמים דיים מבחינה דיגיטלית.

היעדר מסגרת מוסדרת להרחבת השימוש לגופים חוץ ממשלתיים, לצד חסמים רגולטוריים במגזרים מסוימים, מגביל את היכולת של המשק להסתמך על זהות דיגיטלית לאומית בתהליכים שאינם ממשלתיים, אך המחייבים רמת אמון גבוהה, לרבות שירותים פיננסיים ובריאותיים.

[13] 57 גופים פיננסיים, 109 רשויות מקומיות, כ- 60 גופים ציבוריים.

פער בהתמודדות עם איומי העתיד

התפתחותן של טכנולוגיות מתקדמות, ובהן בינה מלאכותית יוצרת, מחייבות מעבר מתפיסה המתמקדת בהגנה על מערכות בלבד לתפיסה רחבה של ניהול סיכוני זהות והונאה.

נדרש חיזוק של יכולות לאומיות לזיהוי מוקדם של פעילות חריגה, ניהול סיכוני התחזות, ניטור והגנה על זהויות דיגיטליות לאורך מחזור החיים שלהן, תוך שמירה על פרטיות ואמון הציבור, בהתבסס על כלי בינה מלאכותית מתקדמים.

פערים אלה מצביעים על הצורך במעבר מתפיסה של אוסף מערכות ותהליכים נפרדים למודל לאומי משולב, שבו הזהות היסודית, הייצוג הדיגיטלי, מנגנוני ההזדהות והשירותים הציבוריים והפרטיים פועלים כחלק מתשתית אמון אחת.

אסטרטגיה זו נועדה לקדם את השירות לתושב ולחזק את הייצוג הדיגיטלי שלו, במטרה להביא להעלאת חוסן, ולערך חברתי וכלכלי עבור ישראל לטובת כלל המשק.

כיווני הפעולה המוצגים במסמך זה נועדו לתת מענה לפערים המנויים לעיל, באמצעות איגום המערכת הממשלתית וגבולות הגזרה הארגוניים, גיבוש תפיסה ביחס לתפקידה של הממשלה מול המשק ואופן החצנת נכסי הזהות הלאומיים, חיזוק תהליכי ההזדהות ואופטימיזציה של הכלים הדיגיטליים, הגברת השקיפות והאמון הציבורי.



חזון לאומי והעקרונות למימושו

ההתפתחויות הטכנולוגיות, השינויים במרחב האיומים והתרחבות השירותים הדיגיטליים מחייבים את מדינת ישראל לעבור משלב של פיתוח יכולות נקודתיות לשלב של תפיסה לאומית כוללת לניהול הזהות הדיגיטלית.

מדינת ישראל רואה במערכת ההזדהות הלאומית תשתית קריטית, ואמצעי משמעותי לצמיחה הכלכלית ובקידום השירותים הדיגיטליים. המערכת תשמש תשתית אמון משותפת לשירותים במגזר הציבורי והפרטי, תאפשר הסתמכות על זהות דיגיטלית מהימנה ותתמוך במתן שירותים באופן פשוט, נגיש ובטוח. המשך פיתוחה יחזק את ההגנה מפני איומי סייבר והונאות זהות, יאפשר אימוץ שירותים ומודלים חדשניים ויתרום לחיזוק מעמדה של ישראל כמדינה מובילה בתחום החדשנות הדיגיטלית.

מתוך תפיסה זו גובש החזון הלאומי:

"זהות דיגיטלית אחת, במרחב בטוח של אפשרויות"

מימוש החזון יישען על אקו-סיסטם דיגיטלי מתקדם, מבוסס תקנים ושותפויות בין מגזריות, אשר יחזק את החוסן הלאומי, יעודד חדשנות ויתמוך בצמיחה כלכלית וחברתית.

חזון לאומי והעקרונות למימושו

החזון מבוסס על ארבעה עקרונות יסוד:

אמון

חיזוק מערכת הזדהות דיגיטלית כך שתאפשר הסתמכות על אמינות הזהויות הפועלות במרחב הדיגיטלי. עיקרון זה יתממש באמצעות תשתית המבוססת על סטנדרטים ותקנים בינלאומיים, מנגנוני ממשל מתקדמים, ושקיפות, אשר יחזקו את אמון הציבור והגופים המשתמשים בה.

הגנת סייבר

חיזוק ופיתוח יכולות מתקדמות להגנה על מערכת ההזדהות הלאומית מפני איומי סייבר, הונאות זהות ושימוש לרעה במידע, תוך ניהול סיכונים מתקדם ושמירה על רציפות תפקודית של השירותים החיוניים גם בתרחישי קיצון.

שימושיות

יצירת חוויית הזדהות פשוטה, נגישה ואחידה לכלל המשתמשים. עיקרון זה יתממש באמצעות הפחתת חסמים בירוקרטיים, איחוד תהליכי ההזדהות ומתן אפשרות לגישה מאובטחת לשירותים מכל מקום, בכל זמן ובאמצעות מגוון אמצעי קצה, תוך צמצום הצורך בריבוי חשבונות, זהויות וסיסמאות.

חדשנות וגמישות טכנולוגית

המשך פיתוח והתאמתה של מערכת מודולרית, פתוחה ומבוססת תקנים, המאפשרת התאמה מהירה להתפתחויות טכנולוגיות, שילוב פתרונות חדשניים, קידום שיתופי פעולה בין המגזר הציבורי והפרטי ותמיכה במודלים מתקדמים של שירותים דיגיטליים.

בהתאם לחזון, האסטרטגיה מגדירה שלושה מישורי פעולה המשלימים זה את זה: זהות אחת חזקה ונקודת פניה אחת לממשלה; אופטימיזציה של כלי ההזדהות; הרחבת יכולות ניהול הייצוג הדיגיטלי עבור התושב מול גופים מסתמכים שאינם ממשלתיים, תוך שמירה על פרטיות, אבטחת מידע וחלוקת אחריות בין הגורמים השונים באקו-סיסטם החדש.

מישור ראשון
זהות אחת חזקה ונקודת פניה אחת לממשלה

מישור שני
אופטימיזציה של כלי ההזדהות

מישור שלישי
הרחבת יכולות ניהול הייצוג הדיגיטלי מול גופים מסתמכים שאינם ממשלתיים



פרק ראשון: זהות אחת בטוחה

המרחב הדיגיטלי במדינת ישראל נשען כיום על מגוון מנגנוני הזדהות אשר אינם מקיימים תאימות מלאה ביניהם, במערכת הממשלתית ומחוצה לה.

במערכות הממשלתיות המרכזיות המשמשות לתהליכי הזיהוי קיימת כפילות ופער מסוים בין הזהות היסודית לייצוג הדיגיטלי. אף על פי שמשרדי ממשלה רבים הצטרפו למערכת ההזדהות הלאומית, עדיין קיימים מאגרים רבים לצרכי זיהוי (לרבות מאגרים ביומטריים), לרוחב הממשלה.

כמו כן, לצד התיעוד הביומטרי, משרדי הממשלה מוסיפים להנפיק תעודות רבות אחרות בתהליכים חלשים יותר, כאשר לא ניתן לאמת ברמת ביטחון מספקת את האוחז בהן. הדבר מחייב את התושב לנהל ריבוי זהויות ואמצעי הזדהות, יוצר כפילות תשתיות ומגדיל את הסיכון להונאות ולהתחזות ולסיכוני סייבר.

פרק זה מגדיר את המהלכים הנדרשים לחיזוק אמינותה, אבטחתה, ועמידותה של הזהות הדיגיטלית, הנשענת על הזהות היסודית של התושב ומהווה בסיס למתן שירותים דיגיטליים ברמת אמון גבוהה.

מימוש מהלכים אלה יבוצע בהתאם למדיניות הלאומית להזדהות בטוחה והקווים המנחים לה[14], אשר מהווים מסגרת מקצועית ונורמטיבית, ובסיס אחיד לקביעת עקרונות ודרישות ורמות אמון בתהליכי הזדהות דיגיטלית לשירותים דיגיטליים בהתאם לרמת הסיכון ומאפייני השירות, בישראל, ובהתאם להנחיות הגנת הסייבר של הקצין המוסמך (מערך הסייבר הלאומי) לפי החוק.

המיקוד בפרק זה ניתן להיבטי הביטחון, התאימות והייחודיות של הייצוג הדיגיטלי על גבי הפלטפורמה הממשלתית. בהמשך המסמך ניתנו דגשים הנוגעים לפרטיות, שקיפות, אחריות והיבטים רלוונטיים נוספים בעלי חשיבות לאמינות הזיהוי.

[14] https://www.gov.il/he/pages/national_policy_for_secure_identification



1.1 היעד הראשון: כתובת אחת בממשלה להנגשת הייצוג הדיגיטלי למשתמשים ולגופים המסתמכים

רשות האוכלוסין היא הגוף האחראי על קביעת הזהות היסודית של התושב בישראל, כאשר מערכת ההזדהות הלאומית, המנוהלת על ידי מערך הדיגיטל הלאומי, היא הפלטפורמה הטבעית לניהול הזהויות כייצוגים דיגיטליים ולהנגשת הנכסים המדינתיים, המבססים זהויות אלה במרחב הדיגיטלי. זוהי תשתית פדרטיבית רוחבית עליה נשענים גופים מסתמכים בישראל (כיום גופים ממשלתיים וציבוריים) כדי לאמת זהויות דיגיטליות לצורך קבלת שירותים דיגיטליים, מידע ומסמכים שונים.

למרות ההתקדמות בקידום השירותים הדיגיטליים, פריסתה של המערכת בממשלה ובמגזר הציבורי עדיין אינה מלאה. כדי להרחיב ולחזק את תפקידה של מערכת ההזדהות הלאומית תקודם **הרחבת הפריסה של המערכת בממשלה ובמגזר הציבורי** - יצירת תוכנית לחיבור כלל גופי הממשלה וגופים ציבוריים למערכת ההזדהות הלאומית. כלל גופי הממשלה יחוברו בהתאם לתכנית שיוביל מערך הדיגיטל הלאומי. ביחס לגופים הציבוריים שאינם ממשלתיים, ומאחר שזוהי קבוצה רחבה והטרוגנית, הכוללת גופים בעלי מאפיינים, תחומי פעילות, היקפי שירות ורמות סיכון שונות, השיקולים לחיבורם למערכת לא יהיה "אוטומטי" או אחיד.

במסגרת התוכנית, בהובלת מערך הדיגיטל הלאומי, יגובשו קריטריונים ומנגנון תיעדוף, לחיבור הגופים, אשר יתבססו, בין היתר על היקף הפעילות והשירותים הדיגיטליים והערך הציבורי שבהצטרפות, ההיבטים המשפטיים וההתאמה הטכנולוגית והתפעולית של הגוף המדובר. התוכנית תפעל לביסוס מערכת ההזדהות הלאומית כ"ברירת המחדל" להזדהות בשירותים ציבוריים, תוך צמצום הדרגתי של מנגנוני הזדהות מבוזרים שאינם נדרשים.

1.2 יעד שני: הגנת סייבר והזדהות בטוחה

ההתפתחות המהירה של שירותים דיגיטליים, לצד חדירתן של בינה מלאכותית יוצרת (Generative AI) ומערכות אוטונומיות, משנה את מאפייני האיום במרחב הדיגיטלי. מוקד התקיפה עובר מפריצה לתשתיות אל ניסיון להתחזות למשתמשים לגיטימיים באמצעות זהויות גנובות, מזויפות או סינתטיות.



כדי לממש יעד זה יש לקדם את המהלכים הבאים:

- **חיזוק מנגנוני האימות וההגנה** - הרחבת השימוש בתשתית ההזדהות הלאומית תחייב חיזוק מתמיד של מנגנוני האימות, ניהול הזהויות והגנת הסייבר ואבטחת המידע, בהתאם למדיניות הלאומית להזדהות בטוחה ובהתבסס על תקינה ופרקטיקות בין-לאומיות עדכניות[15]. במסגרת זו תבחן היכולת לייצר תהליכים נוספים המאפשרים רמות אמון גבוהות בתהליכי הרשמה ואימות[16], המאפשרות הסתמכות על הזהות הדיגיטלית גם עבור שירותים רגישים, זאת בשים לב לפשטות ונגישות תהליך ההזדהות עבור התושב. בכלל זה יבחנו תהליכי רישום שייעשו גם באופן פיזי מול עמדות שירות מפוקחות או אמצעים דומים אחרים.
- **חיזוק מעטפת הגנת הסייבר (Cyber by Design)** – הרחבת פעילותה של מערכת ההזדהות הלאומית וביסוסה כמרכיב ליבה בתשתיות המדינה הקריטיות, מחייבים את הידוק מעטפת ההגנה, תוך הטמעת עקרונות Cyber by Design, לרבות מנגנונים לשמירה על רציפות תפקודית, יתירות והתאוששות מאירועי קיצון.
- **מעבר מתפיסת אבטחה המתמקדת בפעולות נקודתיות להגנה על מערכות, לתפיסה המתמקדת בניהול מחזור החיים של הזהות הדיגיטלית ואמינות הזהות.** לשם כך נדרשת יכולת לאומית מתקדמת אשר תפעל באופן רציף ותשלב יכולות סייבר, ניתוח (אנליטיקה) ובינה מלאכותית אשר תוכל לסייע במעקב אחר האיומים המתפתחים, הערכת סיכונים וסיכולם לאורך מחזור חייה של הזהות/הייצוג הדיגיטלי (Identity Threat & Fraud Management). בהקשר זה ייבחנו האפשרויות לשיתוף אינדקציות המעידות על הונאה עם גופים רלוונטיים וכן הקמת יכולת לזיהוי, ניתוח ותגובה:

01

זיהוי אנומליות

ניטור רציף של פעילות במערכת באמצעות מנגנונים מתקדמים לאיתור חריגות, דפוסי התנהגות חשודים ואינדיקציות להונאה בזמן אמת.

02

ניתוח ואימות

בחינה מעמיקה של האירועים באמצעות שילוב בין מומחי סייבר, מודיעין וכלים אנליטיים מתקדמים, לצורך הערכת הסיכון ואימות החשד.

03

תגובה והפקת לקחים

תהליכים מובנים לטיפול בחריגות ואנומליות, וכן הפקת לקחים ועדכון מתמשך של מנגנוני הזיהוי וההגנה, באופן שישפר את יכולת ההתמודדות עם איומים חדשים ויפחית התראות שווא.

[15] כגון NIST SP 800-63-4, ובהתאם לקווים המנחים למדיניות הלאומית להזדהות בטוחה

[16] יכולת לבצע תהליכי הרשמה ואימות ברמת סמך/ רמת וודאות 4, בהתאם למדיניות הלאומית להזדהות בטוחה.



גישה זו תאפשר למדינה להגן באופן פרואקטיבי על זהויות התושבים, לחזק את אמון הציבור ולהבטיח את רציפות השירותים הדיגיטליים גם לנוכח איומים מתפתחים.

- **תיעוד לאומי כעוגן מרכזי להרשמה ואימות במערכת ההזדהות הלאומית -** מערך הדיגיטל הלאומי ורשות האוכלוסין וההגירה מקדמים פיתוח יישום לאימות ביומטרי מתקדם מול התיעוד הלאומי. היישום ישמש כמנגנון מרכזי לרישום למערכת ההזדהות הלאומית ולביצוע פעולות הדורשות רמת אמון גבוהה. הפתרון, המפותח בשיתוף שני הגופים, ישולב בהמשך גם באזור האישי הממשלתי ובארנק הדיגיטלי הלאומי (להלן), כחלק מחוויית שירות מאובטחת, פשוטה ורציפה.

רשות האוכלוסין תפתח אמצעים נוספים אשר יאפשרו אימות ובדיקת אותנטיקציה מול תעודות הזהות הפיזיות באמצעות כלים דיגיטליים, אשר ישולבו במערכת ההזדהות הלאומית.

1.3 יעד שלישי: תאימות בין הזהות היסודית לייצוג הדיגיטלי

אמינותה של הזהות הדיגיטלית נשענת על זיקה ישירה, מאומתת ומתמשכת לזהותו היסודית של התושב, הניתנת לניהול לאורך מחזור החיים של הזהות ושל אמצעי ההזדהות. מרשם האוכלוסין, מהווה את המקור הרשמי והעוגן המשפטי לזהות במדינת ישראל. לפיכך, כל ייצוג דיגיטלי יתבסס על נתונים מוסמכים, מדויקים ועדכניים, ויכלול רק את הנתונים או מאפייני הזהות הנדרשים לתכלית שלשמה הוא משמש.

לשם כך תיושם תאימות בין הזהות היסודית במרשם האוכלוסין לבין הייצוג הדיגיטלי במערכת, באמצעות מנגנון סנכרון רציף ועדכני, תוך התאמה לאילוצים תפעוליים, לרבות ביחס לתוקף תעודת הזהות שמחזיק התושב. יקבעו מנגנונים לעדכון, לתיקוף או לביטול של ייצוגים דיגיטליים בהתאם לשינויים במקורות המידע, כך שבמועד ההסתמכות ניתן יהיה לוודא כי המידע תקף ועדכני.

1.4 יעד רביעי: היערכות לעידן הפוסט קוואנטום

התפתחות המחשוב הקוונטי צפויה בשנים הקרובות לאתגר את עמידותם של תהליכים מרכזיים בעולם ההזדהות ובפרט את התשתיות המשמשות לחתימה דיגיטלית, לאימות זהויות (אותנטיקציה), לתוקפם של אמצעי זיהוי ותהליכים דיגיטליים ולתהליכי ההצפנה המרכזיים. על מנת להבטיח את חוסנה של תשתית מערכת ההזדהות הלאומית לאורך זמן, תפעל המדינה להיערכות מוקדמת ולבניית יכולת מעבר הדרגתית לתשתיות העמידות להתקפה מבוססת מחשוב קוונטי: **Post-Quantum Readiness of the National Digital Identity Ecosystem**. היערכות זו תבטיח כי הזהויות הדיגיטליות, מאגרי המידע והתהליכים הדיגיטליים המרכזיים, כמו גם תהליכי ההצפנה, ימשיכו להיות מוגנים גם בעידן הטכנולוגי הבא, ואת יכולתה וגמישותה של המערכת להחליף או לחזק את רכיביה, תוך שמירת אמון הציבור וחוסנה של התשתית הלאומית לאורך שנים.

פרק שני: אופטימיזציה של ניהול הייצוג הדיגיטלי

מערכת ההזדהות הלאומית המתפתחת נדרשת לא רק להבטיח את אמינות הזהות ואת אבטחתה, אלא גם לאפשר לתושב חוויית שירות פשוטה, רציפה ויעילה. ניהול חכם של הייצוג הדיגיטלי מצמצם את הנטל הבירוקרטי, מקצר את זמני קבלת השירות, מפחית את התלות במסמכים פיזיים ומעניק לתושב שליטה רחבה יותר במידע האישי שלו, תוך יישום עקרונות של פרטיות (Privacy by Design).

ארבעת היעדים בפרק זה יקדמו את תשתית הזהות הלאומית ככלי מעשי המשרת את התושב לאורך זמן: ארנק הזדהות דיגיטלי לאומי, העלאת המערכות לענן, שקילות מלאה בין התעודה הפיזית לתעודה הדיגיטלית, שילוב סוכני בינה מלאכותית כמייצגים של משתמשים, יאפשרו לתושב לנהל, להציג ולשתף את ייצוגיו הדיגיטליים באופן מבוקר ובהתאם לצורך.

אופטימיזציה של ניהול הייצוג הדיגיטלי



2.1 יעד ראשון: ארנק זהות דיגיטלי לאומי

מה הארנק מאפשר לתושב

הארנק הדיגיטלי הלאומי יהווה עבור התושב אמצעי מרכזי לניהול ולשימוש בזהותו ובתעודותיו הדיגיטליות, ויאפשר הצגה ושיתוף של מידע מאומת באופן פשוט, מאובטח ומבוקר. מערך הדיגיטל פועל בימים אלה להקמת תשתית הארנק הדיגיטלי הלאומי, שבאמצעותה יוכל התושב להחזיק, לנהל, להציג ולשתף תעודות, אישורים ומסמכים דיגיטליים רשמיים המונפקים על ידי המדינה, **ובראשם תעודת הזהות**, וכן להציג ולהוכיח, בהתאם לצורך, מאפיינים, זכאויות, הרשאות וסטטוסים הנוגעים אליו.

מהימנות ועדכניות הייצוגים

המסמכים והייצוגים הדיגיטליים שיונגשו באמצעות הארנק יונפקו על ידי מקורות מוסמכים ויהוו ייצוגים רשמיים ומאומתים. הארנק יפעל בממשק עם מערכת ההזדהות הלאומית, עם גופים מנפיקים ועם גופים מסתמכים, ויאפשר שימוש בזהות ובמידע מאומת הן במרחב הדיגיטלי והן במפגש הפיזי. תוקפם ועדכניותם של הייצוגים הדיגיטליים ינוהלו באמצעות מנגנוני חתימה, תיקוף, עדכון וביטול, בהתאם למאפייני התעודה ולדרישות הגורם המנפיק.

מעמד תעודת הזהות והדרכון

הארנק יתמוך בשילוב הדרגתי של תעודות, אישורים וייצוגים דיגיטליים ממשלתיים וציבוריים, ובהם תעודת זהות, רישיון נהיגה ותעודות ואישורים נוספים. השימוש בהם יתאפשר מול משרדי הממשלה, הרשויות המקומיות, גופי האכיפה ונותני שירותים במגזר הפרטי, באופן פשוט, מאובטח ומבוקר. לצורך כך יוגדרו מנגנונים מאובטחים לניהול מחזור החיים של הארנק ושל התעודות המוחזקות בו, לרבות הנפקה, הפעלה, עדכון, שחזור, החלפת מכשיר, השעיה וביטול.

הנפקה ◄ הפעלה ◄ עדכון ◄ שחזור

החלפת מכשיר ◄ השעיה ◄ ביטול

עקרונות פרטיות ושליטת המשתמש

שיתוף המידע באמצעות הארנק ייעשה ככל הניתן בשליטת התושב ובהתאם לעקרונות של מזעור מידע, פרטיות מעצם התכנון (Privacy by Design) וחשיפה סלקטיבית (Selective Disclosure). בהתאם לכך, הארנק יאפשר לשתף רק את המידע הנדרש לצורך קבלת שירות, אימות נתון או הוכחת זכאות, מבלי לחשוף מידע עודף שאינו נדרש. כך, לדוגמה, ניתן יהיה להוכיח עמידה בתנאי או מאפיין מסוים מבלי לחשוף את מלוא הנתונים הכלולים בתעודה. לצד זאת, תינתן לתושב שקיפות ביחס לפעולות ולשימושים המתבצעים באמצעות הארנק, בהתאם לדין.

אופטימיזציה של ניהול הייצוג הדיגיטלי



הוכחת תפקיד, אפוטרופוסות וייצוג

מעבר להוכחת זהותו ומאפייניו של התושב, הארנק יאפשר בהדרגה גם הוכחה של הקשרים, סמכויות והרשאות שבהם פועל התושב, כגון היותו בעל תפקיד, אפוטרופוס או מייצג. זאת, באופן שיאפשר להוכיח הן את זהותו של האדם והן את ההקשר או הסמכות שמכוחם הוא פועל.

אקו-סיסטם הארנק

מימוש הארנק יתבסס על אקו-סיסטם הכולל גורמים מנפיקים, האחראים למידע ולתעודות המונפקות; התושב, המחזיק ומנהל את הייצוגים הדיגיטליים; וגופים מסתמכים, המבקשים לאמת את המידע לצורך מתן שירות. במסגרת זו יוגדרו תחומי האחריות, מנגנוני האמון, כללי ההסתמכות וההסדרים הנדרשים בין הגורמים.



ממשקים ואימות לגופים מסתמכים

במקביל לפיתוח הארנק יפותחו תשתיות, ממשקים ואמצעים עבור גופים מסתמכים, שיאפשרו קבלה ואימות של מידע ותעודות דיגיטליות המוצגים באמצעות הארנק, לרבות אימות מקורם, שלמותם ותוקפם, באופן שיצמצם את הסיכון לזיוף, התחזות ושימוש בלתי מורשה. יכולות אלה יתמכו הן בשירותים דיגיטליים מרחוק והן במפגש פיזי ובקרבה, בהתאם לתרחיש השימוש, לתקינה הרלוונטית ולדרישות אבטחת המידע.

ארכיטקטורה מבוזרת ותקינה בינלאומית

במסגרת בניית הארכיטקטורה של תשתית הארנק יבחן מודל הזהות הדיגיטלית המבוזרת **(Decentralized Identity)**, במטרה לצמצם את שמירת המידע באופן מרכזי, לצד הצורך בניטור ובניהול אמין של הזהות הדיגיטלית במערכת, כאמור ביעד 1.2. תשתית הארנק והתעודות הדיגיטליות שיונגשו באמצעותה יתבססו על תקנים ומסגרות בינלאומיות מקובלות במטרה להבטיח תאימות, יכולת פעולה הדדית (Interoperability), גמישות טכנולוגית וצמצום תלות בספקים.

אופטימיזציה של ניהול הייצוג הדיגיטלי



הכרה הדדית עם מדינות אחרות

בטווח הבינוני והארוך תפעל המדינה לקידום יכולת הכרה ושימוש הדדי בתעודות ובאישורים דיגיטליים מול מדינות ותשתיות זהות דיגיטלית מחוץ לישראל, בהתאם למסגרות האמון, התקינה וההסדרים המשפטיים הרלוונטיים.

מעמד תעודת זהות והדרכון

תעודת הזהות והדרכון ימשיכו לשמש כמסמכי הזהות המרכזיים וכבסיס מרכזי לעיגון זהותו של האדם גם במרחב הדיגיטלי ובארנק הדיגיטלי. מסמכים אלה ימשיכו להיות מונפקים גם כמסמכים פיזיים וניתן יהיה להמשיך ולעשות בהם שימוש במתכונתם הקיימת לצד הרחבת השימוש בזהות ובנתונים הנגזרים מהם בממד הדיגיטלי. זאת, באופן שימנף את תשתיות התיעוד הלאומי הקיימות, יחזק את תהליכי ההזדהות והאימות ויאפשר מעבר מאובטח והדרגתי לשירותים מבוססי זהות דיגיטלית.

מעבר הדרגתי ושמירה על הכלה דיגיטלית

תעודות, רישיונות ואישורים נוספים המונפקים על ידי הממשלה וגופים ציבוריים יוכלו לעבור בהדרגה למתכונת דיגיטלית ולהיות מונפקים ומנוהלים באמצעות הארנק הדיגיטלי. בהתאם לסוג התעודה, לצורכי המשתמשים ולדרישות הדין, ניתן יהיה לצמצם בהדרגה את הצורך בהנפקת מקבילות פיזיות, עבור תושבים המעוניינים בכך.

המעבר ייעשה באופן מדורג, תוך שמירה על נגישות, הכלה דיגיטלית ומתן חלופות מתאימות לאוכלוסיות שאינן יכולות או אינן מעוניינות לעשות שימוש באמצעים דיגיטליים, ובמטרה לקדם אימוץ רחב של תעודות ואישורים דיגיטליים בכלל המשק.

דרכון דיגיטלי בארנק הלאומי

לאחר ביסוס הארנק לצורך הנגשת שירותים בישראל, יפעל מערך הדיגיטל, בשיתוף רשות האוכלוסין, לקידום שילובו של דרכון דיגיטלי בארנק הלאומי, בהתאם לתקינה הבינלאומית הרלוונטית[17] ולהתפתחויות בתחום מעברי הגבול בעולם. המהלך יבוצע תוך בחינת ההיבטים המשפטיים, הביטחוניים והטכנולוגיים הנדרשים למימושו.

[17] תקן ICAO אשר מדינות העולם מחוייבות אליו, הניח תכנית מדורגת לדרכונים דיגיטליים



2.2 יעד שני: שקילות מלאה בין התעודה הפיזית לתעודה הדיגיטלית

הנגשת התעודות הממשלתיות בארנק הדיגיטלי, ובראשן תעודת הזהות, היא תנאי הכרחי, אך אינה מספיקה כשלעצמה. כדי שהייצוג הדיגיטלי ישמש חלופה מלאה לתיעוד הפיזי, עליו ליהנות ממעמד זה, גם במפגש הפיזי כאשר נדרשת הצגת תעודה רשמית.

לשם כך, תגבש המדינה מסגרת משילות החותרת לתוצאה זו, לרבות בחינת הצורך בתיקוני החקיקה הנדרשים להכרה בייצוג הדיגיטלי של התיעוד הלאומי,

כך שתעודת זהות דיגיטלית תהיה שוות ערך לתעודת הזהות הפיזית. עם השלמת מהלך זה, יוכלו משרדי הממשלה, רשויות מקומיות, גופי אכיפה ונותני שירותים במגזר הפרטי, להסתמך על התעודה הדיגיטלית.

2.3 יעד שלישי: מודרניזציה לתשתיות ההזדהות הלאומיות

התרחבות השירותים הדיגיטליים מחייבת את תשתית המערכת לעבד נתונים בהיקפים גדלים והולכים, תוך שמירה על זמינות גבוהה וזמני תגובה קצרים. הישענות בלעדית על תשתיות מסורתיות (On Premise) מגבילה את יכולת ההתרחבות של המערכת, יוצרת צווארי בקבוק תפעוליים ומקשה על שילוב טכנולוגיות חדשות.

לשם כך תקודם מודרניזציה מקיפה של תשתיות הליבה של מערכת ההזדהות הלאומית ושל מערכות רשות האוכלוסין עמן היא מסנכרנת.

הענן ישמש כאמצעי טכנולוגי מרכזי להשגת "גמישות תפעולית" באמצעות אימוץ תפיסה היברידית. מודל היברידי יאפשר שילוב מיטבי בין משאבי ענן מתקדמים לבין החזקת רכיבי ליבה ונתונים רגישים בסביבות מקומיות ומאובטחות, תוך ניהול סיכונים הדוק. תפיסה זו תבטיח יכולת עיבוד גמישה, הפחתת עומסים, שיפור זמני האימות, וביצוע סנכרון מהיר ואינטגרטיבי בין מערכות הממשלה.

כעיקרון יסוד אסטרטגי, מעבר של רכיבים או שירותים שונים לענן יבוצע תוך שמירה על הריבונות הדיגיטלית והרציפות התפקודית, נוכח סיווגן של המערכות כתשתית קריטית, ובהתאם להנחיות הקצין המוסמך לפי חוק להסדרת הביטחון בגופים ציבוריים התשנ"ח-1998.

תשתית זו הפועלת באופן היברידי, תחזק את העמידות והיתירות התפעולית, ותאפשר שילוב בטוח בסטנדרטים מחמירים להגנת הפרטיות ואבטחת המידע.



2.4 יעד רביעי: זהויות אוטונומיות הפועלות בשם המשתמשים – AI Agents

ההתפתחות המואצת של סוכני בינה מלאכותית (AI Agents) צפויה לשנות את אופן הפעולה במרחב הדיגיטלי, לצד פעולות המתבצעות באופן ישיר על ידי המשתמש. סוכני בינה מלאכותית יפעלו בשם המשתמשים, יבצעו עברם פעולות ויקיימו במקומם אינטראקציות עם מערכות ונותני שירותים ומערכות הפועלות במרחב הדיגיטלי ידרשו לנהל יכולת זו ולנטר אותה.

התפתחות זו מחייבת הרחבה של תפיסת ה"ייצוג הדיגיטלי", כך שתאפשר בעתיד גם זיהוי וניהול של ישויות דיגיטליות הפועלות בשם המשתמשים, ואת היכולת למקסם את הערך השירותי והכלכלי הטמון בהם לצד ההגנה עליהם ועל המערכת. במסגרת זו תבחן האפשרות לשלב סוכני בינה מלאכותית כחלק ממערכת ההזדהות הלאומית, תוך יצירת זיקה מהימנה בין ה"סוכן" לבין האדם – "המשתמש", שבשמו הוא פועל.

נושא זה הוא חלק מתחום רחב יותר של NHI (Non Human Identity) אשר נוגע גם לזיהוי של מערכות/רכיבים והוא משפיע על ניהול מערכות ממוחשבות באופן רוחבי. למען הסר ספק, אסטרטגיה זו מתמקדת בייצוג הדיגיטלי של משתמשי מערכת ההזדהות הלאומית האנושיים, גם באמצעות סוכני בינה מלאכותית.

שילוב יכולת זו תחייב בחינה של שאלות חדשניות הנוגעות לשאלת ההסמכה, ההרשאה במערכת וביטולה, אימות הסוכן והקשר הרציף שלו למשתמש, כיצד הוא פועל לצד או חלף הייצוג הדיגיטלי ה"קלאסי" ושמירה על מהימנות המערכת והייצוגים הדיגיטליים. בחינת שילובן של זהויות אוטונומיות ייעשה תוך שמירה על עקרונות הפרטיות, אבטחת המידע, הגנת המשתמש ובהתאם להתפתחויות הטכנולוגיות והתקינה המקובלים העולם.



פרק שלישי: הרחבת השימוש במערכת ההזדהות הלאומית עבור גופים מסתמכים שאינם ממשלתיים

בהתאם לאסטרטגיה זו, הרחבת השימוש במערכת ההזדהות הלאומית תעשה בשלב הראשון עבור גופי הממשלה וגופים ציבוריים, תוך הבחנה בין סוגי הגופים והשירותים השונים.

ביחס לגופים פרטיים, נוהלו מספר מעגלי השיח, בפרט עם המגזר הפיננסי ומגזר הבריאות, במסגרתם עלה צורך אמיתי לחיזוק תהליכי ההזדהות בשלב ההרשמה ובנקודות רגישות אחרות בתהליך אימות הזהות, מתוך הבנה של הקושי המתגבר במרחב הווירטואלי בביסוס הזהות של המשתמש, ומגמת ההונאות ההולכת וגדלה, כמתואר במסמך זה.

החיזוק הנדרש יכול להתבצע באמצעות הרחבת השימוש במערכת ההזדהות הלאומית לגופים חוץ ממשלתיים ולמגזר הפרטי. הרחבה זו מהווה נדבך מרכזי במימוש הכלכלה הדיגיטלית של מדינת ישראל. בעולם שבו הונאות זהות הופכות מתוחכמות יותר, בין היתר באמצעות בינה מלאכותית, הסתמכות על מנגנוני זיהוי מבוזרים מגדילה את החשיפה לסיכוני התחזות, מכבידה על הציבור ופוגעת ביעילות השירותים.

כיוון הפעולה המרכזי המוצג כאן, הוא המשך ההישענות על המודל הריכוזי הקיים בישראל והרחבתו לטובת גופים שאינם ממשלתיים, תוך גידור הסיכונים השונים והתייחסות לאתגרים רגולטוריים, ההיבטים הכלכליים ולהיבטי הפרטיות והאחריות.



אנו סבורים כי זהו הכיוון הנכון עבור מדינת ישראל, לאחר בחינת המודלים האחרים, מהסיבות העיקריות הבאות:

1. הגנה על נכסי הזהות מהווה תפקיד מסורתי וליבתי של המדינה מיום הקמתה. התפיסה לגבי התשתיות עליהן מנוהלת הזהות היסודית והזהות הדיגיטלית היא כמדובר בתשתיות מדינה קריטיות ובנכסים שעל המדינה חובה להגן עליהם. לפיכך, מבחינה ערכית נכון לשמר תפיסה זו לצד חשיבה על מינוף נכסים באופן שאינו פוגע בשלמותם.

2. במציאות הישראלית, נכסי הזהות מנוהלים על ידי גופי הממשלה וכבר היום מונגשים לגופים מסתמכים שאינם ממשלתיים, כולל גופים במגזר הפיננסי וגופים פרטיים אחרים (באמצעות מערכת לק"ח). האופן שבו הדבר נעשה אינו אופטימאלי, כמתואר לעיל, וכיווני הפעולה המוצעים באסטרטגיה זו הם המשך **התפתחות טבעית של המודל הריכוזי המדינתי**, בהתאמה לקדמה הטכנולוגית ולאתגרים החדשים, בדומה למודל הקיים היום באסטוניה וסינגפור.

3. מבדיקת הדוגמאות **למודלים ריכוזיים המובלים על ידי גורם פרטי** במדינות אחרות, מדובר בדרך כלל בגופים פיננסיים. גופים אלו הקימו היסטורית תשתית הזדהות מרכזית משתי סיבות עיקריות: הממשלה לא הניחה את התשתית הנדרשת לכך, ומחויבותם לרגולציית הלבנת הון חייבה פתרון, כשבשלב מאוחר יותר נשענה על תשתית זו.
אין זו נקודת המוצא בישראל. יתרה מכך, מהשיח המתמשך עם מגזר הבנקאות בישראל - הן במסגרת עבודת אסטרטגיה זו והן בדיונים קודמים לאורך השנים - לא הובע עניין בהקמת פלטפורמה חלופית לפלטפורמה הממשלתית, שתאפשר הסתמכות גם עבור גופים נוספים. לא ראינו יוזמה כזו, גם לא מצד הבנקים ביניהם לבין עצמם.

4. אנו סבורים כי **מודל רישוי** לגורם פרטי לתחום הזהויות פחות מתאים למדינת ישראל, שהיא מדינת אי קטנה יחסית (להבדיל ממדינות אירופה, המקדמות מודל כלל אירופאי כזה, הכולל שוק גדול בהרבה). בדיקתנו העלתה שמצד המודל העסקי, קשה מאד להגיע לרווחיות ונדרש "אורך נשימה" של מספר שנים כדי לעשות כן, גם במדינות גדולות יותר, כאשר מדובר בפלטפורמה יחידה או מרכזית באותה מדינה. יתרה מכך, ידרשו עלויות ותשומות של הליכי הפיקוח, אשר גם יעמיסו הוצאות נוספות על גוף כזה (ועל המדינה), ועל כן לא קיימת לכך התכנות גבוהה. בנוסף לכך, ומתוך הסתכלות על הפעלת מודל הרישוי בתחום דומה, תחום החתימה האלקטרונית[18] אנו רואים כי מודל זה לא הביא לתחרות בין גופים באופן משמעותי התורם למשק.

[18] מודל זה פועל מכוח חוק חתימה אלקטרונית, התשס"א-2001.

שילוב המגזר הפרטי במערכת ההזדהות הלאומית יאפשר להסתמך על זהות דיגיטלית מאומתת ואחידה כבר בשלב ההרשמה (Onboarding) ובכך יחזק את אמינות תהליכי הזיהוי, יצמצם הונאות וישפר את חוויית השירות. תשתית ההזדהות הלאומית תשמש בסיס משותף למתן שירותים בעלי רמת אמון גבוהה, כגון שירותים פיננסיים, תוך שמירה על פרטיות המשתמש, צמצום בירוקרטיה והפחתת הצורך בהתייצבות פיזית ובהצגת מסמכים פיזיים.

הבחירה במודל הריכוזי הישראלי, שיפורו ופתיחתו כשירות למגזר הפרטי, גוררת אתגרים נוספים ומצריכה ניהול סיכונים, כמפורט בפרק זה.

3.1 יעד ראשון: הנגשת מערכת ההזדהות למגזר הפרטי וקביעת מנגנון מתאים

מדינת ישראל תפעל להרחבה מדורגת של השימוש במערכת ההזדהות הלאומית גם למגזר הפרטי ולגופים חוץ ממשלתיים. מהלך זה יחזק את החוסן הדיגיטלי של המשק, ויאפשר לגופים עסקיים להסתמך על עוגן זהות לאומי, אחיד ואמין לצורך זיהוי והרשמת לקוחות וצמתי החלטה רגישים אחרים.

ההצטרפות למערכת ההזדהות הלאומית של גופים מסתמכים שאינם ממשלתיים/ציבוריים תהיה **וולונטרית** ותיעשה לאחר עבודת עומק בנושאים שונים, לרבות קביעת אמות מידה ביחס לסוגי השימושים הרלוונטיים בהתאם לצורכי גופים אלו ובהתאם לקריטריונים שייקבעו, בין היתר, ביחס לסוגי המגזרים והגופים וכן תמחור העלויות והמודל הכלכלי, בשיתוף פעולה עם גופים ומגזרים רלוונטיים (ראו להלן).

השענות גופים שאינם ממשלתיים או ציבוריים על המערכת, אין משמעותה החלפת התהליך המלא של זיהוי הלקוח (KYC), אלא בחיזוק תהליכי הזיהוי תוך התמקדות בשלב ההרשמה ולא בתהליכי האימות השוטפים.

הרחבת השימוש במערכת ההזדהות הלאומית לגופים פרטיים, תעשה באופן מדורג, בהתאם לערך הציבורי ולניהול סיכונים. מערך הדיגיטל והחשב הכללי יקימו צוות מקצועי בינמשרדי ויגבש קריטריונים ותהליכים מתאימים לשם כך. בין הקריטריונים שייקבעו יכללו: תרומת הגוף לציבור, הפחתת הנטל הבירוקרטי, רמת הסיכון בשירות, יכולתו של הגוף לעמוד בתנאי השימוש/החיבור למערכת מבחינה אופרטיבית, טכנולוגית ומשפטית, הצורך ברמת אמון גבוהה בתהליך ההזדהות, סוגיית האחריות והיבטים משפטיים נוספים. בהתאם לקריטריונים אלה, ייבחנו בקשות של גופים לקבל את השירות כגורמים מסתמכים על המערכת.



המגזרים והגופים אשר יבחנו בהקשר זה יהיו, בין היתר, המגזר הפיננסי, מגזר הבריאות, מגזר התקשורת, מוסדות להשכלה גבוהה, ובעלי מקצועות מוסדרים אשר מחויבים באימות זהותו של אדם וכן גופים רלוונטיים נוספים. גישה מדורגת זו תאפשר הרחבה מבוקרת של השימוש במערכת, תוך שמירה על רמת אבטחה גבוהה וניצול מיטבי של משאבי המדינה.

בבחינת הרחבת הגורמים המסתמכים על המערכת לגופים פרטיים, ייבחן גם הצורך בתיקוני חקיקה או הוראות רגולציה.

הרחבת השימוש במערכת ההזדהות הלאומית לגופים פרטיים תחייב **גיבוש מודל כלכלי** שיבטיח את קיומה והמשך פיתוחה של התשתית לאורך זמן. המודל הכלכלי ייגזר, בין היתר, מסוג השירות שניתן, היקף השימוש בו, ומהעלויות הכרוכות בהפעלת התשתית ותחזוקתה. במסגרת זו יבחנו מודלים שונים של תמחור, לרבות תמחור דיפרנציאלי בהתאם למאפייני הגוף וסוג השירות.

קביעת המודל הכלכלי יעשה בצורה מאוזנת בין הצורך בהבטחת קיומה של תשתית לאומית, השקעת התשומות הנדרשות בה וניהולה בסטנדרט גבוה, גם בהיבטי חוסן ורציפות תפקודית, לבין הרצון לעודד את אימוצה/ מימושה בקרב גופים רלוונטיים במשק.

במסגרת זו יובאו גם שיקולים של ערך ציבורי, חלוקת אחריות ותרומת השירות להפחתת הונאות וחיזוק החוסן הדיגיטלי, וכן צורך להימנע מיצירת חסמים בלתי מוצדקים לשימוש בתשתית. הגורמים הפרטיים שיעשו שימוש במערכת יישאו בעלות היחסית בגין פעילותם, במטרה להבטיח הקצאת משאבים יעילה. המטרה היא לגשר על כשל שוק, תוך גביית מחיר כלכלי המשקף את שווי השוק (סיווג התשלום מבחינה משפטית ייבחן בהמשך וכן כחלק מקביעת המודל הכלכלי).

3.2 יעד שני: עקרונות הגנת הפרטיות (Privacy by Design)

הגנת הפרטיות תהווה עיקרון יסוד בתכנון ובהפעלת מערכת ההזדהות הלאומית. ארכיטקטורת המערכת תבטיח הפרדה בין שירות אימות הזהות לבין הפעילות העסקית המתבצעת (מהות/ תכולת השירות) בין התושב לבין הגוף המסתמך.

המדינה לא תיחשף לתוכן השירות או לפעילות העסקית מעבר למידע המזערי הנדרש להפעלת השירות, לאבטחתו, לבקרה ולטיפול באירועי הונאה, וכל זאת בהתאם להוראות הדין. כאמור, המטרה העיקרית היא חיזוק תהליכי ההזדהות בשלב ההרשמה ולא בתהליכי האימות השוטפים. (כאמור, גם היום פונים גופים פרטיים למערכת לק"ח המדינתית לקבלת אימות פרטי רישום, בתרחישים דומים, והיעד הוא שינוי האופן בו הדבר נעשה).

התשתית תיושם בהתאם לעקרונות של מזעור מידע (Data Minimization) וגילוי סלקטיבי (Selective Disclosure), ככל הניתן (ראו האמור בפרק הנוגע לארנק הדיגיטלי בנושא זה).

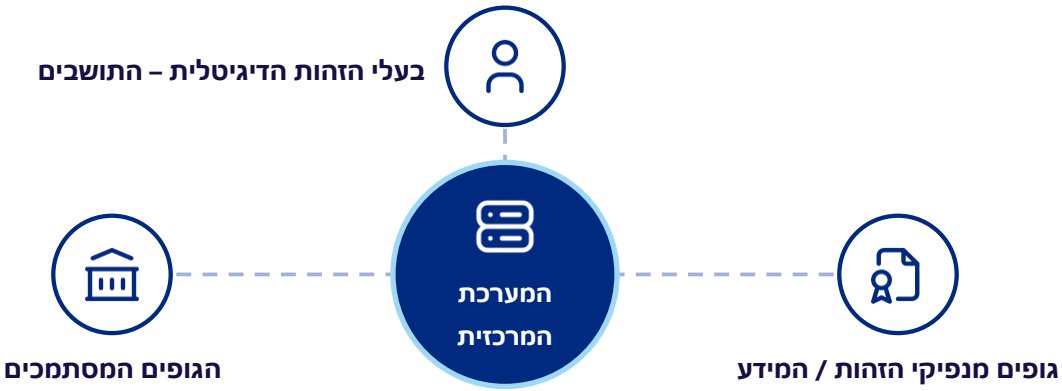
עקרון מרכזי יהיה שקיפות כלפי התושב, ויכולתו לעקוב ולשלוט ביחס לפעילות הנוגעת לזהותו הדיגיטלית כמשתמש במערכת ההזדהות ובארנק הדיגיטלי, וכן שימוש בהתראות יזומות על שימוש בזהות, שינוי פרטיה, תוקפה וכיו"ב, אשר יחזקו את שליטת התושב בייצוג הדיגיטלי ויאפשרו דיווח שלו במקרים הנדרשים לצורך צמצום הונאות.

בנוסף, יישמרו זכויות נושאי המידע בהתאם לחוק הגנת הפרטיות, התשמ"א-1981, לרבות ניהול תהליכי הסכמה, זכות עיון במידע, תיקון מידע ומחיקת מידע בהתאם לדין וצמצום בעלי ההרשאה למידע הרגיש במערכת, למינימום הנדרש. כדי לעשות כן, המערכת תאופיין תוך שילוב רכיבים מיטביים למימוש זכויות אלה, בפשטות ויעילות.

הרחבת השימוש בהתאם לעקרונות אלה, צפויה לחזק את פרטיות התושבים ביחס למצב הקיים היום, ותבסס אמון ארוך טווח בהישענות על התשתית הלאומית.

3.3 יעד שלישי: חלוקת אחריות

בתהליך השימוש במערכת לאימות זהות/ארנק זהויות, ישנם ארבעה גורמים או רכיבים עיקריים שיש בהם כדי להשפיע על מהלך השימוש ומהימנותו: המערכת המרכזית המנהלת את התהליכים הדיגיטליים, הגופים מנפיקי הזהות/המידע, בעלי הזהות הדיגיטלית- התושבים והגופים המסתמכים. עבור גופי הממשלה נותני השירות (המסתמכים) ובמידה רבה עבור גופים ציבוריים רבים, משמש התהליך כמענה כולל לניהול הייצוג הדיגיטלי מקצה לקצה.



עבור גופים שאינם ממשלתיים, הסתמכות על מערכת זו משמעותה חיזוק תהליכי הזיהוי (תהליכי eKYC- Electronic Know Your Customer), **בעיקר** בשלב ההרשמה ויצירת הזהות הדיגיטלית אצלם בפעם הראשונה (ככלי משלים לתהליכי הזיהוי המנוהלים על ידי גופים אלה. עשויים להיות תרחישים נוספים).

כאמור, גם כיום מונגשים נכסי המדינה בתחום ההזדהות לגופים שונים במשק, אלא שהדבר לא נעשה בצורה מיטבית ומעודכנת. המשמעות היא הקמת תהליכים חדשים ובטוחים יותר במרחב הדיגיטלי, המותאמים בצורה טובה יותר לסיכונים עכשוויים, המתפתחים והעתידיים, מתוך הבנה כי יש בכך כדי להעלות את חוסנו של כלל המשק.

הרחבת השירות לגורמים שאינם ממשלתיים מעלה את הצורך בבחינה מחודשת של הסדרי האחריות וחלוקתה בין ארבעה הגורמים המפורטים לעיל. סוגי התקלות העלולות לקרות בתהליך הזיהוי: (1) מניעת שירות מאדם תמים בשל טעות False Negative או תקלה כוללת המונעת שירות אימות זהות; (2) החמצת הונאת התחזות אשר עלולה לפגוע במערכת עצמה או באדם אליו התחזה הגורם הפוגע False Positive.

מסקירת נושא זה עולה כי יש לתת דגש על מספר עקרונות מצד התנהלותה של המדינה בתהליך זה: יצירת נהלים והקפדה על ביצועם תוך תיעוד הפעילות; עמידה בסטנדרטים גבוהים (state of the art) ובתקינה הרלוונטית בהפעלת המערכת ובזמינותה; הפעלת מנגנוני בקרה של גורם חיצוני על תהליכי המערכת; שמירה על אמינות הנתונים עליהם יש הסתמכות ומימוש מנגנון תיקון ככל הנדרש; ניהול רישום הפעילות, שיקופה למשתמש והעלאת התראות מולו ביחס לניהול הייצוג הדיגיטלי; בחינת היכולת להעמדת חלופות לערוץ הדיגיטלי, ככל הניתן.

כמו כן, יש לשקף לכל הגורמים העיקריים את תנאי השימוש במערכת, חובותיהם כלפיה ואופן השימוש בה, במסגרת המתאימה לכך (באופן הסכמי ו/או בהתאם לדין).

נושא זה יצריך מעקב מתמיד ובקרה על תהליכים, כדי לעמוד ברף הנדרש לעבודה ממשלתית תקינה.

3.4 יעד רביעי: התאמת המסגרת הרגולטורית עבור גופים פרטיים במשק

הצלחת הרחבת השימוש במערכת ההזדהות הלאומית תלויה בהתאמת המסגרת הרגולטורית החלה על הגופים המסתמכים, המצויים תחת פיקוח. גם כאשר קיים מענה טכנולוגי מתקדם, גופים פרטיים מפוקחים אינם יכולים לאמצו ללא הכרה רגולטורית מתאימה.

לקידום המהלך, מערך הסייבר הלאומי ומערך הדיגיטל הלאומי יפעלו באופן יזום ומתואם מול הרגולטורים הרלוונטיים, לבחינת החסמים הרגולטוריים הקיימים ולהתאמת ההוראות הנדרשות על ידי הרגולטורים, כך שיתאפשר שימוש בשירותי הזהות וההזדהות הלאומיים כחלק מוכר ותקף מתהליכי זיהוי והכרת לקוח (KYC), בהתאם לדרישות הרגולטוריות ולרמת הסיכון.

מהלך זה יבטיח הלימה בין התשתית הטכנולוגית לבין המסגרת הנורמטיבית, יסיר חסמים לאימוץ התשתית ויאפשר הרחבה הדרגתית ומבוקרת של השימוש בתשתית אחידה בכלל המשק.

מערך הסייבר הלאומי

מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

משרד האוצר

רשות האוכלוסין וההגירה



נספחים

נספח א' – הגדרות ומושגים

מושג (עברית)	מושג (אנגלית)	הגדרה והקשר במסמך האסטרטגיה
אימות ביומטרי	Biometric Verification	אישור (או הפרכה) של טענת זהות באמצעות השוואה של שתי דגימות של אמצעים ונתונים ביומטריים המיוחסות לאותו אדם (1:1).
אימות זהות / אותנטיקציה	Authentication	פעולה אקטיבית המקשרת בפועל את הייצוג הדיגיטלי של המשתמש לזהותו המאומתת בזמן אמת, לצורך קביעה שהאוחז באמצעי ההזדהות הוא אכן בעל הזהות הלגיטימי, באמצעות שילוב גורמי אימות (משהו שאתה יודע, מחזיק, או מאפיין ביומטרי). *הערה: זוהי הפעולה שמבצעת מערכת ההזדהות הלאומית, בשונה מבדיקת/אימות פרטים (ראו מושג נפרד) שמבצעת מערכת לק"ח, שאינה כוללת קישור אקטיבי כאמור.*
אישור מאומת	Verifiable Credential	אישור דיגיטלי הניתן לאימות באמצעים קריפטוגרפיים, שבהם גורם מוסמך (מנפיק) מאשר מידע מסוים לגבי אדם או ישות. האישור מוגן מפני שינוי ומאפשר לכל גורם מאמת לבדוק באופן עצמאי את מקורו ושלמותו, ללא צורך בפנייה בזמן אמת למנפיק.
ארנק זהות דיגיטלי לאומי	National Digital Identity Wallet	יישום ממשלתי מאובטח שבאמצעותו תושבים יכולים להחזיק, לנהל ולשתף תעודות וזהויות דיגיטליות באופן מבוקר.
בדיקת/אימות פרטים	Attribute Verification	שאילתה המשווה נתוני זהות בסיסיים (כגון שם, מספר זהות) מול מרשם האוכלוסין, ללא ביצוע פעולת אותנטיקציה אקטיבית הקושרת את הייצוג הדיגיטלי לזהותו של המשתמש. *הערה: זהו האופן שבו פועלת כיום מערכת לק"ח עבור גופים מורשים (כולל גופים פרטיים).*
גוף מסתמך	Relying Party (RP)	גוף המספק שירות או מבצע עסקה, אשר מסתמך על אישור הזהות, הנתונים או האישורים המאומתים (Verifiable Credentials) המסופקים על ידי ספק הזהות הלאומי או הארנק.
דרכון דיגיטלי	Digital Passport	מסמך נסיעה דיגיטלי (Digital Travel Credential –ICAO DTC) הנגזר מנתוני הדרכון הפיזי הביומטרי (eMRTD/Smartcard) הקיים, ונשמר בארנק הדיגיטלי של בעליו. המגמה הגלובלית (לפי תקינת ICAO) היא שימוש בדרכון דיגיטלי לצורך זיהוי מרחוק לפני טיסה (אפליקציה/בדיקה מקדימה מול רשויות הגבול) וגם למעבר גבול ללא הצגת הדרכון הפיזי (Contactless/Paperless Border Crossing). *הערה: באסטרטגיה הישראלית, שילובו בארנק הלאומי ייבחן בשלב מאוחר יותר, לאחר ביסוס הארנק לשירותים מקומיים.*
הגנת סייבר ואבטחת מידע מעצם התכנון	Cyber by Design	עקרון ארכיטקטורה להידוק מעטפת ההגנה של מערכת ההזדהות הלאומית כבר בשלב התכנון, לרבות מנגנונים לשמירה על רציפות תפקודית, יתירות והתאוששות מאירועי קיצון, לצד מעבר מתפיסת אבטחה נקודתית לניהול מחזור החיים של הזהות הדיגיטלית מול איומי זהות מתפתחים.
הוכחת זהות	Identity Proofing	התהליך הנורמטיבי (בהתאם לתוצר ב' למדיניות להזדהות בטוחה והמבוסס על תקינה ה- NIST SP 800-63-4A) שבו נאספים, מאומתים ומאושרים נתוני הזהות של הפרט לפני הנפקת אמצעי הזדהות, כולל בדיקת מקוריות מסמכים ואימות ביומטרי. שלב הרישום והוידוא הראשוני הקושר באופן מהימן בין האדם הפיזי לבין מזהיו הרשמיים והייצוג הדיגיטלי המונפק לו.
הונאת התחזות	Identity Fraud / Impersonation	שימוש בלתי מורשה בזהותו המלאה של אדם אמיתי וקיים, לרוב באמצעות גניבה, הטעיה או פריצה למסמכי זיהוי, פרטי התחברות או אמצעי הזדהות שלו, במטרה להתחזות אליו ולפעול בשמו מול גופים ציבוריים או פרטיים. בשונה מ"זהות סינתטית" (ראו מושג נפרד), הזהות הנפגעת היא זהות אמיתית וקיימת, לא ישות בדויה שנוצרה מחדש.
היערכות לפוסט-קוואנטום	Post-Quantum Readiness	היערכות למעבר לתשתיות הצפנה, פעולות הזדהות וחתימה דיגיטלית העמידות בפני מתקפות של מחשוב קוונטי עתידי.
הערכת סיכונים וסיכולם לאורך מחזור חייה של הזהות/הייצוג הדיגיטלי	Identity Threat & Fraud Management	ניהול איומי זהות והונאות - יכולת לאומית רציפה לשילוב אנליטיקה, סייבר ו-AI לזיהוי, ניתוח ותגובה לאיומי התחזות לאורך מחזור החיים.

הגדרות ומושגים

מושג (עברית)	מושג (אנגלית)	הגדרה והקשר במסמך האסטרטגיה
זהויות שאינן אנושיות	Non-Human Identities (NHI)	זיהוי וניהול של מערכות ורכיבים טכנולוגיים (לא רק סוכני AI הפועלים בשם אדם) ומשפיע על ניהול מערכות ממוחשבות באופן רוחבי. *הערה: אסטרטגיה זו עוסקת רק בחלק מתחום ה-NHI כייצוג דיגיטלי של משתמשים אנושיים, כולל באמצעות סוכני בינה מלאכותית.*
זהות יסודית	Foundational Identity	זהות שנוצרה במערכת מרכזית על ידי המקור המוסמך לקביעתה (בדרך כלל מדינה), והיא משמשת כעוגן הקובע לתהליכי הרשמה, אימות והוכחת זהות במערכות אחרות הנשענות על אותו מקור מוסמך. בישראל, הזהות היסודית של התושב נוצרת במרשם האוכלוסין ומנוהלת על ידי רשות האוכלוסין מלידה ועד מוות, והיא העוגן להנפקת התיעוד הרשמי במדינה ולתהליכי ההזדהות במערכות אחרות במשק.
זהות סינתטית / הונאת זהות סינתטית	Synthetic Identity Fraud	יצירת זהות מלאכותית המשלבת נתונים אמיתיים (למשל מספר זהות תקף) עם נתונים בדויים, לשם יצירת ישות "לא אמיתית" חדשה שעוברת את בדיקת המערכת (להבדיל מהתחזות לאדם קיים ושימוש בנתוניו האמיתיים במלואם).
זיופים עמוקים	Deepfakes	תוצר של טכנולוגיות בינה מלאכותית יוצרת (Generative AI) המשמש ליצירת אמצעים מתוחכמים חזותיים או קוליים באיכות גבוהה בזמן אמת, המכוון להערים על מנגנוני זיהוי אנושיים ואלגוריתמים לאימות ביומטרי. התוצר יכול להציג אדם אמיתי שיצרו לו שכפול חזותי או קולי או אדם שאינו קיים.
חשיפה סלקטיבית	Selective Disclosure	חשיפת המידע המינימאלי הנדרש לצורך קבלת השירות (כגון הוכחת גיל) ללא חשיפת נתונים עודפים.
ייצוג דיגיטלי / זהות דיגיטלית	Digital Identity / Representation	הטרנספורמציה של הזהות היסודית לישות לוגית במרחב המקוון. נשענת על תקני ISO/IEC 24760, ומאפשרת ביצוע אינטראקציות ועסקאות ברמת אמינות גבוהה מול גופים ציבוריים ופרטיים. זהו למעשה אוסף הנתונים, המזהים ואמצעי הזיהוי המאפשרים לתושב להזדהות ולפעול באופן מאובטח, פשוט ורציף במרחב הדיגיטלי לאורך מחזור החיים.
יכולת פעולה הדדית	Interoperability	היכולת של מערכות זהות, ארנקים ותשתיות קריפטוגרפיות שונות להחליף מידע ולפעול יחד באופן חלק, בהתבסס על פרוטוקולים פתוחים ותקנים גלובליים (W, ICAO, ISO3C, OIDC). בהקשר כאן, תאימות טכנולוגית ונורמטיבית המאפשרת עבודה מול תקנים בינלאומיים והכרה הדדית בתעודות מחוץ לישראל.
מדיניות לאומית להזדהות בטוחה (והקווים המנחים לה)	National Policy for Secure Identification (and Guidelines)	מסגרת מקצועית ונורמטיבית, ובסיס אחיד לקביעת עקרונות, דרישות ורמות אמון בתהליכי הזדהות דיגיטלית לשירותים דיגיטליים, בהתאם לרמת הסיכון ומאפייני השירות. המדיניות והקוים המנחים גובשו על ידי מערך הסייבר הלאומי בהתאם להחלטות ממשלה.
מזעור מידע	Data Minimization	עקרון יסוד בהגנת הפרטיות לפיו פעולות איסוף, עיבוד ושמירת מידע נעשות רק בהיקף ההכרחי למטרה מוגדרת. העיקרון קבוע ברגולציה האירופאית (GDPR), ועוגן גם בחוק הגנת הפרטיות, התשמ"א-1981 ותקנותיו.
נכסי זהות לאומיים	National Identity Assets	מכלול התשתיות, המאגרים והמערכות הממשלתיות (מרשם האוכלוסין, מערכת לק"ח, מערך התיעוד הביומטרי ומערכת ההזדהות הלאומית) המהווים את העוגן האסטרטגי לניהול זהויות וביסוס אמון והחצנת שירותים במדינה. מדובר בתשתיות מדינה קריטיות ותשתיות ציבוריות דיגיטליות (DPI) המנוהלות על ידי המדינה, המהוות מקור אמת יחיד (Single Source of Truth) לאימות זהות ומבטיחות רציפות תפקודית, חוסן וריבונות דיגיטלית.
סוכני בינה מלאכותית	AI Agents	ישויות תוכנה אוטונומיות הפועלות במרחב הדיגיטלי בשם יישויות אחרות, מבצעות עבורן פעולות ומקיימות אינטראקציות עם מערכות ונותני שירותים, תוך יצירת זיקה מהימנה ובת-מעקב בין ה"סוכן" לבין היישות שבשמה הוא פועל. לצורך מסמך זה, המונח מתייחס רק לייצוג של סוכני AI עבור משתמשים אנושיים ולא בייצוג ישויות/רכיבים טכנולוגיים שאינם אנושיים.
תכנון לפרטיות	Privacy by Design	מימוש עקרונות פרטיות משלב תכנון המערכת או קביעת הארכיטקטורה, לרבותהפרדה ארכיטקטונית בין שירות אימות הזהות לבין הפעילות העסקית של הגוף המסתמך, יישום מזעור מידע וגילוי סלקטיבי כברירת מחדל, שקיפות כלפי התושב ויכולתו לעקוב ולשלוט במידע הנוגע לזהותו הדיגיטלית, לצד שמירה על זכויות נושאי המידע בהתאם לחוק הגנת הפרטיות, התשמ"א-1981.

הגדרות ומושגים

מושג (עברית)	מושג (אנגלית)	הגדרה והקשר במסמך האסטרטגיה
ריבונות דיגיטלית	Digital Sovereignty	עיקרון יסוד אסטרטגי לפיו מעבר רכיבים או שירותים של מערכת ההזדהות הלאומית לענן ייעשה תוך שמירה על שליטה לאומית ברכיבי הליבה והנתונים הרגישים ועל הרציפות התפקודית, נוכח סיווג המערכות כתשתית מדינה קריטית.
רמת אמון / רמת סמך	Level of Assurance (LoA)	מידת הוודאות והביטחון הנדרשת בתהליכי ההזדהות (למשל רמת סמך 3 בהתאם לרמת הסיכון ומאפייני השירות הדיגיטלי. זהו מדד נורמטיבי הקבוע במדיניות הלאומית להזדהות בטוחה (ובתקני NIST SP 800-63/ SADIe), המגדיר את רמת תהליכי הרישום (רב"ה), האימות (רב"א) והנדרשים להוכחת הזהות של המשתמש.
קבלה מוטעית/דחיה מוטעית	False Positive / False Negative	שני סוגי התקלות המרכזיים העלולים להתרחש בתהליך הזיהוי הדיגיטלי: (1) False Negative - מניעת שירות מאדם תמים בשל טעות או תקלה המונעת שירות אימות זהות; (2) False Positive - החמצת הונאת התחזות, העלולה לפגוע במערכת עצמה או באדם שאליו התחזה הגורם הפוגע.
שלב הרשמה	Onboarding	שלב זה נועד לבסס את הייצוג הדיגיטלי של המשתמש. בשלב זה נאספות ראיות, פיזיות או דיגיטליות, בהתאם לרמת האמון/ הסמך בהוכחת הזהות שנקבעה בתהליך הסיווג/ הרגישות של השירות.
תהליכי eKYC	Electronic Know Your Customer	תהליכי זיהוי הלקוח באופן מקוון/ דיגיטלי/ אלקטרוני (מוכר בעיקר במגזר הפיננסי /הפרטי). מדובר בתהליך אשר תואם הנחיות רגולטוריות בעיקר למניעת הלבנת הון, והשענות על הזדהות אל מול מסמכי זהות ממשלתיים ברמת אמון גבוהה מאוד.
תקיפת מצג שווא	Presentation Attack (PA)	ניסיון הונאה במערכות זיהוי ואימות ביומטריות באמצעות הצגת אמצעי התחזות מול החיישן/המצלמה. על פי תקן ISO/IEC 30107, ניסיון להטעיית חיישן ביומטרי באמצעות תמונה פיזית, מסכת סיליקון, וידאו מוקלט או Deepfake. ההתמודדות מצריכה מנגנוני גילוי תקיפת מצג שווא (PAD - Presentation Attack Detection).
תשתית מדינה קריטית (תמ"ק)	Critical National Infrastructure (CNI)	מערכות ותשתיות טכנולוגיות לאומיות שהשבתתן, פגיעה ברציפותן או חדירה אליהן עלולות לגרום לנזק חמור לחוסן הלאומי, לביטחון המדינה ולכלכלה ע"פ חוק הסדרת הביטחון בגופים ציבוריים התשנ"ח 1998.
תשתית פדרטיבית	Federated Identity Infrastructure	ארכיטקטורה שבה התושב מזדהה מול ספק זהות לאומי מרכזי (IdP) לקבלת גישה למגוון גופים מסתמכים. בהתאם לתקן NIST800-63-4 C זהו מודל שבו ניהול הזהות והאימות מרוכזים אצל גורם מוסמך, בעוד אישור האימות מועבר באופן מאובטח מול גופים נותני שירות ללא צורך בהחזקת ספריית משתמשים נפרדת בכל גוף.

מעגלי היווצות

מגזר	ארגון
וועדות היגוי	• מערך הסייבר הלאומי • מערך הדיגיטל הלאומי • רשות האוכלוסין וההגירה • בנק ישראל – המפקח על הבנקים • משרד האוצר - אגף תקציבים • משרד האוצר - חשב הכללי • מלווה – חברת Deloitte
פיננסי	• ישראכארד • MAX • בנק לאומי • בנק הפועלים • בנק מזרחי • בנק דיסקונט • בנק הבינלאומי • בנק יהב • בנק One Zero
השקעות וביטוח	• הפניקס • כלל • מנורה
בריאות	• ביה"ח רמב"ם • ביה"ח סורוקה • ביה"ח אסותא • ביה"ח פוריה
תעשייה	• התייעצויות עם חברות פרטיות ישראליות ובינלאומיות ועם מומחים בתחום הסייבר, ההזדהות וביומטריה