מש/5

העתק פרוטוקול ניסוי למערכת הביומטרית במסגרת תקופת המבחן

הרשות לניהול המאגר הביומטרי

מדינת ישראל
State of Israel

רשות האוכלוסין וההגירה
Population and Immigration Authority

<u>הנדון: פרוטוקול ניסוי לתקופת המבחן</u>

בהתאם לסעיף 41 לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע – 2009, תחילתו של החוק תהיה בתקופת מבחן של שנתיים במטרה לבחון את אופן היישום של הוראות לפי חוק זה, את נחיצות קיומו של מאגר ביומטרי ומטרותיו, את המידע שיש לשמור במאגר ואת אופן השימוש בו.

בהתאם לכך נקבע צו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשע"א – 2011, (להלן – הצו) אשר מסדיר את תקופת המבחן.

מצורף בזאת מסמך "פרוטוקול הניסוי", אשר מרחיב את האמור בצו ומפרט את מכלול ההיבטים של תקופת המבחן ואת מכלול התהליכים שייבחנו בתקופה זו על ידי כל הגורמים המשולבים בתקופת המבחן, כולל פירוט מדדים, כחלק בלתי נפרד מהצו וכהרחבה שלו.

מסמך זה קיבל את אישורו של הממונה על היישומים הביומטריים.

מסמך זה מהווה מסמך מחייב אשר על פיו ועל פי הצו יפעלו כל הגורמים הרלוונטיים בתקופת המבחן.

אמנון בן עמי
מנכ"ל רשות האוכלוסין וההגירה

גון קמני
ראש הרשות לניהול המאגר הביומטרי

כ"ב תמוז תשע"ב 11.7.12
תאריך

פרוטוקול ניסוי למערכת הביומטרית

במסגרת תקופת המבחן

גרסה: 1.3

תאריך: 05-07-2012

1. מבוא 9
2. לשון החוק 10
3. הגדרות 12
3.1. ביומטריה 12
3.2. דגימה ביומטרית – SAMPLE 12
3.3. הרכשה - ENROLLMENT 12
3.4. השוואה ביומטרית - MATCHING 12
3.5. ציון - SCORE 12
3.6. סף החלטה – THRESHOLD 12
3.7. אימות זהות – VERIFICATION 13
3.8. זיהוי - IDENTIFICATION 13
3.9. אירוע של אישור מתחזה – FALSE ACCEPTANCE 13
3.10. אירוע של דחיית מורשה – FALSE REJECTION 13
3.11. קצב קבלת מתחזים – FALSE ACCEPTANCE RATIO 13
3.12. קצב דחיית מורשים - FALSE REJECTION RATIO 13
3.13. הרכשה כפולה – DUPLICATION 14
3.14. גרף ROC 15
3.15. מערכת "אביב" 15
4. מטרות ויעדים 16
4.1. רקע 16

4.2. מטרות כלליות של תקופת המבחן...16
4.3. מטרות ראשיות של הניסוי...18
4.4. מטרות נוספות של הניסוי...22
5. תיאור המערכת...24
5.1. עמדת ההרכשה...25
5.2. מערכת "אביב"...26
5.3. המאגר...27
5.4. מערך ביקורת הגבולות...28
6. תרחישים...30
6.1. הרכשה...30
6.2. זיהוי ביומטרי מול תעודת זהות...32
6.3. זיהוי ביומטרי מול דרכון...33
6.4. חיפוש הרכשה כפולה...35
6.5. אימות זהות...36
6.6. זיהוי מול מאגר...37
7. עיקרי השיטה - תקציר...38
7.1. היקף אוכלוסיית הניסוי ופריסה גיאוגרפית...38
7.2. אירועים יזומים...38
7.3. ביצועי המערכת הביומטרית...39
7.4. אימות זהות ראשוני...39
7.5. רישום ותיעוד...39

7.6. שביעות רצון של האזרחים....................39
7.7. סקרים ותהליכים משלימים....................39
8. רכיבים וגורמים מעורבים....................40
8.1. גורמים ארגוניים....................40
8.2. רכיבים....................42
9. הניסוי....................49
9.1. הכנה....................49
9.2. היקף ופריסה....................49
9.3. תרחישי הניסוי....................49
9.4. סקר שביעות רצון....................52
9.5. הצגת התוצאות....................52
10. סיכונים, מגבלות ובעיות....................53
10.1. איתור הרכשות כפולות....................53
10.2. השוואות ביומטריות....................54
10.3. תלות במספר המתנדבים....................54
10.4. התפלגות אוכלוסיית המתנדבים....................55
10.5. התפלגות של אוכלוסיות נבחרות....................55
10.6. הבדלים בין מסמכי הזיהוי....................55
10.7. הערכות של גורמים אחרים....................55
10.8. שירותים שאינם מבוססי ביומטריה....................56
10.9. מדיניות עדכון רשומות ביומטריות....................56

10.10. נושאים שאינם ניתנים לכימות....56
10.11. נושאים שאינם ניתנים לניסוי....56
10.12. מגבלות הטכנולוגיה....56
11. מהלך הניסוי....57
11.1. תשאול....57
11.2. הרכשה ראשונית....59
11.3. השוואה מול תעודת זהות....61
11.4. השוואה מול דרכון....63
11.5. אימות מול המאגר....65
11.6. זיהוי מול המאגר....67
12. בעלי תפקידים....69
12.1. ועדה מייעצת....69
12.2. מנהל הניסוי מטעם הרשות לניהול המאגר הביומטרי....69
12.3. מנהל הניסוי מטעם רשות האוכלוסין....69
12.4. נאמני מחשוב....69
12.5. פקידים....69
12.6. משתתפים....69
12.7. עובדי רשות האוכלוסין, הרשות לניהול המאגר הביומטרי ומערכי ההנפקה....70
13. תיעוד במהלך הניסוי....71
13.1. כללי....71
13.2. תדירות....71

13.3. סקר שביעות רצון......71
13.4. קבלת משוב שוטף......72
13.5. טיוב נתונים ורשומות......72
14. נתונים ומדדים להצלחה......74
14.1. נתוני הרכשה......74
14.2. נתוני השוואות ביומטריות......78
14.3. נתונים הנוגעים לפעילות במאגר......81
14.4. נתוני הנפקת תיעוד......89
14.5. נתונים כלליים......89
14.6. נתונים הנוגעים לביקורת הגבולות......91
15. בטיחות, גהות ונגישות......93
15.1. בטיחות וגהות......93
15.2. נגישות......93
16. אבטחת מידע במהלך הניסוי......94
16.1. סקרי אבטחה......94
16.2. בדיקות חדירה (PENETRATION TESTS)......95
16.3. דירוג תוצאות הסקרים......96
16.4. אתרי גיבוי......99
16.5. הסתייעות בגורמי חוץ......99
16.6. שמירת מידע......100
17. הגנה על הפרטיות......101

17.1. העברת מידע מהמאגר לגורמי חוץ......101
17.2. נגישות למידע במאגר......101
18. עיבוד התוצאות......102
19. נספחים......103
19.1. תקנים ומסמכים ישימים......103
19.2. פרמטרים של צילומי פנים......104
19.3. כלים לאיתור הרכשות כפולות......105
19.4. אופן שילוב הלמ"ס......113
19.5. עמדות מעבר ביומטרי בשירות עצמי - בקורת הגבולות/נתב"ג......115

מעקב גרסאות

גרסה	תאריך	עודכן ע"י	מהות העדכון
1.0	26–06–2012		גרסה ראשונה לפרסום
1.1	02-07-2012	יורם אורן	בעקבות הערות מהלשכה המשפטית/רשות האוכלוסין
1.2	04-07-2012	יורם אורן	שילוב מסמך של ביקורת גבולות
1.2.1	04-07-2012	יורם אורן	תיאום נוסף מול מסמך הממונה על יישומים ביומטריים[1]
1.3	05-07-2012	יורם אורן	בעקבות הערות מהלשכה המשפטית/רשות האוכלוסין

[1] מסמך זה הינו מסמך מסווג.

- בלמ"ס -

1. מבוא

מסמך זה מתאר את תהליכי הניסוי שיערך בתקופת המבחן, הנדרשת כחלק ממימוש חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע 2009 (להלן "החוק"). תקופת המבחן תאפשר לבחון את יישום החוק ולקבוע את הצורה המיטבית שבה יש לממש חוק זה. על פי סעיף 41 של החוק, החלתו תהיה הדרגתית. השנתיים הראשונות תוגדרנה כתקופת מבחן, במהלכה ייבחנו אופן יישום הוראות החוק בכלל ואופן השימוש במאגר הביומטרי בפרט. בנקודת ההחלטה בתום תקופת המבחן תתקבל ההחלטה האם להפוך את המאגר למנדטורי, האם להאריך את תקופת המבחן בשנתיים נוספות או לבטל את המאגר כליל. במהלך תקופה זו, ההצטרפות למאגר תהיה על בסיס התנדבותי בלבד, והשימוש במאגר יהיה אך ורק לצורך התכלית הראשית של החוק (מניעת הרכשות כפולות) ולא לתכליות הנוספות (אכיפת חוק). אזרח או תושב שיגיע ללשכות רשות האוכלוסין כדי להנפיק תעודת זהות, דרכון, או תעודת מעבר יוכל לבחור לקבל את התיעוד הישן או לאפשר צילום פנים וטביעת אצבעות ולקבל את התיעוד החדש. עם תיעוד חדש זה יוכל האזרח או התושב ליהנות מיתרונות רבים בתחומי החתימה האלקטרונית, השירותים המקוונים שיתאפשרו באמצעות הזדהות מאובטחת, שירות משופר בביקורת גבולות בארץ ובעולם ועוד.

תקופת המבחן הינה הזדמנות לבחינה מקיפה של סוגיות נוספות כמו השימוש השוטף בביומטריה (שלא באמצעות המאגר) אך מטבע הדברים המיקוד העיקרי הינו במאגר ובתועלות ממנו. תקופת המבחן נועדה בעיקר לבחון הצעה ייעודית למימוש החוק ולכן תהליכי הניסוי המתוארים להלן מותאמים לצורת המימוש המוגדרת בחוק.

הערה: בכל מקום שבו יש התייחסות ל-"אזרחים" הכוונה היא לאזרחים ותושבים. בכל מקום שבו יש התייחסות ל-"דרכון" הכוונה היא לדרכון או לתעודת מעבר.

2. לשון החוק

להלן סעיף 41 של החוק:

תחולה הדרגתית ותקופת מבחן	41.	חוק זה יוחל בהדרגה, בהתאם להוראות כמפורט להלן:

(1) השר יקבע, בהתייעצות עם שר האוצר ושר המשפטים ובאישור ועדת הכנסת המשותפת, בצו, תקופת מבחן של שנתיים שבמהלכה יחולו ההוראות לפי חוק זה על תושבים שיתנו הסכמתם לכך בכתב, במטרה לבחון בתקופה זו את אופן היישום של הוראות לפי חוק זה על תושבים אלה, את נחיצות קיומו של מאגר ביומטרי ומטרותיו, את המידע שיש לשמור במאגר ואת אופן השימוש בו (להלן – תקופת מבחן); בצו כאמור ייקבעו בפירוט העניינים שייבחנו בתקופת המבחן, המדדים להצלחתו ואופן קבלת ההסכמה מאת תושבים להחלת הוראות לפי החוק לגביהם בתקופת המבחן; בתקופת המבחן יחולו ההוראות לפי חוק זה בהתאם לצו האמור;

(2) תושב שלא נתן הסכמתו לפי פסקה (1), לא יישללו זכויותיו לפי כל דין, בשל אי מתן ההסכמה כאמור; לעניין זה, לא יראו בייעול שירות הניתן למי שיש לו תעודת זהות הכוללת אמצעים או נתונים ביומטריים, והמתאפשר בשל טיבה של תעודה כאמור, כשלילת זכות מתושב שלא נתן הסכמתו לפי פסקה (1).

(3) על אף הוראות פסקה (1), קבע השר כי תושב זכאי למסמך נסיעה בהתאם להוראות לפי חוק הדרכונים, ושוכנע כי ללא מסמך נסיעה הכולל אמצעים או נתונים ביומטריים תימנע כניסתו של אותו תושב למדינה אחרת, ינפיק לו מסמך נסיעה הכולל אמצעים או נתונים ביומטריים אף ללא הכללתם במאגר הביומטרי; השר רשאי לקבוע הוראות לעניין אופן הנפקת מסמך הנסיעה, ורשאי הוא לקבוע כי יחולו לעניין זה חלק מההוראות לפי חוק זה, בשינויים או בלא שינויים, הכל כפי שיקבע.

(4) 90 ימים לפני תום תקופת המבחן, לכל המאוחר, ידווחו ראש הממשלה והשר לוועדת השרים ליישומים ביומטריים, ולוועדה של הכנסת שבה יהיו חברים חברי ועדת הכנסת המשותפת ליישומים ביומטריים וחברי ועדת הכנסת המשותפת, על ממצאי הבחינה כאמור בפסקה (1);

(5) השר רשאי, לאחר הדיווח לפי הוראות פסקה (4), וכן בהתייעצות עם שר המשפטים, בהסכמת שר האוצר, באישור הוועדות האמורות באותה פסקה ובאישור הכנסת, לקבוע, בצו, כי ההוראות לפי חוק זה יחולו על כלל התושבים, וכן לקבוע כי תקופת המבחן תוארך לתקופה שלא תעלה על שנתיים נוספות, וכן כי החלת החוק תהיה הדרגתית ובתנאים, בהתאם לצו שיקבע;

(6) לא הוצא צו על פי פסקה (5) בתוך ארבע שנים מיום תחילתו של צו כאמור בפסקה (1), יימחק המאגר הביומטרי.

3. הגדרות

להלן הגדרות של מושגים עיקריים:

3.1 ביומטריה

זיהוי בעזרת מאפיינים פיזיולוגיים או התנהגותיים הניתנים למדידה ונותרים יציבים לאורך זמן ממושך.

3.2 דגימה ביומטרית – sample

דגימה ביומטרית היא ייצוג ממוחשב של מאפיין פיזיולוגי או התנהגותי. דגימה זו היא לרוב נתונים שהתקבלו מהתקן ביומטרי כלשהו (מצלמה, חיישן טביעות אצבע, סורק וכו'). דגימה יכולה להיות דגימת הייחוס ("gallery") או דגימה לצורך השוואה ("probe") וניתן על פיה לזהות את האדם ממנו ניטלה הדגימה. התוצאה של הדגימה יכולה להיות תמונה (image) או תבנית (template) שהיא נתון המיוצר מהתמונה. יצירת התבנית של טביעות האצבע במקרה שלפנינו תתבצע על פי תקן ISO 19794 פרק 2, כדי ליצור תבניות אינטראופרביליות ולא ליצור תבנית קניינית של ספק מסוים. לצורך זה בוצעה השוואה של שני תהליכים מתוקננים (תקן בינלאומי ISO 19794-2 ותקן אמריקאי ANSI 378) והועדפה התקינה הבינלאומית על פני התקינה היבשתית. אין כיום תקן מקובל דיו ליצירת תבניות מתמונות פנים.

3.3 הרכשה - enrollment

תהליך נטילת הדגימה הביומטרית באמצעות התקן ביומטרי. תהליך זה מתאפיין בין היתר ביכולת לבצע בדיקות איכות לדגימות הביומטריות כדי לבחור את הדגימה האיכותית ביותר, להבדיל מדגימה מאוחרת יותר, לצורך זיהוי או אימות, שמתאפיינת בדרך כלל בצורך להיות מהירה ככל האפשר (כמו בעת מעבר נוסעים בביקורת גבולות).

3.4 השוואה ביומטרית - matching

קבלת החלטה הסתברותית לגבי ההשתייכות של זוג דגימות ביומטריות (דגימת הייחוס ודגימה לצורך השוואה) לאותו אדם. בדרך כלל ההשוואה מבוצעת על ידי השוואת תבניות ולא על ידי השוואת תמונות.

3.5 ציון - score

ערך מספרי המתקבל מתהליך ההשוואה ומציין את ההסתברות להתאמה בין דגימת הייחוס לדגימה לצורך השוואה. ערך מרבי מציין התאמה מושלמת וערך נמוך מציין שוני מוחלט.

3.6 סף החלטה – threshold

מספר שמאפשר לסווג על פיו את ציון ההשוואה לשני מרחבים – זיהוי או דחייה. אם הציון קטן מהסף אזי מתקבלת החלטה של דחייה (זהות הנבדק לא אומתה), אחרת תתקבל החלטה של התאמה (כלומר זהות הנבדק אומתה). באופן אידיאלי יצור סף ההחלטה הפרדה ברורה בין המורשים לאלו

שאינם מורשים. באופן מעשי תיתכן חפיפה בין שתי הקבוצות (וכמעט תמיד יש חפיפה כזו), שתתבטא באירועי דחייה של מורשים או אישור של מתחזים. **קביעה נאותה של סף ההחלטה היא הכיול החשוב ביותר של מערכת ביומטרית כלשהי ואחת המסקנות החשובות של תקופת המבחן**.

3.7. אימות זהות – verification

תהליך שבו האדם טוען לזהות מסוימת והמערכת הביומטרית מאמתת טענה זו על ידי השוואה בין הדגימה מהאדם לדגימת ייחוס בודדת מתוך בסיס הנתונים. תהליך זה מכונה one to one. תוצאת התהליך היא אימות (התאמה) או שלילה של טענת הזהות. בהקשר של מסמכי זיהוי אימות מונע שימוש של מספר אנשים באותו תיעוד.

3.8. זיהוי - identification

תהליך שבו נסרק כל בסיס הנתונים או לפחות חלקו כדי להשוות בין הדגימה מהאדם לכל דגימות הייחוס בבסיס הנתונים. תהליך זה מכונה one to many. תוצאת התהליך היא הזהות (או קבוצת הזהויות) שיש לה את ההתאמה הגבוהה ביותר לדגימה מהאדם. תהליך כזה, שבו טענת זהות מוכחת או נשללת, מכונה גם "זיהוי חיובי" (“positive identification”). במהלך תקופת המבחן יקרה תהליך כזה, שבו תתקבל תשובה של זהות, רק עבור מקרים מעטים של חידוש תיעוד ומקרים של ניסיונות יזומים.

3.9. אירוע של אישור מתחזה – false acceptance

מצב שבו טענת זהות של אדם אומתה למרות שהמידע הביומטרי היה שייך לזהות אחרת. המשמעות בפועל של אירוע כזה היא פגיעה באבטחה. להלן ישמש הקיצור “FA” לצורך ציון של אירוע כזה.

3.10. אירוע של דחיית מורשה – false rejection

מצב שבו טענת זהות לא אושרה, למרות שהמידע הביומטרי שייך לזהות הנכונה. המשמעות בפועל של אירוע כזה היא פגיעה באיכות השירות (כגון יצירת תורים או הפנייה של מורשים לנוהל חריגים עקב אי זיהוי). להלן ישמש הקיצור “FR” לצורך ציון של אירוע כזה.

3.11. קצב קבלת מתחזים – false acceptance ratio

נתון זה מייצג את ההסתברות לאירוע מסוג FA. הוא תלוי באופן מובהק בסף ההחלטה. אם הסף נמוך מדי תאשר המערכת הביומטרית גם מתחזים לעיתים קרובות יותר (החלטה מקלה מדי).

3.12. קצב דחיית מורשים - false rejection ratio

נתון זה מייצג את ההסתברות לאירוע מסוג FR. גם נתון זה תלוי באופן מובהק בסף ההחלטה. אם הסף גבוה מדי תדחה המערכת הביומטרית גם כאלו שהם מורשים (החלטה מחמירה מדי).

3.13. הרכשה כפולה – duplicate enrollment

מצב בו שתי רשומות ביומטריות נפרדות (או יותר) שייכות לאותו אדם, המופיע בבסיס הנתונים בזהויות נפרדות. מצב זה יאפשר לאותו אדם לקבל זכויות שלא כדין ובעיקר לקבל שלא כדין תיעוד **שאיננו מזויף**, עבור שתי זהויות שונות או יותר. כדי למנוע מצב זה מבוצע חיפוש מסוג one to many על כל רשומה, כדי לוודא שמידע ביומטרי כלשהו מצביע רק על זהות יחידה. תהליך מעין זה, של חיפוש והצלבת זהויות כפולות, נקרא בשם de-duplication או גם תהליך מסוג many to many, כי כל זהות מושווית לכל יתר הזהויות שבמאגר. תהליך זה, שבו נבדקת לרוב טענה שמישהו מסוים איננו רשום במאגר נקרא לעיתים בשם "זיהוי שלילי" (“negative identification”).

יש לשים לב לכך שמשמעות השגיאות מסוג FA ו-FR במצב של de-duplication איננה זהה לזו של מערכת ביומטרית רגילה ותלויה באיזו הרכשה מדובר:

3.13.1. בעת הרכשה ראשונה

במצב זה כל שגיאת FA (זיהוי מוטעה) תתפרש כחשד להונאה כי המאגר **לא** מצפה למצוא את הרשומה. יש לבצע במקרה כזה בדיקה ידנית מול מערכת "אביב", תוך שימוש בתמונות המופחתות ובנתונים אלפה נומריים (מין, גיל וכד'), הן של הרשומה החדשה והן של הרשומה השנייה שאותרה כדומה לה.

המשמעות של שגיאת FR (חוסר זיהוי) היא קשה יותר - ניסיון הונאה שהצליח. שגיאה כזו אומרת שאותו אדם שכבר רשום במאגר לא זוהה ככזה. חשוב לציין כי ההסתברות לשגיאת FR על פי שתי אצבעות ופנים נמוכה מאד ואף זניחה. מנגד ההסתברות לאירוע כזה גבוהה הרבה יותר כאשר תעמודנה לרשותנו תמונות פנים בלבד, ללא טביעות אצבע, בגלל המובהקות הנמוכה יותר של נתון זה.

3.13.2. בעת הרכשה חוזרת

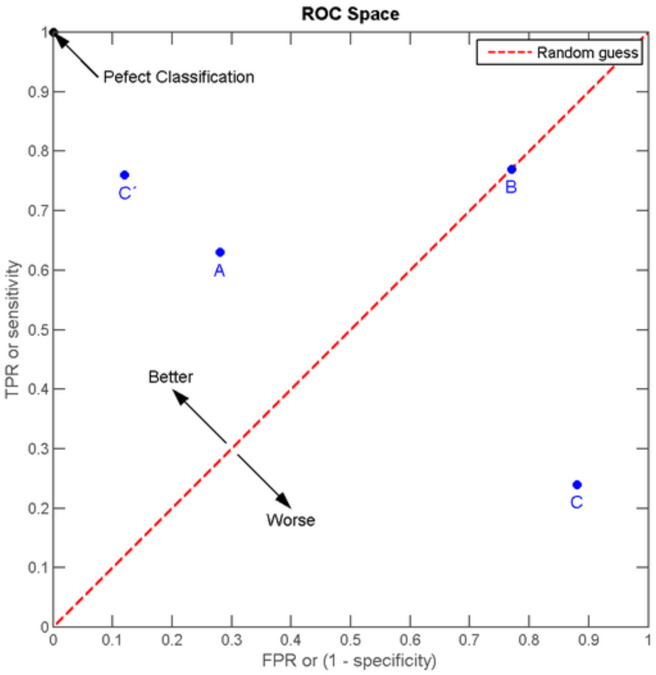
המשמעות של שגיאת FA בהרכשה חוזרת (כגון חידוש תיעוד) היא שהרשומה זוהתה, אך בתור מישהו אחר. גם כאן המשמעות היא התראה על חשד להונאה, שצריך לזכות או לאשר. בכל מקרה החיפוש איננו מסתיים עם הרשומה הראשונה המזוהה כך שבפועל תתקבלנה כל הרשומות הדומות ויבוצע סינון ידני שלהן.

המשמעות של שגיאת FR במצב זה היא התראת שווא על ניסיון הונאה כי הזהות שכבר אמורה להיות במאגר לא אומתה. גם כאן יושלם התהליך באמצעות טיפול ידני.

3.14. גרף ROC[2]

גרף כזה הינו צורה מקובלת להצגה חזותית של ביצועי מערכת ביומטרית, על ידי הצגת התלות ההדדית בין ה-FAR ל-FRR[3], תוך נטרול הנתון של סף ההחלטה. זוהי כאמור צורה מקובלת לבחון את הביצועים של המערכת ולראות האם סף ההחלטה מכויל כראוי. באופן אידיאלי גרף הנמצא על מערכת הצירים מצביע על מערכת טובה יותר (כאשר ה-FRR איננו אפס ה-FAR הוא אחד ולהיפך).

דוגמה לגרף ROC:



בדוגמה זו ציר ה-X הוא נתון ה-FPR (ההסתברות לאירוע מסוג FA) וציר ה-Y הוא ה-TPR (ההסתברות לזיהוי נכון). קו האלכסון מייצג מערכת שמבוססת על ניחוש אקראי (ההסתברות לאירוע FA היא 0.5 כאשר ההסתברות לאירוע של זיהוי תקין היא גם 0.5). נקודת ה-perfect classification מייצגת ודאות מוחלטת של זיהוי כאשר ההסתברות לזיהוי מוטעה היא אפס.

3.15. מערכת "אביב"

מערך המחשוב הראשי של רשות האוכלוסין שבו מנוהל מרשם האוכלוסין.

---

[2] ROC = Receiver Operational Characteristics, מושג ממלחמת העולם השנייה, מהמחקר שבוצע בארה"ב על יכולת הגילוי של מערכות מכ"ם מול התראות השווא המתקבלות מהן, בעקבות ההתקפה היפנית על פרל הארבור.

[3] מקובל להציג גרף כזה גם כתלות של ה-TPR (True Positive Ratio) מול ה-FPR (False Positive Ratio)

4. מטרות ויעדים

4.1. רקע

בהתאם להגדרות סעיף 41 של החוק[4], נועדה תקופת המבחן לבדוק את הנושאים הבאים:

- אופן היישום של הוראות החוק
- נחיצות קיומו של מאגר ביומטרי
- מטרותיו של המאגר הביומטרי
- המידע שיש לשמור במאגר הביומטרי
- אופן השימוש במידע זה

4.2. מטרות כלליות של תקופת המבחן

בהתאם לאמור בחוק תקופת המבחן נועדה כדי לענות בסיומה על השאלות הבאות:

4.2.1. כיצד מיושם החוק?

סוגיה זו נחלקת לסוגיות המשנה הבאות:

4.2.1.1. כיצד מיושם החוק?

השאלה שעליה יש לתת מענה היא "האם החוק מיושם בצורה טובה?". שאלה זו נגזרת ממורכבותו הרבה של החוק ומכך שהוא מפורט הרבה מעל למקובל בחקיקה אחרת. מטבע הדברים פירוט מעין זה מצמצם את מרחב אפשרויות היישום ולכן ראוי לבחון כל פרט ופרט ולוודא שיישומו תואם את לשון החוק בצורה מלאה. בחינה זו תתבצע על ידי סקרים ותיעוד ולא על ידי ניסוי מוגדר.

4.2.1.2. האם יש דרישות בחוק שלא יושמו כראוי

בהמשך וכהשלמה לשאלה הראשונה, השאלה כאן היא "האם יש נושאים שיישומם אינו תואם את לשון החוק?". גם במקרה זה אין מדובר בניסוי אלא בסקר.

4.2.1.3. האם יש לעדכן או לתקן את החוק

ללא קשר לתשובות על השאלות בסעיפים 4.2.1.1 ו-4.2.1.2 וקל וחומר אם עלו מהתשובות להן נושאים הדורשים תיקון או עדכון, השאלה כאן היא "האם התגלו מצבים או מקרים שמחייבים שינוי של החוק (גריעה, תוספת, עדכון)?".

---

[4] ראה נוסח החוק ב: http://www.knesset.gov.il/Laws/Data/law/2217/2217.pdf
ותיקונים ב: http://www.knesset.gov.il/Laws/Data/law/2233/2233.pdf , וראה נוסח של סעיף 41 בסעיף 2 של מסמך זה.

4.2.2. נחיצות קיומו של מאגר ביומטרי

סוגיה זו נחלקת לסוגיות המשנה הבאות:

4.2.2.1. האם מטרת החוק ראויה

השאלה שעליה יש לתת מענה היא "האם יש צורך להתמודד עם הרכשות כפולות?". שאלה זו הינה שאלת מדיניות מובהקת והיא נענתה כבר בחיוב בעצם החקיקה. הניסוי המתואר במסמך זה לא נועד לתת מענה על שאלה זו. למעשה אין, לדעת הגורמים המקצועיים, ניסוי בר ביצוע שיכול לתת מענה על שאלה זו והיא נותרת כשאלה של מדיניות ושל ניהול סיכונים שמקבלי ההחלטות ידרשו להכריע לגביה בתום תקופת הניסוי.

4.2.2.2. האם המאגר מתאים לייעודו

השאלה שעליה יש לתת מענה היא "האם ניתן לאתר ולמנוע הרכשות כפולות בעזרת המאגר?" או במילים אחרות "האם המאגר הביומטרי הוא כלי מתאים לאיתור ומניעת הרכשות כפולות?". שאלה זו תקבל מענה בתקופת המבחן כדי לוודא אם ניתן לאתר בעזרת המאגר הרכשות כפולות (תוך מזעור מצבי השגיאה השונים) או לא.

4.2.2.3. האם המאגר נחוץ/הכרחי

מתוך ההנחה שאנו נדרשים, כחלק מניהול הסיכונים בתיעוד הלאומי, לתת מענה לנושא ההרכשות הכפולות, השאלה שעליה יש לתת מענה כאן היא "האם המאגר נחוץ לשם כך או שיש כלים חלופיים שיכולים לאתר הרכשות כפולות?". גם לשאלה זו אין ניסוי ישיר שיכול לתת עליה מענה, כמוסבר בהמשך, והיא תיבחן באמצעות ניסוי עקיף, כמתואר בסעיף 11.1. ראה גם ניתוח חלופות בנספח 19.3 להלן.

4.2.3. מטרות המאגר

בתקופת המבחן יש לבחון שתי מטרות:

4.2.3.1. מניעת ואיתור הרכשות כפולות

זוהי כאמור מטרתו העיקרית והראשית של החוק והיא תיבדק באופן שוטף בתרחישי אמת ובאמצעות הדמיות, במסגרת הניסוי המתואר במסמך זה.

4.2.3.2. שימושים נוספים

בתקופת המבחן אוסר החוק על העברת מידע לגורמים שאינם רשות האוכלוסין ובהתאם לכך ייבחנו שימושים נוספים אך ורק באמצעות תרחישי הדמיה, בכפוף לאישור משפטי פרטני.

4.2.4. איזה מידע יישמר במאגר?

סוגיה זו נחלקת לסוגיות המשנה הבאות:

4.2.4.1. האם די במידע הנשמר

המדיניות שננקטה בעת עיצוב המאגר היא מדיניות מצמצמת שגורסת נטילה של מידע מזערי שדי בו כדי לתת מענה סביר לצורך. השאלה שיש לענות עליה אם כן היא "האם די בתמונת פנים וטביעות של שתי אצבעות מורות כדי לאתר הרשות כפולות ללא שיעור שגיאות שאיננו סביר או כזה שאיננו ניתן לטיפול?". שאלה זו תקבל מענה במסגרת הניסוי המתואר במסמך זה.

4.2.4.2. אם לא די - מה צריך להוסיף

במקרה של תשובה שלילית על סעיף 4.2.4.1 לעיל, השאלה היא "האם נדרש מידע נוסף כדי לממש את מטרות המאגר?". התשובה על שאלה זו לא תתקבל באמצעות ניסוי אלא באמצעות עבודת מטה, ככל שתידרש.

4.2.4.3. האם ניתן לגרוע מהמידע שבמאגר?

אם התשובה לסעיף 4.2.4.1 תהיה חיובית, השאלה שיש לתת עליה מענה היא "האם ניתן לגרוע מהמידע שיש במאגר?". שאלה זו תקבל מענה במסגרת הניסוי המתואר במסמך זה.

4.2.5. אופן השימוש במידע שבמאגר

השאלה בנושא זה היא "כיצד משתמשים במידע שבמאגר?". גם במקרה זה לא מדובר בניסוי אלא בסקר שיתעד את צורת השימוש ואת תהליכי העבודה השונים הנוגעים למידע ביומטרי.

4.3. מטרות ראשיות של הניסוי

מעבר למטרות הכלליות של תקופת המבחן, להלן המטרות הראשיות של הניסוי גופו, בחלוקה למטרות ארגוניות, טכנולוגיות והתנהגותיות:

4.3.1. מטרות ארגוניות

מטרות אלו נוגעות ליעוד המאגר, לשימוש בביומטריה באופן כללי, לאבטחת המידע ולצדדים התפעוליים של המערכת אותה מנסים בתקופת המבחן:

4.3.1.1. התאמת המאגר לצורך

בהמשך לנאמר בסעיף 41 של החוק, המטרה הראשית של תקופת המבחן היא בחינת המאגר ככלי למניעת הרכשות כפולות. הניסוי נועד כדי לבחון האם המאגר (וצורת המימוש שלו) הוא אכן המענה הראוי, והאם הוא מצדיק את התשומות הדרושות עבורו. הניסוי יכול לתת תשובה חיובית (המאגר עונה לצורך המוגדר ולשיקולי עלות-תועלת) או תשובה שלילית (המאגר איננו נותן מענה ראוי ומייצר למשל התראות שווא בכמות שאיננה סבירה או איננה ניתנת לטיפול). כמו מערכות אבטחה רבות, הבסיס להחלטה זו לא יהיה כמות ההרכשות הכפולות אלא ביצועי המאגר ויעילותו התפעולית, בעיקר בגלל חוסר היכולת לכמת את גורם ההרתעה של המאגר ובגלל

יכולת הבחירה של פושעים לא להתנדב לתקופת המבחן או לא לנסות לבצע הרשכות כפולות בתקופה זו. ההחלטה תסתמך על מספר פרמטרים מרכזיים:

4.3.1.1.1. יכולת איתור ניסיונות התחזות

האם המאגר מסוגל לאתר הרשכות כפולות.

4.3.1.1.2. רמת אבטחת המידע

האם ההגנה על המידע שבמאגר נאותה.

4.3.1.1.3. הגנה על הפרטיות

האם נעשה שימוש בנתונים אך ורק לצרכים המוגדרים בחוק, בתקנות ובצו.

4.3.1.1.4. איכות וביצועים

מהן היכולות של המערכת לניהול המאגר הביומטרי.

4.3.1.1.5. מקצועיות העובדים

האם הרמה המקצועית של עובדי המאגר נאותה.

4.3.1.1.6. יכולת עבודה אוטונומית

האם הרשות לניהול המאגר הביומטרי יכולה לפעול באופן אוטונומי בדגש על נושאי הטיפול במערכות המידע.

4.3.1.1.7. קיום הנחיות ונהלים

האם הנהלים קיימים, מאושרים ועובדים לפיהם, כולל מדיניות מאושרת ותהליכי עבודה מתאימים ומאושרים.

4.3.1.1.8. BCP/DRP[5]

יכולת התאוששות וחזרה לפעולה לאחר אסון.

4.3.1.2. השימוש בביומטריה

מטרה חשובה נוספת היא בחינת השימוש בביומטריה בכלל, כאשר המטרה היא מציאת הדרך המיטבית לכך מבחינה תפעולית. עצם השימוש בביומטריה על תעודת הזהות והדרכון הוא נושא שאיננו שנוי במחלוקת ואף מוגדר בתקינה הבינלאומית (בכל הנוגע לדרכון[6]) ובתקינה יבשתית שאנו מעוניינים לאמץ (כגון הדירקטיבה האירופאית בנושא זה[7]). ההתקדמות בעולם בנושא זה

[5] Business Continuity Plan = **BCP** (זמינות והמשכיות), Disaster Recovery Plan = **DRP** (התאוששות מתקלות ואסונות).

[6] ראה תקן ICAO שמספרו ***DOC9303 Part 1 Volume 2*** שהתקבל גם כתקן ***ISO 7501***.

[7] ראה החלטת מועצת האיחוד האירופאי "***COUNCIL REGULATION (EC) No 2252/2004***" מדצמבר 2004

גם היא נותנת רמת סמך גבוהה שניתן לעשות שימוש נרחב בביומטריה ועם זאת אנו נדרשים לבצע ניסוי, כדי לקבל תובנות על הצורה הטובה ביותר לשימוש זה ולהגיע למסקנות עצמאיות לגבי השימוש בביומטריה לקבלת החלטות ולהשגת מטרות המאגר. נזכיר כי כיום יותר ממאה מדינות מנפיקות דרכונים הכוללים שבב שיש בו לכל הפחות תמונת פנים שיכולה לשמש כנתון ביומטרי ומדינות רבות מתוכן כוללות בדרכונים שלהן גם טביעות אצבע (ובפרט מדינות האיחוד האירופאי). חלק מן המדינות הללו שומרות את הנתונים הביומטריים גם במאגרי מידע מרכזיים.

4.3.1.3. מתן מענה רחב

מטרה חשובה אחרת של תקופת המבחן היא מתן מענה לאוכלוסייה רחבה ככל האפשר, ובכלל זה אוכלוסיות בעלות צרכים מיוחדים ובעלי מוגבלויות.

4.3.1.4. התייעלות

כפי שצוין לעיל, הכללה של נתונים ביומטריים במסמכי הזיהוי עצמם כלל איננה שנויה במחלוקת. לאור זאת, ללא קשר לשאלת המאגר, נדרשת רשות האוכלוסין לבצע הרכשה ביומטרית לכל מי שיונפק לו מסמך זיהוי מהסוג החדש. מטרה ארגונית ראשונה במעלה היא מציאת תהליך יעיל וקצר לביצוע הרכשה זו כמו גם תהליך יעיל לצורך השימוש השוטף בביומטריה. המשמעות הישירה של תהליך יעיל ונוח היא שיתוף פעולה גדול יותר מצד האזרחים והתושבים, והענות גבוהה יותר מצדם. המטרה היא גם לגבש תהליך המטיל עומס לוגיסטי מזערי על רשות האוכלוסין, תוך שמירה על איכות גבוהה של התוצרים.

4.3.1.5. בחינת אבטחת המידע

בתקופת המבחן ייבחן נושא אבטחת המידע הביומטרי בצורה יסודית ומעמיקה, **<u>לא רק במאגר אלא לכל אורך המסלול שלו</u>**. באופן טבעי עיקר המאמץ יופנה למאגר עצמו, לרשות לניהול המאגר הביומטרי ולאבטחתו הפיזית והלוגית של המאגר, אך גם נושאים אחרים צריכים להיבדק ובפרט מחיקת מידע ביומטרי בלשכות רשות האוכלוסין ובמערכי ההנפקה כאשר מידע זה איננו נחוץ עוד.

4.3.2. מטרות טכנולוגיות

מעבר למטרות הארגוניות יש לניסוי מטרות טכנולוגיות:

4.3.2.1. צורת השימוש המיטבי בביומטריה

מלבד הנושאים הארגוניים והתפעוליים שפורטו לעיל נועדה תקופת המבחן לקבוע את צורת ההפעלה המיטבית של המערכות הביומטריות ובפרט לקבוע את סיפי ההחלטה של המערכות. סיפי ההחלטה אינם נוגעים רק להשוואות הביומטריות אלא גם למדידות האיכות של הנתונים

הביומטריים. איכות זו נבחנת במעמד ההרכשה, הן עבור טביעות האצבע והן עבור תמונות הפנים. איכות תמונות הפנים הינה קריטית במיוחד, כדי לתת מענה לאותה אוכלוסייה שלא ניתן ליטול ממנה טביעות אצבע. איכות תמונת הפנים מגדירה את מידת העמידה של תמונה זו בתקן ISO 19794[8]. בדיקת האיכות כוללת פרמטרים רבים, שלכל אחד מהם יש להגדיר סף שיאפשר לסווג את התמונה הנבדקת בהתאם. בנוסף לכך גם להתקנים הביומטריים עצמם יש פרמטרים מסוימים שיש צורך לכייל. אמנם המדיניות שננקטה בהקמת מערך ההרכשה היא שימוש עקבי במוצרים הטובים ביותר שהשוק יכול לספק ("best of breed") אך גם לגבי מוצרים אלו אנו נדרשים לקבוע את תצורת השימוש המיטבית.

4.3.2.2. בדיקת ההתקנים הביומטריים

מטרה חשובה נוספת היא אימות של ההתקנים הביומטריים (חיישן טביעות האצבע והמצלמה) וכלי התוכנה שנבחרו לצורך מערך ההרכשה ולצורך מערך המחשוב של המאגר, כדי לוודא שהם אכן פועלים כראוי ובהתאם למצופה מהם.

4.3.3. מטרות התנהגותיות

מטרה חשובה ביותר היא הסברה נכונה ומאוזנת לציבור כדי שיוכל לקבל החלטה מושכלת בנוגע לתיעוד החכם ולתועלות שבו. מטרה זו דורשת העברה לציבור של מידע נכון, שאיננו מוטה ואיננו חד צדדי. הצורך בחידוש התיעוד הלאומי ובהפיכתו לקשה לזיוף ברור לכל אולם המסע התקשורתי שהובל על ידי המתנגדים למאגר יצר פגיעה תדמיתית קשה, אותה יש לתקן. יתרה על כך – הפעלה מבצעית של התיעוד צפויה לעורר גל חדש של התנגדויות איתן נידרש להתמודד. מעבר לעצם הצורך וההצטרפות לניסוי בתקופת המבחן יש ללמד את הציבור כיצד לעשות שימוש נכון בטכנולוגיה הביומטרית, אילו תועלות לאזרח מתקבלות ממנה והיכן ראוי לעשות בה שימוש.

ראוי להזכיר בנושא זה את הוויכוח המתמשך על יחסי הגומלין בין הביומטריה והפרטיות. על פי הגישה המודרנית חשוב להגדיר נורמות שימוש במידע שיכול להיחשב פרטי[9] כדי שמי שמוסר מידע כזה ידע היטב את "גבולות הגזרה" של המערכת. מלבד הכשרת הלבבות לתיעוד החדש יש להביא את הציבור למצב שבו יידע היטב מה מותר לעשות עם מידע ביומטרי בכלל (ולא רק בהקשר לתיעוד לאומי), למי יש זכות לעשות זאת ובפרט למי אין זכות כזו. ראה גם פרק 17 בנושא זה.

---

[8] תקן בינלאומי לצילום פנים שעליו נסמך התקן הבינלאומי לדרכונים. כדי ליצור אחידות אומץ תקן זה גם עבור תעודת הזהות. ראה גם נספח 19.2 להלן. בפועל עמידה במלוא הדרישות של תקן זה איננה מעשית והשאיפה היא לעמוד בנגזרת של התקן. ראו מאמר הדן בנושא זה בשם "Compliance with facial image standards" מאת Uwe Seidel, שהופיע בירחון בשם:
Keesing journal of documents & identity, issue 19,2006

[9] ראה Helen Nissenbaum / "***PRIVACY IN CONTEXT Technology, Policy, and the Integrity of Social Life***", בהוצאת אוניברסיטת סטנפורד, ארה"ב. הלן ניסנבאום היא חוקרת באוניברסיטת ניו יורק, שהשפיעה בצורה חזקה על מדיניות ועל רגולציה בארה"ב בכל הקשור לפרטיות מידע של צרכנים ואף עסקה נקודתית במערכות ביומטריות והשימוש בהן מזווית הפרטיות.

4.4. מטרות נוספות של הניסוי

מלבד המטרות הראשיות שפורטו לעיל יש גם מספר מטרות נוספות, בדגש תפעולי וטכנולוגי, כגון:

4.4.1. מטרות טכנולוגיות

כאמור בסעיף 4.3.1.5 לעיל מטרה משמעותית ועיקרית היא בחינה כוללת של אבטחת המידע במערך המחשוב של המאגר ובמערכי ההרכשה וההנפקה. אבטחת מידע הינה תהליך שלם ולא רק שילוב של טכנולוגיה כזו או אחרת. בהתאם לכך מטרה חשובה נוספת שיש לתת עליה את הדעת בתקופת המבחן היא בחינה של **הכלים הטכנולוגיים** לאבטחת מידע ביומטרי בשלושת המערכים האלו (מערך המחשוב של רשות האוכלוסין וביקורת הגבולות, מערכי ההנפקה ומערך המחשוב של המאגר).

4.4.2. מטרות תפעוליות וארגוניות

מטרה ארגונית נוספת היא הכשרה ואימון של פקידי רשות האוכלוסין (וגופים אחרים, ככל שיהיו כאלו בתקופת המבחן) כיצד לבצע את התהליכים הביומטריים בצורה המיטבית בהתאם לחקיקה ולפני החלת חובת ההצטרפות למאגר על כלל האוכלוסייה, ככל שתהיה כזו בעתיד. בנוסף לכך נועדה תקופת המבחן לבחינת הצד התפעולי של הרשות לניהול המאגר הביומטרי ובחינת מנגנוני הפיקוח עליה.

4.4.3. מטרות הקשורות לביקורת הגבולות

מערך ביקורת הגבולות (המופעל על ידי רשות האוכלוסין) משולב בניסוי אולם יש למערך זה מאפיינים ייחודיים, השונים מיתר החלקים, בעיקר בשל העובדה שתהליכים המשלבים ביומטריה יתבצעו בעמדות לא מאויישות, בשירות עצמי (בדומה לעמדות הביומטריות הקיימות המתבססות על גאומטריית כף היד). חלק מהנתונים המפורטים להלן נוגעים גם לתהליכי ביקורת גבולות בכלל ולאו דווקא לתהליכים ביומטריים הנוגעים לאזרחים ישראליים.

להלן הנושאים שייבחנו בתקופת הניסוי בנתב"ג:

4.4.3.1. אימות ביומטרי באמצעות טביעת אצבע

יש לבחון את יעילות התהליך המתבסס על השוואת טביעת אצבע הניטלת מהעובר לנתוני ייחוס הנקראים מדרכונו. ראה פירוט התהליך מבחינה טכנולוגית בסעיף 6.3 להלן.

4.4.3.2. אימות ביומטרי באמצעות זיהוי פנים

יש לבחון את יעילות התהליך המתבסס על השוואת צילום פני העובר מול תמונת פניו הנקראת מדרכונו.

4.4.3.3. איכות הנתונים

מיכון המעבר מחייב בחינה של איכות הנתונים הנקראים, הן הדמוגראפיים והן הביומטריים בדרכון, מתהליך הרישום, ההרכשה וההנפקה.

4.4.3.4. זמני מעבר

יש לבחון זמני מעבר כוללים בכל אחד מסוגי התהליכים (עם שער פיזי, ללא שער פיזי, מעבר מבוסס צילום פנים, מעבר מבוסס טביעת אצבע, מעבר מבוסס אימות כפול).

4.4.3.5. זמני תת תהליכים במעבר

יש לבחון את זמני הסריקה, דגימה של תמונת פנים וטביעות אצבע, אימות של תמונת פנים וטביעות אצבע, עיבוד מול מערכת "רותם" ומול תשתית ההרשאות לקריאת מידע מהשבב, הדפסה של אסמכתה, פתיחת שער פיזי ככל שיש כזה).

4.4.3.6. רמות איכות

יש לבחון את ביצועי המערכת הביומטרית מבחינת דיוק ביחס לספים (ראה פירוט בפרק המדדים).

4.4.3.7. התפלגות הצלחה/כשלון - טביעות אצבע

בחינה של ביצועי ביומטריית טביעת אצבע עפ"י פרמטרים (סיפי החלטה שונים, מין, קבוצת גיל). ההתפלגות תיבחן מול נתונים שאינם כוללים מידע אישי.

4.4.3.8. התפלגות הצלחה/כשלון - זיהוי פנים

בחינה של ביצועי זיהוי הפנים עפ"י פרמטרים (סיפי החלטה שונים, מין, קבוצת גיל, תנאי סביבה כדוגמת תאורה). גם במקרה זה ההתפלגות תיבחן מול נתונים שאינם כוללים מידע אישי.

4.4.3.9. בחינת תהליכי זרימה

יש לבחון את תהליכי הטיפול בעוברים, עבור מקרים תקינים ועבור מקרים חריגים.

4.4.3.10.עומסים

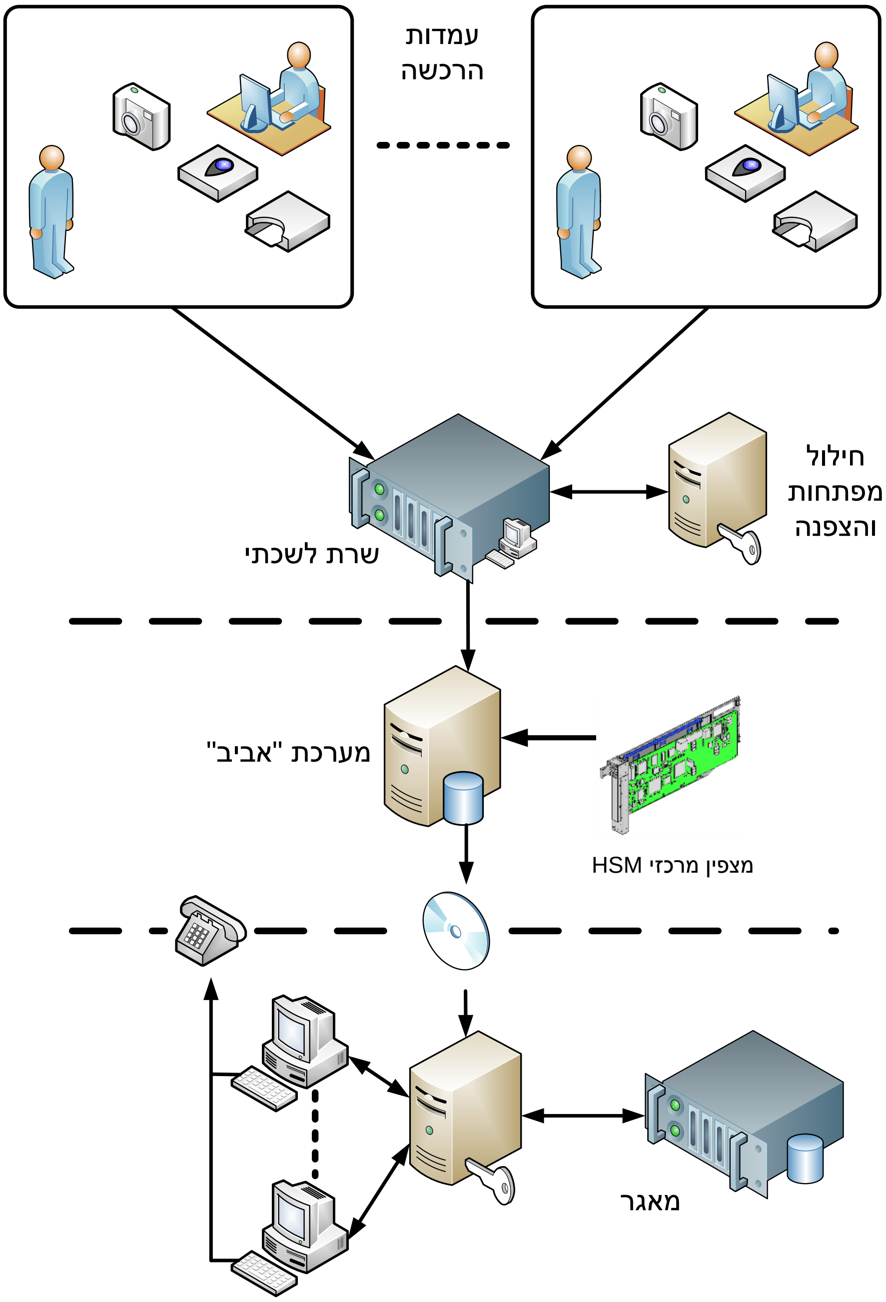
מדידת השפעה של עמדותהמעבר הביומטריות על עומסים במערכת "רותם" (מערכת המידע הראשית של ביקורת הגבולות).

4.4.3.11.תקינות המערכת

תקינות המערכת מבחינת תפעול, הנדסת אנוש, חומרה ותוכנה.

5. תיאור המערכת

להלן תיאור כללי של המערכת הביומטרית שתיבדק בתקופת המבחן, ללא החיבור למערכי ההנפקה של תעודת הזהות והדרכון:



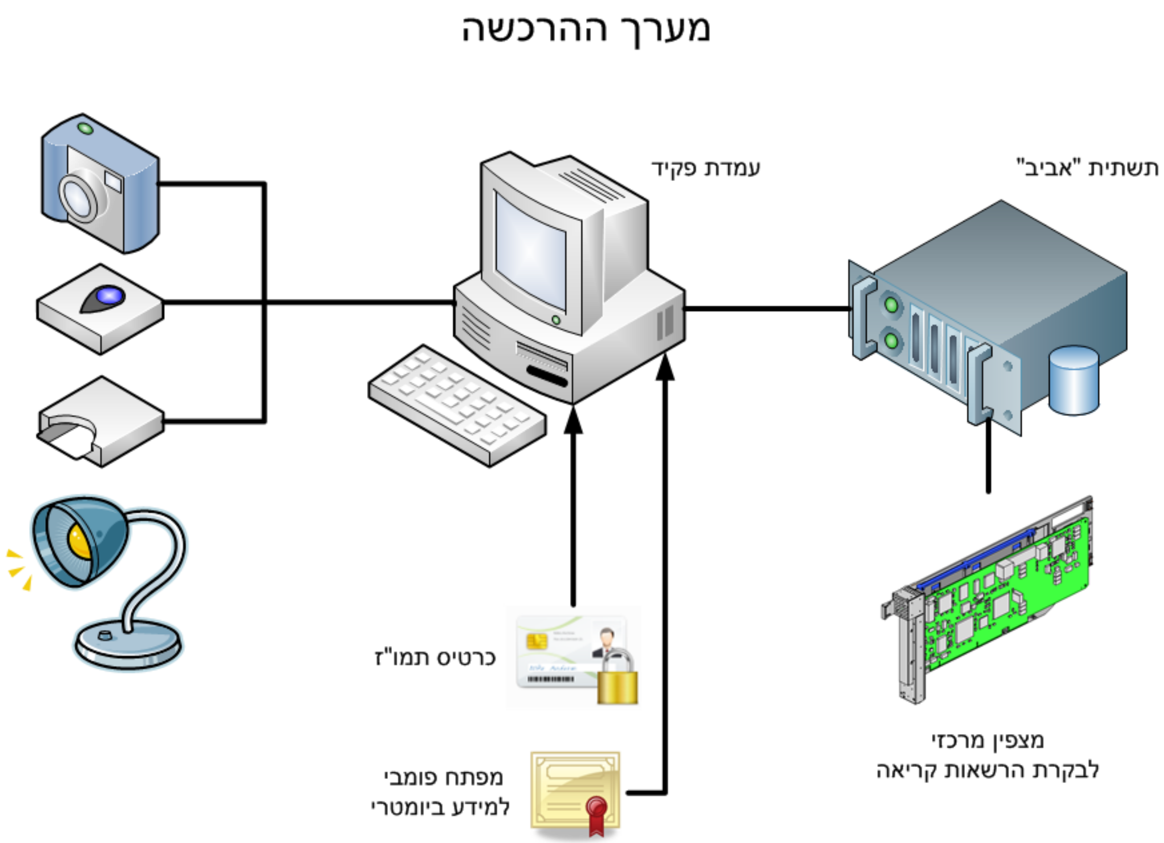
המערכת מורכבת מעמדות ההרכשה הפרוסות בלשכות רשות האוכלוסין, המצוידות בהתקנים ביומטריים (מצלמה וחיישן טביעות אצבע), ממערכת "אביב" וממערך המחשוב של המאגר, השייך לרשות לניהול המאגר הביומטרי ומנותק מיתר המערכת. בנוסף לכך מגיע המידע הביומטרי גם למערכי ההנפקה אולם שם

לא מבוצעת השוואה ביומטרית כלשהי ולאחר רישום המידע לתוך התיעוד הוא נמחק. במהלך תקופת המבחן תיבדק המחיקה של המידע במערכי ההנפקה, כמו גם נושאי אבטחת מידע אחרים, אולם הם אינם שותפים לתהליכי השימוש במידע ביומטרי ולכן חלקם בניסוי שולי. חלק נוסף הוא מערך ביקורת הגבולות, שישולב בניסוי לצורך בחינת השימוש המיטבי בביומטריה במסגרתו, כמפורט בסעיף 19.5 לעיל.

להלן תיאור מפורט של חלקי המערכת והתהליכים הקשורים בהם:

5.1. עמדת ההרכשה

עמדה זו הינה עמדת "אביב" רגילה, שהותקנה בה תוכנה מתאימה ושחוברו אליה ההתקנים הביומטריים. היא תבצע את תהליך ההרכשה (בעת ניפוק התיעוד) ואת תהליך ההשוואה (בעת מסירת תעודת זהות או בעת מתן שירות למי שיש כבר ברשותו תיעוד חכם).



5.1.1 רכיבי העמדה

עמדה זו מכילה חיישן טביעות אצבע, מצלמה ותאורה מתאימה. בנוסף לכך מכילה העמדה גם קורא כרטיסים (לצורך קריאת תעודת הזהות החכמה) וגישה באמצעות רשת רחבה למצפין מרכזי, המאפשר לפתוח את הרשאות הקריאה של מידע ביומטרי מהכרטיסים. בעמדה מותקנת תוכנה

מקומית המסוגלת לקבל תמונה "חיה" של טביעת אצבע מהחיישן (בצורת קובץ WSQ[10] תקני), לגזור ממנה תבנית (template) תקנית[11] ולהשוות את הדגימה החיה מהחיישן לנתונים הנקראים מהכרטיס.

5.1.2. הצפנה

המידע הביומטרי היוצא מעמדות ההרכשה למאגר, כאשר מבוצעת הרכשה, מוצפן באמצעות פרוטוקול הצפנה ייעודי[12]. פרוטוקול זה מבוסס על הצפנת כלאיים (hybrid encryption) כאשר המידע עצמו מוצפן במנגנון הצפנה סימטרי עם מפתחות אקראיים ובהמשך מפתחות אלו מוצפנים במנגנון א-סימטרי. בתהליך ההצפנה מתקבלים ערכי האתחול ומפתחות ההצפנה האקראיים ממחולל רחש אמיתי באמצעות חומרה ייעודית (TRNG[13]), המותקנת בכל שרת לשכתי. בכל עמדה נטען מפתח הצפנה פומבי למידע ביומטרי, המאפשר להצפין אולם אינו מאפשר לפענחו (כחלק ממנגנון ההצפנה הא-סימטרי). בנוסף לכך נחתמת כל בקשת הנפקה הנוצרת בעמדת הפקיד באמצעות חתימה אלקטרונית, על ידי כרטיס עובד אישי שברשותו (כרטיס תמו"ז, שהינו כרטיס עובד תקני במשרדי הממשלה).

5.1.3. קישוריות

תהליך ההרכשה הינו מקומי והמידע המופק ממנו מוצפן כבר בעמדת הפקיד. גם תהליך ההשוואה, הכולל קבלת תמונות מתעודת זהות או דרכון קיימים ומהחיישן, המרתן לתבניות והשוואתן, מבוצע **בצורה מקומית**. הקישוריות היחידה הנדרשת עבור ההשוואה היא גישה למצפין המרכזי, לצורך קבלת הרשאת הקריאה מתעודת הזהות או הדרכון. ללא קישוריות זו לא ניתן לקרוא מידע ביומטרי מהשבב שבתעודה או בדרכון.

5.1.4. תוצאות

בסיום ההשוואה יקבל הפקיד חיווי על כישלון או הצלחה וציון ההשוואה המדויק (בין המידע הנדגם והמידע שנקרא מהתיעוד) ירשם לקובץ היומן (log) אך לא יוצג לפקיד. המידע הביומטרי יימחק בתום התהליך בצורה שלא תאפשר שחזור שלו, באמצעות שימוש בכונן וירטואלי (RamDisk) הנמחק באופן מוחלט בעת סיום התהליך.

5.2. מערכת "אביב"

עמדות ההרכשה השונות, בלשכות רשות האוכלוסין, מחוברות באמצעות תקשורת רחבה (מוצפנת) למערך מחשוב מרכזי המנוהל על ידי רשות האוכלוסין.

---

[10] מבנה קבצים מתוקנן ע"י ה-FBI האמריקאי עבור טביעות אצבע.

[11] התבניות הן תבניות אינטראופרביליות על פי תקן ISO19794 המאפשרות אי-תלות בספק זה או אחר.

[12] ראה תיאור הפרוטוקול במסמך בשם "biometric data encryption" בגרסתו העדכנית. מסמך זה הינו מסמך מסווג.

[13] TRNG = True Random Number Generator, התקן שמספק מידע עתיר אנטרופיה

5.2.1. נגישות למידע ושמירתו

לאחר ההצפנה ומחיקת המידע הגלוי עמדת ההרכשה או מערכת "אביב" אינן נגישות יותר למידע הביומטרי הגלוי מתהליך ההרכשה, כי אין להן את מפתח הפענוח הדרוש לכך[14]. מערכת "אביב" משמשת בשלב זה רק לאגירה זמנית של המידע המוצפן, לצורך העברתו במנות קצובות למאגר ולמערכי ההנפקה. המערכת המרכזית, הנמצאת במרכז המחשבים של "אביב", גם חותמת על כל מנה כזו כדי לאפשר למאגר ולמערכי ההנפקה לאמת את מקורו של המידע, לדחות מידע ממקורות אחרים ולהגן על המידע כנגד שינויים זדוניים. מלבד החתימה על מארז של בקשות הנפקה תיחתם כל בקשה בנפרד, באמצעות כרטיס תמו"ז[15] של הפקיד שטיפל באותה בקשה.

5.2.2. מידע הנשמר

מערכת "אביב" איננה שומרת מידע ביומטרי מההרכשה וכוללת אך ורק שמירה של תמונות מופחתות[16], כחלק מרשומת האזרח שבה ובהתאם להוראות החוק[17]. צורת השימוש בתמונות אלו מוגדרת אף היא בחוק.

5.3. המאגר

מערכות המידע של המאגר מופעלות ומנוהלות על ידי הרשות לניהול המאגר הביומטרי.

5.3.1. רכיבי המאגר

מערך המחשוב של המאגר יפעיל תוכנות השוואה מסוגים שונים, על פי מדיניות החיפוש שתוגדר בו. מדיניות זו תכלול איחוד (fusion) של השוואות פנים וטביעות אצבע ובמידת הצורך שימוש במספר אלגוריתמים לכל סוג ביומטריה (בדגש על טביעות האצבע). השימוש במספר אלגוריתמים נועד לייעל את תהליך החיפוש ולשפר את ביצועיו.

5.3.2. תשובות מהמאגר

על פי דרישת החוק המאגר איננו מקוון ואיננו מחובר לרשתות תקשורת חיצוניות כלשהן. בהתאם לכך התשובות מהמאגר תהיינה טלפוניות עם שליחה במקביל באמצעות דוא"ל ממערכת נפרדת שאיננה מחוברת לרשת הפנימית של המאגר. דוא"ל זה נדרש לצורך אסמכתא ולא יכיל מידע מתוך המאגר אלא רק תוצאת זיהוי.

---

[14] ההצפנה היא א-סימטרית ומפתח הפענוח שונה ממפתח ההצפנה, כך שניתן להפריד בין היכולת להצפין והיכולת לפענח.

[15] כרטיס חכם אישי המשמש לצורך גישה מאובטחת למערכות מידע ממשלתיות.

[16] ראה מסמך בשם "***creating reduced pictures dd-mm-yyyy***" בגרסתו העדכנית.

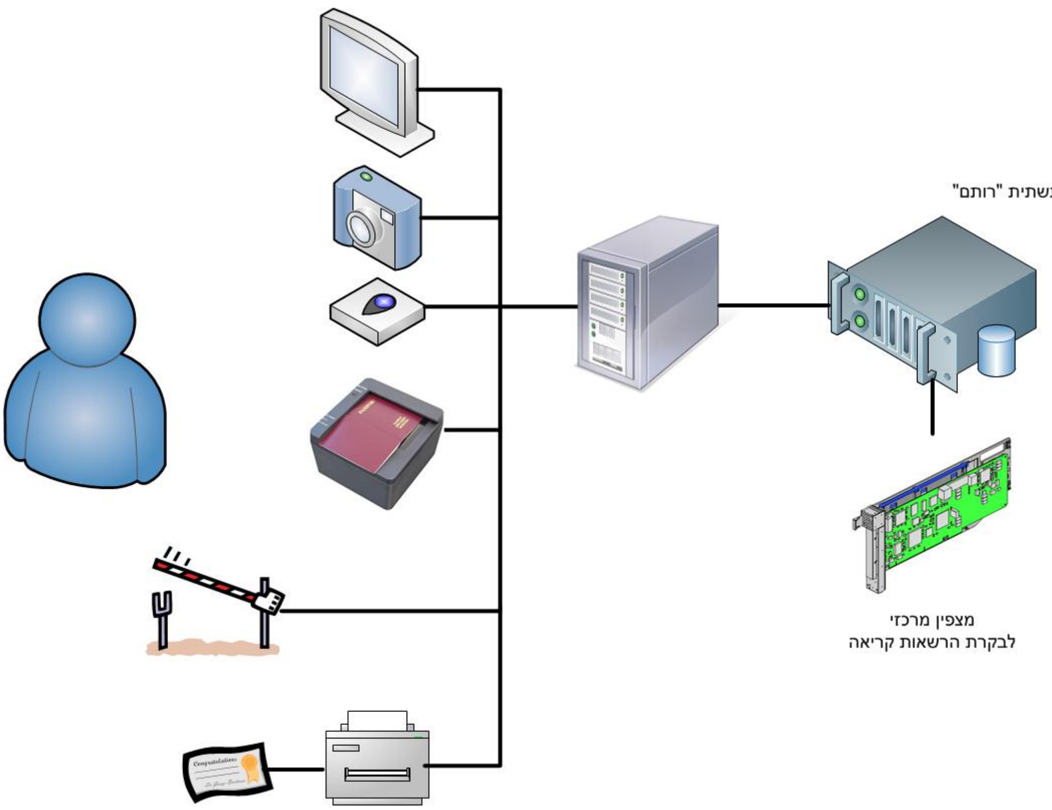
[17] ראה סעיף 27 בחוק http://www.knesset.gov.il/Laws/Data/law/2217/2217.pdf

5.3.3. גישה למאגר

בתקופת המבחן לא תותרנה שאילתות של גורמים נוספים למאגר והשירות היחידי יינתן לרשות האוכלוסין, לצורך הנפקת תיעוד. יתר תרחישי השימוש ייבדקו בעזרת הדמיות (סימולציות) בלבד.

5.4. מערך ביקורת הגבולות

מערכות המידע של ביקורת הגבולות מופעלות ומנוהלות על ידי רשות האוכלוסין.



5.4.1. רכיבי מערכת ביקורת הגבולות

מערך המחשוב של ביקורת הגבולות כולל מערכת מידע ראשית (הנקראת מערכת "רותם") וכוללת כבר היום ממשק למערכת ביומטרית ישנה המופעלת משנת 1997 על ידי רשות שדות התעופה ומתבססת על גאומטריית כף היד כאמצעי אימות זהות. מערכת "רותם" יכולה לקבל ממערכת זו חיווי על הצלחת אימות או על כישלון ומחזירה למערכת זו נתונים על זכאות מעבר (ללא גישה למידע הביומטרי בפועל). בתקופת הניסוי אליה מתייחס מסמך זה תשולבנה במערכת ביקורת הגבולות עמדות מעבר לא מאויישות שתתבססנה על השוואת העובר לנתוני ייחוס שייקראו מדרכונו (ראה

פירוט נוסף בנספח 19.5 לעיל). עמדות אלו תכלולנה חיישן טביעות אצבע, סורק דרכונים אופטי, מצלמה, מדפסת, מסך הנחייה לעובר ובחלק מהמקרים תכלול גם שער פיזי.

5.4.2. נגישות למידע ושמירתו

מעבר בעמדה לא מאויישת של ביקורת הגבולות יתבסס כאמור על השוואה בין העובר למידע הנקרא מדרכונו. בהתאם לתקינה הבינלאומית קריאת טביעת אצבע מדרכון מחייבת תהליכי אימות המבוססים על הצפנה חזקה מאד (ובפרט מנגנון הנקרא בשם EAC[18] וקיים גם בדרכון החכם הישראלי, במודל זהה לזה המקובל באיחוד האירופאי). עמדת הקריאה נדרשת "להוכיח" לשבב שיש לה הרשאת קריאה למידע זה. תהליך זה מחייב נגישות למצפין מרכזי המותקן במערכת "רותם" ומיועד לניהול ההרשאות האלו.

קריאת תמונת הפנים מהשבב איננה מחייבת תהליכי אימות כאלו (למעט קיום של תקשורת מוצפנת כמתואר בסעיף 6.3 להלן). לאחר קריאת המידע מהשבב וביצוע ההשוואה יימחק מידע זה ולא יהיה נגיש יותר.

5.4.3. המידע הנשמר

מערכת "רותם" ובכלל זה עמדות המעבר אינן שומרות מידע ביומטרי בהתאמה להוראות החוק.

[18] EAC = Extended Access Control, ראה פירוט בתקן ICAO בנושא ובמסמכי התקן הנלווים.

6. תרחישים

להלן תיאור כללי של התרחישים השונים שייבחנו בתקופת המבחן. ראה תיאור מפורט של תרחישים אלו בסעיף 9.3 להלן.

6.1. הרכשה

תרחיש ההרכשה יבוצע כולו בלשכות רשות האוכלוסין ויכלול את השלבים הבאים (מתוך הנחה שזוהי ההרכשה הראשונה עבור אותו אזרח/תושב):

6.1.1. מתן הסכמה

האזרח או התושב צריך להביע את הסכמתו להיכלל במאגר בתקופת המבחן ולחתום על טופס ההסכמה.

6.1.2. רישום

תבוצע בדיקה של בקשת ההנפקה מבחינת התנאים המנהלתיים (תשלום האגרה עבור הדרכון, זכאות וכו'). בשלב זה הפקיד יקבל חיווי אם לאזרח שלפניו יש כבר תעודה חכמה. מקרה כזה יטופל כחידוש תיעוד, המתואר בהמשך.

6.1.3. אימות באמצעות תשאול (ABI[19])

תהליך זה כולל אימות של זהות האזרח או התושב באמצעות סדרת שאלות אקראיות שהתשובה עליהן אמורה להיות ידועה לאזרח/תושב אולם לא לאחרים, ותשובה זו אינה מופיעה בתעודת הזהות או הספח שלה.

6.1.4. צילום פנים

צילום הפנים יבוצע באמצעות עמדת הצילום הייעודית המותקנת בדלפקי קבלת הקהל של רשות האוכלוסין. המטרה היא לקבל צילום איכותי, קרוב ככל הניתן להגדרות המופיעות בנספח A של תקן ISO/IEC 19794 פרק 5. באופן מעשי המטרה היא לתת מענה לנגזרת של תקן זה ולא למלוא דרישות התקן[20] (ראה פירוט בטבלה שבנספח 19.2 להלן). תמונת הפנים נשמרת בתעודת הזהות ובדרכון בקובץ מוגן. ראה פירוט מנגנוני ההגנה בתיעוד של תל"מ[21] ובתקן ICAO לדרכונים.

---

[19] **ABI** = **A**uthentication **B**y **I**nterview

[20] ראו מאמר הדן בנושא זה בשם "Compliance with facial image standards" מאת Uwe Seidel, שהופיע בירחון בשם: ***Keesing journal of documents & identity, issue 19,2006***

[21] **תל"מ** הינו הכינוי של פרויקט תעודות הזהות החדשות (ראשי תיבות של "**ת**יעוד **ל**אומי **מ**מוחשב").

- בלמ"ס -

התהליך יכלול צילום ואחריו בדיקת איכות התמונה. ניתן לחזור על הצילום לכל היותר שש פעמים ואם כל הניסיונות לא הניבו תמונה תקינה יידרש אישור מנהל על שימוש בתמונה הטובה ביותר, שתיבחן ידנית.

הערה: צילום פנים יבוצע תמיד ללא משקפיים.

6.1.5. נטילת טביעות אצבע

קבלת דגימה ביומטרית משתי האצבעות המורות תבוצע באמצעות החיישן המותקן בדלפק קבלת הקהל. עבור כל אצבע יבוצעו לכל היותר שישה ניסיונות נטילה, כמפורט בצו. נתון זה יישמר בתעודת הזהות ובדרכון, בקובץ מוגן שהגישה אליו מחייבת שימוש במפתחות הצפנה. ייתכנו מקרים שבהם תבוצע נטילה של טביעות אצבע מאצבעות אחרות, כמפורט בצו.

6.1.6. נטילת דוגמת חתימה

כאשר ביקש האזרח דרכון תורכש גם דוגמת חתימה באמצעות לוח (tablet) ייעודי. נתון זה איננו נתון ביומטרי והוא יילקח כאמור רק אם האזרח נזקק לדרכון ונמצא בטווח הגילאים המתאים. נתון זה איננו נשמר במערכות המידע השונות אלא רק בקובץ ייעודי בדרכון הנקרא DataGroup7[22]. דוגמת החתימה גם תודפס בדף הפרטים של הדרכון, בתהליך מילוי הפרטים. קובץ זה נגיש לכל קורא ומוגן בצורה דומה לקובץ תמונת הפנים, באמצעות מנגנון BAC[23].

6.1.7. הצפנת הנתונים

המידע הביומטרי שהורכש (וגם דוגמת החתימה הגרפית עבור הדרכון, שאיננה מידע ביומטרי) יוצפן באמצעות מנגנון הצפנה א-סימטרי[24], כך שעמדות המחשב של רשות האוכלוסין יכולות לבצע הצפנה אולם אינן יכולות לפענח מידע זה לאחר מחיקת המידע הגלוי. למעשה מוצפן המידע עם מפתחות סימטריים המוגרלים מחדש עבור כל רשומה ומפתחות אלו בתורם מוצפנים באמצעות המנגנון הא-סימטרי[25] (הצפנת כלאיים - hybrid encryption).

[22] ראה תקן ICAO בשם ***DOC9303 part 1 volume 2*** שהתקבל גם כתקן ISO7501.

[23] ראה תקן ICAO בשם ***DOC9303 part 1 volume 2*** שהתקבל גם כתקן ISO7501.

[24] תהליך הצפנה המתבסס על מפתח נפרד להצפנה ומפתח נפרד לפענוח, ללא יכולת להגיע מאחד לשני.

[25] ראה תיאור המנגנון במסמך "***biometric data encryption dd-mm-yyyy***" בגרסתו העדכנית. **מסמך זה הוא מסמך מסווג.**

6.1.8. העברה למערכת "אביב"

המידע המוצפן יועבר בתקשורת רחבה מוצפנת למערכת "אביב", שתעביר אותו בהמשך למערכי ההנפקה ולמאגר.

6.2. זיהוי ביומטרי מול תעודת זהות

תרחיש זה כולל את השלבים הבאים עבור תעודת הזהות ויבוצע בלשכות רשות האוכלוסין[26]:

6.2.1. הכנסת כרטיס תעודת זהות לקורא

כרטיס תעודת הזהות יוכנס לקורא כרטיסים תקני, המותקן ברוב עמדות קבלת הקהל של רשות האוכלוסין.

6.2.2. קריאת נתונים מנהלתיים

יש לקרוא מהכרטיס מספר נתונים מנהלתיים שיאפשרו לבחור את מפתחות ההצפנה המתאימים לאותו כרטיס לצורך פתיחת הרשאות הקריאה. מידע זה איננו דורש הרשאה לקריאתו ואיננו כולל מידע אישי מעבר לשם, מספר זהות ותאריך לידה.

6.2.3. פנייה למצפין מרכזי

לאחר מכן תבוצע פנייה למצפין מרכזי (HSM[27]) המותקן במערכת "אביב" לצורך קבלת תעודות דיגיטאליות מתאימות שתאפשרנה קריאת מידע ביומטרי מהכרטיס. למעשה נדרשת תשתית המחשוב לחתום על אתגור שינפיק הכרטיס באמצעות מפתח הצפנה הקשור לאותן תעודות דיגיטאליות.

6.2.4. פתיחת הרשאת קריאה

עמדת הקריאה תוכיח לכרטיס שיש לה את ההרשאה לקרוא את קובץ טביעות האצבע באמצעות התעודות הדיגיטאליות שהתקבלו מהמצפין המרכזי ואחר כך על ידי חתימה באמצעות מפתח תואם על אתגור אקראי שהכרטיס ינפיק. הדרכון ותעודת הזהות פועלים מבחינה זו בצורה דומה.

6.2.5. קריאת מידע ביומטרי

המידע הביומטרי ייקרא מהכרטיס בהתאם לרמת ההרשאה של העמדה (תמונת פנים בלבד, טביעות אצבע בלבד או שניהם). במקרה של תמונת פנים יתקבל קובץ מסוג JPEG2000[28] ובמקרה של טביעות האצבע יתקבלו שני קובצי WSQ[29].

---

[26] ייתכן שקריאת נתונים ביומטריים במקומות אחרים תמומש באמצעות ארכיטקטורה שונה.

[27] Hardware Security Module = **HSM**, מצפין הממומש באמצעות חומרה ייעודית מוגנת.

[28] JPEG2000 הינה שיטת דחיסת תמונה מיטבית עבור תמונות פנים.

6.2.6. דגימה ביומטרית

תבוצע נטילה של דגימה ביומטרית "חיה" באמצעות החיישן המחובר לעמדה. התוצאה תהיה קובץ מסוג WSQ.

6.2.7. השוואה

תוכנת ההשוואה תשווה את הדגימה החיה למידע שנקרא מהכרטיס ותספק את ציון ההתאמה. ההשוואה עצמה מבוצעת על ידי המרת התמונות לתבניות (templates) והשוואה בין התבניות.

6.2.8. הצגת התוצאה

התוכנה תציג למפעיל את התוצאה הנגזרת מציון ההתאמה: אישור (הציון שהתקבל הוא מעל לסף ההחלטה), דחייה (הציון מתחת לסף בצורה מובהקת) או צורך בניסיון חוזר (הציון גבולי).

6.2.9. מחיקת מידע ביומטרי

כל מידע ביומטרי שטופל במהלך ההשוואה יימחק בצורה שלא תאפשר לשחזרו. ראה תיאור טכנולוגי מפורט של אופן המחיקה במסמך נפרד[30].

6.3. זיהוי ביומטרי מול דרכון

תסריט זה כולל את השלבים הבאים עבור זיהוי מול הדרכון ויבוצע בשלב מאוחר יותר[31] בלשכות רשות האוכלוסין או בעמדה ביומטרית במעבר גבול (בתנאי שיש לו הרשאה מתאימה לגישה למידע הביומטרי):

6.3.1. אחזור רשומת MRZ[32]

בהתאם לתקן הבינלאומי, קריאת מידע מדרכון הכולל שבב מוגנת כדי למנוע קריאה קלה של המידע כאשר הדרכון נישא על ידי האזרח בכיסו. הגנה זו מתבססת על מפתח הצפנה שנגזר ממידע מודפס, כלומר יש לקרוא מהדרכון מידע מודפס כלשהו כדי לגזור ממנו את מפתח ההצפנה שישמש אחר כך לתקשורת עם השבב. מידע זה הינו רשומת ה-MRZ שתאוחזר מהדרכון על ידי הנחת הדרכון על קורא אופטי ייעודי שימיר רשומה מודפסת זו למידע דיגיטאלי במחשב. חלופה אחרת היא קריאת מספר הדרכון המופיע כברקוד בדף מס'3 באמצעות קורא ברקוד (או על ידי הקלדתו) ואחזור רשומת ה-MRZ מתוך בסיס הנתונים של מערכת "אביב". על רשומה זו, ובפרט על שורת ה-MRZ השנייה, יופעל תהליך חישובי תקני, כמפורט בתקן ICAO. תהליך חישובי זה נועד לחשב את מפתח ההצפנה

---

29 **WSQ** = **W**avelet **S**calar **Q**uantization, שיטת דחיסת תמונה מיטבית עבור טביעות אצבע שתוקננה על ידי ה-FBI האמריקאי ואומצה ברחבי העולם גם לצרכים אזרחיים.

30 מסמך זה הינו מסמך רגיש וכולל פרטים טכנולוגיים רבים שהם מחוץ לתחום של מסמך הניסוי.

31 השאיפה היא לטפל בנושא זה שלושה חודשים לאחר התייצבות המערכת וההנפקה השוטפת לאזרחים.

32 **MRZ** = **M**achine **R**eadable **Z**one, שתי שורות המודפסות בגופן תקני ומיועדות לקריאה ממוכנת.

האישי של אותו דרכון, שבאמצעותו תוצפן כאמור התקשורת מול השבב בהמשך. מנגנון זה נקרא בשם BAC[33].

6.3.2. תקשורת מול השבב

מפתח ההצפנה שחושב מתוך נתוני ה-MRZ ישמש לצורך פתיחת ערוץ תקשורת מוצפן ומאובטח מול השבב (בתהליך המכונה בעגה המקצועית בשם “secure messaging”). הגנה זו על המידע נועדה כאמור להקשות על קריאה לא מורשית מהדרכון. התקשורת מול השבב שבדרכון תבוצע באמצעות קורא כרטיסים חכמים ללא מגע על פי תקן ISO14443. קורא מסוג זה יותקן בהמשך בכל לשכה של רשות האוכלוסין אולם לא בכל עמדת קבלת קהל. יתכן שימוש בקורא משולב לכרטיסי מגע ולכרטיסים ללא מגע, כמו זה שמתואר בתמונה הבאה (מתוצרת חברת HID Omnikey):

יתכן במקרים מסוימים גם שימוש בקורא משולב ייעודי, המכיל את הקורא האופטי ואת הקורא של השבב במארז יחיד (נקרא גם קורא מסוג "full page"):

[33] **BAC** = **B**asic **A**ccess **C**ontrol, ראה תקן ICAO.

- בלמ"ס -

6.3.3. קריאת תמונת הפנים

במידת הצורך תבוצע קריאה של תמונת הפנים מהשבב. קריאת קובץ זה של תמונת הפנים (הנקרא בתקן בשם DataGroup2) היא חופשית ואין צורך בהרשאה מיוחדת לקריאתה, למעט מפתח ההצפנה שחושב בסעיף 6.3.1 לעיל. התוצאה המתקבלת היא קובץ JPEG2000.

6.3.4. פתיחת הרשאת קריאה

אם יש צורך לקרוא את קובץ טביעות האצבע (הנקרא בתקן בשם DataGroup3) תוכיח עמדת הקריאה לשבב את הרשאתה באמצעות תעודות דיגיטאליות הנמצאות ברשותה. תעודות אלו הן בעלות תוקף זמני וקצר (משמרת בודדת, יום או לכל היותר מספר ימים). תהליך זה הינו תהליך תקני מקובל, שאומץ עבור כל דרכוני האיחוד האירופאי ומכונה EAC (Extended Access Control)[34].

6.3.5. קריאת מידע ביומטרי

לאחר קבלת הרשאת הקריאה ייקרא המידע הביומטרי מקובץ טביעות האצבע שעל השבב בדרכון. התוצאה שתתקבל היא אובייקט מידע שמכיל שני קובצי WSQ, עבור שתי האצבעות שנסרקו. בדרך כלל תבוצע קריאה של אצבע אחת והשוואה. קריאת האצבע השנייה תבוצע על פי הצורך.

6.3.6. דגימה ביומטרית

תבוצע נטילה של דגימה ביומטרית "חיה" באמצעות חיישן המחובר לעמדה. גם במקרה זה התוצאה היא קובץ WSQ.

6.3.7. השוואה

תוכנת ההשוואה תשווה את הדגימה החיה למידע שנקרא מהשבב ותספק ציון התאמה. ההשוואה נעשית על ידי המרת קובצי ה-WSQ הנ"ל לתבניות והשוואה בין התבניות.

6.3.8. הצגת התוצאה

התוכנה תציג למפעיל את התוצאה: אישור (הציון שהתקבל הוא מעל לסף ההחלטה), דחייה (הציון מתחת לסף בצורה מובהקת) או ניסיון חוזר (הציון גבולי). אם העמדה היא עמדה לא מאוישת (כמו עמדת ביקורת גבולות אוטומטית) יתקבל חיווי ברור לנבדק: הדפסת אסמכתה (“gatepass”), פתיחת המעבר (כאשר יש שער פיזי) או הפנייה לטיפול בעמדה מאויישת.

6.4. חיפוש הרכשה כפולה

תרחיש זה יבוצע במאגר בלבד, עבור כל פעולת הרכשה, ויכלול את השלבים הבאים:

6.4.1. קבלת הנתונים

הנתונים המוצפנים יפוענחו במאגר ויעברו הצפנה מחדש לאחר העברתם לרשת הפנימית. מעבר זה לרשת הפנימית מבוצע באמצעות ערוץ חד כיווני וכולל גם תהליך סינון תוכן. הנתונים כוללים את

[34] ראה מסמך *Technical Guideline TR-03110: Advanced Security Mechanisms for MRTD – EAC, V1.11*.

תמונת הפנים, טביעות של שתי אצבעות ונתון מזהה ייחודי שישמש כאינדקס של הרשומה במאגר (ושאיננו פריט מרשם מקובל כגון מספר זהות). בנוסף לכך, במידת הצורך, יתקבלו גם מדדי האיכות של הנתונים הביומטריים, כדי לאפשר שימוש בהם וכדי להימנע מהצורך לחשבם מחדש בכל השוואה.

6.4.2. חיפוש מסוג one to many

יבוצע חיפוש שיאתר את הרשומה שמידת ההתאמה שלה למידע היא הגבוהה ביותר. יתכן שחיפוש זה יניב מספר תוצאות, בהתאם לאיכות הדגימה. תוצאות אלו תדורגנה בהתאם למידת ההתאמה שלהן.

6.4.3. סינון התוצאות

התוצאות תעבורנה סינון אנושי במידת הצורך. סינון זה יבוצע על ידי מפעילי המאגר.

6.4.4. קבלת החלטה

ההחלטה יכולה להיות "חיובית" (התאמה: הזהות המוצהרת נכונה), "שלילית" (חשד להתחזות: הנתונים הביומטריים שייכים לזהות אחרת ולא לזהות המוצהרת) או "רשומה חדשה" (אין במאגר רשומה קיימת עם מידת התאמה מספקת).

6.4.5. העברת התוצאה

כאשר תתקבל מנת בקשות הנפקה וכולן תקינות (אישור חיובי) יקבלו מפעילי מערכי ההנפקה אישור לכל המנה ולא אישור פרטני לכל רשומה. כאשר תתגלה בעיה (חשד להרכשה כפולה) תתקבל תשובת דחייה פרטנית לרשומה הבעייתית (ללא נתונים ביומטריים). כל הרשומות החדשות, שלא תימצא להן רשומה דומה תקבלנה אישור חיובי בהגדרה.

הערה: התשובות היוצאות מהמאגר אינן תשובות מקוונות מתוך רשת המאגר אלא תשובות שיכולות להיות טלפוניות בלבד. בפועל התשובות תועברנה במקביל לשיחת הטלפון באמצעות מערכת שאיננה מחוברת למאגר (מסכים ייעודיים במערכת "אביב") כאסמכתה.

6.5. אימות זהות

תרחיש זה הינו מקרה פרטי של חיפוש הרכשה כפולה, כאשר יודעים שיש כבר רשומה קיימת לאותו אדם. מצב זה יתרחש בתקופת המבחן רק בעת חידוש תיעוד או בעת הדמיה יזומה של שאילתה משטרתית. לאחר אימות מוצלח (התאמה, כלומר אישור חיובי) תעודכן הרשומה הביומטרית עם המידע

החדש והמידע הקודם יימחק (אם איכות המידע החדש גבוהה דיה[35]). מחיקה הינה מחיקה לוגית, כלומר המידע הקודם עדיין יישמר בטבלאות בסיס הנתונים.

6.6. זיהוי מול מאגר

בתקופת המבחן לא ניתן להגיש שאילתות למאגר מגורמים אחרים (כגון המשטרה) ולכן יש לבצע אך ורק הדמיה (סימולציה) יזומה של שאילתות כאלה, ללא מתן תשובה בפועל. בנוסף יש לבצע ניסיונות יזומים של הרכשות כפולות באמצעות אוכלוסיות מסוימות, כמפורט בהמשך. ניסיונות אלו יכללו גם זיהוי מול המאגר כדי לוודא שהמאגר מסוגל לאתר את הזהות האמתית של הרשומה.

מבחינת הצרכים של רשות האוכלוסין לא יבוצע תרחיש זיהוי מול המאגר. תרחיש זה נועד כולו עבור גורמים אחרים שהחוק מתיר להם להגיש שאילתות למאגר.

להלן שלבי התהליך:

6.6.1. קבלת הנתונים

הנתונים אותם יש לזהות יתקבלו כאשר הם מוצפנים וחתומים על ידי הגורם שהעביר אותם. הם יועברו לרשת הפנימית באמצעות ערוץ חד כיווני, שם הם יפוענחו ויטופלו.

6.6.2. חיפוש מסוג one to many

יבוצע חיפוש שיאתר את הרשומה שמידת ההתאמה שלה למידע היא הגבוהה ביותר. גם במקרה זה יתכן שחיפוש זה יניב יותר מתוצאה אחת, בהתאם לאיכות הדגימה, מהותה ומידת הפירוט שלה. תוצאות אלו תדורגנה בהתאם למידת ההתאמה שלהן.

6.6.3. סינון התוצאות

התוצאות תעבורנה סינון אנושי במידת הצורך. סינון זה יבוצע על ידי מפעילי המאגר או על ידי הגורם שהעביר את השאילתה, בהתאם למקרה.

6.6.4. העברת התוצאה

תוצאת הזיהוי תועבר בצורה טלפונית ותגובה באמצעות מערכת נפרדת, שאיננה מקושרת למאגר. מערכת זו משתמשת במסכים ייעודיים של מערכת "אביב" דרכם מדווח המאגר על אישור או דחייה של מנות ובקשות.

[35] נושא זה, של מדיניות העדכון, צריך להיבחן לאורך זמן לאחר שתתקבל החלטה על שימוש שוטף במאגר. לא ניתן לבדוק אותו כראוי בתקופת המבחן.

7. עיקרי השיטה - תקציר

הניסוי יבחן את הנושאים המוגדרים לעיל בצורה הבאה:

7.1. היקף אוכלוסיית הניסוי ופריסה גיאוגרפית

החלק הארי של הניסוי יתבסס על כלל האוכלוסייה שתתנדב לתקופת המבחן, בפריסה ארצית **ולא על בסיס מדגמי כלשהו**. פקידי רשות האוכלוסין יציעו לכל מי שהגיע ללשכה **לקבלת שירות כלשהו** להתנדב לתקופת המבחן. הצעה זו תכלול מתן עלון והסברים אך לא תכלול ניסיונות שכנוע מעבר לכך. עקב רכיב ההתנדבות, שלא ניתן לצפות את היקפו מראש, האפשרות המעשית היחידה היא לבצע את הבדיקה על אוכלוסייה גדולה ככל האפשר ולבחון את התאמתה הסטטיסטית בדיעבד, באמצעות גורם מקצועי מתאים (במקרה זה - הלשכה המרכזית לסטטיסטיקה, המשמשת כגורם מבקר של הניסוי). בצורה כזו כמות ההרכשות וההשוואות שנבצע תהיה גדולה לעין ערוך מכל מדגם סטטיסטי, גם במקרה שרק מעטים מתוך מבקשי התיעוד יתנדבו לתקופת המבחן (ראה פירוט בסעיף המדדים 14.1.1 להלן). המעורבות של הלשכה המרכזית לסטטיסטיקה מאפשרת גם לבחון את הנתונים בחתכים נוספים, על בסיס מידע שזמין רק ללמ"ס ואיננו זמין לרשות האוכלוסין או לרשות לניהול המאגר הביומטרי (ובפרט נתוני מפקד האוכלוסין).

במערך ביקורת הגבולות אוכלוסיית הניסוי תכלול כל מי שיחזיק דרכון הכולל שבב ומידע ביומטרי ושירצה להשתמש בעמדת מעבר בשירות עצמי. עמדות כאלה תוצבנה בנתב"ג ותשולטנה בהתאם. השימוש בהן יהיה התנדבותי לחלוטין.

7.2. אירועים יזומים

חלק מהבדיקה יתבסס על יצירה של אירועים יזומים, כגון ניסיונות התחזות, הדמיה של שאילתות מהמשטרה[36] והרכשה כפולה. אירועים יזומים אלו יתבססו על אוכלוסייה נבחרת (כגון עובדי מדינה) שבאמצעותה ניתן יהיה לדמות אירועים מסוגים שונים, שלא יקרו באופן טבעי בכמות מספקת. כמות האירועים היזומים מסוג הרכשה כפולה תהיה כעשרה אירועים בחודש. אירועים אלו יהיו כפופים לאישור משפטי וככל האפשר יבוצעו בסביבת בדיקות כדי להימנע מהוספת זהות שאיננה נכונה למרשם האוכלוסין (במקרה של דימוי הרכשה כפולה שלא תתגלה).

[36] בהתאם לסעיף 41 של החוק בתקופת המבחן לא תוכל המשטרה להגיש למאגר שאילתות כלשהן.

7.3. ביצועי המערכת הביומטרית

ביצועי המערכת הביומטרית ייבחנו בעיקר על ידי הפעלת תהליך מסוג many to many במאגר, שייצר כמות רבה של השוואות ביומטריות ויאפשר לקבל את גרף ה-ROC המהימן ביותר[37]. תהליך זה יבוצע על אוכלוסייה קטנה ומוגדרת, עבורה ניתן יהיה ליצור ולאחזר מספר מופעים של המידע הביומטרי, בזמנים שונים. ללא מספר מופעים של אותו אדם לא ניתן לקבוע בצורה מהימנה את הביצועים. בנוסף לבדיקה זו ה-FRR ייבחן בצורה משלימה בעת ביצוע השוואה בין אדם לתיעודו (ללא שמירת מידע אישי). רמת הסמך של תוצאת ה-FRR הזו תיבדק רק לאחר ידיעת כמות ההשוואות שהתבצעו בפועל ובחינת הפילוח של אוכלוסיית המבחן, שצריכה להיות דומה בין תקופת הניסוי וההמשך.

7.4. אימות זהות ראשוני

אימות ראשוני של זהות האזרח יבוצע על ידי תשאול המתבסס על פריטי מרשם שונים (תהליך המכונה Authentication By Interview) ובמידת הצורך תוך הסתייעות במסמכי זיהוי אחרים (breeder documents).

7.5. רישום ותיעוד

מערכות המחשוב של רשות האוכלוסין (ובכלל זה מערכת ביקורת הגבולות) ושל הרשות לניהול המאגר הביומטרי תבצענה רישום ממוכן של רוב הנתונים הדרושים לצורך הערכת איכות התהליך התפעולי ובחינת הנושאים הטכנולוגיים השונים. חלק קטן מהנתונים ייאסף בצורה שאיננה ממוכנת.

7.6. שביעות רצון של האזרחים

יבוצע סקר מדגמי של שביעות רצון מאותם תהליכים שיש להם ממשק ישיר לאזרח.

7.7. סקרים ותהליכים משלימים

חלק מהנושאים שיש לבדוק בתקופת המבחן הם נושאים שמטבעם המדדים שלהם יכולים להיות רק איכותיים ולא כמותיים. הדוגמה הבולטת ביותר היא דרישת החוק לבחון בתקופת המבחן את נחיצות המאגר (האם הוא הכרחי עבור המטרות שהוגדרו) ומטרותיו (האם הן מטרות ראויות), שני נושאים שלא יכולים להיבחן בניסוי בפועל ולכן המדדים שיתייחסו לנושא זה אינם כמותיים, מסיבות שיוסברו בהמשך.

עבור נושאים כאלה יש לבצע בתקופת המבחן תהליכים משלימים שיכללו כריית מידע על מרשם האוכלוסין, סקרי ספרות ומאמרים, פנייה חוזרת לקבלת הצעות מימוש אחרות וכדומה.

[37] ראה דו"ח של פרויקט ה-UIDAI בהודו בשם "***uid_enrolment_poc_report***" המפרט מדיניות דומה בנושא זה וזמין באתר הפרויקט ההודי.

8. רכיבים וגורמים מעורבים

מערך ההרכשה וההנפקה של התיעוד הלאומי כולל מספר ניכר של רכיבים טכנולוגיים ובמקביל מספר ניכר של גורמים ארגוניים המעורבים בתהליך.

8.1. גורמים ארגוניים

להלן הגורמים הארגוניים המעורבים בתהליך בכלל ובניסוי בפרט:

8.1.1. רשות האוכלוסין

רשות האוכלוסין הינה הגוף המפעיל את מערך ההרכשה, את מערכי ההנפקה, את מערך ביקורת הגבולות ואת מערכת "אביב". ברשות האוכלוסין יתבצע גם חלק מהשימוש השוטף בביומטריה (בעת מסירת תעודות זהות או בעת מתן שירות לבעלי תעודות חכמות לאחר מכן). כאמור, מעברי הגבול מופעלים גם הם על יד רשות האוכלוסין. פרטי הניסוי שיבוצע במעברי הגבול, ובכלל זה מדדים רלבנטיים, מופיעים בנספח 19.5 להלן ובסעיפים הרלבנטיים לאורך מסמך זה. רשות האוכלוסין תיעזר גם בשירותיו של מומחה תוכן חיצוני בנושא ביומטריה כחלק מהצוות שילווה את תקופת הניסוי.

8.1.2. הרשות לניהול המאגר הביומטרי

זהו הגוף האמון על הפעלת המאגר, על אבטחתו ועל השימוש השוטף בו. עיקר השימוש בביומטריה יהיה במסגרת גוף זה. גם הרשות לניהול המאגר תסתייע בשירותיו של מומחה תוכן חיצוני בנושא ביומטריה.

8.1.3. מרכזי ההנפקה

גורמים אלו כפופים מבחינה ארגונית לרשות האוכלוסין. מערך הנפקת הדרכון (אתר ראשי בירושלים ואתר גיבוי בנתב"ג) מופעל ישירות על ידי יחידת משנה של רשות האוכלוסין. מערך הנפקת תעודות הזהות (אתר ראשי בקיסריה ואתר גיבוי קר ברעננה) מופעלים במיקור חוץ.

8.1.4. משטרת ישראל

בתקופת המבחן לא תותר גישה למשטרה וזו לא תוכל להגיש שאילתות למאגר. השוואת אדם מול תיעודו במשטרה אפשרית בתקופת המבחן ועל המשטרה להיערך לכך מבחינה תקציבית ומיחשובית. המשטרה תידרש לעמוד בדרישות אבטחת מידע זהות לאלו של רשות האוכלוסין והרשות לניהול המאגר הביומטרי. בנוסף תידרש המשטרה לבצע איסוף נתונים מקיף, בדומה לנתונים הרלבנטיים הנאספים ברשות האוכלוסין (בעיקר לגבי השוואת אדם לתיעודו).

8.1.5. גופי הביטחון

בדומה למשטרה, בתקופת המבחן לא תותר גישה לגופי הביטחון ואלו לא יוכלו להגיש שאילתות למאגר. היוצא מכלל זה הוא הרשות הממלכתית לאבטחת מידע (רא"מ), במסגרת תפקידה כגוף מנחה, הן של רשות האוכלוסין והן של הרשות לניהול המאגר הביומטרי. הגישה של רא"מ מוגבלת לנושאי אבטחת מידע וכוללת גם יכולת לבצע ביקורות ותרגילי תקיפה אך לא כוללת גישה למידע ביומטרי.

8.1.6. הלשכה המרכזית לסטטיסטיקה

הלמ"ס היא הגוף האמון על בקרת הניסוי ובחינה של תקפות התוצאות שלו, כדי לוודא שרמת הסמך של מה שנגזר מהניסוי גבוהה דיה. מעבר לבקרה של תקפות התוצאות על פי נתוני מרשם האוכלוסין והמאגר יכול גוף זה לספק תובנות נוספות, על בסיס נתוני מפקד האוכלוסין שברשותו (ושאינם זמינים לגופים אחרים). ראה פירוט של אופן שילוב הלמ"ס בתקופת המבחן בנספח 19.4.

8.1.7. גורמי פיקוח, רגולציה ובקרה

במסגרת זו נכללים כלל הגורמים המפקחים על ביצוע החוק ועל תקופת המבחן וגורמים שאמורים לקבל דיווחים עיתיים. גורמים אלו הם:

8.1.7.1. ראש הממשלה

על פי הצו, יועבר לראש הממשלה דין וחשבון מפורט אחת לחצי שנה ע"י הרשות לניהול המאגר הביומטרי ועל ידי רשות האוכלוסין, ובו תיאור כל תוצאות הבדיקות שנערכו בתקופת המבחן.

8.1.7.2. שר הפנים

דין וחשבון תקופתי זה יועבר גם לשר הפנים אחת לחצי שנה ע"י הרשות לניהול המאגר הביומטרי ועל ידי רשות האוכלוסין.

8.1.7.3. שר המשפטים

דין וחשבון זה יועבר גם לשר המשפטים אחת לחצי שנה.

8.1.7.4. השר לביטחון פנים

דין וחשבון זה יועבר גם לשר לביטחון פנים אחת לחצי שנה.

8.1.7.5. וועדת שרים ליישומים ביומטריים

וועדה זו תקבל בהתאם לסעיף 41(4) של החוק דין וחשבון מסכם על ממצאי תקופת המבחן. דין וחשבון מסכם זה יוגש לוועדת השרים תשעים יום לפני תום תקופת המבחן על ידי רוה"מ ושר הפנים. בנוסף יוגש דין וחשבון מסכם זה לוועדת הכנסת המשותפת ולוועדת הכנסת ליישומים ביומטריים.

8.1.7.6. וועדת הכנסת המשותפת

זוהי ועדת כנסת ייעודית שנקבעה בחוק. אותו דין וחשבון תקופתי שיוגש לרוה"מ ולשרים יוגש גם לוועדה זו. בנוסף יוגש לוועדה דין וחשבון מסכם בהתאם לסעיף 41(4) של החוק.

8.1.7.7. וועדת הכנסת ליישומים ביומטריים

זוהי ועדת כנסת ייעודית שנקבעה בחוק. דין וחשבון מסכם בהתאם לסעיף 41(4) של החוק יוגש גם לוועדה זו.

8.1.7.8. הממונה על יישומים ביומטריים במשרד רוה"מ

הממונה על יישומים ביומטריים במשרד רוה"מ הינו גורם ממליץ שהוקם במסגרת החוק כדי להתוות מדיניות כוללת בנושא ביומטריה, גם מעבר לנושאים שהוגדרו בחקיקה.

8.1.7.9. וועדה מייעצת

את תהליך ביצוע הניסוי בתקופת המבחן תלווה וועדה מייעצת אשר תכלול את בעלי התפקידים הבאים:

8.1.7.9.1. הסטטיסטיקאי הממשלתי הראשי - למ"ס

8.1.7.9.2. הממונה על יישומים ביומטריים במשרד רוה"מ

8.1.7.9.3. ראש הרשות למשפט וטכנולוגיה במשרד המשפטים

8.1.7.9.4. ראש המטה ללוחמה בטרור במשרד רוה"מ

8.1.7.9.5. נציג ציבור

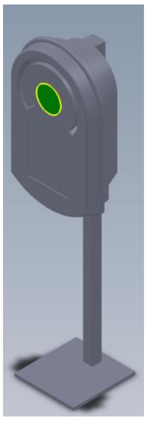
הלשכה המרכזית לסטטיסטיקה היא הגורם הארגוני המבקר את הניסוי כולו ובוחן את תקפות תוצאותיו על פי נתוני מרשם האוכלוסין ונתוני מפקד האוכלוסין (הזמינים לו בלבד). לאור תפקיד זה יש חשיבות רבה לכך שנציג הלמ"ס יהיה חלק מוועדה זו. הוועדה תבצע פעילות אשר תכלול מעקב אחר התנהלות תהליכי הניסוי, מעקב אחרי העמידה ביעדים, סיוע בגיבוש התוצאות ויישום המבדקים ובחינת המדדים כפי שנקבעו במסמך זה ובצו שבחתימת שר הפנים. סיכום תוצאות הניסוי ומשמעותן יבוצע במשותף על ידי נציגי רשות האוכלוסין, הרשות לניהול המאגר הביומטרי והוועדה המייעצת. הוא יועבר על ידי רשות האוכלוסין והרשות לניהול המאגר הביומטרי למקבלי ההחלטות – ועדת השרים וועדת הכנסת.

8.2. רכיבים

להלן תיאור של הרכיבים הטכנולוגיים השונים שישתתפו בתקופת המבחן:

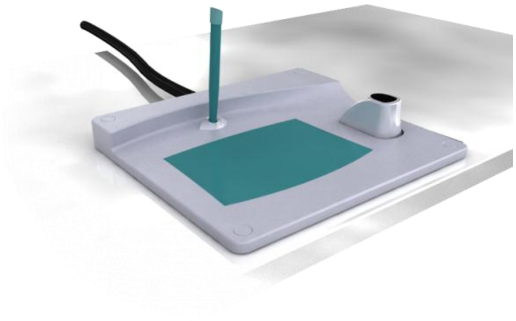
8.2.1. עמדות הרכשה
עמדות ההרכשה המותקנות בלשכות רשות האוכלוסים כוללות את הרכיבים הבאים:

8.2.1.1. מצלמה
מצלמה זו משמשת לצילום הפנים. זוהי מצלמת DSLR מתוצרת חברת Canon, מדגם EOS1000D. האבחנה של מצלמה זו היא 10 מגה-פיקסל. מיקום העדשה בעמדת הצילום מודגש בירוק:



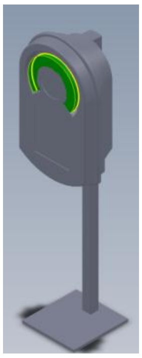
8.2.1.2. חיישן טביעות אצבע
חיישן אופטי מתוצרת חברת Lumidigm, דגם Mercury M301-00, עם אבחנה של 500PPI. חיישן זה משתמש בטכנולוגיה הנקראת multi spectral, המבוססת על הארת האצבע במספר אורכי גל כדי לקבל תמונה מיטבית.

8.2.1.3. משטח חתימה
זהו משטח חתימה (tablet) מתוצרת Wacom המשולב מארז אחוד עם חיישן טביעות האצבע. הדגימה של החתימה הגרפית איננה מיועדת להיות נתון ביומטרי ותשמש אך ורק להדפסתה ושמירתה בדרכון, ללא אגירה כלשהי.



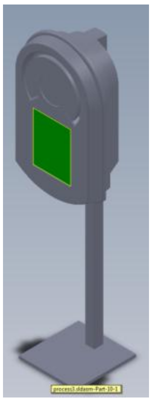
8.2.1.4. תאורה

עמדת הצילום מכילה תאורת LED מעגלית המבוקרת על ידי תוכנת הצילום. השימוש בתאורה מעגלית (ring light) מפחית את הצללים על פני המצולם. תאורה זו מובנית לתוך העמדה ומודגשת בירוק באיור הבא:



8.2.1.5. מסך עזר

בעמדה מותקן מסך עזר לצורך מתן משוב בזמן אמת למצולם. מסך זה מסייע למצולם ליישר את פניו מול המצלמה. מיקום מסך העזר מודגש בירוק באיור הבא:



8.2.1.6. תוכנת בדיקת איכות טביעות אצבע

איכות טביעות האצבע תיבדק באמצעות מדד NIST-NFIQ[38] המגדיר ציונים בטווח "1" (הכי טוב) עד "5" (הכי גרוע).

8.2.1.7. תוכנת בדיקת איכות תמונות פנים

תמונות הפנים תיבדקנה על פי נגזרת של תקן ISO 19795-5 על ידי תוכנה מסוג Facevacs מתוצרת חברת Cognitec. ראה פירוט בסעיף 14.1.5 להלן.

8.2.1.8. קורא כרטיסי מגע

קורא כרטיסי מגע מסוג PC pinpad מתוצרת Gemalto המיועד לקריאת תעודת הזהות. קוראים כאלו יותקנו בכל דלפקי קבלת הקהל בלשכות הרשות ויופנו לכיוון מקבל השירות. לקורא זה יש מקלדת משלו כדי לאפשר הזנת קוד אישי (PIN) ללא חשיפתו למחשב העמדה אליה הוא מחובר.

8.2.1.9. קורא כרטיסים ללא מגע

קורא כרטיסים חכמים דואלי (הקורא גם כרטיסי מגע וגם כרטיסים ללא מגע) מסוג Omnikey5321 מתוצרת Assa Abloy/HID המיועד לקריאת השבב שבדרכון. קורא אחד מסוג זה יותקן בכל לשכה בשלב מאוחר יותר.

[38] ראה פירוט באתר http://www.nist.gov/itl/iad/ig/nbis.cfm

- בלמ"ס -

8.2.1.10.קורא ברקוד

קורא ברקוד לקריאת מספר הדרכון המודפס בדף מס' 3, לצורך אחזור רשומת ה-MRZ (ראה הסבר בסעיף 6.3 לעיל).

8.2.2. המאגר

המפרט הטכנולוגי של המאגר מוגדר במסמך נפרד. מסמך זה הינו מסמך מסווג.

8.2.3. עמדות ביקורת גבולות לא מאויישות

עמדות אלו תוצבנה במסלולי הכניסה והיציאה בנתב"ג (ראה פירוט גם בנספח 19.5 להלן). הן כוללות את הרכיבים הבאים:

8.2.3.1. מחשב עמדה

עמדת ביקורת הגבולות תתבסס על מחשב תקני, שיותקן בצורה מוגנת בתוך מארז העמדה.

8.2.3.2. תוכנה לביצוע מעבר ביומטרי

בעמדה קיימת תוכנה ייעודית שתבצע השוואה בין דגימה "חיה" לנתוני ייחוס שייקראו מהדרכון או ממסמך הנסיעה.

8.2.3.3. תוכנת ממשק מול מערכת "רותם"

מערכת "רותם" הינה מערכת המידע העיקרית של ביקורת הגבולות ועמדת המעבר נזקקת לממשק שיאפשר לה להגיש שאילתות למערכת זו כדי לאמת את זכות המעבר.

8.2.3.4. סורק דף מלא משולב עם קורא שבב

ראה סעיף 6.3 לצורך הסבר על תהליך קריאת מידע מדרכון עם שבב ועל תפקיד הסורק בתהליך זה. תפקיד נוסף של סורקי "full page" הינו איתור זיופים "קלאסיים" של הספרון באמצעות בדיקת הדרכון במספר אורכי גל. הסורק מאיר את הדרכון באור לבן, אור אולטרה-סגול ואור אינפרה-אדום ומשווה את התמונה המתקבלת בכל מצב לתמונת ייחוס ידועה. אם הסורק מזהה חריגה הוא יכול להפעיל התראה על חשד לזיוף.

8.2.3.5. מצלמה

המצלמה מיועדת לצילום העובר לצורך השוואת תווי פניו לתמונה הנקראת מהדרכון.

8.2.3.6. חיישן טביעות אצבע

חיישן זה מיועד לנטילת טביעת אצבע מהעובר, לצורך השוואה מול טביעת הייחוס הנקראת מהדרכון. קריאה של טביעת הייחוס מהדרכון אפשרית רק לאחר תהליך אימות המבוסס על הצפנה חזקה מאד.

8.2.3.7. קורא ברקוד

ראה גם סעיף 8.2.1.10 לעיל. מטרת הקורא הזה היא בחינה של אפשרות נוספת לקריאת מספר הדרכון מדף מס' 3, שם מופיע מספר זה כברקוד תקני (ראה צילום דרכון לדוגמה להלן). מספר הדרכון יאפשר אחזור של רשומת ה-MRZ לצורך "פתיחת" אפשרות הקריאה מהשבב (ראה גם הסבר בסעיף 6.3 לעיל).

8.2.3.8. מדפסת

לאחר אימות זהות העובר הוא יקבל אסמכתה בצורת פתק מודפס, בדומה לפתק המתקבל במערכת הביומטרית הקיימת, המבוססת על גאומטריית כף היד.

8.2.3.9. מסך

מסך זה מיועד לממשק המשתמש של העמדה ויוכל לספק לעובר הנחייה בארבע שפות.

8.2.3.10.שער פיזי

בשתי עמדות ישולב שער פיזי שייפתח לאחר אימות זהות העובר.

8.2.3.11.שרת מרכזי

קריאת מידע ביומטרי (ובפרט טביעות אצבע) מהדרכון מחייבת את עמדת הקריאה להוכיח את זהותה לשבב המשולב בדרכון. תהליך זה מבוצע בעזרת תעודות אלקטרוניות (אשרות, certificates) שהן מבנה נתונים המבוסס על תהליכי צופן חזקים. לצורך זה ישולב במערכת שרת המיועד לניהול, שמירה ויצירה מאובטחת של התעודות האלקטרוניות האלו, המאפשרות גישה מלאה לשבב, בהתאם לתקן הבינלאומי.

9. הניסוי

להלן תיאור מהלך הניסוי:

9.1. הכנה

תהליכים אלו יקדימו את הניסוי:

9.1.1. הכנה טכנולוגית

ההכנות הטכנולוגיות לניסוי כוללות את הקמת והתקנת עמדות ההרכשה ואת הקמת תשתית המחשוב של המאגר. איסוף הנתונים השונים יהיה חלק מהתכונות המסופקות על ידי מערכים אלו ויבוצע על ידן באופן שוטף וממוכן.

9.1.2. הכנת הציבור

מעבר למוכנות הטכנולוגית יש לבצע תהליך פרסום נרחב שיסביר לציבור את חשיבות הנושא, תוך שימת דגש על המעבר להנפקה מרכזית של תיעוד והסיבות לכך, היתרונות של התיעוד החדש והחשיבות של השתתפות אוכלוסייה גדולה ככל האפשר בתקופת המבחן.

9.1.3. הכנה ארגונית ותהליכית בממשלה

הכנת הניסוי כוללת תהליכים ארגוניים שונים ובפרט אישורי תקציבים, הקמת הרשות הייעודית לניהול המאגר הביומטרי (כמפורט בחוק) ובניית תהליכי עבודה ונהלים מתאימים.

9.2. היקף ופריסה

בהתאם למדיניות ההפעלה המוצעת למאגר, תקיף תקופת המבחן אוכלוסייה רחבה ככל האפשר ולא תתבסס על מדגם כלשהו. הפילוח של אוכלוסייה זו ייבדק בדיעבד על ידי הלמ"ס כדי לוודא שהיא אכן מהווה מדגם מייצג עם רמת סמך גבוהה. הפריסה תהיה ארצית, בכל לשכות רשות האוכלוסין. כמות האירועים היזומים תוגדר על פי ההיקף בפועל.

9.3. תרחישי הניסוי

הניסוי יכלול את ביצוע התרחישים הבאים:

9.3.1. תרחיש ההרכשה

תרחיש זה ייבחן באופן שוטף בכל פעם שאזרח ירצה לקבל תעודת זהות חכמה או דרכון (או שניהם). השמירה של מידע ביומטרי במאגר תתבצע גם אם האזרח ביקש רק סוג אחד של תיעוד. לכל אורך התהליך יבוצע איסוף ממוכן של הנתונים השונים, כמפורט להלן. הבחינה תכלול את ההיבטים התפעוליים ואת ביצועי מערכת ההרכשה מבחינת יכולתה לספק נתונים ביומטריים באיכות נאותה.

9.3.2. תרחיש חיפוש ההרכשה הכפולה

תרחיש זה ייבחן באופן שוטף, בעקבות כל אירוע הרכשה. בנוסף לכך יבוצעו אירועים יזומים של הרכשות כפולות מלאכותיות, לצורך בחינת יכולת הגילוי של המאגר ולצורך בחינת תהליך עצירת ההנפקה בעקבות גילוי הרכשה כפולה. אירועים יזומים אלו יתבססו על אוכלוסייה מוגדרת כגון עובדי מדינה, שניתן לבקש מהם לשתף פעולה עם בדיקה זו. הבחינה תכלול את ביצועי המערכת (בעיקר מבחינת התראות שווא ויכולת איתור ניסיונות הרכשה כפולה), את כיול סיפי ההחלטה של המערכת ואת קבלת גרף ה-ROC שלה. לצורך זה תידרש אותה אוכלוסייה מוגדרת לבצע הרכשות חוזרות במרווחי זמן קצובים, כדי ליצור מספר מופעים של אותו אדם.

9.3.3. תרחיש השוואה מול תעודת זהות

תרחיש זה, במסגרתו מושווה האדם מול התיעוד שלו, ייבחן באופן שוטף בשני מצבים:

9.3.3.1. מסירת תעודת זהות

יבוצע אימות ביומטרי של המקבל בעת מסירת תעודת הזהות לאזרח, בעת הגעתו השנייה ללשכה. יתכן שתרחיש זה ייבדק גם במקומות אחרים, אם יוחלט למסור תעודות זהות לאזרחים באמצעות מיקור חוץ.

9.3.3.2. קבלת שירות

אגף התיעוד של רשות האוכלוסין יגדיר מספר שירותים שניתן יהיה לקבלם במסלול מקוצר כאשר ניתן לאמת את מבקש השירות באמצעים ביומטריים בלשכות הרשות. במקרים אלו יבוצע אימות ביומטרי בלשכות רשות האוכלוסין למקבל השירות אם יש כבר ברשותו תעודת זהות חכמה.

הבחינה תכלול את ההיבטים התפעוליים, את ביצועי המערכת הביומטרית (מבחינת קצב דחיית המורשים FRR) את היכולת לקרוא מידע ביומטרי מהתעודה ואת שביעות הרצון של המעורבים בתהליך.

יש להדגיש שרק לשכות רשות האוכלוסין בשלב זה תהיינה נגישות לתשתית הצופן הדרושה לצורך קריאת טביעות אצבע מכרטיסי תעודת הזהות החכמה. גורמים אחרים (כגון משטרת ישראל) יידרשו לעמוד בדרישות אבטחת מידע מחמירות מאד לצורך קבלת הרשאת קריאה כזו.

9.3.4. תרחיש השוואה מול דרכון

תרחיש זה דומה מאד מבחינה טכנולוגית להשוואה מול תעודת הזהות אך איננו רלבנטי ברוב המוחלט של אירועי המסירה, כי הדרכון נשלח לבעליו באמצעות דואר רשום ולא נמסר ידנית בלשכה. בהתאם לכך תבוצע הבחינה של תרחיש זה בשני מקרים אחרים:

9.3.4.1. קבלת שירות באמצעות דרכון

השוואה מול הדרכון תבוצע מספר חודשים לאחר תחילת הניסוי כאשר יגיע אזרח לקבלת שירות בלשכות רשות האוכלוסין ויש ברשותו רק דרכון חדש ולא תעודת זהות חכמה. במצב זה ניתן לבצע השוואה מול הדרכון כדי לזהות בצורה חד ערכית ומהימנה את מבקש השירות. לצורך זה תותקן בשלב מאוחר יותר בכל לשכה יכולת קריאה של דרכון חדש.

9.3.4.2. מעבר גבול/שדה תעופה

השוואה מול דרכון תתבצע במעבר גבול ישראלי, ככל שמעברים כאלו יצוידו באמצעי קריאה וחיישני טביעות אצבע או מצלמות פנים. בטווח זמן רחוק יותר יתכן שימוש ביכולת כזו לא רק עבור ביקורת גבולות אלא גם במסגרת תהליך הטיפול בנוסע בשדה התעופה. השימוש בשדה התעופה, אם לביקורת גבולות ואם לתהליך הטיפול בנוסע, הינו מרכיב קריטי המשפיע על מידת השימושיות של התיעוד החדש ובפרט הדרכון.

9.3.5. תרחיש אימות מול המאגר

תרחיש זה ייבחן באופן שוטף בשלושה מצבים:

9.3.5.1. חידוש תיעוד

חידוש תיעוד מחייב הרכשה מחדש ואימות של זהות המחדש מול המאגר. יודגש שאין יכולת לקבל מהמאגר את הנתונים הביומטריים הקודמים ולכן נדרשת הרכשה מחודשת זו. לאחר אימות חיובי תעודכן הרשומה שבמאגר עם הנתונים הביומטריים האחרונים (אם איכותם גבוהה דיה). הנתונים הקודמים יימחקו במקרה כזה (מחיקה לוגית על ידי סימונם כנתונים היסטוריים ולא מחיקה פיזית). במשך שתי שנות המבחן אנו מצפים למעט אירועים כאלו, בעיקר בעקבות אובדן/גניבה או בעקבות בקשת מסמך זיהוי אחר (דרכון לבעלי תעודת זהות ולהיפך).

9.3.5.2. בדיקות יזומות

בדיקות יזומות בדומה לבדיקות היזומות המתוארות בסעיף 9.3.2 לעיל.

9.3.5.3. הדמיות

הדמיה (סימולציה) של שאילתות מהמשטרה, ללא העברה בפועל של התשובה הסופית.

9.3.6. תרחיש זיהוי מול המאגר

תרחיש זה ייבחן באופן שוטף בשני מקרים:

9.3.6.1. הדמיות

הדמיה (סימולציה) של שאילתות מהמשטרה, ללא העברה בפועל של התשובה הסופית.

9.3.6.2. אירועי הרכשה כפולה

בעת אירוע של הרכשה כפולה, יזום או אמיתי, כדי לזהות למי באמת שייכת הרשומה הביומטרית.

9.4. סקר שביעות רצון

באותם אירועים שהם יש ממשק לתושבים (סעיפים 9.3.1, 9.3.3 ו-9.3.4 לעיל): תהליך הטיפול בבקשה לקבלת התיעוד ותהליך מסירת התיעוד ובהמשך – השימוש בתיעוד, יבוצע סקר שביעות רצון על בסיס מדגמי. הסקרים יעוצבו על ידי הלשכה המרכזית לסטטיסטיקה, שאף תבצע אותם ותעבד את תוצאותיהם. בסקרים יכללו הן את האוכלוסייה שהסכימה להשתתף בניסוי והן את האוכלוסייה שסירבה להשתתף בניסוי או שפרשה ממנו בטרם הושלם תהליך הטיפול בבקשה.

9.5. הצגת התוצאות

תוצאות הסקר יפורסמו במסגרת הדין וחשבון התקופתי כמתחייב ב"צו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי הזיהוי ובמאגר המידע (תקופת המבחן), התשע"א - 2010.
כמו כן, בהתאם לצו כנ"ל יפורסמו עקרי ממצאי הסקר באתר האינטרנט של רשות האוכלוסין וההגירה.
יתכן שממצאי הסקר יפורסמו גם באתר הלשכה המרכזית לסטטיסטיקה (כפוף לאישור הלשכה).
תוצאות ביניים תפורסמנה בכל ששה חודשים ודו"ח סופי בתום תקופת הניסוי, כפי שתיקבע.

10.סיכונים, מגבלות ובעיות

תקופת המבחן מתאפיינת במספר אילוצים חוקיים או אחרים, שאינם מאפשרים לבחון ישירות, באמצעות ניסוי מעשי, חלק מהנושאים. במקרים אחרים גורמים אילוצים אלו ליכולת בחינה איכותית ולא כמותית. סעיף זה דן באילוצים אלו ואחרים ובסיכונים שהם יוצרים בתקופת הניסוי.

10.1. איתור הרכשות כפולות

הניסוי במשך תקופת המבחן יתבסס רובו ככולו על אותה אוכלוסייה שתגיע מרצונה ללשכות רשות האוכלוסין, תביע הסכמה ותבצע את תהליך ההרכשה. בהיעדרו של מניע משמעותי לחזור שנית ללשכה (למעט קבלת שירות מעת לעת במספרים לא ידועים) לא ניתן להסתמך על הרכשות חוזרות כקלט לתהליך בדיקת היכולת לאתר הרכשות כפולות. יתרה על כך, יש סבירות גבוהה שמתחזים ופושעים למיניהם פשוט ימנעו מלבקש תיעוד מהסוג החדש ככל האפשר. מסיבה זו יש ליצור קלט יזום לתהליך זה ולא להמתין להרכשות חוזרות.

גם בעת חזרת האזרח ללשכה לצורך מסירת התעודה לא ניתן לבצע הרכשה חוזרת מלאה, למעט על בסיס התנדבותי, עקב הטלת עומס עבודה רב מדי על הלשכה.[39] סיבה זו מחדדת באופן מובהק את הצורך להסתמך על אוכלוסייה נבחרת שניתן לבקש ממנה לחזור על תהליך ההרכשה שנית. למעשה האוכלוסייה היחידה העונה לתנאי זה הם עובדי המדינה שיעשו זאת כחלק מתפקידם ובפרט עובדי רשות האוכלוסין והרשות לניהול המאגר הביומטרי עצמם. במקרים מסוימים תתווסף קבוצה של מתנדבים לאוכלוסייה זו.

בחינת התשאול ככלי **<u>למניעת</u>** הרכשות כפולות (גם אם לא ככלי **<u>לאיתור</u>** אירועים כאלה, ראה סעיפים 4.2.2.3, 11.1 ו-19.3.1.2) נתקלת במגבלות נוספות, ובפרט בגלל העובדה שכישלון או הצלחה בתהליך זה תלויים בגורמים רבים נוספים, שאינם ניתנים לכימות או לבקרה בניסוי. לדוגמה, במציאות פושעים בעלי תעוזה וכישרון של "הנדסה חברתית" (social engineering) יהיו אלה שינסו את מזלם בתשאול אך בניסוי מבוקר, שיתבסס על האוכלוסיות שצוינו לעיל, לא ניתן לדמות זאת. מצב זה עלול לגרום להטיית התוצאה ולכך שרמת הסמך של תוצאות ניסוי זה תהיה נמוכה ותתקבל תמונה מעוותת. יתרה על כך, בניסוי מבוקר ניתן עדיין לבצע ניסוי כזה אולם במציאות, בהעדר כלי שמסוגל להבחין בין כישלון שנובע מסיבות אחרות ובין כישלון שנובע מהרכשה כפולה, אין דרך להמשיך את הטיפול באירוע כזה ולשלול מאזרח את מסמכי הזיהוי שלו.

---

[39] השתהות של חצי דקה לכל מקבל שירות מצטברת למספר שנות אדם בכל שנה.

10.2. השוואות ביומטריות

כדי לקבל נתונים טובים על ביצועי המערכת הביומטרית (FA, FR ועקומת ROC) יש לבצע כמות גדולה של השוואות והצלבות הכוללות מספר מופעים של אותו אדם. כאמור אין בידי רשות האוכלוסין כלי שיכול לאפשר הזמנה שנייה יזומה של אזרחים שעברו את תהליך ההרכשה, לצורך יצירת מספר ניכר של אירועי השוואה כאלו, בין האזרח לתיעודו. לצורך זה, כאמור גם בסעיף 10.1 לעיל, ניתן להסתמך באופן שוטף רק על אותם אזרחים שעברו הרכשה ביומטרית ושבו ללשכות הרשות לצורך קבלת שירות אחר או לכל הפחות שבו ללשכה לצורך קבלת תעודת הזהות שביקשו.

האילוץ הוא שגם אירועים כאלו (של קבלת שירות לאחר ההרכשה) לא יאפשרו מספר גבוה דיו של השוואות מהסיבות הבאות:

10.2.1. חוסר אפשרות אגירה

החוק והתקנות לא מאפשרים לשמור מידע ביומטרי שנדגם מהאזרחים לאורך זמן. מסיבה זו מתאפשרת רק בדיקה מקומית, של אדם מול תיעודו, ללא יכולת להשוות בינו לבין דגימות אגורות של אחרים או בינו ובין מופעים קודמים שלו כדי לייצר אירועי התחזות מלאכותיים ואירועי השוואה חוזרת.

10.2.2. סוג ההשוואה

השוואה כזו, של אדם מול תיעודו, איננה נעשית מול המאגר והיא מטבעה השוואה מסוג one to one. מסיבה זו ניתן לקבל ממנה אך ורק מושג על שגיאות מסוג false rejection. כאמור לעיל, אין כל אפשרות לייצר במצבים כאלו אירועי התחזות מלאכותיים בהיקף גדול, אם כי ניתן לבצע ניסוי בהיקף מוגבל, שידמה אירועי שגיאות מסוג false acceptance.

10.2.3. כמות ההשוואות

כאמור לעיל, מספר ההשוואות יהיה תלוי במספר האזרחים שישובו ללשכת רשות האוכלוסין לקבלת התעודה שביקשו ומספר האזרחים שיש ברשותם תעודה חכמה ושנדרשו לשירות נוסף בתוך תקופת המבחן. גם מסיבה זו לא ניתן לקבל מספר מופעים של אותו אזרח בכמות מספקת. יתרה על כך – אזרחים שביקשו רק דרכון ולא השתכנעו לקבל גם תעודת זהות יקבלו את הדרכון באמצעות הדואר ולא יחזרו שנית ללשכה (או יחזרו אבל סביר שיקבלו שירות על בסיס תעודת הזהות הישנה). מסיבה זו לא ניתן לבצע עבורם את תהליך ההשוואה.

10.3. תלות במספר המתנדבים

המגבלה המשמעותית ביותר נובעת מהתלות של הניסוי ברצונם של האזרחים להתנדב אליו ולהיכלל בתקופת המבחן. לא ניתן לצפות מראש מה תהיה כמות המתנדבים וללא כמות מספקת לא תיתן תקופת המבחן תובנות ברמת סמך גבוהה דיה.

10.4. התפלגות אוכלוסיית המתנדבים

הניסוי איננו מתבסס על מדגם אלא על הנחת יסוד שכמות המתנדבים תהיה גדולה דיה כדי לכסות את כלל האוכלוסייה בחתכים של גיל, מגדר, מגזר ומקום מגורים. קיים סיכון תמידי לאורך תקופת הניסוי של אוכלוסיית מתנדבים שלא תספק כיסוי בר תוקף לכלל אזרחי המדינה גם אם מספרה יהיה גדול (בגלל חתך גלאים מסוים או מגזר מסוים שיהיה חסר באוכלוסייה זו).

לנושא זה יש השלכה חמורה על היכולת לבדוק את ביצועי המערכת הביומטרית מבחינת FA, FR ועקומת ROC. רמת הסמך של נתונים אלו תהיה תלויה במישרין במידה שבה אוכלוסיית הניסוי מייצגת את כלל האוכלוסייה.

10.5. התפלגות של אוכלוסיות נבחרות

בחינה של חלק מהנושאים תתבצע בעזרת אוכלוסיות נבחרות (כדוגמת עובדי מדינה). יתכן שאוכלוסייה זו איננה משקפת את כלל האוכלוסייה מבחינה סטטיסטית (גילאים, מוגבלויות וכד'). גם זהו סיכון קבוע לכל אורך תקופת המבחן.

10.6. הבדלים בין מסמכי הזיהוי

בעיה משמעותית נוספת של הניסוי נובעת מההבדלים בין הדרכון ותעודת הזהות. לרשות האוכלוסין יש אינטרס מובהק ביותר לשכנע כל מתנדב לקבל את שני המסמכים ולבצע אירוע הרכשה יחיד עבור שניהם. כל מקרה אחר יטיל עומס עבודה רב מדי על הרשות, שהיא תתקשה לעמוד בו. מצד שני, באופן מעשי לרשות האוכלוסין יש מעט כלים לכך כי אזרח שנזקק רק לדרכון יצטרך להגיע שנית (לקבלת תעודת הזהות) ואזרח שנזקק רק לתעודת הזהות יצטרך לשלם את אגרת הדרכון. מסיבה זו יהיו אזרחים לא מעטים שזקוקים רק לדרכון ולא ירצו להגיע שנית לצורך קבלת תעודת זהות ויהיו אזרחים לא מעטים שזקוקים רק לתעודת זהות ולא ירצו לשלם את האגרה עבור הדרכון. סיכון זה תקף לכל אורך תקופת המבחן.

10.7. הערכות של גורמים אחרים

אין כל ודאות שגורמים נוספים יהיו ערוכים בזמן לטיפול בתיעוד החדש ובפרט לשימוש במידע הביומטרי שעליו. גורמים אלו כוללים את משרדי הממשלה האחרים, המשטרה, ביקורת הגבולות ורשות שדות התעופה. עבור חלק מגורמים אלו נדרשת הסדרה חוקית לצורך שימוש במידע ביומטרי. המצב הרצוי ביותר יהיה מצב בו אותם גורמים ערוכים לטיפול כזה מתחילת ההנפקה אך ככל הנראה יהיה הפרש זמנים ניכר בין תחילת ההנפקה ובין הפעלת ההיערכות באותם גופים. בכל מקרה, שיתופם בתקופת המבחן יחייב אותם לאיסוף נתונים מקיף ולעמידה בדרישות אבטחת מידע מחמירות.

10.8. שירותים שאינם מבוססי ביומטריה

מלבד ההיבט של שימוש במידע ביומטרי קיים סיכון נוסף עם השלכה על כמות המתנדבים – כמות שירותי הממשל והשירותים המסחריים שיהיו זמינים באמצעות תעודת הזהות החכמה ללא קשר לביומטריה. שירותים אלו מהווים מניע מרכזי להצטרפות יותר אזרחים לתקופת המבחן.

10.9. מדיניות עדכון רשומות ביומטריות

עקב מיעוט האירועים של הרכשות חוזרות בתקופת המבחן אין יכולת לקבוע מהי מדיניות העדכון העדיפה (שימוש תמיד בנתונים הכי עדכניים, שימוש תמיד בנתונים האיכותיים ביותר וכו').

10.10. נושאים שאינם ניתנים לכימות

חלק מהנושאים שרלבנטיים לתקופת המבחן כלל אינם ניתנים לכימות ובהתאם לכך לא ניתן לקבוע עבורם מדדים מספריים אלא רק מדדים איכותיים. דוגמה בולטת לכך היא אפקט ההרתעה שיש למאגר כנגד הרכשה כפולה או יכולות "הנדסה חברתית" של פושעים בעת תשאול. קיומם של נושאים כאלו מחייב תהליכים משלימים כדי להעמיד בסוף תקופת המבחן לרשות הגורמים המחליטים מידע שלם ככל האפשר.

10.11. נושאים שאינם ניתנים לניסוי

הדיון הציבורי הער סביב המאגר העלה לא אחת שאלות שאינן ניתנות להכרעה באמצעות ניסוי, כגון שאלות של מדיניות, שאלות ערכיות ושאלות חוקתיות. מטבע הדברים נושאים אלו אינם ניתנים לניסוי ואינם בתוך גבולות הגזרה של תקופת המבחן. תהליך קבלת ההחלטות בתום תקופת המבחן יצטרך לשקלל נושאים כאלו מבלי שניתן יהיה להסתמך על נתונים מוצקים.

10.12. מגבלות הטכנולוגיה

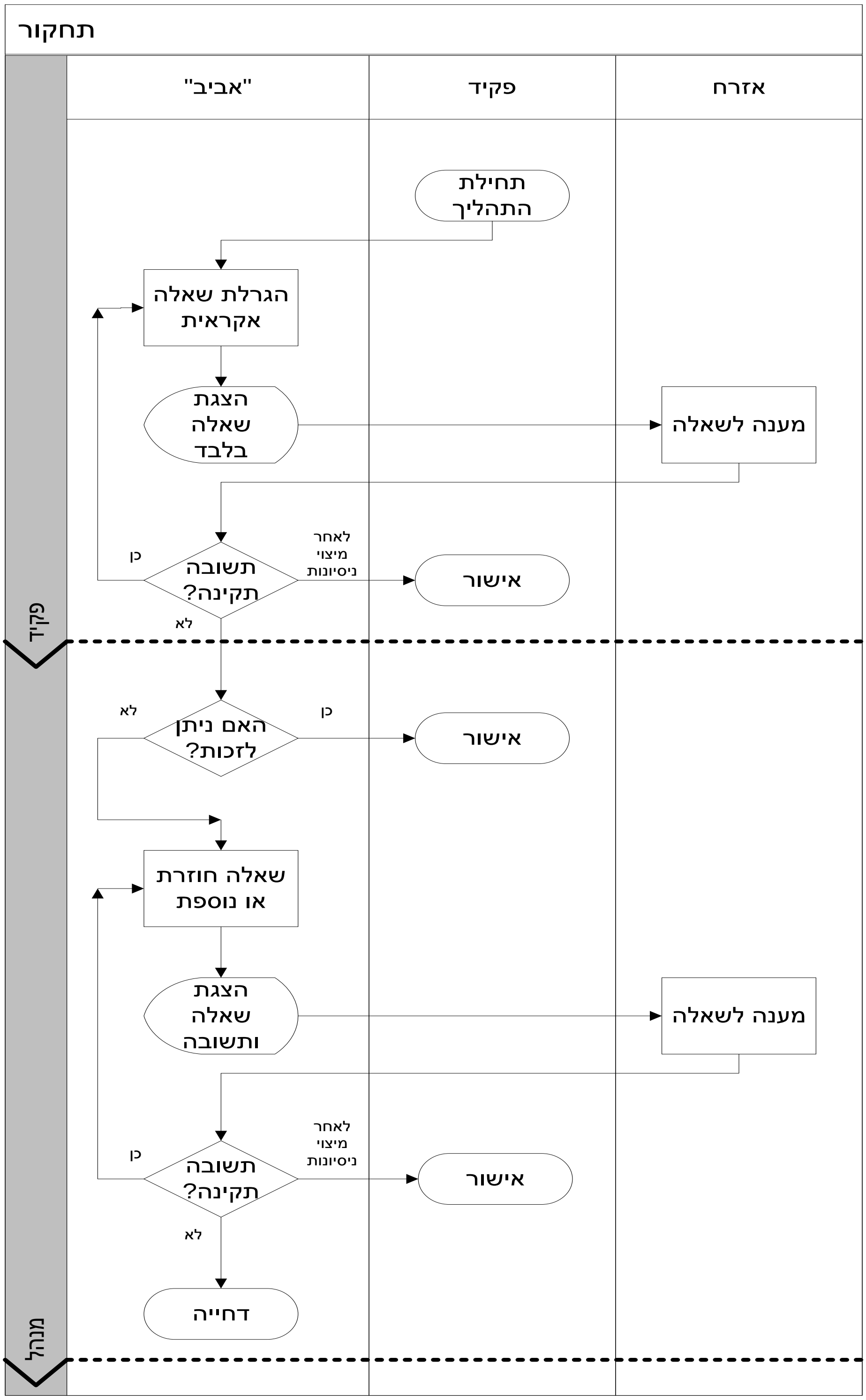
כחלק מחובת המידתיות של השימוש בביומטריה מספקת מערכת זו בדגימה של שתי אצבעות. בדרך כלל תהיינה אלה האצבעות המורות. דבר זה מציב בפנינו סיכון על פיו המובהקות שתתקבל לא תהיה גבוהה דיה ומפעילי המאגר יוצפו במקרים של התראות שווא. נושא זה מחריף עוד יותר לאור העובדה שנבחר חיישן ששטח הסריקה שלו קטן יחסית. כדי לתת מענה ראוי לכך נדרשת תשומת לב רבה יותר מצד הפקידים בתהליך ההרכשה וזוהי אחת הסיבות לכך שנטילת טביעות האצבע נעשית על שולחן הפקיד ובצורה שהוא יכול לראות ולפקח מקרוב על התהליך.

מגבלה משמעותית נוספת נובעת מהשימוש בחיישן של אצבע בודדת, שחושף את המערכת לטעות ברישום סוג האצבע (אצבע מורה, אמה). טעות כזו מכונה "sequence error".

11.מהלך הניסוי

להלן תיאור מפורט של התרחישים השונים:

11.1. תשאול



- בלמ"ס -

תהליך התשאול יתבסס על שאלות אקראיות שתוצגנה לאזרח, ללא חשיפת התשובות הנכונות לפקיד המבצע את התהליך. הפקיד יקליד את תשובות הנשאל ויקבל חיווי על התאמה או אי התאמה בין התשובות בפועל לנתונים הידועים למערך המחשוב.

מקרה של אי התאמה יטופל על ידי פקיד ב-"קו שני", שיהיה חשוף לתשובות הצפויות, כדי לתת מענה לבעיות איות וכדומה. בשלב זה יכול פקיד זה לזכות את התשובה שהפקיד הקודם דחה (אם נוכח שמדובר בטעות הקלדה או איות לדוגמה) או לבצע אימות נוסף בעזרת שאלות חוזרות או שאלות נוספות.

תהליך התשאול הינו תהליך חדש עם משמעויות תפעוליות ניכרות והתובנות לגבי תהליך זה הן חלק משמעותי מהניסוי, למרות שהתהליך איננו תלוי בביומטריה. ידוע ממקומות אחרים בעולם שתהליך זה גרם לבעיות רבות[40] אך היכולת להשתמש במרשם האוכלוסין לצורך זה היא גורם המייחד את המקרה שלנו ממדינות אחרות.

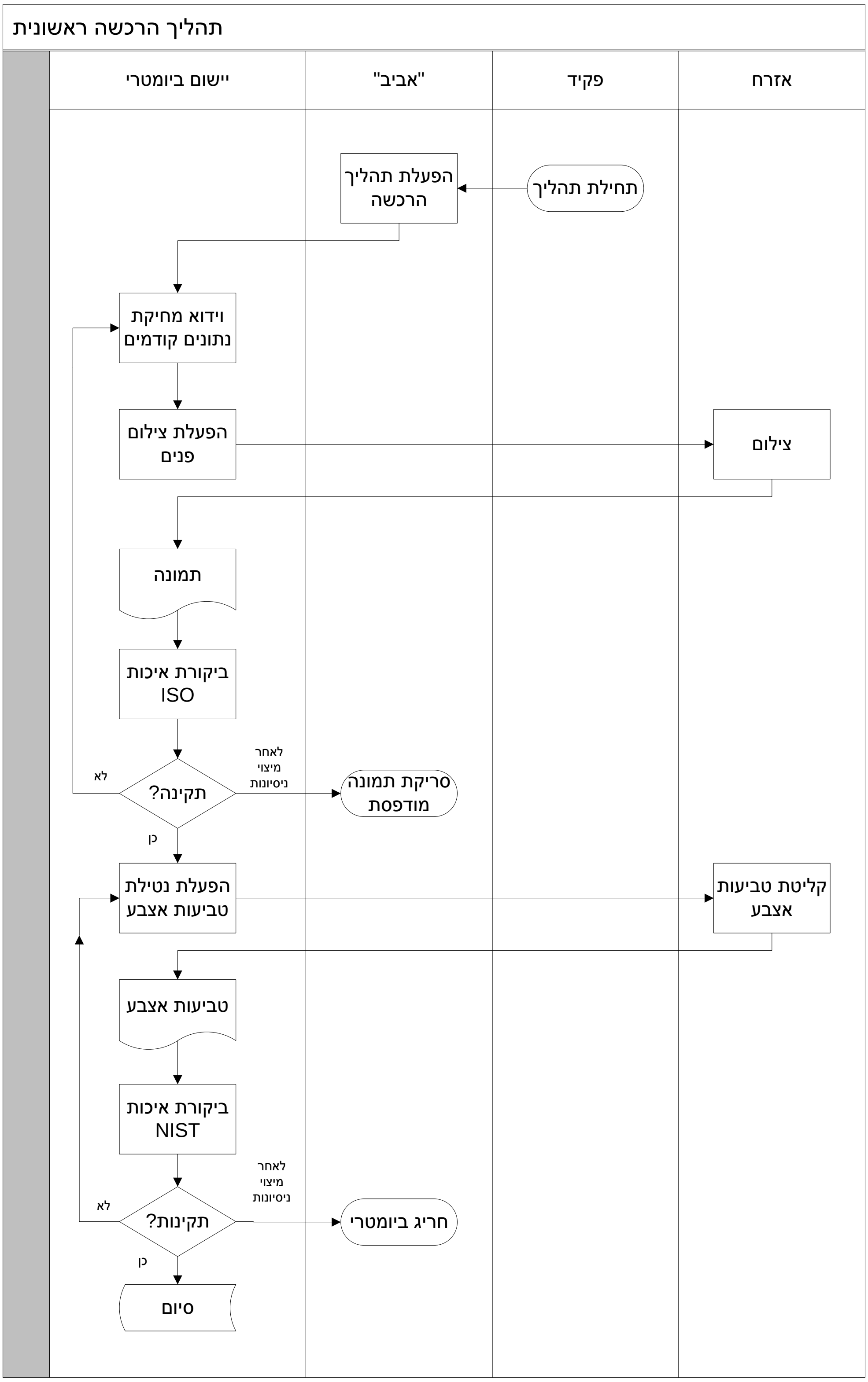
מימוש תהליך זה במערכות המידע של רשות האוכלוסין ישמש גם לניסוי השוואתי עקיף שיבחן את התשאול ככלי **למניעת** הרכשות כפולות, גם אם איננו יכול **לאתר** הרכשה כזו. במסגרת ניסוי זה, שיתבצע בסביבת בדיקות, תבוצע הדמיה של אוכלוסייה מבוקרת, שתקבל תיעוד מהסוג הישן ותעבור רק תהליך תשאול. לאחר מכן אוכלוסייה זו תנסה לעמוד בתהליך התשאול בזהות שונה. במקביל אותה אוכלוסייה תבצע תהליך דומה מול המערכת הביומטרית (קבלת תיעוד בזהות אמיתית ואחר כך בזהות אחרת).

במקרה של כישלון בתשאול לא ניתן כמובן לדעת שמדובר בשני מופעים של אותו אדם (אירוע הרכשה כפולה) אך יתכן שעצם "הגבהת הרף" בקבלת תיעוד תגרום לכך שאותם אירועים **ימנעו**, גם אם לא **יתגלו** כאירועי הרכשה כפולה. פרטי ניסוי זה יסוכמו בהמשך. ראה הסבר נוסף בסעיף 19.3.1.2 להלן ופירוט מגבלות ניסוי זה בסעיף 10.1 לעיל.

---

[40] ראה דו"ח שנתי של שירות הדרכונים הבריטי בסעיפים הנוגעים לתהליך Authentication By Interview והשינויים שחלו בו. בעיקר מדובר על העלויות הגבוהות של תהליך זה עקב העדרו של מרשם אוכלוסין. מסמכים אלו זמינים באתר http://www.ips.gov.uk

11.2. הרכשה ראשונית

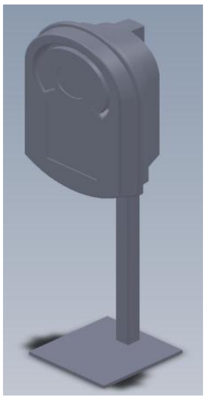


- בלמ"ס -

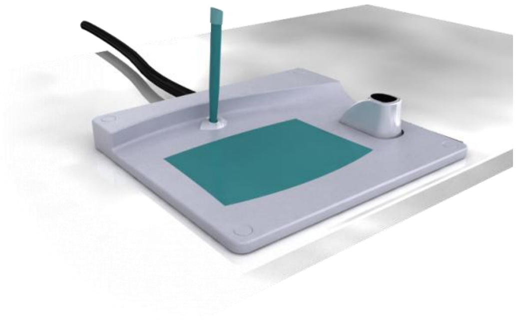
תהליך ההרכשה יכלול צילום פנים ודגימה של טביעות משתי אצבעות. התהליך יבוצע בדרך כלל בעמדות קבלת הקהל של הרשות או באמצעות עמדות ניידות. חלק בלתי נפרד מתהליך זה הוא ביקורת איכות, הן של תמונת הפנים והן של טביעות האצבע. טביעות האצבע נבחנות באמצעות מדד ביקורת איכות של NIST[41] המדרג את טביעות האצבע בסולם של "1" (הכי טוב) עד "5" (הכי גרוע). תמונות הפנים נבחנות באמצעות תוכנת Facevacs של חברת Cognitec המבצעת בדיקה על פי תקן ISO19794, פרק 5, נספח A. הבדיקה איננה כוללת את כל דרישות התקן אלא נגזרת שלהן, כמפורט במכרז 28-2008 ובנספח 19.2.

עבור כל נתון ביומטרי יבוצעו לכל היותר שישה ניסיונות נטילה, בתנאים זהים, עד לקבלת נתון איכותי דיו או עד למעבר לנוהל חריגים.

עמדת הצילום כוללת מצלמה, תאורה ומסך עזר, המספק למצולם משוב על מצג הראש ועל תוצאת הצילום. עמדה זו מותקנת ברוב עמדות קבלת הקהל על הדופן השמאלית (במבט מצד מקבל השירות).



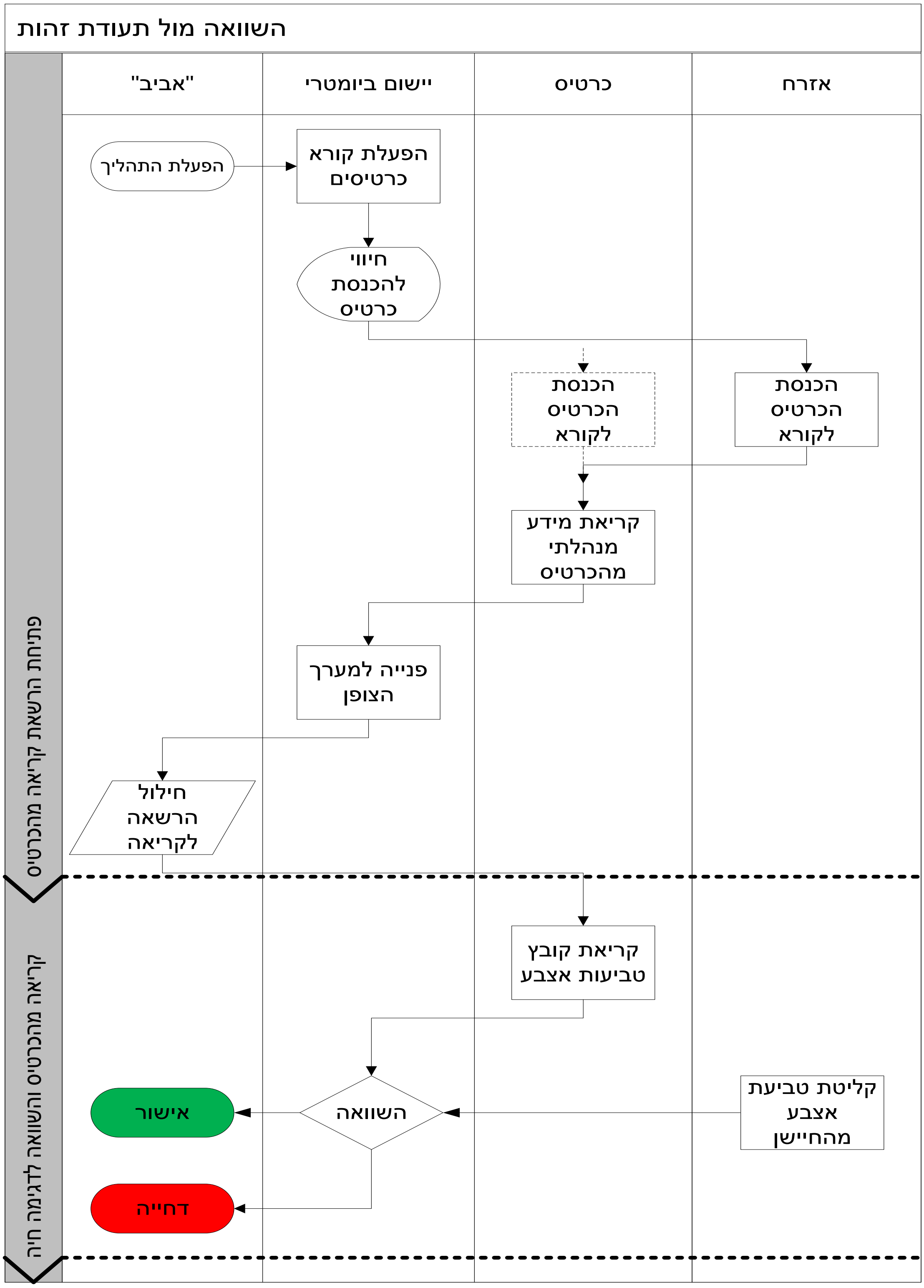
חיישן טביעות האצבע ומשטח החתימה נמצאים במארז ייעודי המונח על השולחן שבין הפקיד למקבל השירות ואיננו מחובר אליו בחיבור קשיח, כדי לתת מענה לימניים ושמאליים.



41 ראה פרטים באתר http://www.nist.gov/itl/iad/ig/nbis.cfm

- בלמ"ס -

11.3. השוואה מול תעודת זהות



בחלק מעמדות קבלת הקהל יותקן קורא כרטיסים לשימוש משרדי (להבדיל מקורא לשימוש ביתי) המאפשר תקשורת עם כרטיס תעודת הזהות. קורא זה, מתוצרת Gemalto, יכיל גם PIN pad לצורך

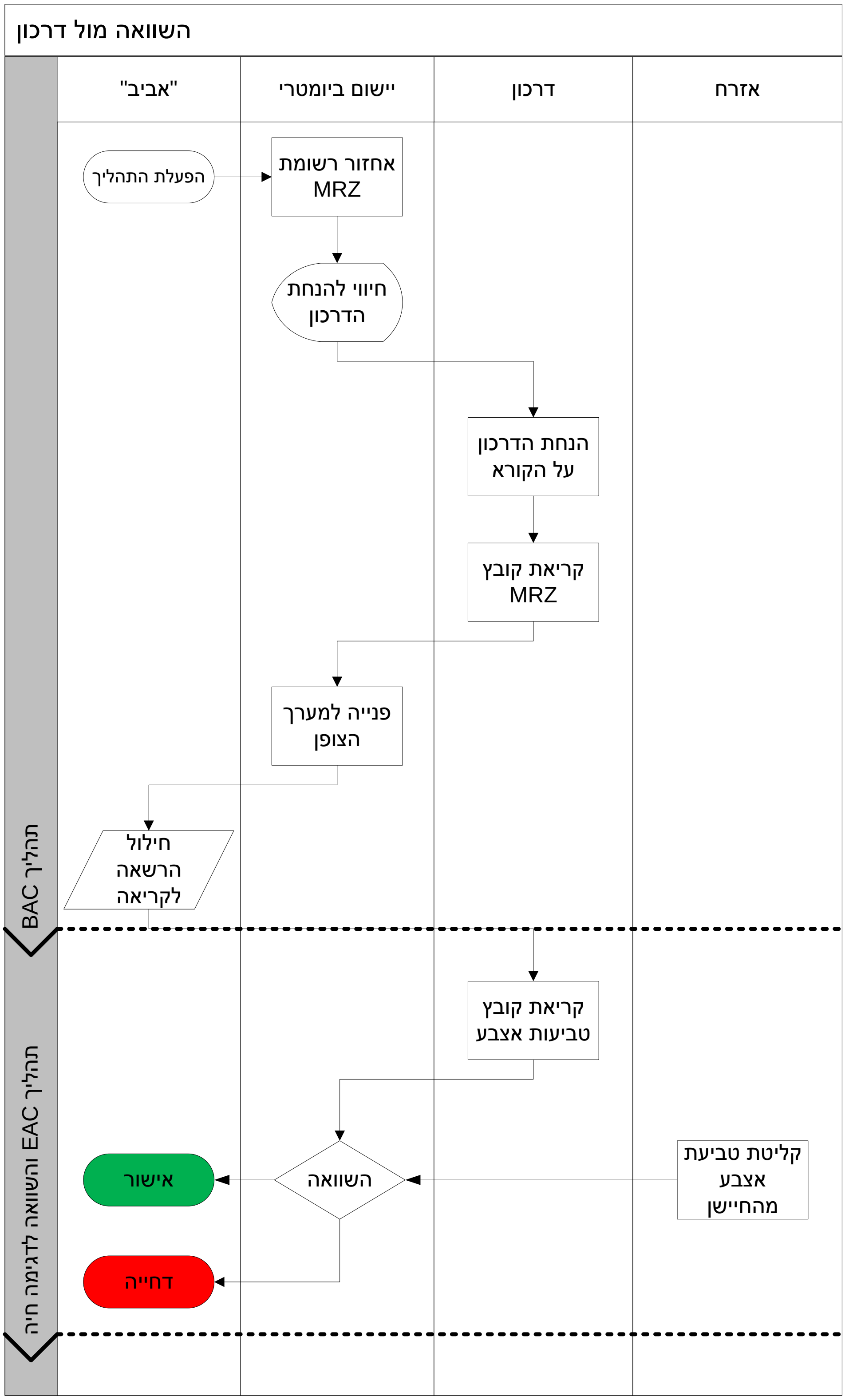
הקשת קוד הזיהוי האישי על ידי מקבל התעודה כאשר מתעורר צורך להשתמש בתעודות הדיגיטאליות שעל הכרטיס או שהאזרח/תושב רוצה לקבוע את הקוד האישי בעת שהותו בלשכה[42]. הכנסת הכרטיס לקורא תתבצע על ידי האזרח עצמו או על ידי הפקיד, בהתאם לצורך. השימוש ב-PIN pad מאפשר להקיש את הקוד האישי בלי לחשוף אותו למחשב של הפקיד.

פתיחת הרשאת הקריאה של קובץ טביעות האצבע מחייבת נגישות לתשתית צופן שמותקנת אך ורק במערכת "אביב". הרשאה זו מתבססת על חתימה דיגיטאלית כאשר היישום הקורא מציג לשבב אשרה (certificate) ואחר כך חותם על אתגור אקראי שהכרטיס מנפיק לו. הכרטיס שומר מפתח פנימי המאפשר לו לאמת את תשובת היישום ולאפשר את קריאת המידע אם תשובה זו הייתה נכונה.

לאחר קריאת המידע הביומטרי מהכרטיס ניתן לבצע את הדגימה החיה באמצעות החיישן ולהשוות בין שני הנתונים. השוואה זו מבוצעת בצורה מקומית בעמדה והנתונים נמחקים מיד לאחר מכן. תוכנת ההשוואה בודקת את ציון ההתאמה כנגד סף ההחלטה ומספקת חיווי ברור על כישלון או הצלחה.

[42] יש אפשרות נוספת לבצע שינוי זה בכל עת, על ידי בעל התעודה, בעזרת תוכנת תל"מ אישי על מחשבו האישי של האזרח/תושב.

11.4. השוואה מול דרכון



למרות הדמיון העקרוני בין התהליכים השוואה מול דרכון שונה במעט מהשוואה מול תעודת הזהות עקב השוני הטכנולוגי ביניהם (כרטיס מגע לעומת שבב עם תקשורת אלחוטית) אך גם שונה עקב השימוש במנגנוני הגנה אחרים האופייניים לדרכון אלקטרוני ומוגדרים בתקינה הבינלאומית בנושא זה[43].

לצורך התקשורת עם השבב בדרכון יש לאחזר את רשומת ה-MRZ[44] שלו, באמצעות קורא אופטי ייעודי או מתוך בסיס הנתונים של מערכת "אביב" באמצעות מספר הדרכון. מתוך נתוני ה-MRZ גוזרים בתהליך חישובי פשוט את מפתח ההצפנה של הדרכון הספציפי. ללא מפתח זה לא ניתן לתקשר עם השבב שבדרכון.

לאחר חישוב מפתח ההצפנה ופתיחת ערוץ התקשורת המוצפן מול השבב יש לקרוא את קובץ ה-MRZ מהשבב (הנקרא DataGroup1) ולהשוות את תוכנו לנתוני ה-MRZ המודפסים או המאוחזרים. אם קריאת קובץ זה הצליחה אזי מפתח ההצפנה שחושב הוא אכן המפתח הנכון. בשלב זה ניתן לקרוא את קובץ תמונת הפנים בלבד, כאשר יתר הקבצים הרגישים אינם פתוחים לקריאה. לצורך קריאת קובץ טביעות האצבע יש לבצע תהליך חישובי מורכב יותר, הכולל חתימה דיגיטאלית של סביבת הקריאה על אתגור אקראי שמייצר השבב. בצורה כזו מוכיחה סביבת הקריאה לשבב שיש לה הרשאה לקרוא קובץ זה[45]. אחת מתוצאות המשנה של תהליך זה היא החלפה של המפתח הראשוני שחושב מתוך ה-MRZ[46] במפתח מאיכות גבוהה יותר. המפתח החדש מספק הגנה טובה יותר לקריאת קובץ טביעות האצבע.

לאחר קריאת הקובץ ניתן ליטול דגימה חיה מהחייש ולהשוות אותה למידע מהדרכון כמקובל. גם במקרה זה נמחק המידע הביומטרי שבעמדת הבדיקה מיד לאחר מכן.

[43] ראה תקן ICAO בשם ***DOC9303 part 1 volume 2*** ונספחיו, שהתקבל גם כתקן ISO 7501.

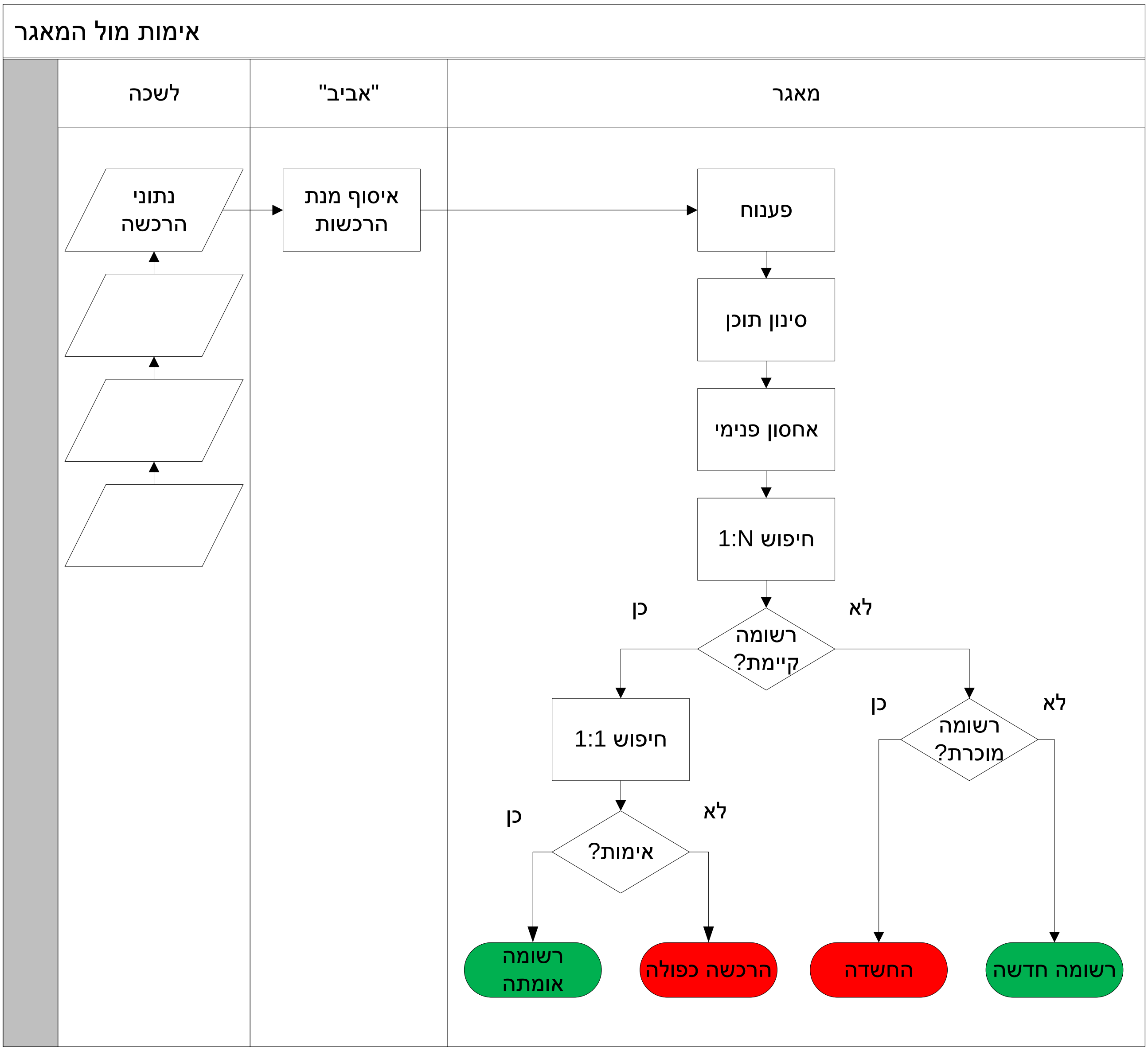
[44] **MRZ** = Machine Readable Zone, שתי השורות המודפסות בתחתית דף הפרטים של הדרכון באמצעות גופן תקני ומיועדות לקריאה ממוכנת ע"י OCR (Optical Character Recognition)

[45] ראה מסמך בשם ***Technical guidelines TR-03110***, גרסה 1.11 מאת ה-BSI בגרמניה, שהתקבל כמודל הרצוי על ידי האיחוד האירופאי ואומץ גם עבור הדרכון הישראלי.

[46] מפתח זה הוא דל-אנטרופיה באופן יחסי ומספק הגנה אפקטיבית כמו מפתח שאורכו 40 עד 45 סיביות בלבד. מפתח כזה טוב דיו נגד קריאה לא מורשית של הדרכון (skimmimg) אך לצורך הגנה על טביעות האצבע נדרש מפתח טוב יותר.

11.5. אימות מול המאגר

תרחיש זה נחלק לשני מצבי משנה מבחינת התוצאה: קליטה של רשומה חדשה, שאיננה קיימת במאגר, או אימות של רשומה קיימת (לדוגמה בעת חידוש תיעוד). אם אימות זה נכשל מדובר בחשד להרכשה כפולה או בטעות רישום. אם הרשומה איננה קיימת במאגר למרות שידוע שהיא מוכרת התוצאה תהיה החשדה של רשומה זו ובדיקה מדוע איננה מזוהה.



השימוש התדיר ביותר של תהליך זה יהיה עבור בדיקת ההרכשות השוטפות כדי לאתר הרכשות כפולות. התהליך יבוצע מדי יום (או מספר פעמים ביום) על מנות של רשומות הרכשה מוצפנות, המגיעות למאגר ממערכת "אביב". מערכת "אביב" תרכז את ההרכשות מהלשכות (שהוצפנו במקור), תחתום על

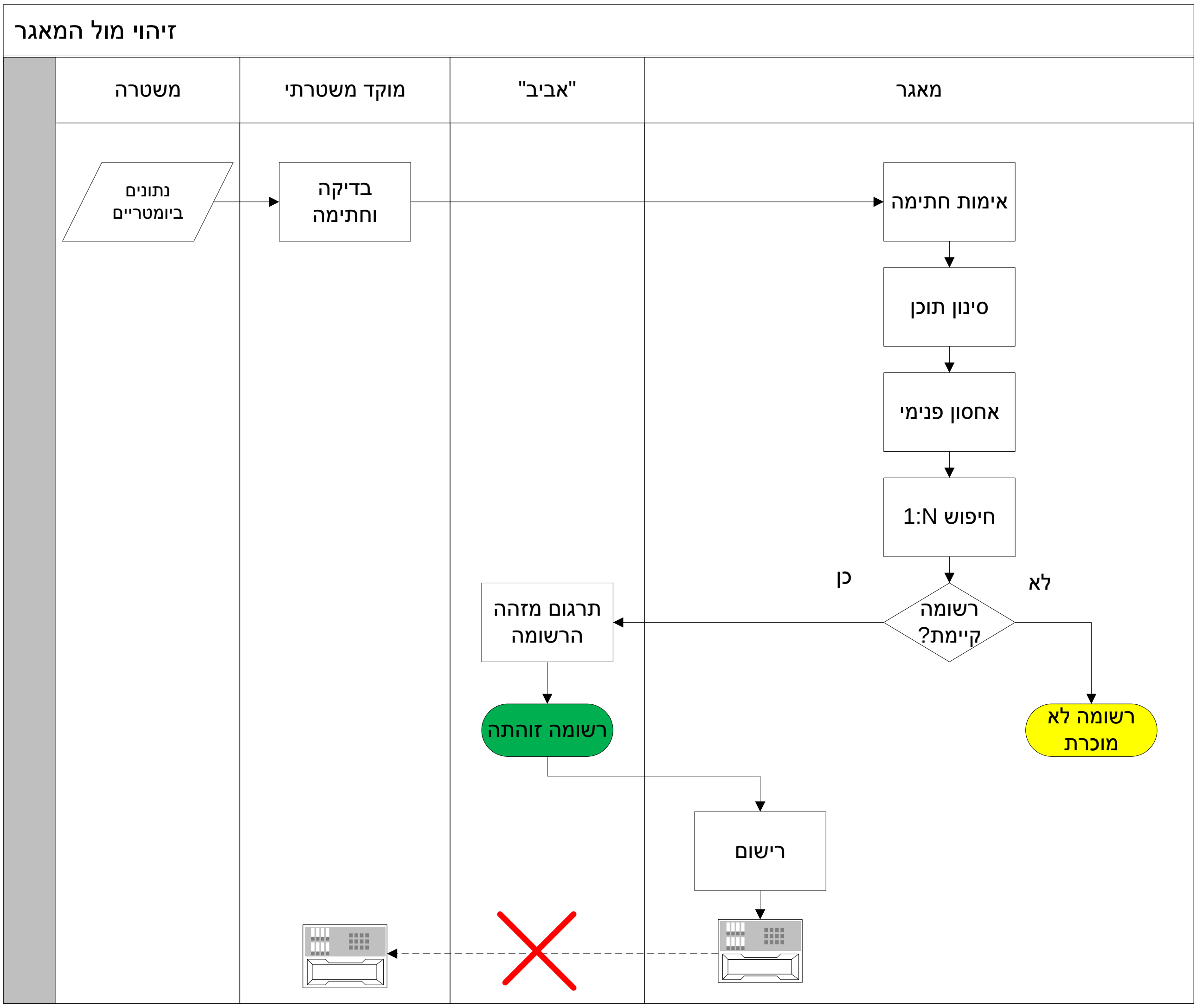
מנת ההרכשות, תעביר מנה זו למאגר (ובמקביל למערכי ההנפקה, כמפורט בסעיפים 3 ו-4 של החוק) ולאחר קבלת אישורו/התייחסותו למערכי ההנפקה המתאימים. לאחר פענוח הרשומות, אימות החתימה של "אביב" וסינון תוכן נגד קוד מפגע יועבר המידע לרשת הפנימית והנפרדת של המאגר ויופעל באופן עקרוני חיפוש מסוג one to many. העברת המנה לרשת הפנימית מבוצעת בצורה ידנית ולא בתקשורת, בצורה שיוצרת קישור חד כיווני שאיננו מאפשר זליגה של מידע לא מוצפן לרשת החיצונית.

חיפוש זה יניב תוצאה אחת באופן אידיאלי או מספר מצומצם של תוצאות, שתעבורנה סינון ידני. למעשה, אם מדובר ברשומה מוכרת למאגר (כמו בעת חידוש תיעוד) תיבדק ההתאמה לרשומה הקודמת במתכונת של one to one ויתכן שיבוצע עדכון שלה, אם איכות הדגימות החדשות גבוהה דיה ונמצאה ביניהן התאמה.

אם לא נמצאה התאמה עבור רשומה מוכרת תוגדר רשומה זו כהרכשה כפולה לכאורה ותטופל בהתאם. באותה מידה, רשומה שלא זוהתה אך ידוע שהיא מוכרת למאגר תוחשד אף היא. אם רשומה לא אמורה להיות מוכרת ולא זוהתה בחיפוש מסוג one to many היא תוגדר כרשומה חדשה ותאוחסן במאגר.

11.6. זיהוי מול המאגר

תרחיש זה ייבדק בתקופת המבחן רק באמצעות הדמיה או בעת איתור הרכשה כפולה אמיתית, כאשר מעוניינים לאתר למי שייכת רשומה ביומטרית ספציפית. יש לזכור שהמאגר איננו מכיל פריטי מרשם כך שהשלמת תהליך זיהוי תחייב שאילתה גם במערכת "אביב" כדי לתרגם בין המזהה שמופיע במאגר ובין מספר זהות בפועל. ההיגיון האבטחתי מאחורי תהליך זה כולל חיפוש בשתי מערכות מידע בלתי תלויות (המאגר ומערכת "אביב") כדי ליצור רשומת קובץ יומן (log) בשתי המערכות.



בתקופת המבחן תבוצענה הדמיות (סימולציות) של שאילתות מהמשטרה. הקשר מול המשטרה יבוצע באמצעות מוקד ייעודי אליו יועברו כביכול נתונים מהשטח. באחריותו של מוקד זה לוודא שהתמלאו כל התנאים להגשת שאילתה, כמפורט בחוק. המוקד יחתום על הנתונים באמצעות כלי חתימה אלקטרונית כדי לאפשר למאגר לאמת את מקורם. ההדמיה תכלול את כל שלבי התהליך אך בסיומו לא תועבר

תשובה למוקד. גם במקרה זה ייתכן שהרשומה לא תאותר כלל ויבוצע תהליך דומה לתהליך שתואר בסעיף 11.5 לעיל כדי לבחון האם הרשומה אמורה להיות מוכרת ומדוע לא זוהתה. יודגש שנית שבתקופת המבחן לא תועבר בפועל תשובה למוקד המשטרתי והתהליך ייעצר לאחר זיהוי הרשומה.

12.בעלי תפקידים

להלן רשימת בעלי התפקידים בניסוי:

12.1. ועדה מייעצת

הועדה המייעצת לתקופת המבחן תכלול נציגים של הגופים הבאים (ראה גם סעיף 8.1.7.9 לעיל):

12.1.1. הסטטיסטיקאי הראשי - למ"ס

12.1.2. הממונה על יישומים ביומטריים במשרד רוה"מ

12.1.3. ראש רמו"ט

12.1.4. רמ"ט לוט"ר

12.1.5. נציג ציבור

12.2. מנהל הניסוי מטעם הרשות לניהול המאגר הביומטרי

מנהל הניסוי יהיה מנהל תחום הגנת הפרטיות ברשות לניהול המאגר הביומטרי.

12.3. מנהל הניסוי מטעם רשות האוכלוסין

מנהל הניסוי יהיה מנהל אגף הפרויקטים ומרכז ההנפקה של מסמכי הנסיעה.

12.4. נאמני מחשוב

נאמני המחשוב בלשכות רשות האוכלוסין יודרכו וישמשו כגורם העיקרי המרכז את אותם נתונים שאינם נאספים באופן ממוכן, כגון התרשמויות של הפקידים מהתהליכים והטכנולוגיה והערות של אזרחים, ככל שתהיינה כאלה.

12.5. פקידים

פקידי רשות האוכלוסין הם אלו שיבצעו את מירב התהליכים שיש להם ממשק לאזרח (הרכשה, מסירת תיעוד, מתן שירות על בסיס תיעוד, הסברה וכו').

12.6. משתתפים

המשתתפים יכללו שתי אוכלוסיות:

12.6.1. אזרחים/תושבים

אזרחים ותושבים שיתנדבו לתקופת המבחן.

12.6.2. מרכזי ביומטריה

עובדי לשכות רשות האוכלוסין שיוכשרו כדי להכיר בצורה מעמיקה את נושא הביומטריה ושילובה במערכת "אביב".

12.6.3. אוכלוסייה לצורך הדמיות

אוכלוסייה נבחרת, כדוגמת עובדי מדינה, לצורך יצירת אירועים יזומים מסוגים שונים כגון אירועי התחזות והרכשה כפולה, מול המאגר הביומטרי. כאמור, אירועים אלו כפופים לאישור משפטי ויבוצעו בסביבת בדיקות כדי להימנע מהכנסת זהויות לא אמיתיות למאגר הביומטרי ולמרשם האוכלוסין.

12.7. עובדי רשות האוכלוסין, הרשות לניהול המאגר הביומטרי ומערכי ההנפקה

ביצוע העבודה השוטפת הנדרשת בתהליך ההרכשה, השוואת הנתונים הביומטריים, אישורם והנפקת התיעוד הנדרש.

13.תיעוד במהלך הניסוי

מערכות המחשוב של רשות האוכלוסין ושל הרשות לניהול המאגר הביומטרי תבצענה רישום ממוכן של רוב הנתונים הדרושים לצורך הערכת איכות התהליך התפעולי ובחינת הנושאים הטכנולוגיים השונים. חלק קטן מהנתונים ייאסף בצורה שאיננה ממוכנת. איסוף המידע הרלבנטי יבוצע על פי העקרונות הבאים:

13.1. כללי

במהלך תקופת המבחן יש צורך לאסוף כמות רבה מאד של נתונים מסוגים שונים (ראה פירוט בסעיף 14 להלן). איסוף זה יבוצע בדרך כלל בצורה ממוכנת, ללא מתן שיקול דעת למפעילי המערכת האם לבצע איסוף או לא וללא מעורבות שלהם. חלק קטן מהנתונים ייאסף באמצעים שאינם ממוכנים, ובכלל זה התרשמויות של מפעילי המערכת, רשמים של אזרחים והצעות לייעול ושיפור התהליך. נתונים כאלו ייאספו באופן שיטתי לאורך כל תקופת הניסוי, בעיקר באמצעות נאמני המחשוב.

13.2. תדירות

הנתונים ירוכזו וייבדקו לפחות אחת לחודש באופן פנימי כדי לקבל תמונה עדכנית על התקדמות הניסוי וכדי לאפשר כיול של פרמטרים שונים להשבחת התהליכים. אחת לחצי שנה יופקו דוחות כנדרש בתקופת המבחן המוגדרת בצו. המידע הנ"ל ודוחות חצי שנתיים הנוצרים בחלקים שונים של המערכת (כדוגמת מערך ביקורת הגבולות) ימסרו למנהל אגף פרויקטים ברשות האוכלוסין.

13.3. סקר שביעות רצון

החל משלושה חודשים ממועד התחלת תקופת המבחן ולכל אורכה יערך סקר שמטרתו למדוד את שביעות רצון התושבים מאותם היבטים של תהליך הנפקת התיעוד החכם בהם מתקיימים ממשקים עם התושבים (תהליך הטיפול בבקשה לקבלת התיעוד ותהליך מסירת התיעוד).

הסקרים יעוצבו ויבוצעו על ידי הלשכה המרכזית לסטטיסטיקה שאף תעבד את תוצאותיהם ותצליב אותם עם משתני רקע דמוגרפיים שיש בידיה.

פרטי סקר שביעות רצון מתהליך קבלת התיעוד:

13.3.1. מהות הסקר

בסקר זה תבחן שביעות רצון התושבים מתהליך הטיפול בבקשה לקבלת תיעוד ברשות האוכלוסין וההגירה ובמקרים של הנפקת תיעוד חכם – גם את שביעות הרצון מתהליך המסירה של התיעוד תוך התייחסות לנושאים הבאים: פרקי זמן, איכות ההסברים, מיומנות הפקידים, אדיבות הפקידים, איכות התוצר ושביעות רצון כללית. הסקר יבחן גם סיבות לרצון או אי רצון לקבלת תיעוד חכם על מנת לאפשר למידה והפקת לקחים לצורך מיקוד פעולות ההסברה.

13.3.2. אופי הסקר

הסקר יהיה סקר טלפוני, שיבוצע באופן מדגמי בקרב שלוש קבוצות התייחסות: המגישים בקשה לקבלת תיעוד חכם, שסיימו את תהליך הטיפול בבקשה והונפק עבורם התיעוד המבוקש; המגישים בקשה לקבלת תיעוד חכם, שהטיפול בבקשה לא הושלם ולא הונפק עבורם התיעוד המבוקש; המגישים בקשה לקבלת תיעוד רגיל (לא מעוניינים בתיעוד חכם).

13.3.3. גודל המדגם

גודלו של המדגם יעמוד על 15,000 איש בשנה; 5,000 איש לכל קבוצת התייחסות. (7500 נדגמים ברוטו בכל ששה חודשים – שיעורי השבה צפויים לסקר 80%).

מסגרת הדגימה תועבר ללשכה המרכזית לסטטיסטיקה, אחת לשבוע, מרשות האוכלוסין וההגירה, לאורך תקופת ביצוע הסקר. הריאיון יתקיים בתוך שבועיים ממועד הפנייה של התושב לרשות האוכלוסים וההגירה לצורך קבלת תיעוד חכם.

סקר נוסף ימדוד בהמשך את שביעות רצון התושבים מאופן השימוש השוטף בתיעוד. בסקר זה תבחן שביעות רצון התושבים מן השימוש בתעודה ובדרכון בלשכות רשות האוכלוסין, בנתב"ג ומול שירותי "ממשל זמין".

נושאי הסקר, דרך איסוף הנתונים, מועד התחלתו, תדירותו והיקפו יקבעו לאחר פרק זמן שיאפשר למידה של התהליך אותו רוצים להעריך, בהתאם ללוחות הזמנים הבאים: לא יאוחר משישה חודשים ממועד התחלת תקופת המבחן - במקרה של בחינת שביעות הרצון מהשימוש בתיעוד החכם בלשכות רשות האוכלוסין; לא יאוחר מארבעה חודשים מהתחלת מועד השימוש בתיעוד חכם בתהליך בקורת הגבולות בנתב"ג - במקרה של בחינת שביעות הרצון מהשימוש בתיעוד החכם בנתב"ג; ולא יאוחר משלושה חודשים מהמועד בו הופעלו חמישה שירותי "My Gov" שונים – במקרה של בחינת שביעות הרצון מהשימוש בתיעוד החכם מול "ממשל זמין".

13.4. קבלת משוב שוטף

לאורך כל תקופת המבחן יש לקבל משוב ממפעילי המערכת (בעיקר פקידי רשות האוכלוסין) כדי לייעל את התהליכים השונים ולכוונן פרמטרים של המערכת.

13.5. טיוב נתונים ורשומות

פועל יוצא של התיעוד הוא שיפור המערכת לאורך תקופת המבחן. במהלך תקופה זו יתבצעו תהליכי טיוב נתונים. טיוב הנתונים במאגר יתבצע על בסיס הרצת המערכת מעבר לשעות העבודה תוך הורדה למינימום של ספ ה-FA (לסף נמוך מהסף שנקבע בתהליך העבודה השוטפת). בנוסף לטיוב הנתונים

והרשומות הקיימות במערכת יתבצעו תהליכים של בקרה עצמית שיבוצעו על ידי בדיקות מדגמיות של גורם מקצועי נוסף לעובד אשר קיבל החלטה באופן שוטף, זיהוי שגיאות של המערכת ומדידתן.

14.נתונים ומדדים להצלחה

להלן הנתונים שייאספו בתקופת המבחן ומולם המדדים שייחשבו כהצלחה עבור נתונים אלו (כאשר ניתן לקבוע מדדים כאלו):

14.1. נתוני הרכשה

נתונים אלו ייאספו בלשכות רשות האוכלוסין (ולא במאגר) ורלבנטיים הן לדרכון והן לתעודת הזהות החכמה:

14.1.1. כמות הנרשמים

כמות ההרכשות שתבצע רשות האוכלוסין היא בראש וראשונה פועל יוצא של כמות הנרשמים לפיילוט אך תושפע גם מהיכולת הטכנולוגית לבצע הרכשה תקינה. לגבי מספר הנרשמים לפיילוט - הערכתנו היא שלפחות 20% מכלל מבקשי דרכון ו/או תעודת זהות יעדיפו את המסלול הביומטרי באופן מובהק. מספר לא גבוה זה נובע בעיקר עקב הפגיעה לכאורה ברמת השירות, בעקבות **<u>המעבר להנפקה מרכזית</u>**[47] המחייבת אותם להגעה נוספת ללשכה לצורך קבלת התיעוד[48] (לאחר ייצורו באתר מרכזי) **<u>ולא בגלל רתיעה מהביומטריה</u>**[49].

מעבר לסיבת ההצטרפות או חוסר הרצון להצטרף ינותחו נתונים אלו בשני אופנים: על פי נתוני מרשם (מין, גילאים, מקום מגורים וכד') ועל פי נתוני מפקד האוכלוסין (הזמינים רק ללמ"ס) ומאפשרים פילוחים נוספים (השכלה, הכנסה וכד').

14.1.2. הצלחת ההרכשה

הנחת היסוד היא שניתן להרכיש תמונת פנים עבור קרוב מאד ל-100% מהאוכלוסייה[50]. לעומת זאת ייתכן שהמובהקות הנמוכה יותר באופן טבעי של תמונות פנים או איכות התמונות עצמן תגרום לכך שלא ניתן יהיה להשתמש בהן בצורה טובה כנתון ביומטרי.

---

[47] מעבר כזה להנפקה מרכזית של תיעוד לאומי הוא מגמה כלל עולמית ונובע הן משיקולי ביטחון והגנה על חומרי הגלם הרגישים שמהם מורכב תיעוד מודרני והן משיקולים כלכליים. ייצור תיעוד מודרני מחייב מיכון מורכב ויקר, שלא ניתן לפרוס בכל מקום. לעומת זאת במקום אחד מרכזי ניתן להצטייד במיכון טוב ובעלות סבירה. הנפקה מרכזית מאפשרת גם גמישות רבה יותר בהיבט הטכנולוגי.

[48] מסירת תעודת הזהות לאזרח לאחר ייצורה כוללת אימות זהות (כדי לוודא שהמקבל הוא אכן מי שפרטיו רשומים בתעודה והפעלת התעודות הדיגטאליות שמחייבת נוכחות פיזית של בעל התעודה).

[49] לדוגמה, בעת הפעלה ניסיונית והתנדבותית של מערכת unipass על ידי רשות שדות התעופה, שהוגבלה אך ורק לנוסעי premium של אל-על, נרשמו תוך שבועות בודדים יותר מ-13 אלף איש, שרובם ככולם הביע התלהבות ניכרת מהטכנולוגיה ומיתרונותיה.

[50] ראה גם דו"ח של שירות הדרכונים הבריטי בשם "***UKPS Biometrics enrolment trial***" משנת 2005.

כדי לאמת זאת יש לאסוף קודם כל את הכמות הכוללת של ההרכשות המתבצעות בלשכות על פי התנאים הבאים:

14.1.2.1.הרכשות מלאות ותקינות

הרכשה מלאה כוללת תמונת פנים ושתי אצבעות מורות.

14.1.2.2.הרכשות חלקיות

הרכשה חלקית תיחשב כל הרכשה הכוללת תמונת פנים ושתי אצבעות אחרות.

14.1.2.3.הרכשות חסרות

הרכשה הכוללת תמונת פנים בלבד.

מנתונים שהתפרסמו במדינות אחרות ידוע שעבור 1-2% מהאוכלוסייה כלל לא ניתן לבצע הרכשה של טביעות אצבע תקינות אך רוב הנתונים שהתפרסמו מתייחסים להרכשה של עשר אצבעות, שמטבעה היא יותר בעייתית. עבור אוכלוסיות שאינן בעלות מוגבלויות הנתונים הם טובים עוד יותר, כאשר מספרם של אלו שלא ניתן ליטול מהם טביעות אצבע נמוך מ-0.8%[51]. אנחנו מצפים לתוצאות מעט יותר טובות אצלנו כי ההרכשה היא רק של שתי אצבעות והחיישן שנבחר עבור מערך ההרכשה (ראה סעיף 8.2.1.2 לעיל) הוא חיישן מתקדם מאד, המצטיין ביכולתו להרכיש תמונה באיכות גבוהה מאד מטווח רחב מאד של אוכלוסיות.

אנו מצפים ליותר מ-90% הרכשות מלאות וחלקיות עבור אוכלוסיות בקבוצות גיל מוגדרות שעבורן יתבצע ניסיון הרכשה מלא. אימות של נתון זה ייחשב כהצלחה.

הערה: כדי למנוע הטיה לרעה של התוצאות יש לבדוק נתון זה רק עבור אותן קבוצות גיל ולהוציא מהמשוואה ילדים מתחת לגיל 12 שעבורם לא תתבצע הרכשה מלאה בכל מקרה.

14.1.3. נתוני סריקה

במקרים חריגים מאד ורק לאחר אישור מיוחד, כאשר לא ניתן לצלם את מבקש התיעוד תבוצע סריקה של תמונה מודפסת. נתון זה יגדיר כמה מקרים טופלו באמצעות סריקת תמונות מודפסות ומה הן איכויות ההרכשה כתוצאה מכך. השאיפה היא לצמצם מקרים אלו ככל האפשר ולהשתמש

[51] ראה דו"ח של שירות הדרכונים האנגלי בשם "***UKPS Biometrics enrolment trial***" משנת 2005.

בסריקת תמונה מודפסת רק עבור אותם מקרים בודדים שבהם לא ניתן לבצע הרכשה כמקובל (חולים מרותקים למיטה וכד').

14.1.4. נתונים תפעוליים

נתונים אלו דרושים כדי לתכנן בצורה מיטבית את תהליכי העבודה בלשכות רשות האוכלוסין. הנתונים ייבחנו בעיקר בחתך של גילאים, כאשר האוכלוסייה הנבדקת תחולק לקבוצות גיל על פי הטבלה הבאה:

10...0
20...10
30...20
40...30
60...40
70...60
80...70
יותר מ-80

הערה: החלוקה לעשורים היא שרירותית ויתכן שלא תהיה שונות רבה בין קבוצות הגיל השונות. נתונים תפעוליים ייאספו אולם לא יוגדרו לגביהם מדדים להצלחה או כישלון, למעט מקרים בודדים.

מעבר ליכולת ההרכשה באופן כללי יהיו המדדים להצלחה תפעולית של התהליך כדלקמן:

14.1.4.1.מספר הניסיונות הנדרשים עד להרכשה מוצלחת

בתקופת המבחן ניתן יהיה לבצע עד שישה ניסיונות לקבלת הנתונים הביומטריים. המדד להצלחה בסעיף זה יהיה קבלת נתונים ביומטריים תקינים (ראה סעיף 14.1.5 לעיל) עבור 90% מהאוכלוסייה תוך שלושה ניסיונות לכל היותר.

14.1.4.2.הזמן הממוצע הנדרש להרכשה מוצלחת

הצפי הוא שזמן הטיפול המרבי הכולל בעמדת קבלת הקהל, מול המבקש, לא יעלה על 10 דקות עבור 90% מהמבקשים. זמן זה כולל הרכשה ביומטרית, תשאול וטיפול כמקובל עבור הנפקת תיעוד לאומי[52]. יש צורך לחלק את פרק הזמן הזה בין שלב התשאול ובין שלב ההרכשה.

14.1.4.3.כמות המורכשים שהועברו לנוהל חריגים

נתון זה ייצג את הבעייתיות של תהליך ההרכשה ויכלול את אלו שעלה חשד לגביהם בשלב התשאול ואת אלו שלא ניתן היה לקבל מהם דגימות ביומטריות תקינות, **<u>מכל הסיבות</u>**. מספר זה צפוי להיות נמוך מ-2% אולם בתחילת הפעלת התהליך, במהלך עקומת הלמידה של מפעילי העמדות, הוא צפוי להיות גבוה יותר, עד 25%. חלק מהמקרים יופנו לסריקת תמונות מודפסות כאמור בסעיף 14.1.3 לעיל.

הצפי הוא שעיקר הבעיות תהיינה בשלב <u>התשאול</u> ולא בשלב <u>ההרכשה</u>.

14.1.4.4.כמה מורכשים זכו לפתרון באמצעות הנוהל לחריגים

נתון זה יספק תובנות על נוהל הטיפול בחריגים ובעיקר יענה על השאלה האם נוהל זה נותן מענה ראוי לבעיות של תהליך ההרכשה. השאיפה היא למתן מענה ל-100% מאלו שטופלו באמצעות נוהל החריגים.

14.1.4.5.מספר ההרכשות שבוצעו לכל זהות

נתון זה נועד לבחון את מידת המאמץ שיש להשקיע בשכנוע הציבור לקבל הן דרכון והן תעודת זהות באותו זמן, כדי להקטין את עומס העבודה בלשכות הרשות. המעבר להנפקה מרכזית מטיל עומס עבודה נוסף על עובדי הלשכות בגלל הצורך למסור את תעודת הזהות בביקור נוסף של האזרח או התושב בלשכה. אם יתגלה מצב שבו רוב משמעותי של האוכלוסייה מגיע יותר מפעם אחת לבצע הרכשה (פעם אחת עבור תעודת זהות ופעם נוספת עבור דרכון) – יש לנקוט בפעולות עידוד נרחבות כדי להניע את אותה אוכלוסייה להגיע פעם אחת בלבד לצורך הרכשה.

14.1.5. נתוני איכות

הצפי הוא שעבור יותר מ-90% מהאוכלוסייה ניתן להרכיש טביעות אצבע באיכות "1" או "2" (על פי מדד NIST[53]) וכך לקבל שמישות מרבית בעתיד. יודגש שגם טביעת אצבע שאיכותה "3" עדיין

[52] ראה גם דו"ח של שירות הדרכונים הבריטי בשם "***UKPS Biometrics enrolment trial***" משנת 2005.

[53] ראה פרטים באתר http://www.nist.gov/itl/iad/ig/bio_quality.cfm

שמישה להשוואה אם כי היא צפויה ליצור קצב שגיאות מעט יותר גבוה. לגבי תמונות הפנים אין נתונים מדויקים מהעולם ויש תלות מאד גבוהה של איכות התמונות במבנה עמדת ההרכשה וסביבתה. לצורך ניתוח איכות ההרכשה יש לקבל את ההתפלגות של תמונת הפנים על פי אותם מדדים הנבדקים בתוכנת ההרכשה. בחלק מהמקרים תישמר אך ורק **תמונה מופחתת** לצורך ניתוח ידני של תמונות פנים מעבר לאותם נתונים הנבדקים על ידי תוכנת הבדיקה. נציין שהרוב המוחלט של עמדות ההרכשה אחיד מאד אך ייתכנו תנאים סביבתיים אחרים שישפיעו על איכות התוצרים ויגרמו לשונות בין העמדות.

מדדי האיכות של תמונת הפנים יתבססו על המלצות תקן ISO19794 פרק 5, נספח A. עמידה בכל סעיפי התקן איננה מעשית[54] ולכן יכללו מדדי האיכות רק את הפרמטרים המתוארים בנספח 19.2 להלן.

14.1.5.1.איכות טביעות האצבע

נתון זה יגדיר איזה אחוז מהאוכלוסייה היה בכל רמה של איכות טביעת אצבע (על פי מדד NIST המדרג טביעה באיכות מרבית בציון "1" וטביעה באיכות גרועה בציון "5"). כאמור, אנו מצפים לקבל טביעות באיכות "1" או "2" עבור יותר מ-90% מהאוכלוסייה. טביעה באיכות "3" עדיין טובה להשוואה (בפרט מסוג 1:1) למרות שקצב השגיאות עבור טביעה כזו יהיה יותר גבוה.

14.1.5.2.איכות תצלומי הפנים

ניתוח הכישלונות האופייניים במדדי איכות תמונת הפנים על פי הבדיקות השונות שמבצעת תוכנת בקרת האיכות ועל פי ניתוח ידני שיבוצע באמצעות התבוננות בתמונות **מופחתות** שתישמרנה במיוחד לצורך זה[55].

14.2. נתוני השוואות ביומטריות

נתונים אלו ייאספו גם הם בלשכות רשות האוכלוסין (ולא במאגר).

מלבד תהליך ההרכשה תתבצע בתקופת המבחן גם השוואה ביומטרית של אזרח מול תיעודו (תעודת זהות או דרכון). השוואות כאלו תהיינה בוודאות חלק מתהליך העבודה בלשכות הרשות אך גם במקומות אחרים כדוגמת משטרת ישראל, נתב"ג או מעברי גבול אחרים. לצורך זה יש לאסוף נתונים שונים שיעזרו לתכנן את אותם תהליכים בצורה מיטבית.

---

[54] ראו מאמר הדן בנושא זה בשם "Compliance with facial image standards" מאת Uwe Seidel, שהופיע בירחון בשם *Keesing journal of documents & identity, issue 19,2006*.

[55] ראה מסמך המפרט את שיטת ההפחתה בשם "***creating reduced pictures dd-mm-yyyy***" בגרסתו העדכנית

תשתית כזו של השוואות איננה קיימת בשלב זה בגופים אחרים וככל הנראה רק בלשכות רשות האוכלוסין ניתן יהיה לבצע זאת באופן שוטף מהיום הראשון לתקופת המבחן. המשמעות בפועל היא שנקבל כמות קטנה מאד של השוואות (מאותה אוכלוסייה שגם הצטרפה לתקופת המבחן וגם חזרה שנית לקבל שירות כזה או אחר, או לכל הפחות חזרה שנית לצורך קבלת תעודת הזהות). מסיבה זו לא ניתן לצפות בשלב זה מה היא הכמות עצמה ולציין מדד כמותי. **דבר זה מחדד ביתר שאת את הצורך לבצע השוואות מסוג many to many במאגר, כדי לקבל תוצאות בעלות תוקף**[56].

יש לאסוף בלשכות רשות האוכלוסין ובמעברי הגבול נתונים על כמות ההשוואות בין נתונים ביומטריים שנקראו מהתיעוד לנתונים שנדגמו בפועל, ובפרט:

14.2.1. כמות כללית של השוואות ביומטריות

נתון זה כולל את מספר ההשוואות הביומטריות שבוצעו בצורה של קריאת נתון ביומטרי מהתיעוד, דגימת בעל התיעוד והשוואה בין הדגימה "החיה" למידע שנקרא מהתיעוד. **נתון זה חיוני לקביעת רמת הסמך של התוצאות מהניסוי ובפרט של נתוני ה-FRR.**

נתון זה ייאסף בפילוח לטביעות אצבע ותמונות פנים. חשוב לחדד שבלשכות הרשות כלל לא תבוצע השוואה של תמונות פנים אלא רק של טביעות אצבע. גורמים אחרים (כגון ביקורת הגבולות) יבצעו השוואות ביומטריות של תמונת פנים ככל שיהיו ערוכים לכך וככל שמותר להם לבצע זאת על פי החקיקה.

הערה: ההשוואות בלשכות הן כולן בתצורה של one to one ולמעשה ניתן לדעת מהן אך ורק נתון של false reject. קבלת נתונים של false accept מחייבת השוואה צולבת בין טביעת אצבע של <u>מישהו אחר</u> לנתונים שנקראו מהתיעוד. אין טעם בהשוואה עם טביעה אקראית בודדת ובכל מקרה יש הנחייה מפורשת בחוק המחייבת מחיקה מידית של הדגימה החיה ושל הנתונים שנקראו מהתיעוד, כך שלא ניתן לשמור טביעות אצבע אחרות לצורך השוואה כזו, <u>למעט במאגר</u>.

כמות זו כוללת באופן טבעי את כל מי שהזמין תעודת זהות חכמה ובא שנית לקבל אותה, יחד עם אותם מקבלי שירות שכבר יש ברשותם תעודה חכמה. לא ניתן לנקוב כאן נתון מספרי שייחשב

[56] ראה דו"ח של פרויקט ה-UIDAI בהודו בשם "*uid_enrolment_poc_report*" המפרט מדיניות דומה בנושא זה.

כהצלחה עקב התלות המובהקת במספר המתנדבים לתקופת המבחן. למעשה יש סבירות גבוהה מאד שמספר זה **<u>יהיה קטן יותר ממספר משתתפי תקופת המבחן</u>**, עקב מקרים של הנפקת תיעוד שלא נמסרו לאזרח ומקרים בהם ביקש האזרח רק דרכון וזה נשלח אליו באמצעות הדואר, ללא הגעה שנייה ללשכה.

גופים נוספים (ובפרט המשטרה) שיקימו תשתית מתאימה יבצעו אף הם השוואות מסוג זה ויידרשו לאסוף את אותם נתונים, תחת אותה מעטפת אבטחת מידע.

14.2.2. כמות ההשוואות המוצלחות

השוואה מוצלחת היא השוואה שציון המעבר שלה היה מעל לציון הסף שהוגדר למערכת. נתון זה מהווה הצלבה לנתוני ה-false rejection אך צפוי להיות מעט יותר גבוה בגלל מצבים שבהם ניתן היה לבצע הרכשה אך לא אימות במועד מאוחר יותר (למשל בגלל פציעה). לאחר עקומת הלמידה אנו מצפים שנתון זה יהיה כמפורט בסעיף 14.3.1 להלן.

14.2.3. כמות החריגים (השוואה שנכשלה)

השוואה שנכשלה יכולה לנבוע מחוסר יכולת לקבל ט"א מהדגימה החיה, מחוסר יכולת לקרוא את התיעוד או מחוסר התאמה מספקת בין האדם לנתון השמור בתיעוד. גם נתון זה מהווה הצלבה לנתוני ה-false rejection כמפורט בסעיף 14.3.1 להלן.

14.2.4. איך טופלו החריגים

נתון זה איננו נתון מספרי אך יפולח בהתאם לצורת הטיפול בחריגים (סריקת תמונה מודפסת, סיוע של מלווה/אפוטרופוס, מענה באמצעות נוהל או צורך בנוהל שאיננו קיים).

14.2.5. מספר הניסיונות הדרושים עד לזיהוי

כאמור ניתן בתקופת המבחן לבצע עד שישה ניסיונות נטילה טרם המעבר לנוהל חריגים. אם ניתן יהיה ליטול נתונים ביומטריים מיותר מ-90% מהאוכלוסייה תוך שלושה ניסיונות לכל היותר ייחשב הדבר להצלחה.

14.2.6. ציון השוואה תקינה: התפלגות

בלשכות הרשות תבוצע רק השוואה של טביעות אצבע ולא של תמונות פנים. מכיוון שציון הסף יעודכן מעת לעת בהתאם לתובנות מהניסוי, לא ניתן לציין מדדים מספריים שיוגדרו כהצלחה. הצלחה כאן תוגדר כיכולת לכייל סף החלטה שייתן ביצועים ביומטריים כמפורט בסעיף 14.3.1 להלן.

14.2.7. ציון דחייה: התפלגות

כנ"ל.

14.2.8. משך הזמן שתהליך ההשוואה ארך

זמן זה כולל קריאה של מידע ביומטרי מהכרטיס, תעבורת רשת מקומית הדרושה לקבלת הרשאת קריאה, תעבורת רשת רחבה לצורך פנייה ל-HSM[57] מרכזי של מערכת "אביב", נטילת דגימה חיה מהאזרח וביצוע ההשוואה. הצפי הוא שתהליך זה יימשך לכל היותר דקה אחת עבור אוכלוסיות ללא צרכים מיוחדים.

14.3. נתונים הנוגעים לפעילות במאגר

מערך התיעוד הלאומי מורכב משני מערכי מחשוב בלתי תלויים, שאינם מקושרים אחד לשני באופן קבוע בקישור מקוון, ולכן יש צורך לאסוף נתונים במקביל בשניהם. הנתונים שלהלן ייאספו **במאגר**, חלקם כהצלבה לנתונים הנאספים בלשכות וחלקם כנתונים העומדים בפני עצמם:

14.3.1. ביצועי הטכנולוגיה הביומטרית

בדיקת הביצועים של המערכת הביומטרית עצמה הינה אחד הנתונים הכי משמעותיים ותתבצע בעיקר בעת העבודה במתכונת של many to many[58] במאגר, כדי להבטיח כמות השוואות גדולה ככל האפשר, ממנה ניתן לגזור תוצאות רלבנטיות לאיתור הרכשה כפולה ברמת סמך גבוהה[59]. מדיניות דומה ננקטה בפרויקטים אחרים בעולם וכך ניתן לקבל מושג על ביצועי הטכנולוגיה הביומטרית בצורה הטובה ביותר. על פי הגדרות החוק והתקנות המאגר הינו המקום **היחיד** בו ניתן לשמור מידע ביומטרי לאורך זמן ואף לשמור מספר מופעים של אותו אדם. מסיבה זו לצורך זה תוגדר קבוצה נבחרת (של 100 איש) שתבצע לכל הפחות חמש הרכשות חוזרות אחת לפרק זמן קצוב. הנתונים של קבוצה זו ישמשו לקביעת עקומת ה-ROC של המערכת הנבדקת.

מדידה זו של ביצועי המערכת הביומטרית תשמש לצורך קביעת סיפי ההחלטה ביתר המקומות שבהן מבוצעת השוואה ביומטרית. באותם מקומות ייבחר סף החלטה ומסף זה נגזר שיעור השגיאות, הן עבור דחייה מוטעית והן עבור קבלה מוטעית.

14.3.1.1. ביצועי 1:1

כאמור ייבחנו נתונים אלו רק במאגר בגלל מגבלות החוק. בטביעות האצבע, עבור אוכלוסייה שניתן ליטול ממנה טביעות אצבע, הצפי לביצועים שייחשבו כהצלחה הוא קצב שגיאות מסוג FA[60] של 1:10000 (0.01%) עבור FR[61] של 1:100 (1%), לטביעת אצבע בודדת במצב של 1:1

---

[57] **H**ardware **S**ecurity **M**odule = **HSM**, מצפין הממומש באמצעות חומרה ייעודית מוגנת.

[58] הכוונה ב-many to many היא לחיפוש זהויות כפולות.

[59] ראה בנוסף הערה בסעיף 14.2.1 והסבר ממצה על נקיטת מדיניות דומה בפרויקט הביומטרי של הודו (ה-UIDAI) במסמך בשם "***uid_enrolment_poc_report***" הזמין באתר הפרויקט הנ"ל.

[60] **F**alse **A**cceptance = **FA**, כלומר אישור של מתחזה

וללא sequence error[62]. עבור זיהוי הפנים הצפי לביצועים שייחשבו כהצלחה במצב של 1:1 הוא קצב שגיאות מסוג FA של 1:1000 עבור FR של 1:50 ואימות של קצב שגיאות זה ייחשב להצלחה. יודגש שנית שהכוונה היא לקצבי שגיאות של זיהוי חיובי בלבד.

תהליכי השוואה מסוג 1:1 של טביעות אצבע יבוצעו בפועל בלשכות רשות האוכלוסין (ראה סעיף 6.2 לעיל). בעמדות ביקורת גבולות יבוצעו תהליכי השוואה הן של טביעת אצבע והן זיהוי פנים (ראה סעיפים 6.3 ו-5.4 לעיל). כאמור, בלשכות רשות האוכלוסין לא יתבצע זיהוי פנים כלל וזיהוי טביעות אצבע יבוצע רק עבור אותם אזרחים שיגיעו לקבל שירות לאחר שכבר יש בידם תעודת זהות חדשה או לצורך קבלתה (בהגעתם השנייה ללשכה). מספרם של אירועים אלו אינו צפוי להיות גדול דיו והוא יגדל בצורה משמעותית רק לאחר שתהיינה תובנות מתקופת הניסוי ופריסה רחבה מאד של ציוד בדיקה במקומות רבים, ואף (ואולי בעיקר) במקומות מחוץ ללשכות רשות האוכלוסין[63]. בתרחיש של אימות זהות בלשכות (בניגוד לתרחיש הזיהוי במאגר), כלל לא ניתן לבדוק FA[64] בגלל חוסר האפשרות לאגור את טביעות האצבע במחשבי הלשכות של רשות האוכלוסין (ראה גם הסבר בסעיף 10.2.1 לעיל). הבדיקה במצב זה תתמקד בדחייה מוטעית (FR) כאימות לבדיקה במאגר. בלשכות אנו מצפים לקצב שגיאות מעט יותר גבוה מהקצב שייבדק במאגר. אם קצב השגיאות מסוג FR בלשכות יהיה נמוך מ-3% ייחשב הדבר להצלחה[65]. קצב שגיאות זה יהיה גבוה יותר בתחילת הדרך וילך וישתפר במעלה עקומת הלמידה. היעד הוא כאמור קצב שגיאות סופי נמוך מ-3%.

קצב השגיאות המתואר לעיל עבור זיהוי פנים בעמדות ביקורת הגבולות נובע מהייחודיות של תרחיש זה (עמדה לא מאויישת, ללא סיוע פקיד, תנאי סביבה קשים ומשתנים, פער איכות ניכר בין תמונת ה-gallery ותמונת ה-probe). במציאות הוא אף יהיה גבוה יותר מזה שיימדד במאגר בגלל איכות הדגימה שצפויה להיות נמוכה באופן משמעותי מאיכות ההרכשה. במקומות אלו יהיה צורך לבחור סף החלטה מתאים כדי ליצור את האיזון התפעולי הדרוש.

---

[61] FR = **F**alse **R**ejection, כלומר דחייה של מורשה

[62] השוואה לאצבע שונה מזו שנדגמה במעמד הרישום.

[63] ראה הסבר נוסף בסעיף 10.2 לעיל.

[64] למעט הדמיות מוגבלות ביותר, שלא תוכלנה לספק תוצאה עם רמת סמך טובה דיה.

[65] עבור כלל התהליך, באמצעות אצבע בודדת ותוך מגבלה של שלושה ניסיונות לכל היותר.

- בלמ"ס -

14.3.1.2.ביצועי איתור הרכשה כפולה

בחינת הביצועים במקרה זה מורכבת יותר ובפרט הגדרת המדדים, בעיקר בשל העובדה שגודל האוכלוסייה איננו ידוע מראש. בהעדר כמות ידועה של רשומות יוגדרו מדדי ההצלחה של תרחיש זה על פי אחוז התראות השווא על הרכשה כפולה ועל פי אחוז ההרכשות הכפולות שלא תתגלינה מתוך המנה היומית של רשומות שתועברנה לבדיקה. לסף ההחלטה יש השפעה ניכרת על ביצועים אלו ולכן יתבצע תהליך טיוב תקופתי שהיעד שלו הוא הבאת המערכת לביצועים המתוארים להלן.

יש להבחין בנוסף בין שני מצבי משנה (ראה הסבר מפורט בסעיף 3.13 לעיל):

14.3.1.2.1.הרכשה ראשונה

עבור מי שאיננו רשום במאגר, בעת השוואת הרכשה מלאה להרכשות מלאות, אחוז התראות השווא נדרש להיות עד 1% מכמות הרשומות היומיות. אחוז ההרכשות הכפולות שלא תתגלינה (בבדיקה על ידי הדמיה) נדרש להיות עד 1%.

14.3.1.2.2.הרכשה חוזרת

עבור מי שכבר רשום במאגר וזו לו הרכשה חוזרת, בעת השוואת הרכשה מלאה להרכשות מלאות, אחוז התראות השווא נדרש להיות עד 0.5% מכמות הרשומות היומיות שתועברנה לבדיקה. אחוז ההרכשות הכפולות שלא תתגלינה (בבדיקה על ידי הדמיה) נדרש להיות עד 1%.

כאמור, בדיקה זו תבוצע <u>**במאגר**</u>, הן עבור טביעות האצבע והן עבור זיהוי הפנים.

14.3.2. מספר הפניות הכולל למאגר

בתקופת המבחן מספר זה צריך להיות זהה למספר ההרכשות כי לגורמים אחרים אין גישה למאגר במשך תקופת המבחן, למעט אירועי הדמיה (סימולציה) שיבוצעו בתקופה זו. מסיבה זו יש צורך להבחין בין אירועי הדמיה ופניות שוטפות.

14.3.3. מספר אירועי ההדמיה של פניות מהמשטרה

נתון זה יכלול את מספר הפעמים שבהם בוצעה הדמיה (סימולציה) של פניית גורם חיצוני (ובפרט המשטרה) למאגר, על פי אותם מקרים שהותרו בחקיקה. לאחר סיכום תצורה מתאימה מול גורמי המשטרה ואכיפת דרישות אבטחה מחמירות, יבוצעו סימולציות להעברת בקשות ועיבוד נתונים ותשובות בין מוקד מוגדר במשטרה למאגר.

14.3.4. אירועי הדמיית הרכשה כפולה או התחזות

בנוסף במהלך תקופת המבחן יבוצעו ניסיונות התחזות בזהות כפולה תוך תיאום עם כלל הגורמים המעורבים בתהליך ותוך הקפדה על כך שלא תהיינה זהויות כפולות במרשם עצמו, על מנת לבחון את יכולות המערכת הטכנולוגית והטיפול האנושי יחד. ניסיונות אלה יבוצעו על ידי עובדי המשרד אשר נתוניהם נמצאים כבר במערכת הבדיקות (ולא במרשם האמיתי). תדירות אירועי ההדמיה בתרחיש הנ"ל תהיה לכל הפחות עשרה אירועים לחודש. תוצאת הניסוי תחשב להצלחה במידה ויזוהו 95% מכלל אירועי ההתחזות בזהות כפולה על ידי המערכת ומפעילי המאגר. כאמור, בניגוד לביצועי המערכת הביומטרית הטכנולוגית לבדה, משקף נתון זה גם את מקצועיות העובדים ואיכות תהליכי העבודה והוא צפוי להשתפר במשך הזמן בעקבות עדכון סיפי החלטה ותהליכי טיוב.

תהליך עבודה מפורט המתאר את תצורת ביצוע ההדמיות מופיע במסמך נפרד בשם "תהליך עבודה לביצוע הדמיות הרכשה כפולה במהלך תקופת הניסוי"[66].

14.3.5. כמה הרכשות בוצעו לכל זהות

ראה פירוט והסבר בסעיף 14.1.4.5 לעיל.

14.3.6. עבור איזה מסמך זיהוי או שירות בוצעה ההרכשה

האם ההרכשה בוצעה עבור תעודת זהות, עבור דרכון או עבור שניהם (הצלבה עם נתוני רשות האוכלוסין).

14.3.7. כמות התראות השווא

התראת שווא על הרכשה כפולה הינה מצב שבו מי שאיננו נמצא במאגר זוהה ככזה בטעות או זוהה כמישהו אחר אך זוכה לאחר בדיקה ידנית. גם כאן מדובר בנתון כולל ולא רק בנתון המתייחס למערכת הטכנולוגית. יש קושי גדול להגדיר נתון זה מראש באופן מספרי עקב חוסר הוודאות לגבי מספר הרשומות וגם להגדיר מה ייחשב להצלחה, אך השאיפה היא שנתון זה יהיה נמוך ככל האפשר. למעשה נרצה שנתון זה יכלול אך ורק את הניסיונות המלאכותיים לייצר אירועי הרכשה כפולה (ראה הסבר בסעיף 10.1 לעיל). המדד להצלחה במקרה זה יעמוד על כמות כוללת של עד 1% ממספר הפניות למאגר בעקבות הרכשה (ראה גם פירוט נוסף בסעיף 14.3.1.2 לעיל).

14.3.8. כמות הרכשות כפולות בפועל

נתון זה כולל את המקרים שזוהו במאגר בוודאות כניסיון אמת של הרכשה כפולה. יש קושי גדול להגדיר נתון זה מראש באופן מספרי וגם להגדיר מה ייחשב להצלחה, בגלל הקושי האובייקטיבי לכמת את גורם ההרתעה של המאגר והנחת היסוד שפושע המעוניין לבצע הרכשה כפולה פשוט לא

[66] מסמך זה הינו מסמך חסוי בגלל הפירוט הרב של תהליכי עבודה פנימיים במאגר הביומטרי, הכוללים פרטים רגישים מבחינת אבטחת מידע.

יתנדב לתקופת המבחן. לפיכך, פרט להדמיות ולמקרים קשים במיוחד, צפוי שנתון זה יהיה נמוך מאד ואפילו אפסי.

הערה: במקרה מתועד בקנייה הופעלה מערכת לאיתור הרכשות כפולות על אוכלוסיית משתתפים בבחירות שגודלה היה כ-1.5 מיליון איש. התגלו יותר מ-1.5% של הרכשות כפולות, למרות שכל משתתפי התהליך ידעו שיבוצע חיפוש כזה, כך שנתון זה מייצג רק את אותם אלו שניסו את מזלם <u>למרות</u> המערכת ולא את המספר האמיתי שהיה מתרחש ללא המערכת. במקרה מתועד אחר, במדינה אחרת, התגלו 20% של הרכשות כפולות.

14.3.9. כמות הרכשות כפולות מדומות

בניגוד לנתון המתואר בסעיף 14.3.7 לעיל, נתון זה כולל את המקרים שזוהו לאחר טיפול כניסיון הרכשה כפולה למרות שלא היו כאלה. גם כאן יש קושי גדול להגדיר נתון זה מראש באופן מספרי וגם להגדיר מה ייחשב להצלחה, אך השאיפה היא שנתון זה יהיה נמוך ככל האפשר. למעשה נרצה שנתון זה יכלול אך ורק מספר קטן ככל האפשר של אירועים מתוך הניסיונות המלאכותיים לייצר אירועי הרכשה כפולה (ראה גם הסבר בסעיף 10.1 ובסעיף 14.3.1.2).

14.3.10. זמני תגובה

TBD - יושלם בהמשך, לאחר טיוב זמני התגובה כאשר המערכת תופעל בצורה מלאה.

14.3.11. אירועי אבטחת מידע במאגר

אבטחת מידע מרבית ומיטבית היא אחד היעדים החשובים ביותר של הרשות לניהול המאגר הביומטרי. במהלך תקופת הפיילוט ייבחנו אירועי אבטחת מידע ויסווגו לשלוש קבוצות על פי חומרתם:

14.3.11.1. אירועים חמורים

אירועים אלו הם אירועים שיש בהם חשש לשימוש לרעה במאגר או לדלף מכוון לצרכי שימוש לרעה של מידע ביומטרי גלוי בהיקף של רשומה אחת או יותר, על פי איום הייחוס. אירוע יחיד כזה, שייקבע לגביו על ידי הרשות הממלכתית לאבטחת מידע כי בעטיו נגרם נזק חמור ומתמשך לביטחון המדינה ייחשב כישלון.

14.3.11.2. אירועים בדרגת חומרה בינונית

כל אירוע אבטחת מידע שלא נבע משימוש לרעה או שגרם לחשיפת מידע של מספר רשומות נמוך מהסף שיוגדר באיום הייחוס שייקבע או שחרג מנהלי האבטחה במאגר. צבר של עשרה אירועים כאלו ייחשב לכישלון.

14.3.11.3. אירועים בדרגת חומרה נמוכה

אירועים שלא נבעו משימוש לרעה, לא גרמו לחשיפה של מידע ביומטרי גלוי כלשהו ולא חייבו טיפול מלבד חידוד הוראות או עדכון נהלים. לאירועים מסוג זה לא נקבעה תקרה מספרית ורק נדרש לתעד אותם.

14.3.12. אירועי עצירת הנפקה

נתון זה יגדיר באיזה שלב משלבי תהליך ההנפקה הייתה עצירה של ההנפקה בגלל הרכשה כפולה. המדד להצלחה עבור נתון זה הוא עצירה של יותר מ-90% מההרכשות הכפולות עוד בטרם הונפקו מסמכי הזיהוי בפועל, כך שלא נוצר בזבוז של חומר גלם יקר (ספרונים ריקים לדרכון או כרטיסים ריקים לתעודת הזהות). שולי הביטחון (של 10% מההרכשות הכפולות) נובעים ממצבי תקלה וחוסר זמינות של המאגר. בכל מקרה משמעות הכישלון היא בדרך כלל רק בזבוז חומרי גלם (למעט אם התיעוד נמסר בפועל למבקש וגם אז ניתן עדיין לטפל במצבים אלו).

14.3.13. כמות הוראות עצירה שהועברו לאתרי ההנפקה

נתון זה כולל את המקרים שבהם הועברה הוראת עצירה למערכי ההנפקה, מפולחים על פי דרכון ותעודת זהות. יש גם כאן קושי גדול להגדיר נתון זה מראש באופן מספרי וגם להגדיר מה ייחשב להצלחה, בגלל הקושי האובייקטיבי לכמת את גורם ההרתעה של המאגר ויכולת הבחירה של פושעים לא להתנדב בתקופת המבחן.

14.3.14. הסיבות לעצירה

כל אירוע של עצירת הנפקה ינותח ויבוצע רישום של סיבת העצירה.

14.3.15. כמה הנפקות היו צריכות להיעצר ולא נעצרו

נתון זה יכלול את המקרים שהתגלו כהרכשה כפולה בדיעבד (למשל בחקירה משטרתית), ולא זוהו ככאלה על ידי המאגר או שזוהו לאחר שהתיעוד כבר נמסר.

14.3.16. מדידת מקצועיות עובדים

בתקופת המבחן תבחן מקצועיותם של עובדי המאגר בכל הנוגע להשוואות ביומטריות, אימות וזיהוי, בעיקר בתרחישי התראה על הרכשה כפולה על ידי המערכת. במקרים אלה, לאחר קבלת רשומות זהות במסגרת הדמיה על העובדים יהיה לקבוע באופן סופי האם אכן מדובר בהרכשה כפולה או שמדובר בשגיאה של המערכת. הבחינה תספק מענה לגבי יכולתם של העובדים בתחום וכפועל יוצא,

הצורך בהיקף הכשרות העובדים או בהסתייעות במומחים חיצוניים או גורמי מז"פ. מבחינת מדידת הביצועים, תידרש הלימה לתוצאות מבחני ההדמיה בהם נדרש להגיע לאיתור של 95% מאירועי ההדמיה (נתון שישתפר לאחר עדכון סיפי החלטה, שיפור תהליכי עבודה ותהליכי טיוב). במסגרת בחינה זו יש לבדוק כמה אירועי החשדה לא טופלו בצורה עצמאית, לאילו תחומי ידע נזקקו עובדי המאגר ומה היה פרק הזמן שנדרש לאירועים כאלו.

מעבר לנתונים הנ"ל ייאספו הנתונים הבאים ברשות לניהול המאגר הביומטרי באמצעות רישומם ב-log של המערכת, כדי לאפשר קבלת הנתונים שלעיל וכדי לאפשר לרשות לספק את הדיווחים שהוגדרו בחקיקה:

14.3.17. דיווחים ממוכנים בנוגע לתפעולו השוטף של המאגר

נתונים אלו נחוצים כאמור עבור הדיווחים המוגדרים ע"י המחוקק וכן נדרשים לצורך ניהול שוטף של המאגר. הם יופקו מקובצי היומן (log) של המערכת ויאורגנו בממשק נפרד, בשלב ראשוני ככל האפשר, על מנת לאפשר גישה נוחה ומהירה אליהם. חלק מנתונים אלו נחשב רגיש ולכן איסופם במאגר יבוצע לצורך מתן דין וחשבון אך ללא חשיפתם או הוצאתם מהרשת הפנימית של המאגר.

14.3.17.1. נתונים הנוגעים למנות הנפקה

כל מנה של הרכשות מוגדרת באמצעות מספר חד ערכי המזהה את המנה המגיעה ממערכת "אביב" וניתן אוטומטית. מנה כזו מכילה מספר רב של קובצי XML המכילים את נתוני ההרכשה. בנוסף למספר המזהה תאופיין כל מנה על ידי:

14.3.17.1.1 מועד הגעה ממערכת "אביב"

הזמן, באבחנה של דקות, שבו הגיעה המנה ממערכת "אביב". מקורו של נתון זה במערכת "אביב" והוא יוזן ידנית למערכת הפנימית.

14.3.17.1.2 מועד תחילת טיפול

זמן תחילת הטיפול במאגר באבחנה של שניות – תחילת הרצה של המנה במערכת.

14.3.17.1.3 מועד תום הטיפול

זמן תום הטיפול במנה, באבחנה של שניות – סוף זמן ההרצה האוטומטית של מנה במערכת.

14.3.17.1.4 כמות קובצי XML

כמות הבקשות (קבצי XML) במנה.

14.3.17.1.5. שלמות פרטי מידע ב-XML

קובץ XML סטנדרטי אמור לכלול שלושה פרטי זיהוי - שתי אצבעות ופנים, אך יתכן מצב בו אחד מפריטים אלו יהיה חסר.

14.3.17.1.6. סה"כ בקשות במאגר.

14.3.17.1.7. סה"כ פריטי זיהוי במאגר

14.3.17.1.8. כיול המערכת

הסף של המערכת הביומטרית שעל פיו טופלה המנה.

14.3.17.2. נתוני המאפיינים זהות

כל זהות (אדם) במערכת תאופיין על ידי הנתונים הבאים:

14.3.17.2.1. מספר מזהה פנימי

מספר חד ערכי (שאיננו מספר זהות מהמרשם) המזהה את המבקש.

14.3.17.2.2. דגל חידוש תעודה או הרכשה ראשונה

חיווי האם אותו אדם מבקש פעם ראשונה את התיעוד או מחדש את תיעוד קיים.

14.3.17.2.3. גיל

חיווי האם הבקשה היא של אדם מעל או מתחת לגיל 12.

14.3.17.2.4. זמן תחילת העיבוד

זמן תחילת הטיפול בבקשה (קובץ XML) באבחנה של שניות, שיתקבל באופן אוטומטי או ידני.

14.3.17.2.5. זמן סיום טיפול בבקשה

זמן הכנסת הנתונים למאגר.

14.3.17.2.6. מספר עובד המבצע זיהוי ביומטרי

נתון מזהה של העובד שביצע את הזיהוי הביומטרי במקרה שהבקשה עברה לטיפול ידני.

14.3.17.2.7. מספר עובד הקובע זיהוי ביומטרי

נתון מזהה של העובד הקובע את זיהוי הביומטרי במקרה והבקשה עברה לטיפול ידני. יתכן שקביעה זו תבוצע על ידי מישהו שונה מזה שביצע את הזיהוי.

14.3.17.2.8. אופי הטיפול

חיווי האם הבקשה טופלה באופן אוטומטי או ידני.

14.3.17.3. נתונים של פריט זיהוי (פנים או אצבע)

כל פריט זיהוי (תמונת פנים, טביעת אצבע) תאופיין על יד הנתונים הבאים:

14.3.17.3.1. מספר אצבע

חיווי המציין איזו אצבע נדגמה. צפוי כי הרוב המוחלט יגדיר את האצבע המורה, אך יכולים להיות מקרים בהם ייעשה שימוש באצבע אחרת.

14.3.17.3.2. התאמה לרשומות במאגר

האם יש התאמה לזהות אחרת.

14.3.17.3.3. מספר מזהה פנימי מולו יש התאמה

מספר המזהה זהות אחרת במאגר מלבד המבקש.

14.3.17.3.4. מידת התאמה

ציון המדרג התאמה עם תמונה קיימת.

14.3.17.3.5. כמות זהויות דומות

מספר זהויות אותן המערכת מזהה כדומה למבקש.

14.3.17.3.6. חיווי לתמונה סרוקה

חיווי המתקבל כאשר תמונת הפנים סרוקה מתמונה מודפסת.

14.4. נתוני הנפקת תיעוד

נתונים אלו ייאספו במערכי ההנפקה של תעודת הזהות והדרכון, כהצלבה לנתונים הנאספים בחלקים אחרים של מערך התיעוד, יחד עם נתוני הנפקה של התיעוד הישן:

14.4.1. כמות הנפקות של תיעוד ישן

נתון זה (ופילוחו על ידי הלמ"ס באמצעות נתוני מפקד האוכלוסין) יאפשר לבדוק את המתאם בין האוכלוסייה שהתנדבה לתקופת המבחן והאוכלוסייה שלא התנדבה, לצורך מיקוד מאמצי ההסברה ולצורך קביעת הצלחה או כישלון של התהליך כולו.

14.4.2. כמות ההנפקות שנעצרו

יש צורך לאסוף נתון זה גם במערך ההנפקה, שהינו מערך מחשוב בלתי תלוי ביתר חלקי המערכת.

14.5. נתונים כלליים

נתונים אלו מיועדים לתכנון תהליכי העבודה בלשכות רשות האוכלוסין וכהשלמה לנתונים הנאספים ביתר חלקי מערך התיעוד. חלקם ייאסף אצל גורמים חיצוניים:

14.5.1. צורך בתחזוקה שוטפת

פעולות תחזוקה נדרשות כגון ניקוי המשטח של חיישן טביעות האצבע, עדשת המצלמה או משטח החתימה (הן משיקולי השפעה על ביצועים והן משיקולי היגיינה).

14.5.2. עבירות זיוף תיעוד שהתגלו במשטרה

נתון זה יכלול את כמות עבירות הזיוף של תיעוד לאומי ישראלי שטופלו או התגלו על ידי המשטרה. כיום המשטרה אוספת מידע סטטיסטי על עבירות שטופלו על ידה אך הן מתויגות בדרך כלל על פי אופי העבירה הראשית, גם אם זיוף תיעוד היה חלק מהעבירה. יש צורך בהיערכות מיוחדת לצורך זה ובהנחיה של גורמי הרישום במשטרה.

14.5.3. עבירות זיוף תיעוד שהתגלו ברשות האוכלוסין

נתון זה יכלול את כמות עבירות הזיוף של תיעוד לאומי ישראלי שהתגלו ברשות האוכלוסין או ביקורת הגבולות.

14.5.4. כמות התיעוד שנפגם

נתון זה כולל את תעודות הזהות והדרכונים שנפגמו לאחר שנמסרו עקב שימוש לא נאות, בפילוח לפגמים חזותיים ופגמים אלקטרוניים. אין לנתון זה נגיעה ישירה לניסוי הביומטרי והוא נועד לתת מושג על אותם מקרים שבהם לא ניתן היה לבצע השוואה של אדם מול תיעודו בגלל חוסר היכולת לקרוא מידע מהתיעוד. מתוך נתון זה ניתן לגזור את יכולת המערכת כולה לספק תיעוד תקין מבחינה טכנולוגית, ללא קשר לביומטריה. יש לתעד את סיבת הפגם ומשך הזמן מהנפקת התיעוד.

14.5.5. כמות התיעוד שנפגם למרות שהשימוש בו היה נאות

כנ"ל.

14.5.6. כמות הזיהויים שבוצעו על פי תמונה מופחתת

נתון זה נועד לבחון את יעילות השימוש בתמונה המופחתת שתישמר במערכת "אביב". למעשה נשאף לכך שזיהוי כזה יבוצע בכל מפגש עם אזרח שעבר תהליך הרכשה, ללא תלות בהשוואה של טביעת האצבע. זיהוי זה לא יבוצע בצורה ממוכנת אלא בצורה חזותית בלבד ויבוצע תיעוד פרטני יותר במקרים של חוסר התאמה לכאורה.

14.5.7. כמות אזעקות השווא כתוצאה מהשימוש בתמונות המופחתות

נתון זה נועד גם הוא לבחון את יעילות התמונות המופחתות, המשמשות להשוואה חזותית אצל הפקיד בלשכה. הצלחה תוגדר כפחות מ-5% של התראות שווא. לצורך זה, מקרים בהם התעורר חשד אך חשד זה הופרך יתועדו אך לא ייספרו ככישלון.

14.5.8. כמות האימותים התקינים בתהליך אימות באמצעות תשאול

נתון זה נועד לבחון את יעילות תהליך התשאול. אין לו השלכה על הנושא הביומטרי אולם תהליך זה הוא חלק בלתי נפרד מאימות הזהות הראשוני. נתון זה יכלול את אותם מקרים שבהם הושלם התהליך בשלב הראשון, אצל הפקיד. בשלב זה התשובות לשאלות האקראיות אינן חשופות לפקיד והוא רק יקבל חיווי על כישלון או הצלחה (ראה תיאור ותרשים בסעיף 11.1 לעיל).

14.5.9. שאלות התשאול

נתון זה יכלול פילוח של השאלות על פי מידת ההצלחה של הנשאלים לענות עליהן, כדי לאפשר ניתוח וטיוב של תהליך התשאול. יש לכלול בנתון זה בעיקר את אופי התשובות שאינן תואמות למצופה והאם ניתנה תשובה שגויה או תשובה שאושרה בבדיקת מנהל. הפילוח יבוצע ללא פרטים מזהים.

14.5.10. כמות הכישלונות בתהליך אימות באמצעות תשאול

נתון זה יכלול את כמות המקרים בהם התשאול בשלב הראשון לא הביא לאימות חיובי. במקרים אלו יימשך התשאול אצל פקיד ב-"קו שני", כאשר התשובות לשאלות התשאול חשופות בפניו.

14.5.11. כמות האימותים שהצליחו בשלב שני

נתון זה יכלול את כמות התשאולים שבוצעו ע"י פקיד ב"קו שני" והביאו לכך שהאימות יהיה חיובי.

14.5.12. כמות הכישלונות גם לאחר שלב שני

נתון זה יכלול את כמות התשאולים שבוצעו ע"י פקיד ב"קו שני" והביאו לכך שהאימות יהיה שלילי. נתון זה יצביע על כמות המקרים שבהם לא הונפק מסמך זיהוי רק על סמך תשאול ויש לפלח אותו על פי חלוקה לאלו שביקשו תיעוד מהסוג הישן ואלו שביקשו תיעוד מהסוג החדש.

14.5.13. כמות המקרים שחייבו שימוש במסמכי זיהוי נוספים

נתון זה יכלול את כמות וסוג המקרים שבהם אומתה זהותו של מקבל השירות באמצעות מסמכי זיהוי אחרים (“breeder documents”) שנדרש להביא או שהיו ברשותו.

14.5.14. כמה קיבלו פטור מאימות באמצעות תשאול

נתון זה יכלול את כמות המקרים בהם ניתן פטור מהתהליך בהתאם לתקנות ולצו תוך פירוט הסיבה המדויקת לכך (מתוך מכלול הסיבות שמפורטות בתקנות).

14.6. נתונים הנוגעים לביקורת הגבולות

נתונים אלו ייאספו במערך ביקורת הגבולות המופעל על ידי רשות האוכלוסין כדי שיאפשרו לבחון ולנתח את הנושאים הבאים בהתאם לסעיף 8(2) של הצו:

14.6.1. מספר הנטילות עד לביצוע השוואה

היעד הוא עד שתי נטילות מכל סוג (תמונת פנים וטביעות אצבע).

- בלמ"ס -

14.6.2. משך הזמן הנדרש לביצוע הנטילה

היעד הוא עד שלוש שניות לצילום פנים ועד שלוש שניות לטביעת אצבע בודדת.

14.6.3. מספר ההשוואות שבוצעו בעמדות המעבר

היעד הוא השוואה אחת מכל סוג (תמונת פנים וטביעות אצבע).

14.6.4. משך הזמן הנדרש לביצוע ההשוואה

היעד הוא שניה אחת להשוואת תמונת פנים ושתי שניות להשוואת טביעת אצבע בודדת.

14.6.5. דיוק ההשוואה הביומטרית

היעד לזיהוי פנים הוא קבלה מוטעית אחת ל-10,000 עוברים ודחייה מוטעית אחת ל-500 עוברים.

עבור טביעת האצבע היעד הוא קבלה מוטעית אחת ל-100,000 עוברים ודחייה מוטעית אחת לאלף עוברים.

14.6.6. סיבות לכשלון בהשוואה

הסיבה שבגללה נכשלה ההשוואה, בהתאם לסוג ההשוואה וללא שמירה של מידע אישי.

15.בטיחות, גהות ונגישות

15.1. בטיחות וגהות

היבטי הבטיחות של תקופת המבחן נוגעים בעיקר לארגונומיה של עמדות ההרכשה. בדלפקי קבלת הקהל של הרשות מותקנת עמדת צילום הפנים בדופן השמאלית (כאשר המבט הוא מצד מקבל השירות) וחיישן טביעות האצבע (המזווד עם משטח החתימה) מונח על השולחן שבין הפקיד למקבל השירות.

אלמנט חשוב נוסף, בעיקר מבחינת בטיחות, הוא הכיסא עליו יושב המצולם. יש לוודא שכיסא זה יציב דיו עבור כלל האוכלוסייה.

מבחינת גהות לא תבוצע בדיקה יזומה כלשהי והטיפול בציוד ההרכשה יתמקד בניקוי מעת לעת ובתחזוקה מונעת, כאשר תדירות הניקוי תיקבע על פי החלטה שרירותית (לדוגמה בתחילת כל יום עבודה) או כאשר יתגלה קושי לקבל טביעות אצבע באיכות נאותה ("1" או "2" על פי מדד NIST, עבור יותר מ-90% מהאוכלוסייה).

15.2. נגישות

הנגישות של מערך ההרכשה (כמו גם של נקודות השוואה של מידע ביומטרי) הינה יעד חשוב, הנובע בעיקר מהחובה המוסרית לדאוג לאוכלוסיות עם צרכים מיוחדים. לשם כך יש להגדיר בכל לשכה לפחות עמדה אחת (קבועה או ניידת) שבה ניתן יהיה לבצע הרכשה של צילומי פנים כאשר המצולמים משתמשים בכיסא גלגלים[67] או בעלי מוגבלות אחרת.

הרכשה של טביעות אצבע לבעלי מוגבלויות גופניות תבוצע רק באותם מקרים שבהם מקבל השירות מסוגל להגיע בכוחות עצמו (או בעזרה מזערית) לחיישן המונח על השולחן. העזרה למקבל השירות תינתן לאחר קבלת הסכמתו המפורשת או באמצעות מלווה, לאחר הסבר של הפקיד על צורת השימוש בחיישן.

[67] ראה מכרז 28-2008 של רשות האוכלוסין, פרק 3.

- בלמ"ס -

16.אבטחת מידע במהלך הניסוי

באופן כללי פועלות כל מערכות המידע של רשות האוכלוסין תחת הנחיית רא"מ ורמת האבטחה של מערכות אלו גבוהה, ואף גבוהה יותר מהמקובל במשרדי ממשלה. מערך ההרכשה וכן מערך המחשוב של המאגר (שבאחריות הרשות לניהול המאגר הביומטרי) מונחים אף הם ע"י רא"מ ועומדים באותם תקנים של אבטחה (אם כי אבטחתם בפועל גבוהה יותר מהנדרש ע"י רא"מ).

תקופת המבחן תשמש בין היתר גם לבדיקה מקיפה של אבטחת המאגר והרכיבים הרלבנטיים במערכות המידע של רשות האוכלוסין (ובכלל זה מערכי ההנפקה וביקורת הגבולות). בדיקה זו תבוצע באופן המתואר להלן, תוך שימת דגש על הצדדים הטכנולוגיים של האבטחה. הנושאים הארגוניים והתפעוליים של אבטחת המידע ייבדקו אף הם אך במתכונת שונה, על פי נוהל מתאים של הרשות הממלכתית לאבטחת מידע[68]. התיאור המפורט של בדיקה זו איננו חלק ממסמך זה.

מערכות המידע של המאגר מנוהלות בשלוש סביבות עבודה עיקריות: סביבת ייצור (כולל קדם ייצור - staging), סביבת פיתוח ובדיקות, סביבת גיבוי והתאוששות מאסון. הבדיקה תתמקד בסביבת הייצור וסביבת הגיבוי.

סיקרי סיכונים ובדיקות חדירה יבוצעו בכדי להבטיח עמידת מערכות המידע של המאגר ומערכי ההנפקה בדרישות מדיניות אבטחת המידע של הארגון ושל מתודולוגיות אבטחת מידע המקובלות במשרדי ממשלה בארץ ובעולם ובהתייחס לקטגוריות הבאות: שיטות, יישומים, בסיסי נתונים ותקשורת. הסקרים יתייחסו למערכות השונות: מערכות בקרת גישה, הצפנה, הפעלה ומערכות גיבוי.

16.1. סקרי אבטחה

במשך תקופת המבחן יבוצע לכל הפחות סקר אחד בכל שנה, שיבחנן באופן פעיל את אבטחת המאגר ויתר המערכות, ומטרתו לבקר את רמת האבטחה על כל היבטיה ובפרט:

16.1.1. מדיניות אבטחת מידע

המדיניות ומערך נהלי אבטחת מידע אשר ייגזרו ממנה ומצרכי אבטחת המידע בארגון.

16.1.2. זיהוי משתמשים

זיהוי ייחודי ומערך הזדהות של המשתמשים.

16.1.3. מערך הרשאות

מי יכול לגשת למידע רגיש ותחת אילו מגבלות.

---

[68] נוהל זה הינו מסמך מסווג.

16.1.4. רמת ההקשחה וההצפנה
האבטחה של תשתיות המחשוב והתקשורת בדגש על הצפנת מידע רגיש.

16.1.5. קובצי יומן (log)
מערך רישום ותיעוד אירועים בקובצי יומן ובפרט יכולת למחוק עקבות של פעולות זדוניות.

16.1.6. ניטור ובקרה
מערך בקרה ואיתור של פריצות ואירועים חריגים.

16.1.7. עמידה בתקנים על פי סיווג
סיווג המערכות ומאגרי המידע, ניהול הרשת והפרדת סביבות.

16.1.8. מידור
מידור מערכות והפרדת סמכויות המשתמשים.

16.1.9. סמכות ארגונית
סמכויות ואחריות מנהלי אבטחת המידע.

16.1.10. מודעות
רמת המודעות של העובדים לנושא אבטחת המידע.

16.1.11. DRP - BCP
גיבוי מידע ותוכנית התאוששות ממשבר (היכן שנושא זה רלבנטי).

16.1.12. אבטחה פיזית
אבטחה פיזית וסביבתית, הערכת סיכונים והגנה מפני ניסיונות פגיעה ופריצה (סמויה וגלויה).

16.2. בדיקות חדירה (penetration tests)
בדיקה כזו תבוצע אך ורק באמצעות גורמים מוסמכים, בעלי סיווג מתאים המאפשר להם נגישות למאגר וליתר רכיבי המערכת שייבדקו, (ובפרט הרשות לאבטחת מידע - רא"מ).

הבדיקה תכלול ניסיונות חדירה בשני תרחישים:

16.2.1. מתכונת "Black box"
תרחיש זה מבוצע כאשר התוקפים אינם מכירים את פרטי המערכת ואת אבטחתה הפיזית והלוגית (כמקובל בעולם ה-hacking). מטבע הדברים זוהי בדיקה שאיננה בהכרח ממוקדת אך יתרונה הוא בכיסוי הרחב שלה.

16.2.2. מתכונת "White box"

תרחיש זה מדמה מצב של תוקף פנימי המכיר היטב את פרטי המערכת. הבדיקה תחולק לסקר תיאורטי ולסקר מעשי. ראשית יבוצע סקר תיאורטי של אבטחת המאגר במתכונת של "white box", כאשר כל מערך האבטחה חשוף לחלוטין לגורם המבצע את הסקר. בדיקה זו היא מאד ממוקדת אך מכסה תחום צר יותר של אפשרויות תקיפה ממודל ה-black box. לאחר מכן יבוצעו ניסיונות חדירה נוספים על בסיס הסקר הראשון, תוך דירוג התוצאות על פי הידע הנדרש לתוקף, עלות מימוש התקיפה, הנגישות הנדרשת, ציוד הדרוש למימוש ומשך הזמן הדרוש למימוש. במקרים מסוימים יש להבדיל בין זיהוי חולשה תיאורטית ובין שימוש בחולשה זו כדי לבצע תקיפה בפועל, הכול לפי המקרה.

16.3. דירוג תוצאות הסקרים

הדירוג של תוצאות בדיקות החדירה יבוצע בצורה הבאה, המתבססת על צורת הדירוג המקובלת בתקני האבטחה הבינלאומיים Common Criteria ומרחיבה אותו במקרים מסוימים:

16.3.1. משך הזמן הדרוש

מדד זה מציין כמה זמן נדרש למימוש התקיפה – שעות, ימים, שבועות, חודשים או שנים. לכל פרק זמן יוקצה ציון על פי הסולם הבא:

פרק הזמן	ציון
שעות	0
ימים	1
שבועות	4
חודשים	6
שנים	10

16.3.2. רמת המומחיות של התוקף

האם יכול תוקף שאיננו מומחה טכנולוגי (כגון "script kiddie" או עובד ממורמר) לממש את התקיפה, האם לא נדרשת הבנה מקצועית כלשהי, נדרש ידע מקצועי בסיסי, נדרשת מומחיות ניכרת או נדרש צוות של מומחים.

סולם הציונים יהיה:

רמת מומחיות	ציון
תוקף שאיננו מומחה	0
תוקף בעל ידע מקצועי	2
מומחה	6
צוות מומחים	10

16.3.3. מידת ההיכרות עם היעד

האם התקיפה יכולה להתבסס על מידע פומבי, האם נדרשת גישה למידע מסווג, האם נדרש איסוף מודיעיני אחר, האם נדרשת היכרות מלאה וכוללת עם פרטי המערכת או האם נדרשת התערבות פעילה בהקמתה.

הסולם יהיה:

מידת היכרות	ציון
שימוש במידע גלוי ופומבי	0
צורך בגישה למידע מסווג	3
צורך באיסוף מודיעיני ממושך	6
צורך בהיכרות מלאה עם פרטי המערכת	9
צורך בהתערבות משלב ההקמה	10

16.3.4. נגישות ליעד

בסעיף זה נבדק האם נדרשת נגישות פיזית ליעד או שניתן לבצע תקיפה מרחוק. במקרה זה יש להבדיל בין גילוי החולשה שיכול להיות קל מאד, ללא צורך בנגישות כלשהי (כגון פרסום פומבי של חולשה באחד מרכיבי התוכנה שבשימוש המאגר) לבין מימוש התקיפה בפועל.

אבטחת המאגר ומערכי ההנפקה מתבססת, בין היתר, על ניתוקם מכל תקשורת חיצונית, כך שכמעט כל תקיפה תחייב נגישות פיזית אליהם.

הסולם של סעיף זה יהיה:

רמת נגישות	ציון
יכולת תקיפה מרחוק דרך תשתית ציבורית (האינטרנט)	0
יכולת תקיפה מרחוק דרך תשתית פרטית(VPN מעל תשתית ציבורית)	3
קרבה פיזית (מחוץ למעטפת האבטחה)	8
נגישות פיזית מלאה	10

16.3.5. ציוד נדרש

בסעיף זה הדירוג הוא על פי הציוד הדרוש לצורך מימוש התקיפה, עלותו ומידת זמינותו. לדוגמה אם מפתחות הצפנה רגישים שמורים ברכיב חומרה ולצורך פריצה לרכיב זה יש צורך בציוד נדיר ויקר של מעבדת מיקרואלקטרוניקה או שניתן לממש תקיפה באמצעות ציוד זול וזמין. הסולם יהיה:

ציוד	ציון
שימוש בציוד זול וזמין הניתן לרכישה או בנייה עצמית	0
ציוד שעלותו אלפי דולרים אך זמין לכל	2
ציוד שעלותו עשרות אלפי דולרים וזמין רק למעבדות מתמחות	5
ציוד שעלותו מאות אלפי דולרים	7
ציוד שעלותו מיליוני דולרים וזמין למעבדות בודדות בעולם	10

16.3.6. הסיכון לתוקף

פרמטר זה, של סיכון לתוקף, איננו נמצא בשיטת הדירוג של תקני Common Criteria אך יש לציין אותו במסגרת הסקר כי הוא בעל חשיבות רבה. הסולם יהיה:

- בלמ"ס -

רמת סיכון	ציון
חוסר הסתכנות וחוסר אפשרות גילוי	0
אפשרות גילוי התוקף אך ללא יכולת לסכנו או להענישו	2
גילוי התוקף ואפשרות הפעלת הענישה הכתובה בחקיקה	10

על פי שיטת דירוג זו הציון המרבי הוא 60. אם סיכום הציונים יהיה 35 או יותר ייחשב הדבר לרמת אבטחה גבוהה ונאותה. כל ציון מצטבר נמוך יותר יחייב מהלך של שיפור האבטחה. נוסף על כך יש לנתח כל תקיפה גם בצורה איכותית, כהשלמה לניתוח הכמותי.

16.4. אתרי גיבוי

אבטחת מידע מטפלת גם בשלמותו של המידע ולא רק בהגנתו מפני דלף. כבר בתקופת המבחן, הנפקת התיעוד החדש תתאפשר רק לאחר בדיקה ואישור על ידי המאגר. סיכון תמידי המלווה את המאגר הוא פגיעה בשירות הניתן ע"י המערכת, ובעקבות זאת פגיעה ביכולת להנפיק תיעוד לתושבי מדינת ישראל. הגורמים למימוש סיכונים אלו עלולים להיות בין השאר כוח עליון (רעידת אדמה, שיטפון, שריפה וכד'), כשל טכני במערכת, טעות אנוש או פעילות מכוונת של גורם עוין חיצוני. על מנת למנוע סיכונים אלו יש להבטיח כי הנכסים הכוללים את האתר הפיזי בו מצויות המערכות, מערכות המידע של המאגר והמערכות החיצוניות הפונות אליו בעקיפין, יגובו וזאת לשם מתן מענה לתרחיש בו מופסקת פעילות המאגר בשל אחת הסיבות שהוזכרו לעיל. על כן עוד לפני תחילת הפעלתו המבצעית של המאגר יש צורך בהקמה של אתר גיבוי בו יאוחסנו שרתים, יישמר מידע ביומטרי ותתאפשר סביבת עבודה מול שרתים אלו על מנת לאפשר יכולת התאוששות מהירה במקרה אסון באופן מאובטח הן פיסית והן לוגית. גיבוי המערכת תוך שימוש באתר הגיבוי תבוצע במהלך תקופת המבחן בתדירות של אחת לחודש. הצלחה תחשב במידה והמערכת תוכיח יכולת התאוששות ותחילת עבודה מחודשת בתוך 60 שעות.

16.5. הסתייעות בגורמי חוץ

במהלך תקופת הניסוי ובמהלך גיבוש תהליכי העבודה ייתכן ויידרש סיוע של גורמי חוץ כגון מומחי מז"פ לצרכי זיהוי ואימות. במידה ויקום צורך שכזה, יגיע מומחה מז"פ בעל התאמה ביטחונית כנדרש למאגר הביומטרי וזאת בכדי להימנע מהוצאת מידע כלשהו מחוץ למאגר. כניסתו של מומחה כזה למאגר תתבצע על פי דרישות החוק לכניסת בעלי תפקידים חיוניים שאינם עובדי הרשות לניהול המאגר הביומטרי.

16.6. שמירת מידע

מידע שייאסף במהלך הניסוי לא יכלול נתונים או אמצעים ביומטריים או מידע מזהה אחר (למעט מקרים של הרכשה כפולה שיועברו לטיפול משטרתי, כמוגדר בחקיקה). באותם מקרים בהם יש לשמור תמונה ממערך ההרכשה (כדי לנתח בעיות תאורה למשל) יש לשמור אך ורק תמונה מופחתת. בדרך כלל יישמר רק מידע לוגיסטי כמפורט בפרק המדדים, ונתוני איכות של התמונות (שאינם מידע אישי) כדי להימנע מהצורך לחשבם בכל פעם מחדש. נתוני איכות אלו גם יועברו למאגר וישמשו כחלק מתהליך קביעת ציון המעבר של הדגימה.

למען הסר ספק: שמירת מידע במהלך הניסוי תכלול רק מידע כללי שחיוני לצורך הסקת מסקנות ובכל מקרה לא מידע אישי.

17.הגנה על הפרטיות

הגנה מפני שימוש לרעה במידע אשר מסרו תושבי מדינת ישראל ואשר שמור במאגר המידע, ופיקוח על שמירת פרטיות המידע הינן חלק מתפקידיה העיקריים של הרשות לניהול המאגר הביומטרי ולשם כך נקבע בחוק (בסעיף 26) כי ימונה בעל תפקיד "הממונה על הגנת הפרטיות במאגר", אשר תפקידו פיקוח על שמירת הפרטיות של התושבים שאמצעי ונתוני הזיהוי הביומטריים שלהם כלולים במאגר הביומטרי.

חובתו של הממונה על הגנת הפרטיות לדווח מדי שנה לשר הפנים, לשר המשפטים, לוועדת הכנסת המשותפת ולרשם מאגרי המידע, על פעולותיו על פי החוק להכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע ועל פי חוק הגנת הפרטיות.

כאמור לעיל, העברת מידע ביומטרי מהמאגר לכל גורם שהוא לא תתאפשר במהלך תקופת הניסוי.

במהלך תקופת הניסוי תבוצענה הדמיות בלבד, ללא העברת תשובות אמת, וייקבעו דרישות האבטחה והממשק הנדרשות מן הגופים אשר מוגדרים בחוק כרשאים לעמוד בקשר מול הרשות לניהול המאגר הביומטרי.

17.1. העברת מידע מהמאגר לגורמי חוץ

כאמור, בתקופת המבחן לא תהיה הוצאה של מידע כלשהו מהמאגר לגורם חיצוני. לרשות האוכלוסין תועבר אך ורק תוצאת תהליך ההשוואה לאחר השוואת הרשומות במאגר (תשובה "חיובית", "שלילית" או "בבירור"). תוצאת הזיהוי תועבר טלפונית ובנוסף על ידי מילוי **ידני** של נתונים בשדה/מסך ייעודי במערכת "אביב". לא יועבר כל מידע נוסף מהמאגר.

17.2. נגישות למידע במאגר

כפי שנקבע בחוק, מספר מורשי הגישה למאגר הינו מצומצם ביותר ומוגבל רק לבעלי תפקידים החיוניים להפעלתו של המאגר. המידע השמור במאגר הביומטרי יהיה נגיש אך ורק לבעלי תפקידים שהינם עובדי הרשות לניהול המאגר, בעלי תפקידים חיוניים כמוגדר בחוק ומומחי זיהוי (בכפוף להתאמתם מבחינת סיווג ביטחוני ולדרישות החוק והתקנות). רק עובדי הרשות לניהול המאגר הביומטרי יוכלו לבצע פעולות מול המאגר.

כל מורשה גישה למאגר יוסמך בכתב מינוי מתאים על ידי ראש הרשות לניהול המאגר הביומטרי ובהסכמת שר הפנים וראש הממשלה, כנדרש בחוק.

במסגרת תקופת הניסוי תיבחן צורת ההפעלה של המאגר בהיבט ההגנה על פרטיות האזרחים. ייבחן כיצד והאם עמדה הרשות לניהול המאגר הביומטרי בכל דרישות ההגנה על הפרטיות המוגדרות בחוק ובתקנות.

18.עיבוד התוצאות

TBD - יושלם בהמשך.

19.נספחים

19.1. תקנים ומסמכים ישימים

ISO/IEC 19794-2	Biometric data interchange formats Part 2: Finger Minutiae Data
ISO/IEC 19794-5	Biometric data interchange formats Part 5: Face Image Data
ICAO DOC9303	Part1 Volume 2: Specifications for electronically enabled passports with biometric identification capability
ICAO NTWG	Guidelines on e-MRTDs & Passenger Facilitation
EU	COUNCIL REGULATION (EC) No 2252/2004
FBI BIO SPECS	Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Specification Version 3.1
ISO/IEC 15444-2:2000	JPEG2000 specifications
Keesing journal of documents & identity	issue 19,2006: Compliance with facial image standards
ICAO Technical Guideline	TR-03110: Advanced Security Mechanisms for MRTD – EAC, V1.11
UIDAI, India	UID enrolment p.o.c. report
NIST	Biometric Image Software (NBIS)
NIST	Biometric Quality: The last 1% Biometric Quality Assessment for Error Suppression
NIST	Usability & Biometrics: Ensuring Successful Biometric Systems
NBSP	Biometric Technology Application Manual vol. 1-3
UK PASSPORT SERVICE	BIOMETRICS ENROLMENT TRIAL Report May 2005

19.2. פרמטרים של צילומי פנים

להלן התכונות הנבדקות בתוכנת בקרת האיכות של צילומי הפנים:

התכונה הנבדקת	חשיבות	הערות
מצג של הראש	גבוהה	איתור סטייה בשלושה צירים
ממדים	גבוהה	גודל כללי, מיקום הראש, מיקום העיניים, מרחק בין העיניים
תכונות התמונה	גבוהה	חדות, רזולוציה, צבע, עיניים אדומות
תאורה	גבוהה	צל על הפנים או בארובות העיניים, נקודות רוויה מבחינת חשיפה (Hot spots), חשיפה
רקע	בינונית	אחידות, צללים, עצמים נוספים בתמונה (כדוגמא - אדם נוסף, או אובייקט)
מצב העיניים	בינונית	זיהוי עיניים עצומות, מבט לצד, הסתרה של העין
הבעה	נמוכה	זיהוי פה פתוח, חיוך

19.3. כלים לאיתור הרכשות כפולות

אחד הנושאים המרכזיים, שיוכרע בתום תקופת המבחן, הוא מידת המענה שנותן המאגר לבעיית ההרכשות הכפולות ונחיצותו. תקופת המבחן, כאמור במבוא למסמך זה, נועדה לבחון הצעה ייעודית ולא כל חלופה למאגר, ככל שיש חלופה כזו. הניתוח שלהלן דן באותן חלופות לכאורה ומסביר מדוע אינן חלופות של ממש או מדוע אינן ניתנות לניסוי בפועל. חלק מהחלופות הועלו על ידי מתנגדי המאגר (ראה העתירה לבג"צ נגד החוק למשל) וחלק אחר הן חלופות שנבחנו ונשקלו כחלק מעבודת המטה לקראת החקיקה ובמהלכה.

מטרת המאגר הינה בראש וראשונה איתור של הרכשות כפולות. עצם חיזוק התיעוד מבחינת חסינותו לזיופים לא מתמודד כלל עם שאלת ההרכשות הכפולות ולכן נדרש כלי כזה. יתרה על כך – כאשר התיעוד עצמו אמין וקשה מאד לזייפו רמת האמון כלפיו עולה. כאשר פושע ישיג תיעוד כזה (על ידי הרכשה כפולה) הוא יוכל להשתמש בו כרצונו והזיוף לא יתגלה לעולם. נושא זה מעסיק מדינות רבות וזוכה מעט לעת לתהודה ציבורית, בפרט באותן מדינות שאין בידן כלי המאפשר להתמודד עם רעה חולה זו[69]. הספרות המקצועית בתחום זה איננה רבה אך במעט שיש ניתן למצוא סימוכין לכך שאין חלופה למאגר[70].

השורה התחתונה של הניתוח שלהלן היא שמאגר מרכזי הינו הכלי היחיד להתמודדות ראויה עם הרכשות כפולות. המשמעות של עבודה ללא מאגר היא התעלמות מבעיית ההרכשות הכפולות והותרת פרצה משמעותית במערך חשוב זה.

הדיון שלהלן עוסק כאמור בחלופות למאגר ולא בחלופות למימוש המאגר (כדוגמת הצעתו של פרופ' עדי שמיר ממכון וייצמן).

---

[69] ראה למשל מאמר (בצרפתית):
http://www.leparisien.fr/faits-divers/plus-de-10-des-passeports-biometriques-seraient-des-faux-19-12-2011-1775325.php

או באנגלית:
http://french-news-online.com/wordpress/?p=8299#axzz1swANXX00

[70] ראה "***Documents: The developer's toolkit***", מאת Diana Ombelli ו-Fons Knopjes, הוצאת Occidentalis, פורטוגל 2008, פרק 7, סעיף 7.2.3.

19.3.1. חלופות למאגר

להלן החלופות לכאורה לשימוש במאגר לצורך איתור הרשות כפולות:

19.3.1.1.הנפקת תיעוד לאומי ללא מאגר

חלופה זו כוללת הנפקה של תיעוד הכולל מידע ביומטרי (תמונות פנים וטביעות אצבע), כאשר מידע זה נשמר אך ורק בתיעוד עצמו, ללא אגירה מרכזית. המשמעות הישירה של חלופה זו הינה **העדר מוחלט** של כלי לאיתור הרכשות כפולות, על כל המשתמע מכך. מצב זה מותיר את מערך התיעוד (ובעצם את כל מערך הזהויות במדינה) **במצב פרוץ**, כאשר יריב לא מתוחכם במיוחד, ללא יכולות טכנולוגיות מרחיקות לכת, מסוגל לתקוף מערך זה ללא קושי וללא סיכוי להתגלות. בהמשך נסקור את החלופות לכאורה ונראה שכאשר לא נשתמש במאגר – לא נוכל להתמודד עם הרכשות כפולות.

חשוב להדגיש שחלופה זו הינה חלופה סבירה, אך ורק אם החלטה כזו מתקבלת בעיניים פקוחות ותוך נטילת אחריות לכך שמערך התיעוד נותר פרוץ.

19.3.1.2.שימוש באימות על ידי תשאול

אחת החלופות למאגר, שהועלתה על ידי רבים מהמתנגדים, גורסת שתשאול מעמיק יותר (ראה סעיף 6.1.3 לעיל) יאפשר **לאתר הרכשות כפולות**. ראשית יש לבחון טיעון זה במבחן השכל הישר. על פי מבחן טריוויאלי זה מתחזה שמבצע הרכשה כפולה יכול לעמוד בתשאול בזהותו המקורית וגם בזהותו הבדויה, **ללא יכולת להצליב בין הזהויות**. עצם התשאול לא יצביע על כך שמדובר בזהות אחרת והתהליך אינו יוצר את הקישור המבוקש בין הזהויות השונות של אותו אדם. יתרה על כך - התהליך כולו בעייתי, יקר וקשה לביצוע[71]. היכולת לבצעו כראוי היא כמובן אחד הנושאים שייבחנו בתקופת המבחן של החוק. יש להדגיש שתהליך התשאול יכול לייצר בנקל התראות שווא ולפגוע בצורה קשה בשירות לאזרחים תמימים. יתרה על כך – כמות השאלות שניתן לשאול בתשאול כזה מוגבלת מאד ויעילות השאלות פוחתת עם הזמן, כאשר "בנק" השאלות יהיה ידוע לכל.

המהות היא כאמור שתהליך תשאול, מעמיק ככל שיהיה, לא מאפשר הצלבה בין שני מופעים של אותו אדם, כך שחלופה לכאורה זו איננה עומדת במבחן השכל הישר מבחינת היכולת **לאתר הרכשות כפולות**. למרות זאת, יבוצע ניסוי עקיף, שיבחן שאלה אחרת, ובפרט "האם עצם הגבהת הרף לקבלת תיעוד נותנת מענה למניעת הרכשות כפולות, גם אם לא ניתן לדעת שכישלון בתשאול נובע מהרכשה כפולה?".

[71] ראו למשל דו"ח של משרד מבקר המדינה האנגלי, על פיו עלות התהליך מתקרבת ל-10% ממחיר הדרכון לאזרח:
"Identity and Passport Service: Introduction of ePassports"
Report by the Comptroller and Auditor General, HC 152 Session 2006-2007, February 2007

19.3.1.3. שימוש במסמכים תומכים

שימוש במסמכים תומכים (breeder documents) מתבסס על הערמת קשיים בפני מי שרוצה לקבל תיעוד. עליו להציג מסמכים שונים המוכיחים את זהותו. יש כאן פרדוקס מובנה כי כדי לקבל מסמך זיהוי מאובטח מאד וחסין נגד זיופים נדרש להביא מסמך אחר, שרמת האבטחה שלו אפסית. היכולת של פקיד, שעסוק במתן שירות לאזרחים, לקבוע שלפניו מסמך אמיתי היא אפסית. נפנה כאן שוב לאותו מאמר מצרפת שמצביע על פער לא סביר זה[72].

גם כאן המהות היא חוסר היכולת להצליב בין שני אירועים שמאחוריהם נמצא אותו אדם, המקבל שני מסמכי זיהוי.

19.3.1.4. יכולת ביטול תעודות

אחד הטיעונים שהעלו המתנגדים למאגר לא אחת גורס שאין צורך במאגר כי ניתן לבטל תעודה קיימת וכך למנוע כפילויות. טיעון זה מעורר תמיהות רבות כי לא מדובר כלל בחלופה למאגר. המטרה של המאגר היא לאתר הרכשה כפולה עכשווית (שכבר קיימת) ולהרתיע כנגד ניסיונות הרכשה כפולה בעתיד. אם נרצה לאתר הרכשה כפולה כזו עלינו לשאול את עצמנו ראשית, כיצד תתגלה הכפילות? ניתן לאתר כפילות אך ורק באמצעות השוואה של נתונים מתעודה מסוימת **<u>לכל</u>** אירועי האימות הקודמים, **<u>של כל התעודות באשר הן</u>**. השוואה רק לאירועי אימות של אותה תעודה איננה משמעותית כמובן כי אין בכך כדי להציף אירועי כפילות (ההשוואה היא תמיד לאותם נתונים ותמיד תחזיר תשובה תקינה). האם ניתן להשיג מטרה זו באמצעות השוואה לאירועי אימות של כל התעודות האחרות? זה אכן אפשרי אם ההשוואה היא מול מאגר ארוך טווח של כל מה שנקרא מתעודות אחרות, אך חלופה זו הינה פוגענית בהרבה ומהווה מאגר הרבה יותר גדול "בדלת האחורית". השוואות כאלה, לכל התעודות, דורשות גם קישוריות נרחבת, שאיננה קיימת היום ויוצרת פגיעה אנושה ומשמעותית בפרטיות, **<u>ללא יכולת מעשית להגן על המידע כאשר יש קישוריות כל כך נרחבת</u>**. זאת לעומת החלופה של רישום חד פעמי למאגר ללא קישוריות. שוב, במבחן השכל הישר אי אפשר להניח שתהיה קישוריות כזו גם בעתיד הנראה לעין וכמובן לא נרצה קישוריות כזו בגלל הקושי להגן עליה כראוי. יש להדגיש שאחד העקרונות המנחים של המאגר, עיקרון שאף הוגדר בחקיקה כדי לקבעו לזמן ארוך, הוא ניתוק המאגר מכל רשת תקשורת ושמירתו במקום יחיד ומוגן.

---

[72] ראה למשל מאמר (בצרפתית):
http://www.leparisien.fr/faits-divers/plus-de-10-des-passeports-biometriques-seraient-des-faux-19-12-2011-1775325.php

או באנגלית :

http://french-news-online.com/wordpress/?p=8299#axzz1swANXX00

כנראה שחלופה זו, שהוצעה על ידי מספר גורמים, נובעת מחוסר הבנה לגבי יחסי הגומלין בין תעודה פיזית ותעודה אלקטרונית/דיגיטאלית. תעודה דיגיטאלית היא מידע ונתונים הנמצאים על תעודת הזהות הפיזית ומשמשים להזדהות מקוונת **ללא צורך בנוכחות פיזית וללא קשר אליה**. בדרך כלל התעודה הפיזית והתעודה הדיגיטאלית תקפים או פגי תוקף ביחד, והמלצתנו לגורמים מסתמכים לבדוק **תמיד** את תקפות התעודות הדיגיטאליות, אך חשוב להבין שלתעודת הזהות יש מספר רב של שימושים ומספר רב של צורות בדיקה, כל אחת עם רמת הסמך שלה. בחלק מהמקרים יתכן שתעודה דיגיטאלית תבוטל אולם הכרטיס הפיזי ימשיך להיות שמיש, ובפרט למי שהשיג כרטיס כזה במרמה. רמת הבדיקה נקבעת תמיד על יד הגורם המסתמך וזה יכול להחליט כרצונו. איננו יכולים להניח שכל מערכת מידע באשר היא, של כל גורם, תבצע בדיקה מלאה כזו.

לצורך ההסבר, להלן צורות הבדיקה והאימות של תעודת הזהות הפיזית:

19.3.1.4.1. בדיקה חזותית

במצב זה נבדקת תקינות התעודה והתאמתה לבעליה בצורה חזותית בלבד, ללא שימוש במכשירים כלשהם או בתשתית מחשוב. ניתן לאמת סימני ביטחון בולטים (השוואה של הצילום "בעין", הולוגרמה, CLI[73] וכדומה).

19.3.1.4.2. בדיקה חיצונית מעמיקה

בדיקה כזו דורשת יותר ידע ושימוש בכלים פשוטים (זכוכית מגדלת, מנורת UV[74] וכדומה).

19.3.1.4.3. בדיקה אלקטרונית/ממוחשבת

בדיקה כזו כוללת קריאת מידע מהשבב ואימותו באמצעות החתימה האלקטרונית על המידע שנוצרת בתהליך ההנפקה. חתימה זו מוכיחה שהמידע הגיע ממערכות המידע של משרד הפנים ובאותה עת מוכיחה גם שהמידע לא עבר שינויים מאז שנכתב. בדיקה כזו תאמת את הנתונים הרגילים (שם, מספר זהות, תאריך לידה) אולם איננה קשורה למידע הביומטרי[75].

19.3.1.4.4. בדיקת התעודה הדיגיטאלית

בדיקה זו מיועדת בעיקר לאימות מקוון, ללא נוכחות בעל התעודה בצד המאמת וללא קשר לביומטריה. האימות מבוסס על יכולות חישוביות של הכרטיס, שהפעלתן תלויה בהזנת

---

[73] CLI = Changeable Laser Image, סימן ביטחון חזותי המציג את מספר הזהות או את תמונת בעל התעודה בהתאם לזווית הצפייה בו.

[74] הכרטיס מכיל רכיבי דפוס שזורחים בצורה מיוחדת באור אולטרה-סגול.

[75] כאשר יש הרשאת קריאה למידע הביומטרי ניתן לאמת את מקורו של מידע זה באמצעות החתימה האלקטרונית אולם אין לכך קשר לאימות הביומטרי גופו.

סיסמה אישית נכונה, בדומה לכרטיס בנקאי. כאמור שימוש זה מיועד למצב מקוון, כלומר מתן שירותי "ממשל זמין" מרחוק ואין בינו ובין השימוש בביומטריה דבר וחצי דבר.

19.3.1.4.5.בדיקה אלקטרונית הכוללת בדיקת התעודה הדיגיטאלית

בדיקה זו הינה עוד יותר מהימנה וכוללת הצלבה בין תקפות הכרטיס הפיזי והתעודה הדיגיטאלית. ההחלטה אם לבטוח בתעודה תלויה במדיניות שיגדיר הבודק. גם כאן אין כל קשר לביומטריה.

19.3.1.4.6.אימות ביומטרי

בדיקה כזו הינה אימות שבעל התעודה הוא אכן זה שפרטיו צרובים בשבב. אימות זה מיועד למצב שבו בעל התעודה נוכח פיזית בצד המאמת.

תעודת הזהות צריכה לתת מענה לכל המצבים ואיננו יכולים להניח שבכל מצב ובכל עת תיבדק גם התעודה הדיגיטאלית במקביל לאימות התעודה הפיזית. היכולת לבטל תעודה דיגיטאלית **<u>כלל איננה קשורה לבעיית הכפילויות</u>**, איננה נותנת לה מענה ובכל מקרה רלבנטית רק לאותם מקרים כאשר נעשה אימות מקוון. **<u>ללא סינון זהויות כפולות באמצעים ביומטריים אין דרך לדעת ששתי תעודות דיגיטאליות שייכות לאותו אדם</u>**.

19.3.1.5.הצלבה בין ת.ז. לדרכון

חלופה נוספת לכאורה הינה הצלבה בין דרכון ותעודת זהות של אותו אדם. גם כאן מתעוררת השאלה מול מה, לשיטתם של מציעי חלופה זו, תתבצע ההשוואה כדי לאתר כפילויות? אם מתחזה מחזיק שתי זהויות ובשתיהן יש לו דרכון וכרטיס תעודת זהות - לא נוכל לאתר את הכפילות כלל כי שוב, כמו בחלופות הקודמות, **<u>אין דרך להצליב בין שתי הזהויות</u>**. יש להניח שאותו מתחזה מן הסתם יהיה חכם דיו ולא ירצה להציג את הדרכון של זהות א' כדי לאמת את זהות ב'. שוב אנחנו חוזרים לצורך במאגר, אלא שהפעם, אם נרצה לבצע הצלבה כזו, יש לשמור כל אירוע אימות באשר הוא, מכל מקום בו הוא מתבצע. זוהי פגיעה חמורה בפרטיות וגם שוללת את היכולת להגן על מידע כזה כי יש לפרוס תשתית תקשורת מכל מקום לכל מקום, כפי שהוסבר בסעיף 19.3.1.4 לעיל.

19.3.1.6.מאגר של ט"א בלבד

על פי חלופה זו ההרכשות הכפולות תאותרנה באמצעות טביעות אצבע בלבד. לכאורה ניתן אמנם להסתפק בטביעות אצבע ולא במאגר משולב של תמונות פנים וט"א. במציאות אמירה זו הייתה נכונה אם רמת הפירוט של טביעות האצבע הייתה גדולה יותר, קרי שמירה של יותר משתי אצבעות (כמו למשל במאגר מבקשי האשרות בארה"ב, במאגר פנקס הבוחרים במקסיקו ובמאגר ההודי, ששומרים נתונים מעשר אצבעות). בנקודה זו נכנס שיקול המידתיות לתמונה.

ההחלטה בישראל הייתה ללכת לכיוון המידתיות ולשמור מידע מזערי של שתי אצבעות בלבד ולא יותר. במצב זה נדרש נתון מזהה נוסף כדי להכריע במצבי שגיאה וספק וכדי לתת מענה לאותם מצבים בהם לא ניתן לסרוק את האצבעות המורות (הצפי הוא ל-0.5% עד 1% מהאוכלוסייה). מלבד זאת, כאשר מתעורר ספק, יש להציג למפעיל המאגר את תמונת הפנים כדי שיוכל להכריע לגבי השאילתה. היכולת של עין אנושית להכריע במקרי ספק הינה יכולת חשובה ביותר כדי לא לשלול תיעוד ממי שזכאי לו.

השמטת תמונות הפנים, מלבד הצורך לתת מענה לאותו פלח אוכלוסייה שצויין לעיל, חשובה גם בהיבטי אבטחה והרתעה. הסתמכות על טביעות אצבע בלבד תותיר פרצה משמעותית כי פושע יכול בנקל לחבל בטביעות אצבעותיו ולבצע הרכשה כפולה ללא יכולת לאתרו.

19.3.1.7.שימוש במיצוי (hash)

חלופה אחרת (ושוב לצערנו לכאורה בלבד) גורסת שניתן לשמור מיצוי של המידע הביומטרי ולא את המידע עצמו. מיצוי הינו "רידוד" של המידע באמצעות תהליך חישובי חד כיווני. הטיעון לגבי קיומה של חלופה כזו מפתיע במיוחד, לאור העובדה שטכנולוגיה כזו **פשוט איננה קיימת**. יתרה על כך - לדעת רבים וטובים יתכן שאף איננה אפשרית כלל. זהו נושא שנחקר רבות אולם ללא תוצאות של ממש. הרעיון מתבסס על כך שמכל דגימה ביומטרית יחושב מספר קבוע, בתהליך חד כיווני, שלא מאפשר לחזור מהמספר המחושב למידע המקורי ממנו חושב. מבחינה מעשית כל דגימה ביומטרית (של אותו אדם) שונה מדגימה אחרת ולעולם לא תחזור על עצמה בדיוק. אדם שיניח את אותה אצבע ברצף, מספר פעמים על אותו חיישן ייצר בכל פעם רצף סיביות שונה מקודמו. כדי לייצר מיצוי כנ"ל המשמעות היא אחת: נדרש תהליך חישובי שייצר פלט של מידע קבוע מתוך קלט של מידע משתנה. ניתן אמנם לסווג את המידע למשפחות וכדומה, אך השורה התחתונה היא שכל תהליך כזה יקרוס כאשר האוכלוסייה היא גדולה. יתכן שנצליח לסווג את טביעות האצבע לקבוצות אך ככל שהאוכלוסייה תגדל נקבל כמות גדלה והולכת של טביעות שונות שתייצרנה מיצוי זהה.

הערה: בתהליך העיצוב של המאגר נבדקה טענה של שני ספקי טכנולוגיה, האחד מנורבגיה והשני מהולנד, שהתיימרו שניהם לספק טכנולוגיה כזו. שתי החלופות (שבינתיים התאחדו לחברה אחת) התבררו כהבל ורעות רוח ושתיהן קורסות כאמור באוכלוסיות גדולות. לשם דוגמה, כאשר מבוצע בעזרת מוצר כזה חיפוש על מאגר של מיליוני רשומות תתקבלנה עשרות אלפי רשומות זהות ואולי גם מאות אלפי רשומות. מעשית, השימוש היחיד של "טכנולוגיה" מפוקפקת כזו הוא סינון מוקדם של מאגר ביומטרי, כדי לאפשר חיפושים מהירים יותר בשיטה רגילה, תוך שימוש במידע הביומטרי המלא.

19.3.1.8.שימוש בתבניות

להבדיל ממיצוי, המתייחס לייצור ערך קבוע מהדגימה הביומטרית, תבנית הינה רידוד של המידע כך שניתן עדיין לבצע השוואה הסתברותית ולקבל ציון התאמה בינה לבין הדגימה בפועל. בלשון החוק ההתייחסות לתבנית היא "נתונים ביומטריים" המופקים מ-"אמצעים ביומטריים". נציין שנושא זה הוסבר בהרחבה בדיונים על החוק בכנסת ונחזור על הסבר זה בקצרה כאן. גם ארגון התעופה האזרחית הבינלאומית ICAO ממליץ להשתמש בתמונות הגולמיות ("אמצעי ביומטרי") ולא בתבניות ("נתון ביומטרי") , אך הצורך העיקרי לכך הוא תפעולי. בעת שמטפלים בשגיאת השוואה יש להציג למפעיל המערכת את **התמונות הגולמיות** לצורך קבלת החלטה. אין לכך חלופה אחרת כי מפעיל אנושי איננו יכול לקבל החלטה על סמך רצף סיביות חסר משמעות מבחינתו. סיבה חשובה נוספת היא הרצון להיות גמישים ולא ליצור תלות בלתי הפיכה ביצרן זה או אחר, המכונה בעגה המקצועית "vendor lockin". במערכות ביומטריות רוב התבניות הן במבנה קנייני של ספק זה או אחר ושימוש בתבנית, ללא שמירה ארוכת טווח של המידע הגולמי, הינה "חתונה קתולית" עם ספק זה. מעבר לספק אחר הינו על סף הבלתי אפשרי ומעורר קשיים רבים. קיימות אמנם תבניות שהמבנה שלהן אינו קנייני אלא מבנה מתוקנן אך רמת הביצועים שלהן נמוכה יותר וקצב השגיאות שלהן גבוה יותר.

חשוב להדגיש שהשימוש השוטף במידע הביומטרי נעשה בכל מקרה באמצעות השוואת תבניות אך כאשר מפעיל אנושי נדרש לבדוק התראה על הרכשה כפולה – הוא **חייב** לראות תמונות ולא רצף סיביות חסר משמעות.

19.3.1.9.שימוש במאגרי משנה קטנים

חלופה אחרת שעלתה היא שימוש במאגרי משנה קטנים שיכללו אוכלוסיות מוגדרות (כגון בעלי עבר פלילי או עולים חדשים). מאגרי משנה אלו ישמשו כדי לחזק את הליך התשאול באמצעותם ורק מול אותן אוכלוסיות מוגדרות ולא מול כלל האוכלוסייה. ראשית חשוב להדגיש שרשות האוכלוסין איננה נגישה למאגרי מידע פליליים ואין זה הגיוני שהשירות לאזרחים יתבסס על נגישות כזו. שנית - שוב נוצרת פרצה משמעותית במערך הזהויות, ללא כלי להתמודד עם פרצה כזו. מי שלא נמצא במאגר הפלילי יוכל לנצל פרצה כזו כרצונו ומבלי שיתגלה. בנוסף, קיים קושי אבטחתי ניכר לטפל בריבוי מאגרי מידע, עם קישוריות נרחבת, לעומת הטיפול באבטחת מאגר מידע ביומטרי יחיד, ללא קישוריות.

19.3.2. סיכום וחידוד הצורך במאגר

ידוע לכל כי חוזקה של כל שרשרת הוא כחוזק החוליה החלשה ביותר. כאשר נבצע ניתוח סיכונים לתיעוד החדש נראה לפנינו פרדוקס מעניין: תעודת הזהות החדשה, כמו גם הדרכון החדש, כוללים

סימני ביטחון מתקדמים ביותר וחסינים במיוחד נגד זיופים. למעשה זיוף תעודת הזהות או הדרכון איננו מעשי יותר לרוב המוחלט של הזייפנים, ובכלל זה זייפנים עתירי יכולות טכנולוגיות ומשאבים ואפילו למעצמת על. מנגד, אפילו כאשר התשאול יהיה מקיף ומעמיק, עדיין יכול פושע מן השורה, ללא יכולות טכנולוגיות וללא הזדקקות למשאבים כספיים כלשהם, להתחזות לאחר מול פקיד בלשכת רשות האוכלוסין ולקבל מהמדינה תעודת זהות או דרכון **אמיתיים לחלוטין**, שיעברו כל בחינה של המחלקה לזיהוי פלילי במשטרה, **אך עם פרטים לא לו**. התמונה תהיה שלו, טביעות האצבע תהיינה שלו אך השם ומספר הזהות או מספר הדרכון יהיו של אחר.

הדרך המעשית היחידה לגשר על פער זה ולהרתיע פושעים מפני ניצול הפרצה הזו, היא ליצור מאגר ביומטרי שישווה את הזהות המוצהרת לזהות ששמורה במאגר. כל יתר "החלופות" לכאורה אינן נותנות מענה כלל לסוגיית איתור ההרכשות הכפולות, או לחלופין גורמות פגיעה קשה ואנושה בפרטיות.

במהלך תקופת המבחן נשמח כמובן לקבל הצעות אחרות להתמודדות עם הרכשות כפולות ולבחון אותן לעומק, ככל שתהיינה כאלה.

19.4. אופן שילוב הלמ"ס

בהתאם לתקנה 10 ב"צו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי הזיהוי ובמאגר המידע (תקופת המבחן), התשע"א - 2010" מוטל על הסטטיסטיקאי הראשי לתת חוות דעת בדבר התאמת תכנית המבחן ויישומה לאמות מידה מקצועיות.

בנוסף על כך הלשכה המרכזית לסטטיסטיקה תהיה מעורבת באופן מעשי במימוש תכנית המבחן ותהיה הגורם המאשר של:

- חישוב מדדי ביצוע
- ביצוע סקרי שביעות רצון התושבים
- סיוע בהכנת דין וחשבון תקופתי

להלן פירוט הסעיפים השונים:

19.4.1. חישוב מדדי ביצוע

חלק מהותי מתוכנית המבחן הוא חישוב של מדדי ההצלחה שנקבעו ליישום חוק הביומטריה בתקופת המבחן (ראו פרק 14). כאמור, לצורך חישוב מדדים אלו תבצענה מערכות המחשוב של רשות האוכלוסין וההגירה וכן של הרשות לניהול המאגר הביומטרי רישום ממוכן של מרבית הנתונים הדרושים לצורך הערכת איכות התהליך התפעולי ובחינת הנושאים הטכנולוגיים השונים. כמו כן, חלק קטן מהנתונים ייאסף בצורה שאינה ממוכנת (התרשמות מפעילי המערכת).

באחריות כל מקור מידע, כמפורט לעיל, להעביר את הנתונים הנאספים על ידו ללשכה המרכזית לסטטיסטיקה, על מנת שתבצע את החישובים הנדרשים לצורך המדידה של יישום חוק הביומטריה בתקופת המבחן בהתאם לתוכנית המבחן. הלשכה המרכזית לסטטיסטיקה תנטר את איסוף הנתונים כדי להבטיח שהאיסוף נערך בצורה מהימנה.

19.4.2. ביצוע סקרי שביעות רצון התושבים

ראו סעיף 13.3.

19.4.3. סיוע בהכנת דין וחשבון תקופתי

על פי "צו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי הזיהוי ובמאגר המידע (תקופת המבחן), התשע"א - 2010" מחויבות רשות האוכלוסין וההגירה והרשות לניהול המאגר הביומטרי להכין, אחת לחצי שנה, במשך תקופת המבחן, דין וחשבון מפורט בכתב שיוגש לראש הממשלה, שר הפנים, שר המשפטים, השר לביטחון פנים ולוועדת הכנסת המשותפת. עוד נקבע בצו, כי הדין וחשבון יכלול את תיאור כלל התוצאות של הבדיקות, הממצאים והאסמכתאות לממצאים.

הלשכה המרכזית לסטטיסטיקה תסייע בגיבוש מבנה עקרוני למסמך הדין וחשבון התקופתי ותאשרו.

כמו כן, הלשכה המרכזית לסטטיסטיקה תסייע בחיבור של כל דין וחשבון במועדו.

19.5. עמדות מעבר ביומטרי בשירות עצמי - בקורת הגבולות/נתב"ג

רשות האוכלוסין מתכוונת להנפיק בקרוב דרכונים ביומטריים לישראלים בהתאם לחוק, לתקנות ולצו. במסגרת זו נערכת רשות האוכלוסין גם לניסוי של מעבר בקורת גבולות לישראלים בעמדות לא מאויישות (להלן "עמדות המעבר" או "קיוסקים"). אוכלוסיית הניסוי תכלול כל אזרח ישראלי שיונפק לו מסמך נסיעה הכולל מידע ביומטרי וירצה לבצע מעבר בקורת גבולות בעמדה לא מאויישת. ניסוי זה יהווה את השימוש/היישום הראשון שיהיה ניתן לעשות באמצעות הדרכון החדש (מעבר לשימוש בו במדינות אחרות).

19.5.1. מטרת הניסוי בנתב"ג

המטרה היא לבחון את המשמעויות הטכנולוגיות והתפעוליות הנובעות משילוב ביומטריה במעבר בקורת גבולות לישראלים בעמדות לא מאויישות, ולאסוף מידע לצורך ניתוח וקבלת החלטה על אופן השימוש המיטבי בביומטריה בתהליכי ביקורת הגבולות. בחינה זו תבוצע במסגרת המטרות שהוגדרו בחוק, בתקנות ובצו שמכוחו.

19.5.2. יעדים

להלן יעדי הניסוי:

19.5.2.1.בדיקת חוקיות ואותנטיות המסמכים

עמדות המעבר תבצענה אימות של מסמכי הנסיעה באמצעות סריקתם באורכי גל שונים (תאורה רגילה, תאורת UV, תאורה אינפרה-אדומה) והשוואת התמונה המתקבלת לתמונת ייחוס.

19.5.2.2.שיפור רמת הזיהוי למניעת מעבר בזהות שאולה

אימות זהות העובר באמצעים ביומטריים נועד למנוע ממי שאינו מורשה לצאת מגבולות המדינה או להיכנס אליה.

19.5.2.3.הזנה אמינה ומהירה של נתוני העובר

קריאה ממוכנת של מידע מהדרכון (ובפרט מהשבב המשולב בו) תאפשר לקבל אמינות גבוהה של המידע הנשמר במערכות המידע של ביקורת הגבולות, כולל אימות של חתימה אלקטרונית על מידע זה.[76]

19.5.2.4.קיצור זמן המעבר

יעד משמעותי מאד הינו שיפור של רמת השירות הניתן לעוברים. היות והניסוי מתייחס לאזרחי ישראל יש ליעד זה גם השלכות לטובה על תחום האבטחה, כי טיפול מהיר ויעיל באוכלוסייה

[76] המידע הרשום בשבב חתום על ידי מערכת ההנפקה באמצעות חתימה אלקטרונית. חתימה זו מקבעת את המידע כנגד שינויים ומבטיחה את מקור המידע.

המהווה סיכון נמוך מאפשר מיקוד של מאמצי הבקרים באוכלוסיות שמטבע הדברים מהוות סיכון גבוה יותר.

19.5.2.5.שיפור רמת שביעות הרצון של העובר

מעבר לשיפור השירות לישראלים, מעבר בינלאומי (כדוגמת נתב"ג) הינו חלק מהותי מהרושם הראשוני של מבקרים זרים. טיפול מהיר ויעיל בעוברים ישראליים יקטין את העומס על דלפקי ביקורת הגבולות ויספק גם לזרים חווית מעבר טובה יותר.

19.5.2.6.תאימות לתהליכי זיהוי ובקרה במעברי גבול בינלאומיים בעולם

בשנים האחרונות, עקב עלייה ניכרת בשימוש בתחבורה אווירית, מתקשים נמלי תעופה רבים לעמוד בקיבול ההולך ומתגבר של נוסעים. אחד האמצעים שנועדו לסייע בהתמודדות עם בעיית הקיבול הוא מיכון של המעבר, ובפרט עבור אוכלוסייה מוגדרת. מבחינה מעשית יוצרים מסלול מהיר של מעבר עבור מי שמוגדר כסיכון נמוך ואותו נוסע יוכל לעשות שימוש במסלול זה אם ניתן לאמת את זהותו ברמת סמך גבוהה. מסלולים ממוכנים אלו נמצאים כיום בנמלי תעופה רבים ומכונים בעגה המקצועית "Registered Traveller". גם בנתב"ג קיים מסלול כזה המבוסס על אימות זהות על פי גאומטריית כף היד, אולם זוהי טכנולוגיה ביומטרית מיושנת מאד (המערכת קיימת משנת 1997) ולמעשה נמצאת בסוף חייה. יעד חשוב של הניסוי הוא בחינה מקיפה של חלופות לעמדות ממוכנות כאלו.

19.5.3. תכולת הניסוי

לצורך הניסוי פותחו 4 עמדות בשתי תצורות:

19.5.3.1.עמדות בתצורת קיוסק ללא שער

שתי עמדות לביצוע הזיהוי הביומטרי וכלל תהליכי הבידוק של בקורת הגבולות, ובסיום קבלת כרטיס אישור מעבר מודפס שייבדק בעמדת ה-"gatepass" בקו מעבר הגבול.

19.5.3.2.עמדות בתצורת קיוסק עם שער

שתי עמדות לביצוע הזיהוי הביומטרי וכלל תהליכי הבידוק של בקורת הגבולות, ובסיום קבלת כרטיס אישור מעבר מודפס ופתיחה אוטומאטית של השער למעבר הגבול.

שתי עמדות (אחת מכל סוג) תוצבנה במסלול הכניסה ושתי העמדות האחרות תוצבנה במסלול היציאה, במיקום מתואם עם רשות שדות התעופה.

19.5.4. התהליכים שייבחנו בפיילוט

במהלך הפיילוט ייבחנו 2 תהליכים עיקריים, כאשר אופן נטילת אמצעי הזיהוי הביומטריים יהיה בהתאם לסעיף 8 (1) של הצו:

19.5.4.1.מעבר מלא בעמדה הכוללת קיוסק ושער

במקרה זה העובר ייגש לקיוסק ויבצע תהליך אימות זהות ביומטרי. תהליך זה כולל סריקת דרכון, צילום פנים ו/או נטילת טביעת אצבע, אימות תווי פנים ו/או טביעת אצבע, הכל ע"פ ההנחיות שתוצגנה לעובר על גבי המסך. במקביל לתהליך אימות הזהות תתבצע בדיקת זכאות המעבר במערכת "רותם".

במידה ותהליך אימות הזהות צלח ולאחר שהתקבל ממערכת "רותם" אישור זכאות למעבר, יונפק לעובר כרטיס GatePass מודפס והשער ייפתח למעבר. במידה ותהליך אימות הזהות כשל או שמערכת "רותם" לא אישרה את זכאות המעבר, לא יונפק כרטיס GatePass והעובר יונחה לפנות לעמדה מאויישת.

19.5.4.2.מעבר בעמדה הכוללת קיוסק, ללא שער

העובר ייגש לקיוסק ויבצע תהליך אימות זהות ביומטרי, הכולל סריקת דרכון, צילום תווי פנים ו/או נטילת טביעת אצבע, אימות פנים ו/או טביעת אצבע, הכל ע"פ ההנחיות שתוצגנה לעובר על גבי המסך. במקביל לתהליך אימות הזהות תתבצע בדיקת זכאות המעבר במערכת "רותם".

במידה ותהליך האימות צלח ולאחר שהתקבל ממערכת "רותם" אישור זכאות למעבר, יונפק לעובר כרטיס GatePass מודפס כאסמכתה. במידה ותהליך האימות כשל או שמערכת "רותם" לא אישרה את זכאות המעבר, לא יונפק כרטיס GatePass והעובר יונחה לפנות לעמדה מאויישת.
במידה והונפק כרטיס GatePass, העובר יגש לשער המאויש ויציג את אישור המעבר.