רשות האוכלוסין וההגירה
Population and Immigration Authority

מדינת ישראל
State of Israel

מנכ"ל
Director General

י בטבת התשע"ב
5 בינואר 2012
או. 2012-226

לכבוד
ח"כ דוד רותם,
יו"ר ועדת החוקה, חוק ומשפט של הכנסת

שלום וברכה,

הנדון: תקנות מרשם האוכלוסין (תקופת תוקפן ופקיעת תוקפן של תעודות זהות), התשע"ב – 2012

בהמשך לישיבה שהתקיימה בוועדת חוקה, חוק ומשפט ביום 28.12.11 אבקש לעדכנך כי שולבו בנוסח התקנות תיקונים אשר סוכמו במהלך הדיון האמור. ריצ"ב נוסח תקנות מתוקן.

בכל הנוגע לקביעת תוקף של חמש עשרה שנים לתעודת הזהות, במקום עשר שנים כפי שהוצע בנוסח התקנות, אבקש לעדכנך כי הנושא נבדק פעם נוספת, וזאת על ידי אנשי המקצוע הרלוונטיים ויועצים של המשרד אשר עוסקים בתחום הביומטרי בכלל, ובנושא הטכנולוגי בפרט.
לעמדתם, וזאת אף לאחר הבחינה המחודשת, לא ניתן לקצוב את תקופת תוקפן של תעודות הזהות לתקופה העולה על עשר שנים. השיקולים העומדים בבסיס עמדה זו הינם שיקולי אבטחה פיזית (בכל הנוגע לסימני הביטחון של הכרטיס), אבטחה לוגית (בכל הנוגע למנגנוני ההגנה שבשבב), עמידות פיזית של הכרטיס המכיל את השבב, ושיקולי שמירת תמונות פנים (הן המודפסות והן אלו שבשבב) וטביעות אצבע עדכניות. שיקולים אלה מובילים למסקנה כי תקופה של 15 שנים הינה אורך חיים שהפלטפורמה הטכנולוגית אינה יכולה לאפשר, ובנוסף לכך שיקולי עדכניות התמונות (הן המודפסות והן אלו שבשבב) וטביעות האצבע תומכים אף הם בעמדה זו. בעניין זה מצורף למכתבי מסמך המפרט את השיקולים לקציבת תוקף תעודות הזהות לתקופה של עשר שנים.

כזכור, בישיבה האמורה הוצגו נתונים לגבי הנעשה בעולם בכל הנוגע לקציבת תוקף תעודת הזהות, וכעולה מנתונים אלה, המדינות האירופאיות נוקטות מדיניות של הגבלת תוקף תעודות הזהות שלהן לעשר שנים, ובמקרים רבים לחמש שנים בלבד (כאשר רק שתי מדינות מאפשרות שימוש על פי גיל נושא התעודה בעת הנפקתה). לבקשתך, נעשה ניסיון נוסף באמצעות מידען מוסמך לבחון את העלויות לחידוש תעודת זהות בבלגיה, שם נעשת חידוש כל חמש שנים. הבדיקה העלתה כי עלות חידוש תעודת זהות בבלגיה דומה לעלות חידוש תעודת זהות ביומטרית בישראל, ומעבר לכך לא ניתן היה לבחון עלויות עקיפות. בהקשר זה יוער כי

מנכ"ל
Director General

מדינת ישראל
State of Israel

רשות האוכלוסין וההגירה
Population and Immigration Authority

לפני למעלה משנה נעשה ניסיון לפתיחת דיאלוג עם בלגיה בכל הנוגע לתיעוד החכם, אולם לא הושג שיתוף פעולה.

לסיום, בכל הנוגע לסעיף המתייחס לביטול תעודות עקב פגם בחתימתו האלקטרונית של ראש רשות האוכלוסין, אבקש לציין כי סעיף זה הובהר והורחב במסגרת תקנות מרשם האוכלוסין (תעודה אלקטרונית לאימות), כולל סעיף המבהיר כי לא יונפקו תעודות חדשות כל עוד לא יתוקן פגם כאמור, ולפיכך נבקש להותיר סעיף זה בתקנות שבנדון, אשר נדרש לצורך ביטול תעודות שכבר הונפקו.

בברכה,

אמנון בן עמי

העתק:
מר אליהו ישי, סגן ראש הממשלה ושר הפנים
עו"ד דניאל סלומון, יועץ משפטי
עו"ד נעמה פלאי, ממונה (כניסה לישראל)

רח' מסילת ישרים 6, ירושלים 94584,
טל: 02-6294855 פקס: 02-6294860

יש לך רשות לקבל שירות
www.piba.gov.il

תקנות מרשם האוכלוסין (תקופת תוקפן ופקיעת תוקפן של תעודות זהות), התשע"ב– 2011 –

נמחק: נוסח לדיון בוועדת החוקה חוק ומשפט ביום 28/12/2011

בתוקף סמכותי לפי סעיפים 26 ו-28א(2) ו-47 לחוק מרשם האוכלוסין, התשכ"ה - 1965[1] (להלן - החוק), ובאישור ועדת החוקה, חוק ומשפט של הכנסת, אני מתקין תקנות אלה:

הגדרות 1. בתקנות אלה –

"גוף ציבורי" – כהגדרתו בפסקה (1) להגדרה "גוף ציבורי" שבסעיף 23 לחוק הגנת הפרטיות, התשמ"א-1981[2];

נמחק: גורם מאשר

"מנפיק תעודות לאימות ממשלתי" – גורם ממשלתי המנפיק תעודות אלקטרוניות לאימות עבור רשות האוכלוסין לפי תקנות מרשם האוכלוסין (תעודה אלקטרונית לאימות), התשע"ב-2012[3];

נמחק: 2011

נמחק: גורם מאשר

"עובד מוסמך" – עובד רשות האוכלוסין או מנפיק תעודות לאימות ממשלתי ששר הפנים או ראש רשות האוכלוסין הסמיך לכך לענין תקנות אלה או חלקן;

"רשות האוכלוסין" – רשות האוכלוסין וההגירה.

תקופת תוקפן של תעודות זהות 2. (א) תקופת תוקפה של תעודת זהות היא עשר שנים מיום הנפקתה.

נמחק: / חמש עשרה שנים

נמחק: [redacted]

מעוצב:גופן: 10 נק', מודגש, גופן עבור עברית ושפות אחרות: 10 נק', מודגש, האר

(ב) על אף האמור בתקנת משנה (א), תקופת תוקפה של תעודת זהות הניתנת לבעל רשיון לישיבת ארעי לפי חוק הכניסה לישראל התשי"ב-1952[4] (להלן – חוק הכניסה לישראל), היא למשך תקופת הרשיון שניתן לו.

(ג) ראש רשות האוכלוסין רשאי לקבוע, בהחלטה מנומקת בכתב, כי בהתקיים אחת מהעילות המנויות להלן תינתן תעודת זהות לתקופה הקצרה מעשר שנים:

(1) החלו הליכים לביטול אזרחותו של בעל התעודה לפי חוק האזרחות התשי"ב-1952[5] (להלן – חוק האזרחות) או לביטול רישיון הישיבה שלו לפי חוק הכניסה לישראל;

(2) בעל התעודה ביקש בשנה האחרונה תעודת זהות שלוש פעמים או יותר במקום תעודה שאבדה, נגנבה או הושחתה.

נמחק:

מעוצב:גופן: 12 נק', גופן עבור עברית ושפות אחרות: David, 12 נק'

עילות לפקיעת תוקפה של תעודת זהות 3. (א) על אף האמור בתקנה 2, יפקע תוקפה של תעודת זהות בכל אחד מאלה:

נמחק: [redacted] המנפיקים [redacted] הנאמן

מעוצב:האר

נמחק:

נמחק: 1

(1) (א) לאחר שהודיע בעל תעודת זהות, שזהותו אומתה בהתאם לתקנה 2(3) לתקנות מרשם האוכלוסין (תעודה אלקטרונית לאימות), התשע"ב-2012, לעובד מוסמך כי קיים חשש ממשי כי נפגעה שליטתו בתעודת הזהות או כי נעשה שימוש שיבוש או שימוש לרעה בתעודת הזהות או במידע או בנתונים השמורים בה.

נמחק: או כי פרט מהפרטים המופיעים בתעודת הזהות או כשבב אינו מבוין

נמחק: ¶

(ב) במקרה שבו בעל תעודת הזהות הוא קטין או חסוי יתבקש גם נציגו, לאשר את ההודעה לפי פסקת משנה (א), ובלבד שהעובד המוסמך אימת את זהותו של הנציג ואת היותו נציג כאמור, הכל

נמחק: הורדו או אפוטרופסו ולחלן – נציגו, לפי הענין

---

[1] ס"ח התשכ"ה, עמ' 270; ס"ח התש"ע, עמ' 270.

[2]

[3]

[4]

[5]

בהתאם לנהלים שיקבע לעניין זה ראש רשות האוכלוסין. לעניין זה, "חסוי", "ינציג" – כהגדרתם בחוק הכשרות המשפטית והאפוטרופסות, התשכ"ב-1962.

(2) לאחר שמצא עובד רשות האוכלוסין, על פי מידע שנמסר ממשטרת ישראל או מגוף ציבורי כי קיים חשש ממשי כי נפגעה שליטתו של התושב בתעודת הזהות או כי נעשה שימוש לרעה בתעודת הזהות או במידע או בנתונים השמורים בה,

(3) התקבלה באחת מלשכות רשות האוכלוסין תעודת זהות שנמצאה שלא ברשות בעליה.

(4) [illegible] קבלת הודעה מראש רשות האוכלוסין בדבר פגם בחתימתו האלקטרונית המאובטחת, או במערכות החומרה והתוכנה המנפיקות את התעודות האלקטרוניות לאימות, שיש בו כדי לפגוע במהימנות חתימתו או במהימנות התעודות האלקטרוניות לאימות שהוא מנפיק,

(5) עם ביטולו או פקיעת תוקפו של רשיון ישיבה לפי חוק הכניסה לישראל או תקנות הכניסה לישראל, התשל"ד-1974 או עם ביטול אזרחותו של בעל תעודת הזהות לפי חוק האזרחות,

(6) עם החלפתה בתעודת זהות חדשה, לרבות בשל בלאי התעודה, שינוי או תיקון של הרישומים שבה; לעניין זה – למעט החלפת הספח בלבד.

(7) בשל מות בעל התעודה.

(ב) בחתקיים אחת העילות האמורות בתקנת משנה (א)(1) עד (6), יציין העובד המוסמך במערכות המחשב של רשות האוכלוסין את עילת הפקיעה ואת פקיעת תוקף תעודת הזהות.

(ג) (1) בהתקיים אחת העילות האמורות בתקנת משנה (א)(1) עד (5), יודיע עובד רשות האוכלוסין לתושב על פקיעת תוקף תעודת הזהות שבידו באמצעות הודעה טלפונית בתוך שני ימי עבודה; לא ניתן, לאחר ניסיון סביר, למסור את ההודעה טלפונית, תישלח לתושב, בהקדם האפשרי, הודעה בדואר רשום למענו הרשום במרשם האוכלוסין.

(2) בהודעה לפי פסקה (1) תצוין גם החובה להחזיר לרשות האוכלוסין את התעודה שפקעה בתוך ארבעה עשר ימים, התובה להחזיק בתעודת זהות, ומשמעות הפרתה, וכן המועד והמקום בהם ניתן לקבל תעודת זהות חדשה, ובלבד שאם התעודה הוגנפקה בהתאם לתקנה 8(ד) לתקנות הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגרי מידע, התש"א-2011, ניתן יהיה לקבל גם את התעודה החדשה בהתאם לאמור בתקנה זו.

3א. תושב שקיבל הודעה על פקיעת תוקף תעודת זהות שבידו חייב להחזירה לאחת מלשכות רשות האוכלוסין, תוך ארבעה עשר ימים מיום קבלת ההודעה.

הודעה על פגיעה בשליטה בתעודת זהות

4. בעל תעודת זהות שנודע לו כי קיים חשש ממשי כי נפגעה שליטתו בתעודת הזהות או כי נעשה בה שימוש או שימוש לרעה בתעודת הזהות או במידע או בנתונים השמורים בה, יודיע על כך מיד לעובד מוסמך באחת מהדרכים האלה:

(1) יתייצב באחת מלשכות רשות האוכלוסין ויודיע על כך;

מעוצב:גופן: 12 נק', גופן עבור עברית ושפות אחרות: David, 12 נק'

[illegible]

מעוצב:גופן: 12 נק', גופן עבור עברית ושפות אחרות: David, 12 נק'

נמחק: ** נוסח מוצע לבדיקה לקראת חתימה חבאת

נמחק: שנמסר

נמחק: ל

נמחק: מרשמך

נמחק: ומנוצא

נמחק: , או כי פרט מהפרטים המופיעים בתעודה או בשבב אינו נכון

[illegible]

מעוצב:גופן: 10 נק', גופן עבור עברית ושפות אחרות: 10 נק'

נמחק: הופש"ב-1952

נמחק: או

נמחק: ב

נמחק: אחד האירועים

מעוצב:לא האר

נמחק: האמורים

נמחק: מהא האירוע שארע

מעוצב:לא האר

נמחק: , ויודיע על כך לתושב בהתאם לתקנת משנה (ב).

מעוצב:מיושר לשני הצדדים

נמחק: ההודעת כאמור בתקנה משנה (ב) תימסר

נמחק: 48 שעות

נמחק: ב

נמחק: בהקדם האפשרי; ההי [1] ...

נמחק: של התושב

נמחק:

נמחק: X

נמחק: באחד אופן

מעוצב [2] ...

מעוצב [3] ...

מעוצב [4] ...

נמחק: תוך הזמן הנקוב בהודעה /

מעוצב [5] ...

נמחק: X

נמחק: , או כי פרט מהפרטים [6] ...

(2) יודיע על כך בטלפון למוקד קליטת הודעות שיוקם לעניין זה, ואשר יהיה זמין 24 שעות ביממה.

תחילה

5. תחילתן של תקנות אלה ביום ז' בשבט התשע"ב (31 בינואר 2012).

הוראת מעבר

6. על אף האמור בתקנה 2(א), תקופת תוקפה של תעודת זהות שניתנה לפני תחילתן של תקנות אלה היא עשר שנים מיום תחילתן.

נמחק: תחילתו של צו לפי סעיף 41(ג) לחוק הכללת אמצעי זיהוי ביומטריים ומאגרי זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשי"ע - 2009.

נמחק: 1

נמחק: ז חמש עשרה שנים

אליהו ישי

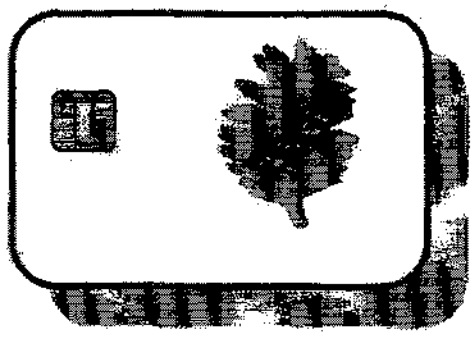
שר הפנים

_____ התשע"ב

(_____ 2011)

(חמ 3 - 4351)

שיקולים לקביעת זמן פקיעת תוקף של כרטיס תעודת הזהות



סקירת משמעויות של קציבת התוקף של תעודות הזהות

yoram@yoren.com

yoram@yoren.com

1. רקע ותקציר

בהמשך לדיון בקציבת תוקף לתעודות הזהות, להלן חוות דעת המפרטת את המשמעויות הטכנולוגיות של שימוש מתמשך בכרטיסי תעודת הזהות ופירוט של הסיבות לכך שיש לקבוע פקיעת תוקף לכרטיס. חוות הדעת כוללת סקירה של חלופות, ניתוח המשמעות של תקופת התוקף מבחינת אבטחה (פיזית ולוגית) וכן ניתוח של המשמעות של תקופת התוקף מבחינת אמינות. בנוסף לכך מפרטת חוות הדעת את המשמעות וההמלצות לגבי שמירה של תמונת פנים וטביעות אצבע עדכניות.

ההמלצה החד משמעית היא לקצוב את תקופת השימוש בכרטיס לעשר שנים, הן משיקולי אבטחה והן משיקולי עמידות פיזית של הכרטיס והשבב המשולב בו.

2. המצב בעולם

למעשה ניתן למנות שלוש חלופות אותן נוקטות המדינות השונות בנושא זה:

- קציבה של תוקף כרטיס תעודת הזהות לעשר שנים או פחות
- שימוש מתמשך, כאשר הכרטיס יוחלף באחר רק כאשר הוא אובד, מתבלה או נגנב.
- שילוב של השנים, על פי גיל מקבל התעודה

אין אף מדינה אירופאית שמאפשרת שימוש בלתי מוגבל בתעודת הזהות. כולן נוקטות מדיניות גורפת ואחידה של קציבת התוקף של כל התעודות לעשר שנים (ובמקרים רבים לחמש שנים בלבד), כאשר רק שתי מדינות מאפשרות שימוש על פי גיל נושא התעודה בעת הנפקתה. מדינות רבות מנפיקות כיום תעודות זהות ומסמכי זהות אחרים, כגון רישיונות נהיגה, כרטיסי בוחר או כרטיסי תושב, המבוססים על טכנולוגיית הכרטיס החכם. קציבת התוקף **איננה** תלויה בשאלה האם הכרטיס הוא כרטיס חכם או לא.

להלן ריכוז של תוקף תעודת הזהות במדינות שונות של האיחוד האירופאי או השוק האירופאי המורחב[1]:

המדינה	תוקף (שנים)	הערות	מנדטורי
בלגיה	5	דומה מאד לכרטיס תעודת הזהות המתוכנן	✓
אוסטריה	10		
קפריסין	10		✓
צ'כיה	10		✓
גרמניה	10		✓
ספרד	10	5 שנים מתחת לגיל 30, לתמיד מעל גיל 70	✓
אסטוניה	5	אחוז השימוש בכרטיס הוא הגבוה בעולם	✓
פינלנד	5		
הונגריה	10		✓
איטליה	10		
ליטא	10		
הולנד	5		✓
לוקסמבורג	10		✓
פורטוגל	5		✓

[1] מבוסס בעיקר על מידע מאתר האיחוד האירופאי הנקרא PRADO שמרכז מידע ממדינות שונות על מסמכי זיהוי, לא רק של האיחוד.
כתובת האתר: http://prado.consilium.europa.eu/en/homeIndex.html

פולין	10		✓
רומניה	10	לתמיד מעל גיל 55	✓
סלובקיה	10		✓
שוודיה	5		
שוויץ	10		
בוסניה הרצגובינה	10		✓

yoram@yoren.com

3. אבטחה פיזית של הכרטיס

סימני הביטחון הראשיים בכרטיס תעודת הזהות כוללים את הרכיבים הבאים:

- דפוס רקע ביטחוני, המתבסס על קווים דקים מאד ועל טקסט זעיר (microtext)
- גרפיקה עם מאפיינים מוגדרים (כדוגמת תבנית Guilloché) שמקשים על העתקה או סריקה
- שימוש בצבעי בסיס בגוונים שקשה לייצר
- מעברי צבע הדרגתיים שקשה לחקותם
- שימוש בקווים בעוביים שונים במקום צפיפות של נקודות כמו דפוס מקובל ליצירת גוונים (tonality)
- חריטת לייזר לצורך מילוי הפרטים
- CLI[2] - רכיב המציג חילוף בין תמונה מוקטנת למספר הזהות על פי זווית הצפייה
- OVI[3] - גרפיקה של דגל המדינה שצבעה משתנה בהתאם לזווית הצפייה
- זריחות שונות כאשר הכרטיס מואר באור אולטרה סגול או אינפרה אדום
- הרכב כימי ייחודי של חלק מהצבעים המשמשים להדפסה
- הולוגרמה מורכבת, הנמצאת בשכבה פנימית וכוללת מיקרוטקסט
- הטמנה של מידע טקסטואלי בתמונה המודפסת, שניתן לראותו בעזרת עדשה מיוחדת
- זריחות שונות כאשר הכרטיס מואר באור אולטרה סגול
- הבלטה (embossing) של טקסט זעיר

כמו הרבה רכיבי אבטחה, גם סימני הביטחון הנ"ל סובלים משחיקה של רמת האבטחה לאורך זמן. רובם ככולם מתבססים על הקושי להשיגם או לייצרם אך לא ניתן להניח לאורך זמן שלא תהיה זליגה של חומרים או טכנולוגיות כאלו לשוק החופשי ומכאן הדרך לידי הזייפנים קצרה. הרבה מהשיטות הנ"ל זוכות לשימוש נרחב לצורך הגנה על קניין (brand protection)[4] ודי לראות תווית של בקבוק מים מינרליים יקרים או אריזה של תרופה יקרה כדי להבין שנעשה שימוש בשיטות דומות. בניגוד לשוק התיעוד, שרובו ככולו הוא שוק של לקוחות ממשלתיים, השוק של הגנה על קניין כולל אלפי ועשרות אלפי יצרנים שאינם אמונים על שיטות אבטחה ואינם יכולים או רוצים להשקיע משאבים בהגנה על חומרי הגלם הרגישים.

המענה היחיד למצב מורכב זה הוא יצירה של "מטרה נעה" לזייפנים, כלומר ריענון וחידוש של אמצעי האבטחה כאשר חלף זמן והם אינם מספקים יותר הגנה נאותה. מסיבה זו ראוי וחשוב לעדכן ואף להחליף אחת למספר שנים את כרטיסי תעודת הזהות כדי להבטיח שהם עדיין חסינים דיים מפני זיופים. כיום רואים זמני מחזור של בין חמש לעשר שנים בין דורות של תיעוד, ומדינות רבות מתחילות לחשוב על הדור הבא מיד

---

[2] CLI = Changeable Laser Image
[3] OVI = Optically Variable Ink

[4] שילוב של סימני ביטחון לצורך מניעת זיופים של מותגים

כאשר הדור הנוכחי מתחיל בהנפקה. יתרה על כך, יש חשיבות רבה לכך שהצד המגן (המדינות המנפיקות תיעוד לאומי) יהיה היוזם ויקדים את הצד התוקף (זייפנים וארגוני פשיעה למיניהם).

yoram@yoren.com

4. אבטחה לוגית של הכרטיס

מלבד האבטחה הפיזית של הכרטיס מכיל כרטיס זה שבב, בדומה לתעודות הזהות של מדינות רבות אחרות[5]. השבב מכיל מנגנוני הגנה מסוגים שונים ומגוונים, המתבססים רובם ככולם על אלגוריתמי הצפנה מסוגים שונים. ניתן לחלק מנגנונים אלו לשתי משפחות עיקריות:

4.1. מנגנוני הגנה על המידע שבתעודה

מנגנונים אלו מאפשרים "לחתום" על המידע בתעודת הזהות או להגביל את הגישה למידע מסוים, על פי רגישותו. הם מאפשרים למי שעושה שימוש בתעודה לדעת, ברמת סמך גבוהה מאד, (1) שהמידע אכן יצא ממערכי המחשוב של המדינה המנפיקה (2) שהמידע לא עבר שינויים מאז שנרשם לשבב.

ניתן לראות דוגמה למנגנון המשמש לבקרת גישה באותו מנגנון הצפנה שמאפשר לשבב לדעת שלפניו קורא חוקי הפונה אליו, לפני שישחרר אליו קובץ רגיש כדוגמת הקובץ של טביעות האצבע.

4.2. תעודות דיגיטאליות

כרטיס תעודת הזהות הפיזי, כמו כרטיסי זהות רבים בעולם, יכול להכיל תעודות דיגיטאליות. תעודות אלו הן קובצי מחשב המקושרים למפתחות הצפנה שנמצאים בכרטיס ונשמרים בתוכו בצורה מאובטחת מאד. תעודות "וירטואליות" אלו מאפשרות הזדהות מקוונת ברמת אבטחה גבוהה מאד (בניגוד למנגנונים מקובלים של שם משתמש וסיסמה, שאינם מאובטחים כלל וחשופים מאד לתקיפה). ניתן גם להשתמש בתעודות דיגיטאליות כאלו לצורך חתימה אלקטרונית.

בניגוד לתחומים טכנולוגיים אחרים, ובפרט שוק המכשירים הסלולאריים, שוק הכרטיסים החכמים הוא שוק מאד בוגר מבחינת אבטחה. יש בשוק זה מנגנוני בקרה והסמכה לתקני אבטחה ויש היצע ניכר של פתרונות טובים מאד (בניגוד כאמור לשוק ה-smartphones, שיודע לספק פונקציונאליות מתקדמת אולם אבטחה אפסית). אחד המאפיינים הבולטים של תחום האבטחה הוא משחק "החתול והעכבר" המתקיים באופן תמידי בין המגן והתוקף. אם בשוק אחר מדובר על זמני מחזור של חודשים ספורים ואף פחות מזה מבחינת אבטחה, הרי שבשוק הכרטיסים החכמים מדובר על מחזור של שנים. ארגונים רבים נוקטים מדיניות של מחזור חודשי לגבי עדכונים של מערכות ההפעלה המותקנות על המחשבים שלהם, ולעיתים קרובות עדכון שוטף של מערכת ההפעלה, ללא המתנה להצטברות של עדכונים. גרסאות מתוקנות של מערכות ההפעלה של טלפונים חכמים יוצאות לשוק אחת למספר חודשים כאשר במקרים רבים העדכון נובע מדרישות אבטחה. מערכות pay TV לצורך הגנה על תוכן טלוויזיוני, המתבססות רובן ככולן על כרטיסים חכמים, מתעדכנות אחת

[5] לדוגמה (רשימה חלקית מאד): בלגיה, גרמניה, ספרד, אסטוניה, פינלנד, איטליה, ליטא, הולנד, פורטוגל, שוודיה

לשנה וחצי או שנתיים. כרטיסים בנקאיים מתעדכנים גם הם אחת לשנתיים או שלוש, למרות העלויות הכרוכות בכך. **המשמעות היא ש"משיכת" הזמן מעבר לעשר שנים איננה זהירה מבחינת אבטחה.**

זהירות זו חייבת להיות קו מנחה מבחינת מדיניות האבטחה, מהשיקולים הבאים:

- **פרסומים שוטפים של מחקר אקדמי היוצרים "כרסום זוחל"** במנגנוני ההצפנה

אלגוריתמי ההצפנה המקובלים כיום הם טובים מאד ולמעשה אינם מהווים בעיה כשלעצמם. גם אם נניח ש-Moore's law ימשיך להיות תקף לאורך זמן ושכוח החישוב הזמין אכן יכפיל את עצמו כל שנה וחצי, הרי שיש היום אלגוריתמים זמינים שיכולים להיות טובים וחזקים לעשרות רבות של שנים. למרות זאת, יש מפעם לפעם פרסומים מדעיים שמוכיחים (או טוענים) כי שולי הביטחון של אלגוריתם זה או אחר אינם כה גדולים כפי שחשבו בתחילה. במקרים נדירים מאד מתגלה חולשה כלשהי של ממש. תהליך זה ממשיך בדרך כלל עד לנקודה בה השימוש באלגוריתם אינו מומלץ יותר ויש לעבור למנגנון חליפי. **ברוב המקרים לא מדובר בקעקוע מוחלט של האלגוריתמים אלא בכרסום זוחל בחוזקם הקריפטוגרפי.**

- גילוי של **טעויות מימוש**

החוזק הגבוה של אלגוריתמי ההצפנה אינו ערובה יחידה לכך שמערכת המתבססת עליהם היא אכן חסינה באופן מוחלט לתקיפה. גם המימוש בפועל של האלגוריתם המתמטי התיאורטי צריך להיות חסין דיו ולא לגרום לזליגה שלא מדעת של מידע רגיש. לדוגמה, פרק הזמן שלוקח כל תהליך חישובי חייב להיות אחיד ובלתי תלוי במידע המוצפן או במפתח ההצפנה. אם כלל זה אינו מקוים ניתן לפרוץ את המערכת באמצעות מדידת זמן התגובה ומשך התהליכים, ומהם להסיק את מפתח ההצפנה או המידע טרם הצפנתו.

המפרט של כרטיסי תעודת הזהות, כמו גם עמידתם בתקני אבטחה מחמירים, ממזערים את הסיכוי לחשיפה של תקלות מימוש כאלה אולם אינם מבטלים אותן לחלוטין. ההסתברות לכך מאד נמוכה אולם אינה אפס. לכרטיס, כמו גם למערכת ההפעלה שלו, יש כאמור הסמכה על פי תקני אבטחה מתקדמים ממשפחת ה-Common Criteria. תקן אבטחה זה התקבל גם כתקן בינלאומי בשם ISO/IEC 15408[6]. הסמכה זו כוללת **ניסיונות תקיפה בפועל** נגד הכרטיס, על ידי מעבדות בדיקה בלתי תלויות. למרות זאת, אם מתגלה שיטת תקיפה חדשה, שלא נבדקה בעבר, יתכן מצב של כרטיס שיהיה חשוף לתקיפה. גם כאן, המענה המעשי היחיד הוא עדכון שוטף של כרטיסים לגרסאות מתקדמות יותר. כדי להבטיח שעדכון כזה יגיע לאוכלוסייה רחבה ככל האפשר יש לקצוב את פרק הזמן בו ניתן לעשות שימוש בכרטיס.

[6] יש מדרג של תקנים מבחינת חשיבותם, כאשר התקנים החשובים ביותר הם התקנים הבינלאומיים, הבאים בתור הם תקנים יבשתיים ואחריהם תקנים מדינתיים.

- התפתחות של תקיפות

אחד ממומחי ההצפנה המובילים בעולם, ברוס שנייר[7], טבע אמרה ידועה לאנשי האבטחה האומרת:

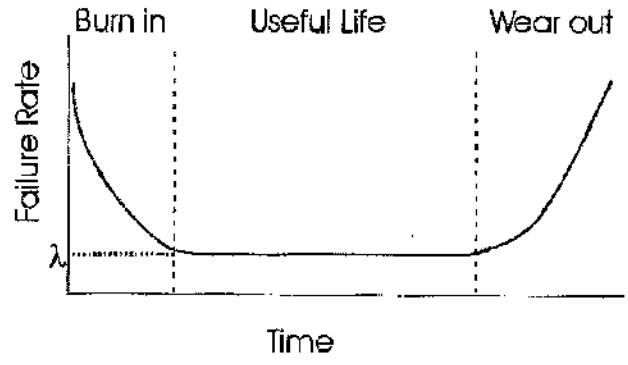
"Attacks always get better; they never get worse"

המשמעות היא שככל שעובר הזמן, שיטות התקיפה הולכות ומשתכללות. מנגנון הגנה שהיה יעיל מאד בעבר יהיה פחות יעיל כעבור מספר שנים ויתכן שיהיה פרוץ לחלוטין כעבור עוד מספר שנים. שוב, המענה המעשי הוא התקדמות עם הזמן ושכלול הכרטיס כדי שיוכל להתמודד עם תקיפות שהולכות ומשתפרות.

[7] Bruce Schneier, http://www.schneier.com

5. אמינות

מלבד נושאי האבטחה יש לשים לב שגם הכרטיס עצמו, הן ברמת הפלסטיקה והן ברמת השבב, אינו יכול להחזיק מעמד יותר מעשר עד שתים עשרה שנים. ככל רכיב אלקטרוני או מערכת טכנולוגית אמינותו תתנהג כמו "גרף אמבטיה" (bathtub curve):



בתחילה קצב התקלות הוא גבוה ויש רכיבים שמתקלקלים מהר מאד, לאחר מכן יש תקופה ממושכת של קצב תקלות נמוך (תקופה של תקלות אקראיות בלבד) ולבסוף, כתוצאה משחיקת הרכיב קצב התקלות עולה. הבדיקות המחמירות של הכרטיסים בתהליך הייצור גורמות לכך שאותם כרטיסים שמתקלקלים בהתחלה נפסלים ואינם מגיעים לידי האזרחים, כך שהגורם המשמעותי הוא אותם כרטיסים שמיצו את אורך החיים הסביר ונכנסו לתקופה שבה קצב התקלות עולה משמעותית.

גורם משמעותי בקביעת רמת האמינות של הכרטיסים הוא צורת השימוש ובמיוחד תדירות השימוש. דפוס השימוש המקובל בעולם לכרטיסי תעודת זהות כולל שמירה שלהם בארנק או בצורה מוגנת וקצב שימוש נמוך משמעותית יחסית לכרטיס בנקאי. זוהי אחת הסיבות שבגללה ניתן לקבל מהם אורך חיים של קצת יותר מעשר שנים, בניגוד לכרטיסים בנקאיים למשל, שקצב שחיקתם גבוה בהרבה.

5.1. כרטיס הפלסטיק

כרטיס תעודת הזהות מיוצר מחומר פלסטי מתקדם וחזק מאד הנקרא פוליקרבונאט. למרות החוזק העצום של חומר זה תיתכן תופעה של היפרדות השכבות (delamination), ניתוק השבב מהכרטיס הפלסטי או התפתחות של סדקים. כרטיס תעודת הזהות מתוכנן לאורך חיים של קצת יותר מעשר שנים, בתנאי שימוש רגילים. השוק איננו מציע כרטיסים לפרק זמן ארוך יותר ולמעשה אין דרישה כזו מצד לקוחות. אפילו שוק התיעוד הלאומי או כרטיסי ביטוח הבריאות אינם זקוקים לכרטיסים עם אורך חיים גדול יותר ולכן אין בשוק מוטיבציה לפתחם.

הגורמים העיקריים לשחיקת הכרטיס הם:

- כיפופים ומאמצים מכאניים
- החיכוך בעת הכנסה לקורא והוצאה
- קרינת שמש ובעיקר קרינת UV
- חשיפה לכימיקלים (כגון חומרי ניקוי ובעיקר סבון כביסה)
- חשיפה לחום גבוה (כרטיס שהושאר ברכב חונה ביום קיץ)
- חולשה של נקודות מסוימות בכרטיס כתוצאה מסימני ביטחון (כגון הבלטה של טקסט המקובלת מאד בכרטיסי אשראי)
- נזק לכרטיס בתהליכי הייצור, המתבטא כעבור מספר שנים, כגון שימוש בקרינת UV כדי למצק דבקים או בועות אוויר בין השבב לפלסטיק שגורמות להיפרדותם בעתיד.

5.2. השבב

הגורם העיקרי המשפיע על אורך חיי השבב הוא העמידות (durability) של רכיב הזיכרון שלו. טכנולוגיית הזיכרון המקובלת ביותר בשבבים של כרטיסים חכמים היא זיכרון מסוג EEPROM[8]. זיכרון זה מבוסס על מטען אלקטרונים ניכר הלכוד בתוך תא הזיכרון כדי לקבוע האם תא זה ייצג "0" לוגי או "1" לוגי. הבחירה בטכנולוגיה זו נובעת בין היתר מהיכולת לבנות תא זיכרון כזה שלא ניתן לקרוא את תוכנו בקלות באמצעות מיקרוסקופ אלקטרוני או לגרום לו לשגיאות מכוונות לצורך תקיפת הכרטיס[9]. החיסרון של זיכרונות כאלו הוא שחיקתם ואמינותם ההולכת ויורדת ככל שנעשה בהם יותר שימוש.

בנוסף יכול השבב להיזק ממאמץ מכאני או מפריקה של חשמל סטאטי (במיוחד במזג אוויר יבש). כרטיס תעודת הזהות המתוכנן הינו כרטיס מגע וגורם כשל נוסף הוא החיבור בין השבב למגשת.

---

[8] EEPROM = Electrically Erasable & Programmable Read Only Memory

[9] טכניקת תקיפה מקובלת, הנקראת fault injection, ומתבססת על גרימת שגיאות מכוונות לרכיב הנתקף. שגיאות כאלו יכולות לגרום לעקיפה או ביטול של מנגנון הגנה שהיה פועל אם הכרטיס היה מופעל בצורה תקינה.

6. עדכניות המידע החזותי והביומטרי

קצב השינוי של מידע ביומטרי הוא נמוך מאד אך לאורך שנים יש שינויים במידע זה. השינויים יכולים לנבוע משינויים ניווניים, שינויים טבעיים של הזדקנות, מחלות, פציעות או חשיפה לחומרים מסוימים. לשינויים אלו יש השפעה הן על הזיהוי החזותי והן על הזיהוי הממוכן (הביומטרי). הפתרון הטריוויאלי לעניין זה הוא עדכון תקופתי. נושא זה נדון בהרחבה בעת גיבוש התקן הבינלאומי לדרכונים, על ידי ארגון התעופה האזרחית הבינלאומית[10]. על פי ארגון זה, התוקף המרבי לדרכון צריך להיות עשר שנים, כדי לשמור את התמונה עדכנית (הן המודפסת והן בשבב).

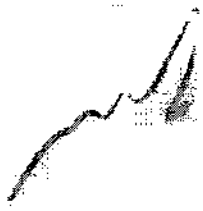
[10] International Civil Aviation Organization = ICAO, גוף המסונף לאו"ם ופועל מכוח אמנה שגם מדינת ישראל חתומה עליה.

7. סיכום והמלצות

לאור כל האמור לעיל יש לחייב החלפה של הכרטיס לאחר עשר שנים לכל היותר. שימוש בכרטיס לזמן ממושך יותר יגרום לפגיעה ניכרת באבטחה של הכרטיסים ולכשלים בהפעלתם.

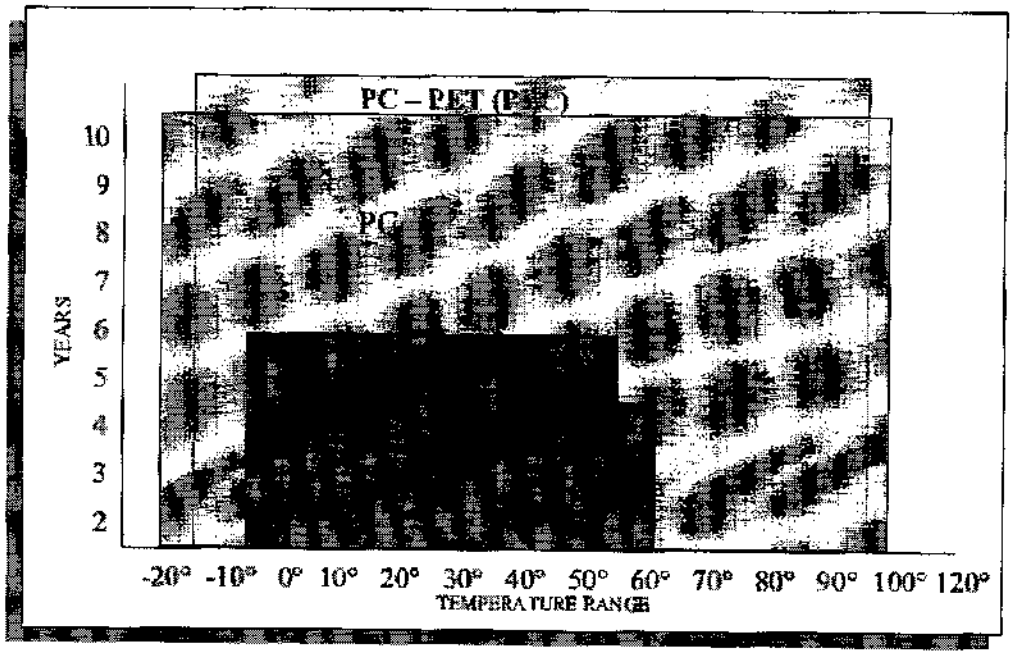
בברכה

יורם אורן



8. נספחים

8.1. השוואה בין סוגי פלסטיק שונים

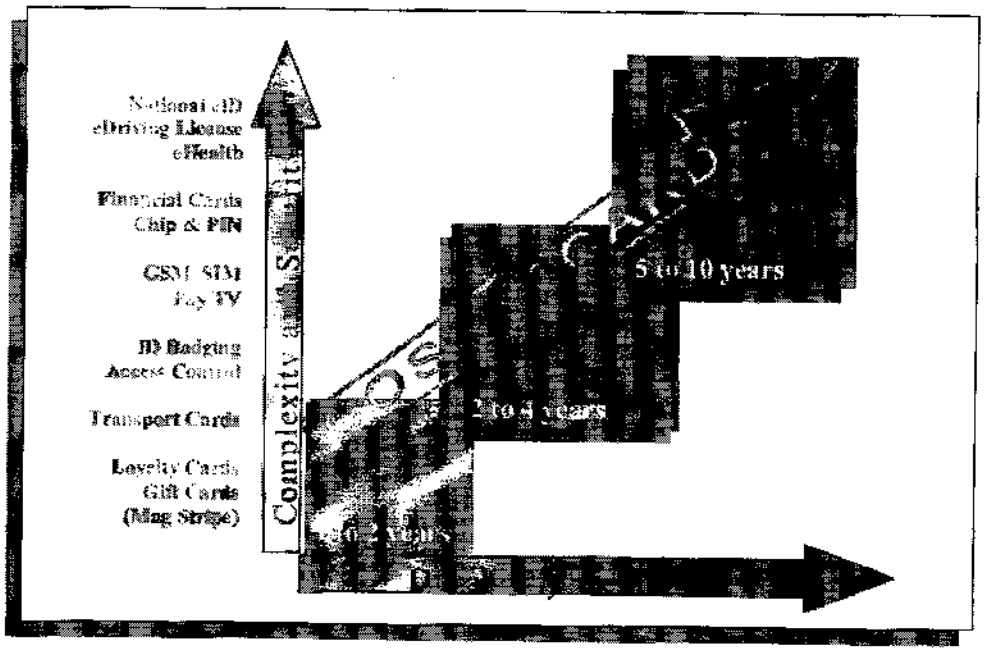


מתוך מאמר שפורסם על יד חברת Datacard בשם:

"DURABILITY OF SMART CARDS FOR GOVERNMENT EID"

ניתן לראות שכרטיסים המבוססים על פוליקרבונאט (PC) מאפשרים אורך חיים של קצת יותר מעשר שנים, בעוד יתר הסוגים (פוליאסטר ופולי ויניל כלוריד PVC) אינם מאפשרים זאת. יש לציין שפער העלות בין פוליקרבונאט ו-PVC הוא כ-7 לאחד. כרטיסים משולבים מפוליקרבונאט וחומר נוסף הנקרא PET (Polyethylene terephthalate, החומר ממנו עשויים בקבוקי משקה) יכולים להחזיק מעמד כ-12 שנים אולם לא ניתן ליישם עליהם חלק גדול מסימני הביטחון, באותה מידה שניתן ליישמם על כרטיס שמורכב רק מפוליקרבונאט.

8.2. השוואה בין סוגי כרטיסים שונים



מתוך מאמר שפורסם על יד חברת Datacard בשם:

"DURABILITY OF SMART CARDS FOR GOVERNMENT EID"

ניתן לראות בשרטוט את יחסי הגומלין בין רמת האבטחה, דרישות העמידות, המחיר והסיבוכיות של כל אחד מסוגי הכרטיסים המקובלים (כרטיסי מועדון לקוחות, כרטיסי תחבורה ציבורית, כרטיסי עובד, כרטיסי SIM, כרטיסי ממירי TV, כרטיסים בנקאיים וכרטיסי תעודות זהות).