



מדינת ישראל

משרד האוצר - אגף החשב הכללי
ועדת האינטרנט הממשלתית
WWW.ITPOLICY.GOV.IL

שם המסמך : כרטיס חכם וממשל זמין
תאריך כתיבה : 13/01/98
גירסה : 1.0

שם לאחזור : docs/smrtcard.doc
כותב המסמך : ויקטור איררה

מבוא

במבוא לספר התקציב לשנת 1998, קבע נשיא ארה"ב ביל קלינטון: "הממשל מעוניין לאמץ וליישם טכנולוגיה של כרטיסים חכמים למטרות רבות, בהן טיולים, רכישות בקנה מידה קטן ובדיקת זהות בכניסה לבניינים ממשלתיים".

דברי קלינטון, כמו גם המסמך שבו בחר הנשיא לכלול אותם, מעידים על החשיבות העצומה שמייחס הממשל האמריקני לחזון הכרטיסים החכמים, או כפי שהוגדר על ידי סגן הנשיא אל גור - "חזון הממשל הזמין".

לפי גור, יאפשרו הכרטיסים החכמים לכל אזרחי ארה"ב לקבל שירותי ממשל באופן ישיר ומידי, באמצעות תשתיות תקשוב נגישות מהבית, המשרד, סוכנות הדואר, תחנות מידע עצמאיות, בתי הספר או הספריות השכונתיות.

בארה"ב כבר חדלו מזמן להסתפק בדיבורים, ככל שדברים אמורים בכרטיסים חכמים. במסגרת פרויקט ממשלתי, המכונה Access America, הוגדרה תוכנית רב-שנתית שיצאה לדרך בנובמבר 97 ונועדה לספק תחילה לכל עובד מדינה כרטיס חכם אחד, רב שימושי ונגיש לכל משרדי הממשל. במקביל, החל בארה"ב תהליך חקיקה למיסוד ומתן תוקף של חתימות דיגיטליות וטכניקות אימות אלקטרוניות, ולשם כך אף הוקם גוף ממשלתי מיוחד בשם NASA.

(National Association Of Certification Authorities), המסמך גורמים המעוניינים לתת שירותי אימות אלקטרוניים בארה"ב.

גם מדינת ישראל נדרשה לסוגיית הכרטיסים החכמים. בגיבוש המסמך "היערכות מדינת ישראל לעידן המידע" נתפס הכרטיס החכם כמפתח לממשל זמין: "כל אזרח במדינת ישראל יקבל אמצעי, שיאפשר זיהוי אמין בעת פנייה למערכות ממשל המחייבות הזדהות. תנאי זה הינו מקדמי והכרחי להשגת יעדי הממשל הזמין".

נכון לעכשיו, הכרטיס החכם נתפס עדיין יותר כחזון ופחות כמציאות יומיומית. ברחבי העולם הורצו במהלך 1997 מאות פרויקטים "חכמים", אך מדינות בודדות בלבד מיישמות כיום הפעלה המונית ושגרתית של כרטיסים חכמים.

לא מעט מכשולים ניצבים עדיין על דרכו של הכרטיס החכם מחזון למציאות: סוגיות משפטיות (שהפכו רלבנטיות מאוד עם הנפקתם של הארנקים האלקטרוניים); סוגיות של אבטחת מידע (שהועלו בהקשר של העברת כסף ומידע רגיש באינטרנט); סוגיות אתיות (שמירה על צנעת הפרט, אופן רישום המידע על גב הכרטיס ואבטחת הסודיות אחר רישום/אי רישום פעילויותיו של מחזיק הכרטיס); וגם סוגיות טכנולוגיות (בעיקר התלות בספק של היישום/מערכת ההפעלה, וכן היעדר תקנים אחידים מוסכמים).

מכשולים כאלה ואחרים מנעו עד כה את פריצתם הצפויה של הכרטיסים החכמים למודעות הציבור, כמו גם את הפצתם ההמונית.

מהו כרטיס חכם?

הכרטיסים המגנטיים, המוכרים לנו מחיי היומיום, הם כרטיסים פסיביים, המאחסנים כמות מידע קטנה מאוד.

כרטיס חכם, שגודלו על פי רוב זהה לזה של כרטיס אשראי, מכיל שבב המעניק יכולת אחסון מידע ועיבודו - והינו מחשב (CPU) לכל דבר. תכונה זו מבדילה את הכרטיס החכם מהכרטיס המגנטי, שהינו בעל יכולת אחסון, אך נטול יכולת עיבוד עצמאית ומשמש כמתווך מול מאגר מידע מרכזי.

איזה כרטיסים חכמים קיימים כיום?

הכרטיסים נחלקים על פי סוג השבב שקיים בהם ולפי אופן הקריאה של המידע.

א. חלוקה לפי סוגי שבבים:

1. כרטיס זיכרון (Memory Card), המכונה גם Chip Card, משתמש ביכולת אחסון גבוהה, אך אינו עוסק בעיבוד עצמאי, בניגוד לכרטיס החכם "האמיתי". כרטיסים אלה מכילים בין 1 ל-8 קילוביט זיכרון, בתצורת EPROM או EEPROM, ומשמשים כיום בעיקר ככרטיסים כספיים פשוטים (למשל, כרטיסי הטלכרט ברוב מדינות אירופה). עלות ייצורם מסתכמת בפחות מדולר לכרטיס.
2. כרטיסים חכמים (Smart Card) בעוצמות שונות, שעלותם נעה בין 2 ל-20 דולר. גודל הזיכרון של הכרטיסים החכמים נע בין 8 ל-64 קילוביט, והם מסוגלים לאחסן גם מידע ביומטרי (המאפשר זיהוי בעל הכרטיס באמצעות טביעת אצבעות, רשתית העין או קול).

ב. חלוקה לפי סוגי קריאה:

1. כרטיסי מגע (contact) - דורשים מגע פיזי עם קורא כרטיסים. כרטיסים אלה נמצאים בשימוש בעיקר במערכת הבנקאית.
2. כרטיסים ללא מגע (contactless) - די בקרבתם למתקן כדי להפעילם. נמצאים בשימוש בעיקר בתחום התחבורה, שם יש צורך במעבר מהיר ככל האפשר של נוסעים רבים.
3. כרטיס משולב (Combicard) - נמצא עדיין בשלבי פיתוח, ויהיה ניתן להפעלה במגע וללא מגע על אותו שבב. באמצעות הכרטיס המשולב ניתן יהיה לבצע מגוון של יישומים.

שימושים עיקריים לכרטיסים חכמים

היכולת של הכרטיס החכם לעבד מידע, ולא רק לאחסן אותו, עושה אותו כלי יעיל להרצה של אלגוריתמים, הדרושים לצורכי הצפנה וזיהוי. הכרטיס הופך אקטיבי בזכות יכולתו למדר את הגישה למידע שבו, ולבצע אינטראקציות מורכבות עם המכשיר ה"קורא" אותו (מימוש פרוטוקולים הכרוכים בתקשורת אינטראקטיבית של "שאלות ותשובות", שימוש במספרים אקראיים וכדומה).

השימושים של הכרטיס החכם בעולם רבים, וחלקם יפורט בהמשך. עם זאת, ניתן לחלקם לשלושה תחומים עיקריים:

1. זיהוי - למשל, פרטיו האישיים של אזרח בכרטיס המשמש כתעודת זהות, או פרטיו של חבר במועדון לקוחות/חברת תעופה.
2. מידע - למשל, תיק רפואי, פרטי רשיון עסק (סוג עסק, שעות פתיחה, שטח

מדרכה וכו'), או מספר הנקודות/המיילים שצבר חבר במועדון הלקוחות/חברת התעופה.

3. **ארנק אלקטרוני** - למשל, ביצוע "רכישות קטנות" (רכישת עיתון, שיחת טלפון מקומית, נסיעה באוטובוס וכד'), שאין אפשרות או כדאיות כלכלית לבצען באמצעות כרטיס אשראי או צ'ק.

כרטיסים חכמים מסייעים גם במניעת זיופים של כרטיסי אשראי מגנטיים, ומייעלים את הטיפול בהם. לדוגמה, שבו שהוכנס בכרטיס אשראי במדינות אירופה מכיל קוד סודי לזיהוי אישי, ומאפשר לספק השירות או המוצר לאמת את זהות מחזיק הכרטיס באופן מקומי, ללא צורך בתקשורת מקוונת למחשב מרכזי. קורא הכרטיס בודק באופן עצמאי את הקוד שבכרטיס מול הקוד המוקש על ידי מחזיק הכרטיס. שיפור זה הפחית במידה משמעותית את היקף הזיופים של כרטיסי האשראי והכרטיסים הבנקאיים המגנטיים באירופה.

היותו של הכרטיס נישא בכיס מחד, ובעל כוח חישובי ניכר מאידך, מאפשרת לו לבצע פעולות שאינן ברות יישום באופן אחר. נציין כאן לדוגמה יישום מקורי של ממשלת איטליה, שלא היה ניתן לביצוע אלמלא הכרטיס החכם.

בצפון איטליה נוצרה בעיה: בהיות מחיר הדלק זול בהרבה ביוגוסלביה לשעבר מאשר באיטליה, נהגו התושבים הקרובים לגבול הצפוני למלא דלק אצל השכנים היוגוסלביים. ניצול חכם של הכרטיסים האישיים שינה מנהג זה: הזנת המרחק בין ביתו של האזרח לגבול על גבי הכרטיס החכם, בשילוב עם מדיניות הקובעת מחיר דיפרנציאלי לדלק עבור תושבים הקרובים לגבול, יצרו כדאיות לתדלוק מקומי ושמרו על רווחיותן של תחנות הדלק האיטלקיות.

מגמות עתידיות

1. התפלגות הכרטיסים בעולם (במיליוני כרטיסים) לפי יישומיהם:

שנה	1996	2000
כרטיסי טלפון	780	1400
בנקאות	120	500
בריאות	65	400
תחבורה	35	400
GSM	30	120
טלויזיה/סרטים	20	120
זיהוי/כ. תושב	4	300
משחקים	2	300
חניה	2	60
מסחר אלקטרוני	2	200
סה"כ	1,060	3,800

2. התפלגות לפי סוג השבב:

כרטיסי הזיכרון (Chip Card), שהיוו 75% מכלל הכרטיסים החכמים בעולם בשנת 1996, יירדו ל 45%- בלבד בשנת 2000. סקר מקיף שפורסם באנגליה (<http://www.sjb.co.uk>), קובע ששוק הכרטיסים החכמים בעולם גדל בקצב שנתי של 50%.

3. מאפיינים טכניים:

בעולם קיימים כיום יצרני שבבים מעטים יחסית לכרטיסים חכמים. בין הגורמים העיקריים בתחום זה ניתן למנות את סימנס, פיליפס, מוטורולה, אינטל, היטאצ'י, טקסס אינסטרומנטס, טושיבה ואס. גי. אס תומסון.

הטכנולוגיה, לעומת זאת, מתקדמת בקצב מסחרר: בשנת '97 הוגבלה יכולת מהירות המעבד (CPU) שעל הכרטיס ל-4 MHZ, ולטיפול ב-8 BITS. גודל הזיכרון הזמני (RAM) הגיע ל-KB

256; גודל הזיכרון ה-NON-VOLATILE וגודל הזיכרון ליישומים (EEPROM) הגיעו ל-8 KB כל אחד.

בשנת '98 תגיע מהירות המעבד (CPU) שעל הכרטיס ל-20 MHz, בטכנולוגיית RISC. הכרטיס יהיה מסוגל לטפל ב-32 BITS, פי ארבעה מבשנת '97. זיכרון ה-RAM יגיע ל-1 KB; גודל זיכרון ה-NON-VOLATILE יגיע ל-64 KB ועוד 32KB ליישומים (ROM).

שיפור זה של עוצמת החומרה, בנוסף לתצורת תכנה המבוססת על JAVA, יאפשר פיתוח מהיר של יישומים מתקדמים בכרטיסים החכמים.

4. כיווני התפתחות עיקריים:

א. קביעת תקנים אוניברסליים (Interoperability) -

עד כה הונפק כל כרטיס חכם על ידי מנפיק (Issuer) אחד, והיישומים שבו (לרוב יישום אחד) היו קשורים ומותנים תלות מוחלטת במערכת ההפעלה (ולרוב היו חלק בלתי נפרד ממנה). עובדה זו מנעה נגישות של הציבור הרחב ליישומי הכרטיס, ורוב הפרויקטים יועדו לאוכלוסייה מוגדרת (סטודנטים בתחום הקמפוס, נופשים בכפר נופש וכד').

כיום יש ניסיון להתאגדות רחבה של חברות וגופים מובילים בתחום, בהם אוראקל, י.ב.מ., מיקרוסופט, אמריקן אקספרס, גיי.טי.אי, דויטשה טלקום, נורת'ל ובל קנדה. חברות אלו ואחרות מעונינות למסד את ה-INTEROPERABILITY במסגרת GCA: GLOBAL Chipcard Alliance. בכנס חברי ה-GCA בנובמבר '97 סוכם, בין השאר, על יצירת חותמת "GCA-approved" לכרטיסים וקוראים העומדים בדרישות, כדי להבטיח שיוכלו לעמוד לשימושו של הציבור הרחב.

ב. מעבר לכרטיסים מרובי יישומים (Multiapplication) -

ניצולו המלא של הכרטיס החכם כרוך, לעתים, בהפעלת מספר יישומים על אותו הכרטיס, לדוגמה: כרטיס תושב (המכונה גם City Card) ובו פרטיו האישיים של התושב (לרבות זיהויו בתמונה או באמצעי ביומטרי), יכול לשמש גם כארנק אלקטרוני ברכישות קטנות, וכן כמאגר מידע ובו מידע רפואי למקרה חירום, נתונים על זכאות להנחות וכד'. כרטיס כזה יוכל לשמש גם לביצוע העברות כספיות ואחרות באינטרנט.

בימים אלה נמצא בפיתוח ה-Java Card, שיספק הפרדה בין היישום למערכת ההפעלה, ויאפשר כתיבת היישום פעם אחת בלבד ויכולת הפעלתו מכל כרטיס. פורום העוסק בפיתוח כרטיס הג'אווה כולל את חברות סאן מיקרוסיסטמס, גיימפלוס ואחרות.

הכרטיס החכם בשירות הציבורי

1. בריאות

הפרויקט הבשל והמוטמע ביותר לתיק רפואי הוא Santal - הכרטיס הרפואי שהונפק ל-60,000- תושבי SAINT - NAZAIRE שבצרפת. הכרטיס מכיל ארבעה סוגי מידע:

- א. זיהוי (פרטים אישיים, סוג הביטוח הרפואי וכד').
- ב. היסטוריה רפואית.
- ג. סוג דם.
- ד. טיפול רפואי (נוכחי וקודמים).

פרויקטים דומים מיושמים בצ'כיה, קנדה ופורטוגל וזוכים להצלחה, מאחר שהכרטיס החכם מאפשר ביטול הניירת ופיקוח הולם יותר על התרופות המסופקות.

2. חינוך

הקמפוסים באוניברסיטאות ובתי הספר מהווים מודלים אידיאליים לשימוש בכרטיס החכם. באנגליה מיושמים ניסויים בכרטיס הכספי מונדקס (Mondex), באוניברסיטאות יורק ואקסטר. אוניברסיטאות נוספות בארה"ב, הולנד, אוסטרליה וספרד אימצו כרטיס דומה.

בארץ מיושם מזה כמה שנים פרויקט באוניברסיטת בר-אילן, שבו חברו יחד בזק, י.ב.מ. ראקום וחברת שלומברגיה (Schlumberger). חברות אלו הנפיקו כרטיס כספי אנונימי, המאפשר לסטודנט לקבל שירותים שונים במסגרת הקמפוס (מכונות צילום, טלפונים ציבוריים, מכונות שתייה וכד').

אוניברסיטאות נוספות בישראל - העברית, תל אביב - החלו גם הן בפעילות ממשית בתחום הכרטיסים החכמים. חברת כספיט ודפוס בארי, השותפים בהנפקת הכרטיס באוניברסיטה העברית, נקטו בגישה שונה מהכרטיס שיושם באוניברסיטת בר-אילן. הכרטיס באוניברסיטה העברית הוא אישי, רב שנתי ומכיל את תמונתו של הסטודנט. הוא החל את דרכו ככרטיס זיהוי, אך מתוכנן להתפתח ליישומים נוספים כמו מאגרי מידע וארנק אלקטרוני.

3. תחבורה

הכרטיס החכם ללא מגע הוא אולי האמצעי היעיל ביותר לתחבורת המונים. הפרויקט הגדול והמורכב ביותר מורץ זה כמה שנים בהונג קונג. עם השלמתו של פרויקט זה, ישתמשו 2.5 מיליון נוסעים ביום בכרטיס אחד בנסיעתם באוטובוסים, אניות ורכבות.

פרויקטים בשלבים מוקדמים יותר מורצים עתה גם במספר ערי מטרופולין אחרות בעולם, בהן לונדון, סידני, לוס אנג'לס, פריז וסיאול. בכמה מערי אירופה הכרטיס משמש אמצעי תשלום במדחנים לחנייה. בפריז, למשל, הותקנו 12,309 מדחני רחוב, שמיועדים לקלוט תשלומים באמצעות כרטיס חכם עד סוף שנת '98.

בארץ החל ניסוי בקואופרטיב התחבורה הציבורית אגד, שמטרתו התקנת קוראי כרטיסים בכ-4,000- אוטובוסים והנפקת כרטיסים חכמים אשר יכילו, בנוסף לארנק אלקטרוני, את זכויותיו של הנוסע (חייל, גמלאי, סטודנט וכד').

4. רווחה

כחלק מהמדיניות ל"היערכות לעידן המידע", רואות ממשלות רבות את עצמן מחויבות לאספקת שירותיהן בערוצי התקשוב. גם כאן יכול הכרטיס החכם לסייע. הפרויקט הגדול ביותר מורץ כעת בספרד, ובמסגרתו חולקו 400,000 כרטיסים משולבים (חכם ומגנטי) לתושבי שלוש ערים. הכרטיס משמש אמצעי לקבלת תשלומי רווחה לזכאים. יתרונותיו הגדולים ביכולתו לאחסן טביעת אצבע על הכרטיס עצמו (ולא במאגר מרכזי), והגישה המיידית שהוא מספק לרשומות האישיות במאגרי המידע הממשלתיים. עד שנת 2000 יונפקו בספרד 40 מיליון כרטיסים, שישימשו בכמה אלפי מרכזים

(ובקיוסקים לשירות עצמי).

הממשל המקסיקני החל בהנפקת 200,000 כרטיסים למשפחות נזקקות. הכרטיסים נועדו לחסל את הזיופים הנפוצים בשיטת האישורים הידניים הקיימים. במדינת אוהיו בארה"ב הונהג כרטיס המחליף את בולי הדואר ומשמש גם לרכישת מוצרים בחנויות.

5. זיהוי

בטיחותו הרבה הופכת את הכרטיס החכם לאמצעי זיהוי מבוקש. במחוז מנדוזה הנפיקה ממשלת ארגנטינה רשיון נהיגה ככרטיס חכם. הכרטיס מכיל רישום עבירות התנועה וקנסות שלא שולמו, כמו גם פרטים אישיים ותמונה. ניתן, על פי בקשת המחזיק, לאחסן בכרטיס גם מידע רפואי למקרה חירום (סוג דם, אלרגיות לתרופות וכן טביעות אצבע). בין שאר היתרונות, מעריך הממשל בארגנטינה שהכרטיס יסייע להעמיק את גביית הקנסות בכ-10 מיליון דולר בשנה.

בכמה מדינות בעולם - דרום קוריאה, אוסטרליה ודנמרק הן הבולטות שבהן - מתקיימים ניסויים בהנפקת תעודת זהות, שיכולה לשמש גם כרטיס תושב, רשיון נהיגה, כרטיס רפואי, ביטוח לאומי ועוד. אך עדיין ארוכה הדרך להנפקת כרטיס חכם המזהה את בעליו במגוון רחב כל כך של תחומים, בעיקר בגלל בעיות של צנעת הפרט והיעדרם של תקנים בינלאומיים בתחומי החתימה וההצפנה הדיגיטליות.

6. תקשורת

עשרה מיליון אנשים ב-85 ארצות בעולם משתמשים כיום בכרטיס חכם בטלפון נייד, המבוסס על שיטת GSM (Global System Of Mobile Communications), השיטה בה מתמודדות הקבוצות במכרז על המפעיל הסלולרי השלישי בישראל.

בטכנולוגיית ה-GSM, כל נתוני הזיהוי (לרבות מספר הטלפון ופירוט השירותים הניתנים) מאוחסנים על הכרטיס החכם ולא במכשיר הנייד עצמו - וכך יכול בעל כרטיס כזה להתקשר מכל טלפון GSM, מכל מקום בעולם. כל שעליו לעשות הוא להכניס את הכרטיס למכשיר, לחייג ולדבר.

מכשירי הטלפון בטכנולוגיית GSM הופכים, למעשה, את המכשיר הנייד למעין "טלפון ציבורי חכם" עבור מחזיקי הכרטיסים. ואכן, בקרוב אמורה בזק לפרסם מכרז לטלפונים ציבוריים מהדור החדש, שיופעלו באמצעות כרטיס חכם, שיחליף את הטלכרט הקיים כיום.

7. ישומים כספיים

יישומו של הכרטיס החכם כארנק אלקטרוני נתפס, ובצדק, כמהפכה עם פוטנציאל כלכלי גדול. בישראל מתארגנות בימים אלה כמה שותפויות אסטרטגיות בין תאגידים גדולים להנפקת ארנק אלקטרוני. במסגרת מאמר זה, המוקדש לשירות הציבורי, לא נרחיב בנושא הארנק האלקטרוני. נדגיש רק כי קיימות כיום שתי התפיסות בעולם בנוגע ליעודו של הכרטיס הכספי:

א. תפיסה הרואה בארנק האלקטרוני כרטיס בנקאי/כרטיס אשראי עם שבב שהוא אישי וקשור לחשבון הבנק של בעל הכרטיס.

ב. תפיסה הרואה בארנק האלקטרוני כרטיס אנונימי, כמו שטר כסף, ללא קישור לחשבון בנק מסוים, ללא קוד אישי, ללא צורך בהרשאה, ללא קבלות, ללא חתימה, ללא ביטוח וללא תדפיס תקופתי. דוגמה לתפיסה זו הומחשה במשחקים האולימפיים באטלנטה '96 (Visa-Cash). לפי תפיסה זו פועלים גם תווי הקנייה המחולקים לעובדים בארץ לקראת החגים.

בסוף שנת '97 החל לרוץ בעיר ניו-יורק ניסוי, במסגרתו חולקו לתושבי צפון מערב מנהטן יותר מ-50,000 כרטיסים כספיים חכמים. במקביל, הותקנו קוראים ב-750 עסקים (מסעדות, חנויות מזון, מכבסות וסוכנויות דואר). בכרטיסים (ויזה ומאסטר-קארד, שמונפקים על ידי סיטי-בנק ובנק צ'ייס מנהטן), ניתן לטעון עד 500 דולר ממכשירי הכספומטים. כמו-כן, מתוכננת אפשרות טעינה

מהטלפון/המחשב בבית ישירות לחשבון הבנק של מחזיק הכרטיס. בשלב זה, לא ייגבו עמלות על השימוש בכרטיס, לא מהחנויות ולא מהתושבים.

8. מסחר אלקטרוני

חברות רבות משקיעות תקציבים גדולים בפיתוח "אמצעים בטוחים" לביצוע העברות כספיות באינטרנט. פיתוח כזה עשוי להועיל, כאשר יושלם, גם בביצוע פעולות מול גורמי שלטון מרכזי ומקומי, במסגרת חזון הממשל הזמין.

9. שונות

א. זה המקום לציין שני פרויקטים ייחודים בכרטיסים חכמים, המיושמים כיום בישראל:

פרויקט הקיבוצים, שבמסגרתו הונפקו על ידי חברת OTI מראש פינה 200,000 כרטיסים ללא מגע, שחולקו בכ-30 קיבוצים. הכרטיסים משמשים את חברי הקיבוץ בניהול תקציביהם, על פי זכויותיהם המשתנות מהגיל הרך ועד לפנסיה. הכרטיסים משמשים גם כמפתח חכם לכלי הרכב של הקיבוץ, לארוחות בחדר האוכל, לרכישה בחנויות הקיבוץ, למשיכת דואר, וכן ככרטיסי נוכחות/גישה למתקנים השונים.

פרויקט רשות שדות התעופה, שבמסגרתו משלם העובד את כל ארוחותיו במסעדות הרשות. על הכרטיס נאגרים פרטי העובד, ההרשאות וזכויותיו בתחומים השונים.

ב. אתרים רלוונטיים באינטרנט:

אתר מדיניות ממשל ארה"ב: <http://www.policyworks.gov/org/main/mg/intergov>

אתר מדיניות האוצר בארה"ב: <http://www.ustreas.gov/treasury/bureaus/fincen>

אתר איגוד הכרטיס החכם: <http://www.smarterd.com/info>

סיכום

כדי לנצל בצורה מוצלחת את האפשרויות שיוצר הכרטיס החכם, על הממשל לחפש פתרון במרחב הפתרונות המוצע על ידי הסקטור הפרטי, ולא לנסות לפתח "פתרון ממשלתי עצמאי".

נכון לימים אלה, הפוטנציאל של הכרטיס החכם עדיין איננו מנוצל. יתירה מכך: פוטנציאל זה עדיין לא נתפס כלל, והוא ימוצה רק עם המעבר לשימוש המוני בכרטיסים חכמים. מעבר מסוג זה יחייב, על פי רוב, מעורבות של הממשל ושינויי חקיקה לתמיכה בטכנולוגיה החדשה (חתימה אלקטרונית, צנעת הפרט, הצפנה, ועוד).

חשוב גם לזכור כי הכרטיס החכם הוא רק "קצה הקרחון": יש להקים/להתאים/לחשב מחדש את תהליכי העבודה/יחסי הגומלין בין נותן השירות לבין הלקוח. גורמי הממשל, וגם עולם העסקים, עדיין רחוקים מהשגת מטרה זו.

GLOSSARY מילון מונחים

אלגוריתם Algorithm

תיאור מדויק של תהליך חישוב מתמטי, או עיבוד נתונים בשלבים, כאשר כל שלב ושלב ידוע, ברור, ומהווה בסיס לשלב הבא.

אוטנטיקיישן/אימות Authentication

האימות אמור להבטיח שההודעה מקורית הגיעה לנמען כפי שנשלחה, וגם כי נשלחה מהמקור עליו הוסכם. שני תנאים אלה הם מהותו של מונח האימות. האימות מבוצע על ידי מאמת.

אוטנטיקטור/מאמת Authenticator

מספר הנשלח עם ההודעה ומאפשר לנמען להבחין בשינויים שנעשו בהודעה מהרגע בו יצאה מהשולח. מספר זה נבנה מתוכן ההודעה, וכן ממפתח סודי.

מק (מקינג) Mac-Message Authentication Code

כינוי נוסף למאמת לפי תקן אמריקאי ANSI X 9.9, שמכסה אימות של הודעות פיננסיות למעבר כסף באינטרנט, בתקשורת טלפונית וכן ברשת מחשבים.

אימות עומד בפני שני סוגי התקפות:

התקפה פעילה Active Line Tap (Wire Tap)

התקפה יזומה, שמטרתה להפריע למערכת התקשורת ולשנות את המידע או ההודעה על ידי השתלת נתונים או הודעה חדשים, חזרה על הודעה שנשלחה, האטה ועיכוב, או מחיקת חלק מההודעה.

התקפה סבילה Passive Line Tap (Wire Tap)

קריאה או ניסיון לקריאה אסורה של ההודעה המשודרת, וכן ניסיון לדלות מידע מהמערכת, ללא הכנסת שינוי בתוכן ההודעה.

פונקציה חד-כיוונית One Way Function

פונקציה של X , $Y = F(X)$. פונקציה כזו מאפשרת לחשב בקלות יחסית את המשתנה בכיוון אחד, אך לא בכיוון השני. כלומר, אם מספר X ידוע, קל מאד לחשב את Y , אך אם מספר Y ידוע, לא ניתן לחשב ערך כלשהו של X לפי: $X = Y^{-1}(Y)$.

קריפטוגרפיה Cryptography

טכניקה של הסתרת והצפנת תוכן הודעה, או מעבר נתונים, על ידי שימוש בקוד או סיפר.

קוד **Code**

שיטת הסתרת (הצפנה) על ידי שימוש בטבלה או טבלאות קוד, המאפשרת תרגום ההודעה בשפה רגילה להודעה מוצפנת בשפה שנייה. לדוגמה, שימוש במילון אנגלי-עברי ועברי-אנגלי.

סיפר **Cipher**

שיטת הסתרה (הצפנה) על ידי שימוש באלגוריתם, המופעל או מיושם על הודעה, או על שורה או אות מתוך ההודעה.

דס **Des - Digital Encryption Standard**

סטנדרט הצפנה אמריקאי, שפותח על ידי הסוכנות לביטחון לאומי בארה"ב, במטרה להוות בסיס לאבטחת תקשורת בין גופי הממשל האמריקאי.

דס מבוסס על תוכנית הצפנה משנות השישים - לוציפר (Lucifer) של חברת י.ב.מ. תוכנית זו הינה הבסיס עד היום לאבטחת מידע פיננסי ולהעברת כסף בין בנקים וגופים פיננסיים אחרים.

דס מתאר במדויק אלגוריתם בעל 16 שלבים, כולם שלבי חישוב כולל הכפלות וחלוקות. הוא עובד על חידות מידע בסיסיות של 64 ביטים, שמכונות Blocks. דס מבוסס על עיקרון המפתח הסימטרי (ראה מפתח א-סימטרי ציבורי).

צופן מפתח ציבורי **Public Key Cipher**

מירב שיטות ההצפנה, הנמצאות בשימוש כיום, משתמשות במפתח סודי הידוע הן לשולח והן לנמען. מקובל לכנות צפנים אלו צפנים סימטריים, הואיל והידע על המפתח הסודי נתון בידי שניים - השולח והנמען - והמידע העובר בכיוון אחד זהה לזה העובר בכיוון הנגדי.

בסוף שנות השבעים הופיעה גישה חדשה בנושא ההצפנות, שבה השולח והנמען משתמשים במפתחות אחרים, שקשורים ביניהם ביחס מתמטי מסוים. מקבל המידע מחזיק במפתח סודי, שבעזרתו הוא מפענח את ההודעה. לעומת זאת, המפתח שנמצא בשימוש על ידי שולח ההודעה, ובעזרתו הצפין את ההודעה, גלוי וחשוף לציבור.

זוהי השיטה הא-סימטרית, המאפשרת תקשורת בכיוון אחד בלבד. ליצירת קשר בשני הכיוונים דרושים עוד זוג מפתחות. השימוש בשני זוגות מפתחות שונים אך מתייחסים זה לזה, כאשר מכל צמד אחד המפתחות ידוע לציבור, מכונה צופן המפתח הציבורי.

חתימה דיגיטלית **Digital Signature**

מספר הנבנה ומתבסס על כל הביטים המופיעים בהודעה, ועל המפתח הסודי של השולח. ניתן לאמתו על ידי שימוש במפתח הציבורי הפתוח, במקרה שנעשה שימוש בהצפנה סימטרית. ניתן לאמת חתימה דיגיטלית על ידי Macing והמפתח הסודי שהוסכם עליו.

כרטיס דור שלישי **Third Generation Card Euro Chip**

כרטיסי דור שלישי פותחו במקביל, הן על ידי חברות התקשורת הגרמנית וההולנדית, והן על ידי חברת התקשורת הצרפתית, בשיתוף עם יצרני הרכיבים. למרות ההגדרה המשותפת, אין שני סוגי הכרטיסים מתאימים זה לזה בדיוק.

הכרטיסים מאופיינים ב-6 תכונות ייחודיות, הקשורות לזכרון המפעיל:

1. מתן זהות לכרטיס. חלק מזיכרון המפעיל הכולל: קוד הוצאת כרטיס, סוג הכרטיס, תאריך ההוצאה, מספר סידורי של הכרטיס או מנת כרטיסים.
2. מונה ספירה: עד חמישה מונים בעלי אורך 8 ביט כל אחד. ביט אחד נצרב בשלב ראשון לאבטחה.
3. תמיכה: מונה פנימי להגנה בפני Antitearing, או מפני הוצאת כרטיס לפני תום השיחה.
4. אימות: אזור הצפנה למפתח סודי של הכרטיס.
5. חתימה - Signature
6. שילוב רב תחומי: אזור בזיכרון, המאפשר הוספת מפתח למפעיל שני, כולל אימות וחתימה נפרדים.

Sam - Security Application Module

סאם

מכון התקנים האירופי לתקשורת (ETSI) מגדיר כך את המונח סאם: "אמצעי לוגי, שתפקידו לספק אבטחה לסביבה לא בטוחה. הוא עצמו מוגן נגד התקפות מבחוץ, ושומר נתונים ואינפורמציה קריטיים".

* המילון מוגש באדיבותו של מר קמי בן-שם מקבוצת לוונשטיין בע"מ.

כיצד מתבצע אימות?

להלן שלבי התהליך, כפי שהם מתבצעים במכשיר טלפון ציבורי אירופי באמצעות תוכנת פניקס (LANDIS & GYR):

1. **שלב הזיהוי ובדיקה ההרשאות.** עם הכנסת הכרטיס למכשיר הטלפון, פניקס חוקר אותו ומבקש את מספר הזהות של הכרטיס. כלומר, פניקס חוקר האם הכרטיס רשאי בכלל לקבל שירות כלשהו.
 2. **שלב האתגר.** פניקס שולח מספר אקראי לכרטיס דרך מכשיר הטלפון, שאותו חישב מתמטית במעבד הפנימי שלו. מספר אקראי זה לעולם לא יחזור שנית בכל מהלך חיי פניקס.
 3. **שלב החתימה.** הכרטיס מחשב, בעזרת יחידת הצופן והאלגוריתם הפנימי שלו, מספר באורך מסוים. מספר זה הוא חתימת הכרטיס. המספר מתבסס על תעודת הזהות של הכרטיס, מצב וערך המונים בכרטיס ועל מפתח אישי סודי הנמצא בכרטיס.
 4. **בדיקת החתימה ומתן הרשאות.** פניקס בודד את החתימה שנשלחה מהכרטיס, מחשב במקביל חתימה פנימית ומשווה את התוצאות. אם החתימה מתאימה, אז, ורק אז, ניתנת לראשונה רשות לפתיחת הקו לביצוע שיחה. השיחה מתחילה, האימות ממשיך. במהלך השיחה נעשות פעולות אימות חוזרות ונשנות, בדיוק לפי הסדר הרשום לעיל.
- בכל פעולת אימות, פניקס שולח מספר אקראי חדש, והכרטיס מגיב במשלוח חתימה חדשה, שכן מצב המונים בכרטיס משתנה לאחר כל פעימה. נתוני הכרטיס נשמרים בפניקס לאורך כל השיחה.

בתום השיחה, פניקס משווה את מצב המונים מתחילת השיחה, הן בכרטיס, והן בתוכו הוא, ומוסיף למונה הפנימי שלו בדיוק את כמות הכסף שהורדה מהכרטיס.

במקרה של כרטיס חכם, הכולל מעבד ומסוגל לבצע טעינה חוזרת, מתבצע תהליך של אימות הדדי בין פניקס לכרטיס. כלומר, פניקס מאמת את הכרטיס, והכרטיס מאמת את פניקס.

הוועדה הטכנולוגית הישראלית לנושא הכרטיס החכם

מזה כשנתיים מתקיים פורום ציבורי לנושא הכרטיסים החכמים, בראשות ויקטור איררה, מנהל אגף מחשוב ומערכות מידע בעיריית תל-אביב-יפו.

בפורום חברים הגופים הגדולים במשק (משרד האוצר, בנקים, בזק, אגד, דן, צה"ל, רשויות מקומיות, רשות הדואר, ביטוח לאומי, ארגונים להגנת הצרכן, ועוד), וכן החברות המתמחות בנושא כרטיס חכם בארץ (IBM, כספיט, ראקום, ועוד).

הפורום מונה במנדט ממשלתי של משרד רה"מ כוועדה טכנית-טכנולוגית לנושא הכרטיס החכם. גובשו בו כמה המלצות ובהן:

- אימוץ תקן ISO 7816
- דרישה לארבעה סאמים (SECURITY ACCESS MODULES), כעתודה בכל מכרז המפורסם על ידי הגופים הגדולים בארץ (ליצירת תשתית לשת"פ בעתיד).

הפורום גם גיבש עמדה בנוגע לגורמים המוסמכים להנפיק כרטיס חכם כספי בישראל.

לאחרונה הופצה בין חברי הוועדה טיוטת "אמנה", המציעה קוד התנהגות למנפיק כרטיס חכם בארץ. מזה כחצי שנה פועלות שתי ועדות מומחים בנושא זה במכון התקנים: האחת בנושא העברית בכרטיס, בראשות ג'וני רוזן, והשנייה בנושא רישום יישומי הכרטיס, על פי תקן ISO 7816 פרק 5, בראשות מר איררה.

התפתחות חשובה נוספת: נגיד בנק ישראל אישר את המלצותיה של ועדה, שמינה המשנה למפקח על הבנקים, בנושא הארנק האלקטרוני בארץ. משרד המשפטים נערך לחקיקה המתחייבת מיישום הדו"ח, שאושר גם על ידי ועדת הכלכלה של הכנסת.

החידושים העיקריים בדו"ח: מתן אפשרות לגופים לא בנקאיים להנפיק, בתנאים מסוימים, ארנק אלקטרוני, בתיאום עם הממונה על ההגבלים העסקיים; ואיסור הנפקה של "ארנק אלקטרוני לאומי" אחד, המשותף לבנקים המסחריים ולחברות כרטיסי האשראי בארץ.