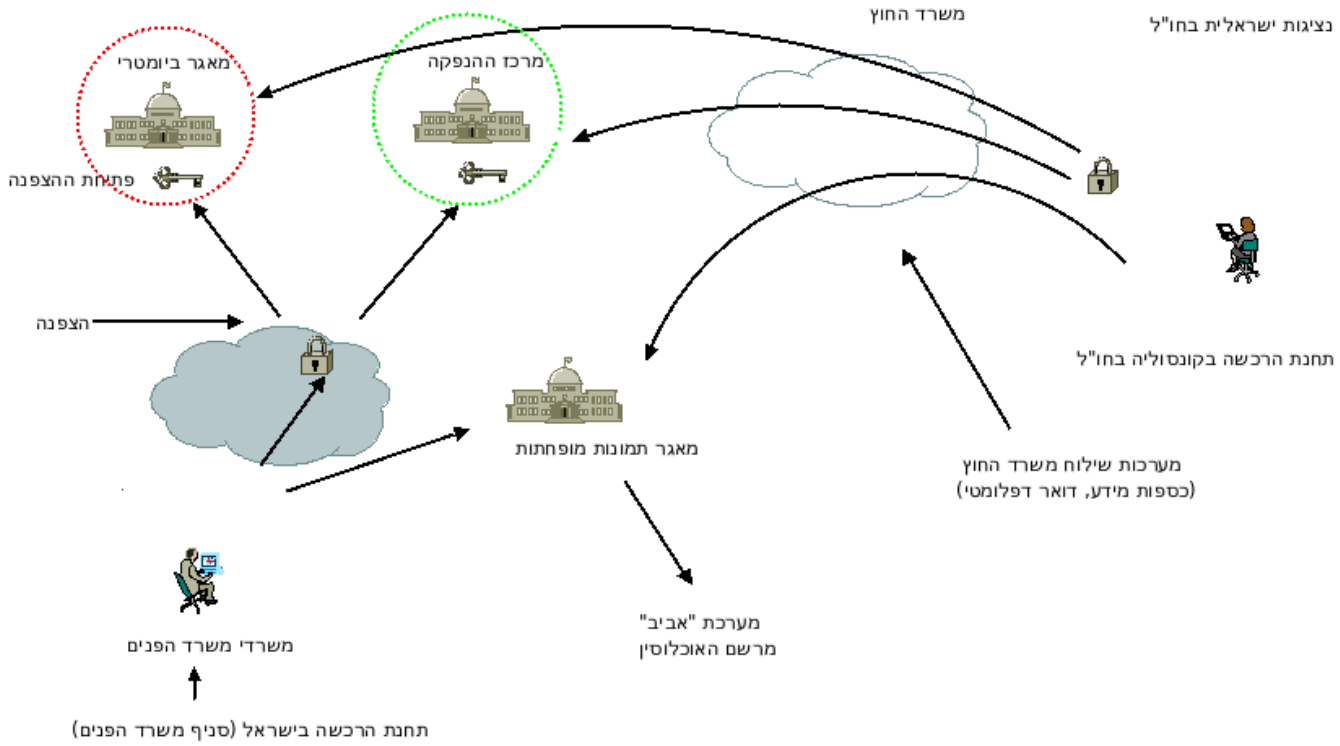
הסבר לחוק הביומטרי, או בשמו המלא:

חוק הכללת אמצעי זיהוי ביומטריים במסמכי זיהוי ומאגר מידע .

- אופק דורון

החוק כולל שלבים שונים אשר אליהם קיימת התייחסות בנושא הביומטרי. באופן כללי התרשים הבא(1) מנסה לתאר בצורה סכמתית כללית את הרכיבים השונים המרכיבים בסופו של דבר את התמונה המלאה:



תרשים 1: אופן זרימת המידע בין הרכיבים השונים המרכיבים את מערכת המידע האחראית בסופו של דבר להנפקה של תעודות זהוי הכוללות נתונים ביומטריים , ואת מאגר המידע.

השלבים השונים המרכיבים את ההליך:

1. אזרח נקרא להתייצב במשרדי משרד הפנים על מנת לקחת ממנו נתונים ביומטריים, המדובר הוא בטביעות אצבע של שני האצבעות המורות ותמונות פניו, כמו כן במעמד זה ייווצרו מהאמצעים הביומטריים (תמונת הפנים ותמונות טביעת האצבע), נתונים ביומטריים (מידע הנוצר מתבניות") , כל המידע הזה יוצפן ויישלח הן למערך המנפיק והן לרשות האחראית על המאגר. כמו כן בשלב זה, תמונת פניו של האזרח תעבור עיבוד על מנת

להנמיך מאיכותה ועל מנת למנוע החזרה שלה לאיכות טובה יותר, מוכנסים אליה בצורה רנדומלית נתונים שגויים, כך שהתמונה מאפשרת רק זיהוי חזותי של האדם.

2. המידע שנותר לאחר הליך הנטילה, יכול להישאר במשרד הפנים עד אשר, יודיעו למשרד הפנים כי הנתונים התקבלו בהצלחה בשני היעדים. בשלב הזה אמור המידע להימחק.
3. המידע מגיע אל מרכז ההנפקה , אך הוא אינו יכול להתחיל בהליך ההנפקה עד אשר תתקבל הוראה מהרשות האחראית על המאגר שלא להנפיק, במידה ולא התקבלה הוראה שכזו ועברו 7 ימים, ייראה בכך מערך ההנפקה כאילו אין התנגדות של הרשות והוא יוכל להתחיל בהליך ההנפקה.
4. הרשות האחראית על המאגר תקבל את הנתונים ממשרד הפנים, ותשווה אותם לנתונים אחרים במאגר, במידה וקיימים נתונים ביומטריים זהים – באחריות הרשות להודיע בתוך שבוע ימים למערך ההנפקה שלא להנפיק תיעוד , המידע החשוד (העתק ב') והמידע שזהה לו (העתק א') יועברו למשרד הפנים ומשם למשטרה לצורך הגשת תלונה וחקירה על נסיון זיוף.
5. בכל הקשור להנפקת תיעוד לאזרחים ישראלים המתגוררים בחו"ל, קונסוליות משרד החוץ מהוות נציגות של משרד הפנים והן אחראיות על הנטילה והעברת המידע לארץ (למשרד הפנים) ולאחר מכן לקבלת התיעוד ממשרד הפנים והעברתו לקונסוליה לצורך לחלוקתו , מרגע שהמידע נכנס אל משרד הפנים , התהליך שהוא עובר זהה לתהליך שעובר המידע בארץ.

<u>מערך ההנפקה:</u>

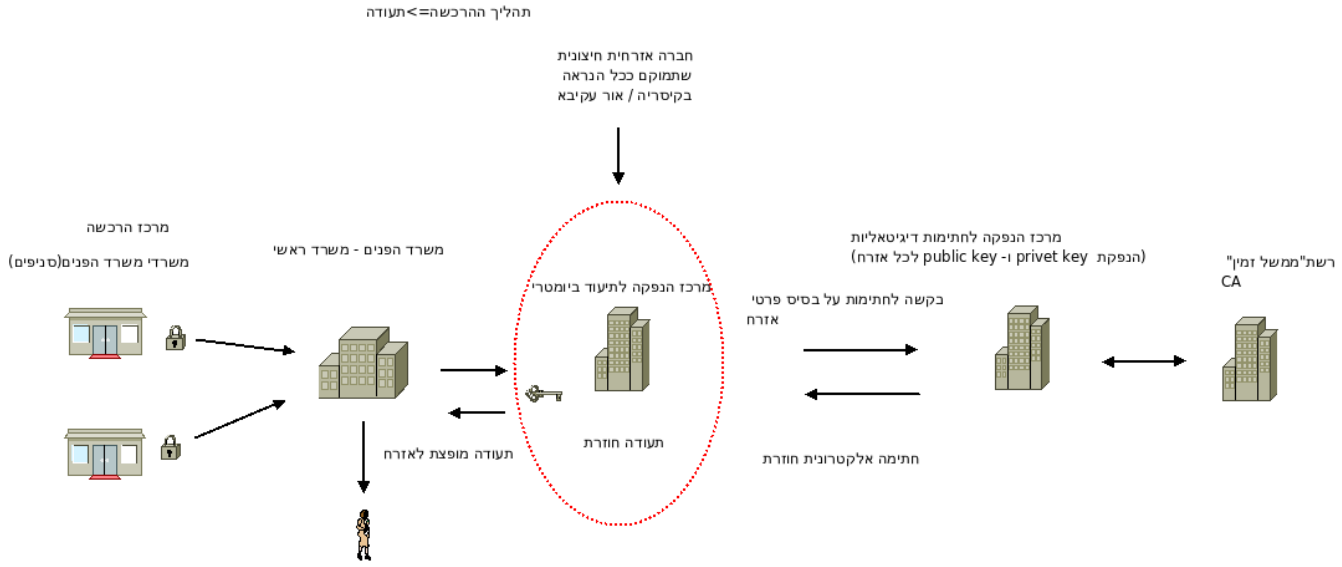
מערך ההנפקה, מעת קבלת המידע (ראה תרשים 2) , צריך לשמור אותו לפרק זמן שבו ניתן לרשות האחראית על המאגר, לבדוק את נתוני הזיהוי של האזרח. פרק זה מוגדר בחוק כשבוע, היה ובמהלך של שבוע ימים לא תתקבל מהרשות התראה על קיומם של נתונים ביומטריים זהים אצלה , ייחשב הדבר כאישור של הרשות להנפיק כרטיס זהות לאזרח.

קיימת נקודה אשר אינה ברורה דיה בהצעת החוק אשר נמצאת לנגד עיניי (ההצעה אשר אושרה בישיבת הוועדה האחרונה) .
למעשה בהצעת החוק מקורית, אשר עברה מספר שינויים, הגוף האחראי על הנפקת המידע הביומטרי (מידע המבוסס על תבניות), הינה הרשות האחראית על המאגר, אולם, בגלל רצון המדינה להראות כי "לא יוצא מידע מן הרשות הזו" , שונתה הצעת החוק, כאשר בהצעה שהתקבלה לבסוף (להלן "ההצעה המקבילית") , המידע הביומטרי של האזרח כפי שהוא נאסף בנקודת הנטילה אמור לעבור ל 2 גופים במקביל (לרשות לצורך הכנסה למאגר, ולמרכז ההנפקה לצורך הנפקת התיעוד).
על מנת להגבר על זה שאין הסמכה בחוק למישהו לייצר מידע ביומטרי (מספרי, מבוסס על תבניות) על בסיס האמצעים הביומטריים (תמונת טביעת האצבע) , דובר על קיומו של הליך אוטומטי במעמד הנטילה אשר ינפיק את המידע הנ"ל , כל המידע , כולל האמצעים הביומטרים וכולל את הנתונים הביומטרים אמור להארז ולהיות מוצפן , לאחר שהתמונת פנים עוברת עיבוד מסויים , ההעתק של התמונה המעובדת (להלן התמונה המופחתת) עובר למערכת "אביב" (מערכת פנימים במשרד הפנים לצורך זיהוי חזותי), והמידע האחר , כאמור, נארז ונשלח הן לרשות והן למערך ההנפקה.
אולם, ככל הנראה, התהליך לא עבר בדיקה מדוקדקת , וכך יוצא שבסעיף 3 (ב) ו- 3 (ג) , עדיין קיימים איזכורים השולחים אותנו לסעיפים אחרים ובין השאר לסעיף 12 (א) שבו נכתב כי :
"הרשות תעביר לעובד משרד הפנים שהשר הסמיכו לכך, לצורך הנפקת מסמך זיהוי, תוצאות זיהוי של מי שניטלו ממנו אמצעי זיהוי ביומטריים לפי סעיפים 3 ו-5, לא העבירה הרשות תוצאות זיהוי כאמור בתוך פרק זמן שקבע השר , יראו זאת לעיניין סעיף 3א (א) כאישור להנפקת מסמך הזיהוי. וכן את האמצעים והנתונים הביומטריים

לצורך הכללתם במסמך הזיהוי" .

כלומר, הנתונים שאמורים להיכלל במסמך הזיהוי, אמורים להגיע מן הרשות, ולכן נשאלות השאלות:

1. למה להעביר מלכתחילה את המידע למערך ההנפקה, אם ממילא על פי הצעת החוק המידע שיכלל בתעודה אמור להגיע מן הרשות.
2. כיצד יוצא מידע מן הרשות – אם לא ניתן להוציא מידע מן הרשות (למעט תוצאות זיהוי).



תרשים 2: מתאר את פעילות מרכז ההנפקה של התעודות זהות.

בנוסף לכך, בעת ההנפקה ישנו הרצון להכניס אל תעודת הזיהוי, מידע השייך לתחום ההצפנה , למעשה, אין לכך ביטוי מובהק בחוק, אלא על בסיס חוק חתימה דיגיאלית, ועל בסיס פרוייקט של תעודת זהות ככרטיס חכם .
ולכן, אמור מערך ההנפקה לבקש / לקבל / להיות מחובר עאל המערכת העוסקץ בנושא של חתימות פרטיות וציבוריות – על מנת להטמיען בכרטיס.
שהיא מצידה אמורה להיות מחוברת למערכת ממשל זמין , וליתר דיוק את ה CA המצוי במערכת ממשל זמין.

<u>יודגש, על פי הצעת החוק הנוכחית יכול משרד הפנים להוציא את ההנפקה לגורם חיצוני מסחרי</u>

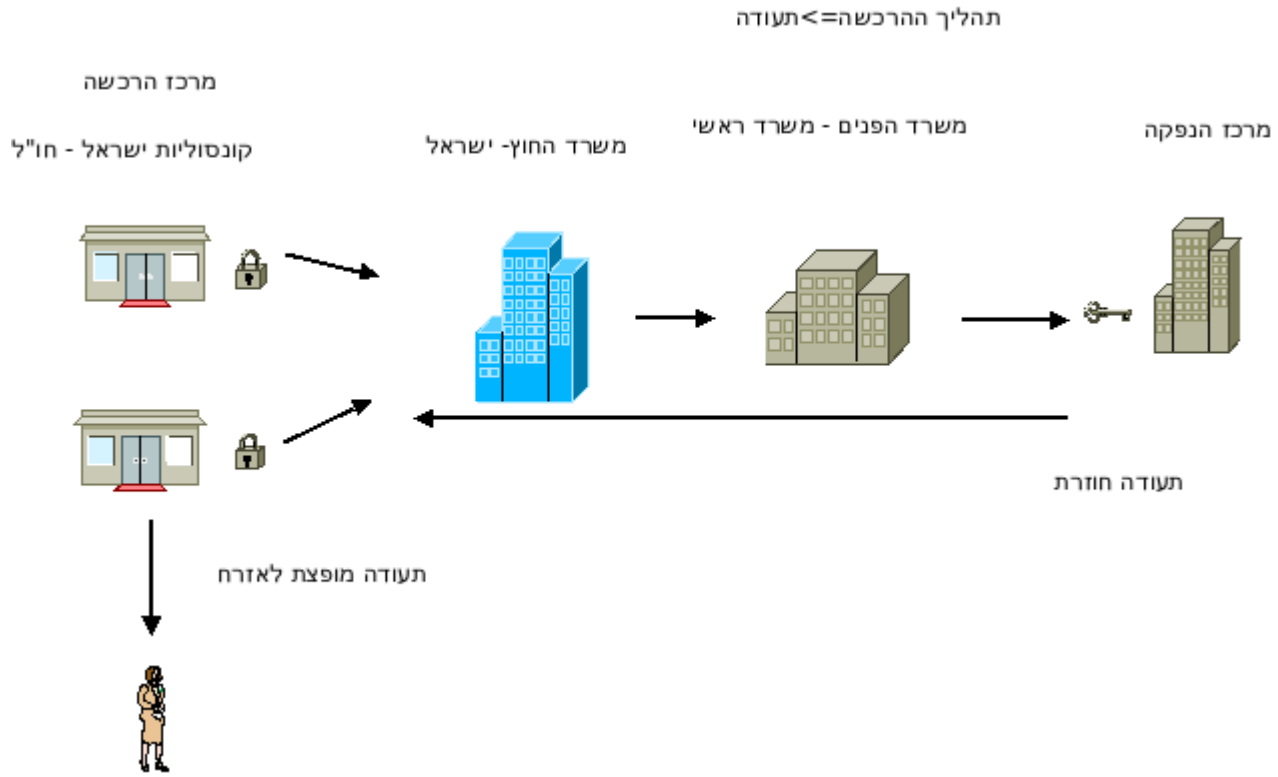
(נושא ההנפקה של החתימה הדיגיטלית והתאמתו או צורת יישומו לא נדונה במסמך זה, אולם לפרטים ניתן לפנות אליי בנושא זה. ד.א.)

<u>גורמי תווך נוספים בהליך ההנפקה:</u>

למעשה מעבר לגורם המסחרי, אשר יכול להפעיל את מערך ההנפקה, גורמים נוספים אשר קשורים למערך ההנפקה הינם משרדי משרד הפנים (כמה עשרות סניפים בכל הארץ) , ומערך ממשל זמין (תהיל"ה) אשר מחזיק ב CA לטובת עבודה עם מפתחות.

מלבד גורמים אלו, קיים משרד החוץ.
משרד החוץ נכנס לפרוייקט זה ב 2 אספקטים שונים, הראשון הוא שמשרד החוץ מהווה היום את מערך ההנפקה של הדרכונים הרשמיים של מדינת ישראל (להלן "דרכון שירות" ו"דרכון דיפלומטי"), כיום ההדפסה של דרכונים אלו נעשית ע"י המדפיס הממשלתי בהזמנה ופיקוח של משרד החוץ (כולל חלוקה לצרכנים) .
למעשה יכולת זו תופקע ממנו , בעת התחלה של העבודה עם מסמכים ביומטריים, על מנת לרכז את כל הטיפול במקום יחיד.
משרד הפנים, יצטרך, להנפיק גם דרכונים רשמיים אלו.

באספקט השני, משרד החוץ על הקונסוליות שלו מהווה נציגות של משרד הפנים, כך שפעילות שאזרחים ישראלים מבצעים מולו, כאילו נעשו מול משרד הפנים – הדבר מקובע בנהלים לפחות על פי הצרכים הקיימים כרגע.
גם לעיניין של הנפקת תעודת זהות ביומטרית משרד הפנים הסמיך את משרד החוץ, כך שהקונסוליות השונות, יוכלו לבצע נטילה של מידע ביומטרי מאזרחים הנמצאים במדינות חוץ, המידע יועבר ע"י מערכות העברת המידע של משרד החוץ בארץ והוא מצידו יעבירן למשרד הפנים לשם הנפקה והכנסה למאגר.
המערכות שישמשו את משרד החוץ הינן או מערכת "כספות ווירטואליות" או מערכת של "דואר דיפלומטי" .
תרשים 3 מדגים את הנושא:



תרשים 3: העברת המידע מקונסוליות בחו"ל לצורך הנפקה והכנסתו למאגר.

<u>עבודה שוטפת מול המאגר:</u>

למעשה מלבד הליכי ההרכשה למינהם, קיימת גם העבודה השוטפת במסגרתה גופי מדינה שונים יכולים לבקש מידע ו/או אישורי מידע מתוך המאגר.
המידע , הגולמי, אמור להילקח מן האדם עצמו או מהתעודה שהוא נושא (תלוי באיזה סוג אירוע מדובר) , ולמעשה לעבור השוואה מול מידע המצוי במאגר .
המחוקק הדגיש בהצעת החוק, שהנוטל במקרה שכזה יכול להשאיר את המידע בידו , עד לעת שהוא לא יהיה נחוץ (לצורך העיניין , כל עוד ההליך נמשך) .
עם זאת יש לזכור כי חלק מההליכים הקיימים כיום במדינת ישראל יכולים להמשך שנים (חקירת משטרה לדוגמה) – דבר העשוי ליצור "מיני מאגרים" בידיהם של גופים שונים, המחוקק לא נתן את דעתו על הנושא של הגנת "מיני מאגרים" שכאלו.

יודגש, על אף רצונו של המחוקק לטעון כאילו מידע לא יכול לצאת מהמאגר החוצה, בסעיף 12 להצעת החוק מתוארת יציאה של מידע מהמאגר החוצה .

בנוסף לכל האמור לעיל, בהצעת החוק הנוכחית, המחוקק לא מצא לנכון להיכנס לסוגיה של הגנת המידע בדרכו אל המאגר או ממנו בשימוש השוטף, כלומר, אין טיפול או הגדרה של הצורך להגן על המידע כאשר הוא עושה את דרכו מרשות מסויימת אל המאגר, כל עוד הוא בתוך אותה רשות או אותו גוף.
לדוגמה, שוטר סיור יעצור אזרח לבדיקת רשיונות ויחליט לתשאל את המאגר בדבר זהות האזרח – במצב שכזה, ניתן להעביר נתונים (במידה וקיים בניידת הסיור ציוד) , אל רשת המשטרה, ומשם אל הרשות האחראית על המאגר, אולם, הנתונים הללו משודרים (במצב שכזה) באוויר על תשתית של רשת מירס או כל נשא סלולארי אחר (פלאפון) , המחוקק התיר לגופים השונים לטפל בהגנה על המידע הביומטרי , כל עוד הוא מצוי ברשת שלהם (הוא כן הגדיר כי יש למחוק את המידע בסיום השימוש בו).

<u>הכרטיס החכם :</u>

למעשה המחוקק, או הוועדה לא נגעו בנושא של סוג הכרטיס.
המידע, למעשה, כפי שאני הבנתי אותו, סודי , לשיטת המחוקק, והאחראים על התחום.

ייתכן, ומדובר בכרטיס contactless , מכוון שככל הנראה קיימת כוונה לשים שבב שכזה בדרכונים , מה גם שלממשלה, כבר קיימים פרוייקטים שונים, אשר בהם נעשה שימוש בכרטיס שהינו contactless .

מה שכן אנו יודעים על הכרטיס עצמו, הוא המידע שיהיה בו.
הצעת החוק (פרק ח' סעיף 2 להצעת החוק) מדברת על סוגי המידע הבאים שיהיו בכרטיס:

1. אמצעי זיהוי ביומטריים או נתוני זיהוי ביומטריים (בהסבר שבע"פ נטען שוב ושוב כי מדובר במילה "ו" ולא במילה "או" אולם עד עתה זה לא תוקן. ד.א.) , כהגדרתם בחוק הכללת אמצעי זיהוי ביומטריים .... אמצעים או נתונים ביומטריים כאמור יישמרו בשבב באופן שתתאפשר גישה אליהם...
2. תעודה אלקטרונית לאימות ואמצעי זיהוי אלקטרוני; תעודה ואמצעי כאמור יישמרו בשבב

באופן שתתאפשר גישה אליהם בידי בעל התעודה בלבד או בהרשאתו;

3. אמצעי חתימה , אמצעי לאימות חתימה ותעודה אלקטרונית , כהגדרתם בחוק חתימה אלקטרונית.
4. פרטים נוספים שיקבע שר הפנים בתקנות.

<u>מפתחות ההצפנה – וזיהוי מבוסס מפתחות:</u>

כחלק מהרצון של המחוקק להביא לכדי מימוש את חוק חתימה דיגיטאלית, רוצה המחוקק לשלב מפתחות הצפנה בתעודת הזהות.
שימוש במפתחות אלו יהיה בהתבסס על חוק חתימה דיגיטלית.

חוק חתימה דיגיטלית עבר לפני מספר שנים , אולם, עד עתה לא נעשה בו שימוש נרחב ולמעשה הציבור לא אימץ אותו – קיימות לכך סיבות רבות , אשר בחלקן נוגעות לנושא של הרגולציה של ה CA ותחולת ההוראות והדרישות אותן רוצה הממשלה מגופי חוץ על מנת להפעיל CA .

ולפיכך, הסמיך הרשם העוסק בנושא של חתמים (שייך למשרד המשפטים) , את תהיל"ה , כגוף אשר מוסמך להפעיל CA .

קיימות מספר בעיות סביב נושא זה, אשר, להבנתי יצמצמו את השימוש בחתימה דיגיטלית ע"י כלל האזרחים, ועד שבעיות אלו לא ייפתרו – לא יהיה שימוש נרחב ליישום, אלא באילוץ של הצרכנים (אזרחים המשתמשים בחתימות).

חוק חתימה דיגיטלית עוסק בהכשר של שימוש בחתימה דיגיטלית, כחתימה ברת תוקף, לא רק בין האדם לממשל אלא באופן כללי.

למעשה, השימוש בחתימה דיגיטלית, בא לקיים, תשתית של פעילות במצבים של "אי אמון" בין הצדדים המעורבים בפעילות – כך הוא נוצר בעולם המיחשוב.

כיום, בממשלת ישראל, ישנם מספר נסיונות להפעיל נושא של כרטיסים חכמים, אולם נסיונות אלו מניחים , כהנחת מוצא , שקיים אמון בין האזרח לגורם המנפיק. הסיבה להנחה זו הינה שהגורם המנפיק , **<u>מנפיק גם את המפתח הפרטי למשתמש</u>**.

האינטראקציה, הינה למעשה, ברובה, בין שני גופים השותפים ליישום , הממשלה מחד והאזרח מאידך, כאשר הממשלה הינה גם הגוף המאשר את החתם, גם החתם בעצמו, וגם צד לעיסקאות מסויימות (העברות כספיות של תשלום מיסים כדוגמה), בהתקיים אינטרקציה של האזרח עם אזרח אחר (מכירת רכב לדוגמה) , הממשלה כמובן אינה צד לעיסקה עצמה (ככל שעיסקת מכירת רכב אפשרית ע"י שימוש בחתימות דיגיטליות) .
יש בכך טעם לפגם כאשר הממשלה הינה גם הגורם המסמיך, גם החתם, גם המנפיק, ובוודאי אם היא גם הגורם שמנפיק את המפתח הפרטי – יכולים להתעורר בעיות מבעיות שונות בהמשך.

אבל, ראוי להסביר כיצד הגענו למצב הזה.

בעיקרון, העולם של השימוש במפתחות הצפנה כפי שאנו מכירים אותן כיום, נולד על התשתית של מיחשוב בה כל אחד יכול להנפיק לעצמו מפתח, במידה והמחשב המנפיק נמצא בשליטתו.
זהו למעשה המפתח הפרטי, וההגדרה בעבורו טוענת כי אסור לחשוף אותו לשום גורם , במידה וקיימת חשיפה שכזו – יש לבטל את המפתח מכוון שגורם זר עשוי להזדהות כבעל המפתח.

כאשר העולם העסקי, רצה לממש נושא זה (בחלק מהמקרים הנוגעים בעיקר לנושא של כרטיסים חכמים) , היתה בעיה שלא נמצא לה פתרון, והיא כיצד מכניסים מפתח פרטי להתקן אחר (כרטיס) בלי לפגוע בו – למעשה, להבנתי , לא נמצא לכך פתרון עד עתה (גם אם המשתמש ייצר את המפתח , בתהליך העברתו אל הכרטיס הוא יוכל להיות מועתק לגורם זר) .
למעשה, יצרני הכרטיסים, מטעמים שלהם (שתכף יוסברו), בחרו לייצר בעצמם את המפתח הפרטי.
למעשה, אין בכך בעיה גדולה מ 2 סיבות:
האחת – היצרן מייצר את הכרטיסים, במרבית המקרים, ללא הידיעה של מיהו האדם שישתמש בהם (כך לגביי כרטיסי SIM או כרטיסים המשתמשים להצפנה של שידורים לוויניים) , הזהות של הצרכן משודכת אל הכרטיס ע"י ספק השירות עצמו , דבר המאפשר עקיבה אחר השימוש וזיהוי של אנומליה בפעילות של אותו כרטיס.
כך לדוגמה, כאשר הייתי אני לפני מספר חודשים בפאריז, וביצעתי רכישה גדולה, לא עברו דקות רבות וקיבלתי טלפון חברת כרטיסי האשראי – על מנת לאשר שאכן אני הוא זה שביצעתי את הפעילת, למעשה מערכת ה BI שלהם זיהתה אנומליה בפעילות של הכרטיס שלי – ותוך דקות יצרו עימי קשר על מנת לוודא שאכן זה אני.
בעצם, ע"י שימוש בכלים חיצוניים, יכול הספק לספק מנגנון ביקורת לשימוש בכרטיס.
לספק עצמו יש אינטרס מהותי בכך שהמערכת לא תיפגע כי הוא המפסיד הגדול באם תתרחש פגיעה שכזו.

הסיבה השניה – במרבית הכרטיסים החכמים , הפעילות של הצרכן הינה מינורית וכך גם הנזק הנגזר ממנה , למעשה אם כרטיס ה SIM שלי ייחשף ויועתק וייעשה בו שימוש , הנזק הפוטנציאלי הוא כמות הדקות שקיימת בחודש כפול המחיר לדקת זמן אוויר – נזק שבמקרה הגרוע יעמוד על כמה אלפי שקלים – אך סביר להניח שהספק הסלולארי שלי , יזהה אנומליה בפעילות תוך פרק זמן מסויים וייצור איתי קשר על מנת לבדוק את הנושא.
כך שלמעשה, בשימוש בכרטיסים חכמים, כל משתמש יכול לספוג נזק מוגבל , כמובן שאם המערכת בכללותה נשברת הנזק הגדול הוא לספק עצמו (נזק של מליונים ואף יותר) – מכוון שכך, הספק , מבצע פעילויות בדיקה ועקיבה ובכל מקרה, בדרך כלל משפה (מלשון שיפוי) את הצרכן במידה וקיימת בעיה.
לספק – יש אינטרס כלכלי ברור לשמור על הגנת המערכת כי הוא זה שעשוי להיות המפסיד הגדול במידה והיא תישבר.

אם נבחן מה קורה בנושא של ממשל מול אזרח, הרי שאם תתקיים פגיעה במערכת או שהיא תישבר בצורה כזו או אחרת – המפסיד הגדול לא תהיה המערכת הממשלתית אלא המשתמש (האזרח). הסיכון למעשה, נמצא לפתחו של האזרח ולא לפתחה של המערכת.

כמובן שבמישור האישי, זה בהחלט לא נעים אם ישכפלו לי את נתוני ה SIM שלי או נתוני כרטיס חכם אחר אשר ברשותי אולם רמת הנזק הינה מוגבלת – אם יגנבו את הנתונים של החתימה הדיגיטלית שלי – אני עשוי לאבד את כל עולמי , כאשר מישהו אחר יוכל למכור את הרכב שלי ולבצע פעולות מהותיות אחרות .
כלומר ההבדל המהותי בין 2 הדוגמאות הוא מי מסתכן יותר כאשר קיים אובדן של מידע – במערכות העסקיות , הספק לוקח על עצמו סיכון, ואילו במערכות הממשלתיות – הצרכן / משתמש לוקח על עצמו את הסיכון.

כמובן, שאין איזכור בחקיקה , לכך שהממשלה תשפה את האזרח במידה ויתקיים שימוש לא נאות בחתימה שלו ..

ולכן, מערכת ממשלתית, אינה יכולה לגזור את שיטת הפעולה שלה משיטת הפעולה של יצרני הכרטיסים לשימוש מסחרי ולייצר בעבורי את המפתח הפרטי – ולו בגלל פוטנציאל הנזק.

אם כבר, היה נכון יותר לגזור את שיטת השימוש – כמו שהיא נהוגה במחשבים (שכל בעל מחשב יכול לייצר לעצמו את המפתח הפרטי) אך אז , אין דרך בטוחה להעביר את המפתח הפרטי עצמו לכרטיס.