Ministry of Justice
The Israeli Law, Information & Technology Authority (ILITA)

משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע

מדינת ישראל
State of Israel

מסמך רקע על חתימה אלקטרונית

חתימה אלקטרונית מאובטחת למול חתימה אלקטרונית מאושרת

גרסה 1.1

מעודכן: ספטמבר 2009

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

1. מבוא

מטרתו של מסמך זה להבהיר את המונחים "חתימה אלקטרונית מאובטחת" (**להלן – חתימה מאובטחת**) ו- "חתימה אלקטרונית מאושרת" (**להלן – חתימה מאושרת**) לפי חוק חתימה אלקטרונית, התשס"א-2001 (להלן – **החוק או חוק חתימה אלקטרונית**) ואת השימושים האפשריים בחתימה המאובטחת לעומת שימושי החתימה המאושרת.

המסמך מובא לצורך מענה לשאלות נפוצות שהופנו לרשם הגורמים המאשרים בדבר משמעותה של החתימה המאובטחת, דרכי ההוכחה כי טכנולוגיה מסוימת מקיימת את תנאי הסף להכרה בחתימה מאובטחת, וההבדלים בין חתימה **מאובטחת** לחתימה **מאושרת.**

2. כללי

חוק חתימה אלקטרונית מגדיר מהי "חתימה" בעולם האלקטרוני, ומסדיר את התוצאות המשפטיות של השימוש בה. החוק מבקש להשיג את הגברת הודאות המשפטית, בשימוש באמצעים אלקטרונים ליצירת מסמכים בעלי תוקף, על ידי קביעת תנאי סף להכרה משפטית באמצעים טכנולוגים. לצורך כך החוק מעמיד דרישות סף לחתימה מאובטחת ולחתימה מאושרת, וקובע הוראות לעניין קבילותה.

לפי החוק הותקנו שני קובצי תקנות: תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001 (להלן – **תקנות חומרה ותוכנה**), ותקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב-2001 (להלן – **תקנות רישום גורם מאשר**).

לפי החוק מונה "רשם גורמים מאשרים" במשרד המשפטים, שתפקידו לפקח על גורמים מאשרים לפי החוק, וכן מוקנות לו סמכויות נוספות הקשורות במימוש החוק.

החתימה המאובטחת אמורה לעשות שימוש בטכנולוגיות המאפשרות קישור חד ערכי בין החותם שחתם על המסר האלקטרוני לבין המסר אותו חתם, וכן לאפשר בדיקה האם נעשו במסר שינויים מאז שנחתם. להדגמה כללית ראה תרשים בנספח א'.

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

החתימה המאושרת אמורה, **<u>בנוסף לאמור לעיל</u>**, גם לזהות זיהוי חד חד ערכי של החותם, כלומר, להבטיח את זהותו גם על ידי אישור צד ג' אמין, הוא ה "גורם המאשר", אשר קיבל את אישור רשם הגורמים המאשרים. להדגמה כללית ראה תרשים בנספח ב'.

חלק גדול מההסדרים בחוק דומים לנורמות המקבילות באיחוד האירופי – המפורטות בדירקטיבה בדבר חתימה אלקטרונית משנת 1999[1].

אף כי מגמת החקיקה הישראלית והאירופאית הינה "ניטרליות טכנולוגית", כלומר ניסיון להימנע מקיבוע חקיקתי של גישה טכנולוגית ספציפית, מימושן בפועל מבוסס במידה רבה על התחום הכללי הידוע כ- "תשתית מפתח ציבורי" (PKI - Public Key Infrastructure)[2], ולמימושים הקיימים של תחום זה השלכה ישירה, כמפורט להלן, על החוק.

כך, לצורך הגברת הודאות והאמינות, על פי החקיקה האירופאית ולצורך מימושה הוקמו קבוצות תקינה שמטרתן כתיבת סטנדרטים טכנולוגים למימוש הצרכים הקונקרטים המוכתבים על ידי החקיקה, ועל ידי המאפיינים של "חתימה".[3] סטנדרטים אלה משמשים אמות מידה מנחות לעניין אופן המימוש הטכנולוגי.

---

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 Septmber 1999, on a Community framework for electronic signatures. http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=en

[2] ראה: http://www.ietf.org/html.charters/pkix-charter.html. תחום זה משמש כמובן לצרכים רבים ונוספים שאינם קשורים לחתימה.

[3] ראה: http://www.ictsb.org/Working_Groups/EESSI/Index.htm, קבוצת העבודה סיימה את עבודתה אם כי התקנים מטופלים ומעודכנים במסגרת משנה. ראה: http://portal.etsi.org/esi/el-sign.asp.

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

3. חתימה מאובטחת

אבן הפינה של החוק הינה הגדרת חתימה מאובטחת. סעיף 1 לחוק קובע, כי חתימה מאובטחת היא:

"חתימה אלקטרונית שמתקיימים בה כל אלה:

(1) היא ייחודית לבעל אמצעי החתימה.

(2) היא מאפשרת זיהוי לכאורה של בעל אמצעי החתימה.

(3) היא הופקה באמצעי חתימה הניתן לשליטתו הבלעדית של בעל אמצעי החתימה.

(4) היא מאפשרת לזהות שינוי שבוצע במסר האלקטרוני לאחר מועד החתימה".

הגדרה זו יש לקרוא יחד עם ההגדרות של "חתימה אלקטרונית"[4], "אמצעי חתימה"[5], ו- "מסר אלקטרוני"[6].

ההגדרה מבטאת את מאפייני ה"חתימה" על מסמך, בשינוי הנובע מכך שהחתימה מופקת באמצעות מכשיר או באמצעות טכנולוגיה, ולא בידו של החותם. מטרת הדרישה היא להבטיח כי בביצוע החתימה האלקטרונית יתקיימו המטרות של דרישת חתימה בעולם הפיזי: גמירות דעת, זיהוי החותם וקשירתו למסמך החתום ומניעת שינויים בנוסח החתום לאחר מועד החתימה. המאפיינים שהוגדרו בחוק לגבי החתימה המאובטחת הם: ייחודיות החתימה, זיהוי אמצעי החתימה של החותם, שליטתו הבלעדית של החותם על אמצעי החתימה (מאחר שההנחה היא שהחתימה נעשית באמצעות מכשיר ולא פיזית על ידי החותם), והאפשרות לזהות שינוי שנעשה במסמך לאחר שנחתם. המימוש הנפוץ של דרישות אלה הינו באמצעות שיטות הצפנה אסימטרית, כמפורט בהמשך.

[4] "חתימה אלקטרונית" – מוגדרת בסעיף לחוק: "חתימה שהיא מידע אלקטרוני או סימן אלקטרוני, שהוצמד או שנקשר למסר אלקטרוני"

[5] "אמצעי חתימה" מוגדר: "תוכנה, חפץ או מידע ייחודים, הדרושים להפקת חתימה אלקטרונית מאובטחת".

[6] "מסר אלקטרוני" מוגדר: "מידע אשר נוצר, נשלח, נקלט או נשמר באמצעים אלקטרונים או אופטיים, כשהוא נקרא, נשמע או מאוחזר באמצעים כאמור".

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

החידוש המרכזי של החוק הוא בעניין התוצאות המשפטיות של חתימה מאובטחת. סעיפים 3 ו- 6 לחוק[7] קובעים כי החתימה המאובטחת תהיה קבילה בכל הליך משפטי כראיה לכאורה לזהות החותם, וכי פלט החתום בה ייחשב כמקור ולא כהעתק, בכפוף לחריגים שנקבעו בתוספת השנייה לחוק[8]. בכך משנה החוק את המצב המשפטי שנהג לפניו, ומקנה לצדדים העושים שימוש בחתימה מאובטחת ודאות, שאינה מצריכה הסדר חוזי נפרד, ביחס לקבילות ולתוקף המשפטי של המסר האלקטרוני והחתימה המאובטחת.[9] ראו תרשים בענין "חתימה מאובטחת" בנספח א'.

3.1. דרכי ההכרה והשימוש בחתימה מאובטחת

למרות שבאופן כללי נוקט החוק בעיקרון הניטרליות הטכנולוגית, הרי שלמען היעילות, נקבעו בתקנה 8(1) לתקנות החומרה והתוכנה שלושה תנאים, שבהתקיימם תחול חזקה שחתימה אלקטרונית הינה חתימה מאובטחת[10].

---

[7] נוסח סעיף 3 לחוק:
"מסר אלקטרוני החתום בחתימה אלקטרונית מאובטחת יהיה קביל בכל הליך משפטי ויהווה ראיה לכאורה לכך -
(1) שהחתימה היא של בעל אמצעי החתימה;
(2) שהמסר האלקטרוני הוא זה שנחתם ע"י בעל אמצעי החתימה".
נוסח סעיף 6 לחוק:
"(א) פלט של מסר אלקטרוני החתום בחתימה אלקטרונית מאובטחת לא ייחשב, בכל הליך משפטי, כהעתק המסר האלקטרוני שעל בסיסו הופק, אלא כמקור.
(ב) הוראות סעיף קטן (א) לא יחולו על סוגים של מסרים אלקטרוניים, סוגים של הליכים משפטיים ושימושים מסויימים במסרים אלקטרוניים, שהשר קבע, באישור ועדת החוקה חוק ומשפט של הכנסת, בתוספת השניה".

[8] התוספת השנייה עוסקת במסמכים לגביהם יש חשיבות למקור כגון פסקי דין, שטרות ושטרי מניה למוכ"ז.

[9] מובן כי אין מניעה שצדדים המבקשים לסכם ביניהם בהסדר חוזי תוקף וקבילות של מסרים אלקטרונים, יעשו זאת שלא באמצעות החוק.

[10] נוסח תקנה 8:
"8. חזקה לעניין חתימה אלקטרונית מאובטחת
חתימה אלקטרונית מאובטחת שמתקיים בה אחד מאלה, חזקה שהיא חתימה אלקטרונית מאובטחת:
(1) לגבי אמצעי לאימות חתימה שמחזיק בידיו המבקש, ואמצעי החתימה שאותו הוא מזהה, מתקיימות לפחות הדרישות כמפורט להלן:
(א) החתימה מופקת באמצעות מפתח המבוסס על תקן מקובל, העושה שימוש באחד מאלה:
(1) מפתח RSA או DSA באורך 1024 סיביות לפחות;
(2) מפתח elliptic curve DSA באורך 160 סיביות לפחות;
(ב) להפעלת אמצעי החתימה או לגישה אליו, נדרש שימוש באמצעים פיזים או הצפנתיים (קריפטולוגים) ייחודים, העומדים ברמת אבטחה של תקן fips 140-2 רמה 1, ברמת ביטחון של תקן common criteria EAL 2 לפחות;
(ג) היתה הפעלת אמצעי החתימה כרוכה בשימוש בסממה, תעמוד הסממה בדרישות אבטחה ברמה הגבוהה לפי ת"י 1495 חלק 3, או בדרישות חלופיות שקבע הרשם, אם נוכח כי ניתן לפטור מהדרישה האמורה.

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

התנאי הראשון קובע הוראות לעניין **אלגוריתמים** ואורכי מפתחות המשמשים לחתימה אלקטרונית לצורך חתימה של בעל תעודה (משתמש קצה).

התנאי השני קובע הוראות לעניין אופן ההגנה על אמצעי החתימה, מבחינת דרישות אבטחת המידע מההתקן.[11]

התנאי השלישי עוסק בהגנה על הגישה והשימוש במפתח הפרטי.

יש להדגיש בעניין זה כי התקנה רק יוצרת **חזקה** לקיומה של חתימה מאובטחת העומדת בדרישות ההגדרה שבסעיף 1 לחוק. עם זאת החזקה איננה מוחלטת, ובמקרים שבהם התרחש כשל טכנולוגי או שיש סיבה אחרת לכפור בתקינות החתימה, יוכל טוען פוטנציאלי לנסות ולסתור אותה.[12] בנוסף, בתקנה 9[13] ניתנה לרשם הגורמים המאשרים סמכות לגופו של מקרה לקבוע כי טכנולוגיה ספציפית עומדת בדרישות תקנה 8(1) או לחילופין כי היא מייצרת חתימה מאובטחת, אף אם אינה עומדת בדרישת תקנה 8(1)[14].

---

(2) היא חתימה אלקטרונית שאישר הרשם לפי הוראות תקנה 9.

[11] בהקשר זה יצויין כי הדרישות המופיעות כיום בתקנות נמוכות מהסטנדרט העולמי המקובל, והמלצות הרשם הן כי רמת האבטחה תהיה ברמה של **common criteria EAL** 4 לפחות, או ברמה של **fips 140-2** ברמה 3 לפחות.

[12] על חזקה שבדין ראה באופן כללי, י. קדמי, על הראיות, כרך ג', עמ' 1260-1257.

[13] תקנה 9(א) קובעת:

"(א) מי שמעוניין בכך, רשאי לפנות בכתב, לשם קביעה -

(1) אם טכנולוגיה מסויימת עומדת בדרישות שנקבעו בתקנה 8(1), פניה כאמור תכלול מסמכים המתארים את הטכנולוגיה, לרבות תעודת התאמה לתקן מקובל, אם ישנה, וחוות דעת של מומחה אבטחת מידע בדבר אמינותה של הטכנולוגיה. הרשם רשאי לדרוש כל מידע אחר הדרוש לו כדי לבחון אם מדובר בטכנולוגיה העומדת בדרישות תקנה 8(1) וכדי לאשרה.

(2) כי טכנולוגיה מסויימת מפיקה חתימה אלקטרונית שחזקה שהיא חתימה אלקטרונית מאובטחת, אף שאין מתקיימות בה הוראות תקנה 8(1). פניה כאמור תכלול מסמכים כאמור בפסקה (1).

[14] צירוף הוראות אלו, יוצר למעשה מספר מסלולי שימוש בחתימה אלקטרונית מאובטחת, ברמה של ודאות משפטית משתנה:

המסלול הראשון, הוא לבחון האם האמצעי בו עושים שימוש, עונה על דרישות "חתימה מאובטחת" בחוק, ולהניח כי פרשנות זו תתקבל על דעת בית המשפט.

המסלול השני, הוא לבחון האם האמצעי בו עושים שימוש עונה על דרישות "חתימה מאובטחת" לפי תקנה 8(1).

המסלול השלישי, הוא לבקש את אישור הרשם לכך שהטכנולוגיה או המוצר מייצרים "חתימה מאובטחת" לפי תקנה 9 (תוך עמידה בתנאי תקנה 8(1) או תוך שימוש בשיקול דעתו של הרשם, כאמור).

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

מעבר לכך, כיוון שמדובר בחזקה בלבד, אין מניעה לקיים את הוראות סעיף 1 לחוק בדרכים אחרות וחלופיות שאינן מנויות בתקנות. במלים אחרות, אין מניעה כי מי שסבור שהפתרון הטכנולוגי שהוא יצר או משתמש בו, עונה מהותית על רכיבי הגדרת חתימה מאובטחת, בין כפי שהם מופיעים בחוק, ובין על פי הנושאים המוסדרים בתקנה 8, יעשה זאת. מובן שיהיה עליו לבסס טענה זו באופן כלשהו (כגון באמצעות חוות דעת טכנולוגית פנימית או חיצונית, או כלפי לקוחות פוטנציאלים של הטכנולוגיה, על מנת למזער טענות בדבר תוקף החתימה בעתיד.

3.2. דרישת **השליטה הבלעדית** באמצעי החתימה המאובטחת

כמפורט לעיל, אחת מן הדרישות להכרה בחתימה המאובטחת היא שהחתימה תופק "***באמצעי חתימה הניתן לשליטתו הבלעדית של בעל אמצעי החתימה***".[15]

בהקשר יסוד ה-"שליטה הבלעדית" הועלתה השאלה באילו נסיבות ניתן לשמור את החתימה האלקטרונית שלא על גבי התקן אישי שמטבעו מצוי <u>בשליטתו הפיזית</u> של בעל החתימה, כגון כרטיס חכם - אלא על גבי שרת מאובטח ייעודי המשמש לביצוע פעולות חתימה אלקטרונית בתקשורת.

לעניין זה נציין כי תקן אבטחת המידע האמריקני FIPS 140-2 ברמה 3 ו -4, מכיר באפשרות של קבלת תו-הסמכה גם לשרת מאובטח המחזיק מפתחות הצפנה, שניתן להשתמש בהם גם לצורך חתימה. זאת בתנאי שהשרת יאפשר לזהות בצורה חד ערכית את המשתמש, ובנוסף, ימנע גישה של מנהל רשת או כל גורם תחזוקה אחר לאמצעי החתימה האישי. כלומר, אין באפסון על גבי שרת, בהכרח, משום פגיעה בשליטה בלעדית, אך יש חשיבות רבה למנגנון המוודא את השליטה הבלעדית.[16]

עם זאת, משום שאמצעי החתימה אינו מצוי <u>בשליטתו הפיזית</u> של החותם, יש להקפיד ולבחון שביחס לסוג השרת והשימוש שנבחר, אכן נשמרת שליטה בלעדית באופן אחר. על פני הדברים נדרשת השלמה של אמצעי אבטחה לצורך כך. ניתן להבחין לעניין זה בין שימוש בשרת מאובטח בתוך ארגון, כאשר החתימות נעשות בעיקר בהקשר ארגוני ומחייבות את הארגון יחד עם האדם החותם, לבין מקרה שבו השרת המאובטח מצוי בידי צד שלישי זר לבעל אמצעי החתימה ולארגון. במקרה האחרון, רף האבטחה שיש להשיג לצורך הוכחת השליטה הבלעדית, יהיה גבוה יותר.

[15] פסקה (3) להגדרת "חתימה אלקטרונית מאובטחת" שבסעיף 1 לחוק.
[16] לעניין זה יש לציין כי גם "אמצעי החתימה" של גורם מאשר, המשמש לחתימה אלקטרונית על גבי תעודות אלקטרונית המשמשות לביצוע חתימה מאושרת לפי החוק, מוחזק על גבי שרת מאובטח.

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

בהקשר הארגוני, ככל שהחתימה נשמרת באמצעי ארגוני, יש להגן על מעמדו של היחיד- החותם, במובן זה שהארגון יטול על עצמו אחריות לשימוש, ולא יפגע בזכויותיו של המשתמש.

לסיכום, ניתן לתאר שלוש רמות של מימוש יסוד השליטה הבלעדית לגבי התקן המאפסן אמצעי חתימה; רמה אחת הינה רמה שבה ההתקן הינו התקן פיזי המצוי בשליטתו המלאה של האדם, כגון כרטיס חכם. רמה שנייה הינה רמה בה נשמר אמצעי החתימה בהתקן פיזי שאינו מצוי בשליטתו הבלעדית של בעל אמצעי החתימה, אולם בארגון שהחותם קשור אליו. ברמה זו יש להציג את האמצעים שבהם תישמר השליטה הבלעדית. בין אמצעים אלה, שימוש בשרתים מאובטחים ייעודיים שנבחנו לצורך כך, וכן בחינת מכלול נסיבות השימוש. הרמה השלישית הינה רמה שבה החתימה נשמרת בידי צד שלישי שאינו החותם או הארגון שהחותם קשור אליו. במקרים אלה, הרף הנדרש לאמצעי האבטחה הינו גבוה עוד יותר.

3.3. יישום טכנולוגי של דרישות החתימה המאובטחת- סיכום

צירוף הוראות אלו, יוצר למעשה מספר מסלולי שימוש בחתימה אלקטרונית מאובטחת, ברמה של ודאות משפטית משתנה:

המסלול הראשון, הוא לבחון האם האמצעי בו עושים שימוש, עונה על דרישות חתימה מאובטחת בחוק, ולהניח כי פרשנות זו תתקבל על דעת בית המשפט.

המסלול השני, הוא לבחון האם האמצעי בו עושים שימוש עונה על דרישות חתימה מאובטחת לפי תקנה 8(1).

המסלול השלישי, הוא לבקש את אישור הרשם לכך שהטכנולוגיה או המוצר מייצרים חתימה מאובטחת לפי תקנה 9 לתקנות (תוך עמידה בתנאי תקנה 8(1) או תוך שימוש בשיקול דעתו של הרשם, כאמור).

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

3.4. זיהוי החותם בחתימה מאובטחת

הגדרת חתימה מאובטחת, קובעת דרישה לעניין זיהוי לכאורה של "אמצעי החתימה", אולם לא מסדירה את אופן הזיהוי של האדם המחזיק באמצעי החתימה. הודאות שיוצר סעיף 3 רלבנטית רק לעובדה שהמסר לא השתנה מאז שנחתם על ידי מחזיק אמצעי החתימה. ראו עוד התרשים ביחס לחתימה מאובטחת בנספח א'.

צד המבקש לדעת ברמה גבוהה יותר של ודאות מיהו בעל אמצעי החתימה, ומבקש ולהסתמך על חתימה מאובטחת, צריך להסדיר באופן אחר כלשהו את בדיקת הזהות. אפשרות אחת, היא יצירת היכרות מוקדמת ישירה, בין הצדדים לתקשורת. דוגמא לכך היא ההסדר בהוראות מס הכנסה,[17] בהן נקבע כי תנאי מוקדם לתקשורת הוא "הסכמה" של הנמען לקבל חשבונית ממוחשבת. הדעת נותנת שבמסגרת הסכמה כזו, יסכימו הצדדים גם על אופן הזיהוי ההדדי שלהם.

אפשרות אחרת, היא הסתמכות על זיהוי על ידי צד שלישי ששני הצדדים סומכים עליו, במסגרת הסדר חוזי או אחר. במסגרת זו ניתן לכלול גם את קבוצת המקרים בהם הצדדים סומכים על מזהה ייחודי המצוי בידיהם, שהונפק על ידי צד שלישי, גם אם אין מערכת חוזית ישירה עמו, כגון הסתמכות על מספר חשבון או מספר כרטיס אשראי.

ניתן כמובן להקים מערך תעודות אלקטרונית פנימי או חיצוני, בהתאם לאפשרויות הטכנולוגיות בתחום ה- PKI [Public Key Infrastructure – ראה לעיל]. חלק מחלופות אלה יש כמובן לגבות בהסדר משפטי, כגון חוזה או תקנון, משום שאינן מוסדרות בחוק חתימה אלקטרונית.

[17] הוראות מס הכנסה (ניהול פנקסי חשבונות), תשל"ג-1973, תקנות מס ערך מוסף (ניהול פנקסי חשבונות), תשל"ו-1976.

Government Campus, 9th floor
125 Begin Road
P. O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת. ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

4. חתימה מאושרת

חתימה מאושרת[18] נותנת מענה לבעיית הזיהוי הוודאי של האדם המחזיק באמצעי החתימה. החתימה המאושרת היא חתימה מאובטחת, שזהות מחזיק אמצעי החתימה המפיק אותה מאומתת ע"י תעודה אלקטרונית שהנפיק גורם מאשר[19], בהתאם לכללים מחייבים המוגדרים בחוק ובתקנות לפיו. התעודה האלקטרונית מוסיפה יסוד של זיהוי על ידי צד ג', הנמצא תחת משטר רישוי ופיקוח, ובכך מגבירה מאוד את הודאות לגבי זהות בעל אמצעי החתימה. ראו תרשים בנושא חתימה מאושרת בנספח ב'.

בשונה מחתימה **מאובטחת,** שאין מגבלות בחוק על רכישת האפשרות לבצעה, האפשרות לבצע חתימה **מאושרת** ניתנת לרכישה רק מ"גורם מאשר" שקיבל הסמכה לפי החוק. להשלמה יצוין, כי בכל הקשור לחתימה **מאושרת**, תקנה 13(א) לתקנות החומרה והתוכנה[20] מחייבת את הגורם המאשר, בהנפיקו תעודה אלקטרונית לפי החוק, לוודא כי בידי המחזיק אמצעי העומד בדרישות תקנה 8. לשון אחר, נשלל מגורם מאשר שיקול הדעת לעניין טווח האמצעים הטכנולוגים שיכולים לשמש לחתימה **מאובטחת**, שכן הוא חייב להשתמש רק בטכנולוגיות המנויות בתקנות, או שאושרו מראש על ידי הרשם לפי תקנה 9.

הניסיון מלמד, כי בדרך כלל, הגורם המאשר הינו גם מי שמוכר לבעל התעודה את אמצעי החתימה, ומכאן שהוא הגורם הנכון להיות אחראי לעמידה בהוראות תקנה 8(1). עם זאת, בתקנה 13(ב), ניתנה לגורם המאשר אפשרות לקבל מבעל אמצעי החתימה הצהרה, לפיה הטכנולוגיה בה הוא משתמש עומדת בהוראות תקנה 8(1); אם אין לגורם המאשר יסוד לחשוד כי ההצהרה כוזבת, על הגורם המאשר להנפיק תעודה אלקטרונית על בסיס אמצעי חתימה זה.

יודגש שוב, כי מבחינת הבסיס הטכנולוגי, כלומר, התשתית המשמשת להצפנה ואמצעי החומרה המגנים על החתימה האישית, יש זהות מוחלטת בין חתימה מאובטחת לחתימה מאושרת על פי התקנות. ההבדל ביניהן מצוי רק ברמת הודאות של זהות בעל אמצעי החתימה.

[18] חתימה אלקטרונית מאושרת מוגדרת בסעיף 1 לחוק כדלקמן- "חתימה אלקטרונית מאובטחת אשר גורם מאשר הנפיק תעודה אלקטרונית בדבר אמצעי אימות החתימה המזהה אותה".
[19] "גורם מאשר" מוגדר בסעיף 1 לחוק כדלקמן: "גורם המנפיק תעודות אלקטרוניות, והרשום במרשם לפי חוק זה".
[20] תקנה 13(א) קובעת: (א).

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

5. הבדלים נוספים – חתימה אלקטרונית מאובטחת ומאושרת

5.1. הוראות בעניין אחריות לחתימה ולשימוש בה

חובות השמירה המוטלות על בעל אמצעי החתימה ביחס לאמצעי החתימה, הן זהות, בין אם החתימה היא מאובטחת ובין אם היא מאושרת, וזאת בשל ההסדר הנובע מסעיף 7(א)(1) לחוק. לפי סעיף 7(א)(1), בעל אמצעי חתימה נדרש לנקוט בכל האמצעים הסבירים לשם שמירה על אמצעי החתימה שלו ולשם מניעת שימוש בו ללא הרשאתו.

לעומת זאת, קיים הבדל בין שני סוגי החתימות ביחס לחובות המוטלות על בעל אמצעי החתימה במקרה שנפגעה שליטתו באמצעי החתימה. בעל חתימה **מאובטחת** צריך למסור הודעה מייד כשנודע לו על "פגיעה בשליטתו" באמצעי החתימה, לכל מי שסביר שיסתמך עליה[21]. בעל חתימה **מאושרת**, לעומת זאת, צריך להודיע על כך רק לגורם המאשר. משלב ההודעה לגורם המאשר, בעל החתימה יהיה פטור מאחריות ביחס לשימוש לרעה באמצעי החתימה. חובתו של הגורם המאשר היא לבטל את התעודה שהונפקה לבעל אמצעי החתימה, ולפרסם זאת ברשימת התעודות הבטלות[22], ובכך למנוע הסתמכות על חתימה שנעשתה תוך שימוש לרעה.

עם זאת, באמצעות הסדרים חוזיים מוקדמים, ניתן לצמצם גם את ההיקף של חובת ההודעה של בעל אמצעי חתימה מאובטחת, על פגיעה בשליטתו באמצעי החתימה. כך, בכל הקשור לחתימה מאובטחת, ניתן להשלים את הסדרי האחריות של סעיף 7 לחוק, באמצעות הסדר חוזי. כך למשל, במסגרת מערך של חתימות מאובטחות, ניתן לקבוע <u>בחוזה</u> בין בעל אמצעי החתימה לבין מנפיק האמצעי המשמש לחתימה מאובטחת (להלן – מנפיק התיעוד), ובחוזה בין מנפיק התיעוד לבין מי שמסתמך על התעודה החתימה המאובטחת, כי בעל אמצעי החתימה ייצא ידי חובתו בהודעה למנפיק

---

[21] סעיף 7 לחוק קובע:
"7. חובות בעל אמצעי חתימה ואחריותו
(א) בעל אמצעי חתימה –
(1) ינקוט את כל האמצעים הסבירים לשם שמירה על אמצעי החתימה שלו ולשם מניעת שימוש בו בלא הרשאתו.
(2) ימסור הודעה, מייד כשנודע לו על פגיעה בשליטתו באמצעי החתימה, לכל מי שסביר שיסתמך על חתימתו האלקטרונית עקב קשרים שגרתיים בינהם, ולכל מי שידוע לו כי קרוב לודאי שיסתמך על חתימתו האלקטרונית.
(ב) קיים בעל אמצעי החתימה את חובותיו כאמור בסעיף קטן (א), לא יהיה אחראי לנזק שנגרם עקב שימוש באמצעי החתימה שלו בלא הרשאתו".

[22] CRL – Certificate Revocation List.

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

התיעוד. מקום שמנפיק התיעוד הוא, ורק הוא, מי שאמור להסתמך על החתימה המאובטחת, יש לציין זאת על גבי האמצעי המשמש לחתימה המאובטחת. אם אחרים אמורים להסתמך על החתימה המאובטחת, ניתן להסדיר חוזית מנגנון של פרסום רשימת תעודות בטלות, בדומה למנגנון הפעולה של גורם מאשר או הסדר מקביל אחר. משמעות האמור כאן היא ייצור הסדר חוזי דמוי ההסדר הקבוע בחוק. מדובר בהסדר מורכב יותר בשל הצורך בהסכמה מוקדמת של בעל אמצעי החתימה ושל המסתמך.

5.2. סעיף 2 לחוק - דרישת חתימה בחיקוק

סעיף 2 לחוק[23] מקנה עדיפות לשימוש בחתימה המאושרת בכך שהוא קובע שרק החתימה המאושרת מקיימת דרישת חתימה המופיעה בחיקוק.[24]. עם זאת, הוראה זו אינה משקפת בהכרח בדיקה של מכלול דרישות החתימה בחיקוק בחקיקה ספציפית. בנוסף, דרישות חתימה בחיקוק עשויות לנבוע מנימוקים שונים– גמירות דעת, זיהוי החותם וקיבוע הנוסח החתום או תיעוד מועד החתימה. לכן, אין מניעה שבהקשרים ספציפיים יחוקק בחיקוק הרלבנטי הסדר פרטני, הממיר את דרישת החתימה המאושרת בהסדר מפורט המבוסס על חתימה מאובטחת. כך, למשל, בהוראות ניהול ספרים[25], נקבעו הוראות מיוחדות לגבי אפשרות חתימה על מסמך ממוחשב **בחתימה מאובטחת**, אם הנישום יקבל את התקבול בגין המסמך באחד מהאמצעים שהוגדרו בחוק, ובאופן המאפשר את זיהויים של הצדדים לעסקה. הוראה זו באה לשמש כתחליף לרכיב הזיהוי שאותו מספקת התעודה האלקטרונית שמנפיק הגורם המאשר בחתימה מאושרת, ומשמשת כאמצעי זיהוי אחר. למעשה, ההסדר קובע שבמקרה זה אם הלקוח ישלם על העסקה באמצעי תשלום המבטיח את זיהוים של שני הצדדים, ניתן לוותר על הדרישה לחתימה מאושרת.

[23] נוסח סעיף 2 לחוק: "2 (א) נדרשה לפי חיקוק חתימתו של אדם על מסמך, ניתן לקיים דרישה זו, לגבי מסמך שהוא מסר אלקטרוני, באמצעות חתימה אלקטרונית, ובלבד שהיא חתימה אלקטרונית מאושרת" (ב) הוראות סעיף קטן(א) לא יחולו על הוראות חיקוק שהשר קבע, באישור ועדת החוקה חוק ומשפט של הכנסת, בתוספת הראשונה".

[24] בתוספת הראשונה לחוק נקבעו מסמכים שבהם אי אפשר לחתום אלקטרונית גם בחתימה אלקטרונית מאושרת, כגון צוואות, פסקי דין ושטרי עסקה במקרקעין.

[25] הוראות ניהול ספרים סעיף 18 ב (ד)

Government Campus, 9th floor
125 Begin Road
P. O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת. ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

6. סיכום

חתימה אלקטרונית **מאובטחת** מקנה לצדדים לתקשורת ודאות בדבר מניעת התכחשות צד לתקשורת לתוכן המסר שעבר ונחתם על ידו. הדרכים למימוש חתימה אלקטרונית מאובטחת נשארות לשיקול דעת הצדדים, כאשר תקנות חתימה אלקטרונית מציעות שתי דרכי מימוש אפשריות מבין דרכים רבות אפשריות. המטרה המוצהרת של הגדרות פתוחות אלה הייתה גמישות טכנולוגית שמאפשרת לצדדים לבחור את סוג הטכנולוגיה שהם מבקשים להתבסס עליה, ובלבד שתעמוד בהוראות החוק. אין דרישה בחוק ובתקנות למעורבות של הגורם המאשר בקיומה של חתימה מאובטחת.

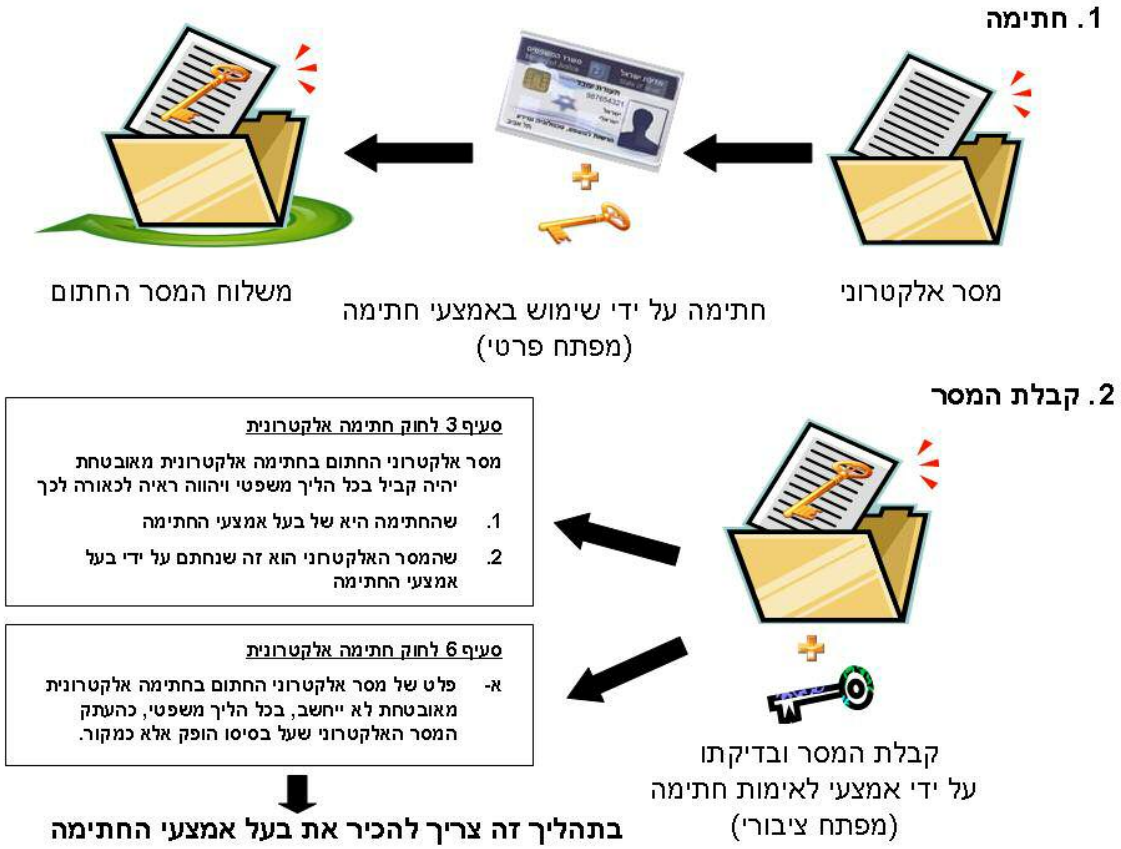
חתימה **מאושרת** מקנה לצדדים לתקשורת את הודאות שצוינה לעיל ביחס לחתימה מאובטחת, אולם היא מכוונת מבחינה טכנולוגית לסוג פתרון מסוים. לצד הגבלה זו, היא מקנה ודאות שהיא חתימה מאובטחת בשל חיובו של הגורם המאשר לעמוד בהוראות התקנות. בנוסף, מקנה חתימה מאושרת לצדדים את הודאות בדבר זהות בעל אמצעי החתימה ותוקפה והיא מפשטת את מנגנון ההודעה על איבוד השליטה באמצעי החתימה.

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

נספח א' - תרשים חתימה אלקטרונית מאובטחת

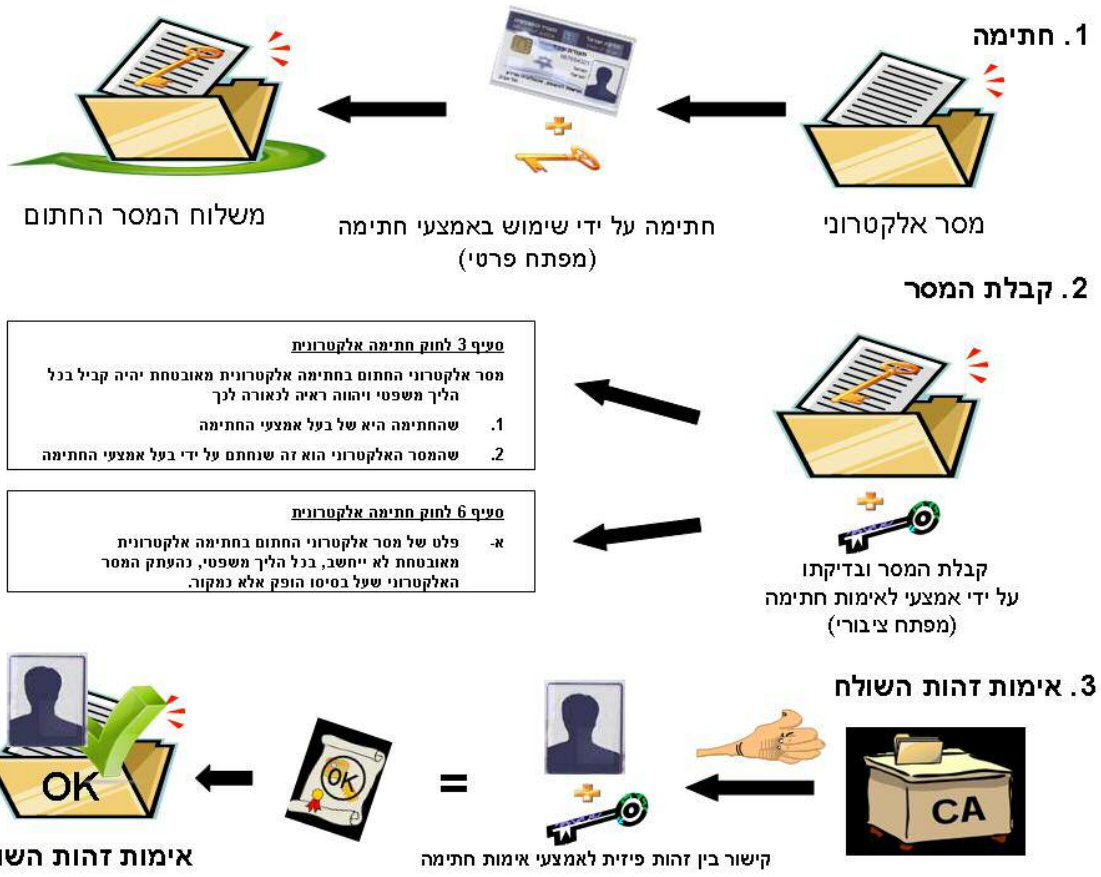


Government Campus, 9th floor
125 Begin Road
P. O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת. ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

נספח ב' – תרשים חתימה אלקטרונית מאושרת



Government Campus, 9th floor
125 Begin Road
P. O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת. ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064