



מדינת ישראל
 משרד האוצר - אגף החשב הכללי
 אתר טכנולוגיות המידע הממשלתי
 WWW.ITPOLICY.GOV.IL

שם המסמך : חתימה דיגיטלית
 תאריך כתיבה : 20/5/01
 גרסא : 1.0
 כותבי המסמך : שגית אהרונסון

חתימה דיגיטלית

תוכן עניינים

1	מבוא	1
2	מהי חתימה דיגיטלית?	2
2.1	שיטת המפתח הציבורי (PKI)	2.1
2.2	איך זה עובד?	2.2
2.3	"גורם מאשר"	2.3
3	חוק חתימה אלקטרונית התשס"א - 2001	3
3.1	מדוע נדרש החוק?	3.1
3.2	חוק חתימה אלקטרונית – מושגי יסוד והוראות	3.2
4	הלכה למעשה – הפרויקט הממשלתי "תמר"	4
5	קישורים	5

1. מבוא

בעשור האחרון חלה התפתחות עצומה ביכולת העברת מידע באמצעים אלקטרוניים. טכנולוגיית המידע ואפשרויות התקשורת המהירה יצרו מציאות חדשה המצריכה הסתגלות בכמה היבטים ובעיות. בעיה אחת ציפתה במשך כמה שנים לפתרון – החתימה הדיגיטלית.

אחד המאפיינים של התקשורת באינטרנט הוא היעדר זיהוי ודאי של הגולש, כלומר, לא ניתן לדעת בוודאות מיהו האדם הספציפי הגולש לאתרים, ממלא טפסים והוראות תשלום. בעוד יישומים רבים ברשת התפתחו על כר האנונימיות שהיא מספקת (צ'טים, קבוצות דיון...), נידונו יישומים אחרים הדורשים וודאות בזיהוי הגולש להמתין כמה שנים עד שתיפתר הבעיה.

בעולם שמחוץ לרשת, בכל פעם שבו נדרשת חתימה אישית של אזרח, חייב הוא להתייצב ולחתום באופן פיזי על הניירת הרלוונטית על מנת שיהיה שיוך פיזי בינו לבין חתימתו.

העדר הזיהוי הוודאי "תוקע" תהליכים ושירותים רבים שהרשויות יכולות לספק לאזרחים באמצעות הרשת, מפני שלא ניתן לדעת בוודאות מיהו האזרח שחתם על טפסים או הוראות תשלום שנשלחו ברשת.

האבטחה שפותחה עבור אתרים הגובים תשלום מלקוחות בשיטת SSL (Secure Socket Layer) מבטיחה לגולש את הוודאות כי האתר הגובה ממנו כסף, הוא אכן האתר האמיתי ולא אתר אחר המתחזה לו וכן מאפשרת הצפנת המידע העובר מהגולש לאתר כך שקשה "להאזין" למידע, אך אין כל וודאות לאתר כי הגולש המשלם, הוא אכן האדם ששמו מופיע בהוראת התשלום.

במטרה לפתור בעיה זו פותחה שיטת החתימה הדיגיטלית, אך כפי שקורה פעמים רבות נוצר פער בין היכולות הטכנולוגיות לבין המצב המשפטי.

הסיבה לפער היא הנכונות לנטילת סיכונים המאפיינת את עולם ההי-טק לעומת השמרנות המאפיינת את העולם המשפטי שבו הנטייה היא לקחת פחות סיכונים ו"ללכת יותר על בטוח".

מבחינה משפטית, חתימתו האישית של אדם, היא הרשאה הנדרשת להנעת תהליכים מסוימים הקשורים בו כגון הסכמים, אישורי תשלום, ייפוי כוח וכו'. חתימה היא שיוך של אדם לסימן

אישי המאפשר לחותם שלא להיות נוכח פיזית בכל השלבים של תהליך מסוים מרגע החתימה. לדוגמה – אם חתם אדם על צ'ק, אין צורך לאמת את זהותו של האדם בשעת ביצוע העברת צ'ק או פדיונו מפני שחתימתו (שנחתמה בתנאים של זיהוי וודאי) מתנססת על הצ'ק.

כדי להתמודד עם בעיית התקפות המשפטית של חתימה דיגיטלית נחקק בישראל חוק חתימה אלקטרונית המאפשר העברת מסמכים חתומים באופן שיקשה מאוד על זיופם.

מאמר זה עונה על השאלות הבאות:

- מהי חתימה דיגיטלית – הטכנולוגיה או איך זה עובד
- חוק חתימה אלקטרונית, התשס"א - 2001

הערה: אין הבדל בין המושגים חתימה אלקטרונית וחתימה דיגיטלית.

2. מהי חתימה דיגיטלית?

חתימה דיגיטלית היא קובץ מוצפן המצורף להודעה או למסמך המאפשר זיהוי של שולח ההודעה או המסמך ומבטיח שהתוכן המקורי של ההודעה או המסמך לא ישתנה אחרי החתימה. חתימות דיגיטליות מבוססות על תיאוריה מתמטית ועל שימוש באלגוריתם. הן דורשות שבעל החתימה חיזיק בשתי מפתחות לחתימה ולזיהוי (מפתח אחד פרטי ומפתח אחד ציבורי – ראה להלן).



2.1. שיטת המפתח הציבורי (PKI)

שיטת המפתח הציבורי מאפשרת למשתמשים בסביבה לא מוגנת כמו למשל אינטרנט להחליף מידע וכסף בצורה מאובטחת ופרטית ע"י שימוש בזוג מוצפן של מפתחות: פרטי וציבורי. לזוג המפתחות קשר מתמטי מסוים. כאשר המפתח הציבורי יכול לזהות את החתימה הדיגיטלית שיצר המפתח הפרטי ולא ניתן בשום דרך מתמטית או ע"י מחשב לגלות או לפענח את המפתח הפרטי באמצעות המפתח הציבורי. לכן ניתן לגלות את המפתח הציבורי לכל מבלי לסכן את המפתח הפרטי.

זוג המפתחות הם למעשה זוג קבצים המוקצה לכל משתמש.

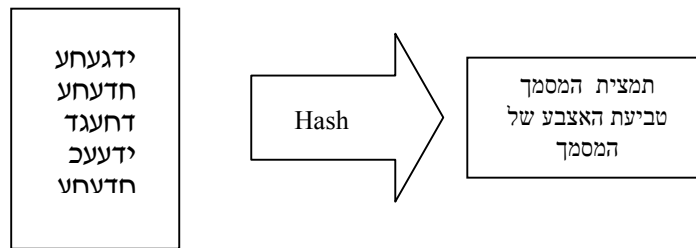
1. מפתח פרטי – קוד מספרי הידוע רק לאדם שהחתימה שייכת לו.
2. מפתח ציבורי – קוד מספרי חופשי לשימוש לכל מי שרוצה לעמוד בקשר עם בעל החתימה. את הקוד הציבורי ניתן לקבל מהאדם עצמו או מרשות מוסמכת.

צירוף של הקוד הפרטי והקוד הציבורי משול לפתיחת המנעול. את המפתח הפרטי יקבל המשתמש על גבי תקליטון, תקליטור, כרטיס חכם או פלאג. את המפתח הפרטי מתקינים על המחשב אך יש חובה לשמור עליו כפי ששומרים על תעודת זהות או דרכון. כמו עם תעודות זהות, יש בחוק חובה להודיע שהתעודה הדיגיטלית נגנבה. האחריות להחזיק בתעודה ולשמור עליה היא של בעליה. את המפתח הציבורי אפשר להוריד בקלות מהאינטרנט. לכל משתמש יהיה מפתח פרטי ומפתחות ציבוריים רבים ששיכים למשתמשים אתם הוא מתכתב.

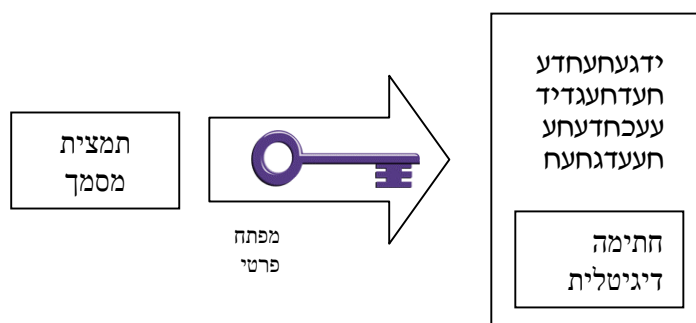
2.2. איך זה עובד?

אדם שולח מסמך וסוגר אותו במפתח פרטי. הנמען, האדם המקבל את המסמך, מצויד במפתח ציבורי שנשלח אליו על ידי השולח. כאמור, צירוף שני המפתחות פותח את המסמך תוך ידיעה וודאית שהוא נשלח על ידי האדם ששלח אותו – האדם המחזיק ברשותו מפתח פרטי. כמובן שפתיחת המסמך אינה מאפשרת למקבל המסמך לדעת מהו הקוד הפרטי. אם לדוגמה ייסגר המסמך על ידי אדם אחר, הקוד הפרטי והציבורי לא יתחברו לפתיחת המסמך. כדי לוודא שמי שקורא את המסמך הוא אך ורק הנמען, יצטרך השולח להצפין אותו ע"י המפתח הפרטי. הנמען יוכל לפענח אותו ע"י המפתח הציבורי שברשותו. דוגמה:

כדי לחתום על מסמך השולח נעזר בתוכנה שמכווצת את המידע במסמך לכמה שורות בלבד ע"י תהליך שנקרא "hashing" - תהליך שיוצר מספר שהוא תמצית מזהה של מסמך כמו טביעת האצבע של המסמך. תמצית מסמך זו נקראת "Message Digest". הטענה היא שקשה מאד לזייף אותו. כלומר, לא ניתן לבנות שני מסמכים שונים בעלי טביעת אצבע זהה.



את טביעת האצבע של המסמך מצפינים ע"י המפתח הפרטי. את התוצאה מצרפים למסמך שרוצים לחתום עליו בחתימה דיגיטלית. מתקבל מסמך חתום בחתימה דיגיטלית.



פענוח וזיהוי המסמך והחתימה ע"י הנמען :
 הנמען מחשב תחילה את טביעת האצבע של המסמך המקורי ע"י יצירת "Hash" של המסמך. אח"כ מפענחת את החתימה הדיגיטלית תוך שימוש במפתח הציבורי. אם פענוח החתימה הדיגיטלית, וטביעת האצבע של המסמך זהות, ניתן להניח כי השולח אכן חתם על המסמך המקורי.

2.3 "גורם מאשר"

המרכיב החשוב בשיטה הוא קיומה של ישות אמינה, הרשומה על פי חוק, שמנפיקה ומפיצה חתימות דיגיטליות. ישות כזאת נקראת "גורם מאשר".
 "גורם מאשר" – סעיף 1 לחוק חתימה אלקטרונית, התשס"א 2001 - "גורם מאשר רשאי להנפיק לאדם מסוים, לפי בקשתו, תעודה אלקטרונית, המאשרת כי אמצעי אימות חתימה מסוים הוא שלו".
 תעודת זיהוי אלקטרונית שבה כתובים פרטיו האישיים של האדם או הגוף מולו מנהלים את התקשורת הוא ראשיתה של כל העברת מידע בטוחה.

על מנת שחתימה דיגיטלית תקבל מעמד משפטי זהה לחתימה רגילה, היא חייבת להיות מונפקת על ידי "גורם מאשר" (Authority Certificate-CA) העומד בתנאים שנקבעו בחוק. הגורם המאשר מוודא בדרכים שונות (פיזית, בטלפון....) את זהותו של אדם המעוניין להחזיק באמצעי חתימה דיגיטלית. לאחר הזיהוי מקבל האדם המעוניין זוג מפתחות פרטי וציבורי. בנוסף מונפקת תעודה האלקטרונית המתלווה למסמך ומאשרת לציבור כי המפתח הציבורי הוא של אדם או גוף מסוים. קשר זה מונע התכחשות של החותם למסמך שחתם בחתימה דיגיטלית. הגורם המאשר פועל כצד שלישי לעסקה ומשמש כגוף מזהה הנאמן על הצדדים. בהיותו גורם אמין ומוסמך יש חשיבות רבה למקצועיות ואמינות הגוף המשמש כגורם מאשר. הגורם המאשר אינו יכול לשמור מפתחות פרטיים של האנשים המזוהים על ידו.

מה שמבדיל בין גופים רציניים וגופים קיקיוניים של חתימות דיגיטליות, הוא התשתית שעומדת מאחוריהם. חב' VeriSign למשל, מחזיקה את המפתח הפרטי שלה שמשמש להנפקת כל התעודות הדיגיטליות שלה באופן מאובטח ברמה הפיסית והדיגיטלית. אם המפתח הזה נגנב, הרי שניתן מיד לזייף את כל התעודות שהונפקו.

3. חוק חתימה אלקטרונית התשס"א - 2001

ונתחיל בציטוט - "חתימה - הנה מושג מתחום דיני החוזים והראיות, אשר זכה לפרשנויות שונות. בעידן הטכנולוגי המתפתח, ניתן לבצע את החתימה בדרכים שונות מאשר בעבר ולכן מתעורר צורך לעגן את האפשרויות הטכנולוגיות בחקיקה... מטרתו העיקרית של החוק המוצע היא להגביר את הוודאות לגבי פעולות המתבצעות באופן אלקטרוני על ידי הבטחת זהותם של החותמים באמצעים אלקטרוניים מסוימים, והכרה במעמדם הראייתי של חתימות אלה. חוסר הוודאות מתעורר במיוחד בהתקשרויות דרך רשת האינטרנט, אשר הנה רשת תקשורת פתוחה, המתאפיינת בהיעדר זיהוי הדדי והיעדר קשר ישיר בין הצדדים המתקשרים בעסקה" (מתוך הצעת חוק חתימה אלקטרונית - תש"ס 2000).

3.1. מדוע נדרש החוק?

להגביר את הוודאות בעולם בו מתן אמון הוא קרקע בסיסית לבצוע עסקאות ברשת. להגדיר את מעמדה המשפטי ואת כוחה של החתימה הדיגיטלית להגדיר את חלוקת הנטל והאחריות להסדיר בפרוצדורה את קיומם של גורמים מאשרים

החוק עצמו התקבל בכנסת ביום 26.3.01 וייכנס לתוקפו ביום 25.9.01. אישור החוק הוא פריצת דרך משמעותית כי הוא קובע שהסטטוס המשפטי של חתימה דיגיטלית יהיה דומה לחתימה הכתובה. המשמעות היא שכל מי שמחזיק בחתימה דיגיטלית יוכל ליהנות מן ההכרה מול אותו גורם עסקי אתו הוא מתקשר דרך הרשת.

3.2. חוק חתימה אלקטרונית – מושגי יסוד והוראות

"חתימה אלקטרונית" – חתימה שהיא מידע אלקטרוני או סימן אלקטרוני, שהוצמד או שנקשר למסר אלקטרוני;

"חתימה אלקטרונית מאובטחת" - 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;

אמצעי חתימה – תוכנה או חפץ או מידע יחודיים, הדרושים להפקת חתימה אלקטרונית מאובטחת.

"חתימה אלקטרונית מאושרת" - חתימה אלקטרונית מאובטחת אשר גורם מאשר הנפיק תעודה אלקטרונית בדבר אמצעי אימות החתימה המזהה אותה;

גורם מאשר - גורם שהוכר לפי הוראות סעיף 22, והרשום במרשם לפי הוראות חוק זה. גורם מאשר רשאי להנפיק לאדם מסוים, לפי בקשתו... תעודה אלקטרונית.

תעודה אלקטרונית - מסר אלקטרוני שהנפיק גורם מאשר לפי הוראות פרק ד', המאשר כי אמצעי אימות חתימה מסוים הוא של אדם מסוים. פרטי תעודה אלקטרונית:

גורם מאשר יכול בתעודה אלקטרונית לפחות את הפרטים הבאים:

1. שמו של בעל התעודה ומספר תעודת הזהות שלו, או פרט מזהה אחר, כפי שקבע השר (שר המשפטים)

2. אישור בדבר בדיקת אמצעי אימות החתימה של בעל התעודה
3. המספר הסידורי של התעודה האלקטרונית במאגר שהוא מנהל
4. ציון האופן שבו זוהה בעל התעודה
5. ציון מועדי התחילה והסיום של תוקף התעודה
6. שמו ומענו של הגורם המאשר, ודבר רישומו במרשם
7. חתימתו האלקטרונית המאובטחת של הגורם המאשר
8. מידע בדבר קיומן של הגבלות על השימושים המותרים לפי התעודה, ככל שישנן, ואם היתה הגבלה על סכום העסקאות שלגביהן ניתן לעשות שימוש בתעודה – פירוט הסכום
9. מידע בדבר קיומן של הגבלות על אחריותו של הגורם המאשר, ככל שישנן
10. הפניה למאגר התעודות האלקטרונית הבטלות כאמור בסעיף 18 (ג).

תוקף חתימה אלקטרונית מאובטחת

קבילות חתימה אלקטרונית מאובטחת – 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 על ידי בעל אמצעי החתימה.

(1) אחריות לפי החוק

חובות בעל אמצעי החתימה ואחריותו –

1. לנקוט בכל האמצעים הסבירים לשמירה על אמצעי החתימה שלו, ולשם מניעת שימוש בו ללא הרשאתו.
 2. ימסור מיד כשנודע לו על פגיעה בשליטתו באמצעי החתימה, לכל מי שסביר שישתמך על חתימתו האלקטרונית עקב קשרים שגרתיים ביניהם, ולכל מי שידוע לו כי קרוב לוודאי שישתמך על חתימתו האלקטרונית.
- חובות גורם מאשר –
1. גורם מאשר לא ינפיק תעודה אלקטרונית אלא לאחר שנקט באמצעים סבירים לזהות את המבקש, לבדוק את אמצעי אימות החתימה ולבדוק כי הפרטים שבבקשה נכונים ומלאים.
 2. גורם מאשר ינהל מאגר תעודות אלקטרוניות שהנפיק וכן מאגר של הבטלות.
 3. לצורך ביצוע תפקידו ישתמש רק במערכות חומרה ותוכנה מהימנות, המעניקות הגנה סבירה מפני חדירה, שיבוש או גרימת נזק ומקנות רמה סבירה של זמינות ואמינות.
 4. לבטל תעודה אלקטרונית בכל המקרים המוגדרים בסעיף 20.

בעקבות אישור החוק קיבל ההליך תוקף חוקי, אולם אין עדיין תקנות ברורות המסדירות את השימוש בחתימה.

שר המשפטים הוא האחראי על הסדרת התקנות שיפרטו מהם הקריטריונים לקביעת "גורם מאשר" כלומר אותו גורם שאחראי להנפיק את התעודות הדיגיטליות, וכן קריטריונים למתן האישור לאותו גורם מאשר, כלומר מהם התנאים למתן תוקף חוקי מטעם המדינה. כמו כן יקבע כיצד ניתן יהיה להשתמש בתעודות הדיגיטליות ומה תהיה רמת התקפות המשפטית של התעודות.

4. הלכה למעשה – הפרויקט הממשלתי "תמ"ר"

תמ"ר - תשתית מפתח ציבורי

פרויקט ממשלתי חדשני שמנוהל במשרד האוצר במסגרת אגף מערכות מידע של החשב הכללי. בצוות הפרויקט משתתפים רוב משרדי הממשלה מטרתו היא לקדם את נושא הממשל הזמין בין האזרח לממשלה בעזרת טכנולוגיית החתימה הדיגיטלית וה- PKI. הנושאים אותם מקדם הפרויקט:

- התקשרות למאגרי מידע אישיים בממשלה;
- חתימה על טפסים;
- ביצוע טרזנאקציות כספיות הדורשות חתימה דיגיטלית.

הפעילות מתחלקת לשניים:

1. בתוך הממשלה
- הפקת תעודה שעליה תהייה חתימה אלקטרונית ומפתח פרטי. התעודה תאפשר זיהוי של בעליה וע"י כך תאפשר ביצוע פעולות מול מערכות המידע השונות.
 - o הפיילוט הראשוני יתקיים במשרד החוץ, כאשר עובדים שיכנסו לבניינים החדשים של המשרד לקראת סוף 2001 יוכלו להזדהות בכל מקום שעוברים בדרך כמו למשל: כניסה לחניון, כניסה לבניין וכן יוכלו לחתום על טפסים ותאפשר להם גישה למערכות מידע של המשרד. לאחר הצלחת פרויקט זה הוא ייושם ביתר קרייית הממשלה.

2. מול אזרחי המדינה
- הנפקת כרטיס חכם (תעודת זהות) שיכלול בין השאר חתימה דיגיטלית ומפתח.
 - o הפיילוט הראשון מתבצע עם משרד הפנים (מנהל האוכלוסין ואנשי פרויקט אביב. הפיילוט כולל הוצאה של מכרז ל-CA וכן לכרטיסים וקוראים חכמים, הפקה של כ-1000 כרטיסים כאלו שבאמצעותם ניתן יהיה למלא טפסים של משרד הפנים באינטרנט, חתימה עליהם והעברתם למשרד הפנים, חתימה דיגיטלית של פקיד עליהם והעברת אישור תוך ביצוע הטרוזאקציה למערכות המידע הפנימיות (הפיילוט אמור להסתיים עד סוף 2001)

כעת, כשהטכנולוגיה קיימת, והחוק עומד להיכנס לתוקפו בסתיו הקרוב, ונותרו רק מספר השלמות טכניות להשלמתו, ובמשרד האוצר שוקדים על פרויקט "תמר", נותר רק להכריז כי עידן החתימה הדיגיטלית התחיל. האם הציבור ומוסדות ציבוריים יאמצו את השינוי התרבותי? האם נתגבר על ההתנגדות לשינויים טכנולוגיים והפחד ממעשי מרמה? ימים יגידו.

5. קישורים

- www.law.co.il - באתר זה יש הסבר משפטי על חוק חתימה אלקטרונית.
- <http://www.geocities.com/NapaValley/1345/digsig.htm> - מושגי יסוד על חתימה דיגיטלית
- http://whatis.techtarget.com/definition/0,289893,sid9_gci211953,00.html - מושגים נוספים בנושא חתימה דיגיטלית
- <http://www.youdzone.com/signature.html> - הצגה ציורית של שיטת ההצפנה והחתימה הדיגיטלית
- <http://www.knesset.gov.il/knesset/hebframe.htm> - חוק חתימה אלקטרונית
- http://www.itpolicy.gov.il/vadat_inter_gov/articles/safe1.htm - מאמר בנושא העברה בטוחה ברשת האינטרנט. במאמר זה הסברים על סוגי הצפנות, שיטות הצפנה וחתימה על מסמכים.
- <http://www.ilpf.org/digsig/digrep.htm> - מאמר המתאר את תהליכי החקיקה ובחינת מודלים שונים בתחום החתימה הדיגיטלית במדינות שונות בארה"ב