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

מדינת ישראל
State of Israel

משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע
מחלקת רישום ופיקוח

תאריך : ל' ניסן תשס"ח
05 מאי 2008
סימוכין : 2008-0015-001019-02

לכבוד
פרופ' דניאל פרידמן
שר המשפטים

ח"כ בנימין אלון
יו"ר ועדת המדע והטכנולוגיה של הכנסת

מכובדי,

הנדון : **דוח רשם גורמים מאשרים לשנת 2007 לשר המשפטים ולועדת המדע והטכנולוגיה של הכנסת**

1. החל"מ מונה ביום 10.01.07 כרשם גורמים מאשרים לפי חוק חתימה אלקטרונית, התשס"א-2001 (להלן – החוק). בהתאם להחלטת הממשלה 4660 (חכ/195) מיום 19.01.06 בדבר הקמת רשות משפטית לטכנולוגיות מידע והגנה על הפרטיות, שולב רשם הגורמים המאשרים במסגרת הרשות.

2. בהתאם לתקנה 16 לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001 (להלן – **תקנות חומרה ותוכנה**), מוגש בזה דין וחשבון בדבר הפעלת סמכויות רשם גורמים מאשרים לשנת 2007 לפי תקנות חומרה ותוכנה.

3. אני לרשותכם לכל הבהרה.

בכבוד רב,
עמית אשכנזי, עו"ד
רשם גורמים מאשרים

העתק:
מנכ"ל משרד המשפטים, עו"ד משה שילה
עו"ד יורם הכהן, ראש הרשות למשפט טכנולוגיה ומידע

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

1. כללי

חוק חתימה אלקטרונית התשס"א - 2001 (להלן – **החוק**) והתקנות שהותקנו מכוחו, נועדו להגביר את הוודאות לגבי פעולות המתבצעות באופן אלקטרוני ע"י הסדרת תוקפה המשפטי ומעמדה הראיתי של החתימה האלקטרונית בישראל. בין ההסדרים שנקבעו בחוק ובתקנותיו:

קביעת דרישות סף לאמצעי טכנולוגי הראוי להיחשב כ- "חתימה" אלקטרונית באופן המקנה למסמך האלקטרוני קבילות, וכן משמש ראיה לכאורה לזהות החותם ולכך שהמסמך האלקטרוני לא שונה מעת חתימתו;

חלוקת אחריות בין הגורמים המעורבים בתהליך החתימה האלקטרונית: החותם ("בעל אמצעי החתימה" בלשון החוק) והגורם המאשר;

הסמכת גורם מפקח, רשם גורמים מאשרים, לנהל מרשם גורמים מאשרים (המהווים צד ג' אמין לאימות תעודות אלקטרוניות המשמשות בתהליך חתימה אלקטרונית מאושרת);

במישור הטכנולוגי, החוק מבוסס במידה רבה על תובנות מקובלות בעולם בתחום "תשתית המפתח הציבורי" (Public Key Infrastructure), ועל חקיקה מקבילה באיחוד האירופי – דירקטיבה[1] בדבר חתימה אלקטרונית משנת 1999.

על פי החוק מונה רשם גורמים מאשרים במשרד המשפטים (להלן – **הרשם**). תפקיד הרשם לרשום את הגורמים המאשרים במרשם הגורמים המאשרים, וזאת לאחר תהליך בדיקה קפדני בדבר עמידתם בתנאים המקדמיים הקבועים בחוק. לאחר רישום גורם מאשר, מפקח הרשם על פעילותם של הגורמים המאשרים, על מנת להבטיח כי הם עומדים בדרישות החוק ותקנותיו.

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 Septmber 1999, on a Community framework for electronic signatures.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

הרשם מפעיל סמכויות בהתאם לחוק וכן בהתבסס על שני קובצי תקנות מקיפים בנושא זה, שהנם 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**).

הרשם הח"מ מונה לתפקידו ב- 10.01.07.

דו"ח זה מוגש לשר ולועדה לענייני מחקר ופיתוח מדעי וטכנולוגי של הכנסת בהתאם לתקנה 16 לתקנות מערכות חומרה ותוכנה, הקובעת כי הרשם יגיש דין וחשבון בדבר הפעלת סמכויותיו לפי תקנות חומרה ותוכנה, לרבות בדבר הטכנולוגיות שאושרו והליכי אישורן.

2. <u>הפעלת חוק חתימה אלקטרונית - רקע</u>

החוק התקבל בכנסת במהלך שנת 2001, ובמהלך שנה זו הותקנו התקנות המסדירות גם את הדרישות המפורטות מגורמים מאשרים. הרשם מונה במהלך שנת 2002, ובתחילת שנת 2003 נרשמו שתי חברות כגורמים מאשרים לפי החוק: חב' סקיורנט וחב' קומסיין.

צעד משמעותי ביישומו המעשי של החוק החל עם הפעלתה בשנת 2003 של מערכת מגנ"א ("מערכת גילוי נאות אלקטרוני") ע"י הרשות לניירות ערך. מערכת זו מיועדת לאפשר לחברות ציבוריות להגיש דיווחים שונים הנדרשים מהן עפ"י חוק ניירות ערך, התשכ"ח - 1968 בפורמט אלקטרוני כשהם חתומים בחתימה אלקטרונית מאושרת.

מערכות נוספות הנסמכות על חתימה אלקטרונית מאושרת, כהגדרתה בחוק, הינן מערכת המצהרים ברשות המסים, מערכת המדווחים לאגף שוק ההון באוצר ומערכת מכרזים מקוונים במשרד הבטחון.

במקביל, נעשה על ידי גופים שונים שימוש גם בחתימה אלקטרונית מאובטחת. כדוגמא, נעשה שימוש בחתימה אלקטרונית מאובטחת בחשבוניות אלקטרוניות, נושא המוסדר בהוראות מס

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

הכנסה (ניהול פנקסי חשבונות), תשל"ג-1973 ובתקנות מס ערך מוסף (ניהול פנקסי חשבונות), תשל"ו-1976. תחום זה אינו בפיקוח ישיר של הרשם, ולכן אין בידינו מידע מדויק על היקף השימוש בחתימה אלקטרונית מאובטחת. לאחרונה החל משרד המשפטים במתן שירות במסגרתו ניתן לקבל באמצעות האינטרנט מידע בפורמט אלקטרוני אודות משכונות רשומים, כשהוא חתום בחתימה אלקטרונית מאובטחת של רשם המשכונות. השימוש בחתימה אלקטרונית מקנה מהימנות טכנולוגית ותוקף משפטי למידע המתקבל, מכוח חוק חתימה אלקטרונית.

במקביל ליישום החוק והתקנות, לרשם תפקיד פעיל בבחינת הצורך בתיקונים ועדכונים שונים לחוק ותקנותיו, לנוכח ההתפתחויות הטכנולוגיות מאז חקיקת החוק והניסיון שנצבר ביישום והטמעה של מערכות חתימה אלקטרונית.

בשנים 2003-2004 פעלה במשרד המשפטים, ליד הרשם, ועדה מייעצת בתחום החתימה האלקטרונית, בראשות פרופסור דני דולב מבית הספר למדעי המחשב באוניברסיטה העברית, ובהשתתפות מומחים בתחום ההצפנה, אבטחת המידע והטכנולוגיה. דיוני הועדה שימשו להתווית המדיניות בתחומים אלה.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

3. פעולות הרשם על פי התקנות

א. מבוא

בראש צוות הפיקוח ביחידת הרשם עומד הח"מ, שהוא משפטן בעל רקע ונסיון בתחום החתימה האלקטרונית. הרשם הוא המוסמך לרשום גורמים מאשרים ולפקח עליהם. לצורך כך מפעיל הרשם את סמכויותיו יחד עם צוות פיקוח. צוות הפיקוח מבוסס על יועצי אבטחת מידע של משרד המשפטים ויועצי אבטחה פיזית ממשרד קצין הבטחון של משרד המשפטים. היועצים הוסמכו לתפקיד זה, והתחייבו בהתחייבויות מתאימות להעדר ניגוד עניינים וסודיות בהתאם לרגישות התפקיד. בשנת 2007, במסגרת שילוב תפקיד הרשם ברשות החדשה למשפט טכנולוגיה ומידע (להלן – הרשות), צורפו עובדים נוספים מהרשות לפעולות הפיקוח. האמור תרם תרומה משמעותית לפעולות הפיקוח.

סמכות נוספת של הרשם הנה לאשר טכנולוגיות להפקת חתימה אלקטרונית מאובטחת כהגדרתה בחוק. לרשם הוגשו שתי בקשות שנמצאות בשלבי טיפול שונים הנובעים מהפרטים שנמסרו לרשם כרקע לבקשה. גם בנושאים אלה הרשם נעזר בגורמי מקצוע בתחום טכנולוגיות המידע, לצורך בחינת הבקשות ואישורן.

על פי התוכנית הארגונית של הרשות למשפט טכנולוגיה ומידע, עיקר תפקידי הרשם אמורים להשתלב במסגרות סמכויות מחלקת הרישום והפיקוח של הרשות, ובכך לנצל את בצורה יעילה יותר את כוח האדם הפיקוחי ואת הנסיון בנושא זה.

ב. הקף הפיקוח בתקופת הנסקרת - כללי

עד תחילת שנה זו היו רשומים במרשם הגורמים המאשרים שתי חברות - חב' קומסיין וחב' סקיורנט.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

במסגרת הפעלת סמכות הפיקוח הוגדרה בעבר תכנית בדיקות לגורם מאשר, פורסמו הנחיות מקצועיות לגורמים המאשרים בתחומים שונים ונבדקו נהלי התפעול והאבטחה של הגורמים המאשרים.

אחת לשנה נבדקים מסמכי הדו"ח השנתי של הגורמים המאשרים הכוללים:

חוות דעת של מבקר בדבר התאמת המערכות שברשותם לדרישות החוק.

תעודות התאמה ודו"חות בדיקה לתקן אבטחת מידע 7799 ולתקן ISO 9000.

מסמכי ערבות וביטוח להוכחת עמידת הגורמים המאשרים בדרישות הפיננסיות.

כחלק מתהליך הקמת הרשות ואיחוד מסגרות פיקוח שונות לכדי פעולה אחידה, שונתה גם מדיניות הפיקוח וזו שילבה גם ביקורות פתע אצל הגופים המפוקחים. פירוט רב יותר על פעילות הפיקוח על פי התקנות מצוי בנספח לדוח זה.

ג. חברת סקיורנט

באמצע שנת 2007 הודיעה חברת סקיורנט לרשם על סיום פעילותה לפי החוק. הודעה מקדימה על צמצום הפעילות התקבלה במסגרת הודעה של חברת סקיורנט לרשות ניירות ערך על כוונתה להפסיק לפעול כ"מאשר חתימה" על פי חוק ניירות ערך, התשכ"ח-1968 בחודש פברואר 2007.

בהתאם לכך ננקטו צעדים לצורך הבטחת סיום פעילות תקין של חברת סקיורנט. בהקשר זה בוצעה ביקורת פתע בתקופת הביניים לבדיקת תקינות הפעילות לאור הסגירה הצפויה, וכן ניתנו הנחיות באשר לאופן סיום הפעילות, בהתאם לתקנה 18 לתקנות רישום גורם מאשר, ולצורך מימוש תכליתן.

נכון למועד הגשת דו"ח זה, בוצעו כל הפעולות הנדרשות לפי תקנה 18 הנ"ל, ובהן הפקדת אמצעי החתימה של הגורם המאשר בידי הרשם, הפקדת עותק של כל התעודות שהונפקו לפי החוק, המסמכים ששימשו להנפקתם, ורשימת התעודות הבטלות האחרונה, המכילה את כל התעודות שהונפקו לפי החוק. פורסמו על כך פרטים גם באתר האינטרנט של הרשם.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

ד. <u>חברת קומסיין</u>

במהלך שנת 2007 בוצעו מספר ביקורות, שתיים מהן ביקורת פתע, בהתאם למדיניות הפיקוח האמורה של הרשות.

במסגרת הביקורות, אשר האחרונה שבהם בשנת 2007 בוצעה בסוף דצמבר 2007 נמצאו ליקויים בדרכי פעולת הגורם המאשר, וננקטים מהלכים לתיקון ליקויים אלה. בנושא זה מתנהל מעקב שוטף. בביקורת שבוצעה בפברואר 2008 נמצא שינוי גישה למול שנת 2007, ושיפור בנושאים שונים שהתגלו בביקורות.

במסגרת הפעילות השוטפת, אושר לקומסיין להתקשר עם ההוצאה לאור של לשכת עורכי הדין, כדי שתשמש כגורם רושם, וזאת בהתאם לסמכות הרשם על פי תקנה 10(1) לתקנות חומרה ותוכנה. בהתאם לכך, מבצעת לשכת עורכי הדין את תפקיד אימות הזהות שהינו השלב הראשון שנעשה בהנפקת תעודה אלקטרונית, וזאת בשמה של חברת קומסיין.

האישור ניתן לאחר בחינת ההסדרה החוזית והנהלית של הנפקת תעודות אלקטרוניות, בין קומסיין לבין ההוצאה לאור של לשכת עורכי הדין. האישור הראשון ניתן בתנאים שנקבעו בו, החל מיום 20.08.07, לתקופה של חצי שנה, כלומר עד ליום 20.02.08. הפעילות לפי הסדר זה החלה רק לאחרונה, ובהתאם לכך הוארך האישור עד לספטמבר 2008.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

4. פעולות נוספות

כפי שצויין לעיל, החוק הישראלי מבוסס במידה רבה על תובנות מקובלות בעולם. בהקשר זה, בוצעה עבודת תקינה והסדרה משמעותית באיחוד האירופי על פי הדין האירופי, במסגרת קבוצות עבודה בארגון התקינה ETSI[2].

בהקשר זה, בשל הדמיון בין הדין האירופי לדין הישראלי, והאינטרס בתנועה חופשית של תקשורת, יזם משרד המשפטים קידום שיתוף הפעולה בתחום זה מול האיחוד האירופי, במסגרת הסכם האסוציאציה עם מדינות האיחוד, ובמסגרת תוכנית שת"פ נוספות ובמרכזן תהליך "יורומד" (הידוע גם כתהליך ברצלונה).

המניעים המרכזיים לקידום שיתוף הפעולה הם לצורך למידה מהנסיון האירופאי וכן לצורך שיתוף פעולה בהכרה הדדית במסמכים לצורך סחר בינלאומי ובהן גם הגשת הצעות למכרזים באיחוד האירופי באופן מקוון.

במסגרת זו הוצג הנושא בשיחות הסחר השנתיות עם נציגות האיחוד בשנת 2005, ואף התקיים מפגש מומחים בדרג מקצועי בדצמבר 2005. העמדה שנמסרה מטעם האיחוד האירופי (נכון לסוף 2005) כי הנושא אינו בשל לשיתוף פעולה פורמלי-דיפלומטי, שכן טרם התגבש ברמה אחידה בתוך האיחוד. נכון לסוף 2005, וגם נכון למועד הגשת דוח זה, מדינות אירופה עצמן טרם גיבשו שיטת הכרה הדדית אחידה, בינן לבין עצמן.

עם זאת, המליצו נציגי האיחוד על קבלתה של ישראל כמשקיפה בארגון הוולנטרי של הרשויות המפקחות על החתימה האלקטרונית באירופה (FESA - Forum of European Supervisory Authorities). מדובר באותן רשויות פיקוח שהוקמו על פי הדירקטיבה האירופית במדינות אירופה.

---

[2] ראה: http://portal.etsi.org/esi/el-sign.asp.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

לישראל אינטרס גבוה להשתתף בדיונים הפנים אירופאיים, מאחר ושהיא תאפשר הערכות ליישור קו ישראלי מול אירופה ועשויה לשמש לפיתוח המדיניות הפנימית בנושא זה. להתאמה זו מול התפיסה האירופית חשיבות רבה גם בתהליך הצטרפות ישראל ל-OECD.

בעקבות בקשת ישראל במפגש שהתקיים ב- 21 ביוני 2006, הוחלט כי ישונה תקנון הארגון כך שגם ישראל תוכל להיות חברה בו, במעמד משקיף. הארגון מקיים מפגשים שלוש פעמים בשנה במדינות החברות. המפגש האחרון, בו השתתף גם הח"מ, נערך בהאג, הולנד באוקטובר 2007.

ב– 12-13 לפברואר 2008 אירחה הרשות למשפט, טכנולוגיה ומידע את המפגש התקופתי של FESA בתל אביב. במפגש השתתפו נציגים מ- 11 מדינות, ובהן אוסטריה, איטליה, בלגיה, הולנד, נורבגיה, טורקיה, הונגריה וצ'כוסלובקיה.

מהדיונים בפורום זה עולה כי במדינות רבות באירופה היישום של החתימה האלקטרונית, בפורמט הדומה לחוק הישראלי טרם זכה לתפוצה משמעותית. השימוש בפועל בחתימה אלקטרונית הוא בפרוייקטים ממשלתיים.

הניסיון המצטבר מאירופה מלמד כי יש חשיבות רבה לתיעוד לאומי כפלטפורמה להפצה נוחה של חתימה אלקטרונית. פלטפורמה אחרת מקובלת הינה בהקשר של כרטיסים בתחום הבריאות והביטוח הלאומי.

בבלגיה, איטליה, ספרד ואיטליה, הונפקו מיליוני תעודות אלקטרוניות במסגרות אלה. בשוודיה יש תשתית ענפה של הסתמכות על חתימה אלקטרונית, אולם מדובר בחתימה שאינה על פי הפרמטרים שנקבעו בדירקטיבה האירופית, ולכן אינם עומדים בה.

ניתן לומר כי יעד מרכזי במדיניות האיחוד בתחום זה (בשונה מהמדיניות בכל אחת מהמדינות) הינה לקדם את האחידות בתחום שירותי "ממשל מקוון" וחתימה אלקטרונית. לצורך כך מממן האיחוד האירופי מחקרים בנושא השימוש בחתימה האלקטרונית במדינות השונות, וכן מיפוי

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

הפערים בין המדינות השונות, לצורך התמודדות עם סוגיה זו על מנת לקדם שימוש בחתימה אלקטרונית "כלל אירופאית"[3].

5. נושאים נוספים

במסגרת הטיפול השוטף בחוק ובתקנות נערכת בדיקה של הצורך להמליץ למחלקת ייעוץ וחקיקה במשרד המשפטים על תיקונים ושינוים בחוק ובתקנות. הנושאים המרכזיים הנבדקים:

א. הפעלת סמכות הרשם "לחתום" בחתימה משלו על תעודה אלקטרונית של גורם מאשר. נושא זה מקובל בחלק ממדינות אירופה ובמסגרת מערך האמון המשמש עובדי מדינה בארה"ב, והינו בין ההמלצות שנדונו בועדה המייעצת לרשם. המטרה היא לייצר זיהוי טכנולוגי של הגורם המאשר, ולקבוע נהלים מחייבים באמצעות התשתית הטכנולוגית המקובלת.

ב. דרישות אבטחת מידע מהתקנים המשמשים לחתימה אלקטרונית. מוצרים המשמשים במסגרת מערך לחתימה אלקטרונית הינם מוצרים שנדרשת לגביהם בדיקה של אבטחת המידע, על פי התקן הבינלאומי Common Criteria for Information Technology, או התקן המשמש בממשל הפדרלי מסדרת FIPS. בנושאים אלה חלו שינויים מאז אישור התקנות, ויש צורך בבחינה של הנושא. עוד יצויין כי בישראל אין מעבדות תקינה המוסמכות לאשר עמידה בתקנים אלה, ולכן על בחינת המוצרים והמערכות להתבצע בחו"ל. מיעוט מעבדות התקינה ויסודיות תהליך הבדיקה עלולים לעכב הגעה של טכנולוגיות לשוק, כאשר קיים תנאי סף של בדיקת איכות מוקדמת.

ג. התפתחויות במחקר ההצפנה. חתימה אלקטרונית מבוססת על שימוש בישומים המבוססים על טכנולוגיות הצפנה מקובלות. ההתפתחויות בתחום מחקר ההצפנה ופריצת הצפנות, הביא לדיון בדבר צורך בשידרוג טכנולוגי[4].

---

[3] ראה לאחרונה: http://ec.europa.eu/idabc/en/document/6485

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

ד. איפיון תעודות אלקטרונית "לתאגיד": בדיונים מול הגורם המאשר ומול גורמים שונים עלה הצורך להגדיר בצורה מדויקת את טיבה של תעודה אלקטרונית למורשה חתימה בתאגיד, ואת ההבדלים בינה תעודה ליחיד. הקושי המרכזי הינו שהגדרת ההרשאה של מורשה חתימה נגזרת בדרך כלל מהחלטות האורגן המוסמך בתאגיד, שעשויות להשתנות מעת לעת ולהיות מורכבות ביותר. יש קושי לכלול מידע זה במלואו על גבי התעודה האלקטרונית למורשה החתימה. בשלב זה נמצא פתרון נקודתי מול הגורם המאשר.

6. סיכום

הרשם ממשיך בפעילות הפיקוח השוטפת במסגרת פעילות הרשות, ועוקב אחר ההתפתחויות באירופה בנושא זה על מנת לבחון את הצרכים בעדכון התקנות והתקנים המוזכרים בהן.

---

[4] ראה: ETSI, TS 102-176 Ver 2.0.0, Electronic Signatures and Infrastructures; Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, ("Algo" paper) באתר ETSI, לעיל.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

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

מדינת ישראל
State of Israel

משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע
מחלקת רישום ופיקוח

נספח - אופן הפעלת סמכויות הפיקוח

כנדרש בתקנה 16 לתקנות חומרה ותוכנה, מפורטות להלן אופן הפעלת סמכויות הפיקוח לפי התקנות השונות בתקופה הנסקרת.

תקנה 2. תקן

נוסח התקנה:

"גורם מאשר יקבל מאת מכון התקנים או מאת מי שאושר לעניין זה לפי סעיף 12 לחוק התקנים קודם לתחילת פעילותו לפי החוק תעודת בדיקה בדבר התאמה לת"י 7799, חלקים 1 ו-2, ויעמוד בתקן במשך כל זמן פעילותו."

הגורמים המאשרים עמדו בדרישה הנ"ל במשך כל התקופה הנסקרת. לידי הרשם נמסרו עותקים של ביקורות שבוצעו בידי בודקי מכון התקנים, והם משמשים אינדיקציה נוספת ובלתי תלויה לנושאים שיש לבדוק או לעקוב אחריהם, כמו גם לנושאים שהטיפול בהם משביע רצון.

בהתאם למידע שהתקבל ממכון התקנים, תוקף ההסמכה לתקן ישראלי 7799 יסתיים ביוני 2008, והחל ממנו תתחייב עמידה בתקן ישראלי 27001. הודעה מתאימה פורסמה על ידי הרשם ונמסרה לחברת קומסיין. מחברת קומסיין נמסר כי היא נערכת לכך.

א. תקנה 3. זמינות

נוסח התקנה:

"גורם מאשר ידאג להבטיח כי במערכות הדרושות לבדיקת מאגרי תעודות בטלות ועדכונן תתקיים בכל עת רמת זמינות גבוהה להנחת דעתו של הרשם."

באופן כללי, הגורמים המאשרים עמדו בדרישה הנ"ל במשך כל התקופה הנסקרת. בינואר 2007 הגיעה אל הרשם תלונה בנושא זה. בתום בדיקתה, שוכנענו מהסבריו של קומסיין כי מדובר בתקלת תוכנה, וכי קיימים בנושא זה נהלים המבטיחים עמידה בחובה זו.

ב. תקנה 4. אמצעי החתימה של הגורם המאשר

נוסח התקנה:

"גורם מאשר ישתמש באמצעי חתימה שמתקיימים בו לפחות כל אלה:

(1) הוא מבוסס על מפתח RSA או DSA באורך 2048 סיביות לפחות או ECDSA באורך 160 סיביות לפחות.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

(2) הוא מוגן באמצעי שמתקיימות בו לפחות דרישות האבטחה של 140-2 FIPS רמה 2.

(3) הוא מגובה באמצעים מוגנים ומאובטחים להנחת דעתו של הרשם. הגיבוי יישמר בנפרד.

(4) דרישות נוספות שהעמיד הרשם לשם קיום אבטחה ברמה סבירה מפני חדירה, שיבוש או שימוש לרעה."

בבדיקה שגרתית התברר לרשם כי אחד השרתים המשמשים להנפקת תעודות אלקטרוניות על ידי קומסיין, עושה שימוש באורך מפתח שהינו באורך 1024 ביט, לשרת המנפיק תעודות אלקטרוניות. זאת בשל עמדה ולפיה אמצעי החתימה של הגורם המאשר אינו בהכרח אמצעי החתימה המשמש לחתימה על תעודות אלקטרוניות לפי החוק, אלא אמצעי חתימה המזהה את התעודות האלקטרוניות המונפקות לפי החוק.

על מנת למנוע ספק, הרשם הנחה להפסיק להשתמש באופן מיידי בשרת זה כשרת הנפקה, בהנחייה מנומקת. נכון למועד הגשת דו"ח זה, למיטב ידיעת הרשם, הגורם המאשר פועל על פי הנחייה זו. הרשם נמצא בדיון מול הגורם המאשר לגבי תעודות שהונפקו משרת זה טרם מתן ההנחיה.

תקנה 5. אבטחת מרכיבי המערכת ואמצעי התקשורת

נוסח התקנה:

"(א) מרכיבי המערכת המשמשים לזיהוי המבקש, להנפקת תעודה אלקטרונית ולביטולה (להלן – פעולות חיוניות) יעמדו ברמת ביטחון של תקן common criteria EAL4 או לפי תקן מקובל אחר המבטיח רמת אבטחה מקבילה להנחת דעתו של הרשם.

(ב) אמצעי התקשורת המשמשים לפעולות חיוניות של הגורם המאשר יעמדו בדרישות אבטחה גבוהות להנחת דעתו של הרשם."

על פי בדיקת הרשם הגורמים המאשרים עמדו בדרישה הנ"ל במשך כל התקופה הנסקרת.

ג. תקנה 6. אבטחה פיזית

נוסח התקנה:

"גורם מאשר יבטיח כי חלקי המערכת החיוניים לפעילותו כגורם מאשר (להלן – "החלקים החיוניים") יישמרו במקום מוגן המונע

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

חדירה וכניסה בלא הרשאה והתואם את אופי פעילותו של גורם מאשר להנחת דעתו של הרשם."

מדוח מבקר מערכות המידע מטעם אחד הגורמים המאשרים, שהוגש באוקטובר 2007, עולה כי בשנת 2006 לא פעלו חלק ממערכות האבטחה של קומסיין, ולא נמסר על כך לרשם כל דיווח. עוד התברר מדוח מבקר מערכות המידע ומפעולות ביקורת של הרשם, כי החל מאמצע שנת 2006, לא עמדה החברה במגבלות הנדרשות על הרשאות גישה של עובד בודד למערכות רגישות בחברה, וזאת בשל סיום עבודתו של מנהל האבטחה בחברה. עקב כך תפקיד מנהל האבטחה ומנהל הטכנולוגיות בחברה בוצע על ידי אותו אדם.

נכון למועד הגשת דוח זה, ועל פי דיווח של מבקר אבטחת המידע ביחס לפעילות החברה, הוחלף מנהל האבטחה, ותוקן נושא זה.

ד. תקנה 7. בקרת גישה והפרדת תפקידים

נוסח התקנה:

(א) גורם מאשר יבטיח כי ביצוע הפעולות החיוניות לא יהא בשליטתו של אדם אחד בלבד

(ב) גורם מאשר יבטיח את מידור הגישה לחלקים החיוניים כך שלאותו אדם לא תהא גישה לכל החלקים החיוניים."

ככלל, הגורמים המאשרים עמדו בדרישה הנ"ל במשך כל התקופה הנסקרת, בכפוף להערה המפורטת לעיל בדבר מנהל האבטחה ומנהל הטכנולוגיות.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

ה. תקנה 8(1)(ג). חזקה לענין חתימה אלקטרונית מאובטחת

נוסח התקנה:

"חתימה אלקטרונית שמתקיים בה אחד מאלה, חזקה שהיא חתימה אלקטרונית מאובטחת:

(1) לגבי אמצעי לאימות החתימה שמחזיק בידיו המבקש, ואמצעי אימות החתימה שאותו הוא מזהה, מתקיימות לפחות הדרישות כמפורט להלן:

(ג) היתה הפעלת אמצעי החתימה כרוכה בשימוש בסיסמה, תעמוד הסיסמה בדרישות אבטחה ברמה הגבוהה לפי ת"י 1495 חלק 3 , או בדרישות חלופיות שקבע הרשם, אם נוכח כי ניתן לפטור מהדרישה האמורה."

עד היום לא התבקש הרשם להפעיל את סמכותו לקביעת דרישות חלופיות לסיסמא לפי התקנה הנ"ל.

עם זאת, במסגרת תיקון נהלים של הגורם המאשר, וכן אישור פעולת ההוצאה לאור של לשכת עורכי הדין, ובהתאם למקובלות בתחום זה, הנחה הרשם כי אורך סיסמת הגישה יהיה **לפחות 6 תווים.**

ו. תקנה 9. אישור לעניין חתימה אלקטרונית מאובטחת.

"(א) מי שמעוניין בכך רשאי לפנות בכתב לרשם לשם קביעה –

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

(ב) אישר הרשם לפי תקנת משנה (א) כי חזקה שחתימה אלקטרונית מסוימת היא חתימה אלקטרונית מאובטחת, יפרסם ברשומות

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

את דבר אישורה של הטכנולוגיה שלגביה אישר כאמור, נוסף על כך ינהל הרשם רשימה מעודכנת של טכנולוגיות שקיבלו את אישורו באתר האינטרנט המשמש לכך."

בשנת 2007 הוגשו לרשם שתי בקשות בנושא זה. ככלל, מוצרים המשמשים לביצוע פעולות הצפנה, והמחזיקות מידע רגיש, כגון חתימה אלקטרונית, נדרשים לעבור הסמכה במכון תקינה לפי תקני אבטחת מידע מקובלים, ובראשם ISO 15408, וכן תקן של ארגון NIST האמריקאי, מסדרת FIPS. הבדיקות לפי תקנים אלה מחייבות תשתיות בדיקה ממוסדות, ידע והכשרה, שאינן מצויות במלואן בשוק האזרחי במדינת ישראל. בהתאם לכך, עמדת הרשם היא כי ככלל יש להסתמך על אישורים שניתנים ממוסד מוכר בחו"ל בהתאם לתקנים אלה.

בנושא זה נערכת בדיקה נוספת בידי הרשם לעניין אופן מימוש הסמכות הנתונה בתקנה זו על רקע האמור.

ז. *תקנה 10(2). זיהוי המבקש*

נוסח התקנה:

"10. לא ינפיק גורם מאשר תעודה אלקטרונית אלא לאחר שאימת את זהות המבקש כמפורט להלן:

(1) הגורם המאשר, או נציגו או שליח מטעמו שאישר הרשם ובתנאים שקבע באישור, זיהה פנים אל פנים את המבקש, ואם היה המבקש תאגיד — את מורשה החתימה מטעם התאגיד;

(2) הגורם המאשר יאמת את פרטי הזיהוי של המבקש:

(א) ביחיד שהוא תושב ישראל — על פי תעודת זהות, וכן על פי דרכון ישראלי תקף או רישיון נהיגה ישראלי תקף עם תמונה או על פי מידע שהתקבל ממרשם האוכלוסין במשרד הפנים (להלן — מרשם האוכלוסין); הרשם רשאי להורות, בהתחשב בעלות קבלת המידע ובתועלת העשויה לצמוח ממנו, כי האימות בהתאם לפסקת משנה זו, לגבי כלל התעודות האלקטרוניות או לגבי תעודות אלקטרוניות מסוימות, יתבצע על פי מידע שהתקבל ממרשם האוכלוסין; בפסקת משנה זו, "מידע שהתקבל ממרשם האוכלוסין" — הפרטים שדרש הרשם, כולם או חלקם, מבין אלה: מספר הזהות של המבקש, שם משפחתו ושם משפחה קודם, אם ישנו, שם פרטי, שם האב, שם האם, שנת לידה, תאריך הנפקת תעודה אחרון, סיבת הנפקת התעודה, מען נוכחי, אם ישנם — סטטוס פטירה ותאריך פטירה;

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

(ב) ביחיד שהוא תושב חוץ — על פי דרכון חוץ או תעודת מסע או תעודת זהות, וכן על פי מסמך זיהוי נוסף הנושא תמונה של המבקש ופרטים מזהים שלו ושל מי שהנפיק את המסמך הנוסף ;

(ג) בתאגיד הרשום בישראל — על פי תעודת הרישום, אישור של עורך דין על קיומו של התאגיד,שמו ומספרו הרשום, או במקום אישור של עורך דין כאמור — על פי אימות במרשמים המתאימים, וכן על פי העתק מאושר של החלטת האורגן המוסמך בתאגיד בדבר מורשה החתימה מטעם התאגיד, או אישור של עורך דין על מורשה החתימה כאמור ;

(ד) בתאגיד שאינו רשום בישראל — על פי העתק מאושר ממסמך המעיד על רישומו, אישור של עורך דין על קיומו של התאגיד, שמו ומספרו הרשום, או במקום אישור של עורך דין כאמור — על פי אימות במרשמים המתאימים, וכן על פי העתק מאושר של החלטת האורגן המוסמך בתאגיד בדבר מורשה החתימה מטעם התאגיד או אישור של עורך דין על מורשה החתימה כאמור ;

(ה) במוסד ציבורי — על פי הצהרת המבקש, לאחר שהגורם המאשר נוכח, על פי מסמך, כי מורשה החתימה מוסמך לפעול בשם המוסד הציבורי ; לענין פסקה זו, "מוסד ציבורי" — משרדי ממשלה, רשויות מקומיות, וכן רשויות, תאגידים או מוסדות אחרים שהוקמו בישראל לפי חיקוק ;

(3) לענין פסקאות משנה (ג) עד (ה) שבפסקה (2) — יזהה הגורם המאשר את מורשה החתימה לפי הוראות פסקאות משנה (א) או (ב) שבאותה פסקה, לפי הענין ;

(4) לענין פסקאות משנה (ד) ו-(ה) שבפסקה (2), "העתק מאושר" — העתק מתאים למקור המאומת בידי אחד מאלה :

(א) הרשות שהנפיקה את מסמך המקור ;

(ב) עורך דין בעל רישיון לעריכת דין בישראל ;

(ג) נציג דיפלומטי או קונסולרי ישראלי בחוץ לארץ."

בהחלטתו מיום 1.1.03 הורה הרשם לגורמים המאשרים לזהות יחידים שהנם תושבי ישראל על סמך מידע שהתקבל ממרשם האוכלוסין.

בביקורות שבוצעו בקומסיין נמצאו ליקויים בתהליך אימות זהות כנדרש בתקנה, ובתהליך בדיקת מורשה חתימה. בעקבות הביקורות נמצא שיפור בנושא זה, ונראה כי הופקו הלקחים מהביקורת.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064

בתיאום עם הגורם המאשר נמצאת בגיבוש הנחייה חלופית לזיהוי ביחס ליחידים שאין להם מסמכי זיהוי כנדרש בתקנה.

ח. תקנה 12. זיהוי לצורך הנפקת תעודה אלקטרונית חדשה

"בהנפקת תעודה אלקטרונית חדשה, על סמך תעודה אלקטרונית שטרם פג תוקפה, יכול גורם מאשר לנקוט הליכי זיהוי שונים מאלה האמורים בתקנה 10, ובלבד שהרשם אישר הליכים כאמור."

במסגרת סמכותו הנ"ל אישר הרשם לגורמים המאשרים לנקוט בהליך זיהוי שונה מזה האמור בתקנה 10 בעת חידוש תעודה אלקטרונית תקפה. במסגרת הליך הזיהוי המתוקן אושר שימוש באמצעי זיהוי חלופיים במקום זיהוי המבקש פנים אל פנים.

ט. תקנה 15. שינוי תקן

"(א) הוחלף תקן מן התקנים הנזכרים בתקנות אלה, לרבות מסמך RFC, בתקן או מסמך חדש, לפי העניין, יהיו התקן או המסמך החדש מחייבים במקביל לתקן או המסמך הישן, זולת אם אין עוד בתקן או במסמך הישן כדי להבטיח תנאי אבטחה נאותים להנחת דעתו של הרשם, שאז יחייב התקן או המסמך החדש בלבד, בתוך זמן שיורה הרשם".

(ב) הרשם יודיע לגורמים המאשרים על שינוי תקן או מסמך RFC מחייב כאמור בתקנת משנה (א) ויפרסם באתר האינטרנט שיועד לכך רשימה מעודכנת ש להתקנים והמסמכים המחייבים לפי תקנות אלה."

בהחלטתו מיום 18.2.04 קבע הרשם כי המסמך RFC 2527 שלפיו יש לערוך מסמך נהלים של גורם מאשר כאמור בתקנה 1 לתקנות יוחלף החל מיום 1.3.04 במסמך חדש המסומן RFC 3647 . בנוסף, כאמור נמסרה הודעה על פי תקנה זו כי עד ולא יאוחר מ– 30.06.08 על גורם מאשר להציג תעודה על התאמה לתקן ישראלי 27001, במקום ההתאמה לתקן ישראלי 7799.

כמו כן נבדקות התפתחויות בתחום ההצפנה ואבטחת המידע לצורך בחינת סוגיית עדכון ההנחיות בנושא זה בתקנות ועל פיהן.

2 Hashlosha St., P.O. Box 9288
Tel Aviv 61092
Tel.: +972-3-6899842
Direct: +972-3- 6899829
Fax: +972-2-6467064

Email: rashamca@justice.gov.il
Web: www.justice.gov.il/MOJHeb/RashamGormimMashrim

רח' השלושה 2, ת.ד. 9288
תל אביב 61092
טל': 03-6899842
ישיר: 03-6899829
פקס: 02-6467064