נוסח שאושר לפרסום

תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"א-2001

בתוקף סמכותי לפי סעיפים 19(א)(1) ו- 24(א)(9) עד (11) לחוק חתימה אלקטרונית, התשס"א-2001[1] (להלן – החוק), ובאישור הועדה לעניני מחקר ופיתוח מדעי וטכנולוגי של הכנסת, לפי סעיף 24(ב)(2), אני מתקין תקנות אלה:

פרק א': פרשנות

הגדרות 1. בתקנות אלה –

"מבקש" – כהגדרתו בסעיף 18(א) לחוק;

"מסמך נהלים" – הוראות נוהל שלפיהן פועל הגורם המאשר, הערוכות על פי מסמך RFC 2527 של הארגון הבין לאומי IETF (להלן – מסמך RFC), צוות המשימה להנדסת האינטרנט, ואשר הוגשו לאישור הרשם;

"מערכת" – מערכת החומרה והתוכנה של הגורם המאשר המשמשת לפעילותו כגורם מאשר;

"RSA", "DSA" ו- "Elliptic Curve DSA" — אלגוריתמים להפקת חתימה אלקטרונית מאובטחת, שהכיר בהם אחד הגופים המפורטים בתוספת;

"FIPS" – סדרת תקנים של המכון הלאומי לתקנים וטכנולוגיה של ארצות הברית של אמריקה, לאבטחת מידע במערכות מחשב;

"Common Criteria EAL" – מדרג של רמות אבטחת מידע, אשר אומץ ~~על~~ בידי ארגון התקינה הבין לאומי, בתקן IS0 15408;

"תושב" – כמשמעותו בחוק מרשם האוכלוסין, התשכ"ה-1965[2], לרבות אזרח ישראלי שאינו תושב כאמור, הרשום במרשם האוכלוסין;

"תושב חוץ" – מי שאינו תושב;

"ת"י" – תקן ישראלי כמשמעותו בחוק התקנים, התשי"ג-1953[3] (להלן – חוק התקנים);

"תקן מקובל" – תקן אבטחת מידע של אחד הגופים המפורטים בתוספת;

"תקן ISO/IEC 9594-8" – תקן של מכון התקנים הבין לאומי, אשר פורסם גם כתקן X509v.3 של הארגון הבינלאומי IETF, צוות המשימה להנדסת אינטרנט.

---

[1] ס"ח התשס"א, עמ' 210

[2] ס"ח התשכ"ה, עמ' 270

פרק ב': מערכות חומרה ותוכנה מהימנות

תקן 2. גורם מאשר יקבל, מאת מכון התקנים או מאת מי שאושר לענין 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.

זמינות 3. גורם מאשר ידאג להבטיח כי במערכות הדרושות לבדיקת מאגרי תעודות בטלות ועדכונן, תתקיים בכל עת רמת זמינות גבוהה, להנחת דעתו של הרשם.

אמצעי החתימה של הגורם המאשר 4. גורם מאשר ישתמש באמצעי חתימה שמתקיימים בו לפחות כל אלה:

(1) הוא מבוסס על מפתח RSA או DSA באורך 2048 סיביות לפחות או Elliptic curve DSA באורך 160 סיביות לפחות;

(2) הוא מוגן באמצעי שמתקיימות בו לפחות דרישות האבטחה של FIPS140-2 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.

אבטחת מרכיבי המערכת ואמצעי התקשורת 5. (א) מרכיבי המערכת המשמשים לזיהוי המבקש, להנפקת תעודה אלקטרונית ולביטולה (להלן – פעולות חיוניות) יעמדו ברמת בטחון של תקן common criteria EAL4 או לפי תקן מקובל אחר, המבטיח רמת אבטחה מקבילה, להנחת דעתו של הרשם.

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

אבטחה פיזית 6. גורם מאשר יבטיח כי חלקי המערכת החיוניים לפעילותו כגורם מאשר (להלן – החלקים החיוניים) יישמרו במקום מוגן, המונע חדירה וכניסה ללא הרשאה, והתואם את אופי פעילותו של גורם מאשר, להנחת דעתו של הרשם.

בקרת גישה והפרדת 7. (א) גורם מאשר יבטיח כי ביצוע הפעולות החיוניות לא יהא בשליטתו של אדם אחד בלבד.

---

[3] ס"ח התשי"ג, עמ' 30

תפקידים

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

(ג) גורם מאשר ינהיג אמצעי זיהוי שיבטיחו זיהוי ותיעוד גישתו של כל אדם למערכת.

(ד) הרשם רשאי לפטור גורם מאשר מהחובות לפי תקנות משנה (א) ו-(ב), מטעמים שיירשמו, ורשאי הוא לקבוע להן חובות חלופיות.

פרק ג': חתימה אלקטרונית מאובטחת

חזקה לענין חתימה אלקטרונית מאובטחת

8. חתימה אלקטרונית שמתקיים בה אחד מאלה, חזקה שהיא חתימה אלקטרונית מאובטחת:

(1) לגבי אמצעי לאימות חתימה שמחזיק בידיו המבקש, ואמצעי החתימה אותו 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 פיזיים או הצפנתיים (קריפטולוגיים) ייחודיים, העומדים ברמת אבטחה של תקן FIPS 140-2 רמה 1, ברמת בטחון של תקן common criteria EAL2 לפחות;

(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;

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

אישור לענין חתימה אלקטרונית מאובטחת

9. (א) מי שמעונין 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 את דבר אישורה של הטכנולוגיה שלגביה אישר כאמור; בנוסף, ינהל הרשם רשימה מעודכנת של טכנולוגיות שקיבלו את אישורו, באתר אינטרנט המשמש לכך.

פרק ד': בדיקת בקשות להנפקת תעודה אלקטרונית

זיהוי המבקש

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 רשיון 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 האלקטרונית 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;

(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 הוראת 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 רשיון לעריכת דין בישראל;

(ג) נציג דיפלומטי או קונסולרי ישראלי בחוץ לארץ.

שמירת מסמכי הזהוי

11. גורם מאשר יקבל לידיו וישמור ברשותו או ברשות נציגו או שליחו כאמור בתקנה 10(1), העתק של כל אחד ממסמכי הזיהוי שהוגשו לפי תקנה 10, למשך 15 שנים לפחות מיום שפג תוקפה של התעודה האלקטרונית שהנפיק, ואולם אם חודשה התעודה לפי תקנה 12, ישמור את המסמכים למשך 15 שנים מיום שפג תוקפה של התעודה האחרונה שהנפיק לאותו מבקש.

זיהוי לצורך הנפקת תעודה אלקטרונית חדשה

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

הנפקת תעודה אלקטרונית

13. (א) גורם מאשר ינפיק תעודה אלקטרונית למבקש רק לאחר שבדק כי המבקש מחזיק בידיו אמצעי חתימה להפקת חתימה אלקטרונית מאובטחת, וכי באמצעי החתימה ובאמצעי לאימות חתימה המזהה את אמצעי החתימה האמור מתקיימות הוראות תקנה 8.

(ב) לענין קיום הוראות תקנה 8(1)(ב) ו-(ג), רשאי הגורם המאשר להסתפק בהצהרה מטעם המבקש, בדבר אמצעי החתימה שבו הוא משתמש, אופן הפעלתו והגישה אליו.

(ג) תעודה אלקטרונית תהיה בהתאם לתקן ISO/IEC 9594-8.

פרק ה': פרטים בתעודה אלקטרונית ושונות

פרטים בתעודה אלקטרונית

14. (א) היה המבקש יחיד אשר זוהה שלא לפי תעודת זהות, תכלול התעודה האלקטרונית שתונפק לו את מספר הזיהוי שעל פיו זוהה, לפי תקנה 10, ואם היה המבקש תושב חוץ – גם את מקום הנפקת המסמך המזהה.

(ב) היה המבקש תאגיד, תכלול התעודה האלקטרונית שתונפק לו את שם התאגיד ומספרו הרשום, שמו ותוארו של מורשה החתימה מטעם המבקש, ואת מספר הזיהוי שעל פיו זוהה, ואם היה תאגיד שאינו רשום בישראל – גם את מקום הרישום.

(ג) היה המבקש מוסד ציבורי, תכלול התעודה האלקטרונית שתונפק לו את שם המוסד, וכן את שמו ותוארו של מורשה החתימה מטעם המבקש, ומספר הזיהוי שעל פיו זוהה.

שינוי תקן

15. (א) הוחלף תקן מן התקנים הנזכרים בתקנות אלה, לרבות מסמך RFC, בתקן או מסמך חדש, לפי הענין, 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, תוך זמן שיורה הרשם;

(ב) הרשם יודיע לגורמים מאשרים על שינוי תקן או מסמך RFC מחייב כאמור בתקנת משנה (א), ויפרסם באתר האינטרנט שיועד לכך רשימה מעודכנת של התקנים והמסמכים המחייבים לפי תקנות אלה.

דו"ח שנתי

16. (א) הרשם יגיש לשר ולועדה לעניני מחקר ופיתוח מדעי וטכנולוגי של הכנסת, אחת לשנה ולא יאוחר מיום 1 באוקטובר של השנה, דין וחשבון בדבר הפעלת סמכויותיו לפי תקנות אלה, לרבות בדבר הטכנולוגיות שאושרו והליכי אישורן.

(ב) הדו"ח האמור בתקנת משנה (א) יפורסם באתר האינטרנט של הרשם.

תחילה

17. תחילתן של תקנות אלה ביום תחילתו של החוק.

תוספת

תקנה 1

1. Internet Engineering Task Force (IETF)
2. National Institute of Standards and Technology (NIST)
3. American National Standards Institute (ANSI)
4. European Telecommunications Standards Institute (ETSI)
5. International Standards Organization (ISO)
6. מכון התקנים הישראלי

_____
מאיר שטרית
שר המשפטים

התשס"א (, 2001)
(חמ 3127-3)