Comsign – דוח אימות חתימה אלקטרונית על פי חוק חתימה אלקטרונית

קומסיין הינה "גורם מאשר" [International Trusted CA] המנפיק חתימות אלקטרוניות **מאובטחות (ומאושרות)** **על פי חוקי מדינת ישראל.**

לא כל חתימה הנחזית להיות מאובטחת – היא אכן מאובטחת. אם היא אינה מאובטחת, עלולה מערכת ניהול ספרים הכוללת מסמכים דיגיטליים מבוססי חתימות לא מאובטחות – להיפסל !

על מנת שחתימה אכן תהיה מאובטחת, צריכים להתקיים בה כל אלה על פי חוקי המדינה:

חוק חתימה אלקטרונית – פרק א' – כללי, סעיף קטן מס' 1:

"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;

תקנות חומרה ותוכנה- פרק ג': חתימה אלקטרונית מאובטחת

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

חזקה לעניין 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 1,024 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 ביטחון 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.