



תקני חתימה אלקטרונית בישראל

התקן	הארגון	היכן נזכר	הדרישה	נושא התקן
תקן ישראלי (ת"י) 7799	מכון התקנים הישראלי	תקנה 2(2) לתקנות חתימה אלקטרונית(רישום גורם מאשר וניהול)	גורם מאשר נדרש להמציא תעודה בדבר עמידתו בתקן	תקן לניהול אבטחת מידע מטפל, בראיה כלל ארגונית בכל ההיבטים הנדרשים למתן פתרונות שלמים לנושאי אבטחת המידע. התקן מתווה שיטה להקמה, לניהול ולתחזוקת כל הבקורות הנדרשות, לנטר אותן בשיטתיות, למנוע תקלות מראש ולהכין דרכי תגובה לאירועים אפשריים. מצגת Power Point ודברי הסבר לתקן של שוקי פרייס ממכון התקנים הישראלי.
ISO-9000	אירגון התקינה הבינלאומי (ISO)	תקנה 2(3) לתקנות חתימה אלקטרונית(רישום גורם מאשר וניהול)	על גורם מאשר להמציא תעודה המעידה על התאמתו לדרישות התקן כתנאי לרישום במירשם הגורמים המאשרים	סדרת תקנים בינלאומית לניהול ולהבטחת איכות. למעלה מ-90 מדינות ברחבי תבל אימצו את התקן כתקן לאומי, ובכללן ישראל (ת"י 9000).
CWA 14167-1	ועדת התקינה האירופאית	התקן לא נזכר כשלעצמו בתקנות, אבל...	גורם מאשר נדרש להמציא תעודה בדבר עמידתו בתקן	תקן לניהול אבטחת מידע מטפל, בראיה כלל ארגונית תקן להוכחת עמידת גורם מאשר בדרישות החוק והתקנות לפיו, ולעניין סטנדרט אבטחת המידע והמהימנות הנדרשים לניהולה ולהפעלתה של מערכת המשמשת לפעולות חיוניות בגורם מאשר. סייגים לתחולת התקן: דרישות אבטחה מהמודול הקריפטוגרפי, הוראות בנושא אלגוריתמים, מגבלות על שימוש במפתחות ומבנה תעודה, הצפנה של מידע קריטי, איסוף מידע הנדרש בדירקטיבה האירופית להנפקת תעודה, תוכן שדה "שם" בתעודה, הוראות בעניין אלגוריתמים לחתימה, מבנה תעודה, עדכון רשימת תעודות בטלות, הוראות בנושא אלגוריתמים.
CWA 14172-3	ועדת התקינה האירופאית	התקן לא נזכר כשלעצמו בתקנות, אבל...	גורם מאשר נדרש להמציא תעודה בדבר עמידתו בתקן	תקן עזר ל-1-14167 CWA
RFC 2527	Internet Engineering	תקנה 1 לתקנות חתימה	גורם מאשר נדרש לערוך	"This document presents a framework to assist the

<p>writers of certificate policies or certification practice statements for certification authorities and public key infrastructures."</p> <p>RFC 3647 יוחלף בתקן 1.3.04 מיום 1.3.04 יוחלף בתקן RFC 3647 *</p>	<p>את הוראות הנוהל, שלפיהן הוא פועל ("מסמך הנהלים") לפי תקן זה</p>	<p>אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות)</p>	<p>Task Force (IETF)</p>
<p>הוראות בדבר דרישות אבטחה מסיסמאות שונות.</p> <p>*מטרת הדרישה לוודא כי הפעלת אמצעי החתימה והגישה אליו תיעשה רק בידי מי שיש לו ההרשאה לשימוש באמצעי החתימה. כאשר מדובר על סיסמת גישה לכרטיס חכם או לאמצעי פיזי אחר, דרישות האבטחה לפי ת"י 1495 חלק 3 עשויות להיות חמורות מדי משום שהן מתעלמות מכך שהמידע מוגן על גבי אמצעי פיזי המצוי בשליטת בעליו, ולא במערכת מידע רגילה. הנחיית הרשם לעניין דרישות חלופיות לת"י 1495 עפ"י תקנה 8(ג) הינה:</p> <ol style="list-style-type: none"> 1. אורך סיסמא (6 תווים לפחות) 2. נעילת סיסמא (חסימה אחרי 7 ניסיונות כושלים) 3. שחרור מנעילה (ע"י הקלדת סיסמת שחרור או ע"י מנגנון ייעודי שיאושר ע"י הרשם) 4. מורכבות סיסמא (שילוב תווים באותיות וקטנות, סימנים מיוחדים וספרות ואפשר שימוש בסיסמאות ארוכות המאפשרות רישום משפטים) 	<p>אם הפעלת אמצעי החתימה כרוכה בשימוש בסיסמה, עליה לעמוד בדרישות אבטחה ברמה הגבוהה לפי תקן זה: הווה אומר, שישה תווים לפחות, הכוללים ספרות, סימנים, אותיות רישיות ואותיות רגילות, אסורים תווים חוזרים על עצמם ותווים סמוכים זה לזה במקלדת.</p>	<p>תקנה 8(1)(ג) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות)</p>	<p>מכון התקנים הישראלי ישראלי 1495 תקן (ת"י) חלק 3</p>
<p>Security Requirements For Cryptographic Modules: "This publication provides a standard that will be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data....This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard</p>	<p>אמצעי החתימה של הגורם המאשר - והן האמצעי, שחזקה כי הוא מחולל חתימה אלקטרונית מאובטחת - צריכים לעמוד בדרישות האבטחה של</p>	<p>תקנות 4(2) ו-8(1)(ב) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות)</p>	<p>National Institute of Standards and Technology (NIST) FIPS 140-2</p>

<p>provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments..."</p>	<p>התקן</p>			
<p>מדרג של רמות אבטחת מידע, אשר אומץ על בידי ארגון התקינה הבין לאומי, בתקן ISO 15408 .</p>	<p>מערכות המחשב של גורם מאשר המשמשות לזיהוי מבקש, להנפקת תעודה אלקטרונית ולביטולה יעמדו ברמות הביטחון של common criteria EAL4 האמצעים המשמשים להגנה על אמצעי חתימה יעמדו ברמות בטחון של common criteria EAL2</p>	<p>תקנות 5 ו-8(1)(ב) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות)</p>	<p>International Common Criteria Project ראה עוד ב- אירגון התקינה הבינלאומי (ISO)</p>	<p>Common Criteria EAL - Parts 1, 2 & 3</p>
<p>תקן לתעודות אלקטרוניות. פורסם גם כתקן X509v.3 של הארגון הבינלאומי IETF, צוות המשימה להנדסת אינטרנט.</p>	<p>תעודה אלקטרונית תהיה בהתאם לתקן ISO/IEC 9594-8.</p>	<p>תקנה 13(ג) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות)</p>	<p>אירגון התקינה הבינלאומי (ISO)</p>	<p>ISO/IEC 9594-8</p>
<p>"This standard specifies a suite of algorithms which can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory. This is known as nonrepudiation since the signatory cannot, at a later time, repudiate the signature".</p>	<p>תקנות חתימה... אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות) קובעות כי חזקה שאלגוריתמים מסוימים מפיקים חתימה אלקטרונית מאובטחת (בהתקיים תנאים נוספים). הגדרת אלגוריתמים אלה הינה "RSA", "DSA" ו-</p>	<p>התקן לא נזכר כשלעצמו בתקנות, אבל.....</p>	<p>National Institute of Standards and Technology (NIST)</p>	<p>FIPS 186-2</p>

- "Elliptic Curve DSA"

אלגוריתמים להפקת

חתימה אלקטרונית

מאובטחת, שהכיר בהם

אחד הגופים המפורטים

בתוספת. NIST הוא אחד

הגופים הללו והתקן מכיר

באלגוריתמים הללו.
