



Head of ILITA

ראש הרשות

תאריך: 26 יולי 2011
כ"ד תמוז תשע"א
סימוכין: 015-99-2011-006824
באמצעות: דוא"ל

לכבוד
פרופ' יעקב נאמן
שר המשפטים

לכבוד
ועדת המדע והטכנולוגיה
כנסת ישראל

נכבדי

הנדון: דו"ח רשם גורמים מאשרים לשנת 2010

1. אני מתכבד להביא בפניכם את הדו"ח אודות פעילות רשם גורמים מאשרים, לפי חוק חתימה אלקטרונית, התשס"א-2001, הפועל במסגרת הרשות למשפט, טכנולוגיה ומידע (רמ"ט). דו"ח זה ישולב במסגרת דו"ח מאוחד על פעילות רמ"ט לשנת 2010.
2. הדו"ח נכתב על ידי עמית אשכנזי, רשם הגורמים המאשרים, בסיוע עובדי מחלקת רישום ופיקוח ברמ"ט אשר עמלו על פעולות הפיקוח - הגב' רבקי דב"ש, הגב' לימור שמרלינג מגניק ומר עזמי טנוס. אבקש להודות להם על פעולתם.
3. דו"ח זה מציג מגוון פעולות שנעשו במסגרת רמ"ט בשנת 2010 בתחום החתימה האלקטרונית, ומעיד על היות רמ"ט רגולטור פעיל בתחום. מקצת מהנושאים המפורטים בדו"ח מציפים בעיות בשוק החתימה האלקטרונית, כמו גם חוסרים בכלי הרגולציה בידי רשם גורמים מאשרים.
4. רמ"ט תשמח להשתתף בדיון בנושא בוועדה ואצל כבוד השר, ולהציג את עיקרי הדו"ח.

בכבוד רב,

יורם הכהן
ראש הרשות למשפט, טכנולוגיה ומידע

העתקים:
ד"ר גיא רוטקופף, מנכ"ל משרד המשפטים
הגב' שרית דנה, המשנה ליועץ המשפטי לממשלה (אזרחי)
מר טל הרמתי, סגן בכיר לחשב הכללי



**דין וחשבון של רשם גורמים מאשרים בדבר הפעלת סמכויותיו בשנת
2010 לפי תקנה 16 לתקנות חתימה אלקטרונית (חתימה אלקטרונית
מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), תשס"ב-2001**

מוגש לוועדת המדע והטכנולוגיה מכח תקנה 16 לתקנות חתימה אלקטרונית (חתימה אלקטרונית
מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001



1. פעולות פיקוח על הגורם המאשר – חברת קומסיין

1.1 נתונים

1.1.1 בתחום חתימה אלקטרונית הוגשו בשנת 2010 7 תלונות המהוות כ-2.5% מכלל התלונות שהגיעו לרמ"ט. ביחס לשנת 2009, עלתה כמות הפניות בתחום חתימה אלקטרונית ב-75%, אולם נתח הפניות בתחום חתימה אלקטרונית מכלל הפניות שהגיעו לרשות, ירד ב-0.5%.

1.1.2 במהלך השנה נפתחו ברמ"ט 13 תיקי פיקוח בנושא חתימה אלקטרונית, המהווים 13% מכלל תיקי הפיקוח שנפתחו בשנה זו. כמו כן, המשיך הטיפול ב-3 תיקי פיקוח בתחום זה שנפתחו קודם לשנת 2010.

1.1.3 חלוקת התיקים לפי סוגיהם היא כדלקמן –

סוג התיק	כמות
תיקי פיקוח לצרכי אישור רשם	11
תיקי פיקוח בשל מהלך ייזום	4
תיקי פיקוח בעקבות תלונה	1
סה"כ	16

1.2 עדכון מסמך הנהלים של קומסיין

1.2.1 בספטמבר 2010 בתום הליך בחינה מקיף אישר רשם גורמים מאשרים הפועל במסגרת רמ"ט (בדו"ח זה – **הרשם**) את מסמך הנהלים החדש של חברת קומסיין בהתאם לתקנות לפי חוק חתימה אלקטרונית, התשס"א-2001 (בדו"ח זה – **החוק**).

1.2.2 מסמך הנהלים של הגורם המאשר מהווה את תקנון השירות שלו, ומסדיר את התחייבויותיו והצהרותיו כלפי לקוחותיו וכלפי מי שמסתמך על התעודה האלקטרונית שהנפיק.

1.2.3 הליך עדכון מסמך הנהלים נדרש בשל עדכון התקן הבינלאומי לפיו ערוכים מסמכי הנהלים בתחום זה (ietf rfc 3647), בשל הצורך לאפשר לקומסיין פעילויות נוספות, ובשל הצורך לעדכן את מסמך הנהלים בעקבות לקחים וממצאים מפיקוחים בעבר.

1.2.4 במסגרת הדיונים על מסמך הנהלים נבחנו בצורה מעמיקה שורה של תהליכים והסדרים הקשורים בפעילות חברת קומסיין. דגש משמעותי בתהליך ניתן להגנה על אינטרסים של בעלי התעודות האלקטרוניות - לקוחות קומסיין. ההנחה היא כי המוצר "תעודה אלקטרונית" הינו מוצר מורכב וללקוחות עשוי להיות קושי להבין את ההיבטים השונים הקשורים אליו או לנהל משא ומתן אפקטיבי עם הגורם המאשר לגבי תנאי השירות. כמפורט בקצרה להלן.

1.2.5 במסגרת זו נקבע כי הגורם המאשר לא יוכל להגביל את אחריותו לתעודות המונפקות לצורך מילוי דרישת חתימה בחיקוק או לפי דרישה של רשות מרשויות המדינה אל מתחת ל- 500,000 ₪ לתעודה אלקטרונית.

1.2.6 יצויין כי קומסיין ביקשה שסכום תקרת האחריות יעמוד על 10,000 ₪ (וזאת לעומת 500,000 ₪ שאליהם התחייבה במסמך הנהלים שאושר לה בעבר). הרשם התנגד נחרצות לבקשה זו משום שכיום מרבית הלקוחות הנזקקים לחתימה אלקטרונית ולתעודה אלקטרונית עושים זאת על מנת לקיים דרישה של רשויות המדינה. ללקוחות אלה אין ברירה או יכולת לבחור במוצר אחר. בנוסף, ללקוחות אלה אין כל דרך להגן על עצמם מפני רשלנות של קומסיין.

1.2.7 השימושים הנפוצים כיום בחתימה אלקטרונית, הינם לדיווחים לרשות ניירות ערך, לרשות המסים ולצורך הגשת מכרזים מקוונים. ככאלה הם עשויים להיות קשורים בפעולות כספיות בסכומים גבוהים יותר. אין כל הצדקה, לשיטת הרשם, לגלגל על לקוחות הגורם המאשר את הסיכונים במקרים שבהם נקבע כי יש לגורם המאשר חבות אזרחית. יודגש כי הגבלת האחריות שביקשה קומסיין לקבוע נועדה לחול גם במקרים שבהם נקבע שהתרשלה.

1.2.8 בפקיח שהחל בשנת 2010 (לאחר אישור המסמך וכניסתו לתוקף) על בסיס מידע שהגיע לרשם, התברר כי בניגוד מוחלט לאמור במסמך הנהלים המחייב אותה, המשיכה קומסיין לקבוע הגבלת אחריות בסכומים נמוכים מזה שאושר בתעודות.

1.2.9 בעקבות הבירור הציעה קומסיין לחזור בה ממגבלה זו ביחס לכל התעודות התקפות שהונפקו על ידה, לרבות אלה שהונפקו לפני ספטמבר 2010. לאחר אישור הצעה זו על ידי הרשם, שלחה קומסיין בהנחיית הרשם הודעה אישית לבעלי תעודה כאמור, וכן פרסמה באתר האינטרנט שלה ובשני עיתונים יומיים, על ביטול המגבלה האמורה. המעקב אחר הטיפול בנושא זה נמשך בשנת 2011. ההתחייבות של קומסיין מפורסמת באתר הרשם.

1.2.10 במסגרת אישור מסמך הנהלים אושר עוד לקומסיין להנפיק תעודות אלקטרוניות לשימוש תאגידי על גבי שרת, בהתאם לנהלים מתאימים. התערבות הרשם נועדה לצמצם את הסיכונים הכרוכים בהנפקה של אמצעי חתימה, שהינו אישי מטבעו, על גבי רכיב המצוי ברשת הארגונית ולכאורה לא נמצא בשליטתו הבלעדית של בעל אמצעי החתימה, כהגדרתו בחוק.

1.2.11 בהתאם לאישור יכולה קומסיין להנפיק תעודה אלקטרונית כאמור רק לגבי מורשה חתימה בתאגיד, משום ההנחה כי החתימה נעשית במסגרת האחריות הכוללת של התאגיד.

1.2.12 נושא תעודות אלקטרוניות על שרת נמצא בבחינה נמשכת על ידי הרשם, בשל היתרונות התפעוליים הכרוכים במימוש זה של חתימה אלקטרונית.

1.3 כשל פרסום רשימת תעודות בטלות (CRL)

1.3.1 בתאריך 1.11.2010 דיווח לרשם צד מסתמך על תעודות אלקטרוניות, כי אירעה תקלה בפרסום רשימת התעודות המבוטלות (CRL) של חברת קומסיין, באופן שכל התעודות שהונפקו על ידי החברה זוהו כלא תקפות



כאשר הושאו למול רשימת התעודות הבטלות (CRL – Certificate Revocation List). לחברת קומסיין נדרשו מספר שעות לאתר את מקור התקלה, שנבעה מאי פירסום קובץ CRL עדכני של שרת העוגן (Root CA).

1.3.2 בעקבות האירוע בוצע פיקוח על ידי רמ"ט, וכן בוצע תחקיר פנימי על ידי החברה שמסקנותיו הועברו לרמ"ט. מממצאי הפיקוח והתחקיר העלו תמונה מטרידה באשר להתנהלות קומסיין וקיום חובות הזמינות של מנגנון התעודות הבטלות על ידה.

1.3.3 מקור התקלה היה העובדה כי תוקף ה-CRL של ה-Root CA שמפרסמת קומסיין פג, ועל כן החל ממועד התפוגה נחזו כל שרתי הנפקת התעודות של קומסיין המנפיקים תעודות אלקטרוניות לחתימה אלקטרונית מאושרת כבטלים (Revoked)¹, וכתוצאה מכך נחזו כל התעודות האלקטרוניות ששרתים אלה הנפיקו כבטלות.

1.3.4 קובץ CRL עדכני של שרת ה-Root CA של קומסיין אמור להיות מופק, להחתם אלקטרונית על ידי שרת ה-Root CA ולהתפרסם כל חצי שנה. פעולה זו, המתבצעת ידנית, לא בוצעה על ידי החברה. הסתבר כי במערכות קומסיין לא הייתה קיימת מערכת המתריעה מראש על הצורך בפרסום קובץ CRL עדכני של ה-Root CA.

1.3.5 בנוסף, במקרה של אירוע חריג כפי זה, בו כל תעודות קומסיין הופכות לבטלות, נשלחו הודעות SMS באופן רצוף ל-6 בעלי תפקידים בחברת קומסיין המתריעות על תקלה. במקרה הנדון, חמישה מהעובדים ציינו כי ראו את ההודעות בשעות הבוקר, ועובד אחד ראה את ההודעות בשעה 3:00 לפנות בוקר, אולם לא התריע על הנושא היות והיה טרוד בעניינים אחרים.

1.3.6 במהלך הביקורת הסתבר, כי בשל רשלנות נוספת של קומסיין, קודם לתקלת ה-CRL, לא עבדו חלק ממערכות התיעוד בשל כשל במעקב אחריהן.

1.3.7 הנסיבות לתקלה, והאופן בו היא טופלה, והבעיות האחרות שאותרו, העידו על כשלים יסודיים בניהול החברה. בעקבות הממצאים הודיעה קומסיין על נקיטת צעדים מתקנים למניעת אירועים כאלה בשנית, ובשל כך הסתיים הטיפול במקרה.

1.3.8 יצויין, כי לרשות הרשם לא עומדת סנקציה של עיצום כספי על אירוע בנסיבות החמורות המתוארות בסעיף זה. הפעלתה של סנקציית התליית הרישום במרשם הגורמים המאשרים, עד לתיקון מלוא הליקויים או לביצוע שינויים משמעותיים הקבועה בסעיף 14 לחוק לא הייתה אפשרית בשל היות קומסיין הגורם המאשר היחיד הרישום במרשם, והתלות גורמים רבים, פרטים וציבוריים, בשירות שהיא מספקת.

¹ בפועל מדובר בכך שהתעודה האלקטרונית של שרת ההנפקה נחשבת כבטלה.



1.4 הארכת מועד אישור הגורם הרושם – ההוצאה לאור של לשכת עורכי הדין

- 1.4.1 בעבר אשר הרשם את ההוצאה לאור של לשכת עורכי הדין (להלן בפרק זה – **ההוצאה לאור**) כגורם רושם, קרי גורם המוסמך לזהות בשם הגורם המאשר את מבקשי התעודות האלקטרוניות. במסגרת האישור של ההוצאה לאור נקבעו תנאים הנדרשים לפעילות.
- 1.4.2 בדצמבר 2009, בוצעה ביקורת בהוצאה לאור בעקבותיה הוארך האישור לשלושה חודשים בלבד, בכפוף לקיום תנאים שבהחלטה. במרץ 2010 הוארך האישור לתקופה נוספת של חודש ימים להשלמת קיום התנאים ושיפור רמת האבטחה. בסוף אפריל 2010 הוארך האישור עד לתום השנה בכפוף לקיום כל הדרישות שנקבעו בעבר, בין היתר יישום שיפור האבטחה והגשת נהלים מתוקנים.
- 1.4.3 על מנת לתת להוצאה לאור ודאות תפעולית, האישורים נקבעו לתקופה ארוכה יחסית. לקראת סוף שנת 2010 נדרשה שוב הארכת תוקפו של האישור בארבעה חודשים על מנת לאפשר השלמה מסודרת של הדרישות.
- 1.4.4 בפיקוח שנעשה אגב הארכת האישור הסתבר כי קיים פער בין הליך ההזדהות של עובדי קומסיין וההוצאה לאור כפי שעוגן בנהלי החברה, לבין אופן ההזדהות בפועל. בנוסף, התברר כי ישנו ליקוי אבטחתי באופן ההזדהות.
- 1.4.5 בעקבות ממצאי הפיקוח הציעה החברה פתרון ברמת החומרה והתוכנה אשר אושר על ידי הרשם, וכן נערכו שינויים ברמת ניהול ההרשאות. מטבע הדברים, בשל סודות מסחריים ושיקולי אבטחת מידע, לא יועבר מידע מעבר למפורט בדו"ח זה.

1.5 אישור מתחמי עבודה נוספים

- 1.5.1 בשנת 2010, בשל הגידול בביקוש לתעודות אלקטרוניות, ביקשה קומסיין להוסיף אתרים פיזיים לאתרים בהם היא נותנת שירות.
- 1.5.2 צוות הפיקוח של רמ"ט בחן את הבקשות ואת היבטי אבטחת המידע הקשורים בהפעלתם. לאחר ביצוע ביקורות באתרים אושר לחברה להרחיב את מתחם ההנפקה בסניף תל אביב (קרית עתידים) וכן במתחם חדש בחיפה.



1.6 אישור מנגנון שחרור מנעילה של כרטיס חכם

1.6.1 בהמשך להנחיית רשם 1-2010 (ראו להלן) בה אישר הרשם יישום מנגנוני שחרור מנעילה במטרה להקל על ציבור המשתמשים בתעודות אלקטרוניות, הגישה קומסיין ביולי 2010 הצעה ליישום פתרון של תהליך שחרור מנעילה של כרטיס חכם.

1.6.2 באוגוסט 2010 לאחר בחינת הנושא החליט הרשם לאשר לחברה להשתמש במנגנון כזה.

1.6.3 האישור האמור הותנה והתבסס על התחייבויות שלקחה על עצמה החברה והצהרות שנתנו, בין היתר, באשר לנטילת אחריות מלאה על הסיכונים הקשורים במימוש המנגנון.

1.7 בקשה לאישור גורם רושם נוסף

1.7.1 באפריל 2010 הגישה חברת קומסיין בקשה לאישור של חברה נוספת כגורם רושם. בשל ליקויים רבים בהליך הגשת הבקשה, הוחזרה הבקשה ביום בתחילת יוני 2010 לקומסיין להגשה מחדש.

1.7.2 בתחילת אוקטובר 2010, לאחר הגשת בקשה מתוקנת, ניתן על ידי הרשם אישור עקרוני לגורם הרושם הנוסף, אשר הותנה בקיומן של מספר דרישות.

1.7.3 הליך הבחינה של הבקשה בהתאם להנחיות נמשך בשנת 2011.

2. בקשות רישום חדשות

2.1 עדכון הנחיות פנימיות לרישום

2.1.1 במהלך שנת 2010 עדכן הרשם את ההנחיה הפנימית המנחה אותו בעת רישום גורמים מאשרים (מבחנים לרישום גורם מאשר עפ"י חוק החתימה האלקטרונית, התשס"א-2001), הקשורה בבדיקות אבטחת המידע והאבטחה הפיזית של הגורמים המאשרים. בשל היבטי האבטחה של הנחיה זו, היא אינה מפורסמת.

2.1.2 ברמ"ט מבוצעת עבודת עדכון כוללת להנחייה זו, הקשורה באופן ההסדרה והפיקוח של גורמים מאשרים. במסגרת זו, פורסמה גם הנחיה 2-2010, כמפורט מטה, שעניינה ביצוע בדיקות לגורם מאשר בידי גורם חיצוני באופן שנועד להבטיח עמידה בהוראות החוק.

2.2 בקשת רישום של חברת סקירנט גורם מאשר בע"מ

2.2.1 במהלך שנת 2010 טיפל הרשם בבקשת רישום חדשה של חברת פרסונל איי.די.בי. (לשעבר סקירנט גורם מאשר בע"מ), במסגרתה נעשה שימוש בהנחיה 2-2010 שנועדה לתת בידי הגורם המאשר שיקול דעת רב יותר באשר לאופן המימוש הטכנולוגי של השירות, תוך שמירה על תכליות ומטרות החוק.

2.2.2 במסגרת הטיפול בבקשת הרישום נערכו בדיקות מקיפות למסמך הנהלים של החברה (תקנון השירות), לנהלי העבודה שלה, ולהיבטי אבטחת מידע לוגיים ופיזיים בפעולתה. הליך הרישום המשיך בשנת 2011.



3. פרסום הנחיות רשם גורמים מאשרים

3.1 בשנת 2010 פורסמו 5 טיוטות הנחיה, מהן 4 נכנסו לתוקף.

3.2 הנחייה 1-2010

3.2.1 הנחיה 1-2010 עוסקת בקביעת דרישות חלופיות לסיסמת הגישה לאמצעי החתימה, כלומר ה"קוד הסודי" המשמש לגישה לביצוע החתימה האלקטרונית. נוסח ההנחיה מצ"ב כנספח א' לדו"ח זה.

3.2.2 קוד הגישה הוא רכיב חשוב מאוד במעטפת ההגנה על אמצעי החתימה של החותם, משום שהוא זה שמאפשר בפועל שימוש בתעודה האלקטרונית לצורך חתימה האלקטרונית. בהתאם לתקנות חתימה אלקטרונית נדרש אמצעי זה, ככל שאינו ביומטרי, לעמוד בהוראות תקן ישראלי 1495 חלק 3 העוסק בסיסמאות. אל הרשם הגיעו תלונות בנושא קושי בטיפול בסיסמא לפי תקן זה.

3.2.3 לאחר בחינה מקיפה של הנושא והתייעצות עם הגורמים הרלבנטיים, ניתנה הנחייה המאפשרת הוראות מקלות יותר, שאינן פוגעות במידת האבטחה והבטיחות של השימוש בחתימה.

3.2.4 בנוסף, עקב תלונות הקשורות במצבים שבהם משתמש שוכח סיסמא, נקבע הסדר ספציפי לנושא זה. בתמצית ייאמר כי לשחרור מנעילה של כרטיס יש חשיבות צרכנית רבה ללקוח, משום שהדבר מאפשר לו לחזור ולהשתמש בתעודה האלקטרונית שלו לחתימה אלקטרונית, מבלי שיידרש להנפיק תעודה אלקטרונית חדשה. מנגד, מנגנון שחרור מנעילה של אמצעי חתימה, טומן בחובו סיכון לשימוש לרעה באמצעי החתימה, שכן ניתן באמצעות המנגנון להשתלט על אמצעי החתימה ולעקוף את מנגנוני ההגנה שלו.

3.2.5 על מנת לאזן בין שני צרכים אלה, כוללת ההנחיה אפשרות להגיש בקשה מתאימה לרשם בה מוצע מנגנון כזה. במועד הגשת הדוח הגישה חברת קומסיין בקשה מתאימה שנבחנה ואושרה². בשל חשיבותו של נושא זה הוא עובר בחינה מחודשת.

3.3 הנחייה 2-2010

3.3.1 הנחיה 2-2010 נועדה לקבוע חובות מהותיות למערכות הטכנולוגיות הייעודיות המשמשות גורם מאשר בפעילותו, ודרכי דיווח אודותן. נוסח ההנחיה מצ"ב כנספח ב' לדו"ח זה.

3.3.2 בהתאם לתקנה 4 ו- 5 לתקנות חתימה אלקטרונית, נדרש גורם מאשר כתנאי סף לפעילותו ובכל עת, כי מערכות הליבה המשמשות את פעילותו יעמדו בתקן אבטחת המידע Common Criteria המוכר גם כתקן ישראלי 15408. תקן זה הינו תקן אבטחת מידע מחמיר, והיצע המוצרים העומדים בו אינו גדול. בנוסף, הוא מקשה על הגמישות התפעולית של הגורם המאשר משום ששינויים שמבוצעים במערכות הגורם המאשר עשויות לחרוג מגדר התקן. מבחינת פיקוח הרשם, נדרשה מעטפת בדיקות לוודא כי מוצרי הליבה מופעלים בהתאם להנחיות ולדרישות של התקינה.

² ראו לעיל.



- 3.3.3 על מנת לאפשר גמישות תפעולית לגורמים המאשרים, להקל על עבודת הפיקוח של הרשם, ולוודא כי מכלול הנושאים המהותיים הנדרשים לבטיחות ואבטחה של מערכת הליבה מטופלים, החליט הרשם ליישם בישראל, בשינויים מסויימים, תוצרים של עבודת ההסדרה האירופאית.
- 3.3.4 בין תוצרי העבודה של גורמי התקינה האירופאים, מצוי מסמך "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements CWA 14167-1³, כלומר ניהול מערכת של גורם מאשר.
- 3.3.5 מסמך זה מגדיר את הפונקציות החיוניות במסגרת מערכת כאמור, ומכסה את התחומים בהם יש דרישה מנדטורית לבדיקה של אבטחת המידע ומהימנות במערכת ניהול תעודות אלקטרוניות של גורם מאשר, וקובע את הדרישות מהן. מטרת התקן להגדיר דרישות אבטחה כוללות מהמערכת. התקן נועד לשימוש על ידי מתכננים של מערכות המשמשות לניהול תעודות לחתימה אלקטרונית, כמו גם ללקוחות של מערכות כאלה.
- 3.3.6 בבירור עם רשמים מקבילים מאירופה, תקן CWA 14167-1 משמש מקור מקצועי לעניין הסטנדרט הנדרש ממערכת המנהלת את התעודות. בנוסף, הוא נקבע גם כמסמך בעל תוקף מנחה, בהתאם להוראות סעיף 3(5) לדירקטיבה.
- 3.3.7 להכרה בתקן ולשימוש בו במסגרת פעילות גורם מאשר יתרונות מבחינת הרחבת היצע המערכות שניתן להשתמש בהן לגורם מאשר, תוך התאמה של מעטפת האבטחה לארגון המסוים בה מוטמעת המערכת. כך למשל באירופה נעשה שימוש בתקן זה לצורך בחינה של מערכות בפיתוח עצמי על ידי הגורם המאשר.
- 3.3.8 אופן בדיקת התקן שונה מהבדיקות הנדרשות לצורך עמידה בתקן Common Criteria. מאחר שבישראל אין מעבדה מוסמכת לתקן זה, יש חשיבות לאפשרות הסתמכות על גורמי בדיקה נוספים. בהתאם למסמך עזר שפורסם למסמך CWA 14167-1, הידוע כ- CWA 14172-3, ניתן להסתמך על חוות דעת מקצועית של גורם מומחה בלתי תלוי לעניין אופן עמידה בתקן. בהתאם לכך נכללו בהנחייה 2-2010 הוראות ודרישות לעניין תנאי הכשירות של עורך חוות הדעת ולגבי אופן עריכתה.
- 3.3.9 ההנחייה נכנסה לתוקף ביולי 2010. נכון לסוף שנת 2010, למרות ארכות, הגורם המאשר הרשום, חברת קומסיין, לא עמדה בהנחייה, הן מבחינה מהותית (כלומר מימוש של עקרונות התקן במערכותיו) והן מבחינה טכנית, כלומר הצגת חוות דעת המפרטת את אופן העמידה בהנחייה. בעקבות זאת נדחה גם כניסתה לתוקף של הנחייה 4-2010, כמפורט מטה.
- 3.3.10 במסגרת הטיפול בהנחייה 2-2010 נחשפו פרטים חשובים ומשמעותיים על פעולת קומסיין. במסגרת זו התברר כי לקומסיין אמנם הייתה בעלת מערכת שהוסמכה לתקן כנדרש בתקנה 5, אולם אופן השימוש בפועל במערכת חרג מההסמכה, באופן שהמערכת לא עומדת לכאורה גם בדרישות

³ CEN Workshop Agreement, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements, June 2003.cbux;



תקנה 5 עובר להוצאת ההנחייה. חברת קומסיין מבצעת מאז דצמבר 2010, שינויים משמעותיים במערכות המידע שלה באופן שמעיד על כוונה לציית להנחיה. נושא זה ממשיך ומתברר במהלך 2011, וידווח בדו"ח לשנה זו.

3.4 הנחייה 4-2010

3.4.1 הנחיה 4-2010 נועדה להשלים את מהלך עדכון האלגוריתמים ואורכי המפתחות לביצוע חתימה אלקטרונית לפי החוק, בהמשך לחוות דעת של ד"ר בני פנקס, וכפי שדווח בדוחות קודמים. נוסח ההנחיה מצ"ב כנספח ג' לדו"ח זה.

3.4.2 בתקופה הרלבנטית לדוח זה היה רשומה במרשם רק חברת קומסיין. מימוש הנחייה 4-2010 הוא בעל השלכות על מערכות המידע של הגורם המאשר מאחר שהוא מחייב חילול והנפקה של מפתחות חדשים לחתימה אלקטרונית של תעודות אלקטרוניות לחתימה אלקטרונית מאושרת בהתאם להנחייה.

3.4.3 מאחר שחברת קומסיין התקשתה לעמוד בהנחייה 2-2010 להנחת דעת הרשם, התקבלה החלטה שכל הקשור למימוש הנחייה 4-2010 לגבי מערכותיה יידחה עד לעמידה של המערכת להנחת דעת הרשם בהנחיה.

3.4.4 בתחילת שנת 2011 נדחה יישום ההנחיה שוב לבקשת גורמי המדינה בשל הצורך בהערכות ליישום ההנחיה. בהתאם לכך הנחייה 4-2010 נכנסה לתוקף בתחילת 2011 לעניין משתמש הקצה החותם, אולם לעניין החתימה של הגורם המאשר היא תכנס לתוקף בהמשך שנת 2011.

3.5 הנחייה 5-2010 - זיהוי חלופי

3.5.1 מטרת הנחייה זו לממש את ההסמכה בתיקון בתקנות חתימה אלקטרונית שנועד לאפשר שימוש במסמך זיהוי חליפי שני שאינו דרכון או רשיון נהיגה, והיא מממשת את תיקון התקנות המפורטות להלן. נוסח ההנחיה מצ"ב כנספח ד' לדו"ח זה.

3.5.2 במקביל לצורך יישום התקנות פנה הרשם לגורמים המנפיקים תיעוד עם תמונה על מנת לבחון אפשרות של הכרה בתיעוד זה כמסמך זיהוי נוסף. למועד עריכת דוח זה לא הגיעו תגובות רלבנטיות.



4. תיקוני חקיקה

4.1 בשנת 2010 היתה רמ"ט שותפה מרכזית בתהליכי חקיקה וחקיקת משנה אשר עדכנו את החוק. במסגרת זו הציגה רמ"ט היבטים מעשיים של יישום החוק למקבלי ההחלטות בממשלה ובכנסת, על בסיס הידע שנצבר אצלה בהפעלת סמכויות הרשם והתמקצעות בנושא משפט וטכנולוגיה.

4.2 חוק חתימה אלקטרונית (תיקון מס' 2), התש"ע-2010

4.2.1 ב- 07.07.2010 אושר תיקון מספר 2 לחוק לאחר דיון מקיף בוועדת המדע והטכנולוגיה של הכנסת. התיקון מבוסס על הצעת חוק ממשלתית שנועדה להסדיר הנפקת תעודות אלקטרוניות לחתימה אלקטרונית מאושרת על ידי המדינה באמצעות יחידותיה, ולקבוע ביחס לפעילות זו את ההרשאות הנדרשות. הצעת החוק קשורה לפרויקט תעודת הזהות החכמה החדשה, אשר במסגרתו מבקשת הממשלה להנפיק תיעוד לאומי (תעודת זהות ודרכון) המבוסס על כרטיס חכם (SmartCard) המכיל שבב מחשב המבצע פעולות עיבוד קריפטוגרפיות.

4.2.2 במסגרת ההסדרה החקיקתית חוק חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009 במסגרתו תוקן חוק מרשם האוכלוסין, התשכ"ה-1965, וזאת על מנת להסדיר את השימוש בתעודה אלקטרונית לזיהוי.

4.2.3 במסגרת תיקון מספר 2 לחוק הוסדרה האפשרות של הממשלה לשמש כגורם מאשר לתעודות אלקטרוניות על גבי התיעוד הלאומי, וכן ביחס לעובדיה. התיקון כולל גם הסמכה מתאימה לחקיקת משנה. במסגרת הדיונים בוועדת המדע והטכנולוגיה הוגבלה היכולת של הממשלה לשמש כגורם מאשר על גבי תעודת הזהות לעניין שימושים שאינם קשורים בממשלה, ונקבע שהיא תהיה בתוקף לתקופה של שלוש שנים מתחילת הפיילוט הביומטרי.

4.2.4 במסגרת תיקון מספר 2 הוסיפה הוועדה פרק אכיפה חלופית המסמך את רשם גורמים מאשרים (בפרק זה – הרשם), במקרה של העדר ציות של הגורם המאשר להנחייתו, להטיל עיצום כספי בסך 70,000 ₪. הפרק מבוסס על עבודת מטה שבוצעה במשרד המשפטים בתחום האכיפה המנהלית החלופית ועל סמך הניסיון שנצבר ברמ"ט בשנים האחרונות בפיקוח על הגורמים המאשרים.

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

4.3.1 במהלך 2010, בעקבות תלונות חוזרות של אזרחים בעניין רף הזיהוי המחמיר הנדרש בתקנות חתימה אלקטרונית, בוצע תיקון לתקנה 10 המרחיב את התיעוד עליו אפשר להסתמך בעת הנפקת תעודה אלקטרונית.

4.3.2 כרקע יצויין כי בשל תופעה של זיופי תעודת זהות, נקבע בתקנות כי לצורך הנפקת תעודה אלקטרונית, המהווה תעודת זהות לעולם המקוון, נדרש זיהוי על בסיס שני מסמכי זיהוי ובמקביל בדיקה מקוונת במרשם האוכלוסין.



4.3.3 הוראות תקנה זו העלו קשיים לגבי אוכלוסיות שאין להן מסמך זיהוי רשמי נוסף מהסוג שנקבע בתקנות (רשיון נהיגה או דרכון). בהתאם לכך תוקנו התקנות לפי הצעת הרשות, באופן המקנה שיקול דעת לגורם המאשר ומאפשר לו להסתמך, אם אין לו חשד גם על אישור בדבר זהות מטעם עו"ד. התקנות הסמיכו את הרשם לקבוע טופס מתאים בנושא זה, שנקבע ופורסם, וכן להרחיב את אפשרויות הזיהוי למסמכי זיהוי רשמיים או מעין רשמיים נוספים. לאחר התקנת התקנות פרסם הרשם הנחייה בנושא זה (ראו לעיל הנחייה 5-2010).

5. פעילות במסגרת FESA

5.1 ב- 13-14.04.2010 התקיים בורשה, פולין המפגש התקופתי של רשויות הפיקוח האירופאיות על חתימה אלקטרונית (Forum of European Supervisory Authorities – FESA), באירוח משרד הכלכלה הפולני והמכון הפולני לחקר המחשבים.

5.2 ארגון FESA הוקם באופן וולנטרי על ידי החברים, ואינו בעל מעמד רשמי של ארגון דיפלומטי אלא מהווה פורום להחלפת דעות ותיאום עמדות בין רשויות הפיקוח.

5.3 החל משנת 2007 רשם גורמים מאשרים הישראלי חבר בפורום זה כחבר משקיף, ובשנת 2008 הרשות למשפט טכנולוגיה ומידע אף אירחה את המפגש בתל אביב.

5.4 במפגש נכחו נציגים של רשויות הפיקוח מהמדינות הבאות: גרמניה, פולין, איטליה, בלגיה, הולנד, צ'כיה, שוודיה, איסלנד, לטביה, פינלנד, יוון, אוסטרליה, שווייץ. כן השתתפו נציג נציבות האיחוד האירופי, ושני חוקרים העוסקים במחקרים מטעם הנציבות לקידום המדיניות האירופית, ונציג הרשות האלבנית (שבסוף המפגש נבחר להיות חבר משקיף).

5.5 בנוסף הוזמנו נציגים של מספר גורמים פרטיים הפעילים בשוק זה להציג את פעילותם. במפגש הנוכחי נדונו מספר רב של נושאים בעלי רלבנטיות לישראל, ובהם עדכונים מנציבות האיחוד על מגמות ההסדרה והחקיקה, קידום סוגיות של תעודות זהות חכמות, הסדרה של רשימה ממוחשבת אחידה כלל אירופאית של "גורמים מאשרים", הצגה של פתרון חתימה המבוסס על טלפונים סלולרים, שירות וידוא תוקף חתימה אירופי ופולני, עדכונים על פעילות התקינה באירופה ובמיוחד על פורמט אחיד למסמכים חתומים וחתימות לטווח ארוך.

5.6 סיכום המפגש מצ"ב כנספח ה' לדו"ח זה.



נספח א'

הנחית רשם גורמים מאשרים מס' 1/2010

דרישות חלופיות לת"י 1495 להפעלת אמצעי חתימה אלקטרונית

1. כללי

- 1.1. אמצעי חתימה, המשמש לחתימה אלקטרונית⁴ לפי חוק חתימה אלקטרונית, התשס"א-2001 (להלן - **החוק**), מצוי בדרך כלל על גבי התקן קריפטוגרפי, שמטרתו שמירה על השליטה הבלעדית של החותם באמצעי זה, בדומה לשליטתו בחתימה שלו.
- 1.2. בתקנה 8(ג) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001 נקבע כי:

"היתה הפעלת אמצעי החתימה כרוכה בשימוש בסיסמה, תעמוד הסיסמה

בדרישות אבטחה ברמה גבוהה לפי ת"י 1495 חלק 3, או בדרישות חלופיות

שקבע הרשם, אם נוכח כי ניתן לפטור מהדרישה האמורה."

- 1.3. מטרת הדרישה לוודא כי הפעלת אמצעי החתימה והגישה אליו תיעשה רק בידי מי שיש לו ההרשאה לשימוש באמצעי החתימה.
- 1.4. כאשר מדובר על סיסמת גישה לכרטיס חכם או לאמצעי פיזי אחר, דרישות האבטחה לפי ת"י 1495 חלק 3 ברמה הגבוהה עשויות להיות חמורות מדי, ואף לא רלבנטיות, בין השאר משום שהן מתעלמות מכך שהמידע מוגן על גבי אמצעי פיזי המצוי בשליטת בעליו, ולא במערכת מידע רגילה. התוצאה של דרישות חמורות מדי עלולה לפגוע ברמת האבטחה, משום שמשתמשים עלולים לציין לצד האמצעי את ססמת הגישה, או שעלולה להיגרם פגיעה אחרת בשימושיות.

2. רקע

- 2.1. באופן כללי, סיסמאות מורכבות הנאכפות ברמה מערכתית מהוות כלי אפקטיבי למניעת שימוש לא מורשה והתקפות על מידע.

⁴ בהתייחסות ל- "אמצעי חתימה" החוק מכוון למה שמכונה בתשתית מפתח ציבורי "מפתח פרטי", כלומר הסוד השמור על גבי ההתקן הפיזי המשמש לחתימה.

Ministry of Justice
The Israeli Law, Information &
Technology Authority (ILITA)
Certification Authorities
Registrar



מדינת ישראל
State of Israel

משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע
רשם גורמים מאשרים

- 2.2. קיימים ארבעה פרמטרים מקובלים אשר משפיעים על יעילות הסיסמה :
- 2.2.1. אורך הסיסמה (**Length**) - משפיע בצורה ישירה על היכולת של פורץ ללא מידע מוקדם, לפצח את הסיסמה ;
- 2.2.2. מורכבות הסיסמה (**Complexity**) - כגון : שימוש באותיות קטנות או גדולות (באנגלית), או שימוש בסימנים ומספרים בנוסף לאותיות - עשויה להקשות על פריצתה ;
- 2.2.3. הגדרת נעילת הגישה אחרי מספר מוגדר של ניסיונות גישה (**Lock-out**) - כיום קיימים כלים המאפשרים לנחש סיסמאות תוך פרק זמן קצר. לכן, נעילת הגישה הופכת סיסמאות לבטוחות יותר. שימוש בנעילת גישה גם עשויה לפצות במידת מה על מדיניות סיסמאות חלשה ;
- 2.2.4. תפוגת סיסמה (**Retention**) - רצוי להחליף סיסמאות בתדירות גבוהה. תדירות ההחלפה צריכה להיקבע תוך התייחסות ליכולת של משתמשים לזכור את הסיסמאות. תדירות ההחלפה צריכה לכלול מנגנון האוסר על שימוש בסיסמאות קודמות או רצף הגיוני של סיסמאות (סיסמה1, סיסמה2 וכו').
- 2.3. ככלל, שימוש בסיסמאות חזקות ומורכבות אשר אינן ניתנות לפיצוח בזמן סביר, מחזק בצורה משמעותית את ההגנה על המידע. אולם, יש לתת את הדעת לסיכונים הנובעים מכך שסיסמאות חזקות ומורכבות מדי עלולות להביא לרישום גלוי של הסיסמא לצד ההתקן או תקלות אבטחה אחרות, ובנוסף לפגוע בשימושיות של אמצעי החתימה. בהתאם לכך, יש למצוא איזון בין מורכבות וחוזק הסיסמה בפרמטרים אלה מפני תקיפה, למול היבטי שימושיות.
- 2.4. **הוראות מקבילות בעניין גישה לאמצעי חתימה**
- 2.4.1. תקן FIPS 140-2 של מכון התקנים האמריקני (NIST) מגדיר דרישות אבטחה ממודול קריפטולוגיה, מהסוג המשמש גם לאפסון מפתחות פרטיים המשמשים לחתימה אלקטרונית.⁵
- 2.4.2. ביחס לאורך הסיסמה⁶, קובע מכון התקנים האמריקני, כי יש להקטין את הסיכוי לפריצת הסיסמה או ניחוש רנדומאלי לפחות מניסיון אחד מוצלח למיליון ניסיונות (1-1,000,000), וכן שאם נעשה מספר רב של ניסיונות

⁵ <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

⁶ שם, בעמ' 18:

The strength of the authentication mechanism shall conform to the following specifications :

- For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods).
- For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur .
- Feedback of authentication data to an operator shall be obscured during authentication (e.g., no visible display of characters when entering a password) .
- Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism.

להזדהות בפרק זמן של דקה, הסיכוי להצליח באקראי או בשל טעות של המנגנון (False acceptance) לא יעלה על 1 ל - 100,000 ניסיונות.

2.4.3. במסגרת פרויקט התקינה בתחום החתימה האלקטרונית באירופה (EESSI)⁷, נכתב תקן (2004) CWA-14890-1⁸. בהתאם לתקן זה, נדרש אורך סיסמה מינימאלי של 6 תווים ומנגנון נעילה המופעל לאחר 3 ניסיונות. כמו כן, נקבע בתקן כי איפוס סיסמה יעשה באמצעות סיסמת ADMIN באורך של 6 תווים לפחות.

3. הנחיה

3.1. על רקע האמור לעיל, הנחיית הרשם לעניין הדרישות החלופיות לת"י 1495 על פי תקנה 8(ג) הינה:

3.1.1. **אורך סיסמה** - סיסמת הגישה לאמצעי חתימה תהיה באורך של 6 תווים לפחות;

3.1.2. **נעילת סיסמה** - האפשרות להקיש סיסמה תיחסם לאחר 7 ניסיונות כושלים;

3.1.3. **שחרור מנעילה** - ניתן יהיה ליישם שחרור מנעילה באמצעות בדרך של איפוס הסיסמה באחת החלופות הבאות:

3.1.3.1. על ידי סיסמת שחרור [PUK] שתעמוד בדרישות הבאות לפחות:

3.1.3.1.1. הסיסמה ייעודית לאמצעי חתימה זה;

3.1.3.1.2. היא תיוצר או תוגדר במעמד הנפקת אמצעי החתימה ותועבר בצורה שתשמור על סודיותה לבעל אמצעי החתימה;

3.1.3.1.3. הסיסמה לא תהיה בשום מקרה סיסמת ברירת מחדל של ההתקן;

3.1.3.1.4. הסיסמה תהיה באורך 8 תווים לפחות.

3.1.3.2. על ידי מנגנון ייעודי אחר שיאשר הרשם, המבוסס על זיהוי המבקש ותוך מניעת אפשרות גישה לאמצעי החתימה שלו בהליך זה;

3.2. לעניין **מורכבות סיסמה**, מומלץ לבחון יישום דרישות אלה ביחס להתקן:

3.2.1. לאפשר הרכבת הסיסמה משילוב תווים מתוך שתיים מקרב הקבוצות הבאות: אותיות גדולות (Capital Letters) באלף בית הלטיני, אותיות קטנות באלף בית הלטיני, סימנים מיוחדים (למשל %) וספרות;

3.2.2. לאפשר שימוש בסיסמאות ארוכות המאפשרות רישום פראזות-משפטים.

⁷ http://www.icts.org/Working_Groups/EESSI/Index.htm
⁸ <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-01-2004-Mar.pdf>

מידע לגבי ההנחיה

1. מס' ההנחיה: 1/2010
2. נושא ההנחיה: דרישות חלופיות לת"י 1495 להפעלת אמצעי חתימה אלקטרונית
3. תאריך פרסום: 9.3.2010
4. בתוקף מתאריך: 9.3.2010
5. חוקים שאוזכרו:
 - א. חוק חתימה אלקטרונית, התשס"ב-2002.
6. חקיקת משנה שאוזכרה:
 - א. תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001.
7. פסקי דין שאוזכרו: אין.
8. מאמרים שאוזכרו: אין.
9. הנחיות היועץ המשפטי לממשלה שאוזכרו: אין.
10. הנחיות רשם גורמים מאשרים שאוזכרו: אין.
11. מילות מפתח: FIPS 140-2 ; False Acceptance ; EESSI ; CWA-14890-1 ; Complexity ; Retention ; NIST ; Lock-out ; Length ; התקן קריפטוגרפי ; חתימה אלקטרונית ; מורכבות סיסמה ; נעילת סיסמה ; סיסמה ; ת"י 1495 ; תפוגת סיסמה.
12. עדכונים

גרסה	פרטים	תאריך

נספח ב'

הנחית רשם גורמים מאשרים מס' 2-2010

תקן מקובל למערכת ניהול תעודות אלקטרוניות בגורם מאשר

מטרת הנחיה זו היא לקבוע הוראות לעניין תקן מקובל לצורך עמידה בהוראות חוק חתימה אלקטרונית, התשס"א-2001 (להלן - **החוק**) והתקנות מכוחו, לעניין סטנדרט אבטחת המידע והמהימנות הנדרשים ממערכת המשמשת לפעולות חיוניות בגורם מאשר והתקנתה, ולעניין אופן בדיקת העמידה בתקן.

4. רקע

- 1.5. הדרישות לעניין מערכת ניהול תעודות בגורם מאשר קבועות בסעיף 18(ד) לחוק, ולפיהן לצורך ביצוע תפקידי הגורם המאשר המנויים בסעיף 18, ישתמש הגורם המאשר "רק במערכות חומרה ותוכנה מהימנות".
- 1.6. סעיף 24(9) לחוק מסמך את שר המשפטים לקבוע הוראות לעניין סוגי מערכות המקיימות, בין היתר, את דרישות סעיף 18 לחוק.
- 1.7. תקנה 4 לתקנות (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001 (להלן - **התקנות**) קובעת לעניין אמצעי החתימה של הגורם המאשר, כי עליו להיות "מגובה באמצעים מוגנים ומאובטחים, להנחת דעתו של הרשם", וכן כי עליו לעמוד ב"דרישות נוספות שהעמיד הרשם לשם קיום אבטחה ברמה סבירה מפני חדירה, שיבוש או שימוש לרעה".
- 1.8. בתקנה 5(א) לתקנות נקבע, כי "מרכיבי המערכת המשמשים לזיהוי המבקש, להנפקת תעודה אלקטרונית ולביטולה יעמדו ברמת ביטחון של תקן Common Criteria EAL4 או לפי תקן מקובל אחר, המבטיח רמת אבטחה מקבילה, להנחת דעתו של הרשם". לפי תקנה 1 לתקנות, מערכת היא "מערכת החומרה והתוכנה של הגורם המאשר המשמשת לפעילותו כגורם מאשר".
- 1.9. בתקנה 2(8) לתקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב-2001, נקבעה דרישה לעריכת חוות דעת של מבקר לפי כללי ביקורת מקובלים להנחת דעת הרשם, ולפי תקנה 4(4) לתקנות אלה על גורם מאשר להגיש חוות דעת כאמור אחת לשנה.
- 1.10. מכאן שהתקנות מקנות שיקול דעת לרשם להרחיב את בסיס התקינה הקבוע בתקנות ולקבוע את אופן מימושו.

1.11. החוק והתקנות לפיו מיישמים עקרונות דומים להוראות הדירקטיבה האירופית בנושא חתימה אלקטרונית משנת 1999⁹ (להלן - **הדירקטיבה**), הן בעקרונות המהותיים, והן בשיטת ההפניה לתקינה טכנולוגית. בשל כך נבחנו הוראות התקינה החלות על מערכות לניהול גורם מאשר באירופה.

1.12. לצורך מימוש הוראות הדירקטיבה, תואם באמצעות ICT Standards Board (ICTSB), שהוא מיוזם של שלושת מכוני התקינה המוכרים האירופאים¹⁰, פרויקט European Electronic Signature Standardization Initiative¹¹.

1.13. ה- European ICT Standards Board, בתמיכת נציבות האיחוד האירופי, שיתף בעבודת התקינה גורמים ממשלתיים פרטים ומסחריים בעלי ידע בנושא זה. במסגרת זו הוסמכו "ועדת התקינה האירופאית" CENJ - "European Committee for Standardization", ומכון תקינת הטלקומוניקציה האירופאי "European Telecommunications Standards Institute", לבצע את העבודה ולפתח את התקנים המקובלים. לצורך עריכת תקנים אלה נערכו "הסכמי תקינה" CEN Workshop "Agreements (CWA)", שמטרתם לקדם סטנדרטים אלה. קבוצת העבודה העבירה את תחזוקת התקנים והמשך עבודת התקינה בפרויקט זה ל- CEN ו- ETSI.

1.14. ועדת התקינה האירופית¹² פרסמה את תקן CWA 14167-1¹³ (להלן - **התקן או תקן CWA 14167-1**) ואת תקן CWA 14172-3¹⁴ (להלן - **תקן העזר**).

1.10.1 התקן מחלק את המערכת למספר חלקים חיוניים שיש לבחון את תפקודם באופן מנדטורי:

1. שירותי רישום נתונים של מבקש תעודה;
 2. שירותי ייצור וחתימה על תעודה בהתאם לנתונים שנרשמו;
 3. שירותי הפצת תעודה לבעל התעודה ולצדדים מסתמכים;
 4. שירותי ביטול תעודה;
 5. שירותי מסירת מידע על ביטול תעודה.
- 1.10.2 בנוסף, כולל התקן שני פרקים וולונטריים החלים לעניין שירותים נוספים שגורם מאשר יכול לספק, וקובע הוראות ביחס אליהם - שירותי אתחול

⁹ Directive 1999/93/EC of the European Parliament and of the Council of 13 September 1999, on a Community framework for electronic signatures. http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=en

¹⁰ ראה: <http://www.icts.org>

¹¹ ראה באופן כללי על הדירקטיבה ועבודות ועדת התקינה למימושה:

http://www.icts.org/Working_Groups/EESI/Index.htm

¹² European Committee for Standardization. כתובת אתר האינטרנט: www.cen.eu

¹³ CEN Workshop Agreement, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, June 2003.

¹⁴ CEN Workshop Agreement, EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures, March 2004.

והפעלה של התקן המשמש לאמצעי חתימה של משתמש קצה, ושירותי Time-stamp.

1.10.3 התקן נקבע כמסמך בעל תוקף מנחה, בהתאם להוראות סעיף 3(5) לדירקטיבה¹⁵ ורשמים מקבילים מאירופה רואים בו מקור מקצועי לעניין הסטנדרט הנדרש ממערכת המנהלת את התעודות, לענין התקנתה בגורם מאשר.

1.10.4 תקן העזר קובע את הדרישות מגורם שמבצע בדיקות אבטחה לפי התקן. דרישות אלה כוללות הוראות בעניין דרישות מקצועיות, אי תלות והתנהלות אתית¹⁶. בנוסף, קובע תקן העזר את השיטה לפיה המבקר צריך לפעול, תוך הסתמכות על מידע נתונים ומסמכים אודות הרכיבים הרלוונטיים, ואופן תיעוד הבדיקות לצורך בקרה על ידי צדדים שלישיים, ובכלל זה הרשם.

1.15. התקן ותקן העזר לבדיקתו מהווים סטנדרט ברור ליישום מעטפת האבטחה בארגון המסוים בו מוטמעת המערכת. התקן מבהיר לגורם המאשר את אופן העמידה בהוראות החוק, תוך הותרת גמישות תפעולית לגורם המאשר.

1.16. ככלי רגולטורי התקן והכללים הקבועים בתקן העזר מאפשרים הרחבת היצע המערכות שניתן להשתמש בהן לגורם מאשר מבלי לפגוע ברמת האבטחה של המערכת. התקן מאפשר למקד את פיקוח הרשם בהיבטים המהותיים של המערכת. על רקע האמור יש צורך בהרחבת בסיס התקינה בהתאם לדגם האירופאי.

5. הנחייה זו פורסמה כטיזטה להערות הציבור ביום 22.02.2010, הועברה לגורם המאשר ולגורמים נוספים, ולא התקבלו ביחס אליה כל הערות.

6. הנחייה

6.1. בהתאם לאמור לעיל, הנחיית רשם גורמים מאשרים הינה כדלקמן:

6.1.1. תקן CWA 14167-1 יחול לצורך הוכחת עמידת גורם מאשר בדרישות החוק והתקנות לפיו, ולעניין סטנדרט אבטחת המידע והמהימנות הנדרשים לניהולה ולהפעלתה של מערכת המשמשת לפעולות חיוניות בגורם מאשר, בהתאם לתקנות 4 ו-5.

6.1.2. תקן העזר יחול לעניין אופן הוכחת עמידה בתקן, בין היתר בשים לב לתקנה (8)2 לתקנות חתימה אלקטרונית (רישום גורם מאשר וניהול), התשס"ב-2001, ועל פי הוראותיה. על עורך חוות הדעת לפי התקן לפרט, בהתאם לתקן

¹⁵ ראה: Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognized standard for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council (notified under document number C(2003) 2439).

להשלמה יצוין, כי באותה החלטה נקבע גם תקן CWA 14167-2, המסדיר את פרופיל ההגנה (protection profile), של הסטנדרט שנקבע במסמך זה הוא פרופיל הגנה לפי תקן common criteria. עם זאת תקן זה עבר שינויים ולאחר מכן שונה לשני תקנים נפרדים: CWA 14167-2 ו-CWA 14167-4.

¹⁶ ראה שם, סעיף 3.5, עמ' 11-12.

העזר, נתונים מזהים אודות המערכת ורכיביה, הבדיקות שבוצעו על ידו ונתונים נוספים ככל שנדרש לצורך הבנה והערכה של חוות הדעת.

6.2. יישום התקן בישראל ייעשה בשינויים המחויבים הנובעים מהוראות דין מקומיות, ובמרכזן הוראות החוק, התקנות מכוחו, תקנים ישראלים, הוראות אחרות של הרשם והוראות מקבילות הרלבנטיות למימוש החתימה האלקטרונית בדברי חקיקה מקבילים. רשימה של הסתייגויות מופיעה בנספח להנחיה זו.

6.3. לצורך הוכחת עמידה בתקן על הבודק או צוות הבדיקה לעמוד בהוראות תקן העזר, בדגשים הבאים:

6.3.1. ניסיון מעשי בתחום ה-PKI להנחת דעת הרשם.

6.3.2. התחייבות להעדר ניגוד עניינים, עבודה על פי כללי ביקורת מקובלים, ויישום הנחיות התקן.

6.4. מאחר שהבדיקה היא פונקציונאלית, מקום בו נבחנו רכיבים של המערכת לפי תקן Common Criteria, ניתן יהיה להסתפק בבדיקה מפורטת פחות, לעניין בחינת היבטים תפעוליים של רכיבים אלה, תוך וידוא כי נעשה שימוש ברכיבים בהתאם לדרישות והתנאים המקדמים המוגדרים בתקינה.

6.5. במקום שבו מדובר ברכיבים או חלקים פונקציונאליים שפותחו באופן עצמאי על ידי הגורם המאשר או מטעמו או באינטגרציה של רכיבים מוכרים יש צורך בבדיקה טכנית מעמיקה יותר, בהיקף הנגזר מהחשיבות הפונקציונאלית, ותוך תיעוד מפורט של הממשקים בין הרכיבים בגורם המאשר.

6.6. למען הסר ספק, זהות הבודק ואופן עמידתו בהוראות אלה, יובאו לאישור הרשם מראש.

6.7. הנחייה זו תכנס לתוקף עם פרסומה הסופי לאחר הערות. לעניין הגורם המאשר הרשום במועד פרסום הנחייה זו, הנחייה זו תכנס לתוקף תוך 45 יום.

נספח - סייגים לתחולת התקן

1. הסימוכין הנורמטיביים שבסעיף 2.1 לתקן CWA 14167-1, לא יחולו בישראל.
2. מבלי לגרוע מהאמור, להלן סייגים ספציפיים לתחולת התקן:

סעיף בתקן	נושא	במקום	סייג/תחולה חליפית
5.1.5.2 [KM1.2]	דרישות אבטחה מהמודול הקריפטוגרפי	הפנייה ל- [CEN CMCSO-pp]	הפנייה לתקנה 4(2) לתקנות
5.1.5.2 [KM1.7] [KM2.6] [KM6.2]	הוראות בנושא אלגוריתמים	הפנייה ל- "מסמך" ALGO ¹⁷	לפי הנחית הרשם 4-2010 בנושא אלגוריתמים
5.1.5.2 [KM3.4]	מגבלות על שימוש במפתחות ומבנה תעודה	האמור בסעיף	על פי האמור בתקינה ישראלית, ולא יחול על תעודות המונפקות לפי חוק ניירות ערך, התשכ"ח-1968
5.1.8 [BK2.2]	הצפנה של מידע קריטי	הפנייה ל- "מסמך" ALGO	שימוש בתקן מקובל
5.2.2 [R 1.3]	איסוף מידע הנדרש בדירקטיבה האירופית להנפקת תעודה	הפנייה לדירקטיבה האירופית	בהתאם לדין הישראלי [החוק, תקנות והוראות דין ספיציפיות כגון חוק ניירות ערך, התשכ"ח-1968].
5.2.3.2 1, [CG1.6]	תוכן שדה "שם" בתעודה	"or pseudonym"	ימחק
5.2.3.2 6, [CG1.6]	הוראות בעניין אלגוריתמים לחתימה	הפנייה ל- "מסמך" ALGO	לפי הנחיית הרשם 4-2010 בנושא אלגוריתמים
5.2.3.2 [CG1.6]	מבנה תעודה	האמור בסעיף	לפי תקן ישראלי
5.2.5.2	עדכון רשימת תעודות בטלות	האמור בסעיף	לפי תקנה 15 והנחיות הרשם לפיה או לפי הוראות או הנחיות לפי חוק ניירות ערך, (במידת התשכ"ח-1968) הרלבנטיות) או לפי הוראות לפי דין אחרות
5.2.6.2	הוראות בנושא אלגוריתמים	הפנייה ל- "מסמך" ALGO	לפי הנחייה 4-2010 בנושא אלגוריתמים

¹⁷ ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.

מידע לגבי ההנחיה

13. מס' ההנחיה: 2/2010
14. נושא ההנחיה: תקן מקובל למערכת ניהול תעודות אלקטרוניות בגורם מאשר
15. תאריך פרסום: 12.10.2010
16. בתוקף מתאריך: 24.11.2010
17. חוקים שאוזכרו:
- א. חוק חתימה אלקטרונית, התשס"ב-2002.
18. חקיקת משנה שאוזכרה:
- א. תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001.
- ב. תקנות חתימה אלקטרונית (רישום גורם מאשר וניהול), התשס"ב-2001.
19. פסקי דין שאוזכרו: אין.
20. מאמרים שאוזכרו: אין.
21. הנחיות היועץ המשפטי לממשלה שאוזכרו: אין.
22. הנחיות רשם גורמים מאשרים שאוזכרו: 4-2010.
23. מילות מפתח: EAL4 common criteria, CWA 14167-1, CWA 14172-3, אבטחת מידע, אמצעי חתימה, גורם מאשר, גיבוי, הנפקת תעודה אלקטרונית, זיהוי, חתימה אלקטרונית, מבקר מערכות, מהימנות, מערכת ניהול תעודות, תקן.
24. עדכונים

גרסה	פרטים	תאריך

נספח ג'

הנחית רשם גורמים מאשרים מס' 4/2010

עדכון אלגוריתמים ואורכי מפתחות לשימוש לפי חוק חתימה אלקטרונית,

התשס"א-2001

7. כללי

- 1.17. חוק חתימה אלקטרונית, התשס"א-2001 (להלן - **החוק**) מגדיר מהי "חתימה" בעולם האלקטרוני ומסדיר את התוצאות המשפטיות של השימוש בה. בתקנות לפי החוק נקבעו הוראות מפורטות יותר.
- 1.18. המימוש המקובל כיום של חתימה אלקטרונית, הינו על בסיס "הצפנה אסימטרית", הידועה גם בשם הצפנת מפתח ציבורי.
- 1.19. חוק החתימה תלוי בחוק ההצפנה, ובהתאם לכך נקבעו הוראות לפי החוק בנושא זה.
- 1.20. במסגרת הצורך לבדוק מעת לעת את תנאי הסף הנדרשים להצפנה זו, על מנת למנוע זיוף או שבירת חתימה, רשם גורמים מאשרים ביקש את חוות דעתו של ד"ר בני פנקס, מומחה ישראלי להצפנה (להלן - **חוות הדעת**), בהתבסס על תקנים מקובלים.
- 1.21. חוות הדעת הצביעה על הצורך בקביעת פרמטרים לפונקציות הצפנה, לפונקציות גיבוב, ולשיטות ריפוד של החתימה, הכל כפי שפורט בחוות הדעת. חוות הדעת פורסמה להערות הציבור, ונערך דיון בנושא זה במשרד המשפטים בספטמבר 2009.
- 1.22. בעקבות הערות הציבור שהתקבלו לגבי חוות הדעת, הדיון בנושא שנערך במשרדי הרשות למשפט טכנולוגיה ומידע, וכן עדכונים נוספים בתחום זה, גובש הנוסח הסופי לחוות הדעת המצורף כנספח להנחיה זו.

8. הנחיה

בהתאם לנוסח הסופי של חוות הדעת, הנחיית הרשם לעניין עדכון אלגוריתמים ואורכי מפתחות לשימוש לפי החוק הינה כמפורט להלן:

8.1 שיטות גיבוב (HASH)

שיטה	אורך פלט	תוקף
SHA-1	160	עד 1.4.2011
RIPEMD-160	160	עד סוף שנת 2012
SHA-224 עם פלט מקוצר ל-160 סיביות	160	עד סוף שנת 2012
SHA-224	224	ללא הגבלה
SHA-256	256	ללא הגבלה
SHA-384	384	ללא הגבלה
SHA-512	512	ללא הגבלה
Whirlpool	512	ללא הגבלה

8.2 שיטות ריפוד (Padding) מקובלות

שיטה	מקור
RSASSA-PKCS1-v1.5	FIPS 186-3 (דומה למסמך PKCS #1 v2.1 ולמסמך ETSI)
RSASSA-PSS	FIPS 186-3 (דומה למסמך PKCS #1 v2.1 ולמסמך ETSI)

8.3 שיטות חתימה ואורכי מפתחות

שיטה	אורך מפתחות	תוקף
RSA	1024	עד 1.4.2011 ורק לחתימות שהן בעלות ערך עד סוף שנת 2016
RSA	2048 סיביות או יותר	ללא הגבלה
RSA	4096 סיביות או יותר	יש להתכונן למעבר לאורכי מפתחות אלו
DSA	(L=1024,N=160)	עד 1.4.2011 ורק לחתימות שהן בעלות ערך עד סוף שנת 2016
DSA	(L=2048,N=224) (L=2048,N=256) (L=3072,N=256)	ללא הגבלה
ECDSA מעל $E(F_p)$	160	עד 1.4.2011 ורק לחתימות שהן בעלות ערך עד סוף שנת 2016
ECDSA מעל $E(F_{2^m})$	224 או יותר	ללא הגבלה

נספח

בחינת אלגוריתמים לפי חוק חתימה אלקטרונית

ד"ר בני פנקס

חבר סגל, המחלקה למדעי המחשב, אוניברסיטת חיפה

תל אביב, יוני 2010

נתבקשתי על ידי רשם גורמים מאשרים במשרד המשפטים, לחוות דעתי המקצועית בשאלות המקצועיות המפורטות מטה. אני מצהיר בזאת כי ידוע לי היטב, שלעניין הוראות החוק הפלילי בדבר עדות שקר בשבועה בבית המשפט, דין חוות דעתי זו כשהיא חתומה על ידי כדין עדות בשבועה שנתתי בבית המשפט. אין לי עניין אישי כלשהו בהמלצות הנדונות בחוות הדעת, פרט לכך שאני חוקר בתחום ההצפנה. ואלה פרטי השכלתי:

- דוקטורט (PhD) במדעי המחשב, מכון וייצמן, שנת 2000.
- תואר שני (MSc) במדעי המחשב, הטכניון, שנת 1991.
- תואר ראשון (BA) במדעי המחשב, הטכניון, שנת 1987.

ואלה פרטי ניסיוני:

- הנני חבר סגל, בדרגת מרצה בכיר, במחלקה למדעי המחשב באוניברסיטת חיפה, החל מחודש אוקטובר 2005. בתפקיד זה אני מלמד בצורה קבועה קורסים בנושאי הצפנה ואבטחת מחשבים.
- פרסמתי יותר מ-45 מאמרים אקדמיים בתחום הקריפטוגרפיה, בכנסים ועיתונים מדעיים אשר מקבלים לפרסום רק אחוז קטן מהמאמרים הנשלחים אליהם. מאמרי הראשון בתחום פורסם בשנת 1990.
- אני משתתף באופן פעיל בוועדות שיפוט של מאמרים הנשלחים לכנסים ועיתונים מדעיים בנושאי קריפטוגרפיה.
- הנני רשום כממציא של 7 פטנטים, ו-13 בקשות פטנט, בנושאי הצפנה.

חוות דעתי מפורטת בהמשך מסמך זה.

1 חתימה אלקטרונית - מבוא:

1.1 הבסיס המתמטי

הבסיס המתמטי לביצוע חתימה אלקטרונית מתבסס על שימוש בפונקציה הנקראת "פונקציה חתימה אסימטרית", בעלת התכונות הבאות:

- הפונקציה מוגדרת על ידי פרמטר סודי, אשר יכונה "מפתח חתימה", או "מפתח פרטי". אם נסמן את מפתח החתימה בסימן SK , נסמן את פלט הפונקציה על הקלט כלשהו X בצורה $F(SK, X)$ ¹⁸.
- קיים פרמטר פומבי, אשר יכונה "מפתח וידוא חתימה" או "מפתח ציבורי", או "מפתח פומבי". אין צורך לשמור ערך זה בסוד. נסמן את מפתח וידוא החתימה בסימן PK . אף אם ידוע ערך מפתח וידוא החתימה, לא ניתן לחשב בצורה יעילה את מפתח החתימה הסודי.
- בהינתן הערך X וערך Y האמור להיות שווה ל- $F(SK, X)$ (חתימה על X), ובהינתן מפתח וידוא החתימה PK , קל לבדוק האם $Y = F(SK, X)$. (כלומר, לוודא שהחתימה על X נכונה).
- ללא ידיעת SK קשה לחשב את $F(SK, X)$ לכל ערך X שהוא וזאת אף אם ידוע ערך המפתח הפומבי PK .

בהינתן פונקציה F המקיימת תכונות אלו, נרצה לבנות מערכת חתימה אשר מבטיחה כי ללא ידיעת מפתח החתימה הסודי SK , לא ניתן לייצר חתימה חדשה. ביתר דיוק, מתקיימת התכונה הבאה:

- 0 יתכן והתוקף יודע את מפתח וידוא החתימה PK .
- 0 יתכן והתוקף יודע גם מספר חתימות על ערכים כלשהם, אשר אולי אף נבחרו בידי התוקף.
- 0 למרות מידע זה אין התוקף יכול לחשב חתימה על אף ערך נוסף.

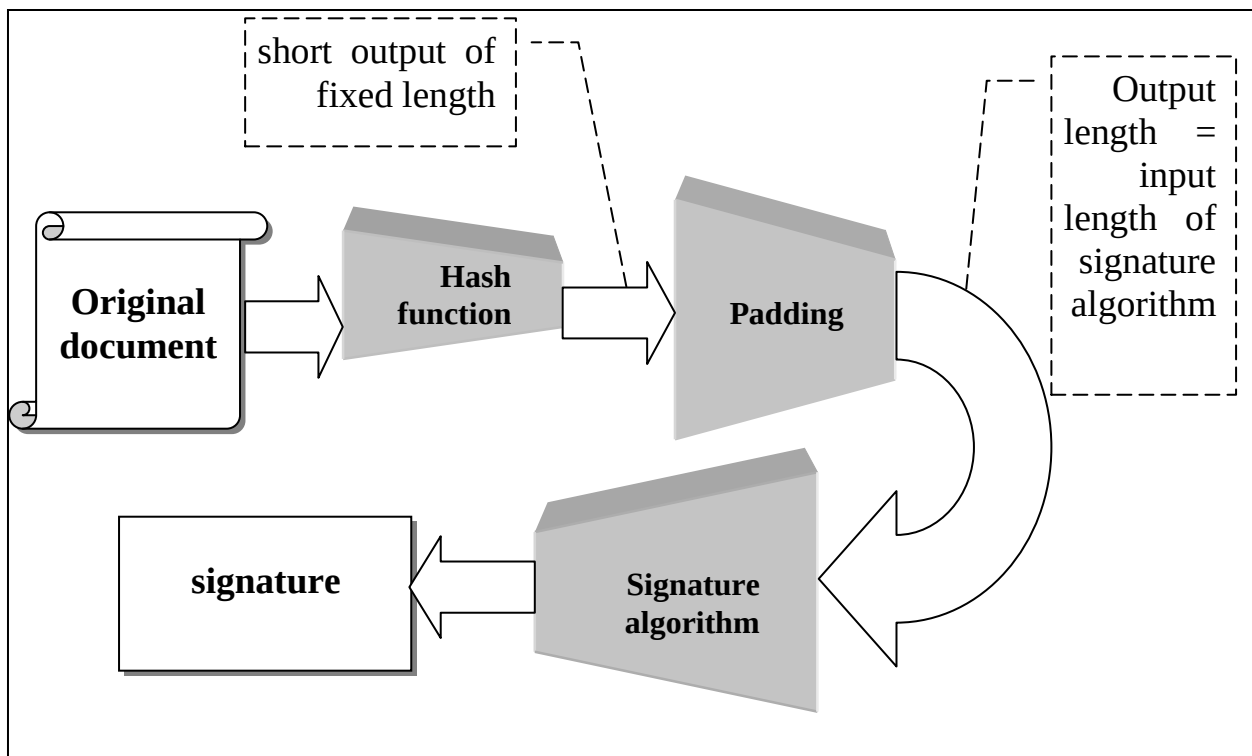
¹⁸ יתכן והפונקציה F תהיה רנדומית, כלומר, חישוב F יהיה תלוי בערכים אקראיים שנבחרים בזמן חישוב הפונקציה. משמעות הדבר שבפעמים שונות בהן יחושב ערך זה, נקבל פלטים שונים של הפונקציה. (תכונה זו מתקיימת במספר סוגי חתימות, לדוגמה DSA). לענייננו אין הדבר עקרוני.

1.2 מרכיבי מערכת לחתימה אלקטרונית

מערכת לחתימה אלקטרונית מורכבת משלושה מרכיבים:

- שיטת גיבוב (hash), אשר מטרתה לתרגם קלט באורך כלשהו לפלט באורך קבוע (לדוגמא, פלט באורך 256 סיביות). שיטות גיבוב ידועות הן, לדוגמא, הפונקציות ממשפחת SHA.
- שיטת ריפוד (padding), אשר מקבלת קלט באורך כלשהו, קצר מפרמטר מסוים (לדוגמא, קצר מ-2048 סיביות), ומטרתה לרפד את הקלט במידע נוסף כך שאורכם הכולל יהיה זהה לערך הפרמטר. שיטות ריפוד ידועות מוגדרות, לדוגמא, בתקן PKCS V2.1.
- שיטת חתימה (signature), אשר מחשבת חתימה אלקטרונית¹⁹. לשיטה זו פרמטרים המגדירים לרוב את אורך ההודעה הנחתמת, ואת אורך וצורת יצור מפתח החתימה ומפתח וידוא החתימה. שיטת חתימה ידועה היא, לדוגמא, שיטת RSA עם מפתח וידוא חתימה באורך 2048 סיביות.

השימוש המקובל במערכות לחתימה אלקטרונית משתמש בשלושת מרכיבי המערכת: ראשית, מופעלת שיטת הגיבוב על ההודעה עליה יש לחתום, ומתקבל פלט באורך קבוע. לאחר מכן, מרופד ערך זה על ידי שיטת הריפוד, כך שאורכו יהיה זהה לאורך הקלט הדרוש לשיטת החתימה. לבסוף, מחושבת חתימה על הערך המרופד. תהליך זה מתואר בתרשים 1.



תרשים 1: מרכיבי מערכת חתימה, והשימוש בהם.

חולשה בכל אחד ממרכיבי מערכת החתימה פוגעת בבטיחות החתימה:

¹⁹ זוהי הפונקציה F אשר תוארה בסעיף 2.1 למעלה, אשר משתמשת במפתח חתימה פרטי ובמפתח וידוא חתימה ציבורי.

- חולשה בשיטת הגיבוב יכולה לפגוע בבטיחות החתימה בצורות הבאות:

- 0 על שיטת הגיבוב לקיים את תכונת **2nd preimage resistance**: כלומר, עבור שיטת גיבוב הממומשת בפונקציה $H()$, צריך להתקיים שבהינתן קלט m והערך $H(m)$, אזי אין דרך יעילה לחישוב קלט m' שונה מ- m , כך שמתקיים $H(m)=H(m')$. אם תכונה זו אינה מתקיימת אזי בהינתן חתימה על ערך m שחושבה בשיטה שתוארה למעלה (כלומר, הפעלת שיטת הגיבוב H על m ואח"כ המשך חישוב החתימה), קל למצוא ערך m' אשר החתימה תקיפה גם לגביו.
- 0 על שיטת הגיבוב לקיים את תכונת **collision resistance**: כלומר, צריך להתקיים שאין דרך יעילה לחישוב שני ערכים m, m' השונים זה מזה ואשר מקיימים $H(m)=H(m')$. אם תכונה זו אינה מתקיימת אזי ניתן למצוא שני ערכים כאלו m, m' , ולבקש חתימה על הערך m , כאשר חתימה זו תהווה גם חתימה על הערך m' .²⁰
- 0 בנוסף, על שיטת הגיבוב להיות עמידה גם ל-**near collision resistance**. כלומר, דרוש שיהיה בלתי אפשרי למצוא שתי הודעות כך שרוב הסיביות של פלט פונקציית הגיבוב זהות עבורן. (שבירת תכונה זו תהיה שימושית ליריב אם האפליקציה המשתמשת בפונקציית הגיבוב מקצצת חלק מסיביות הפלט של הפונקציה. במקרה זה ה-"כמעט התנגשות" עלולה להפוך להתנגשות ממש).

- חולשה בשיטת הריפוד יכולה לאפשר התקפות בהן ניתן ללמוד את מפתח החתימה הסודי או לזייף חתימות על הודעות אשר לא נחתמו על ידי החותם המאושר.
- חולשה בשיטת החתימה יכולה לחשוף את מפתח החתימה הסודי, או לאפשר זיוף חתימה על הודעות שעליהן לא חתם בעל מפתח החתימה.

2 שיטות גיבוב (hash)

2.1 חולשות של שיטות גיבוב ומשמעותן לגבי חתימות אלקטרוניות.

כאמור, שיטת גיבוב H חייבת לקיים את תכונת ה- **2nd preimage resistance** (כך שבהינתן קלט m והערך $H(m)$, אזי אין דרך יעילה לחישוב קלט m' שונה מ- m , כך שמתקיים $H(m)=H(m')$), ואת תכונת ה- **collision resistance** (כלומר, שאין דרך יעילה לחישוב שני ערכים m, m' השונים זה מזה ואשר מקיימים $H(m)=H(m')$).

²⁰ במסמך ETSI ובספרות מתוארת דרישת בטיחות נוספת בשם **preimage resistance**, אשר דורשת שבהינתן הערך $H(m)$ יהיה בלתי אפשרי למצוא בצורה יעילה כל ערך m' שהוא, אפילו $m=m'$, המקיים את התכונה $H(m')=H(m)$ את הערך m . ההבדל בין תכונה זו ובין **2nd preimage resistance** הוא שהתקפה אשר בהינתן $H(m)$ מוצאת את m , תיחשב כפגיעה בתכונת ה- **preimage resistance** אך לא בתכונת ה- **2nd preimage resistance**. לעניינינו תכונת ה- **preimage resistance** אינה רלוונטית, משום שאין צורך לשמור את ההודעה הנחתמת בסוד.

ידוע שקל יותר לתקוף את תכונת ה-collision resistance מאשר את תכונת ה- 2^{nd} preimage resistance.

- בפרט, קל לראות שאם תוקף מצליח להביס את תכונת ה- 2^{nd} preimage resistance אזי ביכולתו לשבור את תכונת ה-collision resistance.

- אכן, התקיפות הידועות כנגד שיטת MD5, והרעיונות הקיימים לתקיפת SHA-1, משפיעים רק על ה-collision resistance ולא על תכונת ה- 2^{nd} preimage resistance. ידוע שהתקפות גנריות, אשר ניתן להפעיל על כל פונקצית גיבוב שהיא, ופועלות על ידי חישוב H פעמים רבות עד לשבירת התכונה, יעילות יותר כנגד collision resistance. ביתר פרוט, אם אורך הפלט של H הינו n סיביות, אזי התקפה גנרית על תכונת ה-collision resistance תדרוש כ- $2^{n/2}$ חישובים של H, בעוד שהתקפה על תכונת ה- 2^{nd} preimage resistance תדרוש כ- 2^n חישובים של H.²¹ (אם יש יותר ממטרה אחת להתקפה אזי ההתקפה תהיה יעילה יותר²²).

2.2 התקפות ידועות על שיטות גיבוב

- ידועה התקפה יעילה המוצאת התנגשויות בפלט של פונקצית הגיבוב MD5. כמו כן, מתבצע מאמץ רב למצוא התנגשויות בפלט של שיטת הגיבוב SHA-1 וההערכה היא כי התנגשויות כאלו ימצאו בקרוב. **עקב כך, אין להניח כי פונקציות אלו מקיימות את תכונת ה-collision resistance.**

- לא ידועות התקפות יעילות על תכונת ה- 2^{nd} preimage resistance של MD5 או SHA-1, או של כל פונקציה אחרת אשר נמצאת היום בשימוש נרחב. יחד עם זאת, ידועות תקיפות 2^{nd} preimage כנגד MD4 (שהינו וריאנט קדום של MD5) וכנגד הודעות חלשות ב-MD5.
- בנוסף להתקפות ספציפיות כנגד פונקציות גיבוב מסוימות, יש לקחת בחשבון גם התקפות גנריות אשר פועלות על ידי חישוב הפונקציה פעמים רבות עד אשר נמצאת התנגשות הפלטים הדרושה. היעילות של התקפות אלו תלויה אך ורק באורך הפלט של פונקצית הגיבוב, ולא בפעולות המתמטיות המתבצעות לשם חישוב הפונקציה. ההערכה המקובלת היא שבהשקעה של עשרות מיליוני דולרים ניתן יהיה בשנים הקרובות, בשיטות גנריות, למצוא התנגשויות של פונקציות שאורך הפלט שלהן הוא כ-160 סיביות, ולתקוף את תכונת ה- 2^{nd} preimage resistance של פונקציות שאורך הפלט שלהן הוא כ-100 סיביות.²³ ראו דיון בסעיף 3.4 למטה.

²¹ ראו "Design principles for hash functions revisited", Bart Preneel, October 2005.

http://csrc.nist.gov/groups/ST/hash/documents/preneel_nist_v2.pdf

²² ראו תיאור ב-, P.C. van Oorschot, Parallel collision search with cryptanalytic applications.

M.J. Wiener, 1996, ובמסמך Design principles for hash functions revisited המצוטט למעלה.

²³ ראו תיאור במסמך Design principles for hash functions revisited המצוטט למעלה.

- התקפות על תכונת ה-collision resistance מוצאות שתי הודעות כלשהן, לאו דווקא הודעות בעלות משמעות, אשר פלט פונקציית הגיבוב עבורן שווה. לכאורה אין בכך סכנה משום שסביר שהתוקף לא יפיק תועלת ממצאת התנגשות של ערכי הודעות מסוג זה. אולם, הודגם בעבר שהמצב אינו כזה:

0 לגבי MD5 הודגם שהתנגשות של כל זוג הודעות ניתנת לתרגום להתנגשות של כל זוג מסמכי postscript, לפי בחירת התוקף²⁴. התקפה זו ניתנת לשימוש מיידי עם כל פונקציית גיבוב אשר ידועה לגביה התנגשות של זוג הודעות כלשהן.

0 בצורה דומה, במקום לייצר מסמכי postscript ניתן, בהינתן התנגשות של ערכים כלשהם, ליצור זוג תכניות מחשב, אשר לכל אחת מהן פונקציונאליות כלשהי לפי בחירת התוקף, ואשר פלט פונקציית הגיבוב המופעלת עליהן זהה. כלומר, זוג תכניות מחשב P1 ו-P2, המבצעות חישובים שונים הניתנים לבחירה על ידי התוקף, ואשר מקיימות $H(P1)=H(P2)$.

0 הודגם (כמתואר למטה) שניתן לשפר את שיטת מציאת ההתנגשויות של פונקציית MD5 כך שאפשר יהיה למצוא התנגשויות של הודעות המתאימות לפורמט של certificates. בצורה דומה, יתכן ושיטה שתימצא למציאת התנגשויות כלשהן בפונקציית גיבוב מסוימת, תהיה ניתנת לשיפור כך שאפשר יהיה למצוא התנגשויות בפורמט המתאים להודעות בעלות ערך לתוקף

- כאמור, לאחרונה תוארה התקפה כנגד CA אשר השתמש בפונקציית הגיבוב MD5. התקפה זו מאפשרת ליצור תעודות אלקטרוניות (certificates) לכל אתר אינטרנט שהוא, כולל אתרים שלא השתמשו בשירותיו של CA זה. התקפה זו מתוארת בנספח. המסקנה מהתקפה זו היא שניתן לעיתים להפוך חולשות מזעריות בשיטות הקריפטוגרפיות להתקפות של ממש על אפליקציות. לכן יש להימנע שכל שימוש בשיטות חתימה או גיבוב אשר קיים חשש כלשהו לגבי בטיחותן.

2.3 משמעות ההתקפות עבור מערכות חתימה

2.3.1 זמן וצורת ההתקפה

קיים הבדל בשימוש שתוקף של מערכת חתימה המשתמשת בשיטת גיבוב H יכול לעשות בכל אחד מסוגי החולשות:

- אם ביכולת התוקף לתקוף את תכונת ה-preimage resistance 2^{nd} אזי בהינתן חתימה על מסמך מסוים הוא יכול לייצר חתימה על מסמך אחר. בפרט, התוקף יכול לבחון חתימה S על מסמך m שנבחר על ידי גוף אחר (שונה מהתוקף), ואשר נחתמה בעבר. כעת, אם התוקף מוצא מסמך שונה m' המקיים $H(m)=H(m')$, הרי שהחתימה S היא גם חתימה על m' .

²⁴ <http://th.informatik.uni-mannheim.de/People/lucks/HashCollisions/>

- אם ביכולת התוקף לתקוף רק את תכונת ה-collision resistance אזי עליו למצוא מראש שני מסמכים m, m' , כך שמתקיים $H(m) = H(m')$, על התוקף להשיג חתימה על המסמך m (כלומר, התוקף חייב לשכנע את החותם לחתום על מסמך שנבחר על ידי התוקף), ואילו התוכן של m' צריך להיות בעל ערך רב לתוקף. כעת יכול החותם להציג את החתימה על m כאילו היא חתימה על המסמך m' .
- ההבדלים העיקריים בין שני סוגי התקיפות הוא שההתקפה מהסוג השני דורשת מהתוקף לדעת מראש, לפני שהחותם מחשב את החתימה, את השיטה למציאת התנגשויות ב- $H()$, ואת זוג ההודעות m, m' , וכן על התוקף לשכנע את החותם לחתום על המסמך m . דרישה זו מקשה מאוד על התקפות. כמו כן יש לה משמעות לגבי הגבלת התקופה בה מותר יהיה להשתמש בשיטות הגיבוב. ראה דיון למטה.
- יש שים לב כי לשם ניצול התקפה על תכונת ה-collision resistance על התוקף להיות מסוגל לבחור את ההודעה עליה תתבצע החתימה, או לפחות להיות מסוגל לבחור חלקים משמעותיים ממנה. במימוש המקובל בישראל של תעודה לחתימה אלקטרונית מאושרת (certificates), המפתח הפומבי נוצר על גבי אמצעי חומרה, כרטיס חכם, שבידי הגורם שמבקש לקבל את החתימה, אולם הגורם מבקש החתימה אינו יכול להשפיע על ערך המפתח, ואינו יודע את המפתח הסודי. לכן, בצורת שימוש זו אין ביכולת התוקף לנצל התקפת collision resistance (לשם יצירת תעודה מאושרת, certificate, אשר הינה תקפה לשני מפתחות שונים) כל עוד התוקף אינו יכול לפרוץ את הגנות הכרטיס החכם.
- כאמור, לשם התקפה על תכונת ה-collision resistance על התוקף להיות מסוגל לבחור את ההודעה עליה תתבצע החתימה, או לפחות להיות מסוגל לבחור חלקים משמעותיים ממנה. מומלץ לכן שגורם מאשר (CA) יכניס מחרוזת אקראית אשר איננה ניתנת לחיזוי על ידי אף גורם אחר, לתוך ההודעה עליה הוא מחשב את פונקציית הגיבוב וחותם. יש להכניס מחרוזת זו לפני השדות אשר תוכנם נקבע על ידי הגורם המבקש את החתימה. (המלצה זו נמצאת במסמך ETSI סעיף 5.2.1 הערה 2).
- מכון התקנים האמריקאי (NIST) מקיים תהליך של בחירת פונקציות גיבוב, אשר יקראו SHA-3, אשר יחליפו את שיטות הגיבוב הקיימות. ההחלטה בעניין צפויה להתקבל בשנת 2012. יש לעקוב אחר תהליך זה ולעדכן את ההמלצות בהתאם.

2.3.2 אורך פלט שיטת הגיבוב

כאמור למעלה, ניתן להתקיף, בעלות כספית ניכרת, את תכונת ה-collision resistance של כל שיטת גיבוב שאורך הפלט שלה הוא עד 160 סיביות. לכן לא רצוי להשתמש בשיטות מסוג זה. מאידך, ישנן שיטות חתימה אשר מקבלות קלט שאורכו עד 160 סיביות (לדוגמא, שיטת DSA עם פרמטר q באורך 160 סיביות). לכן, לא רצוי יהיה להשתמש בשיטות חתימה מסוג זה.

2.4 המלצות לגבי שימוש בשיטות גיבוב

ההמלצות הן ברוח ההמלצות באיחוד האירופי²⁵ ובארה"ב²⁶.

ההמלצות:

1. מומלץ לאפשר להשתמש בשיטות הגיבוב הבאות: SHA-224, SHA-256, SHA-384, SHA-512, Whirlpool (אורכי הפלט של שיטות אלו הינם 224, 256, 384, 512 ו-512 סיביות, בהתאמה).²⁷

2. מומלץ שלא לאפשר להשתמש בשיטת הגיבוב MD5.

3. ניתן, אך לא מומלץ, להמשיך את השימוש בשיטת הגיבוב SHA-1, אך זאת רק עד לסוף שנת 2010.

4. אם יש צורך בשיטת גיבוב אשר אורך הפלט שלה הוא 160 סיביות בתאריך מאוחר יותר, אזי ניתן להשתמש בשיטות הבאות וזאת רק עד סוף שנת 2012:

א. להשתמש בשיטת RIPEMD-160, או

ב. להשתמש בשיטת SHA-224 כאשר מקצרים את הפלט המקורי של הפונקציה לפלט באורך 160 סיביות (למשל, על ידי התעלמות מ-64 הסיביות הראשונות (most significant bits) של הפלט של SHA-224).²⁸

5. עקב החולשות האחרונות שהתגלו לגבי SHA-1, מתקיים כיום מחקר ענף בבטיחות של שיטות גיבוב. בפרט, מכון התקנים האמריקאי (NIST) מקיים תהליך אל בחירת פונקצית גיבוב חדשה, SHA-3. יש לעקוב אחר תוצאות מחקר זה ולבחון מחדש את ההמלצות לאחר פרסום המלצות מכון התקנים האמריקאי (NIST) לגבי SHA-3, אשר יחליפו את שיטות הגיבוב הקיימות. ההחלטה בעניין צפויה להתקבל בשנת 2012.

²⁵ ETSI TS 102 176-1 V2.0.0 Electronic signatures and infrastructures (ESI); Algorithms and parameters for secure electronic signatures; Part 1: Hash functions and asymmetric algorithms, November 2007.

²⁶ NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General (Revised), March 2007.

²⁷ לגבי SHA-224, פונקציה זו מחושבת בצורה דומה ל-SHA-256 אך תוך שימוש בערך אתחול (IV) שונה, ובהוספת קיצוץ של הפלט לאורך של 224 סיביות. לכן, אם ניתן להשתמש ב-SHA-256 לא כדאי להשתמש ב-SHA-224. (המלצה זו נמצאת גם במסמך ETSI, סעיף 5.2.3).

²⁸ לכאורה היה ניתן כאן להשתמש בפלט של SHA-256 ולקצצו לאורך של 160 סיביות. הסיבה להמלצה על חישוב וקיצוץ SHA-224 היא מכיוון ששימוש בערכי אתחול זהים בפונקציות שונות יכול לגרום לבעיות בטיחות. ערך האתחול של SHA-224 שונה מזה של SHA-256. כמו כן, צפוי שלא יהיה שימוש נרחב ב-SHA-224 (לעומת השימוש ב-SHA-256). אנו מעדיפים לכן שהפונקציה שאורך הפלט שלה יהיה 160 סיביות, תהיה מבוססת על ערך ה-IV של SHA-224, שלא צפוי לו שימוש אחר נרחב.

נימוקים להמלצות:

1. שיטות הגיבוב הנ"ל אושרו לשימוש במסמך ETSI, סעיף 5.2. לא ידועות התקפות על תכונת ה- 2^{nd} preimage resistance, או תכונה אחרת, של שיטות גיבוב שלו.
2. שיטת MD5 אינה מקיימת את תכונת ה-collision resistance. היא אינה מותרת בשימוש לפי מסמכים עדכניים (ובפרט, מסמך ETSI ומסמך NIST 800-57).
3. ההערכה כיום היא כי התקפות מעשיות על תכונת ה-collision resistance של SHA1 ימצאו בקרוב.²⁹ ההמלצה של הרשות לביטחון תקשורת בקנדה, Communications Security Establishment Canada, היא לסיים את השימוש בשיטת SHA1 עד סוף שנת 2010.³⁰ מסמך NIST 800-57 ממליץ לא להשתמש בפונקציה במערכות חדשות.
4. לא ידועות התקפות יעילות כנגד השיטות אשר מוצעות בסעיף זה, פרט לשיטות התקפה גנריות אשר טובות כנגד כל פונקצית גיבוב אשר הפלט שלה באורך 160 סיביות. התקפות אלו דורשות השקעה רבה ולכן אינן מהוות סיכון מיידי, אולם כדאי לעבור לשימוש בפונקציות אשר אורך הפלט שלהן ארוך מ-160 סיביות בכדי להתגונן מהתקפות אלו.
 - א. ביתר פרוט, העלות של מציאת התנגשות עבור פונקצית גיבוב שאורך הפלט שלה הוא 160 סיביות, היא כ- 2^{80} הפעלות של הפונקציה, תוך שימוש בכ- 2^{80} מילות זיכרון. הודגם גם על ידי Wiener ו-Von Oorschot כיצד ניתן להפעיל אלגוריתם לחיפוש התנגשויות על הרבה מחשבים במקביל, כך שניתן למקבל את זמן החיפוש.³¹ עלינו לבדוק, לכן, מהי ההשקעה הדרושה בכדי לבצע חישוב כזה. התוקף האפשרי הוא גוף אשר ביכולתו להשקיע כסף רב (עשרות מיליוני דולרים) בבניית חומרה ייעודית להתקפה, או אשר ברשותו מחשבים רבים אשר יכולים לעבוד למען ההתקפה (לדוגמא, תוקף אשר שולט ב-bot net המכיל מאות אלפי מחשבים).
 - ב. Preneel טוען, על סמך מאמרם של Wiener ו-Von Oorschot, כי בעלות של 10 מיליוני דולרים היה ניתן ב-2006 למצוא התנגשויות בפלט של שיטת גיבוב שאורך הפלט שלה הוא 160 סיביות.

29

<http://eurocrypt2009rump.cr.yp.to/837a0a8086fa6ca714249409ddfae43d.pdf>,
<http://eprint.iacr.org/2009/259>

³⁰ <http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html>

³¹ Parallel collision search with cryptanalytic applications, P. C. van Oorschot, M.J. Wiener, 1996.

ג. ניראה שעלות החישוב גבוהה יותר. לדוגמא, ניטען³² ב-2005 שניתן בעלות של 10 מיליוני דולרים לבנות מערכת המכילה 303 מחשבים, כ"א מהם עם 16 לוחות המכילים כ"א 32 LSIs, המכילים כ"א 64 ליבות לחישוב SHA-1. כל ליבה מבצעת 2^{25} חישובי SHA-1 בשנייה. כלומר, המערכת מבצעת כ- 2^{48} חישובי SHA-1 בשנייה. לפי חוק מור, ניתן יהיה בסוף 2009 לבנות בעלות זו מערכת אשר תבצע 2^{51} חישובי SHA-1 בשנייה, כלומר כ- 2^{76} חישובים בשנה. לכן העלות (התיאורטית, יש לציין) של ביצוע 2^{80} חישובי SHA-1 תוך שנה היא כ-160 מיליוני דולר. יש לציין שעלות חישוב פונקציה אחרת (שונה מ-SHA-1) אף בעלת פלט באורך דומה) יכולה להיות שונה.

ד. בצורה דומה, תוקף המשתמש במאות אלפי מחשבים (לדוגמא, על ידי הפעלת bot net), יכול גם כן לבצע חישוב בסדר גודל דומה בזמן סביר.

ה. במאמר משנת 2000 של Lenstra ו-Verheul³³ מחושבים אורכי המפתחות אשר יספקו בטיחות שקולה לזו שסיפקה מערכת DES בשנת 1982, וזאת לכל שנה ושנה. חישוב זה מתבסס על ההתקדמות בקצב החישוב והעלות לבניית מערכות חמרה ותכנה. להערכתם, מפתח סימטרי באורך 80 סיביות (אשר שבירתו שקולה לעלות מציאת התנגשויות בפונקצית גיבוב עם פלט באורך 160 סיביות) יהיה שקול בשנת 2012 לבטיחות שנתן DES בשנת 1982. אם אנו מאמינים ש-DES היה בטוח לשימוש מסחרי עד שנת 1997, אזי לשיטתם נוכל להשתמש עד שנת 2027 בפונקצית גיבוב עם פלט באורך 160 סיביות.

ו. מסמך SP 800-57 של NIST משנת 2006 קובע שאורך מפתח סימטרי של 80 סיביות יהיה בטוח לשימוש עד שנת 2010.

ז. מסמך של ECRYPT³⁴ משנת 2009 מתאר את העלויות הבאות להתקפות מסוגים שונים על מפתחות סימטריים (אורך הפלט של פונקצית הגיבוב צריך להיות לפחות כפול). ניתוח מפורט של האנליזה שהביאה למסקנות אלו נמצא בפרק 5 של המסמך.

³² Hardware Architecture and Cost Estimates for Breaking SHA-1, Satoh, A., 2005.

³³ [Selecting Cryptographic Key Sizes](#), Arjen K. Lenstra and Eric R. Verheul, PKC2000: p. 446-465, 01/2000.

³⁴ [Yearly Report on Algorithms and Keysizes \(2007-2008\)](#), D.SPA.7, IST-2007-216676 ECRYPT, 07/2009. <http://www.ecrypt.eu.org/documents/D.SPA.7.pdf>

ח.

תוקף	תקציב	חמרה	אורך מפתח מינימאלי אשר בטוח כנגד ההתקפה
האקר	\$400	PC/FPGA	כ-60
ארגון קטן	\$10K	PC/FPGA	64
ארגון בינוני	\$300K	FPGA/ASIC	68
ארגון גדול	\$10M	FPGA/ASIC	78
ממשלה	\$300M	ASIC	84

ט. לסיכום, לא ברורה העלות המדויקת של התקפה גנרית כנגד פונקציות שאורך הפלט שלהן הוא 160 סיביות, אולם ניראה שהתקפה כזו היא בגדר הסביר בעתיד הנראה לעין ולכן יש לעבור לפונקציות עם פלט באורך גדול יותר.

5. מתקיים כיום מחקר ענף בבטיחות של שיטות גיבוב. יש לעקוב אחר תוצאות מחקר זה.

3 שיטות ריפוד (padding)

מטרת השימוש בשיטות ריפוד היא לגשר בין אורך הפלט של שיטת הגיבוב ואורך הקלט של שיטת החתימה, במצב בו האורך של פלט שיטת הגיבוב קצר מאורך הקלט של שיטת החתימה. מסיבה זו אין צורך להשתמש בשיטות ריפוד יחד עם חתימות לפי אלגוריתם DSA או עם חתימות בשיטת המבוססות על עקומים אליפטיים (elliptic curves), כי בשיטות אלה החתימה מתבצעת על קלט שאורכו כאורך הפלט של שיטות גיבוב ידועות (כלומר, 160, 224, 256 או 512 סיביות). יש צורך להשתמש בשיטות ריפוד בחתימות לפי שיטת RSA, כי במקרה זה אורך הקלט לאלגוריתם החתימה הוא כאורך המפתח הפומבי (כלומר, 1024 סיביות או יותר) והינו ארוך יותר מהפלט של שיטת הגיבוב. שיטות ידועות לריפוד קלט לחתימות RSA מתוארות במסמך PKCS #1 v2.1³⁵ ובתקן ISO 9796. (קיים גם מסמך קודם, PKCS #1 v1.5, אך לא מומלץ לעבוד לפיו כי הוא הוחלף על ידי PKCS #1 v2.1).

המלצה: יש לבצע את הריפוד לפי אחת השיטות המתוארות במסמך FIPS 186-3, סעיף 5.5.

- שיטות אלו הינן שיטת RSASSA-PKCS1-v1.5 ושיטת RSASSA-PSS, לפי מסמך PKCS #1 v2.1, בשינויים קלים המתוארים למטה.³⁶
- שיטות אלו מתוארות גם במסמך ETSI, סעיף 7.2. מסמך ETSI מאפשר גם שימוש בשיטות לפי תקן ISO 9796.
- מסמך FIPS 186-3 דורש את השינויים הקלים הבאים בשיטות:

0 בשימוש בשיטת RSASSA-PSS (מתקן PKCS #1 v2.1), אורך ה-salt, המסומן כ-eLen, חייב להיות קטן או שווה מאורך פלט פונקציית הגיבוב (hash) בה משתמשים.

0 בשימוש בשיטת RSASSA-PKCS-v1.5 (מתקן PKCS #1 v2.1), בזמן וידוא החתימה, יש לחלץ את ערך ה-hash מההודעה החתומה תוך וידוא שמדובר בסיביות הנכונות המכילות ערך זה, כמתואר בסעיף 5.5(f) במסמך FIPS 186-3.

נימוקים להמלצה:

- ההמלצות הן לפי התקנים הבינלאומיים האחרונים. מסמך PKCS #1 v2.1, המלצות ETSI, FIPS 186-3.
- התיקונים במסמך FIPS 186-3 מתקנים נקודות בהן מסמך PKCS #1 v2.1 לא היה חד משמעי, ואשר היו עלולות לגרום לבעיות בטיחות.

³⁵ <http://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf>

³⁶ יש לשים לב כי ישנו דמיון בין המספור של שמות המסמכים ושל שמות שיטות הריפוד המתוארות בהם. המסמך העדכני הוא מסמך PKCS #1 v2.1, משנת 2002, אשר מחליף את מסמך PKCS #1 v1.5. מסמך PKCS #1 v2.1 מתאר את שיטות הריפוד RSASSA-PKCS1-v1.5 ו-RSASSA-PSS.

4 שיטות חתימה (signing)

4.1 הגבלה על מועד שימוש בשיטות חתימה שיש חיש לגבי בטיחותן בעתיד

ישנו הבדל משמעותי באפשרות לביצוע התקפה עקב חולשה בשיטת החתימה, לעומת ביצוע התקפות עקב חולשה בתכונת ה-collision resistance של שיטות גיבוב³⁷. חולשה בתכונת ה-collision resistance של שיטת גיבוב מאפשרת לתוקף לבקש חתימה על מסמך אחד, ולהשתמש בה כחתימה על מסמך אחר. לכן על התוקף להיות מסוגל לבקש ולקבל חתימה על מסמך לאחר שהתגלתה (או לאחר שהתוקף גילה) חולשה בשיטת הגיבוב. חולשה בשיטת חתימה (לדוגמא, מציאת אלגוריתם פירוק מספרים אשר מסוגל לפרק מפתח פומבי של שיטת RSA), מאפשרת לתוקף לזייף חתימות כל עוד ישנה משמעות לחתימות אשר נוצרו בעזרת שיטת החתימה האמורה. זאת אף אם החתימה המקורית נעשתה לפני שהתגלתה חולשה בשיטת החתימה.

נניח לדוגמא שמערכת חתימה משתמשת בשיטת גיבוב מסוימת (לדוגמא SHA-1) ובשיטת חתימה מסוימת (לדוגמא, RSA עם מפתח פומבי באורך 1024 סיביות). הוגדר שניתן לבצע חתימות חדשות במערכת זו עד תאריך X, אך ניתן להציג ולהשתמש בחתימות מסוג זה עד תאריך Y שהינו מאוחר יותר. משמעות הדבר היא שגילוי אפשרות למציאת התנגשויות ב-SHA-1 יועיל לתוקף אם שיטה זו תתגלה לפני תאריך X. לעומת זאת, אם תתגלה לפני תאריך Y שיטה יעילה לפרוק מספרים בני 1024 סיביות, היא תאפשר זיוף חתימות שנעשו בעזרת המערכת (כיוון שהתוקף יכול לבצע את זיוף החתימה עד תאריך Y).

בניסוח אחר, נניח כי אנו מאמינים כי עד תאריך Z לא יתאפשר למצוא התנגשויות ב-SHA-1 או לפרק מספרים בני 1024 סיביות, אך אנו חוששים שלאחר תאריך זה יתכן ותימצא דרך לבצע אחת מהתקפות אלו. כמו כן, אנו מאמינים שבעתיד הנראה לעין לא יהיו התקפות של ממש כנגד אלגוריתם הגיבוב SHA-256 או חתימות RSA עם מפתח באורך 2048 סיביות. ברשותנו מערכת חתימה א' המשתמשת בשיטת הגיבוב SHA-1 ובמפתח RSA באורך 2048 סיביות. ברשותנו גם מערכת חתימה ב' המשתמשת בשיטת הגיבוב SHA-256 ובמפתח RSA באורך 1024 סיביות. בהתאם להנחות נוכל לאפשר ביצוע חתימות במערכת א' עד תאריך Z, ולאסור ביצוע חתימות כאלו אח"כ. השימוש בחתימות ובדיקתן יכולים להתבצע גם בתאריך מאוחר יותר. לעומת זאת, עלינו לאסור כל שימוש במערכת ב' לאחר תאריך Z, כולל איסור האפשרות להשתמש בחתימות שנחתמו בתאריך מוקדם יותר. זאת משום שהחל מתאריך זה יתכן וקיימת האפשרות לזייף חתימות מסוג זה.

4.2 חתימה לפי אלגוריתם RSA

שיטת החתימה לפי אלגוריתם RSA היא השיטה הנפוצה ביותר בשימוש כיום. היא מבוססת על שימוש במפתח חתימה פרטי המורכב משני מספרים ראשוניים p , q , בעלי אורך דומה זה לזה, ומפתח פומבי (הנקרא גם "מפתח ציבורי") $n = p \cdot q$. כמו כן מכיל המפתח הפומבי מספר נוסף (אקספוננט) e , והמפתח הפרטי מכיל מספר (אקספוננט) d .

המלצות לגבי חישוב חתימות לפי שיטת RSA:

חישוב חתימות לפי שיטת RSA חייב להתבצע בצורה הבאה, המקבילה לדרישות במסמך ETSI סעיף 6.1.2.1:

חישוב חתימות חייב להתבצע לפי מסמך RFC 3447³⁸ (אליו מפנה מסמך ETSI), המתאר את תקן PKCS#1 V2.1, בתוספת הדרישות הבאות המפורטות גם הן במסמך ETSI:

³⁷ כל ההתקפות הידועות כיום כנגד שיטות גיבוב אשר הינן בשימוש נרחב, הינן נגד תכונה זו.

- 0 אורכם של המספרים p ו- q צריך להיות דומה, עד להפרש של 30 סיביות (כלומר, מתקיימת התכונה $|\log_2 p - \log_2 q| < 30$).
- 0 המספרים p ו- q צריכים להיבחר באקראי מקבוצת מספרים ראשוניים גדולה (ההסתברות לבחירת ערך מסוים לאחד ממספרים אלו צריכה להיות לכל היותר 2^{-128}).
- 0 אורך האקספוננט d שבמפתח הפרטי חייב להיות קצר מאורך המפתח הפומבי n , אך קרוב מאוד אליו, עד להפרש של 30 סיביות (כלומר, מתקיימת התכונה $\log_2 n - \log_2 d < 30$).

נימוקים להמלצות:

- ההמלצות מקבילות לדרישות במסמך ETSI סעיף 6.1.2.1.
- ההפניה לתקן PKCS #1 V2.1 קיימת גם במסמך FIPS 186-3, סעיף 5.5.
- הדרישות מעבר לתקן PKCS#1 V2.1, המפורטות במפורש כאן (ובמסמך ETSI), ידועות כחיוניות לשם אבטחת החתימה.

³⁸ RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, J. Jonsson, B. Kaliski. February 2003.

4.2.1 אורכי המפתחות

בטיחות מערכת RSA תלויה בכך שלא ניתן לפרק את המפתח הפומבי n ולמצוא את גורמיו הראשוניים p, q המהווים את המפתח הפרטי. ככל שהמפתח הפומבי n הינו ארוך יותר, קשה יותר לבצע את הפירוק. ידוע שניתן לפרק מפתחות RSA באורך של כ-663 סיביות. שיפורים ביכולת הפירוק יכולים להתבצע באחת מהדרכים הבאות:

0 שיפורים ביכולת החישוב: חוק מור טוען שכוח החישוב מוכפל כל שנה וחצי. כמו כן, ישנם שיפורים מתמדיים ביכולת לרתום מספר גדול מאד של מחשבים לעבודה במקביל לפתרון בעיה. שיפורים אלו מביאים לשיפור מתמיד וניתן לחיזוי, אך איטי, ביכולת לפרק מספרים.

0 שיפורים אלגוריתמיים: מידי פעם (אחת למספר ניכר של שנים) מוצאים חוקרים שיפורים משמעותיים באלגוריתמים לפרוק מספרים. שיפורים אלו מביאים לקפיצה ביכולת לפרוק מספרים. לא ניתן לחזות מראש את המועד בו ימצא השיפור הבא, ואת איכות השיפור.

0 קיימות הצעות לבניית חמרה מיוחדת לפרוק מספרים. העלות של בניית חמרה זו היא גבוהה, אולם ביכולתה יהיה לפרק מספרים ביעילות רבה יותר מאשר בידי חמרה סטנדרטית.

מסמך ECRYPT³⁹ משווה בין אורכי מפתחות RSA (וכן מפתחות של מערכות חתימה מבוססות לוגריתם דיסקרטי, כדוגמת DSA המתוארת בהמשך) לבין אורכי מפתחות סימטריים המספקים בטיחות מקבילה. הטבלה היא כדלהלן:

אורך מפתח RSA או DSA	בטיחות (סיביות של מפתח סימטרי שקול)
768	62
1024	73
1536	89
2048	103

אותו מסמך מביא בפרק 6 סקירה של הערכות שונות המשוות בין הקושי של פרוק מספרים לבין הקושי של שבירת מפתח סימטרי באורך 80 סיביות, כלומר לגבי אורך המפתח הפומבי של RSA השקול בבטיחות למפתח סימטרי באורך 80 סיביות. ההערכות הללו נעות בין אורך מפתח פומבי של 1024 סיביות ל-1536 סיביות (ההערכה השנייה היא המחמירה יותר). ציינו למעלה כי מקובל היום להניח שמפתחת סימטרי באורך 80 סיביות נותן בטיחות גבולית כנגד ממשלות, ובטיחות לטווח בינוני כנגד ארגונים בגודל בינוני⁴⁰. לכן מפתחות פומביים באורך 1024 סיביות טובים לשימוש רק לזמן הקרוב ביותר. מפתחות באורך 2048 צפויים לתת בטיחות סבירה לשנים הקרובות. (יחד עם זאת, הבטיחות של מפתחות באורך 2048 סיביות קטנה משמעותית מזו של מפתחות סימטריים באורך 128 סיביות, אשר נחשבים כמפתחות באורך מינימאלי להצפנה סימטרית. לכן יש להתכונן למעבר לשימוש במפתחות ארוכים יותר.)

הערה: כל ההערכות הללו מתבססות על שיפורים בכוח החישוב ואינן לוקחות בחשבון פריצת דרך מחקרית בשיטות לפירוק מספרים. פריצת דרך כזו, אם תהיה, או אם התגלתה כבר אך לא פורסמה בספרות הגלויה, תאפשר פרוק מספרים ארוכים יותר מאלו המצוינים בהערכות.

המלצות לגבי אורך מפתחות RSA:

0 מומלץ להשתמש במפתח פומבי שאורכו 2048 סיביות לפחות.

³⁹ [Yearly Report on Algorithms and Keysizes \(2008-2009\)](http://www.ecrypt.eu.org/documents/D.SPA.7.pdf), D.SPA.7, IST-2007-216676 ECRYPT, 07/2009.

⁴⁰ מומך ECRYPT, טבלה 7.4.

- 0 ניתן להשתמש במפתח פומבי שאורכו 1024 סיביות, אך זאת רק עד לסוף שנת 2010. יחד עם זאת שימוש זה יהיה אפשרי רק לחתימות שהן בעלות ערך עד סוף שנת 2016 וחירות ערך לאחר תאריך זה. (כלומר, אם יתכן ויהיה צורך לבדוק חתימה לאחר סוף שנת 2016, אין לבצע חתימה זו בעזרת מפתח באורך 1024 סיביות).⁴¹
- 0 גורם מאשר חייב להשתמש, החל מסוף שנת 2011, במפתח פומבי שאורכו 4096 סיביות לכל הפחות.
- 0 בשימושים אחרים בעלי חשיבות קריטית (כגון חתימות על ידי גופים במעמד מקביל לגורם מאשר, או חתימות אשר יש חשש שיותקפו על ידי מדינה או ארגון בעל משאבים גדולים) אסור השימוש במפתחות בני 1024 סיביות, ויש לשקול מעבר למפתח פומבי שאורכו 4096 סיביות לכל הפחות.
- 0 יש להתכונן למעבר עתידי של כל הגורמים החותמים לשימוש במפתחות באורך 4096 סיביות.

נימוקים להמלצות לגבי אורך מפתחות RSA:

- מסמכי ETSI או FIPS 186-3 מרשים שימוש במפתח פומבי שאורכו 1024 סיביות, אך לא במפתחות קצרים יותר. לאחרונה הודגם פירוק של מפתח RSA באורך 768 סיביות (משמעות הדבר שבירה של מערכת החתימה התואמת).⁴²
 - ההמלצה של הרשות לביטחון תקשורת בקנדה, Communications Security Establishment Canada, היא לעבור למפתחות RSA באורך 2048 סיביות החל מסוף שנת 2010.⁴³
 - מסמך ECRYPT מאפשר שימוש במפתח באורך 1024 סיביות (סעיף 14.2), אך, כאמור לעיל, טוען שבכדי להשיג בטיחות כנגד ארגונים בסדר גודל רציני יש להשתמש במפתחות ארוכים יותר.
 - הבטיחות של מפתחות באורך 2048 סיביות קטנה משמעותית מזו של מפתחות סימטריים באורך 128 סיביות, אשר נחשבים כמפתחות באורך מינימאלי להצפנה סימטרית. לכן יש להתכונן למעבר לשימוש במפתחות ארוכים יותר.
- לגבי ההמלצה לגבי הגבלת מועד השימוש בחתימה (לעומת הגבלת מועד יצור החתימה), ראו הסבר להגבלה זו בסעיף 4.1.

4.3 חתימה לפי שיטת DSA

שיטת החתימה לפי אלגוריתם DSA פותחה על ידי ממשלת ארה"ב. השיטה מבוססת על הקושי בחישוב לוגריתם דיסקרטי. השיטה משתמשת בפרמטרים פומביים p, q, g אשר יכולים להיות משותפים לחותמים רבים, כאשר p הוא מספר ראשוני ו- q הוא מספר ראשוני קטן מ- p . הפרמטר g הוא יוצר של תת-חבורה מסדר q מודולו p . המפתח הפרטי מכיל גם מספר x בתחום $0 < x < q$, ואילו המפתח הציבורי מכיל את הערך g^x מודולו p .

המלצה:

⁴¹ כיום ברירת המחדל של תוקף מסמכים חתומים היא שבע שנים. מטרתנו היא להגביל את התוקף של מסמכים הנחתמים על ידי מפתחות קצרים לעד שבע שנים מסוף שנת 2009. כמו כן, במידה ובמהלך תקופה זו תתגלה התקפה על חתימות עם מפתחות בארוכים אלו, יהיה צורך לבטל תוקף של חתימות קיימות ולבצע תהליך של חתימה מחדש על מסמכים רלוונטיים.

⁴² <http://eprint.iacr.org/2010/006.pdf>

⁴³ <http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html>

חישוב חתימות לפי שיטת DSA חייב להתבצע בצורה המתוארת במסמך FIPS 186-3.⁴⁴ יש לשים לב לדגשים הבאים:

- **אורכי מפתחות.** נסמן באות L את האורך בסיביות של הפרמטר p , ובאות N את האורך בסיביות של הפרמטר q . ישנם רק ארבעה צרופים מאושרים של אורכי מפתחות: $(L=1024, N=160)$, $(L=2048, N=224)$, $(L=2048, N=256)$, $(L=3072, N=256)$.

0 **המלצה:** ניתן להשתמש במפתח פומבי עם אורכים $(L=1024, N=160)$, אך זאת רק עד לסוף שנת 2010. יחד עם זאת שימוש זה יהיה אפשרי רק לחתימות שהן בעלות ערך עד סוף שנת 2016 וחסרות ערך לאחר תאריך זה. לגבי חתימות בעלות חשיבות קריטית, אשר יש חשש שיותקפו על ידי מדינה או ארגון בעל משאבים גדולים, יש לעבור בהקדם האפשרי למפתח פומבי לפי צירופי האורכים האחרים המאושרים במסמך FIPS 186-3 (כלומר, $(L=2048, N=224)$, $(L=2048, N=256)$, $(L=3072, N=256)$). גורם מאשר המשתמש בחתימות מסוג זה יהיה חייב לעבור עד סוף שנת 2011 לשימוש במפתח פומבי באורכים המתאימים לצרופים אלה. מבחינת בטיחות עדיף כמובן להשתמש בצרופ עם המפתחות הארוכים ביותר האפשריים באילוצי המערכת.⁴⁵

- נשים לב כי N (אורך הפרמטר q) חייב להיות שווה לאורך הפלט של שיטת הגיבוב בה נשתמש. אין צורך בביצוע ריפוד לערך זה, אולם יש לשנותו לייצוג של מספר שלם (integer) בצורה המתוארת במסמך FIPS 186-3.
- אלגוריתם ה-DSA מגדיר כי בכל ביצוע חתימה יש לבחור ולהשתמש בערך אקראי k בתחום $0 < k < q$. יש חובה לבחור ערך זה באקראי עבור כל ביצוע חתימה. ידועות התקפות על בטיחות המערכת אם ערך זה או חלקים ממנו חזרה אינם נבחרים באקראי.

נימוקים להמלצה:

- DSA הינו תקן חתימה אמריקאי, אשר פותח על ידי ממשלת ארה"ב, ויש לעקוב אחר ההמלצות העדכניות של מכון התקנים האמריקאי לגביו.
- אורכי המפתחות תואמים להמלצות של מסמך ECRYPT.

4.4 חתימה לפי שיטות המבוססות על עקומים אליפטיים (elliptic curves)

חתימות המבוססות על עקומים אליפטיים מתבצעות בשיטה דומה לשיטת DSA, אולם בחבורה שונה – כלומר, במקום לבצע חישובים בחבורה מסדר q מודולו p , החישובים מתבצעים בחבורה המוגדרת על ידי עקום אליפטי. היתרון הגדול של ביצוע חתימות על ידי עקומים אליפטיים הוא שאורכי המפתחות והחתימה קצרים יותר, וזמן החישוב יעיל יותר.

המלצה:

⁴⁴ מסמך FIPS 186-3 מתאריך יוני 2009 מחליף את מסמך FIPS 186-2, ונכתב בהתאם להתפתחויות אחרונות בתחום. מסמך ETSI, סעיף 6.1.2.2, אשר נכתב בשנת 2007 (לפני פרסום מסמך FIPS 186-3), מפנה למסמך FIPS 186-2.

⁴⁵ ההמלצה של הרשות לביטחון תקשורת בקנדה, Communications Security Establishment Canada, היא לעבור למפתחות DSA באורך $L=2048$ סיביות החל מסוף שנת 2010. <http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html>

שיטות חתימה המתבססות על עקומים אליפטיים יתבצעו לפי מסמך ETSI, סעיפים 6.1.2.3-6.1.2.6, בשינוי הבא: במקומות בהם מסמך ETSI מסתמך על מסמך FIPS 186-2 יש להסתמך על מסמך FIPS 186-3. ביתר פרוט

- אלגוריתם ECDSA אליפטי מעל שדה מסדר ראשוני $E(F_p)$. זהו אלגוריתם DSA בהתבסס על עקום אליפטי מעל שדה מסדר ראשוני $E(F_p)$. (סעיף 6.1.2.3 במסמך ETSI): הסעיף מאפשר שימוש בעקומים אליפטיים סטנדרטיים המתוארים במסמך FIPS 186-2 ובמסמך brainpool.⁴⁶ מסמכים אלו אפשרו שימוש בעקום אליפטי באורך 160 סיביות. מסמך FIPS 186-3 אינו מאפשר יותר שימוש בעקום בגודל זה, והעקום המינימאלי הוא באורך 224 סיביות.

המלצה: ניתן להשתמש בעקומים אליפטיים באורך 160 סיביות רק עד סוף שנת 2010.⁴⁷ לאחר תאריך זה יש לעבור לשימוש בעקומים אליפטיים סטנדרטיים (לפי מסמך ETSI) באורך גדול מ-160 סיביות. יחד עם זאת שימוש בעקומים אליפטיים באורך 160 סיביות יהיה אפשרי רק לחתימות שהן בעלות ערך עד סוף שנת 2016 וחסרות ערך לאחר תאריך זה. לגבי חתימות בעלות חשיבות קריטית, אשר יש חשש שיותקפו על ידי מדינה או ארגון בעל משאבים גדולים, יש לעבור בהקדם האפשרי לשימוש בעקומים אליפטיים סטנדרטיים (לפי מסמך ETSI) באורך גדול מ-160 סיביות.

0 אלגוריתם ECDSA אליפטי מעל שדה מסדר ראשוני $E(F_{2^m})$. זהו אלגוריתם DSA בהתבסס על עקום אליפטי מעל שדה בינארי $E(F_{2^m})$. (סעיף 6.1.2.4 במסמך ETSI): הסעיף מאפשר שימוש בעקומים אליפטיים סטנדרטיים המתוארים במסמך FIPS 186-2. המלצה: יש לעבוד עם העקומים האליפטיים המוגדרים במסמך FIPS 186-3. ניתן להשתמש בעקומים אליפטיים באורך 160 סיביות רק עד סוף שנת 2010. לאחר תאריך זה יש לעבור לשימוש בעקומים אליפטיים סטנדרטיים (לפי מסמך FIPS 186-3) באורך גדול מ-160 סיביות. יחד עם זאת שימוש בעקומים אליפטיים באורך 160 סיביות יהיה אפשרי רק לחתימות שהן בעלות ערך עד סוף שנת 2016 וחסרות ערך לאחר תאריך זה. לגבי חתימות בעלות חשיבות קריטית, אשר יש חשש שיותקפו על ידי מדינה או ארגון בעל משאבים גדולים, יש לעבור בהקדם האפשרי לשימוש בעקומים אליפטיים סטנדרטיים (לפי מסמך FIPS 186-3) באורך גדול מ-160 סיביות. (גורם מאשר המשתמש בעקומים אליפטיים יהיה חייב לעבור עד סוף שנת 2011 לשימוש במפתח פומבי באורכים המתאימים לצורפים אלה.

- הערה: מסמך ETSI מאפשר להשתמש גם אלגוריתם EC-GDSA מעל חבורה מסדר ראשוני $E(F_p)$, או מעל חבורה בינארית $E(F_{2^m})$. אלגוריתם זה הוא הגרסה הגרמנית לאלגוריתם ECDSA. בכדי לא להרחיב ללא צורך את מסמך האפשרויות לאלגוריתמי חתימה, לא נאפשר חתימות בשיטה זו.

נימוקים להמלצה:

יש לעקוב אחר ההמלצות העדכניות בעולם לגבי חתימות מסוג זה. יש לעבור לשימוש בעקומים גדולים יותר מאורך של 160 סיביות מהסיבות הבאות:

- עקומים אלו דורשים שימוש בפונקציות גיבוב עם פלט באורך 160 סיביות.

⁴⁶ <http://www.ecc-brainpool.org/ecc-standard.htm>

⁴⁷ ההמלצה של הרשות לביטחון תקשורת בקנדה, Communications Security Establishment Canada, היא לעקומים אליפטיים באורך 256 סיביות החל מסוף שנת 2010. <http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html>

- כמו כן, שימוש בעקומים באורך 160 סיביות ניתן להתקפה על ידי שיטת **baby step**, **giant step**, בעלות של 2^{80} פעולות ו- 2^{80} זיכרון,

5 אורכי מפתחות בשימוש גורם מאשר (CA)

המלצות:

- גורם מאשר חייב יהיה להשתמש בשיטת גיבוב עם פלט של 256 סיביות לפחות.
- לגבי שיטת החתימה, גורם מאשר חייב יהיה להשתמש באורכי מפתחות שלא יפלו מאלה המאושרים לשימוש כללי. כמו כן, מסוף שנת 2011 יהיה חובה על גורם מאשר להשתמש באחת השיטות הבאות
- 0 שיטת RSA עם מפתח באורך 4096 סיביות לפחות, יש להדגיש שמדובר הן בחתימות על מפתחות של הגורם המאשר (self signed root) והן בחתימות על תעודות של משתמשים.
- באפליקציות מסוימות, בהן יש מגבלה על אורך המפתחות בהם ניתן להשתמש, ניתן יהיה להשתמש בתעודות חתומות על ידי מפתח CA באורך 2048 סיביות, אך זאת רק באישור הרשם.
- 0 או שיטת DSA עם פרמטר q באורך 256 סיביות לפחות,
- 0 או שיטות חתימה מבוססות עקומים אליפטיים באורך 256 סיביות לפחות.

נימוק ההמלצה: שבירה של חתימות המבוצעות על ידי גורם מאשר מאפשרת לזייף חתימה מאושרת של כל גורם אחר. עקב כך יש חשיבות להבטיח ביתר וודאות את בטיחות החתימות של גורם מאשר.

6 יצור מספרים אקראיים

יצור המפתחות של מערכת החתימה חייב להתבצע בצורה בטוחה. יש לעקוב אחר ההנחיות במסמך FIPS 186-3 לגבי יצור המפתחות ולגבי בחירת מספרים אקראיים המשמשים בתהליך החתימה.

7 טבלאות מסכמות

7.1 שיטות גיבוב

הערות	תוקף	אורך פלט	שיטה
כנראה ישבר בקרוב	עד סוף שנת 2010	160	SHA-1
כנראה יכול להישבר בהשקעה גדולה	עד סוף שנת 2012	160	RIPEMD-160
כנראה יכול להישבר בהשקעה גדולה	עד סוף שנת 2012	160	SHA-224 עם פלט מקוצר ל-160 סיביות
לא ידועות תקיפות	ללא הגבלה	224	SHA-224
לא ידועות תקיפות	ללא הגבלה	256	SHA-256
לא ידועות תקיפות	ללא הגבלה	384	SHA-384
לא ידועות תקיפות	ללא הגבלה	512	SHA-512
לא ידועות תקיפות	ללא הגבלה	512	Whirlpool

7.2 שיטות ריפוד

מקור	שיטה
FIPS 186-3 (דומה למסמך PKCS #1 v2.1 ולמסמך ETSI)	RSASSA-PKCS1-v1.5
FIPS 186-3 (דומה למסמך PKCS #1 v2.1 ולמסמך ETSI)	RSASSA-PSS

7.3 שיטות חתימה

מקור	תוקף	אורך מפתחות	שיטה
ETSI, ECRYPT, Canada	עד סוף שנת 2010 נרק לחתימות שהן בעלות ערך עד סוף שנת 2016	1024	RSA
ETSI, ECRYPT, Canada	ללא הגבלה	2048 סיביות או יותר	RSA
	יש להתכונן למעבר לאורכי מפתחות אלו	4096 סיביות או יותר	RSA
FIPS 186-3	עד סוף שנת 2010 נרק לחתימות שהן בעלות ערך עד סוף שנת 2016	(L=1024,N=160)	DSA
FIPS 186-3	ללא הגבלה	(L=2048,N=224) (L=2048,N=256) (L=3072,N=256)	DSA
ETSI יש להשתמש בשדות המוגדרים במסמך ETSI	עד סוף שנת 2010 נרק לחתימות שהן בעלות ערך עד סוף שנת 2016	160	ECDSA מעל $E(F_p)$
FIPS 186-3 יש להשתמש בשדות המוגדרים במסמך FIPS 186-3	ללא הגבלה	224 או יותר	ECDSA מעל $E(F_{2^m})$

8 נספח: החולשה בשיטת הגיבוב MD5 ומשמעותה

שיטת הגיבוב MD5 הוצגה בשנת 1992 ומאז הייתה בשימוש נרחב אע"פ שלאורך זמן התגלה חשש לגבי בטיחותה. בשנת 2004 הוצגה שיטה למציאת התנגשויות ב-MD5, כלומר למציאת זוגות קלטים m, m' כך שמתקיים $MD5(m) = MD5(m')$. לאחר מכן שופרו הטכניקות למציאת התנגשויות כך שאפשר יהיה למצוא זוג certificates (תעודה אלקטרונית שהנפיק גורם מאשר, לצורך חתימה מאושרת) בפורמט סטנדרטי, כך שערכי ה-MD5 שלהם זהים. לאחרונה, בסוף שנת 2008, הודגם שניתן להשתמש בערכים מסוג זה בכדי לקבל תעודה אלקטרונית מאחד מה- root CAs של האינטרנט⁴⁸. הדבר מאפשר התקפה רבת עוצמה, בצורה הבאה:

- רוב ה-root CAs אינם משתמשים יותר ב-MD5, אך מספיק לאתר CA בודד המשתמש בשיטה זו.
- יש למצוא זוג תעודות אלקטרוניות, כך שערך ה-MD5 שלהן זהה. אחת מהן היא עבור אתר תמים, השנייה היא לתעודה המסמיכה את בעליה להיות CA בעצמו.
- יש לבקש חתימה על התעודה הראשונה מ-root CA. התוקפים אכן הצליחו לקבל חתימה כזו.
- חתימה זו מהווה גם חתימה על התעודה השנייה, המסמיכה את התוקפים להיות CA. כעת ניתן באמצעות תעודה זו לחתום על תעודות אלקטרוניות נוספות, חתימות אלו אינן חייבות להתבצע בעזרת MD5, אלא באמצעות כל שיטת גיבוב או חתימה שהיא. ניתן לדוגמא לחתום על תעודה המאשרת שיוך של מפתח פומבי מסוים לבנק, או לכל מוסד פיננסי אחר.
- כעת, באמצעות תעודה זו ניתן להתחזות לבעלי המוסד הפיננסי ולזייף אתר אינטרנט האמור לאפשר גישה לאותו מוסד. משתמש שייגש לאתר המזויף יקבל תעודה אשר תעבור את כל הבדיקות של הדפדפן, ויהיה משוכנע שזהו האתר המקורי. (שימו לב שההתקפה משפיעה על כל אתר, ולא רק על אתרים המשתמשים ב-MD5, או בתעודה מה-CA הבודד אשר משתמש ב-MD5).

המסקנה מההתקפה זו היא שניתן לעיתים להפוך חולשות מזעריות בשיטות הקריפטוגרפיות להתקפות של ממש על אפליקציות. לכן יש להימנע שכל שימוש בשיטות חתימה או גיבוב אשר קיים חשש כלשהו לגבי בטיחותן.

⁴⁸ראו MD5 considered harmful today, Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger, <http://www.win.tue.nl/hashclash/rogue-ca/>, Dec. 30, 2008.

מידע לגבי ההנחיה

25. מס' ההנחיה: 4/2010
26. נושא ההנחיה: עדכון אלגוריתמים ואורכי מפתחות לשימוש לפי חוק חתימה אלקטרונית, התשס"א-2001
27. תאריך פרסום: 1.7.2010
28. בתוקף מתאריך: 1.4.2011
29. חוקים שאוזכרו:
- א. חוק חתימה אלקטרונית, התשס"א-2001.
30. חקיקת משנה שאוזכרה: אין.
31. פסקי דין שאוזכרו: אין.
32. מאמרים שאוזכרו: אין.
33. הנחיות היועץ המשפטי לממשלה שאוזכרו: אין.
34. הנחיות רשם גורמים מאשרים שאוזכרו: אין.
35. מילות מפתח: אלגוריתמים, אורכי מפתחות, גיבוב (hash), הצפנה אסימטרית, הצפנת מפתח ציבורי, חתימה אלקטרונית, ריפוד (padding).
36. עדכונים

גרסה	פרטים	תאריך
1.1.	דחיית תחילת תוקף עד 25.2.2011	2.1.2011
1.2.	דחיית תחילת תוקף עד 1.4.2011	23.2.2011



תאריך: 30 דצמבר 2010
כ"ג טבת תשע"א
סימולין: 015-99-2010-005292
תיק: פק 10-699 קומסיין
- עמידה בהנחיה
02.2010
באמצעות: דואר אלקטרוני

לכבוד
[רשימת תפוצה – חתימה אלקטרונית]

א.ג.ג,

הנדון: דחיית יישום הנחיה 4-2010

הריני לעדכנכם, בדבר החלטת רשם גורמים מאשרים (להלן – **הרשם**), לפי חוק חתימה
אלקטרונית, התשס"א-2001 (להלן – **החוק**), כדלקמן:

1. בהתאם להנחיה 4-2010, נדרשת קומסיין לעדכן את אמצעי החתימה המשמש אותה עד סוף
שנת 2010.
2. בשל אי הערכות חברת קומסיין לעמוד בדרישות הנחיה 4-2010 להנחת דעת הרשם, החליט
הרשם לדחות את תחילת ההנחיה, בכל הנוגע לאורך המפתחות לחתימה שבשימוש חברת
קומסיין עד ליום 25.02.2011.
3. לידועתכם.

רוז ברנר, עו"ד

מחלקת רישום ופיקוח

העתקים:

מר יורם הכהן, ראש הרשות למשפט טכנולוגיה ומידע
מר עמית אשכנזי, רשם גורמים מאשרים
גבי רבקי דב"ש, מנהלת מחלקת רישום ופיקוח כאן.



תאריך: 23 לפברואר, 2011
מ"ט אדר א', תשע"א
סימוכין: 015-99-2011-000740
פק 10-699
באמצעות: דואר אלקטרוני

לכבוד:
[רשימת תמוצה חתימה אלקטרונית]

א.ג.ב.,

הנדון: דחיית יישום הנחייה 4-2010 ליום 01.04.2011

הריני לעדכנכם, בדבר החלטת רשם גורמים מאשרים (להלן – **הרשם**), לפי חוק חתימה אלקטרונית, התשס"א-2001 כדלקמן:

1. תחילת הנחייה 4-2010 (להלן – **הנחייה**) נדחתה מיום 01.01.2011 עקב אי הערכות הגורם המאשר חברת קומסיין להנחות דעת הרשם.
2. במקביל, פנתה חברת קומסיין לרשם, בבקשה שלא להפסיק להשתמש בפונקציית גיבוב SHA-1 בהתאם להנחיה.
3. בתום בירור של נושא זה מול ספקי טכנולוגיה ומול רשמים מקבילים באירופה, ובשים לב לאופי השימוש הגובר בחתימה אלקטרונית, והאיומים בנושא זה בהקשר הישראלי, החלטתי שלא לסטות מחוות דעתי המקצועית של ד"ר פנקס אשר צורפה להנחיה ומהמלצותיו לעניין השימוש בפונקציה זו.
4. תחולת הנחייה 4-2010 תדחה ליום 01.04.2011.

בכבוד רב,

עמית אשכנזי
רשם גורמים מאשרים ויועץ משפטי
רמ"ט

העתיקים:

מר יורם הכהן, ראש הרשות למשפט טכנולוגיה ומידע
מר עמית אשכנזי, רשם גורמים מאשרים
גבי רבקי דב"ש, מנהלת מחלקת רישום ופיקוח כאן.

נספח ד'

הנחית רשם גורמים מאשרים מס' 5/2010

**בדיקת הזהות בפני הגורם המאשר לפי תקנות חתימה אלקטרונית (חתימה
אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001**

1. כללי

- 1.1. ביום 7.7.2010 נכנס לתוקפו התיקון⁴⁹ לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001 (להלן - **התקנות**).
- 1.2. לאחר התיקון, סעיף 10 לתקנות, קובע חלופות למסמך מזהה, הנוסף על תעודת זהות ומידע ממרשם האוכלוסין, באמצעותו יחיד שהוא תושב ישראל יזדהה בפני גורם מאשר לצורך הנפקת תעודה אלקטרונית.
- 1.3. בין החלופות, ניתן למסור אישור של עורך דין על זהותו של המבקש.
- 1.4. כמו כן, הרשם רשאי לאשר, מטעמים שיירשמו, מסמך מזהה אחר אשר ישמש את הגורם המאשר בעת אימות זהות.
- 1.5. מטרת הנחיה זו היא לקבוע את נוסח אישור עורך דין על זהות, וכן להבהיר את אופן הגשת הבקשה לאישור מסמך מזהה על ידי הרשם לפי התקנות.

2. הנחיה

- 2.1. בהתאם לסמכויות שניתנו לי בסעיף 10 לתקנות, הריני לקבוע כדלקמן:
 - 2.1.1. אישור עורך דין על זהות לצורך תקנה 10(א)(4)(ג) לתקנות יהיה על פי הנוסח **שבנספח א' - נוסח אישור זהות בידי עורך דין**.
 - 2.1.2. פנייה לאישור מסמך מזהה על ידי הרשם לפי תקנה 10(א)(4)(ב) לתקנות תכלול התייחסות לכל הפרטים המנויים **בנספח ב' - פרטים נדרשים בפנייה לבקש אישור מסמך מזהה**.

⁴⁹ תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות) (תיקון), התש"ע-2010. נוסח התיקון התפרסם באתר משרד המשפטים בכתובת:
<http://www.justice.gov.il/NR/rdonlyres/F2CBAB4E-B377-4B18-B081-CCE36C91DB97/21216/6907.pdf>



2.1.3. מסמך מזהה שאושר על ידי הרשם יתפרסם באתר האינטרנט של הרשם

בכתובת: <http://ilita.justice.gov.il> וברשומות.

נספח א' - נוסח אישור זהות בידי עורך דין

לפי תקנה 10(2)(א)(4)(ג) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001

אני הח"מ, עורך דין _____, מס' רישיון _____ שכתובתי _____, ומס' הטלפון שלי הוא _____, מאשר בזה כי מר/גב' * _____, נושא תעודת זהות מס' _____, אשר תמונתו/ה * מצורפת בזאת וחתומה בידי, מוכר לי אישית ופרטי הזיהוי שלו הם כפי שפירטתי לעיל.

אני מודע לכך כי אישורי זה נועד לתמוך בבקשה להנפקת תעודה אלקטרונית לפי חוק חתימה אלקטרונית תשס"א-2001.

כאן תצורף תמונה של המבקש עם
חתימה וחותמת של עורך הדין, על גביה

ולראיה באתי על החתום –

היום _____

עו"ד _____

_____ חתימה וחותמת

* מחק את המיותר

נספח ב' - פרטים נדרשים בפנייה לבקש אישור מסמך מזהה

לפי תקנה 10(2)(א)(4)(ב) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001

5. שם הגוף המבקש ;
6. שם המסמך המזהה לגביו מתבקש האישור ;
7. מסמך רשמי, החתום על ידי בעל התפקיד הבכיר האחראי על הנפקת המסמך המזהה, הכולל פירוט הפרטים הבאים :
 - 7.1. האם התעודה המונפקת כוללת תמונה ומספר זהות.
 - 7.2. מקור הסמכות לפיו מופקת התעודה (חוק, תקנות וכו').
 - 7.3. מהם תהליכי הזיהוי הננקטים על מנת לוודא את זהות מבקש התעודה, ובפרט את עדכניות התמונה.
 - 7.4. באיזו תדירות מחודשת התעודה, אם בכלל.
 - 7.5. מה הכללים לגבי הנפקה מחודשת של תעודה במקרה של אובדן או גניבה. האם מבוצע תהליך ההנפקה מחדש.
 - 7.6. נתונים לגבי המסמך :
 - 7.6.1. סוג המסמך (תעודה/כרטיס וכד') ופרטים טכניים אודותיו, כולל נתוני המדיה לשמירת/עיבוד נתונים המשולבת בו, אם קיימת.
 - 7.6.2. הפרטים המודפסים עליו.
 - 7.6.3. מנגנוני ההגנה מזיוף המשולבים בו, אם קיימים.
8. צילום ברור של דוגמת המסמך המזהה הנדרש לאישור.

מידע לגבי ההנחיה

37. מס' ההנחיה: 5/2010
38. נושא ההנחיה: בדיקת הזהות בפני הגורם המאשר לפי תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001
39. תאריך פרסום: 26.7.2010
40. בתוקף מתאריך: 26.7.2010
41. חוקים שאוזכרו:
- א. חוק חתימה אלקטרונית, התשס"א-2001.
42. חקיקת משנה שאוזכרה:
- א. תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001
43. פסקי דין שאוזכרו: אין.
44. מאמרים שאוזכרו: אין.
45. הנחיות היועץ המשפטי לממשלה שאוזכרו: אין.
46. הנחיות רשם גורמים מאשרים שאוזכרו: אין.
47. מילות מפתח: בדיקת זהות, גורם מאשר, הנפקת תעודה, זיהוי, מבקש תעודה, מסמך מזהה.
48. עדכונים

גרסה	פרטים	תאריך



נספח ה'

הנדון: סיכום מפגש תקופתי של רשויות הפיקוח האירופאיות על חתימה אלקטרונית [FESA]

1. ב- 13-14.04.2010 התקיים בורשה, פולין המפגש התקופתי של רשויות הפיקוח האירופאיות על חתימה אלקטרונית (Forum of European Supervisory Authorities – FESA), באירוח משרד הכלכלה הפולני והמכון הפולני לחקר המחשבים.
2. ארגון FESA הוקם באופן וולנטרי על ידי החברים, ואינו בעל מעמד רשמי של ארגון דיפלומטי אלא מהווה פורום להחלפת דעות ותיאום עמדות בין רשויות הפיקוח.
3. החל משנת 2007 רשם גורמים מאשרים הישראלי חבר בפורום זה כחבר משקיף, ובשנת 2008 הרשות למשפט טכנולוגיה ומידע אף אירחה את המפגש בתל אביב.
4. במפגש נכחו נציגים של רשויות הפיקוח מהמדינות הבאות: גרמניה, פולין, איטליה, בלגיה, הולנד, צ'כיה, שוודיה, איסלנד, לטביה, פינלנד, יוון, אוסטריה, שווייץ. כן השתתפו נציג נציבות האיחוד האירופי, ושני חוקרים העוסקים במחקרים מטעם הנציבות לקידום המדיניות האירופית, ונציג הרשות האלבנית (שבסוף המפגש נבחר להיות חבר משקיף). בנוסף הוזמנו נציגים של מספר גורמים פרטיים הפעילים בשוק זה להציג את פעילותם. במפגש הנוכחי נדונו מספר רב של נושאים בעלי רלבנטיות לישראל, ובהם עדכונים מנציבות האיחוד על מגמות ההסדרה והחקיקה, קידום סוגיות של תעודות זהות חכמות, הסדרה של רשימה ממוחשבת אחידה כלל אירופאית של "גורמים מאשרים", הצגה של פתרון חתימה המבוסס על טלפונים סלולרים, שירות וידוא תוקף חתימה אירופי ופולני, עדכונים על פעילות התקנה באירופה ובמיוחד על פורמט אחיד למסמכים חתומים וחתימות לטווח ארוך.
- א. מגמות ההסדרה ברמת נציבות האיחוד האירופי
5. הטיפול בנושא החתימה האלקטרונית מטופל ביחידת DG Information Society, העוסקת בגולציה וחקיקה בתחום האינטרנט והתקשורת. לצד הטיפול של DG Information Society, יחידת DG Internal Market, העוסקת בהסדרת השירותים (services), גרמה למהפכה זוטא בתחום זה, בכך שקידמה חקיקה המונעת יכולת שלא לקבל חתימה אלקטרונית לפי הדירקטיבה שהונפקה במדינה אירופאית אחת, במדינה אחרת.⁵⁰
6. התוצאה הישירה של הטמעת מדיניות זו במדינות האיחוד הינה הסרה גורפת של חסמים לשימוש בחתימה אלקטרונית בין מדינות אירופה. החלטה זו נובעת כפי הנראה מסדרת מחקרים שנערכת על ידי מוסדות האיחוד לאיתור חסמים לשימוש בחתימה אלקטרונית (ראו גם להלן).

⁵⁰ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN:PDF>



7. במסגרת הפעילות המשולבת של שני משרדים אלה, אף התקבלה בתום דיונים מרובים בשנת 2009 החלטה של הנציבות המחייבת כל מדינה לנהל רשימה ממוחשבת של הגורמים המוסמכים להנפיק תעודות אלקטרוניות לפי הדירקטיבה. רשימה כזו נועדה ליצור מאגר פורמט אחיד ובמקום קבוע, שיאפשר בדיקה מהירה ואמינה של מהימנות תעודה אלקטרונית שהונפקה במדינת האיחוד. לצורך תמיכה ברשימה זו נקבע תקן אירופאי המפרט את אופן עריכתה. ההחלטה נכנסה לתוקף בסוף 2009, ולפי הנתונים שנמסרו במפגש, יושמה על ידי רוב מדינות אירופה. בנוסף, הנציבות מרכזת את "רשימת הרשימות" של גורמי האמון האירופאים.

8. יצוין כי במסגרת מאמצנו בשנים 2003-5 להביא להסכמי הכרה הדדית בין ישראל לאיחוד בתחום החתימות האלקטרוניות, התברר כי על אף קיומו של דין אחיד לכאורה באירופה, דה פקטו אין הכרה הדדית בחתימות אלקטרוניות בין מדינות אירופה לבין עצמן, ובשל כך לא היה בסיס לקידום הכרה הדדית ברמת הנציבות עם ישראל.

9. במסגרת המפגש הוצגו לקחים ונתונים אודות המימוש של נושא זה, וכן שאלות לעניין האפשרות שהנציבות תקח על עצמה לרכז את "רשימת הרשימות". אופן עריכת רשימת הרשימות של גורמי האמון, והכללים החלים, רלבנטים מאוד לישראל משום שאם תתאפשר הכרה הדדית ברמה המהותית, הדרך המעשית לממשה היא בפורמט הטכני של עריכת רשימת רשימות זו.

ב. שירותי בדיקת תוקף חתימה/ תעודה

10. במסגרת הדיון המוזמן הציגו שני גורמים מסחרים, אחד גורם מאשר פולני, והשני שירות אירופאי אחר, שירות שהם מציעים לצורך בדיקה של תוקף חתימה על מסמך או בדיקה של תוקף תעודה.

11. שירות זה מאפשר למסתמך לבדוק את תוקף החתימה מול מקור אחד בלבד ומבלי צורך לפנות לכל אחד מהגורמים המאשרים באירופה, בדרך של שאילתא נקודתית פשוטה מול אתר ספק השירות.⁵¹

12. השירות הוצג במתכונת של שאילתא רגילה דרך דפדפן אינטרנט, וכן באפשרות של מימוש פרוטוקול המבצע את הבדיקה ומחזיר תשובה באופן אוטומטי על בסיס פרוטוקול SOAP.

ד. הסדרה של חתימה אלקטרונית בפורמט התואם את הדירקטיבה האירופית במסמכי PDF

13. מר Julian STERN, ששימש עורך של תקן של מכון התקינה ETSI, בנושא של פורמט PDF חתום בהתאם לדרישות הדין האירופי.⁵²

⁵¹ ראה: <http://www.certum.eu/certum/cert,offer DVCS WebNotarius.xml>

⁵²

של לעתונות הודעה etsi :

http://www.etsi.org/website/newsandevents/200909_electronicsignature.aspx



14. במסגרת עבודת התקינה תוקנן אופן השילוב של חתימה אלקטרונית, ומידע אודות תוקפה, בפורמט הסטנדרטי של pdf.

15. מר STERN הציג את פרקי התקן, בדגש על פרק 4, קביעת מנגנון להוכחת תוקף החתימה גם לטווח ארוך. בתמצית, אף שניתן לבדוק תוקף חתימה סמוך לזמן עריכתה, ככל שמתרחקים ממועד זה, עלולים להיות קשיים לוידוא תוקף החתימה בזמן עריכתה. בנוסף, בשל התקדמות פריצת הצפנות, עולה חשש שמסמכים ישונו לאחר שמנגנון החתימה שלהם כבר אינו חזק דיו (אף שהיה חזק דיו בעת עריכת המסמך).

16. על מנת להתמודד עם קושי זה, תוקנן פתרון המשמר את בדיקת מהימנות החתימה בעת עריכתה, ומאפשר גם לרענן תוקף בדיקה זו באופן שהיא תהיה תקפה באופן קבוע.

מעבר למידע המועיל שנמסר אודות התקן, והעלאת המודעות שלנו לנושא זה, הרלבנטי גם לפרויקט ארכיטקטורת אלקטרונית שאנו מקדמים, אציין הערה מעניינת של האחראי על הפיקוח בגרמניה, שהציג שיטה חלופית לשמירת תוקף של חתימה המבוססת על תפיסה המכונה כ- chain model.

ה. חיתום זמן

17. במסגרת הדיון הציגו המדינות השונות את האופן שבו הן מסדירות שירותי חיתום זמן, כלומר שירותים שבהם מוצמדת חותמת מהימנה עם זמן המבוסס על מקור זמן מהימן, למסמך כלשהו, וכך מספקת ראייה לקיומו במועד הנטען.

18. נושא זה מתוקנן בתקינה האירופית, אולם לא מוסדר משפטית בכל מדינות האיחוד.

19. בדיון עלה כי במדינות רבות יש הסדר רלבנטי, ושירותים אלה מפוקחים במסגרת הפיקוח על גורמים מאשרים.

20. יתרה מזו, בחלק ממדינות אירופה (גרמניה ואוסטריה), יש חובה שמקור הזמן יתבסס על מקור הזמן הרשמי במדינה – מכון מטאורולוגי.

ו. פתרון חתימה המבוסס על טלפונים סלולרים

21. סוגייה מרכזית המהווה חסם להפצה רחבה של חתימות אלקטרוניות היא שהן מחייבות חומרה מיוחדת, שמטרתה שמירה על אמצעי החתימה, הוא מפתח החתימה הסודי, המשמש לחתימה. בנוסף, במציאות יש קשיים בהטמעה של חומרה כאמור בשל הצורך בתמיכה בהתקנתה, תחזוקה, וממשקיה אל המערכות הסטנדרטיות.

22. נושא זה מאתגר זמן רב את העוסקים בתחום.

23. במסגרת הדיון הציגה חברה איטלקית [aliasLab]⁵³ פתרון המבוסס על ארכיטקטורה שבה חתימתו של החותם מצויה על גבי התקן מאובטח מרכזי, והפעלתו נעשית מרחוק באמצעות

⁵³ www.aliaslab.net



הטלפון הסלולרי של בעל החתימה. [הפתרון מכונה SecureCall Sign]. הפתרון של החברה האיטלקית משמש לפרויקטים רגישים של חתימה אלקטרונית באיטליה, ואושר גם על ידי הרשות המפקחת האיטלקית.

24. נושא זה עורר דיון סוער בין החברים, משום שהוא מאתגר את הדרישה הקיימת בדיון האירופי, וגם בישראל ל – "שליטה בלעדית" של החותם באמצעי החתימה שלו.

25. העובדה שהחתימה מצויה על גבי שרת מרכזי, ולא בכיס של החותם, מהווה סמרטוט אדום לחלק מהרשויות.

26. אחרים, ביקשו לדעת מהו ההסדר שנקבע בנושא זה, וכיצד בוקר, וזאת משום שתיאורטית ניתן ליצור מערכת של בטוחות שימנעו חששות מפני שימוש לרעה. ככלל ניתן לומר כי רוב הנוכחים בדיון סברו כי עד לתיקון של הדין האירופי, פתרון כאמור אינו קביל. זו לא היתה כמובן גישתו של הנציג האיטלקי.