



כ"ב בניסן התשפ"א
4 באפריל 2021
מר. 1972-2021

מענה לשאלות ההבהרה בבקשה לקבלת מידע (RFI) בנושא אימות חתימות אלקטרוניות מאובטחות על מסמכים המוגשים למערכת מרכב"ה

מס"ד	שאלה	תשובה
1.	בסעיף 1.1 הוזכר "חתימה אלקטרונית מאובטחת" בחוק חתימה אלקטרונית משנת 2001, הוזכרו שני סוגי חתימה: חתימה אלקטרונית מאושרת מאושרת על ידי תעודה אלקטרונית שהונפקה על ידי CA מוכר חתימה אלקטרונית מאובטחת שחתומה באמצעי חתימה כמו עט אלקטרוני או כל אמצעי המזוהה עם החותם חתימה זו מאובטחת בצורה כזאת שאי אפשר לשחזר או להעתיק, או לבצע שינוי בגוף המסמך שנחתם באיזה סוג חתימה מדובר?	הבקשה מתייחסת לחתימות מאובטחות בלבד העומדות בדרישות תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), תשס"ב-2001.
2.	במקרה של חתימה מאושרת, באיזה תעודות אלקטרונית מדובר, האם הכוונה היא לחתימות שהונפקו בארץ על ידי CA – ים ישראלית?	הבקשה מתייחסת לחתימות מאובטחות בלבד העומדות בדרישות תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), תשס"ב-2001.
3.	במקרה של חתימה מאובטחת, המסמך ננעל על ידי תעודה אלקטרונית. מי הגורם המאשר של התעודה?	ספקים שאליהם הופנתה הפניה - ספקי המערכות המפיקות מסמכים החתומים בחתימה אלקטרונית מאובטחת, ובכלל זה ספקי מערכות חשבונאיות המפיקות חשבוניות החתומות בחתימה אלקטרונית מאובטחת בהתאם להוראות רשות המיסים.
4.	האם החתימה המאובטחת מתבססת על חתימה גראפית, האם נדרש זיהוי של חותם החתימה?	החתימה מתבצעת באמצעות תעודה לחתימה באמצעות תשתית PKI. לא מדובר בחתימות גראפיות.
5.	האם יש עומק לחתימה מהירה, לחץ, תדר דגימה?	השאלה אינה ברורה. בכל מקרה, לא מדובר בחתימות גראפיות.



מס"ד	שאלה	תשובה
6.	האם בחתימה אלקטרונית מאובטחת, יש דרישה ליישם חוק חתימה אלקטרונית ללא פרצות?	על חתימה מאובטחת לעמוד בדרישות תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), תשס"ב-2001.
7.	האם מבנה הקבצים בחתימה אלקטרונית מאובטחת, צריך להיות בתקינה אירופאית קיימת המאפיין את המבנה לשמירת המידע הביומטרי בקובץ החותם (סטנדרטיזציה -ISO/IEC DIS 19794)?	אין צורך בשמירת מידע ביומטרי.
8.	האם יש גישה למאגרי ה-CRL לתעודות משאלות 3 ו-4?	הפניה הופנתה לספקי המערכות המפיקות מסמכים החתומים בחתימה אלקטרונית מאובטחת, ובכלל זה ספקי מערכות חשבונאיות המפיקות חשבוניות החתומות בחתימה אלקטרונית מאובטחת בהתאם להוראות רשות המיסים. ספקים אלה הם שאמורים להפיק את קבצי ה-CRL שמולם מתבצע תהליך האימות.
9.	בסעיף 1.3 נאמר מערכת חיתום, האם יש דרישה לחיתום ולא רק לאימות?	כפי שהודגש בסעיף אליו מפנה השאלה, מטרת הבקשה הינה בחינת אופן אימות החתימות המאובטחות על מסמכים המתקבלים במערכותיה ולא רכישת מערכות חיתום או אימות חיצוניות.
10.	באיזה מערכות החתמה חיצונית מוחתמים הקבצים שמתקבלים?	לא ידוע. הבקשה עוסקת בתהליך האימות בלבד.
11.	האם מדובר בקבצי PDF בלבד או גם סוגים נוספים? אם כן באיזה סוגים	לרוב קבצי PDF, אך לא רק. פתרון האימות נדרש להיות אוניברסאלי
12.	בסעיף 3.1 מדובר בתעודה לחתימה אלקטרונית מאושרת, או תעודה אלקטרונית לצורך נעילת המסמך וחתימתו בחתימה מובטחת, שהונפקו על ידי CA מוכר במדינה. גורם זה היינו היחידי שיש לו את רשימת ה-CRL - ים, האם הספק יקבל מה-CA את רשימת ה-CRL - ים?	מטרת הבקשה הינה בחינת אופן אימות החתימות המאובטחות כמשמעותן בתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), תשס"ב-2001.
13.	האם הספק חייב להיות CA מאושר על ידי המדינה?	לא



מדינת ישראל
החשב הכללי
מרכבה



<u>תשובה</u>	<u>שאלה</u>	<u>מס"ד</u>
לא	האם שרת ה- CA קיים פנימי בפרויקט מרכב"ה?	.14