25 אוגוסט, 2020

הנדון: <u>מכרז פומבי מספר 2/20 - לאספקת מערכת מרכזית להנפקת חתימות אלקטרוניות עבור משרד הדיגיטל הלאומי – רשות התקשוב הממשלתי – קובץ הבהרות מספר 3</u>

1. בהתאם לסמכותה על פי מסמכי המכרז, לרבות סעיף 1.6 בפרק 1 למסמכי המכרז, מתכבדת בזאת ועדת המכרזים ליתן הודעה למציעים, להלן בנספח א', בדבר הבהרה יזומה מטעמה.

2. כל ההבהרות והשינויים בהודעה זו יחשבו לחלק בלתי נפרד ממסמכי המכרז.

3. אלא אם נאמר אחרת, לכל המונחים האמורים בהודעה זו תהיה המשמעות שנקבעה להם במסמכי המכרז.

4. אין להסתמך על כל הסבר או פירוש שניתן בעל פה או בכתב או בכל דרך אחרת על ידי מי מטעם ועדת המכרזים או על ידי כל גורם אחר, ככל שניתן, בכל פורום או צורה שהיא. השינויים היחידים מהאמור במסמכי המכרז וכן כל הפירושים וההבהרות להם, הינם כמפורט במכתב זה בלבד, ובמכתבי הבהרות נוספים שיצאו מטעם ועדת המכרזים, ככל שיצאו.

5. אין בהודעה זו כדי לשנות מהוראות מסמכי המכרז, אלא ככל ששינוי כזה נעשה במפורש.

בכבוד רב,

גיל לוי

מרכזת ועדת המכרזים

נספח א'

הבהרה יזומה מטעם ועדת המכרזים או מי מטעמה

להלן תסריטי בדיקות מעבדה.

בדיקות מעבדה -
בדיקות לצורך בחינת עמידה בדרישות חובה

מספר	סעיף – פרק 2	דרישת החובה	הבדיקה
.1	2.1.5	חילול צמד מפתחות בהתבסס על תקן מקובל לחתימה אסימטרית, העושה שימוש במפורט להלן, בהתאם לתקן ישראלי (ת"י) 14888 חלק 2 ולתקן ISO/IEC המקביל אליו, ולתקן ישראלי (ת"י) 15946 ולתקן ISO/IEC המקביל אליו, בהתאמה, או תקן שווה ערך של ה- NIST.	תהליך ההרשמה: יצירת משתמש כולל צמד מפתחות RSA2048 והנפקת תעודה דיגיטלית מ-CA.
.2	2.1.2	תמיכה בחתימה ארגונית, המאפשרת למשתמשים מוגדרים בארגון מסוים, גישה לחותם הארגוני של אותו ארגון.	תהליך חתימה: חתימה של קובץ בכל אחד מהפורמטים הנדרשים (PAdES, ,XAdES, ASIC CAdES) ובחינה של התוצר - גם באמצעות העלאת הקובץ עצמו וכן באמצעות שליחת ה-HASH בלבד וחתימה עליו.
.3	2.1.4	תמיכה מלאה בחתימה בתקנים הבאים: 1) תקני חתימה של eIDAS (PAdES, XAdES, CAdES) i. ASiC - ETSI TS 103 174 ii. CAdES - ETSI TS 101 733 iii. XAdES - ETSI TS 101 903 iv. PAdES - ETSI TS 102 778 2) PDF - PDF Reference 1.7 (ISO 32000-1) 3) XML-Sig/XML-Dsig לפי RFC 3075 4) CMS\ PKCS#7 לפי RFC 2315	

מספר	סעיף – פרק 2	דרישת החובה	הבדיקה
.4	2.1.3	תמיכה במספר חתימות של משתמשים שונים על מסמך, או באופן כללי – מסר אלקטרוני, מסוים.	ביצוע של שלוש חתימות על קובץ בהתאם לסטנדרטים המפורטים לעיל בסעיף 2.
.5	2.1.6	יישום וביצוע חותמת זמן (timestamp), באמצעות התממשקות מול שרת זמן/שעון אטומי, בהתאם ל- RFC 3161.	בדיקת תהליך הנפקת חותמת זמן (time stamp) כחלק מתהליך בדיקת חתימה בתקנים השונים.
.6	2.1.8	ממשק ניהול המאפשר כניסה מאובטחת הכוללת אימות על ידי שני גורמים-2FA (2 Factors Authentication), למנהלי המערכת, והתומך בהפרדת התפקידים והגדרת תפקידים.	ביצוע כניסה לממשק הניהול, של בעלי תפקיד שונים, באמצעות הכנסת שם משתמש, סיסמה, טלפון וקבלת SMS עם קוד חד פעמי או שם משתמש וכרטיס חכם והזנת קוד על ידי המציע, ובחינת היכולות המוצגות בממשק הניהול לכל בעל תפקיד (הפרדת תפקידים) ואפשרויות הגדרת התפקיד.
.7	2.1.9	בממשק הניהול ניתן יהיה להגדיר שפעולות רגישות מסוימות תחייבנה הזדהות של שני משתמשים שונים, או יותר, לדוגמה: ה- System Admin יוכל לבצע פעולה מסוימת אבל היא לא תתבצע עד שה- Security Admin ייכנס למערכת ויאשר אותה.	הגדרת פעולה רגישה המחייבת הזדהות כפולה בממשק הניהול. ביצוע הזדהות של בעל תפקיד אחד והזדהות כפולה ובדיקה האם ניתן לאשר הפעולה רק בהזדהות הכפולה.
.8	2.1.10	יתאפשר מידור בין מפתחות פרטיים, כך שלמשתמש מורשה מסוים תהיה גישה למפתח פרטי מסוים ואילו למשתמש מורשה אחר תימנע הגישה למפתח הפרטי של משתמש אחר.	הצגת הסבר על מנגנון המידור בין המפתחות.
.9	2.1.14	רכיב - ה- HSM המוצע עומד בכל התקנים הקריפטוגרפים המפורטים להלן: 1) הסמכה ל- Common Criteria ברמה EAL 4 או ל- NIST – FIPS140-2 רמה 3 או לתקן אחר כמפורט בסעיף 2.1.5	בדיקת התיעוד אשר צורף כמענה לנספח ב' בפרק 3.

מספר	סעיף – פרק 2	דרישת החובה	הבדיקה
		לפרק 1. 2) Random Number Generation – SP 800-90a 3) Encryption Algorithm – ת"י 10118 (ISO/IEC) 4) Hash Function – ת"י (ISO/IEC) 18033	
10.	2.1.15	במקרה של התקפה ו/או פגיעה בהתקן הרשתי עליו להבטיח כי, יבוצע איפוס של כל המידע הרגיש השמור על גבי ההתקן הרשתי.	הצגת הסבר על מנגנון האיפוס.
11.	2.1.16	הוכחת יכולת התממשקות ל- CA (בשלב המעבדה תיבדק הוכחת יכולת התממשקות בלבד. לא נדרש לבצע בפועל התממשקות ל- CA של המשרד.)	תהליך הנפקת תעודה דיגיטלית למשתמש עבורו נוצר מפתח באמצעות CA בשני הפרוטוקולים הבאים: 1. CMP 2. PKCS10
12.	2.1.17	ממשק יישומי (API) באמצעותו ניתן להעביר את פרטי המשתמש, סוג החתימה הנדרשת, והמידע עצמו המיועד לחתימה. המסר החתום יוחזר אף הוא דרך ממשק זה.	הצגת ממשק יישומי (API) לרכיבי המערכת התומך ב- REST וב- SOAP - מנגנון הגירה ומנגנון ההגנה וניהול הזהויות.
13.	2.1.18	ממשק יישומי (API) לניהול המפתחות ותעודות החתימה – ממשק להקמת ומחיקת משתמשים, חילול צמדי מפתחות לכל משתמש, יצירת קבצי בקשות להנפקת תעודות דיגיטליות (CSR) וקבלת תעודות דיגיטליות הכוללות המפתחות הפומביים של אותם משתמשים ובכלל זה כל הנדרש לניהול המפתחות ותעודות החתימה.	
14.	2.1.17 2.1.19 2.1.20	יכולת הגירה/ הסבה/ קליטה של משתמשים וכלל המידע אודותיהם (מיגרציה).	

בדיקות מעבדה -
בדיקות לצורך בחינת עמידה בדרישות איכות

מספר	דרישה	בדיקה	תוצאה (סימון הריבוע המתאים)
1.	יכולת גיבוי של המשתמשים והמפתחות שלהם בצורה מאובטחת ומוצפנת, כאשר המפתחות ניתנים לגיבוי כאובייקט מפתח על פי PKCS#8 המוגן באמצעות סיסמה חזקה שתחולל על ידי המערכת ותהיה ניתנת לקריאה רק בהרשאות ספציפיות של מנהלי המערכת וכן שלצורך שחזור המפתח תידרש פעולה של רכיב נוסף כדוגמת TOKEN שיוחזק בנפרד מהרכיב בו מגובה המפתח.	מנהל המערכת יבצע הזדהות וכניסה לממשק הניהול / ממשק CLI יבצע גיבוי ושחזור משתמשים ומפתחות בממשק הניהול בהתאם למפורט בדרישה ויבצע בדיקה לתקינות השחזור.	☐ התהליך הוא מלא וניתן בעזרת ממשק משתמש גרפי ☐ התהליך הוא מלא ללא ממשק ☐ התהליך חלקי או שאין ממשק משתמש גרפי ☐ לא קיים
2.	מנגנון Audit מקומי אשר ביכולתו לשמור תיעוד של כלל האירועים המתרחשים במערכת לתקופה של לפחות 3 חודשים ללא תלות במערכת SIEM של המשרד, כולל יכולת חיפוש אירועים בסיסית.	מנהל המערכת יבצע הזדהות וכניסה לממשק הניהול / ממשק CLI יבחן ויחפש הפעולות כפי שבוצעו במעבדה והתיעוד להן במנגנון ה-AUDIT.	☐ המנגנון קיים והוא כולל ממשק גרפי שמאפשר חיפוש, סינון ומיון של האירועים ☐ המנגנון קיים אך הוא לא כולל ממשק גרפי או שהממשק חלקי ☐ המנגנון לא קיים
3.	תמיכה בפרוטוקול CMP ליצירת תעודות דיגיטליות.	שליחת בקשה לתעודה בפרוטוקול CMP וקבלת התעודה מה- CA בהתאם.	☐ קיים ☐ לא קיים
4.	תמיכה בפרוטוקול PKCS#10 ליצירת תעודות דיגיטליות.	שליחת בקשה לתעודה בפרוטוקול PKCS#10 וקבלת התעודה מה- CA בהתאם.	☐ קיים ☐ לא קיים

5.	ממשק תמיכה בחתימה גרפית בפורמט PAdES. המערכת מאפשרת ממשק לשמירה של חתימה גרפית ושיוכה למשתמש או ארגון. במקרה של חתימה ארגונית, מתועדת הזהות הפרטית של מבצע החתימה הארגונית.	מנהל המערכת יבצע הזדהות וכניסה לממשק הניהול. יבצע שיוך חתימה גרפית בעזרת ממשק הניהול למשתמש בחינת החתימה הגרפית לאחר החתימה של אותו משתמש.	☐ כולל ממשק גרפי המאפשר ניהול של החתימה הגרפית ושיוכה למשתמש ☐ קיים אבל לא כולל ממשק גרפי ☐ לא קיים
6.	תמיכה בניהול משתמשים מנהלים (פנימי) ב- LDAP ו- LDAPS.	הצגה אם קיים	☐ יש תמיכה והיא כוללת ממשק גרפי שמאפשר את הניהול של המשתמשים ☐ יש תמיכה אבל היא לא כוללת ממשק גרפי ☐ אין תמיכה
7.	ממשק יישומי (API) לרכיבי המערכת, התומך ב- REST.	הצגה אם קיים	☐ קיים ☐ לא קיים
8.	ממשק יישומי (API) לרכיבי המערכת, התומך ב- SOAP.	הצגה אם קיים	☐ קיים ☐ לא קיים
9.	תמיכה בחידוש תעודות דיגיטליות לחתימה באופן אוטומטי דרך API .	הצגה אם קיים	☐ קיים ☐ לא קיים
10.	תמיכה בחידוש תעודות דיגיטליות לחתימה באופן ידני.	מנהל המערכת יבצע הזדהות וכניסה לממשק הניהול. יבצע חידוש תעודה ותבדק תקינותה.	☐ קיים ☐ לא קיים
11.	מנגנון הגנה על צריכת API של השירות. הפתרון נדרש לספק שכבת הגנה שתאפשר לבצע Delegation מבוסס על פרוטוקול OAUTH 2.0 .	הצגה אם קיים	☐ קיים ☐ לא קיים
12.	מנגנון הגנה על צריכת API של השירות. הפתרון נדרש לספק שכבת	הצגה אם קיים	☐ קיים ☐ לא קיים

	הגנה שתאפשר לבצע Delegation מבוסס על פרוטוקול SAML 2.0.		
13.	ביצועים – זמן חתימה לביצוע 100 פעולות חתימה (טרנזקציות) בהתאם למסמך השוואת ביצועים (Benchmark) שנערך למוצר המוצע.	בחינת מסמך	☐ עד 0.5 שנייה ☐ מ-0.5 שנייה ועד 1 שנייה