

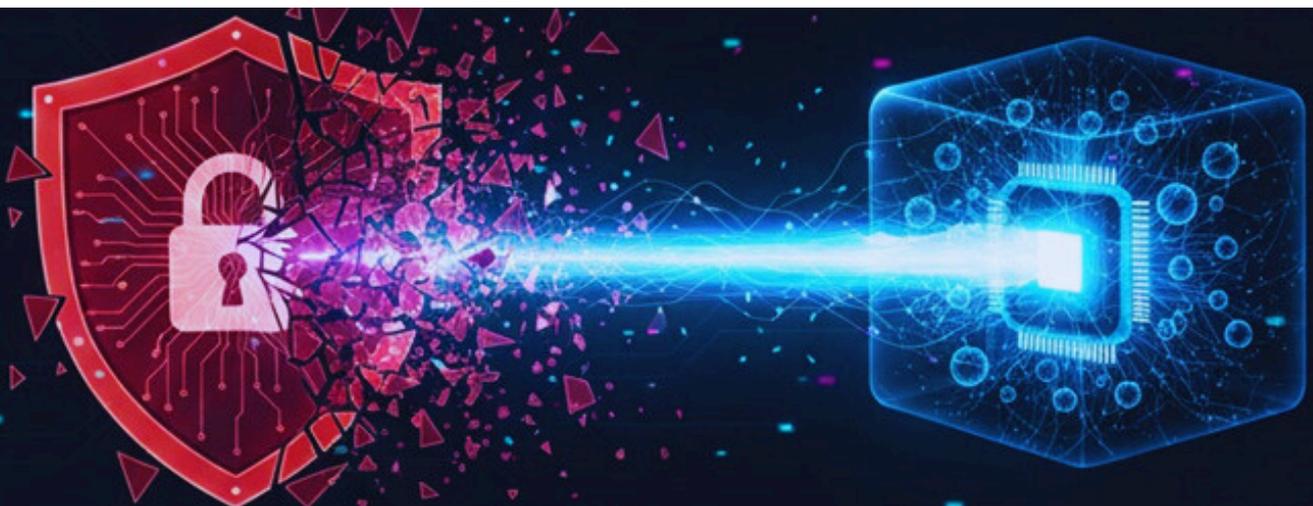
SIGNER PQ

שרת חתימה דיגיטלית לעידון ה Quantum



המסמכים שלך חתומים - אבל לכמה זמן? Harvest Now. Decrypt Later.

מחשבים קוונטיים צפויים לשבור את אלגוריתמי ההצפנה והחתימה הנפוצים כיום כמו RSA ו-ECC - ומה שנראה היום "מאובטח", עלול להפוך מחר לפגיע. המשמעות היא שגם מסמכים שנחתמים ונשמרים עכשיו עשויים להיות "נאספים" כבר היום, כדי להיפענח ולהיערך בעתיד ברגע שהיכולות הקוונטיות יבשילו (Harvest Now, Decrypt Later). לכן ארגונים שמנהלים שמירת מסמכים ארוכת-טווח - חוזים, רשומות, מסמכי רגולציה ותיעוד קריטי - נמצאים בסיכון ממשי לפגיעה באמינות, לשלמות המידע וליכולת להוכיח מה באמת נחתם ומתי. במקביל, זה כבר לא רק תרחיש: רגולציות ותקנים מובילים כמו NIST, ETSI ו-IETF כבר מכתיבים את המעבר ל-PQC (Post-Quantum Cryptography), והארגונים שמתחילים להיערך עכשיו יהיו אלה שיגנו על המידע שלהם, יעמדו בדרישות, וימנעו מרדף יקר תחת לחץ בהמשך.



SIGNER PQ

שרת חתימה דיגיטלית לארגונים בעידן הקוונטי

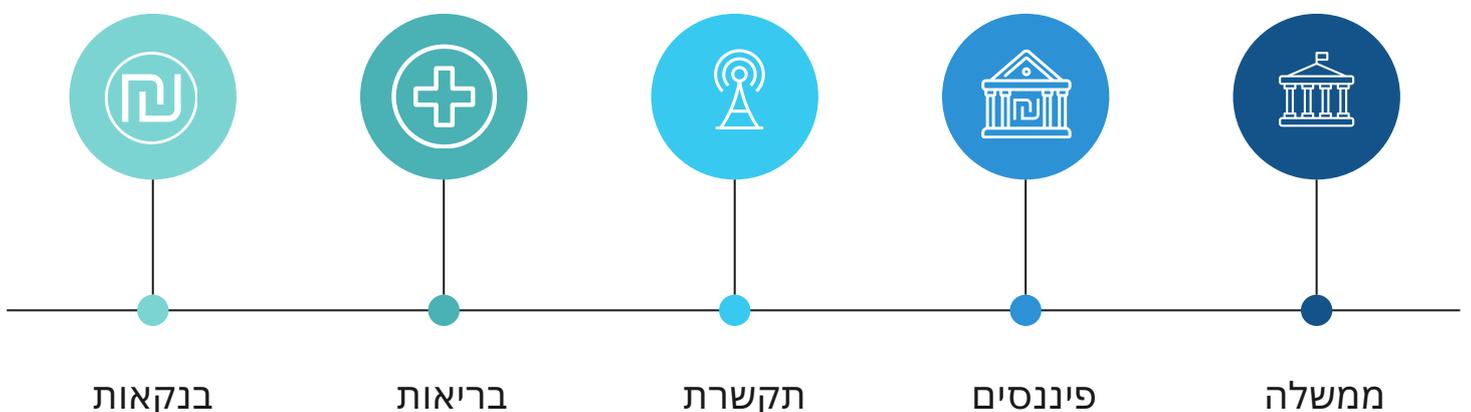
Signer PQ הינה מערכת חתימה דיגיטלית מתקדמת המהווה תשתית טכנולוגית לחתימה מרוכזת על אלפי מסמכים אלקטרוניים שנשלחים ללקוחות הארגון, המוכנה לעידן ה PQ ומאפשרת מיגרציה שקטה וחלקה.

חתימה מרוכזת באמצעות שרת החתימות הדיגיטלי, מייעלת את משלוח המסמכים מהארגון ללקוחות ספקים ועובדים.

המערכת מאפשרת שימוש בתעודות חיתום המותאמות לעידן הקוונטי, ומוגנות מפני פריצת האלגוריתמים. מסמכים הנחתמים בתעודת PQ נשארים מוגנים אף בפני מחשב קוונטי.

המערכת תומכת בתעודות היברידיות המותאמות הן לסטנדרט החיתום הנוכחי והן לסטנדרטי חיתום PQ.

מסמכים החתומים בתעודות שאינם PQ לא יהיו חסינות מפני מחשב קוונטי **וניתן יהיה לזייף אותם!** התקדמו עוד היום והיו מוכנים בזמן!



יתרונות עיקריים של Signer PQ

המערכת יכולה להכיל מאות ואלפי חותמים של הארגון כאשר לכל חותם יש זיהוי חזק ולא פציח לחתימה שלו בלבד



תואם במלואו ל-eIDAS כולל SAM



מונע זיופים ומותאם לעידן הקוונטום (PQC)



חסכון בזמן - ללא הדפסה, חתימה וסריקה



שמירה ואחסון מאובטחים



אבטחת מידע ופרטיות של מסמכים דיגיטליים



ייעול תהליכי החתימה הדיגיטלית באמצעות אוטומציה של Signer PQ



ניתן לחתום עם Signer PQ על המסמכים הבאים:

- | | |
|-----------------------|--------------|
| קבלות ✓ | חשבוניות ✓ |
| מכרזים ✓ | הצעות מחיר ✓ |
| מסמכים סרוקים ✓ | הצעות רכש ✓ |
| כל מסמך שדורש חתימה ✓ | טופסי 101 ✓ |
| חיתום קוד ✓ | חוזים ✓ |

פתרונות משולבים נוספים עם Signer PQ

Signer PQ משלב בין מודול הפעלת החתימה (HSM) המאובטח והמתקדם של קומסיין, שאושר כהתקן מאושר ליצירת חתימה דיגיטלית על פי תקן eIDAS (QSCD):

- מספר בלתי מוגבל של חותמים
- ביצועים גבוהים בתהליך חתימת אצווה בנפח גדול
- חתימה על מספר מסמכים באמצעות מספר חתימות בו-זמנית
- תמיכה באלגוריתמים מוגני PQC

מודול אימות מתקדם

מודול האימות מאפשר ל- Signer PQ לאמת מסמכים חתומים דיגיטלית באמצעות:

- גורם מאשר (CA) כולל OCSP
- מידע מפורט לגבי החותם והארגון
- חותמת זמן בהתאם ל- RFC 3161



מודול ארכיב דיגיטלי

מודול הארכיב הדיגיטלי מאפשר ל- SIGNER PQ לאחסן בצורה מאובטחת ולטווח ארוך פורמטים שונים של מסמכים חתומים דיגיטלית וקבצים אחרים. ניתן לחפש ולאחזר נתונים מאוחסנים בקלות, ולהחליף ארכיונים פיזיים מגושמים.



מאפיינים ראשיים Signer PQ

כמוצר מאובטח מבוסס ענן, Signer PQ תוכנן לענות על הצרכים של ארגונים וחברות שזקוקות לעיבוד חתימה בכמויות גדולות.

1 מודול אבטחת חומרה (HSM) פנימי או חיצוני - עם תמיכה בתקני FIPS לאלגוריתמי PQC

מודול אבטחת חומרה (HSM) מגן על חתימות דיגיטליות מפני שינוי על ידי שילוב תהליכי הצפנה מאובטחים. Signer PQ כולל HSM של יצרנים המובילים בעולם - Utimaco, nCipher, Thales ואחרים. כל ה-HSMs הנם בעלי אישור של לפחות (140-2) FIPS רמה 3 (CC ELA4+).

2 גישה קלה לחותמים מורשים

ניתן לסנכרן חותמים מורשים באופן אוטומטי דרך שירות ה-active directory של הארגון או על ידי העלאת פרמטרים וקבצים שונים של מסדי נתונים המנוהלים באמצעות Dash Board של אפליקציות אינטרנט.

3 פתרונות של סיסמה חד פעמית (OTP) או הזדהות ביומטרית (באמצעות פנים או אצבע) להגברת האבטחה

כדי להגן על שרת SIGNER PQ מפני התקפות סייבר מתקדמות, משתמשים מבצעים תהליך אימות מאובטח דו-שלבי תוך שימוש באמצעים ביומטריים או (ONE TIME PASSWORD) OTP כדי לקבל ולאשר גישה מאובטחת למפתח הפרטי השוכן בשרת החתימה.



תכונות נוספות

- תמיכה בתקני FIPS206 | FIPS203, FIPS204, FIPS205
- חתימות PAdeS תואמות ל-eIDAS
- חתימת CAPI עם תמיכה SHA256/SHA512 בכל פלטפורמות Windows
- חתימת PKCS#11
- אפשרות הוספת שרת עם חותמת זמן דיגיטלית התואם ל - RFC3161
- הגדרת תצורה מבוססת פרופיל
- תפקידים מבוססי Active Directory להגדרת המערכת וגישה למפתחות בנוסף לאימות PIN/PAD מול התקן החומרה
- תמיכה בהתקני יצירת חתימות מאובטחות (Q/SSCD) ומפתחות תוכנה
- תמיכה בפורמטים מקוריים של חתימה של PDF, OpenXML, XML, של OpenOffice, Word, PPT, Excel
- כלי Multipage TIFF מוטמע לחתימה ואימות
- ביקורת ורישום של כל פעולות החתימה והמערכת
- תמיכה בקבצים גדולים
- תמיכה בחתימות PKCS#7 נפרדת
- רישום מרכזי
- הצבת גרפיקה חזותית בתצורת הפרופיל
- כלי תיקוף חתימה
- תמיכה ב-SNMP



CONTACT US



www.comsigntrust.com



*8770



info@comsigntrust.com



[Comsigntrust](#)