Datey Check(שם זמני)

עולם הבעיה:

כיום לא ניתן לדעת בצורה ודאית מתי קובץ כלשהו נוצר.

מערכת ההפעלה windows מאפשרת לבדוק מתי נוצר קובץ, מתי שונה ומתי ניגשו אליו (כפי שמוצג מטה). שדות אלו ניתן לשינוי בצורה קלה ופשוטה באמצעות קוד (לצרף קוד שמאפשר לשנות את הזמנים). בעיה נוספת במנגנון הנוכחי היא שהשעה הקבועה מתבסס על השעון של המחשב והוא כמובן גם ניתן לשינוי בצורה פשוטה מאוד ואי אפשר לוודא שהוא בכלל מכוון לשעה האמיתית.

Created:	Friday, 2 June, 2017, 1:34:39 PM
Modified:	Saturday, 3 June, 2017, 8:25:49 AM
Accessed:	Saturday, 3 June, 2017, 8:25:48 AM

חזון:

ממשק אשר מאפשר לחתום על הקובץ ועל תאריך העלאתו, כלומר תאריך החתימה. בדרך זו יהיה ניתן לדעת באופן ודאי מתי נחתם המסמך. במידה וינסו לזייף זאת יהיה ניתן לאמת באמצעות גישה לממשק.

בדרך זו נוכל להכניס עוד אסמכתא משפטית אשר אינה קיימת כיום. במסמכים כתובים ניתן לזייף תאריכים בקלות רבה ובמידה ומסה קריטית של מסמכים יהיו חתומים כך מנגנון חתימה זה יוכל להוות אסמכתא.

דרך מימוש:

אופי השירות הינו אינטרנטי כיוון שכל תהליך החתימה מחויב להתבצע בצד השרת כדי להוות מקור אמין, אחיד ובעל יכולת בדיקה ואימות.

צד לקוח:

הלקוח יוכל להשתמש באתר שעליו יהיה ניתן לעלות קבצים ולהוריד אותם עם תוספת החתימה (יש לבחון כיצד ניתן לעשות זאת באמצעות הmetadata) . אופציה נוספת תהיה שימוש בתוכנה לוקאלית אשר תהיה מחוברת תמיד לאינטרנט (אחרת לא תעבוד) ותבצע את התהליך בצורה פשוטה יותר ללקוח, על אף שאת הפרטים הרלוונטיים תעביר לשרת בכל מקרה כי תהליך החתימה יתבצע בשרת בלבד.
בנוסף, עבור כל משתמש רשום יהיה איזור שבו יופיע הקבצים עליו חתם בעבר והזמן שבו חתם עליהם, הוא יהיה יוכל לספק אסמכתא חתומה מהאתר שהחתימה אכן נעשתה במועד שבעל הקובץ טוען.

צד שרת:

צד השרת יכיל DB אשר יחזיק בhashים חד חד ערכיים לכל פרק זמן מוגדר (יהיה צורך להחליט האם מדובר בדקות או שניות בהמשך כיוון שמדובר בגדלים עצומים). השרת יקבל hash מהמשתמש ויחזיר לו hash חדש אשר מתבסס על hash הזמנים ועל הhash שקיבל מהמשתמש.
בנוסף לכך, יש לבחון קיומו של מאגר ובו פרטים על כל הקבצים שהמשתמשים חתמו עליהם. בדרך זו יהיה ניתן לאמת בעלות נמוכה מאוד את מועד החתימה על הקובץ כיוון שהזמן יהיה נתון וכל אשר יהיה צריך לעשות הוא לבצע את הhash בשנית ולאמת מול מה שהמשתמש מעלה.

במידה ולא יהיה נתון הזמן שבו נחתם הקובץ (במידה וגורם אחר ירצה לוודא את אמינות הנתון שבעל הקובץ מספק לו למשל) יהיה ניתן "לנסות" את כל טווח הזמנים האפשרי שמציע המשתמש וכך לראות האם באמת הקובץ נחתם בזמן הזה או שמא נחתם בזמן אחרת. מדובר בתהליך יקר ורב משאבים ולכן יהיה יקר וייחודי בהתאם לבקשת הלקוח.

הכנסות:

1. הכנסות ממשתמשים רשומים אשר יחתמו על קבצים שלהם והנפקת אסמכתאות עבורם.
2. ההכנסה הגדולה תהיה ממשתמשים אשר ירצו לאמת את מועד החתימה של מסמך כלשהו וכך ינסו לשער מתי נחתם הקובץ והמערכת תנסה את כל האופציות ותחזיר להם תשובה האם הקובץ באמת ממועד זה או לא.

הוצאות:

1. אחזקת שרתי ענק אשר יריצו את החישובים הדרושים לשם החתימה.
2. אחזקת DB אשר יחזיק את פרטי המשתמשים ופרטי החתימה על הקבצים שלהם.