Future of Online Signatures: The One-Sign Feature[1]

Om Ranashing, Prateek Hajare, Hussain Sheikh
Department of Computer Science, AISSMS Polytechnic, Pune, MH, India

DOI:10.37648/ijrst.v12i02.002

Received: 14 March 2022; Accepted: 17 April 2022; Published: 17 April 2022

ABSTRACT

Have you ever messed up trying to sign a document digitally? If you did, then you know how difficult it is to use your index finger as a god-given stylus; To draw between those tiny exact spaces and redo it, again and again, in case the screen does not capture your finger drawn signature properly. Shouldn't there be a better convenient, hassle-free way to do this? Something that ensures authenticity, accountability, security, and at the same time doesn't feel like 'draw-wrestling'? Here we present our solution in the form of a software system as a hypothesis going by the name 'the One sign feature'. The feature is a cross-platform, profile-based, Sign Insertion method, which works when a password is successfully accepted, thereby inserting the sign on the document where selected. It is proposed as a solution to the "Small Screen, Too Much Work, Less Authenticity and Less Accountability" problem statement, which are common limitations of all the current solution offerings. The paper does a brief comparative study of all the popular technologies available in the industry used to digitally sign a document; discussing their drawbacks and drastic impacts of their limitations in terms of loss of money, productivity, and time. All this with the motive to prove that the 'Smart era' of Online Signatures is yet to come to its breakthrough and that there is still a wide opportunity gap for a system that could increase Data Privacy, overcome the limitations of the current systems, and eliminate loopholes.

Keywords - *Digital Signature, Document Certification, Signature Accountability.*

INTRODUCTION

The Markets have seen a sharp rise in the widespread adoption of Digital Contracts and Digital Documentation. Easily marking the biggest shift, as 'the era of Screens' took over. So much so that the global Digital Signature market is valued at a near 2.5 billion USD per year (Bloomberg global estimates) as the need to certify digital documents and maintain records is ever increasing. Institutions are investing heavily to make sure that their documents are either scanned or recreated as digital copies to cut down the costs of maintaining warehouses of critical documents. Companies that often struggled with the problem of maintaining a huge archive of documents, each signed on a date, have found their relief in the digital way of storing them. Why one may ask? As it not only reduces the major clutter of managing so much hardcopy data but also reduces the costs to maintain huge library-like archives with regular maintenance to battle the risk of paper documents being damaged by tears, pests, and moisture. Not to mention often these documents contain sensitive information and critical agreements which add to the risk of being stolen or misplaced. Out of all the paper agreements available in the world, only a few hold a billion-dollar asset valuation. Most are small case agreements between vendors to sales, service providers to clients, and employees to their employers; accounting for valuations under 200 thousand dollars at a time. Especially as the rise in freelance and outsourcing has also pushed for the sharp rise for online contracts and as the rise in online documentation increases, so does the need to sign them. But to the surprise of the industry, the digital signing procedure hasn't evolved as much as the Digital Contract has been for wide public usage. Only a few high authentication products like 'Passkey thumb drives' with biometric authentication access have shown limited usage to an ultra-rare target sector, for the rest of the public use the technology hasn't evolved much. The reason

[1] *How to cite the article:*
Ranashing O., Hajare P., Sheikh H., Future of Online Signatures: The One-Sign feature, IJRST, Apr-Jun 2022, Vol 12, Issue 2, 6-11, DOI: http://doi.org/10.37648/ijrst.v12i02.002

being many of these contracts are made on Microsoft-word (and similar publishing software) sent by mail, then signed as PDFs. This makes them hold very little accountability value, mostly these are declarations of terms and pricing as compared to strict to-be-followed constraints that could be contested in courts for consequences.

OVERVIEW

Current Market offerings to Online signatures are into limited technological advancement and rather trying to gain market access. Most tools provide the same functionality with similar interfaces and different Brand Names.

Mentioned here are majorly used provisions to commit to documents using online signatures:

A. Insert Signatures as Image/Scanned Image
To sign the document the user has to insert an image of its signature or scan a sign using a provided visual capture software via a smartphone camera, to extract a sign digitally.

B. Click and Draw-out Signature from a touch-screen or a track-pad
The user draws out a signature using a figure gesture or Stylus to sign the document, some variants convert the draw into an image and allow to drag and drop, to reposition the signature, others place it automatically in the "Signature-box".

C. Hash-input Pass-Key
In order to sign using this method the Creator of the document, inserts a hash key, on the document sign-box and The Signing user enters the key provided by the creator and if valid the document is signed.

D. Thumb Drive Access Key,
Which involves a thumb drive with a fingerprint scanner embedded in it. The Signing user is provided this "Key" physically, the drive holds encryption keys to the hash on the document. Once the drive is attached to a system it requests a password, if positive allows Signature access.

Another variant of this, works with biometrics usage, where after the system connection it requests for Biometrics access via an Embedded sensor on the Thumb drive, if the access is positive, the document is signed if, if not then there is an entry of failed signature, for next attempt.

E. Image Dragging
Here users use an image/document editing software to insert an image of their signature in the allotted space.

These are the major methodologies by which a document is signed. But they all hold different means of inefficiency and drawbacks that act as their limitations to market adoption. Each serves a niche limited market, creating an asymmetry in the signing outputs, to be viewed as evidence. For the masses there, the features provide no regard for authenticity, accountability, and efficiency. Some methods are nevertheless right out of the books of forgery, legal because the Signing authority is forging its sign onto a digital medium. Each of them holds limitations to their technology or methodology, which gives rise to a necessity for a better way to commit documents using Online Signatures.

NECESSITY

The process of digital signing hasn't taken as much innovation as expected. It's been the same as it was since the 2000s, the user has to use a finger to draw his/her signature over a screen and the screen captures it and places it in the document either or a different way. Going to devices such as desktop computers or laptops, it is very hard for the user to draw out a signature with the mouse movement, leading to bad signatures that don't represent the same value as they did when users signed on an actual paper. But despite these flaws as the smartphone got cheaper and the number of touch screens at a nominal price increased, digitally signing a document became an acceptable practice.

Even the big shipping giants like Amazon, Ebay, and Flipkart started to adopt this method, by addressing the flaw with their delivery boys carrying a separate tablet like a machine provided by the company which stood as a bigger platform to sign onto. But they soon realized that it affected the 'seamlessness' of the process. Being not only an expensive option but a feature that was negatively affecting the user experience. Another issue is, that there is no method to verify if the document was signed by the intended person or not, or did someone else sign it?

This part of the problem was solved by PDF applications. They integrated Digital Signing as one of their prime features, Acrobat being the popular one, placed a 'box' displaying 'Digitally signed by name-of-the-person on the date-time in the blank space provided, once the user successfully entered the passkey generated for it. That being a tedious process had its influence limited to a limited corporate-to-corporate sector or E2E documents, where the document Creator had to create a Hash

key and then share it with the person signing it, who would enter the key and 'sign the document'.

Then came the era of copy-pasting or inserting images of signatures into sign-boxes, especially when sending documents became a common institutional practice. Matching with directly forging your sign in a digital medium, leaving no regard for authenticity and accountability as evidence.

Until websites like *'Docusign'* and *'Singnaturely'* introduced a method to allow users to create form-like fields on their documents and get to manually sign on it, draw-their-signature-on-it. Again, asking the users to draw their signatures out, without the provision of proper signing hardware. Not only that but these platforms took the desktop signing out of the picture and made the user smart-phone and stylus dependent.

Hardware involving methods like The Biometrics thumb-drives or Thumb drive PassKeys stayed relevant only to top Legal firms and multi-million-dollar deals. As the cost and the effort of maintaining a biometric embedded thumb drive put a limitation on the masses, serving its 'Exclusivity and Security' proposes.

But still there remains a significant gap to fill in terms of reducing the effort of digitally signing at the same time, making the output more accurate enough to be used as credible evidence, for accountability. the 'Small screen, too much work, less accountability, and Less Authenticity' problem statement still is a long way from getting solved 'seamlessly' by an ideal solution.

METHODOLOGY

This part of the paper tries to solve all the aforementioned problem statements and highlights a few more by describing the Concepts of Proposed Alternatives in form of functionalities to a hypothetical Cloud-based Signing platform named 'One-Sign'.

The proposed 'One Sign' methodology tries to solve all the major issues to be the safest and yet the easiest way to digitally sign a document. The idea is to create a software platform or interface as a website or plugin for desktops and a mobile App or inbuilt functionality in the case of smartphones; Which will create a profile for the user to login into. To sign up the user would have to undergo device/identity user–verification (Confirm phone numbers and emails using OTP) to make sure of the user identity and uniqueness of the profile. (Authenticity).

Post User Identification, the system will ask the users to draw their ideal signature via touch screen draw and save it in their profile along with a password. The password could either be a 'screen-unlock like' pattern unlock functionality or a simple key password. The System will also serve as a 'Documentation File Manager' platform to register the stats of signing and record the time and date when the document was signed and by whom. To sign the document the user needs to be part of the platform and needs to hold a credible profile. (Accountability).

The Admin User' - a user who is creating these documents and requesting Signatures from other users; will use the platform to invite members to sign a document. The platform will allow the admin to generate a document with sign-box blank spaces and invite users by a uniquely sent mail link, which opens when given access by the admin on Discretionary Access Control.

When the Signing user receives the admin sent mail and opens the link to the document, he/she will select the area where they want to sign. This shall open a dialogue box to enter their password in the form of a Pattern unlock or a Passkey. Once confirmed positively the software shall automatically insert the saved signature from its profile in the selected area. Post-signing the system will also send a mail update, to the admin and the user who signed it as a digital certificate of signing the document.

Share Tracer Functionality

Usually signed documents are sent from one hand to another, from one office to another, ultimately landing in the storage and then either trashed or returned. While this is going on the Signing party, is completely unaware of where their critical information is going? Who is handling it? And who has access to it? Asking big questions on misuse, sharing, and confidentiality loss.

The One-Sign platform solves this by adding a 'Share Tracer' to the document. Whenever a signed document is shared with someone, its Admin and Signing user gets an update about it. So, after signing, if the admin or any user for that matter shares a document with someone (authority/individual/office/company), the Signing user is immediately notified about it by receiving details about the *Document Receiving party's* profile details, its system IP (location), and MAC ID in form of notification or profile record. The same is to happen when the document is edited or signed by someone.

Viewer History Functionality

Another sub functionality is to maintain the history of 'Document viewing'. It will display a history of user views on the document with its date and time stamp, mentioning the latest viewers. The main motive is, that whenever the document is shared, downloaded, edited, or viewed, the Signing parties and the admin should receive information about who is viewing their information and their details. (Boost to Transparency and Accountability)

Document Travel Route and Declaration of Access Features

There could be options to take Signing users' permission to share or download the document. Before signing the document, The Admin would have to declare the 'Travel Route' of the document as a prerequisite. It shall display a list of people, users, and their authorities who will have access to the document. With this, the Pre-requisite shall also display where the document is traveling to, its location, and where it will be stored (its data center).

Anyone apart from those who are mentioned in the Document Travel Route, wanting to access/print/download/screenshot the document needs Signer's permission. The platform shall also hold a history of real-time activity to the document, made available to admins and signing parties.

The Signing User's dashboard will also have provisions to display a list of documents the user has signed, been invited to sign, and its own created documents (In a table format). It shall also show the status of the signing (Mail-sent/Seen/Signed/Finalized).
If the authentication fails, due to a mismatch of passwords, or multiple attempts the admin receives real-time data based on it, on the dashboard.

The system approach is aimed at drastically reducing the efforts of signing; All the Signing user has to do is to open the document and then enter the pass or pattern unlock, and the digital signature is placed in the sign-box (Seamlessness and Effort reduction). But at the same time maintain high levels of Accountability and Transparency all with the motive to ensure Data Security.

One-ign For Computers Users

The major problem of desktop users is the absence of touch hardware. Meaning if any new control interface is required, it is to be bought as hardware and then attached to the PC, unlike the touch screens where the control interface changes with the system and app requirements. How this affects in case of Signing Digitally for PCs, is by putting a hardware availability entry barrier amongst users, to either connect their Desktops with some touch hardware like tracer-pads/ styluses or directly perform *draw-out-with-mouse*, where you hold the cursor and drag it on the mousepad simultaneously trying to draw your signature out on the monitor screen, which again does not work to acceptable standards. In the case of laptops even with the availability of touch-sensitive mousepads, drawing out a signature is never a good option to sign a document.

If not that, then they have to rely on creating pdf sign-hash-keys, which like access passwords, that once matched insert a block of text saying "Signed by user" and timestamp as discussed earlier. The easiest option and the most preferred one, unfortunately, is by inserting a Signature as an image, by dragging and resizing it in the sign-box blank spacing.

Also, the PDF signed Documents stand out from other paper signed documents if they are to be printed and be clubbed with as evidence, due to the absence of uniformity in the signature methods, they often to be left undetected for forgery.

With One-sign Desktop users could sign the document easily and seamlessly without having to go through the entire tedious process of creating individual keys or inserting images. The One-sign platform surpasses all these limitations, as it is cloud-hosted and supports multiple-device access at the same time. The user could create their profile using a touch screen device and sign documents from the desktop as well, where they just have to enter the passkey or pattern and the sign will automatically appear in the signature box. Making signing from desktops/laptops a viable option.

USER FLOW

User levels

a. Doc Admin: User that Creates the document and invites other users to sign it
b. Signing User: The user who signs the document once invited
c. Spectators: Users who can view the document
d. Sub Admin Access: Users who are not admins but can Add to the document or fill in the blank spaces.

Onboarding

1. Landing Site/Open app
2. User Sign up

a. Personal Details: Enter Name, birth date, Broad Country-State-City, Phone. NO (OTP), Email (OTP)
b. Username and Password creation
c. Profile Creation:
    I. Profile Photo upload
    II. Signature Draw-Out
    III. Confirm Details
1. User Login
1. Dashboard
1. Log-out

To Create Document

1. Login
2. Dashboard
3. Select: "Create Document" Option
4. Enter Titles, Texts, formatting, Signing Blocks, Edit if necessary, and Save to Directory
5. Select Document Accesses, Add users, Settings for Permissions, Enter Pre-requisites
6. Invite users via Mail text and email link to be the Signing Users/Sub admins/spectators
7. Back to the dashboard: Document Entry is available in the table of "Created Documents"
8. Updates about documents in the Notification Module
   Notifications Include:
    a. Signing Status (Viewed /Terms Approved-Signed/Rejected) with Date-time Stamps
    b. Document Failed to reach the Signing user's Mail (Invalid mail/Other Issues)
    c. Document View/Edit/Sign Activity History

9. Documents Settings to block/change view access, Settings to Delete/Finalize Document
   Once all the necessary users sign and fill in the details the document is "Finalized", The admin Clicks the "Finalize" button to lock the Document from Further Changes and sends a PDF of the signed copy to the Signing users.
10. Logout

To Sign a Document

1. Click on the Email received link
2. Login
3. Approve document Prerequisites
   Prerequisites Include:
    a. Document Description, Document status, Date-time of sent, and Unique Code of Identification
    b. See who else will be signing the document
    c. Date and time of document Creation and Expiry
    d. Document Route and Storage Database Details
    e. Termination details if the document was to be terminated after a certain period
    f. To whom are the Document Accesses provided and on-click opens their profiles
    g. Terms and Conditions of documents
    h. Approve To terms and Details (Sends updates to Admin about terms approval to view the document)
4. Opens Document
5. Select Sign Box to either sign / Reject Signing
6. Enter User and Pass
7. View Signed copy
8. Add a comment if necessary
9. Confirm submit
10. Document signed / Rejected Certificate Mail sent to Admin and respective Signing user's email
11. Back to Dashboard, Document entry found in the "Signed Documents" Table
12. Updates about documents in Notification Module: Document View/Edit/Sign Activity History

To View a Document

There are two types of Access approvals provided under Spectate Access by the Admin:

a. View Content Only (Allows the user to only view the Document Contents)

b. View on Complete Spectate (Allows user to see, Travel Path, members involved, authority, and access to commenting on the document)

1. Admin sets Access settings and sends a link to the respective user
2. Open Mail-sent Link
3. Approve Prerequisites
4. Opens document
5. Add a comment if necessary
6. Back to Dashboard
7. Document View entry Found under Viewed Documents Table

8. Notifications of 'View activity' sent to Admin, Sub Admin, and Signing User.
9. View History about itself as visible, in the system.

CONCLUSION

Global Electronic-Sign and online legal documentation Market is worth 2.5 billion USD by Bloomberg global estimates, ranging from all the applications to e-sign a document, to getting stock inheritance legality cleared using online verification. This paper compared Digital Documentation and Paper (Hard copy) Documentation of legal contracts, advocating for Digital acceptance. It also analyzed major electronic signature solutions available in the market and critiqued them for their inefficiencies and lacking in the current market solution offerings.

The Problem statement Factors found in the research were as follows:

A. Lack of 'seamless' User-experience in Digital Signing mediums,
B. Lack of accurate signature scanning mechanisms for wide-use smartphones and computers without the need to buy hardware
C. A significant gap in Easy-to-use Digital signing solutions for Laptops and Desktops,
D. Lack of Data Accountability of Signed documents
E. Ideal Solutions to deal with Hardware Limitations (The absence of large touch screens) are unavailable from current market offerings.

The paper also highlights the impact of these inefficiencies, in terms of User-experience, Customer satisfaction, Business practice, and hardware investments directly leading to monetary casualties.

The paper proposes the 'draw-once-sign-everywhere' concept. under the hypothetical example of the 'One-Sign' platform and some of its functionalities as a solution to the aforementioned problem statements.

Thus, we reach the conclusion, advocating for a much-awaited breakthrough in the market sector of Digital Signatures and leg-tech and Reg-tech.

REFERENCES

1. System and method for processing and for funding a transaction by Robert Minter Alexander IV, Charles Aaron Rosenblatt, Daniel R. O'MALLEY, Scott David Grimes https://patents.google.com/patent/US11244318B2/en?q=online+transaction+systems&oq=online+transaction+systems
2. Digitally signing documents using digital signatures https://patents.google.com/patent/US10880093B1/en?q=Document+signing&oq=Document+signing
3. Secure Sign: Signing Document Online: https://ieeexplore.ieee.org/document/8592954
4. 21 of the Best Signature Apps: https://blog.hubspot.com/sales/electronic-signature
5. Sign Word Online: https://zegal.com/blog/post/sign-word-document-online/
6. Online/Offline verification of short signatures by Yillang Zhang, Fuchun Guo, https://www.researchgate.net/publication/220848559_OnlineOffline_Verification_of_Short_Signatures
7. Benefits of Signing the documents Online by Laura Worrad https://lawpath.com.au/blog/benefits-of-signing-your-documents-online
8. 57 Essential e-Signature Statistics: 2021 Market Share Analysis & Data https://financesonline.com/25-essential-e-signature-statistics-analysis-of-trends-data-and-market-share/