PREFACE

Organizations are adopting electronic signature (e-Sign) to ensure compliance, security, and auditability in their efforts to accelerate daily work processes. Software providers that offer the automation of paper documents requiring signature are enabling e-Sign solutions every day.

If you are one of these 3,000+ software companies, consider the opportunity to control your own destiny and provide this key service as a tightly integrated part of your overall solution.

In this paper, we'll examine the pluses and minuses of using a white label e-Sign solution and its impact on you and your customers. Additionally, we'll put costs and opportunities to the test to determine if there is a competitive differentiator so you will make money in the process.

CONTENTS

e-SIGN – WHAT IT IS, AND WHAT IT'S NOT

An electronic signature, or e-Signature, refers to data in electronic form which is logically associated with other data in electronic form, used by the signatory to sign. This type of signature provides the same legal standing as a handwritten signature, as long as it adheres to the requirements of relevant law (e.g., eIDAS in the European Union, E-SIGN in the USA).

An electronic signature, done correctly, has the same meaning as an ink signature on paper, under laws and regulations.

Electronic signatures are a legal concept distinct from digital signatures, a cryptographic mechanism often used to secure electronic signatures. While an electronic signature can be as simple as a name entered in an electronic document, digital signatures are increasingly used in eCommerce and in regulatory filings to secure electronic signatures in a cryptographically protected way.

PAPER SIGNATURES ARE THE NEXT DODO BIRD

There many reasons organizations are quickly adopting electronics signatures, including:

- Lower cost
- Better audit trail and forensics
- Green initiatives
- Improved reliability and security
- Process acceleration
- Improved workflow management

Today, the overall electronic signing process can be handled simply and intuitively with any device, including tablets and phones. If your business or your customers are still using paper and pen, you need to evaluate the options of advancing your solutions before your competitors gain the advantage.

Market analysts like Gartner are predicting the continued 30-40% compound growth rate of the electronic signature market over the next several years. In fact, many industries have moved quickly, and ink signatures on paper are becoming a rarity.

TIME TO ACT

You're finally ready to evaluate options for your business- great. Let's look at some of the common options you have available:

1. Integrate with a commercial SaaS end-user solution, like Adobe Sign® or DocuSign®.
2. Integrate with an OEM specific solution, offering SaaS and in-stack (on prem).
3. Build your own solution.
4. Do nothing.

Each of these options, except for the last one of course, requires commitment and effort to execute. Let's examine the pluses and minuses of each option for your business.

Integrate with a commercial end-user solution, like Adobe Sign® or DocuSign®

Commercial, end-user solutions are cloud-based by definition and are self-branded. They allow for the manual or ad-hoc use case, where the user simply imports their documents to be signed and graphically assigns signing tasks to the participants. The solutions also offer API integration that would allow for a deeper connection, but still maintain their solution independence.

Pluses:

- These are well-known and trusted products. Your customers would likely already be aware of Adobe Sign and DocuSign and there is plenty of general support material available on the web.
- These products are cloud-centric (SaaS only).
- As end-user tools, these products have a vast array of supported, pre-integrated products out-of-the-box. This allows the end-user to select from a large list of available vendors for most any application.
- Users have a lot of options for direct licensing with both Adobe Sign and DocuSign, starting at $10.00 per month per user. These programs are targeted at the individual and often have functional limitations and transactional limits.
- If the customer is using this electronic signature vendor for other applications, they have the opportunity to aggregate their volume for all their use cases.

Minuses:

- These products are branded by the manufacturer. In other words, your customer will always know that they are using Adobe Sign or DocuSign, even if it is tightly integrated with your solution. You may be able to add logos and change color schemes, but you cannot hide their cloud URLs nor the inevitable control mechanisms they implement.
- Customization and optimization features are generally offered at a higher price per transaction for these products. Even items as simple as reminders or notifications are not available at the lowest price points. These are highly fragmented products that require significant effort to accurately price for most applications.
- DocuSign reports to having over 1,200 product integrations through their efforts or that of partners. How many of those products compete with yours? Are the other integrations functionally better? Do they offer your customer a reason to change?
- Customer control is lost, as your customer will be required to license their electronic signature volumes from the commercial supplier. In this case, your customer will likely have to work with multiple salespeople and maintain multiple contracts. The support will generally fall to you, as your application is the key interface that the customer is using- even when the problem lies with the electronic signature vendor.
- Sensitive customer data will reside in two systems (yours and the e-Sign vendor – as sensitive data is typically added to documents requiring signature). This makes compliance and risk management more complex for your customers.

Making Money:

Monetizing this type of relationship is difficult to quantify and produce results. While you make money selling your solutions, you don't make any on the halo effect that you extend for the electronic signature vendor. The general result is a net gain of zero with a possible downside if there are support complications. If your solutions require electronic signature, using a commercial end-user SaaS solution may not be in your best interests.

Integrate with an OEM specific solution

There is a new breed of electronic signature solution that is focused on providing software manufacturers with the benefits of building on their own, but without the hassle and cost. In this example, a software company would include the electronic signature platform as part of their technology stack as a natural extension of their existing product(s). There are six key questions to ask that differentiate an OEM specific solution from a more traditional bolt-on:

- **Who controls the customer interaction?** For most software manufacturers, the answer they want is themselves. While that sounds simple, this is contrary to the typical interaction you see with commercial electronic signature products. If you want to control the sales process, pricing, marketing, and all the customer business interaction, an OEM specific solution may be your only choice.
- **Is the integration seamless?** Asking your customers to do something that is neither intuitive nor natural may accelerate their departure from your products. A consistent user experience is critical for both adoption and long-term success.
- **Does this solution enhance your brand?** During the electronic signature process, is the user experience seamless or do your customers feel like they have jumped to a new site altogether? Has the look and feel of the experience changed, potentially causing confusion and lessening your brand?
- **Does the solution allow you to brand and your customers to sub-brand?** As a software company, you want your brand to be front and center. Your customers, however, will want their brand to be present when they are working with their signing participants. This concept of branding and sub-branding is not common among electronic signature vendors but is a critical implementation detail for software companies looking to deploy a white label solution.
- **Do you have the tools to be successful with this implementation?** Being in control of sales and marketing with this new tool requires a basic foundation of support. Can your electronic signature provider provide selling tools (user documentation, presentation materials, modifiable content, FAQs, etc.) to help your sales and marketing team be effective?
- **Is your provider a vendor or a partner?** Does your provider seek your input and can or will they make foundation product changes to accommodate your requirements? What does happen when a client needs functionality that they currently do not provide?
- **Can you meet your customer's compliance and risk management needs?** Your solution has to pass muster with your client's security, legal, compliance, and risk management requirements. Now you have to double that with an external SaaS e-Signature vendor. Being able to maintain full control of your customer's data is a differentiator for you.

Build your own solution

While there are many companies that have completed or attempted to complete this approach, cost becomes the major barrier to its effectiveness. Let's examine some of the core components that are required to understand how to build a regulatory compliant electronic signature solution:

- A deep and vast knowledgebase of electronic signature legislation and regulations. Requires dedicated resources to keep up to date regarding US, state, or foreign government regulatory standards.
- Strong technical implementation knowledge of the technical standards required to build and maintain such an application.
- A cloud infrastructure sufficient enough to be able to house and maintain electronic signature operations and historical data. This must include both the physical security but also the operational security capable of

meeting the necessary standards (such as SOC 2 compliance).

- The technical resources necessary to architect, build, maintain, and modernize the applications.
- The technical resources necessary to devise, build and maintain the connectivity to other applications within your infrastructure that need to consume electronic signatures.

In summary, even many of the largest use cases do not justify the costs associated with building and maintaining their own private implementation. In fact, if your organization already has its own private implementation, we encourage you to evaluate the costs of maintenance in the marketplace vs. the option of using existing infrastructure.

Pluses:

- The top reason that any software company would build their own electronics signature solution would be to have total and complete control over the finished solution. However, many of the legal and regulatory requirements must be met for the solution to be considered compliant.
- With total control of the development, you would have the ability to build and maintain new features that you require that are not available in other solutions.

Minuses:

- The total cost of ownership is almost always an order of magnitude greater than that of using existing solutions.
- Time to market is significantly longer than licensing existing solutions.
- General acceptability in the market is lower due to the lack of existing customer experience and alternative use cases.

Making Money:
Options for creating positive cash flow while building and maintaining your own electronic signature solution could be years in the making or not at all. Companies that build and maintain their own electronic signature solution generally do so for non-monetary reasons.

Do nothing

The total number of products currently integrated to one of the several commercial electronic signature records is well over 2,000. If your product or solution requires the ability of an electronic signature, doing nothing is not likely a viable alternative. Your customers will either tell you what they need, or they will leave for other products that support the functionality their businesses require.