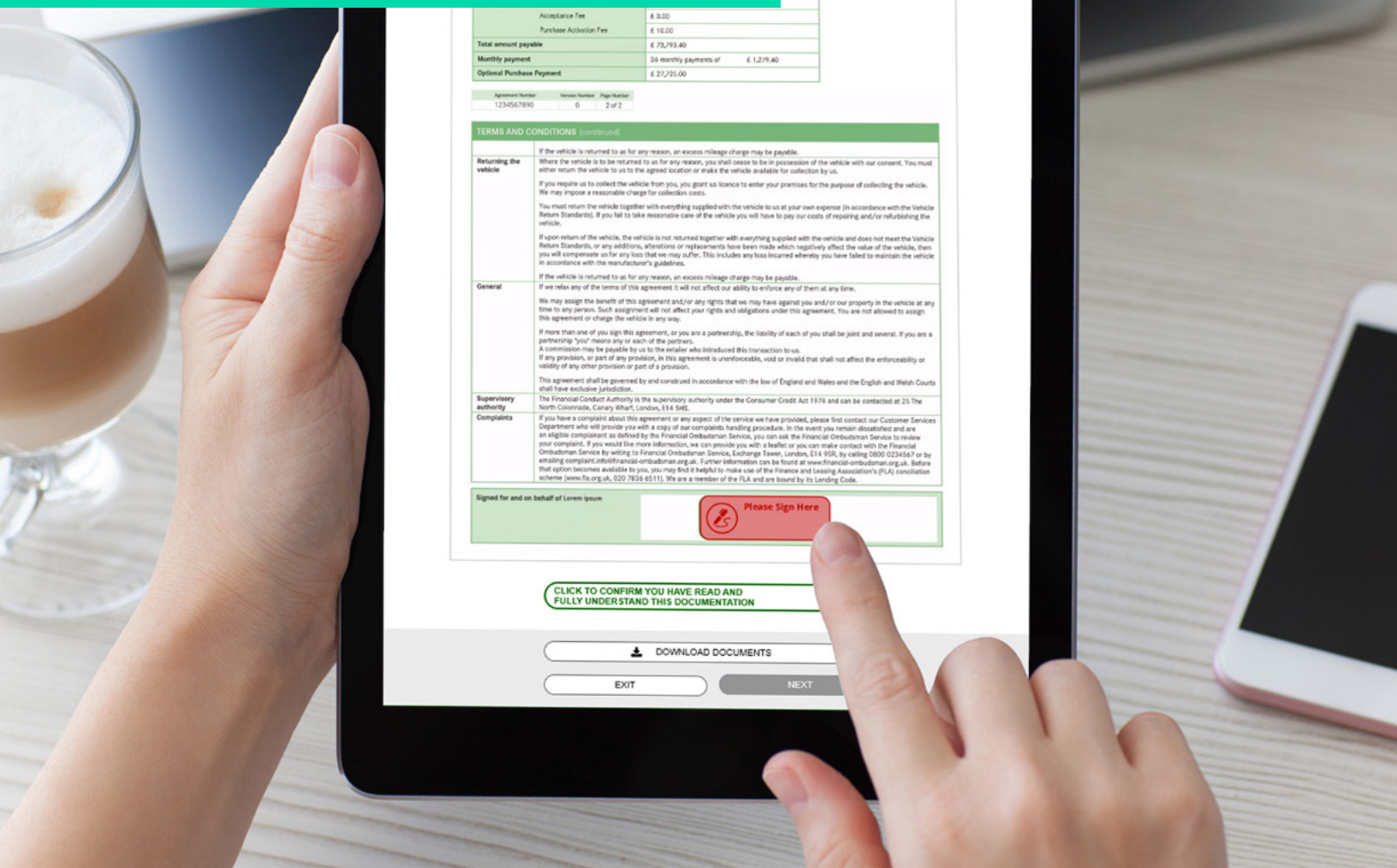


BEST PRACTICES FOR BUILDING YOUR E-SIGNATURE WORKFLOW FLEXIBLE OPTIONS FOR ENSURING EASE-OF-USE AND HIGH ADOPTION

WHITE PAPER



Acceptance Fee	£ 9.00
Purchase Activation Fee	£ 18.00
Total amount payable	£ 73,793.40
Monthly payment	36 monthly payments of £ 1,279.40
Optional Purchase Payment	£ 21,725.00

Agreement Number	Version Number	Page Number
1234567890	0	2 of 2

TERMS AND CONDITIONS (continued)	
Returning the vehicle	<p>If the vehicle is returned to us for any reason, an excess mileage charge may be payable.</p> <p>Where the vehicle is to be returned to us for any reason, you shall cease to be in possession of the vehicle with our consent. You must either return the vehicle to us to the agreed location or make the vehicle available for collection by us.</p> <p>If you require us to collect the vehicle from you, you grant us licence to enter your premises for the purpose of collecting the vehicle. We may impose a reasonable charge for collection costs.</p> <p>You must return the vehicle together with everything supplied with the vehicle to us at your own expense (in accordance with the Vehicle Return Standards). If you fail to take reasonable care of the vehicle you will have to pay our costs of repairing and/or refurbishing the vehicle.</p> <p>If upon return of the vehicle, the vehicle is not returned together with everything supplied with the vehicle and does not meet the Vehicle Return Standards, or any additions, alterations or replacements have been made which negatively affect the value of the vehicle, then you will compensate us for any loss that we may suffer. This includes any loss incurred whereby you have failed to maintain the vehicle in accordance with the manufacturer's guidelines.</p> <p>If the vehicle is returned to us for any reason, an excess mileage charge may be payable.</p>
General	<p>If we relax any of the terms of this agreement it will not affect our ability to enforce any of them at any time.</p> <p>We may assign the benefit of this agreement and/or any rights that we may have against you and/or our property in the vehicle at any time to any person. Such assignment will not affect your rights and obligations under this agreement. You are not allowed to assign this agreement or charge the vehicle in any way.</p> <p>If more than one of you sign this agreement, or you are a partnership, the liability of each of you shall be joint and several. If you are a partnership "you" means any or each of the partners.</p> <p>A commission may be payable by us to the estate agent who introduced this transaction to us.</p> <p>If any provision, or part of any provision, in this agreement is unenforceable, void or invalid that shall not affect the enforceability or validity of any other provision or part of a provision.</p> <p>This agreement shall be governed by and construed in accordance with the law of England and Wales and the English and Welsh Courts shall have exclusive jurisdiction.</p>
Supervisory authority	<p>The Financial Conduct Authority is the supervisory authority under the Consumer Credit Act 1974 and can be contacted at 25 The North Colonnade, Canary Wharf, London, E14 5AF.</p>
Complaints	<p>If you have a complaint about this agreement or any aspect of the service we have provided, please first contact our Customer Services Department who will provide you with a copy of our complaints handling procedure. In the event you remain dissatisfied and are an eligible complainant as defined by the Financial Ombudsman Service, you can ask the Financial Ombudsman Service to review your complaint. If you would like more information, we can provide you with a leaflet or you can make contact with the Financial Ombudsman Service by writing to Financial Ombudsman Service, Exchange Tower, London, E14 9GB, by calling 0800 0234567 or by emailing complaint.info@financialombudsman.org.uk. Further information can be found at www.financialombudsman.org.uk. Before that option becomes available to you, you may find it helpful to make use of the Finance and Lending Association's (FLA) conciliation scheme (www.fla.org.uk, 020 7836 6511). We are a member of the FLA and are bound by its Lending Code.</p>

Signed for and on behalf of Lorem Ipsum

 Please Sign Here

CLICK TO CONFIRM YOU HAVE READ AND FULLY UNDERSTAND THIS DOCUMENTATION

 DOWNLOAD DOCUMENTS

EXIT

NEXT



TABLE OF CONTENTS

Executive Summary	3
Standard Steps in the E-Signature Workflow	4
Step 1: Access	5
Step 2: User Identification and Authentication	7
Step 3: Presenting the Documents	9
Step 4: Forms and Data Capture	10
Step 5: Document Upload and Update	11
Step 6: Signing	11
Step 7: Document Delivery	14
Conclusion	15



EXECUTIVE SUMMARY

Today, customers expect companies to be easy to do business with. They want everything to be available quickly, at their convenience, in their preferred channel, and on their preferred device. Few people have time to drive to an insurance agency, bank branch, or government service center just to sign a piece of paper – especially when a few taps on a mobile device or a few clicks of a mouse can produce the same legally enforceable contract.

Most customers see the lack of paper as a burden being removed, but simply offering a digital process is not enough to guarantee a great user experience. People who apply for a loan, insurance policy, or government permit through your self-serve portal will experience the transaction differently than those who transact in person with an employee or remotely with the help of a call center agent. So the question becomes: how do you build an optimal user experience across all channels, while ensuring compliance? And as you think about all the opportunities to go digital across all channels, what is required to build e-signatures as a shared service across the organization, considering the many diverse signing processes in each line of business and channel?

The answer is flexibility. An e-sign platform should offer flexible workflow options based on years of customer feedback and industry experience. This white paper explores those options by going step-by-step through the e-signature process. We explain why some options are better than others in delivering the best overall customer experience for a given use case, along with real-world examples. We'll answer questions like:

- What is the best way to authenticate signers?
- What workflow mistakes can result in signer abandonment?
- Do you build the e-sign workflow to be device-specific?
- When and why should you capture a digital image of the signer's handwritten signature?

Standard Steps in the E-Signature Workflow

Most people view e-signature technology as a means of capturing consent, but an e-signature solution actually does much more than this. In order to produce an enforceable end result, an e-signature solution must be able to manage the entire signing process end-to-end. That includes the following steps:

1. Give signers access to the documents
2. Identify and authenticate signers
3. Present documents for review in a compliant form
4. Capture data from participants and/or upload documents at the time of signing (if applicable)
5. Optionally reverify the signer's identity at the time of signing
6. Establish intent and capture consent through the act of signing
7. Provide the ability to insert additional documents into the transaction (if applicable)
8. Deliver the final signed documents to all parties

To ensure high user adoption, we recommend looking for an e-signature solution that offers options for configuring each of these steps to fit your process, channel, and use case. Some options will be better than others in delivering the best overall customer or user experience for your requirements.

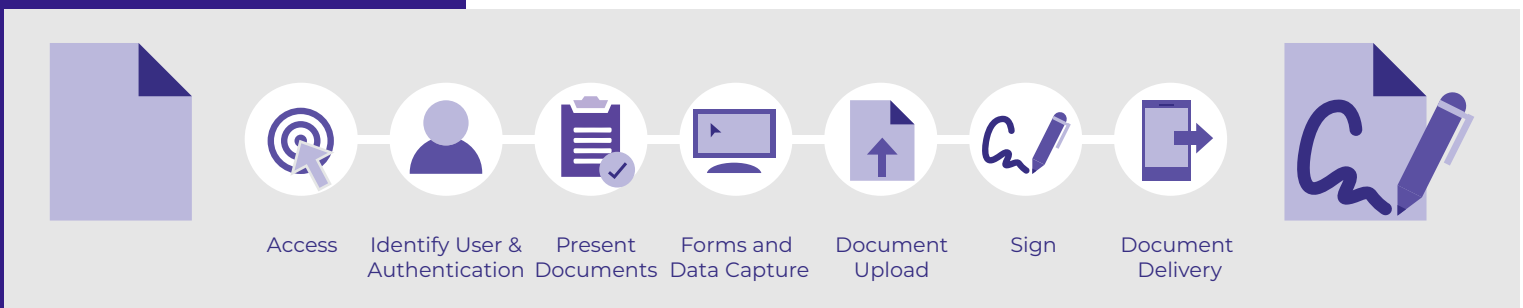


Figure 1

As a general rule, most of your decisions about which options to choose will come down to whether e-signing is taking place:

- Remotely on the signer's own device, or
- In-person on a corporate- or agent-owned device that is shared with the customer

Figure 1 represents the typical steps in any e-signature workflow and will anchor our explanation of what options are available for each step. It is worth noting that not every workflow will include all seven steps. There will be use cases that do not require steps four and five as part of the process. In addition, you will not always need the e-signature platform to manage all steps for you. As you'll see throughout this paper, some steps can be managed by other systems you already use. To customize the process and create an optimal user experience, it's important to have the flexibility to include, exclude, and adapt each of these steps.

Let's look at the options and best practices for digitizing different types of use cases.



A NOTE ABOUT EMAIL INVITATIONS:

Research shows that 43% of email recipients will delete a message based solely on the email address or “From” name. To avoid such a high level of abandonment, best practice is to select an e-signature solution that enables you to customize emails with your logo, colors, and design. The actual domain from which emails are sent should be branded with your company name. The same applies to the “From” and “Reply-to” email headers.

Step 1: Access

Once a document is ready to be e-signed, how will your signers access it? While many people assume that the entry point will be email, it is just as common to see direct integration scenarios where the e-signature process is integrated in a web or mobile application. The choice of access method depends on factors like:

- Is this a face-to-face or remote use case?
- If this is a remote use case, are your signers already online or not?
- Will you integrate e-signatures with another web application or portal, or do you need an integration-free solution?

For most organizations, the goal is to change as little as possible in the existing process. If signers are coming to you through the call center, then it makes the most sense to have the call center rep send them an email invitation. However, if signers are coming to you through a web app, then providing access to e-signatures through that app will logically create the best customer experience.

At the same time, while some of the options listed below will make sense for your initial e-signature process, you may be considering extending e-signatures to other departments in the future. The trend we see among our customer base is customers grow their use of e-signatures across the organization by an average of 22 percent each year. While access via a web, mobile, native, or third-party app may not be an immediate requirement, it will likely become so in the future. With a flexible e-signature platform, you'll be able to easily make changes in the future as your needs and technology environment evolve.

Remote E-Signing

When signers come into the transaction via a browser, best practice is to bring them to a secure site. An email invitation to bring the signer into the transaction is fine, but it is never recommended to email documents as attachments due to privacy risks and support issues.

Whether your signers are external (e.g., customers, suppliers, independent agents) or internal (employees), they will need access to the documents. Your options are:

- 1. Email invitation:** Send your signers an email with a link back to the e-signature login page.
- 2. Invite signers to login to a web portal or web app** and access the documents there. This could be a bank's customer portal, an insurance carrier's agent portal, or your company's employee portal.
- 3. Link embedded in any native or third-party application:** E-Signatures can be integrated with any application. You can add an e-sign button to your core systems or even cloud applications like Salesforce, and that button can take signers directly into the signing ceremony.
- 4. Link embedded in a mobile app:** You can add an e-sign button to your mobile app. Many organizations don't want to ask the customer to download a standalone e-sign app that is separate from the organization's app. By using a mobile e-signature software development kit (SDK) to integrate e-signatures directly into a proprietary app, the customer is able to access their documents directly through the app.
- 5. QR code or shortened URL on an advertising poster or any print document:** This is used primarily when trying to sign up new customers (e.g. application forms) in the field, during events, etc. The customer scans the code and opens the signature process on their phone.

Note that all of the above options (with the exception of email invitation) involve some level of integration. However, there is another integration-free option known as “Fast Track”. If your organization doesn't have an IT department or if your IT team does not have the bandwidth to take on another project, there is a simple way to enable employees or agents to initiate a remote e-sign process. “Fast Track” was created so your employees could easily take a prebuilt document template that already contains placeholders for the name and signature fields, and quickly send it out to the signer without much manual work.

This is different from accessing the documents through a web app or web portal, for example, because Fast Track does not involve any integration. The Canadian Olympic Committee is using this option to give athletes and volunteers [access to the onboarding documents](#) they need to sign to participate in the Pan Am and Parapan Am Games.

In-person Use Cases

In a face-to-face scenario, an employee or company representative initiates the signing process through an enterprise application portal or dashboard. He or she then shares the company device with the customer and the signing takes place on that device.

There are many in-person use cases where the customer is guided through the electronic signing process by an agent or company representative. One example is BMW Financial Services. For their end-of-lease process, dealers and customers do wear-and-tear inspections together using a company iPad to document vehicle damage. The dealer generates the proper documents on his or her iPad right on the spot and passes the tablet to the customer to use for document review and signing. The customer doesn't do anything to access the transaction; the employee does it for them.

In face-to-face transactions, there is never any guarantee that the customer will have a laptop or mobile device onhand which they can use to immediately review and e-sign documents. You want to complete the signing process while you have the customer in front of you, which is why it generally doesn't make sense to send the customer an email invitation like you would in a self-serve web-based transaction. And while there are in-person use cases where you will want to leverage the customer's own device for the act of signing, it is advisable to have the rep access and initiate the transaction on behalf of the customer.

Multiple Access Points in the Same Transaction

Look for an e-signature solution that can support multiple signers coming into the same transaction through different channels. For example, the first signer may be on-site at a bank branch, but additional signers may be invited to e-sign remotely via email invitation. This is convenient for transactions involving spouses, business owners, and student/parent co-signers, since all parties do not have to be on-site together (or even on-site at all).






Step 2: User Identification and Authentication

When the signer arrives at the e-signature welcome page, how will they prove their identity in order to securely enter the e-sign session? The options you choose will depend on the type of transaction, the risk involved, and whether you are dealing with a new or existing customer.

New Customers

In the case of a prospective customer or new applicant who does not have a previous relationship with your organization, your organization must have a method of verifying the applicant's identity documents. This can include a proof of residence, passport, driver's license, state-issued ID, or other uniquely identifying documents. With new technology and regulations, such as the U.S. MOBILE Act, you can now digitize the ID verification process and securely identify a remote, unknown applicant. Harnessing the power of mobile devices, your organization can accept a scanned copy of the customer's photo ID and use digital identity verification such as that offered through the OneSpan Verification Hub (V-Hub) to verify its authenticity.

Identity Verification for New Customers		
Check Type	Description	Go-to-market Partners
ID document capture & verification	Verification of the validity of a document image (e.g., driver's license, passport, etc.) at an algorithmic level	US & EU Mitek & Jumio  
Face comparison	Biometric verification ("selfie") of applicant against a verified official photo-identity document	
One-time passcode (OTP)	Transmission of a one-time, single-use passcode via SMS or email for subsequent entry by the applicant during a signing or verification process	

Existing Customers

With existing customers, best practice is to use credentials that your organization has already issued. In this case, you may not even need to authenticate the signer through the e-signature platform. If the signer comes in through a customer portal (e.g., an online banking portal), they will have already entered their existing banking credentials and will already be authenticated. In that case, there is no need to re-authenticate again during the e-sign session. This is an example of why it's important that the e-signature platform offer the flexibility to exclude steps from the workflow if they are being handled by another system.

However, this is a general rule and there are exceptions. In certain industries and use cases, the signer must be re-authenticated each and every time their signature is required. As an example, CFR 21 Part 11 requires that certain use cases in the health sciences industry must involve user re-authentication every time the signer applies their signature to the document.

Tips to Increase Adoption

Look for an e-signature solution that works with whatever authentication technology or method you already have in place and provides the flexibility to adapt the authentication to any requirements. An e-signature solution that supports a wide range of options enables you to calibrate the level of authentication to the risk

associated with the process. This is important, because it will help you balance authentication with usability to ensure an optimal user experience. According to [Forrester Research](#), “[E-Signature] Adoption will depend on the customer experience that you provide. Authentication that relies on complex credential challenges will lower adoption significantly.”

Overly complex authentication is one of the biggest sources of customer drop-off. Having a wide range of authentication methods and the ability to configure them according to your use cases makes it easier to provide a fast, seamless, and secure experience. This includes:

- Using digital identity verification for new applicants and authentication for existing customers
- Ability to adapt the identification and authentication to each signer (you may have a new and an existing customer involved in the same transaction, e.g. spouses opening a joint account)
- Adapting the authentication for staff/agents, so they can be authenticated differently from customers
- Ability to configure different authentication methods within the same transaction

Authentication for Existing Customers			
Options	Description	Remote	In-person
Login Credentials	<ul style="list-style-type: none"> • Signer is authenticated by the sending party's system prior to accessing the e-signature transaction (e.g., through a customer portal which requires a username/password). • Customer logs in to their account once and is considered authenticated. 	✓	
Email Authentication	<ul style="list-style-type: none"> • An email notification sent to a signer's corporate or personal email account presumes only that person has access to the account. The authentication happens when the signer logs into their email account. This, combined with the fact the customer clicked the link in the email, establishes a connection to the signer and helps validate his/her identity. 	✓	
Static Knowledge-based Authentication (KBA)	<ul style="list-style-type: none"> • Knowledge questions are presented to the signer. These are commonly referred to as “shared secrets” since the sender needs to know something about the customer to establish the questions. The two parties will often agree to the answers over the phone before initiating the transaction. Common questions include last four digits of a SSN, application ID number, etc. The customer must correctly answer the question(s) before being given access to the e-signature transaction. 	✓	
SMS Authentication	<ul style="list-style-type: none"> • A unique PIN is automatically generated by the e-signature service and sent to the customer's phone. The signer enters his/her PIN into a web page to authenticate. 	✓	✓
Digital Certificates & Smart Cards	<ul style="list-style-type: none"> • In the U.S. government, personnel and contractors routinely e-sign forms on a desktop PC, laptop, or iPad, using a digital certificate that is stored on their Common Access Card (CAC) or PIV smart card. In Europe and other parts of the world, signers may use a Qualified E-Signature enabled by a third-party digital certificate stored on a smart card or similar device. 	✓	✓



Step 3: Presenting the Documents

Next, determine how you will present documents to signers, so they can read them before signing. The options are simple: present documents on-screen or on paper.

In most cases, it makes sense to present documents on-screen, since not everyone will have the ability to print out documents. Even if they do, it is difficult to be sure the print copy will comply with regulatory rules. Best practice is to have the e-signature service present documents through a web browser. If the signer needs nothing more than a browser, then they won't have to download any new software, which eliminates the risk of software incompatibilities. You can always print out copies if it's easier for signers to review documents on paper, but document presentation on-screen needs to be built into the process.

Why Go Back to Paper?

While presenting documents for review on paper may seem to defeat the purpose, you should have the flexibility to accommodate paper when necessary, even in a “paperless” digital transaction. We've seen situations in face-to-face channels, such as in-branch, retail point-of-sale, and home meetings with insurance representatives, where customers find it easier to read printed documents. In these situations, you should be able to adopt a hybrid approach. Your e-signature solution should give you the ability to provide customers with a paper review copy, while still using a computer or mobile device to capture the customer's e-signature, so the process moves forward electronically.

Consider a hardware store offering financing for major purchases. E-Signatures allow the retailer to close business directly on the store floor by presenting the customer with a printed financing contract with a QR code. The customer reads the documents and, when ready to sign, scans the code using their smartphone. This allows them to enter a few key pieces of information and then provide their handwritten signature through their own touchscreen device.



The QR code uniquely links the paper version of the contract to the e-signed electronic contract, and the e-contract is submitted immediately to the finance company for processing – all without any special equipment or extensive integration with your core system.

Presenting Documents through a Mobile Browser

We continue to see a surge in the number of people combining mobile devices with e-signatures. Web-enabled tablets have become an especially popular method of presenting documents to clients during face-to-face interactions with agents. Devices like the iPad facilitate the document review and signing process with relatively larger screen sizes.

For organizations subject to regulatory rules regarding the exact appearance of customer-facing forms and documents, this is a critical step in the workflow. This is even more true for organizations that want to transact with mobile customers, considering what worked well with paper does not always apply the same way on a mobile device. Signing documents on smartphones presents unique challenges due

to the limited screen real estate. In this case, look for an e-signature provider that takes a “mobile-first” approach for smartphones and tablets, with:

- A responsive design where document display is adapted to each device to ensure an optimal user experience (no need to build a device-specific workflow)
- The ability to pinch and zoom, especially to read fine print
- A user friendly mobile interface with navigation buttons that are easy to find
- A simple view that pulls out associated fields from a multi-page document so users can easily confirm information



Step 4: Forms and Data Capture

As part of the signing process, you can add data fields (text fields, check boxes, radio buttons, etc.) to the document for signers to fill in. While most e-sign transactions begin at the point when a final document is created (forms data is captured as part of an e-app or other core application and merged with a document template) there are processes where you need the ability to capture data **at the time of signing**. The e-signature solution must be able to support this capability. Simple examples include insurance applications where the signer is asked to confirm supplementary coverage options at the time of signing or contracts where the signer is asked to check a box to confirm agreement with the terms and conditions. In all cases, that data becomes part of the document and is secured with a tamper-evident digital signature.

The data capture capability can also be used more extensively. If you do not have a web portal or application built to electronically capture forms data, this should not prevent you from benefitting from e-signatures. Form fields can be used in the e-signature transaction to capture all the data needed for the process. When integrated



with a CRM or other systems, the data can be extracted from the signed document and made available to these systems.

Step 5: Document Upload and Update

In certain business processes, you or your customers may need to add documents to a transaction. This is common in insurance, where an insurance carrier's independent field agents often have their own documents to add to a new business application process. These are often non-standard legal documents supplied by the customer, such as a power of attorney form, medical report, or other documents that are not included in the typical application forms package. Once the agent has received the document from the customer, he or she should be able to upload a scanned version to the e-signature service and insert it into the transaction. Other examples include a credit union member application where the new member is asked to provide proof of affiliation with a university or employer, or any e-commerce transaction where the signer may need to show a membership card to receive a discount.

Step 6: Signing

This is the step in the workflow that people most often think about when they imagine e-signatures – the “clicking” to sign. It is a very important step in the process, since this is the moment that you are capturing intent. Once again, however, there are different ways to accomplish this.

Which signature capture method best suits your process? There is no one-size-fits-all answer. It all depends on the process being automated. The ideal is to choose an e-signature service that offers multiple signature capture options. If your e-signature solution limits you to one method of signing, this will affect adoption. For example, you may want to capture a hand-drawn signature, but if the software supports only a click-wrap or click-to-sign, you would be limited in the types of processes you could automate.

Best practice is to pre-set the type of signature capture required for your process, rather than leave it up to the customer to decide.

There are three types of signature methods available depending on the hardware that is being used:

Click-to-sign: In the browser on a PC, laptop, or mobile device, it is common to use a simple “click-to-sign” or “tap-to-sign” button.



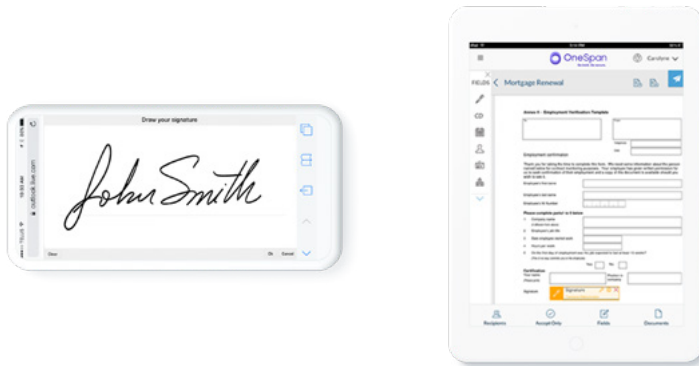
“

It's like when you walk into the Apple store and you have to sign something, they bring out the iPad and you sign that. It's just the way we do investment banking at RBC.

”

Keith Wilson
Senior Manager Business
Technology Strategy,
RBC Royal Bank

Digitized handwritten signature capture: If a touchscreen device is available (e.g., tablet, phone, or dedicated signature capture pad), then cursive signature capture can be used. In this case, a dialog box opens allowing the signer to sign their name much like in a retail transaction or when signing for a courier package. The e-signature solution should allow signers to use their own device to draw their signature on the go.



Smartcard signing: U.S. government personnel and contractors routinely e-sign forms and documents using a digital certificate that is stored on their Common Access Card (CAC) or PIV smartcard. In Europe and other parts of the world, signers may use a Qualified E-Signature enabled by a third-party digital certificate stored on a smart card or similar device.



Before choosing which signature capture method best suits your process, the first step is to understand that a signing process must ensure the conspicuous capture of intent. The placement of signature cues is very important. You want these buttons to be directly on the signature line, not adjacent to the signature block. You also want to give signers the ability to opt-out of the process if they prefer to drop back to paper.

Other important considerations:

- **The needs of your employees, representatives, and agents.** Choose a means of capturing signatures that supports their way of working. Use devices that enhance the experience rather than detract from it. Ideally leverage devices that can serve multiple purposes. For example, a tablet like an iPad can be used to capture data, review documents, and capture signatures.
- **The needs of your customers.** Choose a signing method that supports the channels they are transacting in and devices they are using. For example, click-to-sign is considered the standard for online processes and works well on any computer or device, in any channel.
- **The regulatory or business requirements that govern your process.** As an example, some financial services account opening processes require a handscripted signature and cannot use the click-to-sign option.
- **Signing order:** Depending on the process, the number of signers and their respective roles, you may want to impose a sequential or concurrent signing order.

Recommended Signature Capture Methods		
Use Case	Channel	Description
B2C / G2C	Online	The choice is simple: click-to-sign. While there are other means of capturing a binding signature, clicking is the best signing method for a remote self-serve transaction, because consumers don't need any special hardware or software to sign other than their web or mobile browser.
	Mobile	Tap-to-sign or use the mobile device as a signature capture pad and draw a handwritten signature
	Call center	Click-to-sign online or tap-to-sign on a mobile device
	Remote F2F	While click-to-sign is possible, it is often preferred to capture a digitized hand-scripted signature because it feels natural and culturally familiar. This can be accomplished either through a signature capture tablet (think of those used by courier companies) or a web-enabled tablet such as an iPad.
	In-branch	Click-to-sign or cursive signature capture on a signing pad or tablet
E2E	Internal	Click-to-sign, tap-to-sign on a mobile device, or sign using a smart card
B2B / G2B	Online	Click-to-sign or smart card signing



Step 7: Document Delivery

Once all documents have been e-signed, you will need to offer secure electronic copies for download or send securely printed copies through the mail. As with the authentication step, this can be done through the e-signature solution or through another enterprise system such as a customer communications management (CCM) platform.

Depending on the use case, it may make sense to offer electronic or print copies of the signed records or give customers the choice.

When sending out copies of e-signed documents, there are a few industry best practices to keep in mind:

- First, if you send the customer an email with a link to a secure site, they will be able to come to your site and download copies, an action which is logged on the server and provides your organization proof that the customer did in fact obtain a copy. The customer can also keep that email for future reference if they need additional copies – an example of the little extras that make for a great customer experience.
- Second, if transacting with mobile customers, a key consideration is their ability to download and retain documents on a mobile device. The question becomes, how do you store documents when using only browser-based apps? Your e-signature solution must provide the ability to download documents (through the browser and in the app) either to the mobile device or to cloud storage.

This is also the step where you need to consider your organization's document retention policies. Best practice is to store and manage e-signed records and audit trails according to your own data retention policy, which is usually best accomplished by storing everything in your existing CMS. For that to work:

1

E-Signed documents and audit trails must use a stable file format. Because it is an industry and ISO standard, PDF is the only acceptable format for e-signed records.

2

E-Signed documents must be self-contained. You should not have to store the e-signed record in the e-signature service. It is recommended to avoid e-signature solutions that require you to access a server to verify the signature or document. Not only is this an inconvenience for users, it introduces major problems in the event that you terminate your subscription or the vendor goes out of business. The e-signed record should securely travel through any email, storage, or archiving system without being compromised or requiring additional programming. This enables you to manage e-signed records in a manner that meets your long-term records retention policies. In other words, the e-signed document can be indexed, stored, and retrieved easily in the system of record of your choice, and you can leverage your investments in those systems.

3

It must be easy to verify (independently of the vendor) that no changes have been made to the signed record. Look for intuitive, one-click signature and document verification. If the verification process is too cumbersome, users may wrongly assume that the document and signatures are valid, without proper verification.

Recommended Document Delivery Options

Use Case	Channel	Description
B2C / G2C	Online / Mobile	Document download
	Call center	Document download
	Remote F2F	Since there is often no printer available in the field, it is best to offer to download copies of documents in real time and/or send a printed copy in the mail as well.
	In-branch	Offer the customer the choice of document download or paper.
E2E	Internal	Document download
B2B / G2B	Online	Document download

Conclusion

As you think about how to turn your paper process into a digital process, familiarize yourself with your process, delivery channels, the devices your signers use, and other requirements. An e-signature solution, such as OneSpan Sign, provides the flexibility to support any requirement you have today and tomorrow — no matter how simple or complex. This will enable you to use the same core solution across your organization, while customizing the signing workflow as needed to each individual process. From a single platform, your business can offer customers an optimal user experience online, in-branch, through a field agent's mobile device, through the call center, or other channel.

At OneSpan, we have extensive experience in taking business processes digital and can provide tailored best practices guidance for providing an intuitive, straightforward, and compliant user experience. We have been doing this for two decades, primarily with regulated organizations in financial services, insurance, government, healthcare, pharmaceutical, and other industries, where automating transactions is always more challenging. To learn more, visit us online at Onespan.com/esignature-solutions



OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.



Copyright © 2019 OneSpan North America Inc., all rights reserved. OneSpan™, DIGIPASS® and CRONTO® are registered or unregistered trademarks of OneSpan North America Inc. and/or OneSpan International GmbH in the U.S. and other countries. All other trademarks or trade names are the property of their respective owners. OneSpan reserves the right to make changes to specifications at any time and without notice. The information furnished by OneSpan in this document is believed to be accurate and reliable. However, OneSpan may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use. Last Update: April 2019

LEARN SECURITY BEST PRACTICES FOR IMPLEMENTING E-SIGNATURES

