OneSpan
Be bold. Be secure.

USER AUTHENTICATION FOR E-SIGNATURE TRANSACTIONS

THE RIGHT AUTHENTICATION METHODS TO PROVE WHO SIGNED

WHITE PAPER

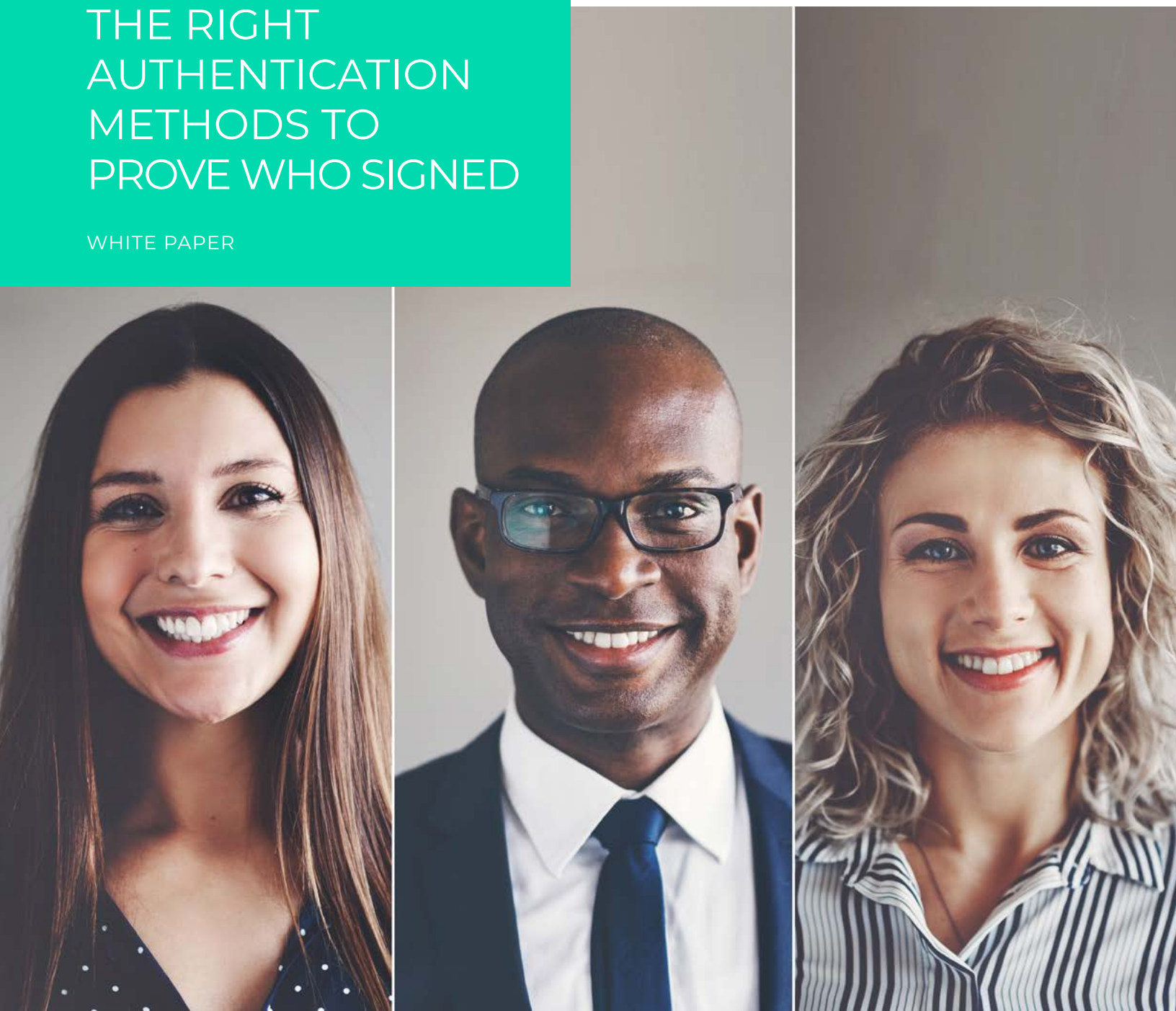


TABLE OF CONTENTS

INTRODUCTION

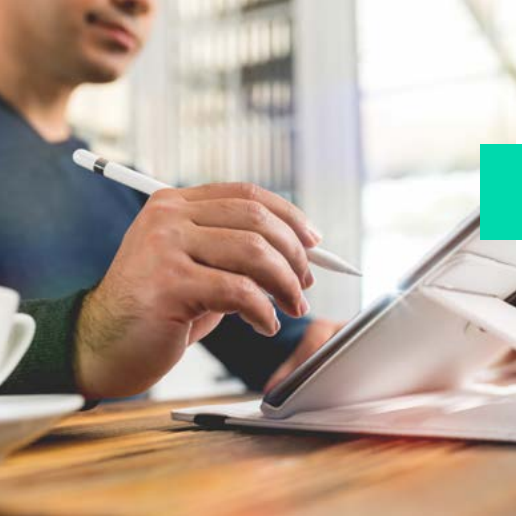
Executed well, user authentication builds trust and loyalty. Done poorly, it can lead to frustration and abandonment. This white paper provides best practices to help you provide secure signing experiences, with minimal friction for customers and citizens.

The majority of digital business transactions are faceless, conducted remotely with online and mobile customers. While there are tremendous benefits to offering customers, vendors and partners the ability to use e-signatures to do business digitally, clearly the organization initiating the transaction must know who they are transacting with to create a trusted environment for all parties.

User authentication plays a crucial role in electronic signature transactions. It is the layer of security that is put in place to associate an e-signature to the person signing, thereby reducing the risk of repudiation. Authentication helps to ensure enforceability of the e-signed record and directly impacts customer experience. Executed well, user authentication builds trust and loyalty. Done poorly, it can lead to frustration and abandonment.

To provide guidance on how to select and implement authentication techniques related to e-signature transactions, this white paper shares must-know tips, best practices and answers to questions like:

- How do I select the right authentication for my requirements?
- At what stage(s) during the transaction do I need to authenticate the signer?
- How do I implement strong authentication, without making the process difficult for the customer?
- Can I leverage existing user authentication credentials?
- Can I adjust my user authentication criteria for different transactions and processes?
- What are other organizations using? What best practices do they rely on?
- What authentication is available out-of-the-box with e-signatures?
- When do I need to integrate with other systems?
- Will I have to pay additional fees?



FRAUD AND REPUDIATION

Even though global e-signature laws and regulations (e.g., ESIGN Act, eIDAS, etc.) do not specify the type of authentication to be used with e-signatures, the legal definition of an electronic signature always includes language around signer identity. The same applies to industry and government regulations. This means that for purposes of enforceability and compliance, organizations need to take steps to authenticate signers and they need to tie that authentication to the e-signature and e-signed record.

According to Patrick Hatfield, Partner with Locke Lord LLP and author of the 6 Point Risk Analysis Framework for electronic signatures and transactions, "Authentication risk is the risk that the electronic signature obtained is from a forger, not from the actual person whose name is associated with the electronic signature. The risk is that a company relying on an applicant's electronic signature seeks to enforce the document bearing the person's signature and the person claims, "That is not my signature!"

> "Authentication risk is the risk that the electronic signature obtained is from a forger, not from the actual person whose name is associated with the electronic signature."

While the vast majority of legal disputes challenge the terms and conditions of a signed document – not whether a signature belongs to a person – user authentication is still a risk organizations must address, especially when doing business with new and unknown customers over the web.

In addition to the authentication techniques and mechanisms laid out in this paper, it is important to realize that a combination of events and evidence is typically used to establish the identity of a party to a transaction. This includes conversations with agents or representatives, the provision of personal information, exchange of documents, payment records and more. As an example, in the event that a person denies having e-signed the record, a point to consider for determining the legitimacy of the claim is did the person, subsequent to the transaction, make a payment to obtain the product or service?

Fraudulent transactions are often based on skipping or misrepresenting information and taking advantage of the fact that there is enough time that will pass before it is detected. Paper-based processes slow transactions and give criminals more time to carry out the fraud. Unlike paper, digital business processes are executed immediately and workflow rules make it impossible to skip steps and intentionally omit signatures. A digital process makes it easier to verify user information quickly enough to detect fraud before the damage is done.

IDENTIFICATION VS. AUTHENTICATION

Step 1

User Identification

User identification is the process of presenting and making a claim to an identity. Whether the transaction is taking place on paper or electronically, this is the first step in determining who you are doing business with, so naturally it takes place the first time two parties conduct a transaction.

A good example is a new customer who goes to the bank to open an account. The new customer meets face-to-face with a bank representative and provides proof of identity with a government issued ID such as a driver's license or passport.

Take that same in-person transaction and replace the paperwork and ink signatures with a digital process and electronic signatures. That is exactly what U.S. Bank has been doing since 2013. Identification takes place just as it did with paper – the two parties meet in the branch, the new customer shows a government-issued ID such as their driver's license, the bank representative verifies it, the account opening documents are presented on-screen and the customer e-signs on a signature capture pad.

This in-person transaction is conducted with what is called an "unknown signer." The customer has never done business with the bank before and is, therefore, an unknown signer until their identity has been verified. Should the customer wish to do further business with the bank, they will henceforth be a "known signer" because the bank has already verified their ID in a previous transaction.

How do you identify new digital customers – people with whom you have no previous relationship and will likely never meet face-to-face?

But what happens when you take that account opening process out of the branch and offer it through your website or mobile app? How do you identify new digital customers – people with whom you have no previous relationship and will likely never meet face-to-face?

Thousands of organizations have faced this question since e-signature laws and regulations (e.g., ESIGN Act, eIDAS/EU Directive, Electronic Transactions Act, etc.) first made e-signatures legal in the late 1990s and early 2000s. The good news is, early adopters helped establish a comprehensive set of best practices. One of the first things to keep in mind is that identity is proven at multiple points in the process, including:

- The actual identification and/or authentication process.
- Any conversations with agents or representatives.
- The personal information provided by the customer during the application process. (As an example, a significant amount of personal information is collected about an applicant in the context of an insurance or mortgage application process. All of that data is part of the process of establishing the applicant's identity.)

There are different ways to identify a first-time customer and the choice of identification method will depend on the risk profile of the process. Any of these options can be used alone or in combination:

1. **Personally Identifiable Information (PII):** Leverage the authentication methods used in your other remote channels, such as the call center and by mail. This includes collecting and verifying information used to trace an individual's identity, such as name, social security number (SSN), date/place of birth, address and more.

2. **ID Verification:** If the participant in a transaction is a "known customer" to the bank, the bank already has the customer's identifications on file to authenticate the customer. However, if the participant is an "unknown customer," the bank must have a method of verifying the customer's identity documents. This can include a proof of residence, passport, driver's license, state-issued ID, or other uniquely identifying documents.

   There are two methods of ID Verification:

   - In-person Verification: This requires the customer to show a bank associate a physical copy of their government-issued photo ID. The associate must then confirm that the ID is genuine and approve the transaction.
   - Digital ID Verification: With new technology and regulations, such as the U.S. MOBILE Act, organizations can now digitize the ID verification process. Harnessing the power of mobile devices, banks can accept a scanned copy of the customer's photo ID to verify its authenticity, and ask the customer to upload a selfie to match against the scanned ID. .

3. **Knowledge-based Authentication:** For high risk, high value transactions, use a third-party identity proofing and verification service for dynamic knowledge-based authentication (KBA).

DYNAMIC KBA FOR ONBOARDING & ACCOUNT OPENINGS OVER THE WEB

In this use case, a bank or financial services organization would first integrate their account opening system with OneSpan Sign, which has an out-of-the-box integration with the Equifax eIDVerifier™ service. The identity verification step is seamless – the e-signature and ID verification services work together behind the scenes so the online applicant sees only the bank's branded interface. The workflow is simple and takes place in real time:

1. The applicant enters their personal information into a form on the bank's website.
2. The bank's system transmits the data to their electronic signature solution, which in turn submits it to Equifax.
3. Equifax eIDVerifier returns a multiple-choice questionnaire randomly compiled from information managed by consumer and business information sources.
4. The electronic signature solution displays the multiple choice questionnaire to the applicant in English, Spanish or French (available via Equifax U.S. and Equifax Canada).
5. The applicant submits their answers. Correct answers confirm the applicant's identity and enable the applicant to complete and e-sign the online account opening agreement. Incorrect answers block the applicant from continuing with the process.

Dynamic KBA provides a high degree of assurance that a new and otherwise unknown signer is who they say they are. Unlike static KBA, dynamic KBA does not require a previous relationship with the user. With dynamic KBA authentication, questions are compiled from public and private data such as marketing data, credit reports or transaction history. To initiate the process, basic identification factors (name, address, date of birth) must be provided by the signer and are checked against a third-party service such as Equifax. After the signer's identity is verified, out-of-wallet questions are generated in real-time, making it difficult for anyone other than the actual user to answer correctly. Out-of-wallet refers to information that wouldn't typically be held in someone's wallet, social media site or even a utility bill, making it more difficult to impersonate that individual. For example, questions about previous addresses or the amount of their last car loan payment.

Mobile ID Verification

As an alternative to Dynamic KBA, banks can also deploy Mobile ID Verification. This ID verification process used to be a paper process relying on government issued credentials, but now with the help of mobile devices, the process can be streamlined without relying on third-party services.

1. **Verify:** Verifies ID document authenticity in real-time
2. **Compare:** Ties the person to their ID document
3. **Pre-Fill:** Extracts data from the ID and pre-fills the form
4. **Sign:** Captures e-signatures and audit trail

> Two authentication methods used together is known as two-step authentication, while two-factor authentication is a combination of different factors

Step 2

User Authentication

Once the customer's identity is confirmed, the customer is typically given credentials such as a username and password to facilitate future transactions. User authentication is the process of verifying credentials, prior to giving access to a system – in this case, the e-signing ceremony. The most widely accepted standard for user authentication in online transactions has traditionally been username and password. When combined with email notification, it provides a usable, reliable and cost-effective way to authenticate signers.

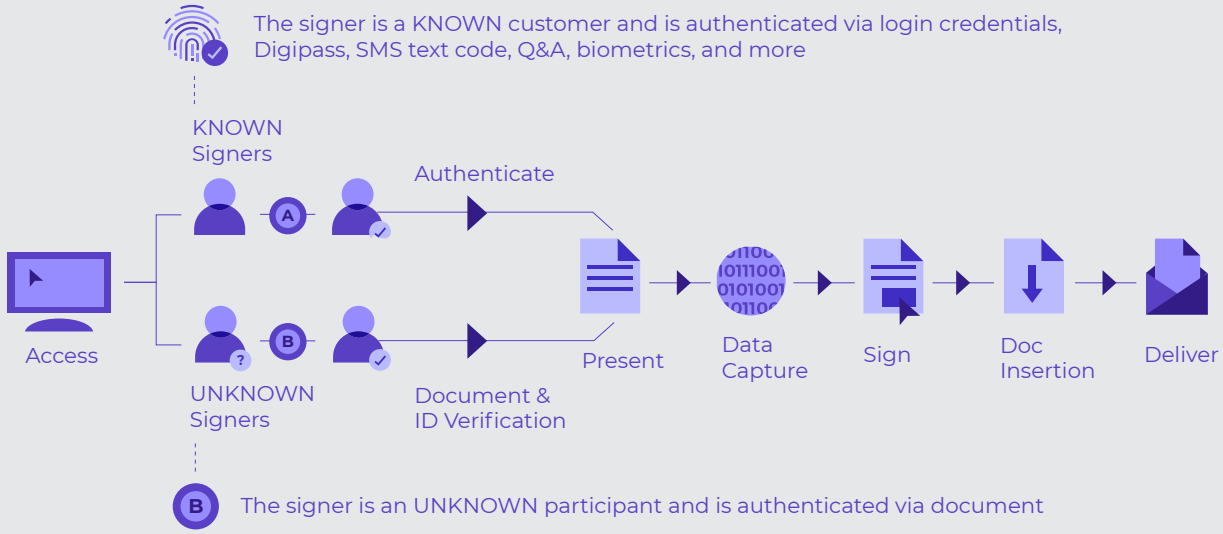
For existing customers, it is highly recommended to leverage credentials you have already issued (e.g. logins for online banking or an insurance portal). Not only are such credentials generally reliable if they have been used over time, it saves the customer the hassle of having to remember yet another password.

Authentication can take place in one step or in a combination of steps and factors. Two authentication methods used together is known as two-step authentication, while two-factor authentication is a combination of different factors, meaning:

- Something the user knows (e.g., password);
- Something the user has (e.g., hardware or software token, government-issued smartcard, mobile phone);
- Something the user is (e.g., biometrics such as a fingerprint or facial recognition).

WORKFLOW DIAGRAM

The Role of Identity and Authentication as Part of the Signing Workflow



Authentication happens at the beginning of the process, using:

- Verify government ID
- Email authentication
- Login credentials (including SSO)
- Secret question challenge
- SMS PIN
- Dynamic knowledge-based authentication (KBA)
- Digipass® multi-factor authentication
- Biometrics

Authentication can also take place a second time, at the point of signing, using:

- Digital certificates stored on smart/chip cards
- Derived credentials
- Digipass or third-party authentication service
- Biometrics

Note: While the hand-scripted signature is not an authentication method and therefore not included here, some organizations find that capturing a hand-scripted e-signature on a touchpad or signature capture device increases consumer adoption. In banking, for example, the traditional signature card is used as a security measure to compare a signature on a check against the signature sample on-file in the branch. The same comparison can take place with hand-scripted e-signatures, provided the two e-signatures were captured on the same type of device.

Authentication Options

Select an e-signature solution that supports a broad range of options, providing the flexibility to adapt the authentication to any process and any set of requirements. This includes:

Email Authentication

The signer is sent an email, inviting them to access the e-signing ceremony by clicking a link embedded in the email. In this case, the authentication happens when the signer logs in to their email account. This, combined with the fact they clicked the link in the email invitation, establishes a connection to the signer due to the uniqueness of their email address as well as the uniqueness of the link sent by OneSpan Sign.

Sample Use Case: Email Authentication & Password

Interior Savings Credit Union has 82,000 members, 21 branches and assets exceeding $1.9 billion. The credit union uses e-signatures for mortgage renewals. According to the business process improvement specialist, “Mortgage renewals are a relatively low risk process as the paperwork and documentation is really just the member accepting the new terms and not the debt itself.” To authenticate the member, staff provide them a password over the phone. An email invite is then sent to the member’s personal or work email. The member clicks the link in the email and is taken to a login page. The member enters the password and gains access to the documents that require signature.

Login Credentials

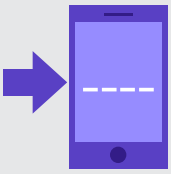
The signer is authenticated by the sending party’s system prior to accessing the e-signature transaction (e.g., through a customer portal such as online banking, a government services portal or even a SaaS account, which requires a username/password combination). Using the online banking portal example, the customer logs in to their account, is presented with the documents and e-signs from within the portal.

Static KBA (aka Secret Question Challenge)

Challenge 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.

Sample Use Case

“We chose to use the Q&A method since we would have already interacted with the borrowers and can agree with them on the answer to the security question. Although our electronic signature vendor offers up to three Q&As, we decided to use one Q&A for each borrower. Email invitations are automatically sent out to all signers with a link. When borrowers click that link, they are directed to a secure website and are asked to enter the answer to their respective security question. The borrower is then given access to the signing ceremony.” - Bob Catlin, President of Signature Mortgage



SMS Authentication

A unique PIN can be automatically generated and sent to the customer's cell phone. The signer types it into a web page to authenticate. Email authentication, combined with SMS PIN, provides a reliable two-factor authentication process. And unlike other e-sign vendors, there is no additional charge for SMS authentication with OneSpan Sign.

Sample Use Case

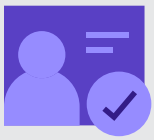
One of the largest US mutual life insurers has implemented e-signatures for disability insurance processes. Customers click to sign online from anywhere. To access and e-sign the "Future Increase Option" form, the customer is sent an email with a link to the documents. The customer must access their email account with their username and password (something the user knows), then a one-time SMS passcode is texted to their phone (something only the user has). The customer types the PIN into a web page to authenticate.

Dynamic Knowledge-based Authentication (KBA)

OneSpan Sign can connect to the Equifax eIDverifier service to obtain a multiple-choice questionnaire that is generated on the fly and presented to the signer. These out-of-wallet questions are generated in real-time, making it difficult for anyone other than the actual user to answer correctly.

Digital Certificates

OneSpan Sign leverages digital certificates issued by third-party Trust Service Providers (TSP) and certificate authorities (CA). When using a personal digital certificate to e-sign a document, OneSpan Sign verifies the certificate's status and the action requires a PIN or password to complete the signing process. This mechanism is typically reserved for internal processes or processes with repeat signers involved in higher risk transactions. When using a digital certificate issued by a qualified trust service provider, this creates a Qualified E-Signature (QES), in accordance with the requirements of the European Union's eIDAS regulation.



Government Smart Cards & Derived Credentials

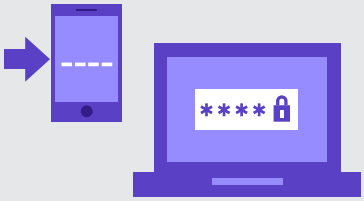
Government personnel and contractors routinely e-sign forms and documents using a digital certificate that is stored on a smart card, such as a U.S. Department of Defense Common Access Card (CAC) or a Personal Identity Verification (PIV) card. This provides strong two-factor authentication with something the user knows (the PIN for their card), and something the user has (the card).

See how this works

Sample Use Case

USDA employees e-sign documents by inserting their LincPass smartcard into a slot on their keyboard or laptop. They then enter a 6-8 digit PIN. Once successfully authenticated, they can apply their e-signature to documents for full non-repudiation.

U.S. Census Bureau's 8,000 field employees carry laptops with derived credential chip technology. At the point of e-signing, OneSpan Sign prompts the employee to select their digital certificate and that is used to apply their e-signature to the document.



Digipass

Multi-factor authentication provides a constructive element of layered security by requiring users to prove their identities using two or more verification methods before they can access and complete the transaction. In this way, if one factor is compromised or broken, there is at least one more barrier to breach the digital transaction. OneSpan Sign integrates with OneSpan's multi-factor authentication solutions to support strong authentication with one-time passwords (OTP) and/or visual cryptograms during the upfront user authentication and at the time of signing.

See how this works

Learn more about the technology

Biometrics

Further reduce your risk with biometric authentication. This is typically reserved for high risk or high value transactions with existing customers. OneSpan Sign can leverage both face and fingerprint authentication methods to quickly validate user identities based on unique human characteristics. OneSpan Sign integrates with OneSpan's Mobile Security Suite to use something as simple as a fingerprint or "selfie" to authenticate the user before the signing process is complete.

See how this works

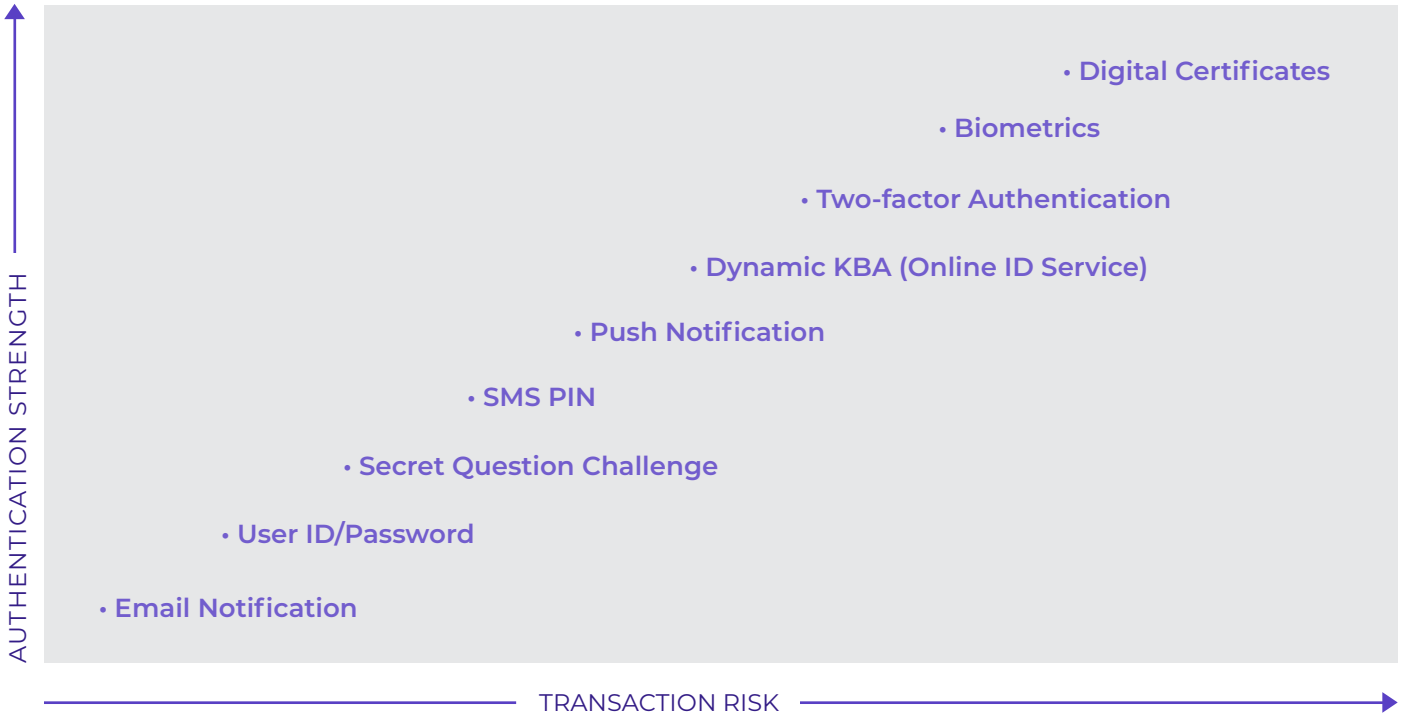
SELECTING THE RIGHT METHOD(S) FOR YOUR USE CASE

There are many secure and user friendly options for authenticating signers online. Ultimately the choice of authentication depends on the process being automated.

- Is it an internal process or a legally enforceable transaction with a vendor or customer?
- In what channel does it take place?
- What types of documents are involved?
- What is the value of the transaction?
- How much risk is involved?

While risk is inherent to any process – paper or electronic – the key is to know your process well enough to recognize where the authentication safeguards are already built in, and keep that in mind when designing the digital process. For example, a proposed insured goes through an underwriting process before receiving a policy and a credit check is done on loan applicants before funds are disbursed.

According to Locke Lord LLP, "There are authentication risks, repudiation risks and compliance risks with the traditional process of using wet ink and hardcopy paper to complete transactions. Many companies have not examined such risks until they begin developing an e-process. For most electronic signature and e-discovery processes, the goal will be to have the transaction, on the whole, be no riskier than the current processes."[1]



General Guidelines

For internal processes taking place between employees, best practice is username and password. Or where available, SSO.

For NDAs, basic contracts, expense approvals and other day-to-day signing processes between you and your business partners, members and/or customers, we recommend email authentication.

For more sensitive processes, consider:

- **Secret question challenge** (static KBA). This authentication method is ideal to use for transactions such as renewing an insurance claim or an electronic fund transfer. For financial transactions or insurance applications, set up to two or three challenge questions.
- **SMS authentication** through the signer's phone. SMS authentication allows you to verify your signer's identity by sending a secure PIN code to their mobile number. The recipient must enter the PIN to access the signing ceremony.
- **Combining multiple authentication methods and factors**. This adds an additional layer of security, and does not necessarily mean more complexity for the signer. For processes that require two-factor authentication, access to the e-signing ceremony can be secured by:
  - Username/password + SMS PIN
  - Secret question challenge + SMS PIN
  - Dynamic KBA + SMS PIN

In the last scenario, OneSpan Sign will first prompt the signer for the SMS PIN, then present the dynamic KBA questions. If the signer comes back to a document package, either to download a document from a completed package or to finish signing documents in a package that is in progress, they will be prompted for the SMS PIN. For example, in a package where John Smith will be asked to use both methods:

- Monday: John opens his invitation email, clicks the link and sees the prompt for the SMS PIN. John enters the PIN and is then presented with the Equifax questions. John answers correctly and is immediately shown the documents he needs to sign. However, John does not complete the signature process.
- Tuesday: John re-opens his invitation email, clicks the link and gets prompted for the PIN he received via SMS. John enters the PIN and is immediately driven to the documents he needs to sign (no Equifax questions).

Smile & Sign

This innovation brings together next-gen biometrics (e.g., face authentication), fraud analytics and mobile e-signature technologies to help you deliver secure and convenient mobile experiences. It leverages e-signatures to capture intent in a legally binding way and something as simple as a selfie to validate the customer's identity before the signing process is complete. Financial services and other regulated industries focused on reducing fraud while improving the customer experience will benefit from this solution.

Learn more

IN-PERSON VS. REMOTE PROCESSES

Proving who e-signed a document can be more challenging in a point-of-sale environment than it is over the web. Examples of in-person, point-of-sale transactions include:

- A car dealer and customer closing the financing on a vehicle, using the dealer's tablet to capture the customer's e-signature.
- An insurance agent meeting with the customer to complete and e-sign an insurance application on the agent's laptop or tablet.

In a self-serve transaction online, customers log in to the signing ceremony using their personal credentials and are in sole control of when and what documents they sign. This is not always the case when processes take place in-person because service representatives often share their laptop or desktop computer with customers.

Capturing a handwritten signature on a signature capture tablet has been one approach to addressing this issue. But that involves purchasing and managing hardware dedicated to the sole purpose of capturing signatures. Instead, in face-to-face transactions, many organizations are using the click-to-sign method. This can raise questions about who actually clicked to sign – the customer or the representative?

There are various ways to solve this:

SMS Authentication

SMS authentication provides an extra layer of security, while eliminating the need to purchase signature capture hardware for agents.

- A unique PIN is automatically generated by the e-signature system and sent to the customer's phone.
- The agent hands their laptop or tablet to the customer.
- The customer enters the SMS PIN into the web page to continue.
- This, combined with an affidavit that the customer can e-sign, enables the customer to confirm they are indeed the individual performing the act of signing.

Mobile Signature Capture

Mobile Signature Capture is another option. If the customer has a smartphone, they can use their own device as a signature capture pad. This feature allows signers on a desktop or laptop system to capture a handwritten signature on their mobile device, and then relay that signature back to the document on the desktop/laptop system. The fact that the customer is hand-scripting their signature instead of clicking a button helps alleviate any need to attribute the signature to its owner.

Biometrics

Biometrics is an option, but only for existing customers because the biometric data must be compared against registered biometrics data (e.g., face or fingerprint) in a database.

AUTHENTICATION METHOD	REMOTE (ONLINE, CALL CENTER)	IN-PERSON (BRANCH, F2F WITH AGENT)
Username/Password	✔	
Email Notification with Link	✔	
Secret Question Challenge (Static KBA)	✔	
Dynamic KBA	✔	✔
SMS PIN	✔	✔
Digital Certificate/Smart Card/Derived Credential	✔	✔
Two-factor Authentication (Digipass)	✔	✔
Government-issued ID (Driver's License, ID Card)	✔	✔
IP Address	✔	
Signature Capture	✔	✔
Biometrics	✔	✔
Photo, Video		✔

BEST PRACTICES

When researching e-signature authentication capabilities, the best approach is to look for a solution that will allow you to leverage a mix of existing and new technologies that mitigate risk of fraud and repudiation, can be configured to meet the requirements of each process and channel, and provide a fast, seamless experience for the customer.

An E-Signature Solution Should Therefore Provide:

- Options for identifying remote signers, either through third-party databases, biometrics or personal information verification (PIV).
- The ability to upload images as part of the e-sign transaction (e.g., a photo of a driver's license) as further proof of the signer's identity.
- Standard authentication options such as email, shared secrets and SMS available at no extra cost to the sender.
- The ability to customize the questions, if using secret question challenge.
- The ability to configure different authentication methods within the same transaction – both upstream before the signer enters the transaction and downstream at the time of signing (if required).
- The flexibility to adapt the authentication method to the risk profile of your organization, to each process being automated and even to each signer (e.g., Signer 1 could be identified through email authentication while Signer 2 could confirm their identity through username/password. The same concept applies to company representatives who are typically authenticated differently from a customer.)
- Options for in-person signature attribution, such as hand-off affidavits, texting a one-time PIN to the signer's phone or leveraging Mobile Signature Capture to capture a hand-scripted signature instead of click-to-sign.
- Options that make it easy to get up and running immediately with at least one method of single and multi-factor authentication.
- It is also important to look for a solution that supports Single Sign On (SSO) which makes it easy for on-site and remote employees to access a variety of SaaS applications without having to use different login credentials each time. (Through support for SAML2, OneSpan Sign can be configured to interoperate with any third-party SSO provider)
- An audit trail that captures all of the authentication data, as well as IP address, date and time of signing.
- The ability to verify IDs via mobile devices.

Conclusion

As you think about how to turn your paper process into a digital process, familiarize yourself with your process, requirements and risk tolerance. While there are many secure and user friendly options for identifying signers online, ultimately the choice of authentication method depends on the risk profile of the process being automated and the underlying digital transaction. The key point here is to securely authenticate users without diminishing their experience. As such, look for an e-signature solution that offers a wide range of authentication options to better fit your needs and as a result, enable better experiences.

In addition to user identification and authentication, you likely have other security requirements. Security is understandably a top concern with online transactions, so it is important that e-signature providers meet the highest security standards. Security frameworks like Service Organization Control (SOC) 2 and FedRAMP attest to the security behind an e-signature system and confirms that the necessary controls and procedures are in place at the system level, day in and day out. To learn more about security, authentication or any other e-signature topic, contact us or visit OneSpan.com/sign

1 https://www.OneSpan Sign.com/resource-center/top-6-legal-risks-of-electronic-signatures-and-e-transactions/

OneSpan

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.

CONTACT US
For more information:
info@OneSpan.com
www.OneSpan.com