DocuSign | Signer Authentication WHITE PAPER

A common question arises as people migrate to electronic signature and electronic contract execution from paper and ink signatures. "How do I know my intended signer is the actual signer?" This question leads to "What is the best way to authenticate my recipients?" and "How much authentication is enough?" The answers to these questions, in some part, can be based in your current business practices. Most businesses that currently manage signed documents do so with some thought about the risk of signer repudiation and have evaluated the risks and settled on a process. In many cases, authentication of signers for paper-and-ink signing is minimal.

Review Your Current Authentication Practice

Most paper signing processes take place via mail, overnight express, or in person. These processes have likely been in place at your business for a long time. In order to evaluate your signer authentication strategy when moving to an e-signature process, consider a few important questions about how your signing process for your business works today:

1. What types of authentication are used in your processes today?

How do you obtain signatures and validate users in your current processes? Do you use third party authentication tools? Do you verify drivers license information? Do you use other methods to verify a person's identity before signing?

2. Do you have a history of challenges to your executed contracts?

Do you have a history of contracts being signed by people who are not who they say they are? What percent have these types of problems? Does your business have a history of problems with signer verification? If so, what manual processes have you put in place to prevent it?

2. What would be the impact on your business of a contract being signed by someone who is not your intended signer?

What is the extent of the damage to your business? What is the cost? When you do have a problem with signer authentication and lose a transaction because of it, what is the possible dollar cost impact to your business?

What Authentication Mode Do You Use?

In addition to your current business practice around authentication, consider what authentication MODE your business uses today. There are two types: "Prior Authentication" and "Post Authentication" and they are used for different purposes. Prior Authentication Processes These processes deal with authenticating a signer BEFORE a contract has been signed, and are designed to prevent a signer from improperly representing his or her identity. Prior authentication is often used where funds or value will transfer on the basis of the signature. If the signer is posing as someone else, the funds or value may be lost. Prior authentication always takes place BEFORE the contract or transaction is agreed. Examples of prior authentication are validating a driver's license, Knowledge Based Authentication, validating a signature against a known prior signature, or using a notary. Prior authentication causes more customer confusion and restricts transaction volume because of the additional steps required to obtain access to the transaction. For this reason, some businesses decide "the risk is worth it" and forego prior authentication practices.

Post Authentication Processes

The vast majority of business transactions rely on post authentication measures because the act of signing binds a person to a contract. But in order to execute the contract, several steps must be taken that will only be possible as an act of the proper person and that person can be easily found later. An example of a post authentication process is relying on a person's signature when that person is not known to the person collecting the signature. Only in the event of a challenge would post authentication begin, for example a handwriting analysis may show a person's handwriting was in fact theirs. Actually, an astoundingly large number of transactions are executed with little or no PRIOR signer authentication.For example, the following are all examples of transactions where prior authentication is rarely used:

1. Credit card transactions.

Rarely today is a buyer required to show a valid drivers license unless it is written on the card. In many cases, the buyer is not even required to sign, for example at Starbucks. Why? The business decision was made that the cost of fraud prevention (signing a ticket and presenting a drivers license) was far more costly than the small amount of fraud that actually happens.

2. Non-disclosure agreements — "Print this out, sign it and fax it back."

There is no prior authentication. A signature and a fax number are the only factors. The recipient is rarely validating the signature against a "known good" signature. They also rarely dismiss faxes from Kinko's or from a hotel lobby.

Moving Authentication Online

Online Authentication models typically focus on Prior Authentication modes where we are identifying the user before allowing access. There are three general categories or factors of authentication.

1. Something you know. Such as a password or token value.

2. Something you have. Such as an access card, a cell phone, or key fob.

3. Something you are or do. Such as a fingerprint, retinal scan, or voice pattern.

To raise the level of authentication assurance, companies require the person to provide authentication from more than one category. This is called "two-factor" authentication. Using a password and an access card is an example of two-factor authentication. Using two passwords is not "two-factor" authentication, but rather "multi-factor" authentication. Using two-factor authentication to raise authentication assurance is more effective than using multi-factor authentication.

The Federal Financial Institutions Examination Council (FFIEC) prescribes a standard of authentication required for many financial transactions which is defined as "multifactor" authentication. FFIEC is an interagency body of the U.S. government that works with Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, and many others. Systems exist which can provide system authentication such as installed digital certificates, machine addresses, and network adapter card addresses. But these do not identify a person, but rather identify a machine.

Identifying a Person Online

Identifying a Person Online Ideally, the objective with online authentication is to identify the person, not the equipment. Relying on the relationship of equipment to people is not as effective an indicator of identity as other methods of authentication. It may not be reasonable to expect any person to have a particular piece of equipment. It may not be reasonable for a particular piece of equipment to be used only by a particular person. Requiring specific software, certificates, or hardware for authentication purposes will hamper the adoption of the underlying solution and the success of authentication for a broad group of people. Below we discuss several online authentication levels below in order of increasing security.

1. Self-Authentication. The lowest level of authentication relies on customers authenticating themselves. This may be a simple registration that does not validate anything. In fact, many services that allow a user to "self provision" a certificate are, in fact, self authenticating. This level has really no Prior Authentication at all. Even the validation of receipt of an email will improve the authentication assurance.

2. Email Authentication. This method of prior authentication requires a user to prove they have access to an email address. It is a very light form of authentication because email accounts may be obtained without authentication. Some email authentication systems are set to reject a list of "free" email systems such as Gmail, Yahoo, etc. and will only allow corporate email systems to be used to increase the security of this method. Email authentication is a weak form of third party or system validation andprior authentication.

3. Shared Secret. When using a shared secret or a passphrase, the recipient must know or have been given some data that they will need to use to access a transaction. Delivery of the shared secret to the customer should take place "out of band" from other communications methods used to deliver the transaction. For example, if you send the customer a link to a document in one email, you should send the shared secret or passphrase by phone or another method but NOT by email. A shared secret is a Prior Authentication mode.

4. Knowledge Based Authentication (KBA). Using a third party data provider to generate a set of questions only the person would be able to answer. Common types of questions relate to prior addresses, phone numbers, and names of relatives. This is a very popular form of third party authentication because it works in real time, it generates dynamic questions and possible answers, it includes questions where more than one answer or no answers are correct, and does not require the customer to have a device. For these reasons, it is very difficult for someone to pass another person's knowledge-based authentication questionnaire. This tool uses credit or noncredit questions. Knowledge based authentication provides very strong Prior Authentication.

5. Phone Based Authentication. Phone based authentication relies on person being available to use a known wireless phone or wired phone number. When used with a password, a phone based authentication method qualifies as two-factor authentication — using the "what you know" and "what you have" categories. Phone authentication works by requesting the customer enter in a code in a web session that is provided via a phone call to the known phone number. Another example involves sending a code to a wireless phone. Depending on how it is used, phone authentication may be a Prior or Post Authentication mode.

6. Digitized Signature. Collecting a handwriting sample on a digital pad is common to anyone who shops these days. Collecting a digital representation of a person's handwriting does not really qualify as a Prior Authentication because it is not being compared to earlier samples, but it does provide a good source for Post Authentication if there is a problem. Some signature pads also capture motion and pressure, but again without a previously recorded "known good" sample, it is not Prior Authentication.

7. Software or service based Private Key Infrastructure (PKI). PKI has been around for a long time. Using a public and private key and a trusted certificate authority (CA) a system can be setup to validate a private key held by a customer. That customer can apply their key to transactions to verify his or her identity. These PKI "certificates" may exist on the signers PC or in an online account in some instances. The challenges with PKI that have prevented it from being broadly used are:

• How hard is it to obtain the PKI Certificate? Certificates can be very easy to obtain or may require some additional effort to obtain. A selfprovisioned certificate is relatively easy to obtain. However, self-provisioned certificates provide minimal assurance of authentication. To increase authentication assurance, provisioning steps are added such as requiring a notarized transaction, requiring a physical presence, and requiring a payment to obtain a certificate. Adoption of PKI certificates to identify individuals has been limited due to these issues.

• How hard is it to view the details and authenticity of the digital signature? Applying the digital signature to a record requires the customer also have software that is able to process the signature. This typically means limiting the user to a few document formats such as Microsoft Word or PDF. This requirement also creates significant overhead in complexity. For example, the software used to view the document contents and the digi- tal signature must be aware of and trust the certificate authority in order for that signature to be shown as valid.

PKI is a prior authentication process.

8. Hardware-based PKI. Hardware-based PKI is similar to soft- ware certificate PKI, but the certificate is installed on a small piece of computer hardware such as a USB token. These are password protected and carried by the authenticated user. Hardware PKI introduces new issues for usage above and beyond those that exist for software PKI.

• How is a certificate controlled once obtained? PKI Certificates can be installed locally on the signer's PC on a key FOB, or in the cloud. For non-cloudbased certificates, if these are lost or compromised, there is a single point of authentication failure. Once someone has a PKI certificate, how can you be sure it is protected by and in control of the intended user and only that user?

9. Biometric Authentication. Biometric authentication requires recognition of a physical attribute of a person to authenticate that person. Examples of a physical attribute used in biometric authentication include 4 fingerprint, iris, voice, face, and palm. The challenge with biometric authentication as with the Digitized Signature is that we need a "known good" starting point from which to compare later access attempts. This is the strongest form of authentication, but is also the most cumbersome because the customer typically needs a hardware device, and must have established a prior known good sample. Biometric is a prior authentication mode of authentication.

For practical purposes, any authentication mode that requires the customer to possess local software or specialized hardware is not practical for broad use and should be avoided. These tools may be used for internal processes where the business controls the access points and employees.

The Difference between Authentication and the Electronic Signature

Many consider authentication and the electronic signature to be the same thing. They are not. Business processes and the law consider the authentication and the signature process to be different steps in the same transaction. For example, just because your iris scan has authenticated you, this does not mean you have actually reviewed and agreed to the terms of a contract. Likewise, simply because you were able to use your PKI token to electronically apply your digital signature to an electronic record does not necessarily mean you could even see the document.

For this reason, DocuSign makes an important distinction between Authentication and Signing. They are both important, but they are not the same thing. In DocuSign, they are tied together into the overall transaction or ceremony of agreement.

With DocuSign's authentication model, you now have an ability to leverage several different authentication tools for both prior authentication and post authentication modes. There are two general signing scenarios DocuSign addresses — "remote" over the internet and "in-person" where the signer is present. DocuSign provides several layers of authentication that are improvements over typical business practices.

DocuSign's Authentication Options

DocuSign provides an integrated authentication system that works with the signature process to ensure any level of authentication can be provided and that the authentication provides positive identification of the person signing, not the equipment.

In addition to standard email address authentication, DocuSign offers an industry-leading choice of authentication services for customers, partners and developers. By default, authentication is at the point of signing, making it a seamless process that keeps business digital.

Email Address. Requires access to a specific email address before access is granted.

Access Code. Requires the signer to provide a sendergenerated code shared out of band, usually over the phone. The signer must enter the code to open the document.

SMS. A two-factor solution that requires the signer to provide a randomly-generated one-time passcode sent via SMS text message to the signer's mobile phone to open the document.

Federated Identity/Single Sign-On. Federated Identity validates authentication by an external system integrated with DocuSign via industry-standard protocols including LDAP and SAML. As an option, Single Sign On detects email domains at login and redirects to your domain's Identity Provider for authentication.

Third-party. Validates the signer's Salesforce, Google, Yahoo!, or Microsoft account credentials, with additional options for social network credentials from Facebook, Twitter and LinkedIn.

DocuSign Credentials. Validates a recipient's existing DocuSign account associated with a username and password.

ID Check. This third-party service by LexisNexis validates a signer using a KBA (knowledge-based authentication) process. The signer must correctly answer a list of personally identifying questions to open the document.

1. OFAC Checking. As a part of ID Check, validates whether a signer's name is on the Specially Designated Nationals List administered by the Office of Foreign Assets Control.

2. Age Verification. As a part of ID Check, validates a signer's age is correct as entered and ensures the signer is of the proper age to sign.

Two-Factor Phone Authentication. This third-party service by Authentify validates a signer's access to a phone number and predetermined access code for entry. The signer's spoken name is also recorded as a biometric print.

STAN PIN System. Validates the person's Student Authentication Network as entered.

In addition, the DocuSign authentication system supports a workflow of authentication for integrated customers. This enables decision-making during the authentication process. For example, if a person's age verification results in an age older than 18 years, then the authentication process will also include knowledge-based authentication or if the age is 18 years or younger then the authentication process will also include the Federal STAN PIN system.

In addition to these prior authentication tools, DocuSign collects IP addresses of all users and time stamps all activity into the audit trail along with all the authentication results.

Signers Who Sign In-Person

If your signing process takes place in person, consider what authentication steps you require today. Depending on your business, you may do one of the following:

1. No authentication other than accepting a signature. The vast majority of processes happen this way. The signer appears, signs a contract, and it is considered good. In this case, your electronic authentication process is really nothing. Simply have the signer appear in person and sign. No need to use additional authentication.

2. Identification before signing. In some cases, the signer is required to produce a valid drivers license or other form of picture ID for the person hosting the transaction to identify the signer.

3. Notarization. This is the most stringent form of in-person authentication and it is used in only very sensitive situations.

DocuSign's In-Person Process

Using DocuSign, it is possible to sign in person by selecting the recipient type as 'In-Person Signer'. Once this is selected for a recipient, the system asks for a signing host, and depending on the business process defined will require whatever credential is typically used. For example a drivers license may be used for authentication.

DocuSign's In-Person Signing process is a witnessed signing with credential collection support. Once the signer is authenticated by the witness, he or she may electronically sign on the local computer. Once done, the witness must re-apply their signature to record he or she was present for the whole signing. In addition to the local credential collection, the signer may also be requested to process a knowledge-based authentication or a shared secret for multi-layer authentication. Therefore, this can be either a prior authentication mode or a post authentication mode authentication process.

Signing Remotely

The most common form of electronic signing using DocuSign is signing "remotely" where the signer is notified by email that they have a document to sign. This remote signing process uses at least email authentication and sender may elect to use additional layers of authentication for more sensitive transactions.

Signing in an Embedded Portal

In situations where the signing process is embedded into another portal or website, that portal's authentication can be passed along when signing starts, and used as the only authentication process or supplemented by the authentication tools DocuSign provides.

DocuSign Record of Signature

In all cases, the authentication of the signer is recorded in the DocuSign Audit Log and the DocuSign Certificate of Signing regardless of whether the person signed In-Person, Remote, or Embedded. The Audit Log and the Certificate of Signing are encrypted and tamper-proof.

Summary

When considering your signer authentication strategy it is important to evaluate your current processes and risks. Then establish any increased or decreased risks that might be present by moving your paper process to an electronic one. Once these are understood, it is simple to establish the policies and authentication procedures you should use with your electronic contract execution system.