Online E-Signing

Send a Document for Signature or Prepare it for your Own Signature

Capturing the value of digital transformation will be important in most industries—and critical for the survival of some. Organizations that sell virtual rather than physical products, especially, have a cost base largely focused on processing and servicing, which makes them highly susceptible to digital transformation. There will need to be a concerted focus on automating core activities to boost self-service and "straight through" transaction processing.

With online e-signing it's easy to get documents signed and to complete business on any device. You can sign documents yourself, send documents out for signature to other persons, get instant visibility into your document status, access completed documents and much more. Whether you or your recipients are in the office, at home, or on the go, online e-signatures work every time from every device.

If you send documents out for signature, the recipient gets an email with a link to your document and can sign on a smartphone, tablet, or any web/HTML5-enabled device without the need to download anything. You can have multiple signers and get them to sign in the order you need. E-signatures don't just let you reach customers on the devices they most commonly use; they also let you create comfort. E-signature solutions allow you to build in markers (tags) and metadata about documents that can help consumers understand what they are signing and what fields they have to fill out. Electronic documents can also include auto-check tools that identify common mistakes to eliminate human error. All these functions finally add up to a better customer experience.

First, this white paper helps you to select the most appropriate methodologies for authentication and signing, deployment model, and document format. Then we take a deeper look at important security aspects. After discussing the best architectural choices for a fast and seamless integration into your environment, we look at all the aspects that are important specifically to online scenarios. There you will see that e-signing is about more than simply signing digital documents—it's about productivity.

Table of Contents

1 Typical Functionalities

Online signing solutions typically consist of the following three basic functionalities:

- Sending
- Signing
- Managing

Each task has certain typical steps, which we outline in detail in the following paragraphs in this chapter.

1.1 Sending

- Start a new envelope (a container used to send one or more documents for signature)
- Add documents
- Add recipients
- If you are uploading a PDF document with form fields, the fields are automatically detected
- Place tags/markers in the document for signatures, attachments and other information
- Add your subject and the message for the email
- Set recipient options, reminders, expirations, and more
- Send the envelope/document for signature

1.2 Signing

- Signers receive an email with a link to the document
- They click the link
- There is typically no need to download or sign up for anything
- They may have to further authenticate themselves
- They can review and print the document or complete form fields and add attachments
- Whenever they are ready, they sign using a mouse or stylus or their smartphone or they "Click to sign" or "Type to sign" from any web-enabled device

1.3 Managing

- Typically, you will have a kind of dashboard to check the status of your documents. This way you always know where your document is in the signing process. You can set reminders and be notified at each step of the process.
- Further, you can manage internal users and adjust branding.

2 Authentication methods

An important feature of an online e-signature solution is the ability to add signer authentication to a document (envelope). Signer authentication requires document recipients to verify their identity before they can access a document. Especially in scenarios where you have no forensically identifiable signature from the signer, this is the only way to prove that a certain signer was the one who signed a certain document. It also protects the access to the document content. Therefore both aspects—proof of identity and access control—have to be taken into consideration.

2.1 Email-only authentication

This scenario is typically suited for non-business-critical documents that you want to make as easy as possible for the signer. You simply send the link to the inbox of the recipient and there is no further authentication necessary. In case of a dispute, you can prove with the audit trail that you sent the document to a specific email address and often you have the IP-address of the computer and geolocation as well, if the recipient did not block it.

All of the following authentication methods start with this scenario and add additional authentication steps.

2.2 Require recipients to enter an access code before they can view the documents

In addition to the above, you can present the recipient with a security request page and require entry of the code to access the documents for viewing and signing. After the access code has been entered correctly, the recipient is taken through the normal signing process. The access code is not sent in the same email together with the link, as this would make it completely unsecure. Typically, the code is not even sent by email at all, but instead is communicated via another channel such as by phone. To have a code that works for a longer time, you can choose to have the access code agreed upon between the parties in a separate process.

The value of this is in case of a dispute: The sender can prove that the signer must have had access to the access code in order to sign the document.

2.3 Leveraging trusted authentication models that you already have in place

Some businesses have customer portals or other software already in place and the user is identified by those systems. Let’s assume the user is within a banking application where he manages all his transactions. If the user has to sign a document and has already been authenticated then there is no need for further authentication. But the proof of authentication has to be included in the audit trail.

Another scenario is one in which the recipient uses a secure authentication method (e.g. a token) already for other purposes and this infrastructure is repurposed to authenticate him for document signing. Like above, the authentication process must be included into the audit trail of the signed document.

2.4 Using social networking IDs such as Facebook login

For this scenario, popular social networking sites are used for authentication. Most of them provide services for third-party applications to authenticate users. The quality of this authentication depends very much on the quality of the social network profile that is used for authentication. In addition, the quality of the data that you get about the user from the social network for the audit trail has to be taken into consideration.

2.5 Sending an SMS with a one-time password to the signer's mobile phone

This authentication method utilizes the fact that mobile devices are, world-wide, a very good identification method for their owners. Many people carry mobile phones around the whole day and have them within reach at all times. The mobile telephone number is a unique identifier for the owner. This is why many banking and other applications already use this method for online transactions.

Additional security can be added if the one-time password is time-limited, e.g., the recipient has to enter it within the next 5 minutes.

Another consideration is whether the one-time passcode should be valid only for one signature or for the whole document/envelope.

In addition, it's recommended to include a unique identifier for the transaction in the SMS sent to the recipient together with the one-time password. This unique identifier should also be displayed in the security dialogue where the recipient has to enter the password, to allow him to prove that the password is really for this transaction and not used for another one.

All of these considerations have to be supported by a proper audit trail to be able to prove everything in case of a dispute.

It's worth thinking about how the sender should be able to handle and define the one-time password settings. There are three main scenarios for this:

1. The recipient has the possibility to enter his mobile phone number himself. Clearly this is convenient for the sender and the recipient, but it opens a door for potential misuse by the recipient.
2. The sender defines upfront which mobile number which has to be used and the recipient cannot change that. This scenario is very common as it adds quite a bit of security to this process.
3. Finally there can be scenarios where both parties—recipient and sender (e.g. a sales employee)—should have no chance to define (change) the mobile number for the recipients and often do not even see them. In this scenario, the sender can only select the recipient from a list. The mobile numbers are stored in a central place and cannot be adjusted by the sender. This can be even taken a step further with an upstream process in which the recipient agreed in writing that, in the future, a one-time password sent to his predefined mobile number can be used as an equivalent for his signature.

Some countries give a proper implementation of this method the same legal value as a handwritten wet-ink signature. In some of these cases, a defined method by the country has to be used, an example being "Handysignatur" in Austria.

2.6 If your business demands it, you can require signers to use a third-party digital certificate for signing.

In cases where the recipient has already a PKI infrastructure (smart card, token, certificate on the computer) in place, the certificate can be used to authenticate the signer. More than that, the certificate can also be used to digitally sign the document. In some countries, this is referred to as a qualified signature and has the highest legal value.

In other scenarios, it's not primarily a question of legal weight but an attempt to reuse the existing PKI infrastructure, which was in place for other purposes. This allows you to take advantage of the existing certificate and use it for the digital signing of the document.

Digital certificates can be used to authenticate the signer of documents. When ownership of a digital certificate's secret key is bound to a specific signer, a valid signature based on that certificate shows that the document was signed by that same signer.

3 Signing methods

First, there is an important difference between methods in which:

- the captured handwritten signature of a person is forensically identifiable (also known as a biometric signature)
- the embedded signature in the signature field is only a placeholder, making additional authentication methods and audit trails necessary to be legally binding
- signatures with personal digital signing certificates

Thus, the main question in capturing handwritten signatures is whether the captured signature data is forensically identifiable. Roughly speaking, one can say that in all scenarios featuring the use of a pen or a stylus and proper implementation of the capturing software, the result will be signatures that are forensically identifiable.

In other scenarios like signing with a mouse, touchpad or finger—or where the necessary capturing software and or hardware is not in place—the signature is not forensically identifiable. This second category is what we'll call placeholder signatures.

Certificate-based signatures, by contrast, require a PKI infrastructure and while they are a very popular model for e-signing within your own organization (because you can manage the PKI rollout yourself), they only can provide limited penetration in any other scenario like B2C or B2B contract.

Regardless which of those three signature methods is used, the signed document always should be sealed with a digital signature in order to protect its integrity (see chapter 4.2).

3.1 Placeholder signatures

The big advantage of placeholder signatures is that they do not require the signer to install anything. They are simply formatted to work on any HTML5-enabled Web device. Depending on the authentication method (see chapter 1), they also do not require complex signup procedures, so they are perfectly suited for online B2C and B2B scenarios.

However, for all cases where the signature in the signature field is a placeholder, the whole process is fully dependent on the proper authentication of the recipient (see chapter 1). If it is securely documented in an audit trail (see chapter 4.3) then this authentication provides reliable evidential weight. Furthermore a proper audit trail which is not too technical to be understood by a judge —that doesn't force a judge to go for an expert opinion—puts the burden of proof immediately on the signer in most cases.

The question of how this placeholder should look is more a question of convenience for the signer and isn't primarily a legal question. Maybe one can argue that if the signer selected or constructed the placeholder (signature) himself—by, for example, typing the name—it has more legal weight compared to methods where that's not the case, because it better demonstrates the signatory's intent to sign the document.

3.1.1 Click-2-Sign

This is somewhat the equivalent of the stamp imprint in the old paper world. Proper e-signature software will allow you to define the elements of the stamp imprint. Depending on the use case, you might only want to include the name of the signer, or also IP-address, geolocation and other information. Maybe you even want to add a text that states this is an electronic signature and not a real one.

3.1.2 Typing the name

This method allows the possibility to enter the name and use various handwritten fonts to convert the name into a placeholder that looks like a handwritten signature.

3.1.3 Draw with finger, mouse or stylus

The final method allows the signer to draw their signature as they are used to doing on paper. This is close to methods where you try to capture the real signature, but typically people are not able to draw their signature with a finger and most people definitely cannot with a mouse. Also, even if a stylus is used, the signature image is not forensically identifiable. Therefore, the separate authentication step is still required.

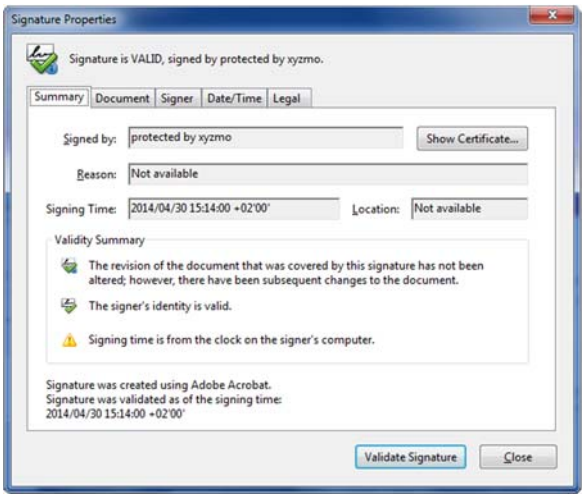
3.2 Certificate-based personal signature

Some industries or countries demand certificate-based personal digital signatures. In this case, senders need to be able to require signers to apply digital signatures with third-party signing certificates.

The process is very similar to the standard process:

- Create a new envelope and add documents to the envelope normally
- Add recipients normally
- Require the signer to apply a personal digital signature
- Add any other authentication options for the recipient
- Add any other recipients for the envelope. You are not required to set any security options or digital certificate requirements for the other recipients.
- Complete designing the document and sending your envelope normally
- The recipient opens the envelope and adds information in all the required fields as with all other methods. When the signer is ready to complete the signing process, he/she digitally signs the document
- The signer is asked to review and confirm the information, maybe including the reason for the signature, their company, and location

After that, everyone can inspect the digital signature in a popular PDF interface like Adobe Reader to review the signature and X.509 information for the completed PDF.



3.3 Forensically identifiable signatures (biometric signature)

A forensically identifiable signature is much more than just a digitized image of a handwritten signature. It requires recording the handwritten signature of a person using all available parameters, such as acceleration and speed—meaning the writing rhythm. These parameters are unique to every individual and cannot be reproduced by a forger. That's why the digitized signature will be forensically identifiable.

When someone claims, "I didn't sign that," a forensic expert can perform a deep manual signature verification at any time afterwards, using specialized software to get an admissible result just as the expert would with a signature on paper. Some solutions also provide a signature verification that authenticates a signature against a pre-enrolled signature profile database in real time. This then allows you to not only secure the execution of certain transactions, but also to provide a ready-to-use audit-trail in case of a dispute, thus putting the burden of proof immediately on the signer.

Any biometrical signature data should be encrypted asymmetrically, using a public key, directly while the signature is being recorded. Reading the signature for verification purposes should only be possible by decrypting it with the corresponding private key, which should either be stored offline, (such as with a notary) or online, for example in a High Security Module (HSM), if that is what's required.

To prevent theft of the captured biometric data from, for example, a signature tablet, there's a range of security mechanisms. One can encrypt the communication between the signature-capturing device and the computer, or there can be an end-to-end encryption of the signature data on the signature-capturing device itself.

Capturing forensically identifiable signatures always requires a local component on the computer, on the mobile device or a proper applet for web applications. By definition, HTML5 alone can only capture images of signatures, not biometrical data. Thus, it can only be used for placeholder signatures as introduced in chapter 3.1.

3.3.1 Stylus

Signing with a capacitive stylus gives you the feeling of signing with a pen. There are still a few shortcomings compared to signing with a native pen, which typically result in larger signatures that are written with a slower speed. However—in contrast to signing with a finger—the captured writing rhythm of signatures by an individual with a stylus is still unique and similar enough to a native-pen signature that a forensic (also called *graphology*) analysis can be applied.

3.3.2 Native pens

Native pens typically provide a signing experience that is, compared to a capacitive stylus, even closer to the act of signing we all grew up with.

The reason for this is that native pens provide:

- A thin pen tip like your ink-to-paper pen that enables you to sign with your regular small letters
- Palm protection so that you can touch the screen while signing without reducing the quality of the captured signature

On top of that, native pens also provide a better data quality because

- They provide a higher data rate, allowing you to capture all aspects of even very fast signatures
- Many also capture the pressure information of your writing, which—while not mandatory for capturing a biometric signature—adds extra security as it's additional signature data a forensic expert can analyze

3.3.3 Capturing devices for biometric signatures

On the one hand, there are the traditional signature pads and their pen-enabled screens. On the other hand, there is also a broad selection of smartphones and tablets that have native pen support. In addition, there are special pens that allow very good signature capturing on devices that have no pen support out-of-the-box, like the iPad or iPhone. Many of these special pens even delivery pressure values, some promise even palm protection, but in many cases the palm protection and data rate are not as good as with native pens. However, if you do not have a native pen, you still can use a capacitive stylus as discussed earlier.

In this chapter, we focus on the use case with smartphones, since this is a device that virtually everybody already uses today and thus does not necessitate a special purchase. For a discussion about signature pads & screens, please refer to the white paper "eSigning at the Inhouse Point of Sale".

Use a Smartphone as a Signature Pad

This scenario is perfect for those instances in business when you want to capture biometric signatures, but do not want to deploy signature pads or pen displays.

The typical process is:

- Review documents or complete form fields and add attachments on any computer in the browser—maybe together with a customer, employee or business partner—and use a smartphone as a signature-capturing device
- A native app turns a smartphone into a signature-capturing device. This app should be available on iOS, Android and Windows Phone.
- When the signer is ready to sign a document, a secure communication between the smartphone and the host computer is established
- The signature is captured on the smartphone. It's highly recommended to use smartphones with native pens or a stylus for that, because otherwise you most likely lose the possibility that the signature is forensically identifiable
- After the signature is captured, it's transferred via the secured channel and embedded into the document

4 Security Aspects

Since the signed documents are legally binding originals, security aspects are a major topic. Security has to be bulletproof; otherwise, the digital originals would become worthless.

4.1 Authenticity protection of signatures

Core to all security aspects of e-signing is protecting the authenticity of a signature and its binding to a certain document, and position within that document. It simply must not be possible for an attacker to access, and copy the signature data of one document and paste it somewhere else—whether that be within the same document or onto a new document. Thus securely binding the signature to a unique document via a document fingerprint (hash value) is key—regardless of whether placeholder signatures, biometric signatures or personal digital signatures are used.

4.2 Integrity protection

Once a document is signed, it is essential that it be easily determined whether the signed document is still an original or if it has been altered after the signature was applied. This kind of integrity analysis must be easily available to everyone who is viewing/reading the signed document; otherwise, forging the content of e-signed documents is as easily done as on paper. The actions of every recipient on a signed document should be sealed with a digital signature. As a result, documents are tamper-evident not just at the end of the signing process but from the moment that the transaction is started.

4.3 Audit trail

Paper-based processes can feel safe when it comes to regulatory laws and compliance because they are familiar. But a good e-signature solution creates a built-in audit trail that makes it much easier to validate that proper measures are being taken in the method of signing and distributing a document.

Audit trails should track what happened with a specific document in what order, at what time, and where. A self-contained document with all signatures and digital certificates, including its audit trail, can reside in any storage system and does not need to be kept in a proprietary vault, as a trail consisting of papers would. The audit trail is a powerful tool that can prove who signed a document and when they signed it.

Typically, an audit trail keeps track of the following events and more:

- Date & software version used
- Unique reference that identifies the completed tasks
- Fingerprint of the signed documents
- Emails and notifications sent

- Signer's consent to use e-signatures
- User authentication provided: This is especially very important in cases where there is no capturing of forensically identifiable signatures. In these cases it's the only way to prove that the person in question really signed the document
- Identification, IP address and geolocation of the signer
- Pages viewed by each signer
- Signature creation
- Transaction completion
- Document downloads
- Cancellations
- All other actions on the document

5 Standard vs. Proprietary Approaches

5.1 Document format

According to Gartner Research (Publication ID Number: G00159721), the best document format is self-contained, so it includes the content to be signed, the signature, and the metadata to make it searchable. It should store the information needed for proof in addition to the signature—the date, time, and consent. Lastly, it should require only a reader that's freely and ubiquitously available to show the document in its originally archived form.

The open Portable Document Format (PDF) fulfills all these requirements. PDF not only is an open standard defined in ISO 32000-1:2008 but also comes in a variant designed for long-term activation defined as a PDF/A in ISO 19005-1:2005. Additionally, digital signatures are well defined within the PDF itself (Adobe PDF Reference PDF 32000-1:2008 12.8.3.3 PKCS#7 Signatures—as used in ISO 32000), meaning that every standard compliant viewing application, such as Adobe Acrobat Reader, correctly shows digitally signed PDFs. Therefore, a PDF or PFD/A file is the perfect analogue to paper in the digital world for archiving signed document originals. All signatures and their cryptographic information should be embedded into the signed PDF. There is no reason why you should need to be a customer of a certain e-signature provider or return to their website just to check the validity of documents.

5.2 True digital signatures versus proprietary e-signature solutions

Some providers try to force their standards on their clients. In some cases, they even call something like that "the new standard." In reality, it's a vendor lock-in. If you use such a solution, you need to be and stay a customer and visit the website of the provider to prove the validity of documents. In case of a dispute, you are dependent on the tools and support of the provider to prove the validity of documents.

Alternatively, you can use solutions that support the ISO PDF standard and true digital signatures, with no proprietary e-signature technology. All signatures and their cryptographic information are embedded in the signed PDF. All signatures are true digital signatures based on documented technical standards that aren't proprietary to the vendor.

In this case, signed documents can be verified easily using free PDF reader software. There's no need to go to any website for verification. By using true digital signatures, you record a history of what each document looked like at the time it was signed and the history is embedded into the PDF document.

You can take a look at the embedded signature history within compliant PDF viewers, even if you're not connected to the internet. In this way, you can see exactly how the document looked when each signer signed.

6 Deployment methods

Some providers focus solely on cloud deployments. You should not choose a vendor that presents you with only this one option: It is not the only possible deployment method. There are still good reasons—data protection and residency issues are just some of the obvious examples—to deploy on-premises behind a firewall, providing maximum control over data and systems.

There is no one-size-fits-all solution. Enterprises and large organizations might even decide that for different needs there are different channels. At a minimum, the following three questions have to be considered:

- How much dependency on internet issues and support from the provider is acceptable to me?
- Which kind of documents do I produce? Are there legal and data privacy issues if I store them on a public server in the internet?
- Since starting with a cloud service is much easier than getting out, how do I get out of the cloud service if I do not want to continue with the provider? What happens to my signed documents and how can I prove in the future that they are properly signed without being dependent on that provider again?

6.1.1 On-Premises

- All applications and documents are within your data center
- You are not dependent on external systems or internet issues

6.1.2 Private Cloud

- Applications are managed by the e-signature provider
- The server is dedicated to you
- You can choose among different geographic regions and maybe even select the provider itself

6.1.3 Public Cloud

- Applications are managed by the e-signature provider
- The server is not dedicated to you
- You can choose among different geographic regions but you cannot select the provider itself
- Your documents are stored on a public server. In many cases they are encrypted, but still are publically accessible.

About xyzmo

xyzmo is a private company based in Ansfelden, Austria, with international offices in the United States and Romania. xyzmo and its predecessors have a combined history of more than 10 years of digital signature expertise. Our solutions have processed millions of electronic signatures around the globe to date.

Trusted by the World's Most Respected Brands

T··Mobile· vodafone kpn Phone House INTESA SANPAOLO BANCO BMG Gruppo Posteitaliane GENERALI