icon uk

SIGNificant

BY XYZMO

Abstract

It is commonly agreed that only organisations investing in process improvements that are driven by the digital transformation and its supporting technologies will emerge as leaders in tomorrow's competitive business world. Digital technologies such as e-contracting will – among other advantages - help these organisations gain market share, get greater margins and profits and hire the best available talent.

However, a very broad spectrum of different e-signing solutions is currently available on the market. Thus, you need to make sure that you select one that fits your business and covers not only the requirements you face today, but also the ones you will face tomorrow.

This whitepaper will help you choose the e-signature solution that is right for you. It will not only introduce the most popular e-signing technologies for each use case, but also explain why you have to look beyond pure e-signing activity to speed processes, lower operating costs, avoid lost or missing data and documents and provide superior customer experience. You will learn about the benefits of having a multi-channel e-signature platform, what you need for a reliable proof of signature and how to keep your signed documents safe. Then we discuss what is necessary for a true platform approach that can cover all the required use cases and fits into your IT environment. Finally, we point out the advantages of standard-based versus proprietary approaches and highlight the key benefits you can achieve by implementing SIGNificant for your e-contracting needs in more detail.

Table of Contents

1 E-Signatures - SIGNificantly Easy and Flexible

As you start to think about how to turn your old paper-based process into a digital process, keep in mind that you will need a high level of flexibility within your e-signature suite. There are many different use cases, participants in the process and types of devices that you and your clients will want to use during the process and actions that have to be completed within this last step in completing a contract.

A robust e-signature solution helps you manage the e-signature process from beginning to end in a complete and entirely secure way while also ensuring that all participants can easily access the final signed document. The goal is to have the best possible user experience when completing a document-based transaction so that she or he would like to do it again, potentially leading to new business opportunities.

Thus, an e-signature solution has to do more than just capture a signature: It has to improve the entire process that comes with it, including processes inside and outside the document itself. Additionally, customers want an omni-channel experience, with the flexibility to start a transaction in one channel and complete it in another one. Consequently, they have to be able to close transactions from anywhere, at any time, on any device.

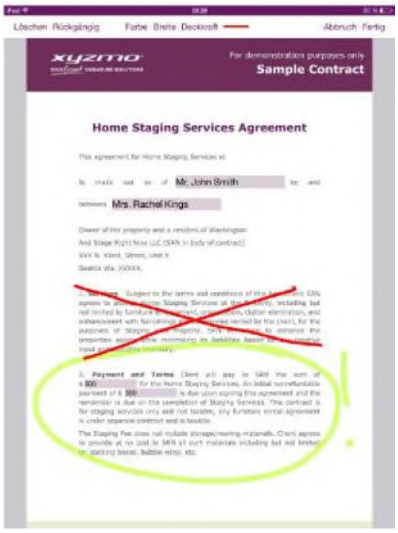
All these requirements are best fulfilled with a true e-signature platform built to support the relevant business cases end-to-end.

1.1 More than just signature capturing

Completing a contract not just involves signing, but potentially also editing, filling out the document itself, or attaching other documents. The more complex this process is, the more likely it is that mistakes will be made, which makes providing proper guidance to the signers highly desirable to avoid expensive process mistakes. Finally, workflow rules for document distribution and completion help ensure that all participants are automatically involved at the right time so that the sender only has to step in if something goes wrong.

1.1.1 Enable signers to work with documents as if they were paper

In many cases a document has to be edited by the signer before he or she can actually sign it. For example, the signer may need to fill out form fields (such as answers to health questions in an application for a life insurance), add photos at a pre-defined location at a certain size (e.g., as proof for a real-life situation) or attach document scans (e.g., of the signer's ID) or other attachments. Additionally, you may even want to allow the signer to edit the document without any constraints as if it were a piece of paper. For example, the signer could make annotations (with a typewriter or freehand) or highlight certain areas (with a text marker), which are basic document tools often used when concluding a contract.



For demonstration purposes only

Sample Contract

Home Staging Services Agreement

This agreement for Home Staging Services at

is made and as of Mr. John Smith by and

between Mrs. Rachel Kings

Owner of the property and a resident of Washington

And Stage Right Now LLC (SRN in body of contract)

XXX N. [illegible] Street, Unit X

Seattle Wa. XXXXX.

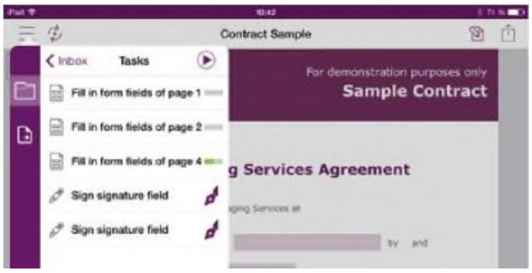
~~1. Services. Subject to the terms and conditions of this Agreement SRN agrees to provide Home Staging Services at the Property, including but not limited to furniture placement, organization, clutter elimination, and enhancement with furnishings and accessories rented by the client, for the purposes of Staging the Property. SRN will strive to enhance the properties assets while minimizing its liabilities based on any creative input [illegible] deems necessary.~~

2. **Payment and Terms.** Client will pay to SRN the sum of $ 800 for the Home Staging Services. An initial nonrefundable payment of $ 300 is due upon signing this agreement and the remainder is due on the completion of Staging Services. The contract is for staging services only and not taxable, any furniture rental agreement is under separate contract and is taxable.

The Staging Fee does not include storage/moving materials. Client agrees to provide at no cost to SRN all such materials including but not limited to: packing boxes, bubble wrap, etc.

1.1.2 Guide signers in a document

You have to be able to design the optimal user experience and enforce workflow rules within a document in order to eliminate expensive process failures such as missing signatures, data entries or attachments. Therefore, you will want to add signature fields and other tags to help your signers know precisely what actions you want them to take, where in the document you want them to sign or to add information such as user data or photos.



Contract Sample

Inbox Tasks

Fill in form fields of page 1

Fill in form fields of page 2

Fill in form fields of page 4

Sign signature field

Sign signature field

For demonstration purposes only

Sample Contract

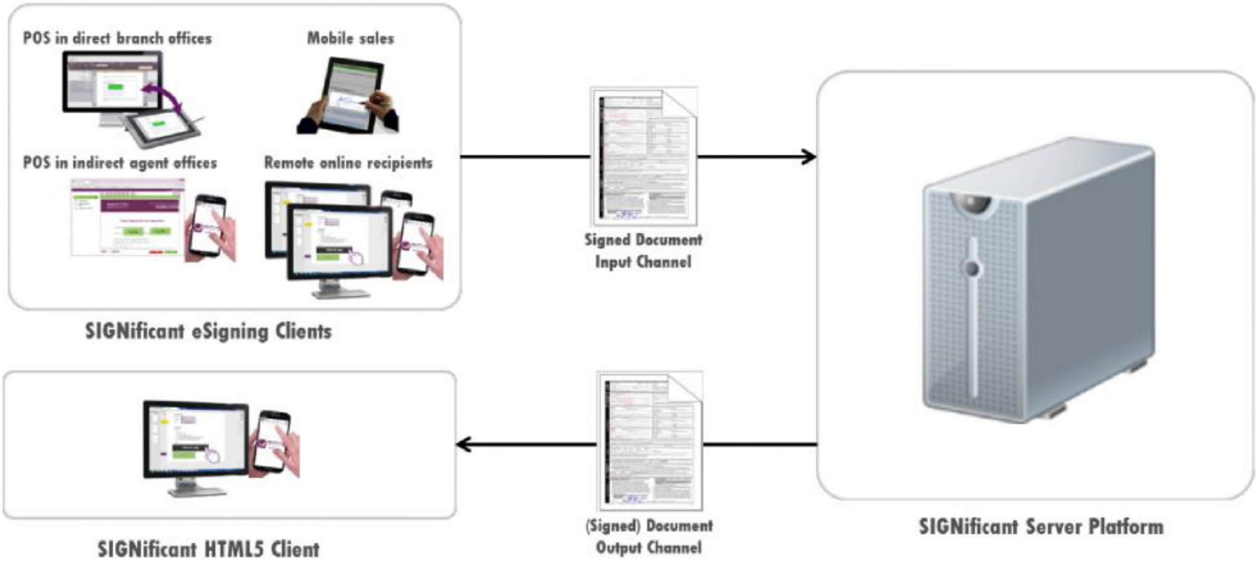
g Services Agreement

1.1.3 Easy and secure access to the signed document

Once a document is signed you typically need to provide all external signers an easy way to access the signed document. However, a simple e-mail will not work, because e-mail is not a secure delivery mechanism.

To overcome this issue, the recipient only receives a download link to the document. To ensure that only the intended recipient downloads the actual document you may define a required client authentication – for example via SMS/TAN using the mobile phone number you already got (e.g. from the application form / signed document). This way the recipient does not even need a registered user account, which means he does not need to remember login data such as username and password.

The same process can also be used to safely deliver documents to signers that have been created based on a signed document. An example for this is an insurance policy that has been created based on a signed insurance application form.


POS in direct branch offices
Mobile sales
POS in indirect agent offices
Remote online recipients
SIGNificant eSigning Clients
Signed Document Input Channel
SIGNificant Server Platform
SIGNificant HTML5 Client
(Signed) Document Output Channel

1.2 Multi-channel and device support

Closing transactions anywhere, at any time and on any device means providing full coverage for the following channels:

- In-house point-of-sale (POS) in branches, stores, receptions, etc. - e.g. on a POS-PC with a signature screen used to display the document to be signed and capture a client's signature directly on the displayed document.
- External point-of-sale through independent business partners (such as agencies) - e.g. on a POS-PC with a smartphone, so that the PC displays the document to be signed on its screen and the smartphone is used to capture the client's handwritten signature.
- Mobile sales and service delivery (door-to-door agents) - e.g. on a mobile tablet that is used to display the document to be signed and capture a client's signature directly on the displayed document.
- Online/remote - e.g. directly on whatever device the client is using, be it a standard PC, tablet or smartphone.

Given that five years from now the majority of signature transactions are expected to be closed on mobile devices, your company needs to be fully committed to offering e-signatures on all mobile platforms. That means choosing an e-signature solution that is mobile-ready and enables capturing e-signatures through any browser-based mobile device, and on the major mobile platforms through e-sign-enabled native apps.

2 Use Case Driven E-Signature Technologies

The choice of which e-signing technology will be best in a given case typically depends on the respective use case and its unique requirements. An overview of the requirements per use case is provided in the table below. A more detailed discussion on them is provided in the use case specific white paper that you can download from:

http://significant.icon-uk.net/resources/e-signature-whitepapers.

E-Signing In-Shop / - Branch	**Mobile Signing in the Field**	**Send Documents for Signature to External Recipients**	**E-Signing within the Organisation**
Use pen displays as a marketing & feedback channel (videos, pictures, questionnaires) when idle	Sign on portable devices based on iOS, Android, or Windows Support mobile sign pads with classic notebooks that don't have touch screens or pen input.	Use any web-enabled device to view, fill out, and sign documents online with • Click to Sign • Type to Sign • Draw to Sign	E-sign online on virtually any web-enabled device
Integration of iOS, Android, and Windows tablets & smartphones in point-of- sale scenarios	Browse and review multipage documents before e-signing them	No need to download or sign up for anything	Alternatively, use signature pads of your choice or
Flexibility to use and exchange signature pads of your choice – incl. smartphones	Complete PDF forms on the go	Alternatively, biometrically sign on smartphones via a small capturing app, while the document is viewed on the PC screen	Or use your existing PKI infrastructure (smart cards, USB tokens, software certificates, HSM)
Support for terminal services	Add scans of driver's licenses, passports, or any other photos		Available browser-based with no local installation
Option to verify a signature in real time	Works even offline		
SIGNificant E-Signature Platform			

For all these use cases, each of the following e-signing technologies has its pros and cons, but most of the time one is preferable:

- Forensically identifiable signatures (aka biometrical signatures) in which the unique characteristics of real handwritten signatures are captured (e.g. speed, acceleration, pressure).
- HTML5 signatures in which the act of signing a signature field is executed by, for example, a click on an "I agree" button or by drawing a signature with a finger or stylus. To ensure that such a signature is authentic, an additional authentication step is required (e.g. a one-time password, e-mail access, portal logins, etc.). All user actions are typically recorded in an audit trail which is required for legal proof.
- Certificate-based signatures that require a public key infrastructure (PKI) which provides personal digital signing certificates for all signers (e.g., using smart cards, software certificates or HSM).

2.1 In-person / face-to-face meetings → biometric signatures (handwritten; forensically identifiable)

Capturing a handwritten signature is still the best choice for getting documents signed when meeting clients face-to-face, either in your premises or on the go. In this scenario, you can present the client with the document on your own infrastructure (e.g., on a point-of-sale computer or a tablet) and the client can sign using whatever device you provide.

The market offers a broad range of signature capturing devices for this use case, such as:

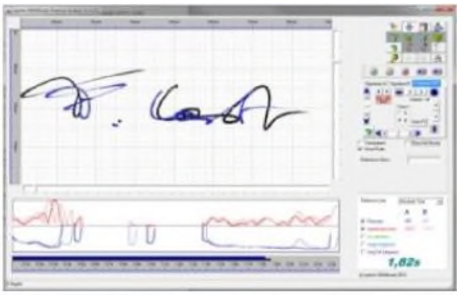
- Basic signature pads with a b/w display,
- Signature pads with a color display,
- Pen-enabled screens with a display size of usually 10" or more,
- Smartphones, and
- Mobile tablets running iOS, Android or Windows.

The type of signature capturing device that best fits such a scenario is mainly defined by the specific use case and environmental conditions at hand.

- Based on current technology, signature pads and pen displays still are often justified, as they provide a superior signing experience and are cheap and easy to deploy and maintain on a large scale, especially in point-of sale scenarios.
- Another very interesting option is to review documents, complete form fields and add attachments on any computer screen, and then use a smartphone or tablet instead of a signature pad for signature capturing. When the signer is ready to sign the document, a secure communication between the smartphone and the host computer is established and a native app turns the smartphone into a signature-capturing device with the ability to capture forensically identifiable signatures.

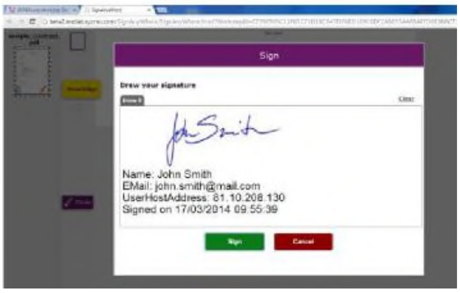
- Mobile apps that allow you to do everything directly on the document displayed on the tablet or smartphone (similar to working with paper) are often the preferred solution when mobility is a key requirement. Especially in this area, offline capabilities have to be provided from the e-signature solution.

There are many choices that only a device-independent e-signature solution offers, the key being the necessary flexibility to integrate the capturing device that fits your current and (maybe not yet known) future needs best. This flexibility is addressed with a modular architecture that enables the introduction of new signature capturing hardware through plug-and-play. Ideally, you can even completely exchange the devices that are in use today with newer devices that are released tomorrow without having to redo your custom integration of the e-signing solution.



Although there are other technologies available, handwritten signatures that are forensically identifiable (also known as biometric signatures) have finally emerged as the industry standard for electronic signatures in such a use case, because handwritten signatures are socially widely accepted and capturing their biometrical data is seen as non-intrusive for the masses - especially when the signing environment at the point-of-sale (either on a stationary PC or mobile tablet) is pre-installed and ready to use, so that the basic process for a consumer is the same as on paper.

2.2 Online transactions with remote recipients -> HTML5 signatures



Sign

Draw your signature

Name: John Smith
EMail: john.smith@mail.com
UserHostAddress: 81.10.208.130
Signed on 17/03/2014 09:55:39

HTML5 signatures, in contrast, are best suited for processes in which the customer, employee or business partner has to sign a document remotely on virtually any Internet-enabled device without a physical face to face meeting. HTML5 signatures do not require any upfront installation, making it easy for the signer to sign on his or her own device (e.g. smartphone, tablet or computer).

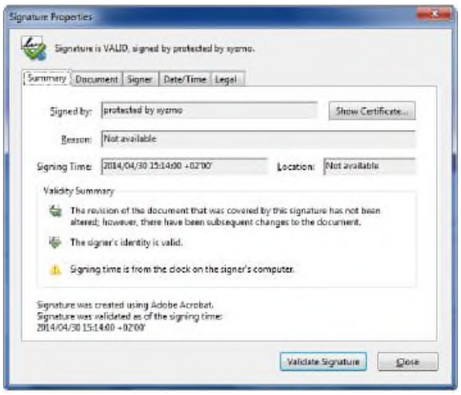
HTML5-based approaches can typically only capture handwritten signatures of mediocre quality, not comparable to signatures from signature pads or tablets equipped with a stylus/pen and a native app. Thus, an extra step of securely authenticating the signer has to be added, as the image of the signature itself (even if a handwritten one is used) will not stand up in the case of dispute.

For corporate signers, access to the corporate e-mail which contained the link to the original document is often seen as sufficient. When doing business with consumers, however, more solid authentication methods are required. Popular examples include SMS-TANs sent to the recipient’s mobile number and reusing the existing login token. If this authentication is securely documented in an audit trail, then an HTML5 signature provides reliable evidential weight.

The big advantage of HTML5 signatures is that they do not require the signer to install anything. They simply work on virtually any HTML5-enabled web device. In addition to their authentication, they also do not require complex signup procedures, so they are perfectly suited for online B2C, B2E and B2B scenarios.

In situations in which the advantage of not having to install anything on a field agent device outweighs the disadvantage of having signatures that are of lower quality (e.g. because they are authenticated anyway with scanning their ID) and being dependent on Internet availability to close the business, HTML5 signatures may even be used for in-person meetings.

2.3 PKI infrastructure given -> certificate-based signatures



Signature is VALID, signed by protected by xyzmo.

Signed by: protected by xyzmo

Reason: Not available

Signing Time: 2014/04/30 15:14:00 +02'00'

Location: Not available

Validity Summary

The revision of the document that was covered by this signature has not been altered; however, there have been subsequent changes to the document.

The signer's identity is valid.

Signing time is from the clock on the signer's computer.

Signature was created using Adobe Acrobat.
Signature was validated as of the signing time:
2014/04/30 15:14:00 +02'00'

Some use cases, industries and countries demand certificate-based personal digital signatures. In those cases, the highest legal value of a signature - which is deemed to be equivalent to a wet ink on paper signature - can only be realised by using certificated based signatures. This generally applies to the so-called Qualified Electronic Signatures (QES) used in the European Union.

For these scenarios, the e-signature software has to be able to require signers to apply qualified digital signatures with third-party signing certificates.

Also, in cases in which the signer already has a Public Key Infrastructure (PKI) with a personal digital signing certificate (such as on a smart card, USB token or purely as a file on a computer) in place, this certificate can be used to not only authenticate the signer, but also to digitally sign a document. Most of the time, pure certificate-based signature implementations are considered when a PKI infrastructure already exists for other purposes.

Some European national identity cards provide functionality for executing a qualified electronic signature (QES). Although this is theoretically a great way to use these identity cards, market penetration and user acceptance is often a problem. Typically, card owners have to activate and pay for this function separately and also require a card reader to use it. This results in low market penetration, which makes its use problematic in B2C scenarios. Thus, the other two previously mentioned e-signature technologies are the only viable option for most scenarios.

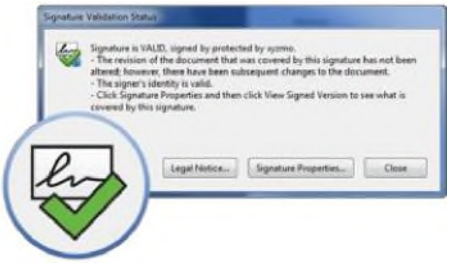
3 Security

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

3.1 Authenticity protection

Protecting the authenticity of a signature and its binding to a certain document and position within the document is core to all security aspects of e-signing. It simply must not be possible for an attacker to access and copy the signature data of one document and paste it somewhere else - be it within the same document or into a new document. Thus, linking the signatures to the document and encrypting them securely is key. If the biometric signature data is stored outside the signed PDF document in a database, which is an optionally implementation method, the link between the signature data and the document (= hash value of the document to be signed) must be provided via a digitally signed audit log, which authenticity and integrity itself is guaranteed. The same applies to HTML5 signatures.

3.2 Integrity protection



Signature is VALID, signed by protected by xyzmo.
- The revision of the document that was covered by this signature has not been altered; however, there have been subsequent changes to the document.
- The signer's identity is valid.
- Click Signature Properties and then click View Signed Version to see what is covered by this signature.

Once a document is signed, it is essential that it is easily accessible, whether the signed document is still an original or has been altered after the signature has been applied. This kind of integrity analysis should be available to everyone viewing/reading the signed document within the most popular PDF readers. Having to depend on coming back to the signature vendor's website to view the signed document is not only inconvenient, but also a big burden for long term archiving.

It should also be possible to fully automate this integrity check before the PDF is further processed or stored in an archive.

3.3 Limiting access to documents

In contrast to paper, digital files can easily be copied without losing any of their characteristics. If a digital file is an original, a digital copy of it creates another valid original. This has a lot of positive aspects, but can also be an issue for cases of dispute in the future, assuming that technology progress might make it possible to fake the original using a technology of tomorrow. If you want to be certain that there is only one valid original, which you also manage centrally, you have to limit access to the original signed document. Therefore, you have to make sure that the e-signing solution does not simply distribute the original PDF to all decentralised signing stations - which would greatly increase the complexity of securing access to the signed original.

3.4 Allow only authenticated users to sign a document

You may want to increase process security further by ensuring that only authenticated users are able to sign a certain document. If you document the results of the user verification in a secure audit trail, you not only greatly reduce fraud, but also dramatically increase the evidential weight of the signature and place the burden of proof on the signer.

With biometric signatures you can do that, simply by dynamically verifying the signatures in real-time against a pre-enrolled biometrical signature profile database. Well-known examples here are client authentication for bank transactions and management/staff authentication for high value purchase orders.

With HTML5 signatures, this is accomplished with a required upfront authentication, which can even include multiple steps, such as e-mail access combined with an SMS-TAN sent to a registered phone number. As this method is typically used for remotely signing a document, you can also use this method to block access to the document for unauthenticated users.

4 Long-term Document Archiving

4.1 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. In addition, it should store the signature process evidence data, such as the signing date, geolocation and the like. Last, it should require only a reader that's freely and universally available to show the document in its original 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 storage and 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 analogy to paper in the digital world for archiving signed document originals in any archiving solution of your choice. All signatures and their cryptographic information should be embedded into the signed PDF. There is no reason why you should be locked in to one provider (e.g. need to be a customer of a certain e-signature provider or return to their website just to check the validity of documents, something that becomes increasingly risky over time as online processes or commercial preferences may change).

4.2 Digital signatures are time-bound

The Digital signature technique is designed for short-term to medium-term validation of digital documents. Digital signatures are intended for validation of documents immediately after transfer. Even the authentication function of digital signatures has a life cycle.

If the authentication of the signer is not provided by the digital certificate but via biometric signature data — see chapter 2.1 — then the impact of an expired digital signature is reduced. In such scenarios, the digital certificate/signatures are typically only used for the following two reasons:

- Prove the document's integrity,
- Prove the identity of the issuer (not the signer!) of the signed document (through the used digital certificate).

One solution for dealing with expiring digital signatures is the re-signing of the documents and/or the preservation of the original bitstream and the validation chain in a proper archiving solution. The signature renewal is typically performed by means of a qualified time stamp and must include the respective data: the old signatures and the time stamp. It is not necessary to renew each individual document with its own time stamp. Several documents can be grouped and signed together with a joint time stamp. In order to provide an attestation for the integrity of a document stored in a longterm archive, the archive system must generate an evidence record for the document, which must contain a seamless chain of valid time stamps / digital signatures - retroactively until the point in time at which the document entered the archive system.

5 Process Evidence

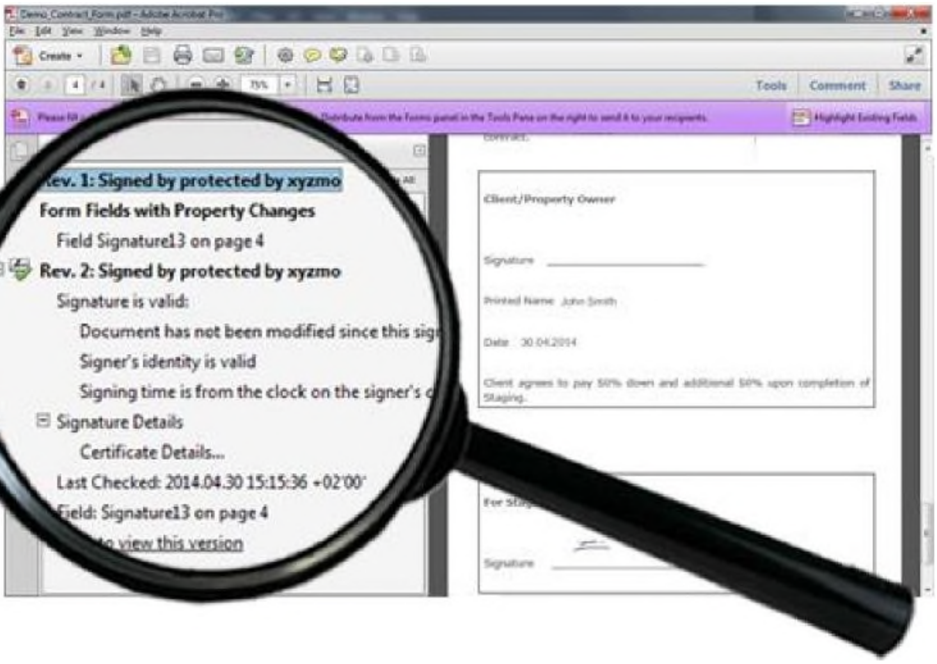
Proving the authenticity of an e-signed document depends on the audit trail that the e-signature solution, which has been used to sign the document, provides. This audit trail can either be stored in the document itself, enabling the document to be self-contained - see chapter 4.1 - or separated, or a combination of both.

Audit trails can also do much more. A proper audit trail that includes authentication results for the signers shifts the burden of proof toward the signer in a court proceeding, especially if the solution has processed a lot of documents already without problems. The judge will automatically have a legitimate expectation that the solution also worked for the document in question. It is important that the audit trail is understandable by the involved judge and lawyers without the need to consult a technical expert for interpretation. If the user actions have also been logged, then this can be used as process evidence and further increase the evidential weight.

Note: Particularly if you use cloud-based solutions, you have to be sure that you have everything you need to proof the authenticity of documents many years later, even if by then you are no longer a client of the vendor or the vendor simply does not exist anymore.

5.1 Evidence provided by a digital signature/certificate

By reviewing the digital signatures in a PDF document, you can look at the embedded signature history within standard-compliant PDF viewers, even if you are not connected to the Internet. This way, you can see exactly what the document looked like when each digital signature was applied.


Demo_Contract_Form.pdf - Adobe Acrobat Pro
File Edit View Window Help
Create
Tools
Comment
Share
Highlight Existing Fields

ev. 1: Signed by protected by xyzmo
Form Fields with Property Changes
Field Signature13 on page 4
Rev. 2: Signed by protected by xyzmo
Signature is valid:
Document has not been modified since this sig
Signer's identity is valid
Signing time is from the clock on the signer's c
Signature Details
Certificate Details...
Last Checked: 2014.04.30 15:15:36 +02'00'
ield: Signature13 on page 4
o view this version

Client/Property Owner
Signature
Printed Name John Smith
Date 30.04.2014
Client agrees to pay 50% down and additional 50% upon completion of Staging.
Signature

Additionally, the digital signature also provides evidence about the following important aspects:

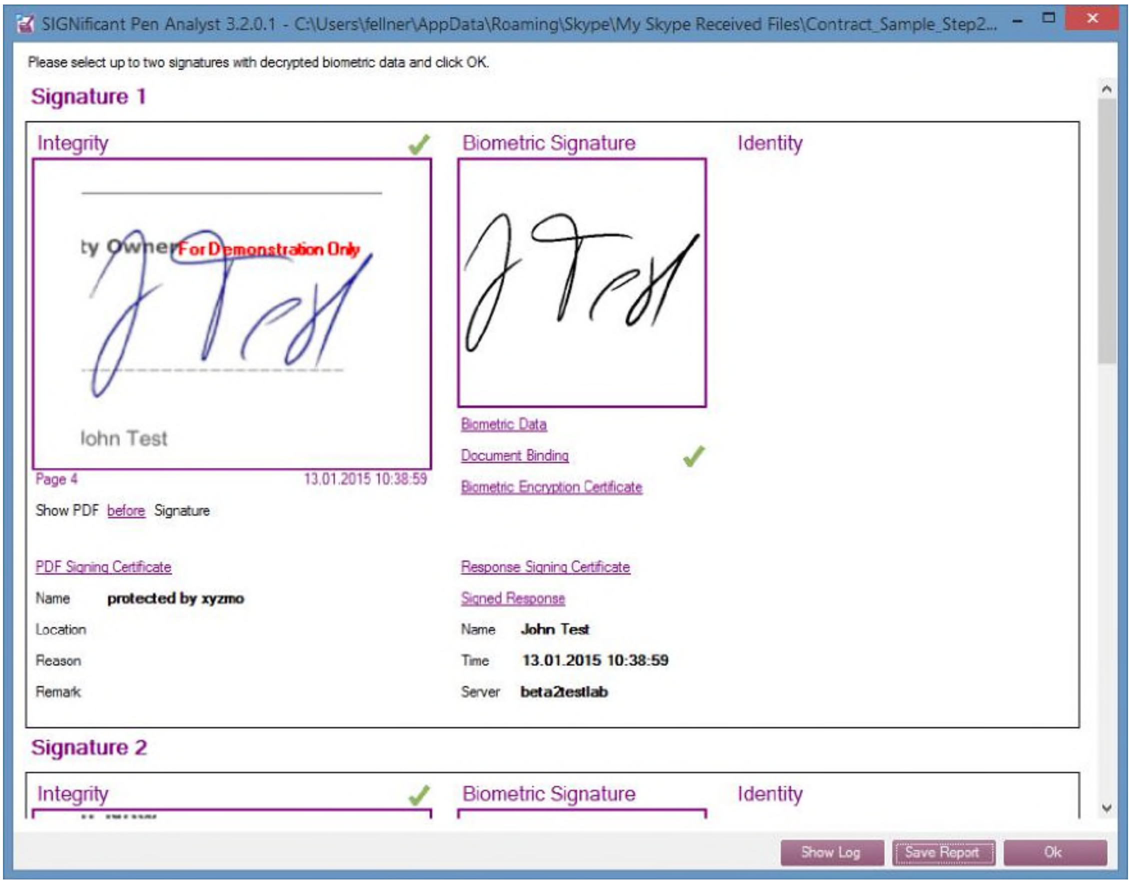
- The document's integrity (see chapter 3.2),
- The date and time the document was signed—optionally through a trusted time stamp service,
- The geolocation where the document was signed (GPS data if provided),
- The issuer of the signed document (through the used digital certificate).

5.2 Evidence provided by biometric signature data

The biometric signature allows you to identify who has signed the document without any additional server-based audit-trails (see chapter 5.3). However, this kind of evidence requires:

1. That it is possible to decrypt the signature data from the document, which can be done using its securely stored private decryption key,
2. That, as in the paper world, a signature expert (graphologist) is able to do a manual signature verification.

The second bullet point may not be necessary in case you can provide evidence that the recorded biometric signature data has been reliably verified in real-time against known sample signatures of the signer before being embedded in the document. To provide trustworthy evidence, the biometric signature must be linked with a signed response to an identified signature verification server (see chapter 3.4). This signed response must be digitally signed to make sure that the system is not vulnerable to bypassing it (e.g. through a hijacked verification service). This way, you can easily prove that the recorded verification results have been provided by a successfully authenticated and certified verification system and thus provide evidential weight.



SIGNificant Pen Analyst 3.2.0.1 - C:\Users\fellner\AppData\Roaming\Skype\My Skype Received Files\Contract_Sample_Step2...

Please select up to two signatures with decrypted biometric data and click OK.

Signature 1

Integrity ✓

ty Owner For Demonstration Only

Iohn Test

Page 4 13.01.2015 10:38:59

Show PDF before Signature

PDF Signing Certificate

Name protected by xyzmo

Location

Reason

Remark

Biometric Signature

Biometric Data

Document Binding ✓

Biometric Encryption Certificate

Response Signing Certificate

Signed Response

Name John Test

Time 13.01.2015 10:38:59

Server beta2testlab

Identity

Signature 2

Integrity ✓

Biometric Signature

Identity

Signature audit trail incl. a signed biometric verification response of a self-contained PDF document

5.3 Typical server-based audit trails

Server-based audit trails can be stored independently from the signed document (e.g. in a central location), which may simplify document archiving and distribution.

5.3.1 Action log

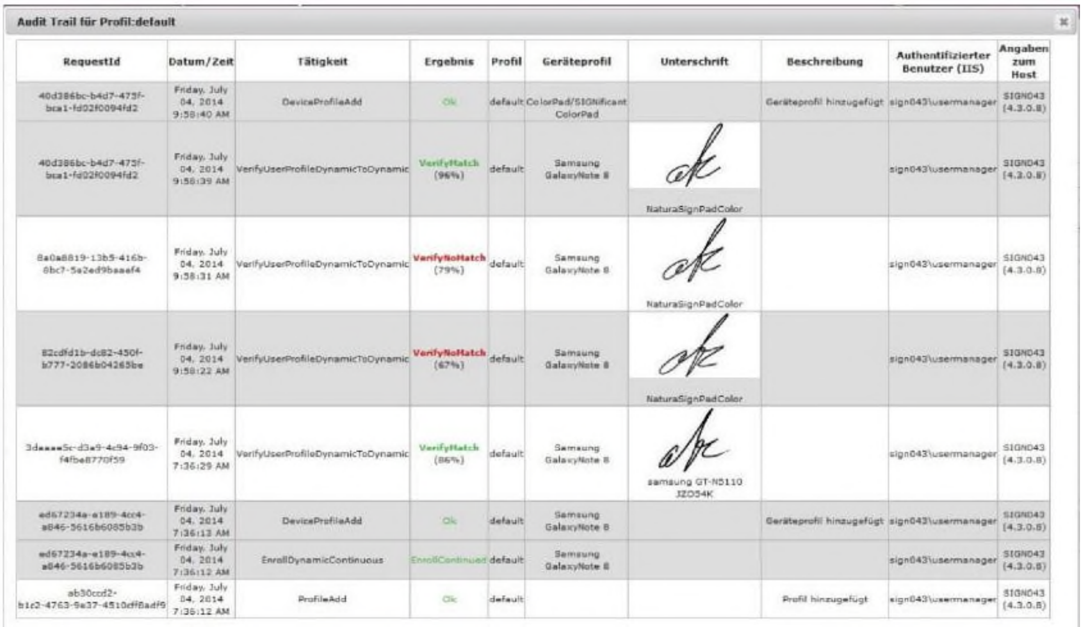
Server audit trails develop their full potential when they provide process evidence such as logging document distribution to a specific point-of-sale or field agent and the executed actions within a document. Audit trails should document what happened to a specific document, in what order, at what time and where. This can include confirmation of pages where special tags have been set which forced the signer to confirm that he or she read the marked sentences. The log should at least keep track of the accomplished tasks that have been performed by the signer based on the predefined guiding through the document (see chapter1.1.2). Certainly, detailed information about executed authentication steps such as typically required with HTML5 signing (e.g. SMS-TANs sent to

registered phone numbers, or scanned IDs) are most critical.

5.3.2 Biometric real-time signature verification audit trail

In case you want to store the captured biometrical data only in a central location - as opposed to storing them in the PDF documents as well - you may simply reference it from the action log (see chapter 5.3.1), using the identifier (RequestID) of the performed verification request, to the audit log of the signature verification server (see image below).

Additionally, as this audit log does not include the biometrical data itself (see chapter 5.2) but only references them, the signature authentication proof is much more accessible because access to it (e.g. the ability to show it to a judge) does not require its decryption using the private key that you need to extract the biometrical signature data from a PDF.



Audit Trail für Profil:default

RequestId	Datum/Zeit	Tätigkeit	Ergebnis	Profil	Geräteprofil	Unterschrift	Beschreibung	Authentifizierter Benutzer (IIS)	Angaben zum Host
40d386bc-b4d7-473f-bca1-fd02f0094fd2	Friday, July 04, 2014 9:58:40 AM	DeviceProfileAdd	Ok	default	ColorPad/SIGNificant ColorPad		Geräteprofil hinzugefügt	sign043\usermanager	SIGN043 (4.3.0.8)
40d386bc-b4d7-473f-bca1-fd02f0094fd2	Friday, July 04, 2014 9:58:39 AM	VerifyUserProfileDynamicToDynamic	VerifyMatch (96%)	default	Samsung GalaxyNote 8	NaturaSignPadColor		sign043\usermanager	SIGN043 (4.3.0.8)
8a0a8819-13b5-416b-8bc7-5a2ed9baaef4	Friday, July 04, 2014 9:58:31 AM	VerifyUserProfileDynamicToDynamic	VerifyNoMatch (79%)	default	Samsung GalaxyNote 8	NaturaSignPadColor		sign043\usermanager	SIGN043 (4.3.0.8)
82cdfd1b-dc82-450f-b777-2086b04265be	Friday, July 04, 2014 9:58:22 AM	VerifyUserProfileDynamicToDynamic	VerifyNoMatch (67%)	default	Samsung GalaxyNote 8	NaturaSignPadColor		sign043\usermanager	SIGN043 (4.3.0.8)
3daaaa5c-d3a9-4c94-9f03-f4fbe8770f59	Friday, July 04, 2014 7:36:29 AM	VerifyUserProfileDynamicToDynamic	VerifyMatch (86%)	default	Samsung GalaxyNote 8	samsung GT-N5110 JZO54K		sign043\usermanager	SIGN043 (4.3.0.8)
ed67234a-e189-4cc4-a846-5616b6085b3b	Friday, July 04, 2014 7:36:13 AM	DeviceProfileAdd	Ok	default	Samsung GalaxyNote 8		Geräteprofil hinzugefügt	sign043\usermanager	SIGN043 (4.3.0.8)
ed67234a-e189-4cc4-a846-5616b6085b3b	Friday, July 04, 2014 7:36:12 AM	EnrollDynamicContinuous	EnrollContinued	default	Samsung GalaxyNote 8			sign043\usermanager	SIGN043 (4.3.0.8)
ab30ccd2-b1c2-4763-9a37-4510df8adf9	Friday, July 04, 2014 7:36:12 AM	ProfileAdd	Ok	default			Profil hinzugefügt	sign043\usermanager	SIGN043 (4.3.0.8)

Using such an audit trail of executed real-time signature verifications that is easily readable by non-technical person and by a non-product expert (such as a judge or counselor), as shown in the image above, and the signed response data of an executed verification stored in the signature field of a signed document (see chapter 5.2), you can greatly increase a signature's evidential weight and reliably prove that only an authenticated and documented person was able to sign a specific document. Thus, the burden of proof that the document was not signed by this person is more or less now put on the signer himself or herself (= reversal of burden of proof).

6 The Platform Approach

Only an enterprise software platform enables you to choose the best solution for every channel, business process and department need, while still maintaining all the advantages of a homogeneous platform. For example, you should be able to deploy native mobile apps for your field agents, kiosk-based systems with signature screens for branch offices, and email document links to end customers for online signing on any web-enabled device. All e-signature solutions should be built on the same core technology, and it should be possible to easily integrate them with each other. You should be able to easily find the most important features across the platform. Many features are typically server-based, but, alternatively, you might need some of them to also be available as stand-alone products.

It might be appealing to simply buy signature capturing hardware, use the original SDK that comes along with it and integrate the devices into an existing process by yourself or with one of your system integrators. But in the long run, you will most likely built a suboptimal, non-integrated solution that way, so it is crucial to have the full platform view in mind before starting an e-signature project.

6.1 Architectural options

6.1.1 Standalone UI or seamless integration via SDK

If you require a fast and cost-efficient deployment, a ready-to-go graphical user interface is typically the best choice. This option usually still allows easy customisation of color schemes, logos, etc. to your requirements.

If you do require a seamless integration into an existing application (without a UI context switch) then the SDK approach will be the right one. Here you can manage the detailed user experience and all GUI elements through advanced coding yourself. Powerful SDKs allow much more than simple integration of core functionality – such as providing a complete adaptable user interface with a framework to seamlessly integrate it.

6.1.2 Using a server-based solution—pros and cons

Some businesses might consider a pure decentralised approach, but for most use cases the server-based approach is preferred as it provides the following advantages:

- The integration to existing systems is purely server-side, which is the natural choice for a server-based back-end architecture.
- The PDF document is only stored in the secure data-center and not automatically distributed to the clients, where access to the signed original can hardly be managed securely.
- A central audit trail documents all user interactions.
- Contrary to the opinion that server-based approaches need a constant network connection from the client, duly built apps can provide offline support for mobile tablets and smartphones through document caching and templating within the app itself.
- There is only one back-end integration necessary for all supported channels / use cases and e-signing technologies (see chapter 2).
- It is perfect for companies which centralise their front-end software through terminal service solutions as e-signature client applications provide a much better scalability than fat apps that are not distributed over client and server.

In contrast, purely desktop/local-based signing approaches are typically preferred if:

- The document to be signed is created dynamically by the client itself and should not be sent to a server before it can be signed by the client.
- Server-side integration is not necessary.
  Very poor network connectivity between clients and server, resulting in low stability, network bandwidth and high latency (which however can be widely mitigated through local caching and background syncing).

6.2 Deployment methods

Some platform providers focus solely on cloud deployments. You should not choose a vendor that presents you with only this one option unless you are certain that you will never need another approach across your entire organisation! There are still good reasons - data protection and legal data residency issues are just some of the obvious examples - to deploy on-premises behind a trusted firewall, providing maximum control over data and systems.

There is no one-size-fits-all solution. Enterprises and large organisations might even decide that for different needs, different deployment models are preferred. At a minimum, these questions have to be considered:

- How much dependency on Internet issues and support from the vendor is acceptable?
- Which kind of documents do I produce?
- Are there legal and data privacy issues to be considered if I store documents on a public server in the Internet?
- Does it matter if this server is owned by a US company?
- Since starting with a cloud service is much easier than getting out of that service, how do I get out of the cloud service if I choose not to continue with the provider?
- If I do leave the service, what happens to my signed documents and how can I prove, in the future, that they have been properly signed without becoming dependent on that provider again?

Typical choices are listed in the next chapters.

6.2.1 On premises

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

6.2.2 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 hosting provider itself.

6.2.3 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 with the right authorisations or in the case of successful hacking attempts.

6.3 Enterprise integration

There are various options for how you can integrate an e-signature application into your business workflows. The most basic integration is to automate the handover of the document that needs to be signed to the e-signature solution. This can either be done via a virtual printer, through the solution's integration API or through a standard plug-in.

Another option is to start the e-signing process in the system where the document originates - e.g. a quote in a CRM system - and store the signed document back into that system connected to the right entities, such as contacts or accounts. This can either be done manually through the UI and file system, or automatically through integration APIs or plug-ins.

On top of that, managing the users of the e-signing solution in an integrated way with your IT infrastructure - e.g. LDAP - also has to be considered.

6.3.1 Virtual printer

A very straightforward way to integrate an e-signature solution is via a virtual printer driver that uploads the document to be signed to the e-signature solution for further processing. While this is a very flexible and easy to set up option, the drawback is that storing the signed document is typically a manual process.

6.3.2 Integration APIs

A very powerful way to seamlessly integrate the e-signature solution into your existing workflow is through its integration APIs. For server-based systems, SOAP-based APIs have proven to be very effective as they provide broad technology compatibility. The advantage of integration APIs is that they enable you to create a very tight, purpose built and highly automated integration. Although this consequently means that custom development of the integration logic is required, the effort is quite manageable, because integration APIs are typically rather simple.

6.3.3 Plug-ins

Standard plug-ins provide integration out of the box and thus do not require custom integrations. Their disadvantage is that they may not provide the integration in the way you like it, especially if you use a highly customised business application.

Microsoft Office

The Office plug-in allows you to load any document with the click of a button into the e-signing software (such as Word or Excel).

Business Applications (CRM, ERP, etc.)

Here, you typically want to define signers and recipients and the documents which should be signed within your business application. Creating the details of the signing workflow and adding tags for guiding the signers is typically done within the e-signature application. It is convenient to be able to view the current status of the documents within the business application itself. Once the documents are signed, the data should be mapped back to your CRM system and the signed documents should be attached to the relevant entity (e.g. contact or account).

6.3.4 User administration

The e-signing application typically has the following user types that have to be managed:

- Power user - a user who has access to all functionalities, including definition of signing ceremonies, envelopes, and workflows.
- Restricted types of power users - e.g. a signing host which can create and host in-person meetings.
- Registered signer - A user who can sign documents for which he/she is a signer and who receives an overview of all documents that he/she signed.
- Recipient - a user who can sign and /or receive a copy of the documents.

Whereas a recipient can be anybody and thus has an open user account, all other users (power user, signing hosts and registered signers) require a sign-on that needs to be managed in a user database. A single sign-on is a typical requirement here.

6.3.5 Infrastructure

In case you want to deploy the e-signature solution on your own premises, which many enterprise customers still prefer, you have to think about how the solution fits into your existing IT environment and how you can ensure flawless operations even at a high load volume that may dynamically change based on demand.

It is important to consider the cost of running the platform, if necessary, in a load balanced and failure enabled environment that guarantees the required high availability. The ability to virtualise the servers and a linear scalability are basically a necessity in order to be able to react to changing high load requirements.

A more important factor than what OS the servers are running on is actually which client platforms the e-signing software supports, because the signing clients must be able to run on the client machines that are already in use, regardless of whether those machines use Windows, Linux, virtualised thin clients or any of the tablet operating systems. The servers, in contrast, can always run as a virtualised guest OS on your desired server machines.

7 Standard versus Proprietary Approaches

Some providers try to force their standards on their clients. In some cases, they even call something like that “the new standard.” In reality, such an approach is a vendor lock-in. If you use such a solution, you will need to remain a customer and visit the website of the provider to prove the validity of documents. This may be fine for trivial transactions. However, in the case of a dispute, you will be dependent on the availability of tools and support of the provider to prove the validity of your documents. This may become increasingly challenging if systems change after the transaction occurs; it is rare for even large organisations to consistently maintain the highest standards of change and version control necessary for documents to be used as reliable court evidence when events in question occurred years prior to the case being heard.

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 are not proprietary to the vendor. Digital signatures are placed at every signature in the document and produce a tamper-evident seal. If there is an attempt to make unauthorised changes, the e-signed document will be marked invalid. In this case, signed documents can be verified easily using free PDF reader software. There is 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 are not connected to the Internet. In this way, you can see exactly what the document looked like when each signer signed. Long term histories are not a problem with this approach.

Captured biometric signatures should be exportable via the biometric data interchange formats ISO/IEC 19794-7:2014. Thus a graphologist can use his or her own analysis software and is not dependent on the e-signature vendor.

The right stress test for any implementation is to assume that your vendor disappears and ask yourself what you will have to take to court.

8 Dump the Old World Paper-Based Processes with SIGNificant

Using the SIGNificant enterprise platform enables you to choose the best solution for every channel, business process, and department need, while still maintaining all the advantages of a homogeneous platform. For example, you can deploy native mobile apps for your field agents, kiosk-based e-signing on signature screens for branch offices and email document links for end customers to sign online on any web-enabled device. All our e-signature solutions are built on the same core technology and can easily be integrated with each other. You will find the most important features across our platform. Many features are available both as server-based and as stand-alone products.

- Save money on the costs that accrue when you use a physical material.
  - Printing
  - Scanning
  - Sending/logistics
  - Re-keying errors
  - Archiving
  - Shredding
- An optimised process leads to more sales.
  - Spend more time with clients because you don't need to print, retrieve/find and send paper documents any more.
  - Electronic feedback forms allow better communication with clients.
  - Point of sale advertising opportunities exist (especially with a large screen).
  - High quality customer email addresses can be used for direct marketing.
  - Signed documents can be retrieved immediately, enabling real-time decision making.
- Delight customers.
  - Customers have a higher comfort level because they are enabled to receive documents online.
  - An omni-channel user experience allows clients to start a transaction in one channel and complete it in another.
  - E-signatures present a modern image of your company.
- Make use of increased security and fraud prevention.
  - Documents cannot be altered.
  - Only authenticated users can sign documents.
  - Putting the burden of proof on the signer puts you at lower risk.
- Save the environment and generate good PR.
  - Lower your company's carbon footprint.

Icon^{UK} and Namirial

Icon^{UK} is the sole UK distributor for Namirial's leading e-signature suite in the British Isles. We supply Namirial software, services, associated hardware devices and digital assets, together with complementary solution components to our clients and partners. We do this through a mix of direct and channel partner relationships. Our goal is to support client organisations to become fully digitally enabled with efficient 'straight-through' workflows with embedded identity management.

Having conducted reviews of all e-signature providers, IconUK can assure prospective clients that Namirial technology facilitates secure, legally robust and easy to use digital signing capabilities more comprehensively than any other e-signing provider for organisations that demand high levels of control with excellent user experience.

We not only provide best-of-breed functionally for document centric Identity Management, but also for Customer Communications Management with icon Document Creation and Output Management software, and specialist hardware (e-signing pens and pads) from leading providers such as Wacom. Our high calibre team designs innovative application infrastructure solutions with analytics, biometric security and industrial scale 'personalised automation' for maximum impact.

Use cases are as different as our customers across every market sector - with each implementation being tailored to provide competitive advantage. To do so we deploy multi-talented teams that can not only configure or implement technology, but firstly understand the customer and their users' journeys – both current and future. Together with our Partners, we can provide business and technical consulting, architecture, integration, implementation, support, data migration and information management services.

Trusted by the World's Most Respected Brands