E-Signing at the Inhouse Point of Sale

Paperless B2C Contracting in Branch Offices and Retail Stores

In today's competitive business climate it is essential to seek cost-cutting possibilities to improve operational efficiency and to pay attention to customer interests and demands to improve the bottom line. Printing documents just to capture a customer signature is not only completely outdated in today's tablet-pervasive everyday life, but is also a great waste of time and money. More than that, paper handling is very time-consuming for sales and service personnel and thus reduces the possibilities for efficient customer communication, which in turn limits upsell and cross-sell opportunities.

Modern e-signature-based digital document processes are now geared up to remedy the situation, as they are able to close the final gap in the quest to go fully paperless at the point of sale (POS). This white paper looks at the specific requirements for such e-signature software in typical business-to-consumer (B2C) use cases in stationary environments as can be found in today's bank branches, retail stores and customer centers.

First, this white paper helps you to select the most appropriate way to e-sign your digital documents in your POS scenario. 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 fixed POS installations. Next, we point out that e-signing is much more than simply signing digital docuuments—it's about productivity. Finally, the paper introduces the xyzmo SIGNificant e-signature platform and outlines a few case studies that show different implementations in stationary POS scenarios across the industry.

1 Selecting the Right Methodology

Today, there are quite a few different biometrical e-signature solutions for mobile use cases available on the market. They can mainly be differentiated in the following three areas:

- document format
- signing device
- deployment model.

1.1 E-signature technology

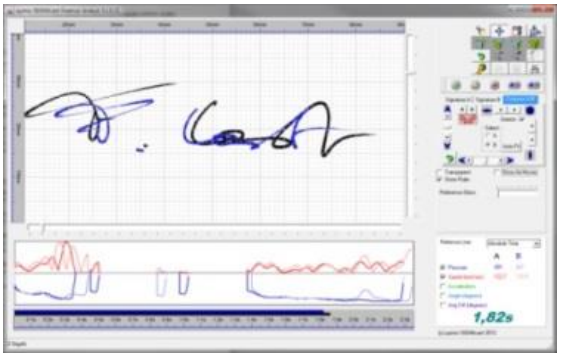
The most popular e-signature technologies for B2C processes are:

- online signatures in which user actions (e.g. click on “I agree” button or signing with an image) are recorded in some kind of audit trail and where user authentication can be provided through additional steps (e.g. one-time password, e-mail access, portal logins, etc.);
- forensically identifiable signatures (aka biometrical signatures) in which the unique characteristics of real handwritten signatures are captured (e.g. speed, acceleration, pressure);
- certificate-based signatures that require a public key infrastructure (PKI) that provides personal digital signing certificates to potential users (e.g. using smart cards or online access).

In a B2C POS scenario, PKI-based approaches do not work well. A reason might be that the penetration even of “national initiatives” is still quite low, most likely because of the costs and inconvenience of such approaches, especially to people that are not used to working with the latest technologies. Consequently, companies must expect that potential clients either simply do not own a personal signing certificate or cannot use it if they have one (e.g. because they forgot the access PIN or the smart card that stores the certificate).

Online signatures, in contrast, are best suited for B2C processes where the client needs to sign a document remotely without meeting a sales person physically face to face, because they do not require any upfront installation, meaning that the client can easily sign on his own device (e.g. smartphone or PC). In this case, the extra step of authenticating via another method then the pure signature act (e.g. drawing/writing the name) seems to be acceptable for clients.

This is why capturing a handwritten signature is still the best choice for getting documents signed in person, in real time, by presenting a document to a customer. Although there are other biometrical technologies available, handwritten signatures that are forensically identifiable have finally emerged as the de facto industry standard for electronic signatures in B2C environments, 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 POS is pre-installed and thus ready to use and the basic process for a consumer is the same as on paper.



1.2 Document format

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

Other than proprietary document formats and document databases, the open portable document format (PDF) fulfills all these requirements. PDF is not only an open standard defined in ISO 32000-1:2008, but it also comes in a variant designed for long-time archivation defined as a PDF/A in ISO 19005-1:2005. Addtionally, 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. So, a PDF or PFD/A file is the perfect pendant to paper in the digital world for archiving signed document originals.

1.3 Deployment model

Finally, you need to choose the deployment model of your e-signature back-end infrastructure should you choose a client/server architecture (see Chapter 3.2 for the pros and cons). It is possible either to run it in the public or private cloud and consume it through a SaaS model, or to deploy and run it on your own premises.

Whereas the cloud model is faster and easier to set up, and also typically provides a limited option to define where your servers and data should be located, the on-premises option is still preferred by many organizations. The reason is that all applications and files are located within your data center, which means that you are consequently not dependent on external systems or Internet issues. Additionally, only the on-premises model gives you full control over data privacy, which is something that cloud services simply cannot guarantee.[1]

With an on-premises model you simply need to choose between a native installation, in which the software runs natively on the computer, and a virtualized approach, e.g. using VMWare, Citrix or Microsoft virtualization technologies.

[1] http://www.zdnet.com/how-one-judge-single-handedly-killed-trust-in-the-us-technology-industry-7000032257/

2 Security Aspects

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

2.1 Authenticity protection

Protecting the authenticity of a signature and its binding to a certain document and position within a document is core to all security aspects of e-signing. It simply must not be possible that an attacker can 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 secure encryption of the raw data—the captured biometrical signature—together with the document fingerprint (= hash value) is key.

In addition to the traditional signature verification by a forensic expert, online signature verification allows you to authenticate a signer in real time. Through that, you can guarantee that a document or transaction can be signed only by the right person, which also dramatically increases the evidential weight. Well-known examples here are client authentication for bank transactions and management/staff authentication for high value purchase orders.

2.2 Integrity protection

Once a document is signed it is essential that it is easily assessible whether the signed document is still an original or whether it has been altered after the signature has been applied. This kind of integrity analysis must be easily available to everyone who is viewing/reading the signed document, otherwise forging the content of signed documents is as easy as on paper.

2.3 Audit trail

Audit trails should track exactly what happens with a specific document in which order, at what time and where. A self-contained document with all signature and digital certificates including its audit trail can reside in any storage system and does not need to be kept in a proprietary vault.

2.4 Limiting access to documents

In contrast to paper, digital files can be easily copied without losing any of their characteristics. If a digital file is an original, a digital copy of it creates another valid original. In case you want to limit access to an original signed document for security reasons, you have to make sure that the e-signing solution does not simply distribute the original file to all decentral signing stations—which would very much increase the complexity of securing the access to the signed original.

3 Architectural Choice for a Fast and Seamless Integration

An e-signing application typically consists of a front-end and a back-end component. While the front-end software manages all user interactions, the back-end software processes the document and takes care of its integration into the overall document workflow.

The front-end software component naturally runs on a front-office computing device, which can be either a traditional desktop PC, which then e.g. uses an external signature screen or signature pad to capture a handwritten signature, or a tablet computer. The front-end can either run as a stand-alone pre-packaged GUI application, or as an SDK that can be seamlessly integrated into an existing client application.

The back-end software component either can run locally together with the front-end inside the same application/on the same computer, or can be split off into a separate server application, which means that the e-signing application is distributed over a client and a server.

In the next chapters we look at the pros and cons of each option.

3.1 Pre-packed GUI app or SDK

If you require fast and cost-efficient deployment with ready-to-go graphical user interfaces a pre-packaged GUI application is typically the best choice. If done well, this option still allows the easy customization of color schemes, logos, etc. to customer requirements.

If, however, you 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, moreover, allow much more than the simple integration of core functionality—they also provide a complete adaptable user interface with a framework to seamlessly integrate it.

3.2 Signing on the server—pros and cons

Even when opting for an on-premises deployment model versus a cloud service, in many scenarios a centralized server-based approach for the back-end software component running from your own data center has a lot of advantages over a purely desktop-based approach. These include:

- If existing systems for document creation, workflow management and document archiving are also server-based, the server-side integration is simply much easier.
- The PDF to be signed only needs to be stored and secured in the data center and does not get automatically copied and distributed to all clients, where access to the document could hardly be securely managed.
- A server provides a single point and type of integration for all the different client options you may use to sign documents with:
    - signature pads—managed by a Web application or local SDK;
    - signature screens—controlled by a local Kiosk SDK;
    - smartphones—that run a small signature capture app that connects with a Web application to view the document;
    - tablets—that run native signing clients to display, edit and sign documents;
    - any device—that runs an HTML5 browser.

On top, many companies even centralize their front-end software through terminal service solutions such as those from Citrix or Microsoft Windows, because it makes software deployment and management a lot easier.

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

- the document to be signed is created on the client itself, meaning that transferring it to the signing server would introduce an additional step;
- server-side integration is not necessary at all;
- poor network connectivity to the decentral clients is a big issue, resulting in low network bandwidth and high latency—thus poor overall performance—although this point can be widely mitigated, e.g. through local caching and background syncing.

4 Aspects that Are Important Specifically to Fixed POS Installations

The typical end-to-end business process for e-signing in branch offices, retail stores and customer centers pretty much differs from other use cases such as e.g. mobile signing in the field and customer self-service scenarios. Consequently, companies that want to equip their rather stationary and face-to-face oriented POS environments with e-signing typically are faced with requirements that often are unique to this use case. The most important ones are listed below.

4.1 Flexibility to use signpads from the manufacturer(s) of your choice

The type of signature capturing device that fits best is very much defined by the specific use case and environment condition at hand. The market itself offers a very broad range of devices, including very basic signature pads with a b/w display, signature pads with color display, smartphones, pen-enabled screens with a display size of 10” or more, and tablets running iOS, Android or Windows.

A device-independent solution offers the necessary flexibility and leads to improved satisfaction rates because each customer can integrate the solution using the capturing device that fits their needs best. This is best 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.

4.2 Fast operation in low bandwidth environments

Especially when deploying a server-based architecture, questions about response times and bandwidth requirements between client and server become important. Server-based solutions can minimize their bandwidth requirements through local caching and background synchronization.

Response times are dependent not only on server performance and scalability, but also on the response time of the signature capturing device. While tablets with native apps and signature screens by design work with virtually no delay, this is not the case with USB signature pads. The reason is that signature pads are peripheral devices that only display the content they receive through their USB connection—typically as images. The typical response time of signature pads with color display is about 2–3 seconds for transmitting the data from the host PC (desktop) to the signature pad.

4.3 Show the whole document

Signature pads

It is possible to show the document to be signed already on a signature pad with a color LCD of 4–5” given that it provides a high enough resolution. This is basically true for many models including Wacom STU-530, SIGNificant ColorPad 6, StepOver naturaSign Flawless Pad, etc. To overcome their limited display size the devices allow you to scroll the document on the signature pad, either autonomously or through communicating with the e-signature software running on the host PC

(desktop). As outlined above, the response time of the data transmission has to be taken into account.

Signature screens

Signing on screens with a size of 10” or above very much requires e-signature software that manages it appropriately, otherwise you will not have the benefit of all their strengths. The reason for this is that they simply act as a second screen while signature pads operate as peripheral devices that only show what is explicitly pushed on their display.

An advantage of signature screens is clearly their instant responsiveness, which is pleasantly different from the rather slow multi-second response time of color signature pads. Screens also work great for showing videos and high-resolution images, which works very well for running commercials when they are idle.

However, in a typical set-up you are using the signature screen next to the main screen for the operator. Even more, the operator simply may not see what is shown on the signature screen. Thus the e-signature software needs to take care of the following:

- When the client reviews and signs a document on the signature screen, the operator must be able to use his screen in parallel without being blocked by the client’s interaction with the e-signing application. Thus, the e-signature solution must block the signature screen from grabbing the focus.
- What is shown on the signature screen versus the operator screen needs to be fully automated, because having to move application windows around manually on two different screens is simply too big a hassle.
- The operator should see what the client is doing on his signature screen, allowing the operator to guide and assist the client using a preview window on his main screen.
- Interactive screens are great for collecting customer feedback. Thus the e-signature solution should be able to present surveys to the client and collect the answers after they have completed the transaction.
- When the signature screen is in idle mode, it should show pre-defined ads such as presentations or videos that are centrally managed by the marketing department. This advertising mode should not interfere with other applications running in parallel on the connected computer of the operator.

Multi-purpose tablets

Mobile tablets like the iPad, Galaxy Note 10 or Surface Pro are primarily built for a mobile use case. However, as they can be used for multiple purposes, provide a rather large screen that allows comfortable display of full page documents, are fairly cheap owing to their mass production and availalble easily, they are also very interesting to use in an in-house POS scenario. If the sales agent does not work off a single desk, but has to be somewhat mobile, they are even more interesting.

An additional advantage is that these multi-purpose devices are turned into biometrical signing devices through a native application that can also be used to cache data, making them independent from unreliable network connections, bandwidth issues and/or slow server response times.

On top, it is very beneficial if the signing application on such tablet devices is tightly integrated with the overall signing solution, which can also be used with other signature capturing devices such as signature pads and screens. Only then is a mixed infrastructure with switching between signature pads and mobile devices, depending on the use case, easily possible.

4.4 Capture biometrical signatures simply with your smartphone

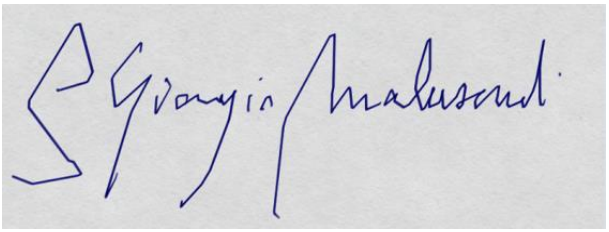
Smartphones, meanwhile, have achieved very impressive market penetration. Nearly everyone has one. So why not use them for capturing handwritten signatures and their biometrical data—especially in situations where you cannot equip the salesperson with special purpose signature pads, screens or tablets? You may not want to equip independent sales agencies with such devices, but you can count on every salesperson in that organization having a smartphone that can be used for signature capturing—so let's use them.

All that needs to be done is to install a small biometrical signature capturing app on the smartphone that is compatible with the back-end component of your e-signature software. Simply sign with a capactive stylus, a finger or with the native pen should the smartphone come with one.

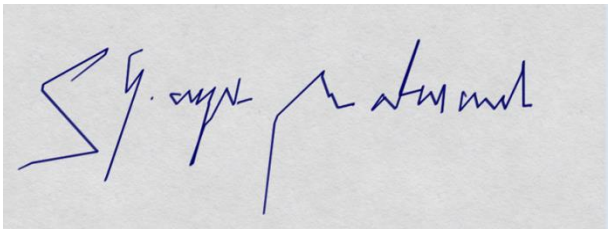
4.5 Enable thin clients to use USB signature capturing devices

In case your desktops are virtualized with Citrix, VMWare or Windows RDP/Terminal Services, your e-signature software needs to locally buffer the data recorded by the USB signature device on the thin client, otherwise some of the captured biometrical data packets will be lost owing to network latency. The reason is that signature pads send the data they record with fire-and-forget, which is not an issue as long as the receiving software runs locally. However, in a thin client environment, the buffer that stores the received biometrical data packets may not read them in time, because access from the receiving software component is delayed by the network's latency. Thus, a simple pass-through does not work.

The illustrations below show how network latency influences the quality of signature capturing without a local software component to take care of correctly receiving the data packets from the USB tablet:



60 ms latency



100 ms latency

4.6 Option to verify a signature in real time for the highest process security

In addition to the deep manual signature verification a graphologist can do in case of a legal dispute anytime after the document was signed, you can also assess the true identity of a signer in real time and document it in a secure audit log.

With this real-time signature verification against a pre-enrolled biometrical signature profile database, you can very much increase your evidential weight and reliably prove that only that certain person was even able to sign a specific document. Thus, the burden of proof that a document was not signed by the authenticated person is more or less now put on the signer himself (= reversal of burden of proof).

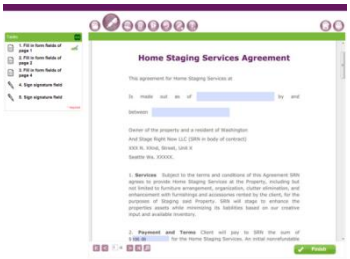
Additionally, some European countries (e.g. Italy) even allow this verification technology based on biometrical signatures to be used instead of a numerical PIN to access a qualified personal signing certificate that is stored in a central high security module (HSM). In this case, users can execute a qualified electronic signature (QES) on digital documents simply with their handwritten signature.

As an electronic signature verification can use all recorded biometric data, the false acceptance/rejection rates it is able to achieve are much better than when simply comparing two or more signature images. Important here is that the solution stays up to date with natural shifts in signing habits over time. In addition, signature capturing has the advantage of lacking the invasive nature of other biometrical authentication methods such as fingerprint, face or retina scanning. A signature, even if hacked, is not reusable since no one can ever sign the same way twice—signatures are bound to be different from one another. Also, the signer can always change a signature and create a new personal profile. By contrast, fingerprints etc. do not change (they are static) and may be used again and again.

5 More than Capturing a Signature

5.1 Avoiding incomplete contracts

Trying to fix ill-signed contracts is often very time-consuming and costly, because when you discover the problem the client typically is long gone and not that easily accessible anymore. Thus it is a huge benefit if you can control and govern all steps in the completion and signing process of documents, including filling out form or signature fields, reading pages, accessing scanners or the camera for adding attachments such as ID scans and much more. Ideally, you can specify compulsory or optional tasks depending on the use case and document, thus giving you the flexibility you need to best cover all your business cases.



Additionally, through defining policies that enable or forbid certain actions on or with the document, such as making annotations, saving, e-mailing, or printing documents, you can exercise any required further control over what clients and operators are allowed to do with your originally signed documents.

5.2 Allow document reading and editing as if on paper

Ideally clients want to work with digital documents as they are used to doing with paper documents. This means that the e-signing application certainly must allow clients to browse and review multi-page documents before editing and signing them—ideally directly on the signing device.

With tablets you can easily go beyond this as they also allow editing documents the way you are used to in the paper world. This includes free-hand and text annotations, mark-ups, attachments, and filling out machine readable form fields. Also the integration of the tablet-based signing solution with the document workflow is key, as you may want to push a pre-filled form document (e.g. a client contract) from a POS PC to a specific tablet device, then allow the client to read and update its form field values before saving any update the client did to the form field values back into your own database.

6 Industry Examples with xyzmo References

With SIGNificant, xyzmo provides an enterprise e-signature platform that allows you to go completely paperless at the point of sale (POS), regardless of whether it is stationary in a branch office or shop, on the go with a mobile sales force or online in a self-service scenario. SIGNificant simply provides you with the user interface and tools needed to define an optimal e-signature process and user experience. Whether for signature pads, interactive pen displays, mobile devices or Web-based signing, the platform's building blocks make it easy to pick and choose the best combination of e-sign solutions and signature capturing devices for each use case in a broad range of industry verticals.

To better illustrate how xyzmo's SIGNificant can be applied in selected industries for their specific use cases in stationary environments, the following section outlines real case studies with their end-to-end business process that has been implemented.

6.1 Retail banking: GE Money Bank (Czech Republic)

GE Money Bank

Use case:

- client bank transactions (deposits, withdrawals, transfers)
- standard contracts (account opening, credit card, etc.)
- loan contracts and agreements
- financial investment contracts

Deployed products:

- Signing application: SIGNificant Server with Web Signing Interface and Linux-based Citrix Components on Dell Thin-Client Terminals.
- Authentication application: SIGNificant Biometric Server—Enterprise Edition with Oracle signature database.
- Signature capturing hardware: SIGNificant ColorPad 6.

End-to-end business process:

1. The client goes to the branch and is welcomed by an employee.
2. If the client is not yet enrolled in the signature database the client authenticates to the operator using an identity card (e.g. national ID) and enrolls in the SIGNificant signature database.
3. The operator processes the client's request (e.g. cash withdrawal).
4. The client reviews the document to be signed directly on the SIGNificant signature pad and signs it directly with his handwritten signature on the pad.
5. The SIGNificant Biometric Server verifies the handwritten signature in real time against the client's signature profile stored in the signature database to execute an authentication check on the transaction.
6. If the result of the authentication is positive, the request is processed and the SIGNificant Biometric Server signs the transaction document with the captured biometrical signature data and then digitally seals it with a trusted time-stamp and a certificate managed securely inside the customer's HSM.
7. The system puts the signed PDF/A document into a legal archive.

8. Nothing is printed unless the client strongly wants a paper copy.
9. The client can access the signed doc on the Web application.

6.2 Retail market: REWE Stores (Germany)

Use case:

- Digitally sign electronic debit process receipts and credit card receipts on self-checkout points with a handwritten signature.

Deployed products:

- Signing application: SIGNificant Server with Cash Register Plugin.
- Signature capturing hardware in shops: Wacom STU-500.

End-to-end business process in the shops:

1. The client goes to the checkout point in the store and registers his purchasing goods for checkout.
2. The client selects to checkout with either electronic debit process or credit card.
3. The client reviews the final bill, time and date, and payment method on the screen of the Wacom STU-500 signature pad and directly signs on it with his handwritten signature.
4. The SIGNificant Server signs the document with the handwritten signature and then digitally seals it with the REWE signing certificate.
5. Nothing is printed unless the client wants a paper copy.

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.

REWE GROUP

Trusted by the World's Most Respected Brands

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