Mobil elektronisch unterschreiben

Papierloser Vertragsabschluss im Außendienst und Service

NAMIRIAL GmbH

Legal Office: Seilerstätte 16, 1010 Wien, Austria
Main Office: Haider Straße 23, 4025 Ansfelden | Phone: +43-7229-88060 | www.xyzmo.com
Fiscalnumber 09 258/9720 | VAT-ID: ATU70125036

Einleitung

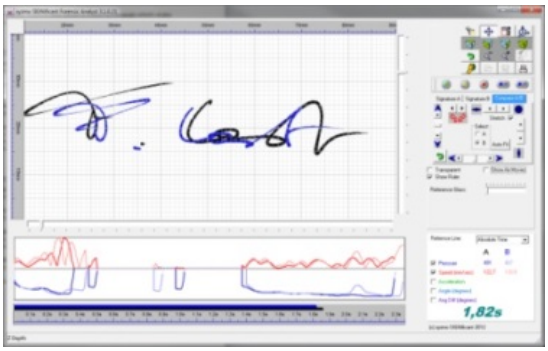
In der heutigen wettbewerbsorientierten Wirtschaft ist es wesentlich, nach Kostensenkungspotentialen zu suchen. Gleichzeitig ist auf die Interessen und Wünsche der Kunden zu achten. Dokumente nur deshalb auszudrucken, um die Unterschrift eines Kunden einzuholen, ist in der heutigen Zeit mit allgegenwärtigen Smartphones und Tablets nicht nur völlig überholt, es ist auch eine enorme Verschwendung von Zeit und Geld. Hinzu kommt, dass das Hantieren mit Papier zwangsläufig zusätzlichen Zeitaufwand seitens des mobilen Vertriebs- und Servicepersonals erfordert und daher die Möglichkeiten für eine effiziente Kundenkommunikation reduziert werden, was im Endeffekt die Up-Selling- und Cross-Selling-Möglichkeiten verringert.

Moderne, auf elektronischen Unterschriften basierende, digitale Dokumentenprozesse schaffen hier Abhilfe, da sie in der Lage sind, die letzte Lücke hin zu einem gänzlich papierlosen Arbeiten zu schließen, und dies selbst unterwegs bei Terminen mit Kunden. Dieses Whitepaper untersucht die spezifischen Anforderungen an eine Software für den elektronischen Abschluss von Verträgen in typischen Anwendungsfällen bei mobilen Vertriebs- und Serviceorganisationen, wie sie z.B. in Versicherungs- oder in Dienstleistungsorganisationen gefunden werden können.

Zunächst soll Ihnen dieses Whitepaper dabei helfen, das geeignetste Unterschriftserfassungsgerät, die IT-Architektur sowie das Dokumentenformat auszuwählen. Dann werden wir uns wichtige Sicherheitsaspekte genauer anschauen. Nach Diskussion der Wahlmöglichkeiten hinsichtlich der besten Architektur für eine schnelle und übergangslose Integration der Software in Ihre Umgebung schauen wir uns schließlich noch jene Aspekte an, die speziell für mobile Einsatzszenarien wichtig sind, wobei Sie auch sehen werden, dass ein elektronischer Vertragsabschluss viel mehr ist als nur das elektronische Unterschreiben von digitalen Dokumenten – es geht vor allem um Produktivitätssteigerung und Fehlervermeidung. Schließlich werden wir auch Geschäftsprozesse darstellen, die bestehende Kunden für das mobile Unterschreiben mit SIGNificant implementiert haben.

Inhaltsverzeichnis

1 Die richtige Unterschriftsmethode auswählen



Digitale Dokumente mit einer handgeschriebenen Unterschrift zu unterzeichnen, die forensisch identifizierbar ist, ist in einem mobilen Verkaufs- oder Dienstleistungsszenario eindeutig die bevorzugte Methode. Obwohl auch andere biometrische Technologien zur Verfügung stehen (wie z.B. Fingerabdruck, Iris-Scan, etc.), haben sich handgeschriebene Unterschriften, die wie beim Unterschreiben auf Papier von einem Graphologen authentifiziert werden können (nämlich basierend auf der Erfassung von Daten wie Geschwindigkeit, Beschleunigung, Druck, etc.) und die eindeutig mit einem bestimmten Dokument verknüpft sind, de facto als der Standard für das Unterschreiben digitaler Dokumente in einem mobilen Szenario etabliert. Der maßgebende Grund dafür ist wohl der Umstand, dass die Verbraucher "kulturell" verstehen, dass der Akt des Unterschreibens per Hand „bedeutsam“ ist. Wenn alle Schritte unter der Kontrolle des Unterzeichners stattfinden, intuitiv und - wie beim Papierprozess - klar ersichtlich sind, dann werden auch Gerichte diese Methode leichter und besser anerkennen, als andere „elektronische“ Methoden des Unterschreibens. Eine handschriftliche Unterschrift auf einem Dokument wird weltweit als Zeichen einer vertraglich verpflichtenden Vereinbarung akzeptiert. Das wird sich nicht so schnell ändern, speziell wenn eine persönliche Unterschrift verlangt ist.

Da der Unterzeichner während eines persönlichen Treffens auf einem Mobilgerät Ihres Vertriebs- oder Dienstleistungsmitarbeiters unterschreibt, haben Sie die technische Umgebung und daher die geeignete Erfassung handgeschriebener Unterschriften voll unter Kontrolle. Für diesen Anwendungsfall bietet das Installieren von nativen Anwendungen die beste Benutzererfahrung und ermöglicht es Ihnen, die biometrischen Daten auf geeignete Weise zu erfassen. [1] HTML5Anwendungen, die keine Vorausinstallation erfordern, sind ebenfalls eine Möglichkeit, aber vom Design her liefern diese nur ein Bild der Unterschrift ohne biometrische Daten; außerdem bedeuten sie eine 100%ige Abhängigkeit des Vertriebs/Service-Mitarbeiters von einer Online-Verbindung.

Auf dem Markt sind verschiedene biometrische Unterschriftstechnologien für den mobilen Vertriebs- und Dienstleistungssektor erhältlich. Sie können hauptsächlich in folgenden drei Bereichen unterschieden werden:

- Unterschriftserfassungsgeräte
- IT-Architektur
- Dokumentenformat

[1] Die Browser-Schicht einer HTML5-Anwendung erlaubt per Definition nicht die geeignete Aufzeichnung von zeit- und druckbasierten biometrischen Unterschriftsdaten. Drucksensitive Stifte werden ebenfalls nicht in HTML5 unterstützt.

1.1 Unterschriftenerfassungshardware

Portabilität ist die wesentliche Voraussetzung für Geräte zum Erfassen von Unterschriften in einem mobilen Szenario. Das Einfachste ist natürlich, wenn man dabei direkt auf dem Mobilgerät unterschreibt, wie dies bei Touchscreen-Geräten (z.B. Tablets oder Phablets) möglich ist.

Falls Sie mit einem traditionellen Notebook ohne Touchscreen unterschreiben möchten, können Sie ein externes Gerät – ein Signaturpad – oder auch ein Smartphone – z.B. ein Samsung Note mit Stift oder ein iPhone mit Stylus - für das Erfassen von Unterschriften benutzen.

Tablets/Phablets mit einem nativen digitalen Stift

Tablets sind perfekt für das mobile elektronische Unterschreiben geeignet, da sie einem das Benutzererlebnis vermitteln, die derjenigen auf Papier am nächsten kommt: man liest, bearbeitet und unterschreibt das Dokument direkt am Bildschirm. Idealerweise können Sie alles tun, was Sie auf Papier auch tun können – nur eben mit einem digitalen Stift. Falls das Tablet mit einem Stift ausgestattet ist, hat dieser optimalerweise folgende Eigenschaften:

- Er bietet Handauflageschutz (Sie können also den Bildschirm mit Ihrer Handfläche berühren, während Sie schreiben).
- Er besitzt eine natürliche Form mit einer eher dünnen Stiftspitze (wie z.B. ein Kugelschreiber), die es ermöglicht, auch dünne Linien zu zeichnen.
- Er hat eine nicht zu rutschige Oberfläche.

Ist dies gegeben, dann ist das Schreibgefühl sehr ähnlich dem auf Papier – was es auch Benutzern ohne weitere technische Erfahrung ermöglichen wird, auf geeignete Weise zu unterschreiben, wenn sie das zum ersten Mal tun.

Die Frage, wie wichtig es ist, dass der Stift in der Lage ist, auch Druckinformationen aufzuzeichnen oder nicht, wird kontrovers diskutiert. Es kann sein, dass Sie eine höhere Beweissicherheit vor Gericht erreichen, wenn mit einem drucksensitiven Stift unterschrieben wird – aber ein Graphologe braucht umgekehrt für ein Gutachten nicht unbedingt diese Druckwerte. [2]

Tablets/Phablets mit einem kapazitiven Stift

Falls das Tablet Ihrer Wahl über keinen nativen digitalen Stift verfügt (wie z.B. ein iPad), können Sie es dennoch sehr gut für elektronische Unterschriften benutzen. Obwohl das Unterschreiben mit dem Finger technisch funktioniert, ist es empfehlenswert, einen kapazitiven Stift (Stylus) zu verwenden, da er dem Benutzer ein besseres Schreibgefühl

[2] Siehe Experten-Meinung von Dr. Caspart.

bietet; niemand ist es wirklich gewöhnt, mit einem Finger zu unterschreiben. Natürlich kann das Schreibgefühl dabei nie so gut sein, wie mit einem nativen digitalen Stift – aber es ist trotzdem besser, als Sie vielleicht glauben; man schreibt typischerweise nur etwas breiter und langsamer.

Alternativ können Sie auch drucksensitive Stifte aus dem Zubehörhandel benutzen, die einen der entscheidenden Vorteile bieten, die weiter oben bereits erwähnt wurden, also:

- Handballenauflageschutz,
- dünne Stiftspitze,
- Aufzeichnen von Druck.

Unter diesen Vorteilen ist ein guter Handballenauflageschutz (Sie können Ihre Handfläche auf das Gerät aufsetzen, während Sie unterschreiben) das Feature, das dem Unterzeichner den größten Komfort bietet, da viele beim Unterschreiben dazu neigen, die Geräteoberfläche mit der Handfläche zu berühren, was sonst mit dem Erfassen der Unterschrift kollidiert.

Laptop Computer mit einem Signaturpad

Falls Sie einen Laptop Computer ohne Touchscreen für das Darstellen und Bearbeiten von Dokumenten benutzen, dann können Sie ein peripheres Gerät zur Aufzeichnung von Unterschriften samt den dazugehörigen biometrischen Daten benutzen. Spezialgeräte (sogenannte Signaturpads) von Anbietern wie z.B. Wacom sind am besten geeignet, um ein gutes schreibegefühl und die notwendige Portabilität anzubieten. Um das Abgreifen der erfassten biometrischen Daten vom Signaturpad zu verhindern, gibt es Sicherheitsmechanismen, die von der Chiffrierung der Kommunikation zwischen dem Signaturpad und dem Computer bis zu einer End-To-End-Verschlüsselung der Unterschriftsdaten auf dem Pad selbst reichen.

Laptop-Computer mit einem verbundenen Smartphone

Falls ein Signaturpad keine Option ist oder sonst nicht erwünscht ist, z.B. weil Sie mit einem unabhängigen Vertriebskanal arbeiten und diesem die Anschaffung einen Signaturpads nicht zumuten möchten, dann können Sie stattdessen auch ein Smartphone als Signaturerfassungsgerät verwenden. Für eine reine mobile Lösung muss die Verbindung zwischen dem Laptop und dem Smartphone auch ohne Internetverbindung funktionieren (z.B. via Bluetooth oder WLAN). Wenn ein Dokument zu unterschreiben ist, dann wird die Verbindung zwischen einer nativen App am Smartphone und der Software am Hostcomputer hergestellt und die App macht zudem aus dem Smartphone ein Gerät zum Erfassen einer Unterschrift.

1.2 Bereitstellungsmodel (Deployment)

Sie können entweder eine vollständig lokale Unterschriftssoftware verwenden oder Sie können einen Client/Server-Lösungsansatz wählen (siehe Kapitel 3.2 Verwendung einer

Server-basierten Lösung – Vor- und Nachteile). Unabhängig davon, für welche Option Sie sich entscheiden, ist Offline-Support in beiden Varianten möglich (siehe Kapitel **Error! Reference source not found.**).

Falls Sie eine Client/Server-Architektur vorziehen müssen Sie entscheiden, wo die Serverinfrastruktur laufen soll. Es ist möglich, sie in einer öffentlichen oder in einer privaten Cloud laufen zu lassen und über ein SaaS-Modell zu benutzen, oder sie mit ihrer eigenen Infrastruktur bereitzustellen und zu betreiben. Während das Cloud-Modell schneller und leichter einzurichten ist, bietet es typischerweise allerdings nur sehr begrenzte Optionen, um zu definieren, wo sich Ihre Server und Daten befinden sollen, und Sie machen sich außerdem 100% abhängig vom jeweiligen Anbieter, was die Verfügbarkeit und die Sicherheit betrifft. Deshalb gibt es gute Gründe – Datenschutz und Fragen der länderspezifischen Datenspeicherung sind nur zwei der offensichtlichen Beispiele – die Server in der eigenen Infrastruktur zu betreiben, die dann von einer Firewall geschützt werden, was zu einer maximalen Kontrolle über die Daten und Systeme führt. Beachten Sie auch, dass es viel leichter ist, mit einem Cloud-Service zu starten als wieder daraus auszusteigen. Stellen Sie daher sicher, dass Sie jederzeit entscheiden können, die Anwendungen falls nötig wieder in Ihr Rechenzentrum zu verlagern und prüfen Sie, was Sie vor Gericht noch in der Hand haben würden, wenn Ihr Anbieter einmal nicht mehr existieren sollte oder Sie keine gut funktionierende Geschäftsbeziehung mehr mit ihm haben sollten.

1.3 Dokumentenformat

Nach Gartner-Research (Veröffentlichungs-ID-Nummer: G00159721) ist das beste **Dokumentenformat** “eigenständig” (=von Drittsystemen unabhängig), so dass es den zu unterschreibenden Inhalt, die Unterschriften und die zugehörigen Metadaten, sowie die Beweisinformationen zur jeweiligen Unterschrift (wie Datum, Zeit, und Ort) vollständig enthält. Es sollte weiters auch nur eine kostenlose und leicht zugängliche Lesemöglichkeit (Viewer) erfordern, um das Dokument in seiner **ursprünglichen** Form anzuzeigen.

Im Gegensatz zu den proprietären Dokumentenformaten und Dokumentendatenbanken erfüllt das offene Portable Dokument Format (PDF) all diese Anforderungen. PDF ist nicht nur ein offener Standard, der in ISO 32000-1:2008 definiert ist, sondern existiert auch in einer Variante die für eine langfristige Archivierung vorgesehen ist, definiert als PDF/A in ISO 19005-1:2005. Hinzu kommt, dass digitale Signaturen innerhalb von PDF selbst gut definiert sind (Adobe PDF Reference PDF 320001:2008 12.8.3.3 PKCS#7 Signatures — wie in ISO 32000 benutzt), was bedeutet, dass jeder Viewer, der sich an den Standard hält (wie Adobe Acrobat Reader), digital signierte PDFs korrekt anzeigt. Daher ist eine PDF- oder PFD/A-Datei in der digitalen Welt das perfekte Gegenstück zu Papier, um unterschriebene Dokumentoriginale zu archivieren. Alle Signaturen und deren kryptographische Information sollten in das signierte PDF eingebettet sein. Es sollte nicht so sein, dass sie Kunde von einem bestimmten E-Signatur-Anbieter sein müssen oder auf dessen Website gehen müssen, nur um die Gültigkeit von Dokumenten prüfen zu können.

2 Sicherheitsaspekte

Elektronisch signierte Dokumente sind künftig ihre rechtlich bindenden Originale. Deren Sicherheit und Integrität muss unbedingt gewährleistet sein, andernfalls wären diese wertlos. Deshalb sind Sicherheitsaspekte ein wesentliches Thema. Die wichtigsten Aspekte hierfür werden in diesem Kapitel aufgezeigt. Für detailliertere Informationen fragen Sie bitte nach dem SIGNificant Sicherheitswhitepaper.

2.1 Authentizitätsschutz

Der Schutz der Authentizität einer Unterschrift und ihre Verbindung mit einem bestimmten Dokument und zusätzlich mit einer bestimmten Stelle innerhalb des Dokuments sind von zentraler Bedeutung. Es muss für einen Fälscher unmöglich sein, auf die Unterschriftendaten auch nur eines einzigen Dokuments zugreifen, sie kopieren und woanders einfügen zu können (sei es im selben Dokument oder in einem anderen Dokument). Deshalb ist die Verbindung der Unterschrift zum Dokument zusammen mit einer sicheren Verschlüsselung der aufgezeichneten Unterschriftendaten mittels Dokumentenfingerprint (Hashvalue) ganz wesentlich.

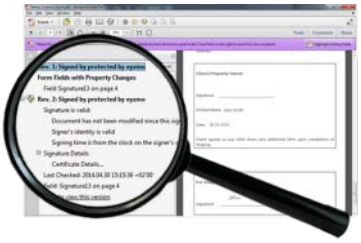
Die Verwendung von asymmetrischen Verschlüsselungsverfahren mittels hybridem RSA/AES- Verschlüsselungsalgorithmus wird als sicher eingestuft und hat sich de-facto zum Branchenstandard entwickelt. Heutzutage können nahezu alle wichtigen Unterschriftenerfassungsgeräte diese asymmetrischen Verschlüsselungsvorgänge direkt auf den Geräten selbst ausführen und so effizient die biometrischen Unterschriftendaten vor unerlaubten Zugriff schützen.

Selbstredend sollte auch die Prüfung der Unterschriftenbindung zu den Dokumenten nicht von der Verfügbarkeit des Unterschriftenerfassungsgeräts, auf dem die Unterschrift erfasst wurde, abhängig sein. Unterschriebene Dokumente haben eine weitaus längere Lebensdauer als die Erfassungsgeräte.

2.2 Integritätsschutz

Sobald ein Dokument unterschrieben ist, ist es essentiell, dass es für jedermann leicht überprüfbar ist, ob das unterschriebene Dokument noch das Original ist oder ob es geändert wurde, nachdem es unterschrieben wurde. Diese Art von Integritätsanalyse muss für jeden, der das unterschriebene Dokument anschaut bzw. liest, mit gewöhnlichen PDF-Readern durchführbar sein. Eine Abhängigkeit von einem Webservice eines Anbieters wäre hier nicht nur sehr umständlich, sondern würde auch eine unabhängige Langzeitarchivierung unmöglich machen. Weiters sollte es möglich sein, diese Integritätsprüfung vollständig zu automatisieren, ehe das PDF-Dokument weiter verarbeitet oder in einem Archiv abgelegt wird.

2.3 Protokolle (Audit-Trail)



Protokolle sollen aufzeichnen, was mit einem bestimmten Dokument, in welcher Reihenfolge, zu welcher Zeit und wo passiert ist. Ein in sich abgeschlossenes Dokument mit allen Unterschriften und digitalen Zertifikaten, inklusive seiner Protokollaufzeichnungen, kann sich auf jedem Speichermedium befinden und muss deshalb nicht auf einem proprietären Speichersystem archiviert werden.

2.4 Begrenzung des Zugriffs auf Dokumente

Im Gegensatz zu Papier können digitale Dokumente leicht kopiert werden, ohne irgendeine ihrer Eigenschaften zu verlieren. Neben vielen positiven Aspekten ergibt sich bei elektronisch unterschriebenen Dokumenten auch ein Nachteil für etwaige zuküftige Streitfälle. Angenommen, der technologische Fortschritt macht es irgensdwann möglich, diese elektronisch unterzeichneten Originaldokumente zu fälschen. Wenn Sie sicher sein wollen, dass es nur ein Original gibt, welches Sie zentral verwalten, müssen Sie den Zugriff auf die signierten Originaldokumente strikt begrenzen. Dazu müssen Sie sicherstellen, dass die elektronische Unterschriftenlösung nicht einfach die originale PDF-Datei auf allen dezentralisierten Unterschriftsstationen verteilt, was die Komplexität des Zugriffschutzes auf das Originaldokument massiv erhöhen würde.

3 IT-Architektur für eine schnelle und nahtlose Integration

Eine E-Signatur-Anwendung besteht typischerweise aus einer Frontend- und einer Backend-Komponente. Während die Frontend-Software sämtliche Benutzer-Interaktionen behandelt, verarbeitet die Backend-Software das Dokument und kümmert sich um seine Integration in den allgemeinen Dokumenten-Workflow.

Die Frontend-Software-Komponente läuft auf einem Front-Office-Computergerät, das eines der folgenden Geräte sein kann:

- Ein traditioneller Laptop (Notebook), der einen externen Signatur-Bildschirm oder ein Signaturpad verwendet, um eine handgeschriebene Signatur zu erfassen.
- Ein Tablet-Computer.

Typischerweise ist der Frontend-Teil entweder eine unabhängige vorkonfigurierte GUI-Anwendung oder ein SDK, das nahtlos in eine existierende Client-Anwendung integriert werden kann.

Die Backend-Softwarekomponente kann entweder zusammen mit einer Frontend-Komponente innerhalb derselben Anwendung/auf demselben Computer lokal laufen oder sie kann in eine getrennte Server-Anwendung aufgespalten sein, was bedeutet, dass die E-Signatur-Anwendung über einen Client und einen Server verteilt ist.

In den folgenden Abschnitten werden wir uns die Vor und Nachteile jeder Option anschauen.

3.1 Eigenständige GUI-Anwendung oder SDK

Falls Sie eine schnelle und kosteneffiziente Bereitstellung mit sofort einsetzbaren Benutzerschnittstellen benötigen, dann ist eine eigenständige GUI-Anwendung typischerweise die beste und auch kosteneffizienteste Lösung. Gut gemacht erlaubt diese Option immer noch die Personalisierung von Farbschemen, Logos, etc. gemäß Ihren Anforderungen.

Falls Sie jedoch eine nahtlose Integration in eine existierende Anwendung benötigen (ohne UI-Kontextwechsel), dann ist die SDK-Lösung die passende. Hier können Sie sämtliche Details, wie der Benutzer mit der Software interagiert, und alle GUI-Elemente durch Programmierung verwalten. Leistungsfähige SDKs bieten viel mehr als nur die einfache Integration der Grundfunktionalitäten und bieten darüber hinaus komplett adaptierbare Benutzeroberflächenkomponenten, um sie nahtlos zu integrieren.

Sie sollten jedoch den Aufwand nicht unterschätzen, der erforderlich ist, um aus einem SDK eine funktionsfähige Lösung zu machen. Es kann zu viel höheren Kosten führen, wenn Sie Ihre eigene Lösung programmieren im Vergleich zum Personalisieren einer Standardlösung. Mit einer vorkonfigurierten Lösung zu starten kann wesentlich schneller sein, da der Personalisierungsprozess typischerweise innerhalb von ein paar Tagen gemacht ist. Außerdem gibt es zusätzliche Kosten wie Wartungskosten und zukünftige Entwicklungen, die ebenfalls berücksichtigt werden sollten.

Ein anderer wichtiger Aspekt beim Integrieren von elektronischen Signatur-Lösungen ist, dass es bei der Benutzung eines SDK's nötig sein wird, dass Ihre IT-Abteilung alle Sicherheitsgesichtspunkte eigenständig lösen muss. Sie muss z.B. handgeschriebene Unterschriften von Kunden davor schützen, in ein nicht erlaubtes Dokument übertragen zu werden oder irgendwo im Rohformat gespeichert zu werden, was eine enorme Sicherheitsbelastung und ein Risiko für die IT-Abteilung darstellt. Dazu gehören auch Bemühungen, den Missbrauch und nachlässiges Programmieren seitens der eigenen Mitarbeiter des Unternehmens zu verhindern, was die Aufgabe, ein ausreichendes Sicherheitsniveau zu gewährleisten, erschwert. Es ist eine Tatsache, dass - selbst wenn alle Sicherheitsmaßnahmen implementiert werden - den Endkunden und Drittparteien diese Ängste in der Regel nicht leicht genommen werden können, da das Unternehmen ja theoretisch die Möglichkeit hat, diese sensiblen Daten zu missbrauchen. Im Gegensatz dazu kann man bei einem Szenario mit einer einsatzfertigen Lösung den Endkunden und falls nötig einem Gericht im Fall eines Rechtstreits leicht beweisen, dass man keine Möglichkeit hatte, die Unterschriften irgendwie zu manipulieren.

Im Endeffekt müssen Sie selbst entscheiden, was die beste Lösung für Ihre Zwecke ist. Beachten Sie aber, dass, im Gegensatz zu dem, was man oft auf den ersten Blick erwarten könnte, eine einsatzfertige Lösung kostengünstiger und leichter zu installieren ist, als ein SDK-basierter Ansatz.

3.2 Verwendung einer Server-basierten Lösung – Vor- und Nachteile

Selbst wenn Sie sich für ein lokales Bereitstellungsmodell entscheiden und nicht für ein Cloud-Service, so hat in vielen Szenarien ein zentraler, server-basierter Ansatz für die Backend-Software-Komponente, die in Ihrem eigenen Rechenzentrum läuft, viele Vorteile gegenüber einem nur desktop-basierten Ansatz:

- Wenn bereits vorhandene Systeme zur Dokumentenerstellung, Arbeitsablaufverwaltung und Dokumentenarchivierung auch serverbasiert sind, ist die serverseitige Integration um vieles einfacher.
- Das PDF-Dokument ist nur im sicheren Rechenzentrum gespeichert und wird nicht automatisch an die Clients verteilt. Damit kann der Zugang zu den signierten Originalen sicher verwaltet werden.
- Ein serverseitiges Protokoll, dass zusätzliche Prozessnachweise bietet.
- Ein Server bietet eine einzige Integration für verschiedenste Clientoptionen:
    - Signaturpads — von einer Webapplikation oder einem lokalen SDK verwaltet. In einer individuellen Clientapplikation integriert.
    - Stiftbildschirme — von einem lokalen Kiosk -DK gesteuert, das ganz einfach in Ihre eigene Webapplikation integriert werden kann.
    - Smartphones — auf denen eine App zur Unterschriftenerfassung läuft, die sich mit einer Webapplikation verbindet, um das Dokument anzuzeigen.
    - Tablets — auf denen native Unterschriftenclients laufen, um Dokumente anzuzeigen, zu bearbeiten und zu unterschreiben.
- Kompatibel mit anderen Vertriebskanälen — Wiederverwendung der elektronischen Unterschrifteninfrastruktur und Softwareintegrationen, die für den POS implementiert wurden, für eine Multi-Channel-Umgebung, die auch Mobile- und Online-Channels beinhaltet.

Im Gegensatz dazu, werden reine desktop-/lokalbasierte Unterschriftenlösungen vorgezogen, wenn:

- Das zu signierende Dokument am Client dynamisch (und nicht basierend auf einer lokalen statischen Vorlage) erzeugt wurde, was den Einsatz einer Client/Server Lösung im Offline-Betrieb unmöglich macht.
- Eine Serverseitige Integration nicht nötig ist.

4 Aspekte, die für mobile Geschäftsprozesse wichtig sind

Der typische Geschäftsprozess für das Unterschreiben unterwegs unterscheidet sich von anderen Anwendungsfällen wie z.B. dem stationären Verkaufspunkt. Deshalb hat man es oft mit Anforderungen zu tun, die nur bei deisem Anwendungsfall auftreten. Die wichtigsten sind nachfolgend aufgeführt.

4.1 Arbeiten mit Offline-Dokumenten – ohne Internet-Verbindung

In einem mobilen Szenario ist es entscheidend, dass Sie Ihre Geschäftstransaktionen auch in Situationen abschließen können, wenn keine Internetverbindung vorhanden ist. Das bedeutet, dass Sie in der Lage sein müssen, die Dokumente zu lesen, zu bearbeiten, auszufüllen und zu unterschreiben, selbst wenn Sie offline sind – also z.B. wenn Sie einen Kunden zu Hause treffen. Idealerweise sollten Sie in der Lage sein, neue Dokumente von bestehenden Vorlagen aus zu erstellen, Formularfelder optional mit Daten von Drittanwendungen auszufüllen und Dokumente lokal ohne Netzwerkverbindung zu verwalten. Das bedeutet, dass Client-/Server-Anwendungen die benötigten Daten lokal zwischenspeichern müssen, um solche Offline-Anwendungsfälle zu unterstützen. Natürlich werden Sie, falls das PDF-Dokument selbst auf dem lokalen Gerät erzeugt wird (wie z.B. durch eine Drittanwendung), eine Standalone-Unterschriftenlösung benötigen, um die komplette Offline-Verarbeitung zu erlauben (andernfalls benötigen Sie eine Online-Verbindung, um das Dokument auf den Server hochzuladen, bevor Sie offline weiterarbeiten können).

4.2 PDF-Formulare bearbeiten und ausfüllen wie auf Papier

Idealerweise wollen Unterzeichner mit digitalen Dokumenten so arbeiten, wie sie es mit Papierdokumenten gewohnt sind. Das bedeutet, dass die Unterschriftslösung es den Unterzeichnern erlauben muss, dass sie mehrseitige Dokumente durchgehen und überprüfen können, bevor Sie diese bearbeiten und unterschreiben – idealerweise direkt auf dem Gerät mit dem später unterschrieben wird.

Die Möglichkeiten gehen jedoch über diese Grundfeatures hinaus, da speziell Tablets auch das Bearbeiten von Dokumenten erlauben, wie Sie es aus der Papierwelt gewohnt sind. Dazu gehören das Hinzufügen von freihändigen und Text-Anmerkungen, Markups, Anhängen und das Ausfüllen von maschinenlesbaren Formularfeldern. Außerdem ist die Integration der Unterschriftslösungen in den Dokumenten-Workflow wesentlich. Diese soll es ermöglichen, dass Sie ein vorausgefülltes Formulardokument (wie z.B. einen Kundenvertrag) z.B. aktiv auf ein Tablet eines bestimmten Außendienstmitarbeiters schicken wollen, dem Kunden dort das Lesen des Dokuments und das Erfassen bzw. Ändern der Formularfeldwerte erlauben wollen und dann die vom Kunden vorgenommenen Änderungen am Dokument inklusive der Unterschriften wieder zurück vom Tablet in Ihre eigenen Anwendungen synchronisieren wollen, sobald eine Online-Verbindung zum Tablet besteht.

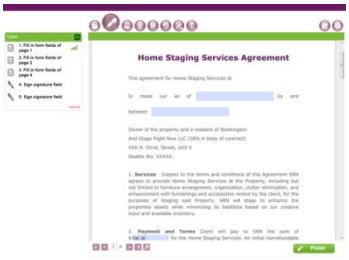
4.3 Fotos hinzufügen, die mit der Kamera des Gerät aufgenommen wurden

Mobile Geräte wie Tablets oder Smartphones sind mit eingebauten Kameras ausgerüstet, die perfekt geeignet sind, um den Dokumenten Fotos hinzuzufügen, wie z.B. Ausweiskopien oder Beweisbilder von einem Schaden. Das hinzugefügte Foto muss eindeutig mit dem Dokument verbunden sein, das unterschrieben werden soll, und es darf nicht bearbeitet werden können, ohne das digitale Siegel der Signatur zu beschädigen. Idealerweise kann das Foto dem Dokument in jeder Größe und an jeder Position hinzugefügt werden, entweder durch eine Ad-hoc-Festlegung oder über eine vordefinierte Vorlage. Alternativ sollte es möglich sein, es wie jede andere Datei einfach dem PDF-Dokument anzuhängen.

4.4 Der Unterschrift Standortdaten (GPS) hinzufügen

Manchmal ist es wichtig zu wissen, an welchem Standort bestimmte Dokumente unterschrieben werden, oder man fügt die Ortsinformation als zusätzliches Beweismittel hinzu. Mobilgeräte wie Tablets oder Smartphones besitzen einen eingebauten GPS-Sensor, der benutzt werden kann, um digitale GPS-Koordinaten in die digitale Signatur hinzuzufügen.

4.5 Vermeiden von unvollständigen Dokumenten



Zu versuchen, fehlerhafte Dokumente im Nachhinein zu korrigieren, ist meist sehr zeitraubend und teuer; wenn Sie das Problem einmal entdecken, befinden sich die Außendienstmitarbeiter typischerweise nicht mehr beim Kunden. Daher ist es von großem Nutzen, wenn die Unterschriftssoftware alle notwendigen Schritte anzeigt und das Erledigen der Mussanforderungen (wie z.B. das Ausfüllen von Formularfelder oder Unterschriftsfelder oder das Anhängen des Fotos eines Ausweises und vieles mehr) gleich überprüft. Idealerweise können Sie, abhängig vom Anwendungsfall und vom Dokument, spezielle obligatorische oder optionale Schritte angeben, was Ihnen die Flexibilität verleiht, alle Ihre Geschäftsfälle abzudecken.

Zusätzlich können Sie dem Anwender durch das Definieren von Richtlinien bestimmte Aktionen am oder mit dem Dokument erlauben oder verbieten – wie z.B. Anmerkungen zu schreiben, Dokumente lokal am Gerät zu speichern, Dokumente via Email zu versenden oder Dokumente zu drucken

4.6 Integration in eine Unterschriftenplattform

Es ist sehr nützlich, wenn die mobile Unterschriftslösung Bestandteil einer allgemeinen Unterschriftsplattform, die auch andere Geschäftsprozesse wie In-House-POS oder reine RemoteOnline-Szenarien abdeckt, ist. Nur dann können Sie sicherstellen, dass Sie ein Gesamtsystem erhalten und keine reine Insellösung bauen.

5 SIGNificant-Referenzen

SIGNificant bietet eine Unterschriftenplattform, die es Ihnen ermöglicht, in einem mobilen Verkaufs oder Service-Szenario ganz ohne Papier auszukommen. SIGNificant stellt Ihnen die Benutzerschnittstellen und die Werkzeuge, die nötig sind, um den optimalen Unterschriftenprozess und die optimale Benutzerschnittstelle zu definieren, auf ganz einfache Weise zur Verfügung. Die Bausteine der Plattform machen es Ihnen leicht, die beste Kombination von Unterschriftenerfassungssoftware und Unterschriftenerfassungshardware auszuwählen und auch später auszuwechseln, so wie Sie es benötigen.

Um besser zu illustrieren, wie SIGNificant in unterschiedlichen mobilen Szenarien angewendet werden kann, behandeln die nachfolgenden Abschnitte reale Fallstudien mit einem End-to-end Geschäftsprozess, der implementiert wurde.

5.1 Swiss Life Select

Anwendungsfall:

- Anwendungen für Finanzinvestitionen und Versicherungsverträge, die direkt durch die Vertriebsmitarbeiter vertrieben werden.

Eingesetzte Produkte:

- Unterschriftenlösung: SIGNificant-Server mit iPad-App, Android-App und Web-Signatur-Interface.
- Unterschriftenerfassungshardware: iPads, Android, Surface-Pro-Tablets und Wacom-Signaturpads.

End-to-end Geschäftsprozess:

1. Der Finanzberater lädt die Verträge, die er unterschreiben lassen will, über das Swiss Life Select Vertriebsportal auf sein Tablet.
2. Der Berater besucht den Kunden, bei dem keine 3G/Internet-Verbindung zur Verfügung stehen muss.
3. Der Kunde liest den Finanzdienstleisungsvertrag und füllt die erforderlichen Formularfelder in einer maschinenlesbaren Form (Text, Checkboxen) direkt auf dem Tablet oder Notebook aus.
4. Der Kunde unterschreibt schließlich den ausgefüllten Verischerungs- oder Investment-Vertrag direkt auf dem Tablet oder einem Signaturpad, das mit einem Notebook verbunden ist.
5. Sobald wieder eine Internetverbindung vorhanden ist, synchronisiert sich die App mit dem SIGNificant Server, der das Dokument verarbeitet und es mit einem Swiss Life Select Zertifikat versiegelt.
6. Swiss Life Select archiviert die biometrisch signierten, originalen PDF-Dokumente.
7. Der Kunde kann entweder auf eine vereinfachte (flache) oder digital signierte Kopie des Originaldokuments zugreifen oder sie per Email zugesandt bekommen.

5.2 Nürnberger Versicherung

Anwendungsfall:

- Lebensversicherungen und andere Versicherungsverträge, die über ihren unabhängigen Vertriebskanal verkauft werden.

Eingesetzte Produkte:

- Unterschriftenlösung: SIGNificant-Server mit iPad-App, Android-App und Web-Signier-Interface.
- Unterschriftenerfassungshardware: iPads, Android-Tablets und StepOver-Signaturpads.

End-to-end Geschäftsprozess:

1. Der Markler legt durch die Eingabe der relevanten Kundendaten auf dem Nürnberger Vertriebskanalportal ein oder mehrere Versicherungsantragsdokumente an, die elektronisch unterschrieben werden sollen.
2. Der Markler lädt die gewünschten Versicherungsanträge/-verträge auf sein Tablet.
3. Der Berater besucht den Kunden, bei dem keine 3G/Internet-Verbindung zur Verfügung stehen muss.
4. Der Kunde unterschreibt schließlich den ausgefüllten Versicherungsvertrag.
5. Sobald wieder eine Internetverbindung vorhanden ist, synchronisiert sich die App mit dem SIGNificant Server, der das Dokument verarbeitet und es mit einem Nürnberger Zertifikat versiegelt.
6. Die Nürnberger archiviert die biometrisch signierten, originalen PDF-Dokumente.
7. Der Kunde kann entweder auf eine vereinfachte (flache) oder digital signierte Kopie des Originaldokuments zugreifen oder sie per Email zugesandt bekommen.

5.3 Niederösterreichische Versicherung

Anwendungsfall:

- Lebensversicherungen und andere Versicherungsverträge, die über Direktvertrieb verkauft werden.

Eingesetzte Produkte:

- Unterschriftenlösung: SIGNificant-Client, der auf Windows-Laptop-Computer läuft.
- Unterschriftenerfassungshardware: Wacom STU-500 Signaturpads.

End-to-end Geschäftsprozess:

1. Der Vertriebsmitarbeiter lädt die benötigten Versicherungsanträge/-verträge auf seinen Laptop-Computer.
2. Der Berater besucht den Kunden, bei dem keine 3G/Internetverbindung zur Verfügung stehen muss.

3. Der Kunde liest den Versicherungsvertrag und füllt die erforderlichen Formularfelder in einer maschinenlesbaren Form (Text, Checkboxen) direkt auf dem Laptop aus.
4. Der Kunde unterschreibt schließlich den ausgefüllten Versicherungsvertrag auf dem Wacom STU-500-Signaturpad.
5. Der SIGNificant Client startet ein Post-Processing-Programm, das den unterschriebenen Versicherungsvertrag sicher archiviert.
6. Der Kunde kann entweder auf eine vereinfachte (flache) oder digital signierte Kopie des Originaldokuments zugreifen oder sie per Email zugesandt bekommen.