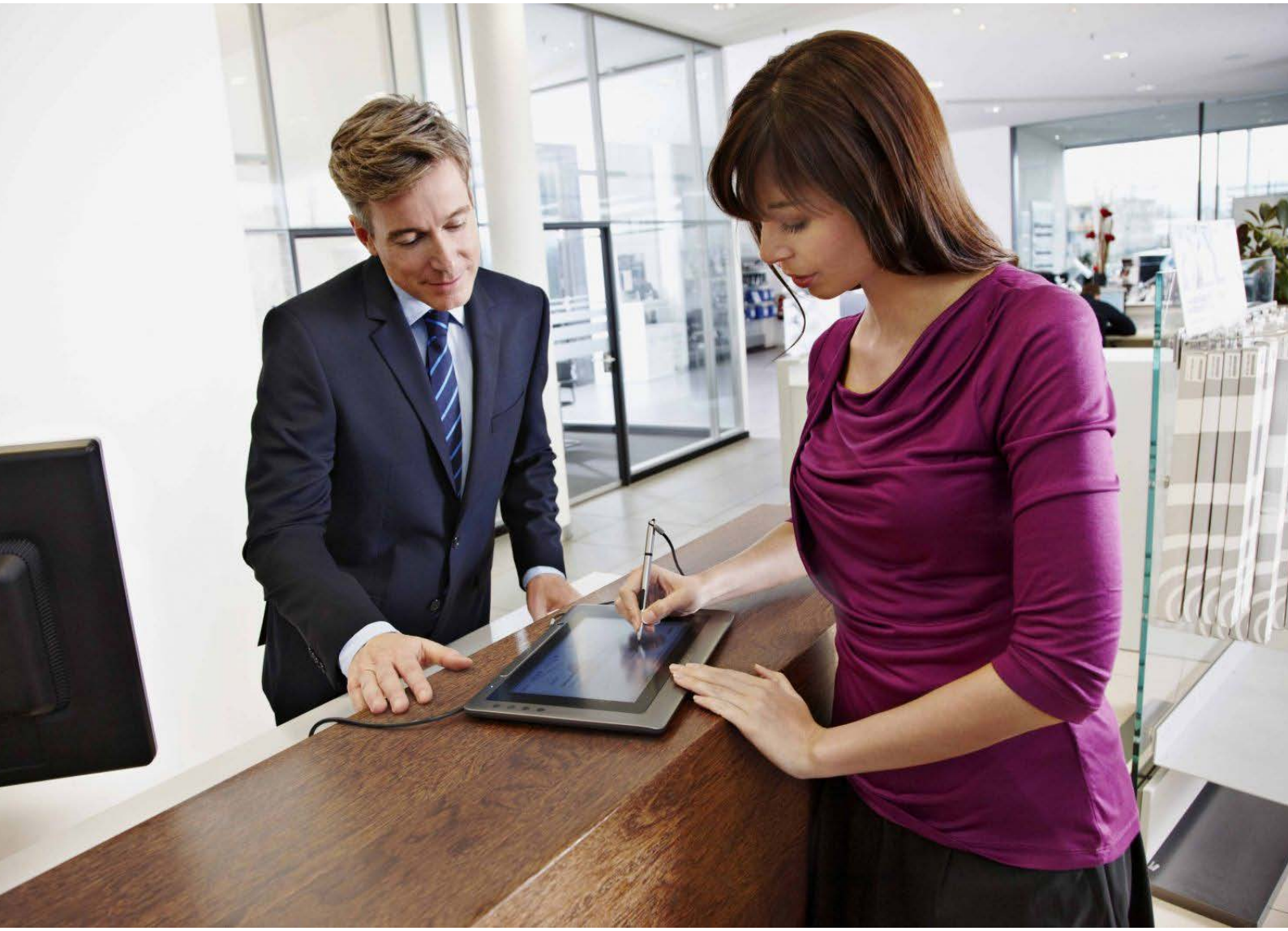
Elektronisches Unterschreiben am Point-of-Sale

Papierlose Vertragsabschlüsse mit Endkunden direkt oder über Partner



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 muss man auf die Interessen und Wünsche der Kunden achten. Dokumente nur deshalb auszudrucken, um die Unterschrift eines Kunden einzuholen, ist heute mit allgegenwärtigen Smartphones und Tablets nicht nur völlig überholt, sondern auch eine enorme Verschwendung von Zeit und Geld. Das Hantieren mit Papier bindet zwangsläufig Personalressourcen, was die Möglichkeiten für eine effiziente Kundenkommunikation reduziert. Dies verringert letztendlich die Up-Selling- und Cross-Selling-Chancen.

Moderne, auf elektronischen Unterschriften basierende, digitale Dokumentenprozesse schaffen hier Abhilfe, da sie in der Lage sind, die Lücke zu einem gänzlich papierlosen Arbeiten am Point-Of-Sale (POS) zu schließen. Dieses Whitepaper untersucht die spezifischen Anforderungen an eine Software für den elektronischen Vertragsabschluss in typischen Anwendungsfällen mit Endkunden (B2C). Dabei werden sowohl die Anforderungen von Szenarien mit direktem Vertriebsweg, wie zum Beispiel in der Bankfiliale, im Einzelhandel und im Kundencenter, als auch solche mit indirektem Vertriebsweg, wie bei Agenturen oder Händlern, berücksichtigt.

Zunächst soll Ihnen dieses Whitepaper dabei helfen, die beste elektronische Unterschriftenlösung zu finden, um Ihre Dokumente am Point-Of-Sale digital zu bearbeiten. Nachdem wir aufgezeigt haben, warum Sie über eine rein elektronische Unterschriftenerfassung hinausblicken müssen, um optimale Produktivitätssteigerungen zu lukrieren, werden die wichtigsten Sicherheitsaspekte hervorgehoben. Nach einer Einführung in die Vor- und Nachteile der verschiedenen Möglichkeiten von Hardware zur Unterschriftenerfassung, wird gezeigt, wie die Authentizität der unterschriebenen Dokumente gewährleistet wird und wie im Streitfall die Gültigkeit der Dokumente bewiesen werden kann. Daraufhin wird auf die wichtigsten Themen zur Integration und Bereitstellung der elektronischen Unterschriftenlösung in Ihre IT- und Applikationsumgebung eingegangen. Schließlich stellen wir Ihnen unsere SIGNificant Unterschriften-Plattform vor und führen einige Fallbeispiele an, die die Implementation von SIGNificant in POS-Szenarie quer durch die Industrie zeigen.

Inhaltsverzeichnis

1 Die richtige Unterschriftenmethode auswählen

Heutzutage sind mehrere verschiedene elektronische Unterschriftenlösungen für direkte und indirekte Point-Of-Sale (POS) Prozesse am Markt verfügbar. Während bei allen Lösungen das elektronische Unterschreiben der Dokumente möglich ist, können deren Funktionen in folgende drei Schlüsselbereiche unterschieden werden:

- Elektronische Unterschriftentechnologie
- Dokumentenformat
- Software-Architektur

Als ersten Schritt wollen wir die verschiedenen verfügbaren Möglichkeiten für die oben genannten Bereiche beleuchten.

1.1 Elektronische Unterschriftentechnologien

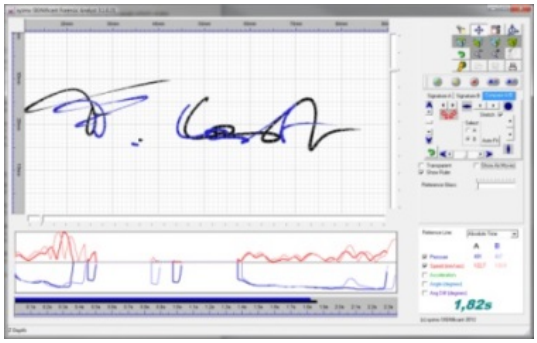
Die bekanntesten elektronischen Unterschriftentechnologien in B2C Prozessen am POS sind:

- **Forensisch identifizierbare Unterschriften** (aka Biometrische Unterschriften), bei welchen die einzigartigen Merkmale einer von Hand aufgezeichneten Unterschrift erfasst werden (zum Beispiel Geschwindigkeit, Beschleunigung, Druck), sodass ein Graphologe eine Unterschriftenüberprüfung vornehmen kann. Der Unterschriftenprozess und die Unterschriftenprüfung laufen weitestgehend gleich ab wie bei Unterschriften auf Papier.
- **HTML5-Unterschriften**, bei denen der Unterzeichner ebenfalls mit seiner handschriftlichen Unterschrift wie auf Papier unterzeichnet. Jedoch kann aufgrund von Restriktionen der HTML5-Technologie die elektronische Unterschriftensoftware keine verlässlichen forensischen Daten aufnehmen, was folglich die Nachweisbarkeit der aufgenommenen Unterschrift mindert. Dadurch wird eine zusätzliche Benutzerauthentifizierung (zum Beispiel Einmal-Passwort, SMS-TAN, ID Prüfung, etc.), die zusammen mit der Unterschrift in einem Protokoll archiviert wird, nötig. In diesem Punkt unterscheidet sich der Unterschriftenprozess und die Unterschriftenprüfung vom Prozess auf Papier.
- **Zertifikatsbasierte Unterschriften** mittels einer Public Key-Infrastruktur (PKI), welche persönliche, digitale Signaturzertifikate für sämtliche Unterzeichner bereitstellt (zum Beispiel Smart-Cards oder Software-Zertifikate). Hierbei ist der Unterschriftenprozess im Vergleich zu handgeschriebenen Unterschriften (auf Papier) von Grund auf verschieden. Dieser Prozess ist eher mit Passauthentifizierung an einer Grenz- oder Eingangskontrolle zu vergleichen.

In einem B2C-POS-Szenario funktionieren PKI-basierte Ansätze schlecht. Ein Grund dafür ist die eher schwache Verbreitung von sogenannten “nationalen ID-Karten mit Signaturfunktion”. Dies liegt sehr wahrscheinlich an den Kosten und der eher umständlichen Nutzung. Gerade für Personen, die an den Umgang mit neuen

Technologien nicht gewöhnt sind, ist dies eher ungeeignet. Infolgedessen muss man berücksichtigen, dass potentielle Kunden entweder kein eigenes persönliches Unterschriftenzertifikat besitzen oder dieses nicht verwenden können / wollen (zum Beispiel weil sie den Zugangs PIN vergessen haben oder die Smart-Card selbst nicht dabei haben).

Im Gegensatz dazu, sind HTML5-Unterschriften bestens für B2C-Prozesse geeignet, in denen der Kunde virtuell, ohne eine Verkaufspersonal zu treffen, unterschreiben soll. HTML5-Unterschriften benötigen keine Vorab-Installation am Client. Das bedeutet, dass der Kunde ganz einfach auf seinem eigenen Gerät (zum Beispiel Smartphone oder PC) unterschreiben kann. In diesem Fall ist der zusätzliche Schritt einer Authentifizierung zusätzlich zum reinen Unterschriftenakt für den Kunden typischerweise akzeptabel.



Die Erfassung einer forensisch identifizierbaren, eigenhändigen Unterschrift ist die beste Möglichkeit, ein Dokument persönlich und in einem Treffen vom Kunden unterschreiben zu lassen. Auch wenn andere biometrische Technologien am Markt verfügbar sind, hat sich die biometrische Unterschrift schlussendlich als Standard für elektronische Unterschriften im B2C-Bereich durchgesetzt. Das liegt wahrscheinlich daran, dass eigenhändige Unterschriften von der breiten Masse sozial akzeptiert sind und gerade, wenn die Geräte zur Unterschriftenerfassung am POS vorinstalliert und zur Verwendung bereit sind, keinen zusätzlichen Aufwand für den Kunden mit sich bringen. Der Unterschriftenprozess ist derselbe wie am Papier und erfordert keine Umgewöhnung.

1.2 Dokumentenformat

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

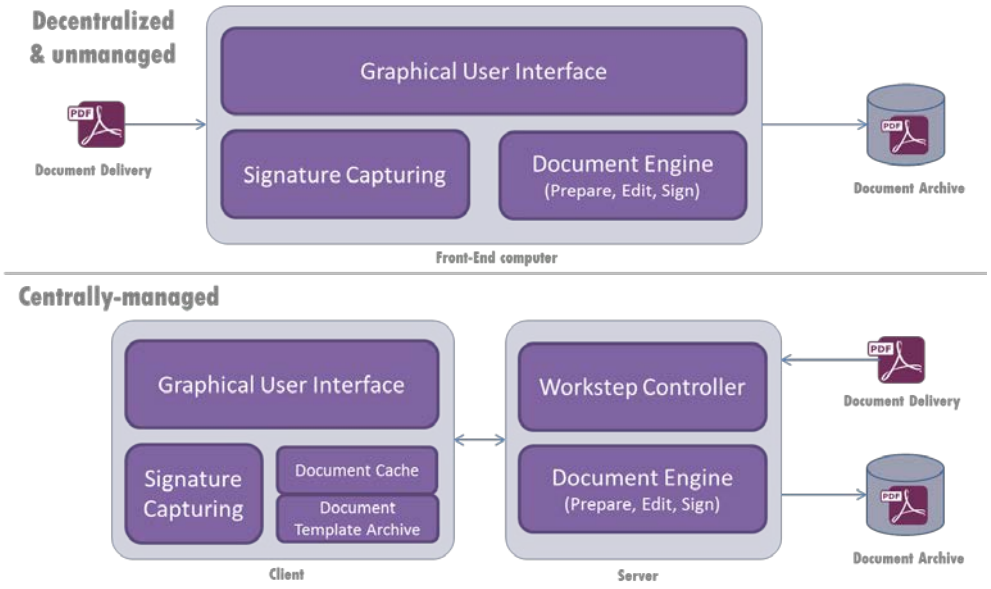
Im Gegensatz zu den proprietären Dokumentenformaten und Dokumentendatenbanken erfüllt das offene Portable Dokument Format (PDF) all diese Anforderungen. PDF ist nicht nur ein offener Standard, der in ISO 32000-1:2008 definiert ist, sondern existiert auch in einer Variante, die für eine langfristige Archivierung 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 32000- 1:2008 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 Dokumentenoriginale zu archivieren.

1.3 Softwarearchitektur

Eine Unterschriftenapplikation besteht typischerweise aus Front-end- und Back-end-Komponenten. Während die Front-end-Software alle Benutzerinteraktionen verwaltet, wickelt die Back-end-Software die Dokumente ab und achtet auf die Integration in den gesamten Arbeitsablauf.

Die Front-end-Softwarekomponente läuft normalerweise auf einem POS-Gerät, dieses kann ein PC oder auch ein Tablet-Gerät sein. Die Back-end-Softwarekomponente kann entweder lokal zusammen mit der Front-end-Komponente innerhalb derselben Applikation bzw. am selben Computer laufen, oder getrennt in einer separaten Serverapplikation, was bedeutet, die elektronische Unterschriftenlösung ist über einen Client und einen Server verteilt.



SIGNificant – Architektur-Optionen

In vielen Szenarien besitzt das Client/Server-Modell mit einer zentralisierten Back-end-Softwarekomponente viele Vorteile gegenüber elektronischen Unterschriftenlösungen, die separat auf jedem lokalen POS Gerät installiert werden müssen. Diese sind:

- 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.

Zusätzlich zentralisieren viele Unternehmen ihre Front-end-Software durch Terminal-Service- Lösungen, wie zum Beispiel von Citrix oder Microsoft, weil sich dadurch die Bereitstellung und Verwaltung der Software einfacher gestaltet.

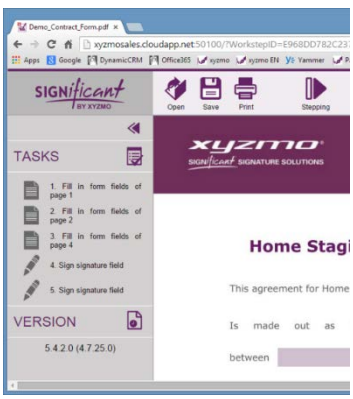
Im Gegensatz dazu, werden reine desktop-/lokalbasierte Unterschriftenlösungen vorgezogen, wenn:

- das zu signierende Dokument am Client dynamisch erzeugt wurde, was einen zusätzlichen Schritt, den Transfer zum Unterschriftenserver vor der Verarbeitung am Client, bedeuten würde.
- eine Serverseitige Integration nicht nötig ist.
- eine schlechte Netzwerkverbindung zu den Clients gegeben ist, welche typischerweise durch eine niedrige Netzwerkbandbreite und/oder hohe Latenz verursacht wird.
  Dieses Problem lässt sich aber durch lokale Dokumenten-Vorlagen (Templates), Caching und Background Synchronisation leicht umgehen.

2 Mehr als nur Unterschriftenerfassung

Um einen Vertrag abzuschließen, benötigt man oft nicht nur eine Unterschrift. Unter Umständen müssen Dokumente bearbeitet oder ausgefüllt werden. Je komplexer der Prozess, desto größer ist die Wahrscheinlichkeit, dass Fehler entstehen. Deshalb sollten, durch eine ordnungsgemäße Führung des Unterzeichners durch das Dokument, fehlende Unterschriften oder freigelassene Formularfelder, vermieden werden.

2.1 Vermeiden von unvollständigen Verträgen



Der Versuch, lückenhafte Verträge nachträglich zu vervollständigen, ist meistens sehr zeit- und kostenaufwendig, da der Kunde, wenn Sie den Fehler bemerken, meist nicht mehr im Haus und schwer erreichbar ist. Deshalb ist es von großem Vorteil, wenn Sie alle nötigen Schritte im Unterschriftenprozess eines Dokuments kontrollieren und regeln können. Diese Schritte können sein: Ausfüllen eines Formulars, Lesen wichtiger Absätze, Verwenden von Scanner oder Kamera, um Anhänge wie ID-Scans hinzuzufügen, Unterschreiben auf Unterschriftenfeldern, und viele mehr.

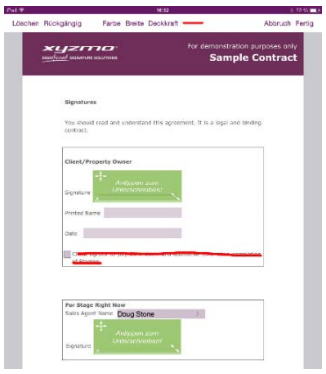
Idealerweise können Sie, abhängig vom Anwendungsfall und Dokument, dem Benutzer verpflichtende Aktionen zum Bearbeiten am Dokument vorgeben oder ihm für andere die Wahl lassen, ob er Aktionen durchführt oder nicht. Dies gibt Ihnen die Flexibilität, die Sie benötigen, um all Ihre Geschäftsfälle abzudecken.

Um zusätzlich zu kontrollieren, welche Funktionen Kunden überhaupt vornehmen dürfen, können Sie Richtlinien aufstellen, die bestimmte Aktionen auf oder mit dem Dokument erlauben oder verbieten. Wie zum Beispiel Freitext-Anmerkungen machen, speichern oder drucken.

2.2 Formularfelder und Anhänge

Weiteres ist es wichtig, dass die elektronische Unterschriftenlösung das Ausfüllen von Formularfeldern, wie zum Beispiel Checkboxen oder Textfeldern, und das Anhängen von Elementen, so wie Scans oder andere Dateien (entweder als sichtbares Element z.B. auf einer neuen Seite oder als Anhang) erlaubt. Die eingegebenen Daten und Anhänge müssen danach im Dokument mit jeder bereitgestellten Unterschrift versiegelt werden. Dadurch wird gewährleistet, dass jede nachträgliche Veränderung im Dokument sichtbar ist. Sie können zusätzlich den Prozessnachweis erhöhen (siehe Kapitel 5.3.1), indem Sie die Benutzeraktionen, die mit der elektronischen Unterschriftensoftware durchgeführt wurden, in einem integrierten Protokoll erfassen.

2.3 Freihand- / Freitextanmerkungen



Es ist nicht immer möglich, alle Informationen im Voraus in das Dokument zu inkludieren oder sie via Formularfeld zu parametrisieren. Die elektronische Unterschriftenlösung muss es Ihnen ermöglichen, Anmerkungen wie zum Beispiel eine Beschreibung, Freihand- oder Freitext mittels Tastatur hinzufügen zu können.

Ein weiteres Beispiel ist ein komplexer Vertrag, bei dem Beteiligte gewisse Bereiche z.B. in einem Foto markieren, Zeichnungen im Dokument vornehmen oder den Inhalt noch flexibel abändern können sollen. Spezielle Werkzeuge für Freihand- / Freitextanmerkungen bieten Ihnen hierfür die nötige Flexibilität.

2.4 Dokumente wie am Papier lesen und bearbeiten

Idealerweise bieten Sie dem Kunden die Möglichkeit, mit digitalen Dokumenten auf dieselbe Weise wie mit Dokumenten auf Papier zu arbeiten. Das bedeutet, dass die elektronische Unterschriftenlösung dem Kunden erlauben muss, mehrseitige Dokumente, idealerweise direkt am Unterschriftengerät, zu überprüfen, bevor er unterschreibt. Mit mobilen Tablets (siehe Kapitel 4.2.3) ist dies leicht durchführbar, da es auf Tablets möglich

ist, das Dokument wie auf Papier zu bearbeiten. Dies inkludiert Freihand- und Freitextkommentare, Anhänge und Ausfüllen von Formularfeldern.Sehr wichtig ist auch die Integration einer Tablet-basierten Unterschriftenlösung in den Dokumenten-Workflow, wenn Sie ein vom POS-System befülltes Formular (zum Beispiel einen Kundenvertrag) auf das Tablet bringen wollen, um dem Kunden dort die Möglichkeit zu bieten, es zu lesen, die Datenfelder zu aktualisieren und danach zu unterschreiben. Anschließend sollten typischerweise alle Eingaben des Kunden aus den Formularfeldern ausgelesen und in einer Datenbank gespeichert werden.

3 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.

3.1 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 (siehe Kapitel 4) 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.

Wenn die biometrischen Unterschriftendaten nicht in der PDF-Datei selbst, sondern in einer Datenbank gespeichert sind, was optional möglich ist (siehe Kapitel 5.3.2), muss der Link zwischen Unterschriftsdaten und Dokument (= Hashwert des zu signierenden Dokuments), mittels einer digital signierten Protokolldatei (Audit Log, siehe Kapitel 5.3.1) gegeben sein, welches wiederum dessen Authentizität und Integrität garantiert.

3.2 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.

3.3 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 zukünftige Streitfälle. Angenommen, der technologische Fortschritt macht es irgendwann 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.

3.4 Echtzeitüberprüfung der Unterschrift für höchsten Prozesssicherheitsstandard

Falls es, nachdem das Dokument unterzeichnet wurde, zu einem Streitfall kommt, können Sie immer eine Unterschriftenprüfung durch einen Graphologen vornehmen lassen. Zusätzlich können Sie unmittelbar nach der Unterschriftsaufzeichnung eine Echtzeitüberprüfung durchführen und dies alles in einem sicheren Protokoll dokumentieren (siehe Kapitel 5.3.2). Die Echtzeit-Unterschriftenprüfung vergleicht die aufgezeichnete Unterschrift mit Musterunterschriften, welche in einer Datenbank gespeichert sind. Dies stellt sicher, dass ein Dokument oder eine Transaktion nur von der richtigen Person unterzeichnet werden kann. Dadurch wird nicht nur Missbrauch reduziert, sondern auch die Beweislast drastisch erhöht. Bekannte Beispiele hierfür sind die Kundenauthentifizierung bei

Kontotransaktionen und Management- bzw. Mitarbeiter-Authentifizierung bei hohen Bestellwerten.

Eine elektronische Unterschriftenüberprüfung verwendet die gesamten erfassten biometrischen Daten (Geschwindigkeit, Beschleunigung und Druck), weshalb die False-Accept- und False-Rejec-Rate um vieles besser ist als wenn einfach Unterschriftenbilder miteinander verglichen werden. Wichtig ist hierbei, dass die Musterunterschriften in Bezug auf natürliche Veränderungen der Gewohnheiten beim Unterschreiben aktuell bleiben. Weiters hat die biometrische Erfassung der Unterschrift gegenüber anderen biometrischen Authentifizierungsmethoden wie Fingerabdruck, Gesichts- oder Retinascan den Vorteil, dass sie sozial akzeptiert ist und als nicht invasiv empfunden wird. Zudem ist eine Unterschrift, auch wenn sie gehackt wurde, nicht wiederverwendbar, da keiner auf genau dieselbe Weise zweimal unterzeichnen kann und die Unterschriften sich per Definition voneinander unterscheiden müssen. Außerdem kann ein Kunde immer wieder ein neues Unterschriftenprofil kreieren, indem er seine Unterschrift verändert. Im Gegensatz dazu verändern sich Fingerabdrücke etc. nicht - sie sind statisch - und könnten wieder und wieder verwendet werden.

Zusätzlich erlauben einige europäische Länder (zum Beispiel Italien) die Freischaltung eines qualifizierten, persönlichen Unterschriftenzertifikats, das in einem zentralen Hochsicherheitsmodul (HSM) gespeichert ist, mittels biometrischer Verifikation anstatt mit einem numerischen PIN. In diesem Fall können Benutzer eine qualifizierte elektronische Signatur (QES) ganz allein mit ihrer persönlichen Unterschrift durchführen.

4 Geräte zum Erfassen von biometrischen Unterschriften

Der typische Gesamtgeschäftsprozess für elektronische Unterschriften in Filialen, Einzelhandel und Kundencentern unterscheidet sich von Anwendungsfällen, bei denen Mobilität im Vordergrund steht. Die verwendeten Geräte sind meist größer, sodass sie bequem das Dokument anzeigen können. Auch andere Faktoren, wie das Abspielen von Werbungen in Pausen und die Möglichkeit, Fragebögen anzuzeigen, um Feedback vom Kunden zu bekommen, sind oft wesentlich. Die wichtigsten Anforderungen an elektronische Unterschriftenlösungen am POS sind weiter unten aufgelistet.

4.1 Unterschriftenpads vom Anbieter Ihrer Wahl

Welche Unterschriftenerfassungsgeräte am besten passen, hängt hauptsächlich von den speziellen Anwendungsfällen und den vorliegenden Umgebungskonditionen ab. Am Markt sind eine Vielzahl von Geräten zu finden, vom einfachen Signaturpad mit schwarz/weiß Display über Unterschriftenpads mit Farbdisplay, Smartphones, Stiftbildschirmen mit einer Displaygröße von 10 Zoll und mehr, bis hin zu Tablets, die auf iOS, Android oder Windows laufen.

Nur eine geräteunabhängige Unterschriftenplattform bietet hierfür ausreichende Flexibilität. Somit können Sie einfach das für den jeweiligen Anwendungsfall am besten passende Gerät nutzen. Dies wird mit einer modularen Architektur erreicht, die es

ermöglicht, neue Unterschriftenerfassungshardware mittels Plug-and-Play hinzuzufügen. Im bestmöglichen Fall können Sie die zurzeit verwendeten Geräte mit Neueren austauschen ohne ihre bestehende spezifische Integration der elektronischen Unterschriftenlösung anpassen zu müssen.

Dadurch sind Unternehmen nicht von Anbietern von Unterschriftenhardware abhängig und können, jedes Mal wenn ein altes Gerät ersetzt werden muss, eine gut durchdachte Entscheidung treffen. Zudem erwarten Experten, dass der Markt für Unterschriftenerfassungsgeräte in den nächsten Jahren mit ziemlicher Wahrscheinlichkeit nicht mehr so aussieht wie heute.

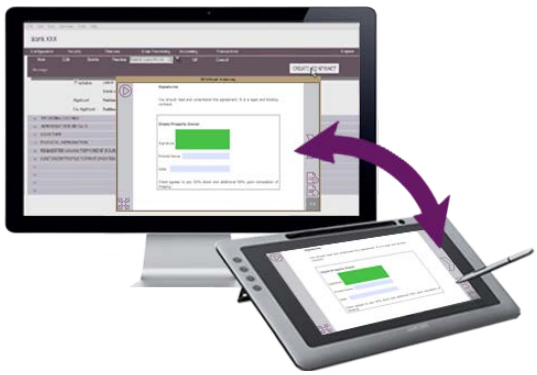
4.2 Das gesamte Dokument anzeigen

Viele Anwendungsfälle und in manchen Ländern auch das Gesetz verlangen, dass nicht nur ein Unterschriftenfeld, sondern der gesamte Inhalt des Dokuments auf dem Display angezeigt werden muss. Mit schwarz/weiß Signaturpads ist es möglich, jenen Teil des Dokuments als Hintergrund anzuzeigen, über dem das Unterschriftenfeld liegt. Um jedoch das gesamte Dokument durchzublättern und ganze Teile gut lesen zu können, wird ein Gerät mit Farbbildschirm und hoher Auflösung benötigt.

4.2.1 Unterschriftenpads

Mit einem Unterschriftenpad mit einem hoch auflösenden 4-5-Zoll-Farb-LCD ist es bereits möglich, ein zu signierendes Dokument in seiner vollen Breite lesbar darzustellen. Beispiele für funktionierende Geräte sind Wacom STU-530, SIGNificant ColorPad 6, StepOver naturaSign Flawless Pad und einige mehr. Die limitierte Displaygröße erlaubt, durch das Dokument am Unterschriftenpad zu scrollen. Dies geschieht entweder autonom oder über eine elektronische Unterschriftensoftware, die am verbundenen PC (Desktop) läuft. Wie in Kapitel 0 dargestellt, muss die Antwortzeit der Datenübertragung beachtet werden.

4.2.2 Stiftbildschirme



Wenn Sie mit einem Stiftbildschirm als Zweitbildschirm arbeiten, der die Größe von 10 Zoll oder mehr hat, benötigen Sie eine elektronische Unterschriftenlösung, die das Zusammenspiel mit dem Hauptbildschirm entsprechend managen und automatisieren kann. Andernfalls können Sie nicht von all den Stärken profitieren, die diese Geräte anbieten. Windows behandelt z.B. den Stift des Stiftbildschirms als zusätzliches Eingabegerät. Jedes Mal, wenn der Kunde mit dem Stift den Bildschirm berührt, wird der Fokus vom Betriebssystem auf die berührte Stelle am Stiftbildschirm (Zweitschirm) verschoben und die Aktion am ersten Bildschirm wird unterbrochen. Zudem

ist es schwierig, Anwender darin zu schulen, dass Sie zu unterschreibende Dokumente problemlos je nach Bedarf zwischen Erst- und Zweitbildschirm hin und her schieben können.

Ein klarer Vorteil von Unterschriftenbildschirmen ist ihre Antwortzeit, welche sich deutlich von der eher langsamen Antwortzeit der Unterschriftenpads mit Farbbildschirm unterscheidet. Bildschirme im Idle-Modus eignen sich außerdem für Marketingzwecke, um Videos oder Bilder mit hoher Auflösung anzuzeigen.

Normalerweise verwenden Sie den Stiftbildschirm für Kunden parallel zum Hauptbildschirm des Angestellten. Allerdings hat der Angestellte oft keine freie Sicht auf den Stiftbildschirm des Kunden und kann daher nicht direkt sehen, was der Kunde gerade macht. Deshalb muss folgendes beachtet werden:

- Wenn der Kunde ein Dokument auf dem Stiftbildschirm überprüft und unterzeichnet, muss der Angestellte parallel auf seinem Bildschirm arbeiten können, ohne von der Kundeninteraktion mit der elektronischen Unterschriftenlösung blockiert zu werden. Deshalb ist zu verhindern, dass während der Bearbeitung am Stiftbildschirm der Mausfokus am Hauptbildschirm verloren geht.
- Der Anzeigewechsel zum Stiftbildschirm muss vollautomatisch ablaufen. Die Applikationsfenster manuell auf zwei Bildschirmen herumzuschieben wäre ein zu großer Aufwand.
- Um besser unterstützen zu können, sollte der Angestellte auf dem Hauptbildschirm in einem Überwachungsfenster sehen können, was der Kunde am Stiftbildschirm macht.
- Interaktive Bildschirme sind praktisch, um Kundenfeedback zu bekommen. Hierfür sollte die Unterschriftenlösung dem Kunden Umfragen anzeigen und die Daten der Antworten sammeln können.
- Wenn sich der Bildschirm im Idle-Modus befindet, sollte vorgefertigte Werbung, wie zum Beispiel Präsentationen oder Videos, angezeigt werden können. Dieser Werbemodus sollte andere Applikationen, die parallel auf einem verbundenen PC laufen, nicht beeinträchtigen.

4.2.3 Multifunktionale Tablets

Mobile Tablets, wie das iPad, das Galaxy Note 10 oder das Surface Pro sind hauptsächlich für mobile Anwendungen entwickelt worden. Diese vielseitig einsetzbaren Geräte besitzen einen angemessen großen Bildschirm, mit dem man Dokumente bequem ansehen kann und sind dank Massenproduktion vergleichsweise günstig zu bekommen. Das macht sie auch für POS-Prozesse sehr interessant. Gerade, wenn Ihr Vertrieb nicht nur am stationären POS arbeitet, sondern teilweise mobil sein muss, können sie ihre Stärken ausspielen.

Ein zusätzlicher Vorteil ist, dass diese multifunktionalen Geräte einfach durch eine native Applikation in biometrische Unterschriftenerfassungsgeräte verwandelt werden können. Nebenbei laden sie auch noch sämtliche Daten im Hintergrund und speichern sie lokal, was die Transaktionen von Netzwerkverbindungen, Bandbreitenproblemen und/oder langsamer Antwortzeit des Servers unabhängig macht (siehe Kapitel 6.2). Zudem sind

multifunktionale Tablets ideal, um Kunden ein Arbeiten wie auf Papier zu ermöglichen (siehe Kapitel 2.4).

Darüber hinaus bringt es viele Vorteile, wenn die Unterschriftenanwendung auf den mobilen Geräten in die gleiche elektronische Unterschriftenlösung integriert ist, wie jene für Signaturpads und Stiftbildschirmen. Nur so ist es möglich, einfach zwischen Signaturpads und mobilen Erfassungsgeräten hin und her zu schalten.

4.3 Verwendung eines Smartphones, um biometrisch Unterschriften zu erfassen

Smartphones haben sich inzwischen weitgehend am Markt durchgesetzt. Nahezu jeder besitzt eines. Deshalb ist deren Verwendung als biometrisches Unterschriftenerfassungsgerät naheliegend — speziell in Situationen, bei denen Verkaufspersonen nicht mit speziellen Signaturpads, Stiftbildschirmen oder Tablets ausgestattet werden können. Auch wenn Sie selbstständige Außendienstmitarbeiter nicht mit einer Unterschriftenerfassungshardware ausstatten wollen, können Sie sich meist darauf aufbauen, dass jede Verkaufsperson ein Smartphone besitzt und dieses für die Unterschriftenerfassung somit verwenden kann.

Alles was Sie tun müssen, ist eine kleine Unterschriftenerfassungsapplikation für biometrische Daten für diese Smartphones zur Verfügung zu stellen. Diese sollte mit der Back-end-Komponente Ihrer elektronischen Unterschriftensoftware kompatibel sein. Dann kann einfach mit einem Stylus, dem Finger oder einem nativen Stift auf dem Smartphone unterschreiben werden.

Das typische Verfahren inkludiert die folgenden Schritte:

- Dokumente werden am Computerbildschirm im Browser angesehen, Formularfelder ausgefüllt und Anhänge wie z.B. Ausweiskopien hinzugefügt - vielleicht zusammen mit einem Kunden, Mitarbeiter oder Geschäftspartner - und dann ein Smartphone als Unterschrifterfassungsgerät verwendet.
- Eine native Anwendung verwandelt das Smartphone in ein Unterschriftenerfassungsgerät. Diese Anwendung sollte auf iOS, Android und Windows Handys verfügbar sein.
- Wenn der Unterzeichner bereit ist, das Dokument zu unterschreiben, wird zwischen dem Smartphone und dem Host-Computer eine sichere Verbindung aufgebaut.

- Diese sichere Verbindung zur Serverapplikation wird mit Hilfe eines Tokens aufgebaut. Dazu muss weder der Host-PC noch das Smartphone aufwendig konfiguriert werden — beide können einfach existierende Netzwerkverbindungen verwenden. Der Token kann z.B. bequem in der Unterschriftenapplikation am Smartphone über die Kamera mittels QR-Code-Reader eingelesen werden.
- Die Unterschriftenerfassungsapplikation zeigt dann einen Erfassungsdialog, bei dem das Dokument visuell im Hintergrund angezeigt wird.

- Die Unterschrift wird auf dem Smartphone erfasst. Es wird empfohlen, Smartphones mit Originalstift oder einen Fineline-Sylus aus dem Zubehörhandel, aber zumindest einen Stylus für die Unterzeichnung zu verwenden, weil nur mit dem Finger aufgezeichnete Unterschriften forensisch schwer verwertbar sind.
- Nachdem die Unterschrift erfasst ist, wird diese über die gesicherte Verbindung an den Host-PC übertragen und verschlüsselt in das Dokument eingebettet.

5 Prozessnachweis

Der Beweis über die Authentizität eines digital signierten Dokuments hängt hauptsächlich vom Aktivitäten-Protokoll (Audit Trail) der elektronischen Unterschriftenlösung ab. Dieses Protokoll kann entweder in unterschriebenen Dokument selbst, was es dem Dokument ermöglicht eigenständig zu sein (Kapitel 1.2), separat, oder in einer Kombination aus beidem gespeichert werden.

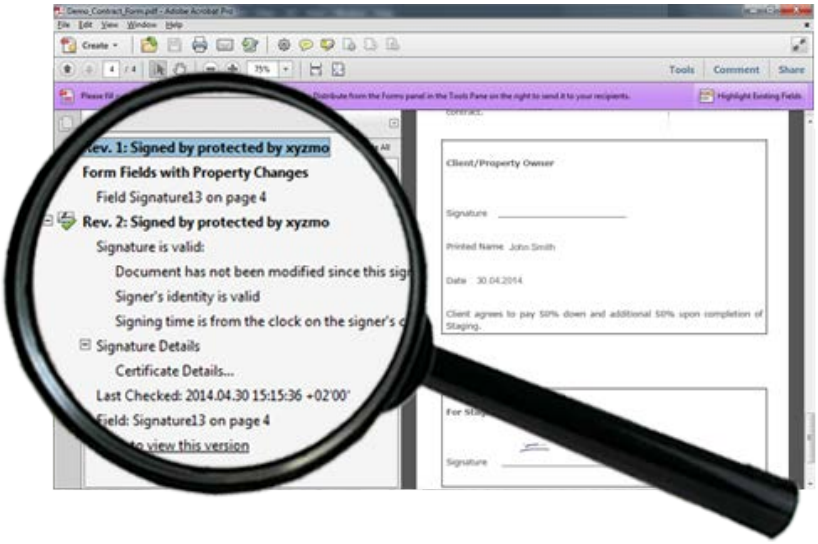
Protokolle können noch viel mehr. Ein ordnungsgemäßes Protokoll, das Authentifizierungsergebnisse für die Unterzeichner beinhaltet, verlagert die Beweislast bei einem Gerichtsverfahren auf den Unterzeichner, insbesondere wenn die Lösung bereits viele Dokumente ohne Probleme verarbeitet hat. Der Richter wird in so einem Fall voraussichtlich annehmen, dass die Lösung auch für das in Frage gestellte Dokument angemessen funktioniert hat. Wichtig ist hierbei, dass das Protokoll für die involvierten Richter und Anwälte ohne eine Konsultierung eines technischen Experten verständlich ist. Wenn alle Aktionen der involvierten Unterzeichner aufgezeichnet wurden, kann dies als Beweis des gesamten Prozesses verwendet werden und unterstützt zusätzlich die Beweislage.

Anmerkung: Insbesondere wenn Sie Cloud-basierte Lösungen verwenden, müssen Sie sichergehen, dass Sie alles, was Sie zum Beweisen der Authentizität der Dokumente, auch einige Jahre später, benötigen, besitzen. Vor allem für den Fall, wenn Sie nicht länger Kunde dieses Anbieters sind oder der Anbieter nicht mehr existiert.

5.1 Nachweis durch digitale Unterschriften/Zertifikate

Auch bein einer biometrischen Unterschrift ist, um Kompatibilität zum PDF Signaturstandard zu wahren (siehe Kapitel 1.2), das Dokument mit jeder einzelnen Unterschrift auch digital zu signieren. Hier erfolgt die digitale Signatur einfach mit einem allgemeinen Zertifikat (z.B. auf den Anbieter ausgestellt), da die Authentizität der Unterschrift inklusive der Identität des Signatars eben mit den biometrischen Daten der aufgenommenen eigenhändigen Unterschrift festgestellt werden kann.

Dies hat den großen Vorteil, dass wenn Sie digitale Unterschriften in einem PDF überprüfen, Sie mit einem Standard-konformen PDF-Viewer einen Einblick in die eingebettete Unterschriftenhistorie haben, auch wenn Sie nicht mit dem Internet verbunden sind. So können Sie exakt zurückverfolgen, wie das Dokument bei jeder erfassten digitalen Unterschrift ausgesehen hat.



Zusätzlich liefern digitale Unterschriften Beweise für die folgenden Gesichtspunkte:

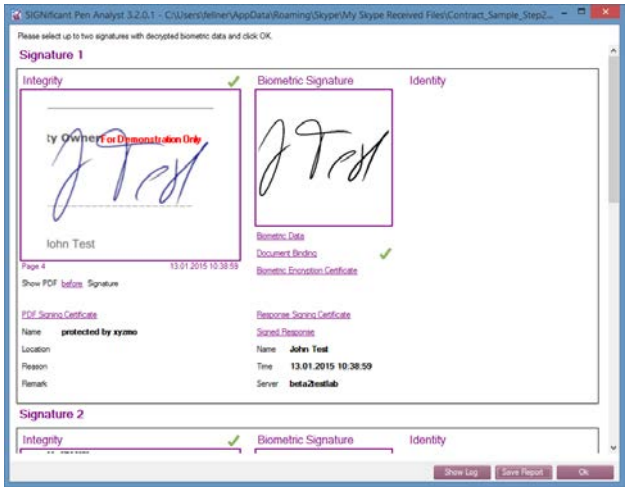
- Die Integrität des Dokuments (siehe Kapitel 3.2),
- das Datum und die Zeit, an dem das Dokument unterzeichnet wurde — wahlweise durch einen vertrauenswürdigen Zeitstempel,
- der Ort, an dem das Dokument unterzeichnet wurde (eventuell GPS unterstützt),
- der Aussteller des unterzeichneten Dokuments (durch verwendete digitale Zertifikate).

5.2 Beweise durch biometrische Unterschriftendaten

Die biometrische Unterschrift erlaubt es Ihnen, ohne zusätzliche serverbasierte Protokolle (siehe Kapitel 5.3), die Authentizität eines unterzeichneten Dokuments zu überprüfen. Allerdings benötigt man dafür:

1. Die Möglichkeit, die Unterschriftsdaten des Dokuments zu entschlüsseln. Dies geschieht mit einem sicher verwahrten privaten Entschlüsselungsschlüssel.
2. Die Möglichkeit, wie am Papier, einer manuellen Unterschriftenprüfung durch einen Experten (Graphologen).

Punkt zwei ist nicht zwingend notwendig, wenn Sie Beweise liefern können, dass die erfasste biometrische Unterschrift in Echtzeit gegen ein gespeichertes Unterschriftenmuster des Unterzeichners verlässlich vor dem Einbetten in das Dokument geprüft wurde. Um vertrauenswürdige Beweise liefern zu können, muss die biometrische Unterschrift mit einer signierten Antwort von einem identifizierten Unterschriften-Verifikationsserver (siehe Kapitel 3.4) gekoppelt sein. Diese digital signierte Antwort ist notwendig, um sicherzugehen, dass das System nicht anfällig für Umgehungen ist (zum Beispiel durch einen gehacktes Prüfservice). So können Sie einfach sicherstellen, dass der Nachweis über ein authentifiziertes und zertifiziertes Prüfsystem erfolgt ist.



Unterschriftenprotokoll eines eigenständigen PDF Dokuments inkl. signierter biometrischer Verifikation

5.3 Typische Serverbasierte Protokolle (Audit Trails)

Serverbasierte Protokolle können unabhängig von den signierten Dokumenten gespeichert werden (zum Beispiel in einem zentralen Archiv), was deren Archivierung und Verteilung einfach gestaltet. Bei der biometrischen Unterschrift sind diese optional, etwa um die Beweislast zu erhöhen bzw. die Beweisführung zu vereinfachen.

5.3.1 Aktionsprotokolle

Serverprotokolle entfalten ihr volles Potential erst dann, wenn sie auch sämtliche durchgeführte Aktionen beinhalten (= Prozessbeweise), wie zum Beispiel die Verwendung eines bestimmten Dokuments auf einem dezidierten Point-Of-Sale oder durch einen bestimmten Vertreter oder die in einem Dokument ausgeführten Tätigkeiten. Protokolle sollten genau dokumentieren, was mit einem spezifischen Dokument, in welcher Reihenfolge, zu welchem Zeitpunkt und wo passiert. Dies kann auch die Anzeigebestätigung von speziell markierten Stellen in Dokumenten beinhalten, die vom Anwender gelesen werden müssen. Das Protokoll sollte zumindest die ausgeführten Schritte des Unterzeichners, basierend auf dem vordefinierten Leitfaden durch das Dokument (siehe Kapitel 2.1), nachverfolgen können. Allerdings sind detaillierte Informationen über ausgeführte Authentifizierungsschritte, wie sie zum Beispiel bei

HTML5-Unterschriften verwendet werden (wie SMS-TANs an registrierte Handynummern, oder gescannte IDs), am wichtigsten.

5.3.2 Prüfprotokoll biometrischer Echtzeitunterschriften

Falls Sie die erfassten biometrischen Daten nur in einem zentralen Archiv speichern wollen — im Gegensatz zur zusätzlichen Speicherung im signierten PDF-Dokument — können Sie auf diese mit Hilfe der Kennung (RequestID) der durchgeführten Verifikation vom Aktionsprotokoll aus (siehe Kapitel 5.3.1) ins Prüfprotokoll des Verifikationsservers (siehe Bild unten) verweisen.

Da dieses Prüfprotokoll des Verifikationsservers die biometrischen Daten selbst nicht enthält, sondern nur darauf referenziert, ist der Beweis über die erfolgte Unterschriftenauthentifizierung viel zugänglicher. Der Nachweis der erfolgten Überprüfung, um diese zum Beispiel in einem Gerichtstreit vorzulegen, erfordert keine Entschlüsselung der Unterschriftsdaten und kein Graphologen-Gutachten.

Audit Trail für Profil:default

RequestId	Datum/Zeit	Tätigkeit	Ergebnis	Profil	Geräteprofil	Unterschrift	Beschreibung	Authentifizierter Benutzer (IIS)	Angaben zum Host
40d386bc-b4d7-475f-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-b4d7-475f-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)
3daaaae3c-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-b1c2-4763-9e37-4510cff8adf9	Friday, July 04, 2014 7:36:12 AM	ProfileAdd	Ok	default			Profil hinzugefügt	sign043\usermanager	SIGN043 (4.3.0.8)

Mit Hilfe eines solchen Prüfprotokolls und des im Dokument selbst gespeicherten signierten Überprüfungsergebnisses einer Unterschrift (siehe Kapitel 5.2), das auch von Personen einfach zu lesen ist, welche keine Kenntnis der verwendeten Technologie oder Produkte haben (wie Richter oder Anwälte), können Sie die Beweiskraft einer Unterschrift massiv steigern. Dementsprechend kann die Beweislast, dass das Dokument nicht von dieser Person unterzeichnet worden ist, auf den Unterzeichner selbst übertragen werden (Beweislastumkehr).

6 Integrations- und Bereitstellungsanforderungen

Zusätzlich zu den funktionalen Anforderungen an die elektronischen Unterschriftenlösung selbst, die in den vorhergehenden Kapiteln dargestellt wurden, bestehen Anforderungen rund um die Integration der Lösung in Ihre existierende IT- und Applikationsumgebung. Die Wichtigsten finden Sie hier.

6.1 Eigenständige GUI-App oder SDK

Wenn eine schnelle und kosteneffiziente Entwicklung nötig ist, ist eine eigenständige Anwendung mit einer fertigen graphischen Benutzeroberfläche die beste Lösung. Diese Möglichkeit erlaubt normalerweise immer noch eine einfache Anpassung der Farbschemen, Logos, etc.

Falls eine nahtlose Integration in eine bereits vorhandene Applikation (ohne einen UI-Kontextwechsel) gewünscht wird, dann ist die Verwendung eines SDK die richtige Wahl. Auf diese Weise können Sie das Nutzererlebnis und alle GUI-Elemente durch Programmierung selbst managen. Mächtige SDKs bieten viel mehr als nur einfache Integration der Grundfunktionen — Sie können damit eine komplett adaptierbare Benutzeroberfläche mit Framework nahtlos integrieren.

Je mehr Funktionalitäten das SDK anbietet, desto besser ist es. Mächtige SDKs bieten den vollen Umfang an Funktionen für die Benutzeroberfläche und deren Konfiguration. So benötigen Sie für die Parametrisierung nur ein paar Tage, im Gegensatz zu den Wochen, die Sie benötigen würden, wenn Sie eine low-level-SDK nutzen. Diese bieten zudem meist nur die Grundfunktionalitäten wie die Unterschriftenerfassung.

Ein wesentlicher Nachteil bei der Verwendung eines **low-level-SDKs**, der nur die nötige Unterschriftenerfassung und Dokumentenbearbeitungsfunktionen unterstützt, besteht darin, dass die IT-Abteilung des Unternehmens eine Vielzahl von Sicherheitsanforderungen selbst managen muss (zum Beispiel den Schutz der Unterschriftsdaten des Kunden vor unautorisiertem Zugriff). Für die IT- und Compliance-Abteilung bedeutet dies eine große Herausforderung, da derartige Anwendungen typischerweise nicht zum Kerngeschäft zählen, was viele Fehlerquellen ermöglicht. Eine derartige Entwicklung ist sehr sicherheitskritisch, sodass nicht nur gegen nachlässiges Programmieren Vorsorge getroffen werden muss, sondern auch gegen bewusst erstellte Schadsoftware. Selbst dann, wenn alle Sicherheitsvorkehrungen getroffen wurden, kann es schwierig sein, einem Endkunden oder einer Drittpersonen ein hohes Sicherheitsgefühl zu vermitteln, da das Unternehmen / die Angestellten durch die Eigenentwicklung theoretisch die vertraulichen Daten missbrauchen könnten. Deshalb ist ein entsprechend mächtiges SDK, das eine gesamte Standardapplikation umfasst, die bessere Wahl. Das Unternehmen kann so beweisen, dass es nicht möglich ist, die Unterschrift zu manipulieren.

6.2 Schneller Betrieb trotz geringer Bandbreite

Gerade wenn eine serverbasiere Architektur verwendet wird, ist es wichtig, auf die Antwortzeit und nötige Bandbreite zwischen Client und Server, zu achten. Durch lokales Caching und Hintergrundsynchronisation können serverbasierte Lösungen diese sehr stark optimieren.

Antwortzeiten sind nicht nur von der Serverperformance und der Skalierbarkeit abhängig, sondern auch von der Antwortzeit des Unterschriftenerfassungsgerätes. Im Gegensatz zu USB-basierten Signaturpads arbeiten Tablets mit nativen Apps und Stiftbildschirme nahezu ohne Verzögerung. Diese Signaturpads sind Peripheriegeräte, die nur den Inhalt,

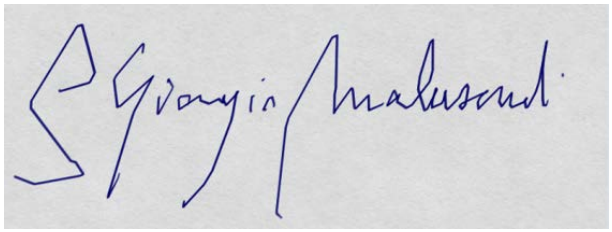
typischerweise als Bild, anzeigen, den diese über die USB Verbindung erhalten. Die übliche Antwortzeit der Datenübertragung vom Host-PC (Desktop) auf ein Signaturpad mit Farbdisplay sind ca. 2-3 Sekunden.

6.3 USB- basierten Unterschriftenerfassungsgeräte auf Thin-Clients

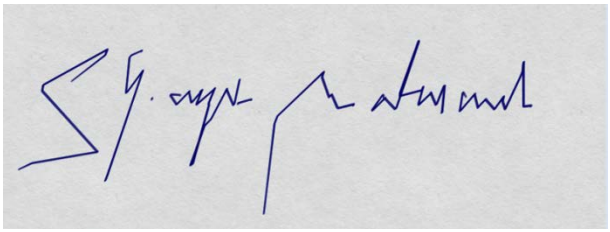
Falls Ihre POS-Client-PCs mit Citrix, VMware oder Windows RDP/Terminal Services virtualisiert sind, muss Ihre elektronische Unterschriftenlösung die vom USB-Unterschriftengerät am Thin-Client erfassten Daten lokal zwischenspeichern. Ansonsten gehen Teile dieser erfassten biometrischen Unterschriftsdaten aufgrund von Latenzen im Netzwerk schlichtweg verloren.

Dies passiert, weil Signaturpads die erfassten Daten an einen lokalen Pufferspeicher einfach mittels „fire-and-forget“ weitergeben, was kein Problem darstellt, solange die Software, die die Daten ausliest und verarbeitet, ebenfalls lokal läuft. In einer Thin-Client-Umgebung kann dieser lokale Pufferspeicher allerdings eventuell nicht rechtzeitig ausgelesen werden, da der Zugriff über das Netzwerk erfolgen muss und Latenzen einen rechtzeitigen Zugfriff verhindern. Ein einfaches Durchschleifen der USB-Verbindung reicht hier also nicht.

Die Abbildungen unterhalb zeigen, wie die Netzwerklatenz die Qualität der Unterschriftenerfassung auf einem Thin-Client-Terminal, der die Daten via USB einfach durchschleift (also ohne lokale Zwischenspeicherung durch die Unterschriftenlösung), negativ beeinflusst.



60 msec Latenz



100 msec Latenz

6.4 Innerhalb der eigenen Infrastruktur oder in der Cloud

Wenn Sie sich für eine Client/Server-Architektur entschieden haben (siehe Kapitel 1.3 Vor- und Nachteile), müssen Sie ein Bereitstellungsmodell für Ihre Back-end-Infrastruktur wählen. Entweder erwerben Sie den Betrieb mit der Lösung gemeinsam in einer privaten Cloud, nutzen ein SaaS-Model oder Sie betreiben die Lösung in Ihrer eigenen Infrastruktur.

Obwohl ein Cloud-basierter Ansatz schneller und einfacher aufzusetzen ist und gewisse Möglichkeit bietet, zu entscheiden wo Ihre Server betrieben und die Daten gespeichert werden, verwenden viele Unternehmen weiterhin ihre eigene Infrastruktur. Bei diesem Ansatz sind alle Applikationen und Dateien in Ihrem lokalen Rechenzentrum abgelegt, was bedeutet, dass Sie nicht von externen Systemen oder Internetverfügbarkeit abhängig sind. Außerdem bietet nur der Betrieb in der eigenen Infrastruktur die volle Kontrolle über den Datenschutz, was Cloud-Services einfach nicht garantieren können.[1]

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

Wenn Sie Ihre eigenen Server verwenden, können Sie einfach zwischen einer nativen Installation, bei der die Software direkt am Rechner läuft, und einem virtualisierten Ansatz (z.B. mit Virtualisierungssoftware von VMware, Citrix oder Microsoft) wählen.

7 SIGNificant-Referenzen

SIGNificant ist eine elektronische Unterschriftenplattform für Unternehmen, die es Ihnen ermöglicht, am Point-Of-Sale (POS), egal ob direkt in der Filiale, im Shop oder über indirekte Verkaufskanäle die Sie selbst nicht ausstatten können, ganz ohne Papier auszukommen. SIGNificant stellt Ihnen die Benutzeroberfläche und die Werkzeuge, die nötig sind, um den optimalen Unterschriftenprozess und das optimale Nutzererlebnis zu definieren, zur Verfügung. Die verschiedenen Bausteine der Plattform machen es Ihnen möglich, die beste Kombination aus Unterschriftenlösung und Unterschriften-erfassungsgeräten für jeden Anwendungsfall zu wählen. Egal ob für Signaturpads, interaktive Stiftbildschirme, mobile Geräte oder webbasierte Unterschriften.

Um besser zu illustrieren, wie SIGNificant in verschiedenen Branchen für deren spezielle Anwendungsfälle am POS angewendet werden kann, zeigt das folgende Kapitel reale Fallstudien inklusive deren Implementierung im Geschäftsprozess von Anfang bis Ende.

7.1 Retail banking: GE Money Bank (Tschechische Republik)

Anwendungsfall:

- Kontotransaktionen von Kunden (Einzahlungen, Geldbehebung, Geldtransfer)
- Standardverträge (Kontoeröffnung, Kreditkarten, etc.)
- Kreditverträge und Vereinbarungen
- Verträge bei Geldanlagen

Eingesetzte Produkte:

- Unterschriftenapplikation: SIGNificant Server mit Web-Signin-Interface und Linux-basierte Citrix Komponenten auf Dell Thin-Client Terminals.
- Authentifizierungsapplikation: SIGNificant Biometric Server — Enterprise Edition mit Oracle DB
- Unterschriftenerfassungshardware: SIGNificant ColorPad 6.

Anwendung im Geschäftsprozess:

1. Der Kunde kommt in die Filiale und wird von einem Angestellten begrüßt.
2. Wenn dieser kein eingetragener Kunde in der Unterschriftendatenbank ist, muss sich der Kunde beim Bankangestellten mittels ID-Karte ausweisen (zum Beispiel nationale ID-Karten) und in die SIGNificant-Unterschriftendatenbank eingetragen lassen.
3. Der Angestellte bearbeitet die Kundenanfrage (zum Beispiel Geldbehebung).
4. Der Kunde überprüft das zu unterzeichnende Dokument und unterschreibt es mit seiner handschriftlichen Unterschrift, beides direkt am SIGNificant Signaturpad.

5. Der SIGNificant Biometric Server verifiziert die eigenhändige Unterschrift des Bankkunden in Echtzeit im Vergleich zu dem in der Datenbank gespeicherten Unterschriftenprofil des Kunden, um eine Authentifizierungsprüfung während der Transaktion auszuführen.
6. Wenn das Ergebnis der Authentifizierung positiv ist, wird die Anfrage des Kunden durchgeführt und der SIGNificant Server unterzeichnet das Dokument zur Transaktion mit den erfassten biometrischen Unterschriftendaten, setzt einen vertrauenswürdigen digitalen Zeitstempel auf das Dokument und versiegelt dieses mit einem Zertifikat, das im HSM der Bank sicher verwaltet wird.
7. Das System legt das signierte PDF/A-Dokument in einem Archiv ab
8. Wenn der Kunde nicht explizit nach einer Kopie verlangt, wird nichts gedruckt.
9. Der Kunde kann auf das signierte Dokument über die Webapplikation zugreifen.

7.2 Einzelhandel: REWE Kaufhaus (Deutschland)

Anwendungsfall:

- Digitales Unterschreiben elektronischer Belege von Lastschriftverfahren und Kreditkarten bei Selbstbedienungskassen mit einer handschriftlichen Unterschrift.

Eingesetzte Produkte:

- Unterschriftenapplikation: SIGNificant Server mit Cash Register Plug-In
- Unterschriftenerfassungshardware in Shops: Wacom STU-500

Anwendung im Geschäftsprozess:

1. Der Kunde geht zur Kassa in der Filiale und erfasst die Waren, um zu zahlen.
2. Der Kunde wählt zwischen elektronischer Lastschrift oder Kreditkartenzahlung.
3. Er oder Sie überprüft die Rechnung mit Zeit, Datum und Zahlungsmethode auf dem Bildschirm des Wacom STU-500 Signaturpads und unterschreibt direkt mit seiner oder ihrer handschriftlichen Unterschrift.
4. Der SIGNificant Server unterzeichnet das Dokument mit einer handschriftlichen Unterschrift und setzt mit dem REWE Unterschriftenzertifikat einen Sicherheitsstempel darauf.
5. Wenn der Kunde nicht explizit nach einer Kopie verlangt, wird nichts gedruckt.