Elektronische Unterschriften online einholen

Dokumente im Web Browser unterschreiben. Überall. Jederzeit. Auf jedem Gerät.

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

Die Digitalisierung von Geschäftsprozessen ist für die meisten Branchen wichtig – und im Wettbewerb am Markt oft überlebenswichtig. Organisationen, die eher virtuelle Produkte anstatt physischer verkaufen haben eine Kostenbasis, die sich hauptsächlich auf Entwicklung, Marketing & Vertrieb sowie auf Services konzentriert, was sich sehr gut für eine Digitalisierung eignet. Das bedeutet eine konsequente Ausrichtung auf die Automatisierung der zentralen Geschäftsabläufe, um den Self-Service-Grad zu erhöhen und vollständig digitale Geschäftsprozesse zu ermöglichen.

Mit Online-Unterschriftenlösungen ist es sehr einfach, Unterschriften von Personen über das Internet einzuholen, die diese direkt auf ihren eigenen Geräten durchführen ohne Sie persönlich zu treffen. Sie können also Links auf Dokumente einfach zum Unterschreiben an andere schicken, haben sofortigen Einblick in den Status des versandten Dokuments, können auf fertiggestellte Dokumente zugreifen und vieles mehr. Egal ob Sie oder Ihre Empfänger im Büro, zu Hause oder unterwegs sind, Online-Unterschriften funktionieren zu jeder Zeit und von jedem Gerät aus.

Wenn Sie Dokumente zur Unterschrift versenden, erhält der Empfänger eine E-Mail mit einem Link zu Ihrem Dokument und kann es auf einem Smartphone, Tablet oder auf jedem Web/HTML5-fähigen Gerät unterschreiben, ohne etwas herunterladen zu müssen. Sie können mehrere Unterzeichner definieren und diese in der von Ihnen geforderten Reihenfolge unterschreiben lassen. Mit Online-Unterschriften können Sie Kunden über die Geräte erreichen, die Sie ohnedies schon benutzen. Zusätzlich ermöglicht es die Nachvollziehbarkeit von Geschäftsabschlüssen sowie eine äußerst komfortable Nutzung. Online-Unterschriftenlösungen erlauben Ihnen, Markierungen und Metadaten auf Dokumenten zu erstellen, die Kunden dabei helfen, zu verstehen, wie sie unterschreiben und welche Felder sie ausfüllen müssen. Elektronische Dokumente können auch Prüftools enthalten, die häufig auftretende Fehler rechtzeitig identifizieren und somit menschliche Fehler vermeiden. All diese Funktionen summieren sich schließlich zu einer besseren Vertragsqualität und Kundenzufriedenheit.

Dieses Whitepaper hilft Ihnen zu verstehen was eine gute Online-Unterschriftenlösung bieten sollte. Der Schwerpunkt liegt auf dem Aspekt, warum die Schritte des Kunden bis zur online Unterschrift genau gemanagt werden müssen und was diese beinhalten. Das Whitepaper soll Ihnen helfen, die geeignetsten Methoden zur Authentifizierung des Unterzeichners, ohne ihn persönlich zu treffen, auszuwählen. Des Weiteren wird diskutiert welche Unterschriftentechnologie – biometrisch, HTML5 oder zertifikatsbasiert – die beste Lösung für welchen Anwendungsfall sein kann. Dabei werden Sie sehen, dass elektronisches Unterschreiben viel mehr ist als das einfache Aufzeichnen elektronischer Unterschriften – letztendlich geht es darum, den gesamten Prozess zu optimieren. Schließlich wird ein Fallbeispiel, wie einer unserer Kunden (The Phone House) seinen End-to-end Geschäftsprozess implementiert hat, vorgestellt.

Inhaltsverzeichnis

1 Typische Funktionen

Online-Unterschiftenlösungen bestehen in der Regel aus den folgenden Basisfunktionen um dokumenten-basierte Transaktionen mit räumlich entfernten Empfängern effizient über das Internet abzuwickeln:

- Definition der Transaktion (Zusammenstellen der Unterschriftenmappe)
- Durchführung der Transaktion (Ausfüllen und Unterschreiben)
- Berichtswesen (Status, Ablage und Wiederfinden der Unterschriftenmappen)

Jede Aufgabe hat typische Schritte, die in den folgenden Abschnitten dargelegt werden. Zusätzlich muss das System Funktionen zur Administration wie die Verwaltung der Benutzer und Vorlagen und – falls erforderlich – ein anpassbares Branding bieten.

1.1 Definition der Transaktion (Unterschriftenmappe)

Aktionen die vom Versender durchzuführen sind:

- Beginnen Sie mit einer neuen Unterschriftenmappe (ein „Umschlag“ / „Kuvert“, der benutzt wird, um ein oder mehrere Dokumente zur Unterzeichnung zu versenden) oder starten Sie von einer Vorlage.
- Fügen Sie die notwendigen Dokumente zur Unterschriftenmappe hinzu.
- Fügen Sie die Empfänger hinzu. Dies können Unterzeichner oder Empfänger einer Kopie sein.
- Falls Sie ein PDF-Dokument mit Formularfeldern hochladen, werden die Felder automatisch erkannt.
- Legen Sie für Unterschriftenfelder, Anhänge und andere Informationen im Dokument entsprechende Markierungen an.
- Fügen Sie den Betreff und den Bodytext für die E-Mail hinzu.
- Stellen Sie Empfängeroptionen, Erinnerungen und weiteres ein.
- Versenden Sie die Unterschriftenmappe an die zuvor eingetragenen Empfänger.

Kapitel 2 - Managen aller Schritte bis zur Online-Unterschrift - erläutert diese für den Versender wichtigen Prozessschritte im Detail.

1.2 Durchführung der Transaktion (Unterschreiben)

Aktionen die hier von einem oder mehreren Empfänger(n) durchzuführen sind:

- Unterzeichner erhalten ein E-Mail mit einem Link zum Dokument.
- Diese klicken auf den Link.
- Es besteht keine Notwendigkeit, irgendetwas herunterzuladen oder sich wo anzumelden.
- Die Empfänger müssen sich optional je nach Vorgabe vom Versender authentifizieren.
- Die Empfänger können das Dokument überprüfen, Formularfelder vervollständigen und Anhänge hinzufügen.

- Wenn die Empfänger bereit sind unterschreiben sie ein Unterschriftsfeld mittels
    - o „Draw to Sign“ (Aufzeichnen der Unterschrift auf einem Smartphone oder Tablet mit Finger oder Stylus)
    - o „Click to Sign“ (Simpler Bestätigungsdialog)
    - o „Type to Sign“ (Zusätzliche Eingabe des Namens im Bestätigungsdialog)

  auf einem internetfähigen Gerät (Tablet, Smartphone oder Standard-PC der nur Maus und Tastatur besitzt).

Die Anforderungen und Möglichkeiten zu den wichtigsten Aktionen dieses Prozessschrittes werden in nachfolgenden Kapitel im Detail erläutert:

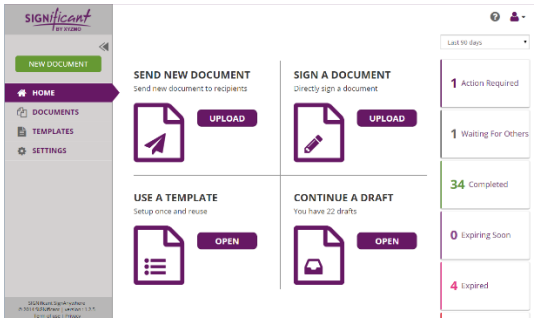
- Benutzerauthentifizierung (Unterzeichner) (siehe Kapitel 3)
- Ausführung der Unterschrift (siehe Kapitel 4).

1.3 Berichtswesen

Ein effizientes Reporting soll die Aufmerksamkeit des Versenders auf jene Transaktionen richten, welche für einen erfolgreichen Abschluss noch Aktionen benötigen. Erfolgreiche Transkationen werden dokumentiert und aufgezeichnet um sie jederzeit wenn nötig beweisen zu können. Eine einfache Übersicht ist hier somit unerlässlich:

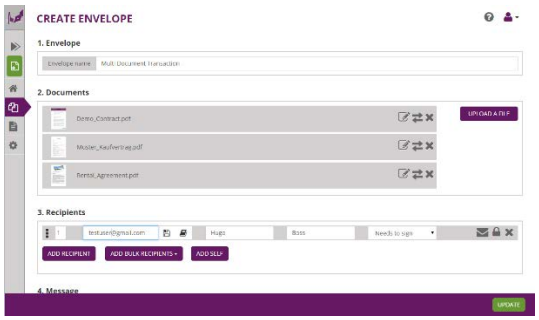
- Dashboards um den Überblick über all Transkationen zu behalten
- Detailansichten um den Status jeder Unterschriftenmappe bequem einsehen zu können. Auf diese Weise wissen Sie immer wo sich Ihre Dokumente in dem Unterschriftenprozess gerade befinden.
- Einfacher Zugriff auf Aktionsprotokolle (Audit Trail) um diese bei Bedarf als Beweismittel abrufen zu können
- Benachrichtigungen einrichten um sich selbst oder Empfänger über wichtige Prozessschritte automatisch zu informieren

2 Managen aller Schritte bis zur Online-Unterschrift



Gerade in Szenarien bei denen der Empfänger online, ohne ein persönliches Meeting mit dem Vertrieb oder Businesspartner, ein Dokument unterzeichnen soll, ist es unerlässlich, dass die Online-Unterschriftenlösungen die Prozesse ordnungsgemäß weitgehend automatisch durchführt. Nur wenn etwas schief läuft sollte ein Alarm ausgelöst werden. Da über 80% aller Unterschriftentransaktionen keine manuellen Tätigkeiten des Versenders verlangen, kann der Arbeitseinsatz damit stark reduziert werden.

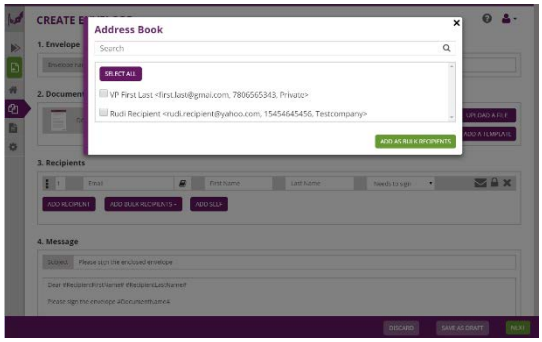
2.1 Transaktionen mit mehreren Dokumenten



Oft müssen für eine Transaktion mehrere Dokumente unterzeichnet werden. Mit Hilfe des Konzepts der Unterschriftenmappen können Sie bequem definieren, welche Dokumente für eine Transaktion benötigt werden.

Mit der Definition von wiederverwendbaren Vorlagen lässt sich zudem viel Zeit sparen, da Sie auf bereits getane Arbeit zurückgreifen können.

2.2 Routing / Workflow



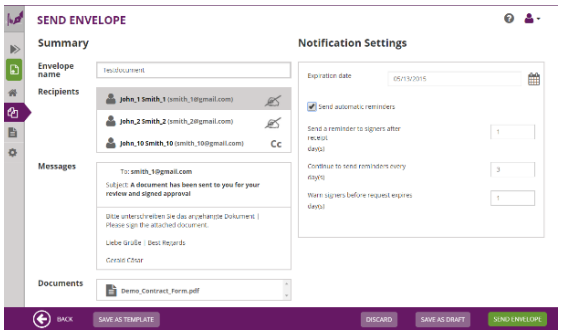
Sie können die Reihenfolge der Personen festlegen, in der sie unterzeichnen müssen und wer am Ende eine Kopie erhält. Dies kann parallel oder sequentiell geschehen, wobei Sie bei letzterem präzise angeben in welcher Reihenfolge jeder Empfänger den Link zum Dokument erhält.

Zusätzlich können Sie dasselbe Dokument gleichzeitig an eine große Anzahl von Empfängern senden, wobei das Dokument selbst dabei für jeden Empfänger getrennt kopiert wird. Was besonders vorteilhaft ist, wenn eine größere Gruppe von Personen dasselbe Dokument unterzeichnen muss. Ein Dokument mit Richtlinien, dass alle Angestellten unterzeichnen müssen wäre ein Beispiel hierfür.

2.3 Den Dokumentendurchlauf für jeden Empfänger definieren

Dabei definieren Sie im Webbrowser welche Aktionen jeder Empfänger zu vervollständigen hat, um ihren/seinen Teil der Transaktion abzuschließen. Dies kann das Ausfüllen eines Formularfeldes, Hinzufügen eines Anhangs oder Unterzeichnen eines Unterschriftenfeldes sein. Alternativ können Sie diese Aktionen auch einfach automatisch durch externe Applikationen über API-Aufrufe steuern oder Textmarker zur Markierung von Unterschriftenfeldern verwenden.

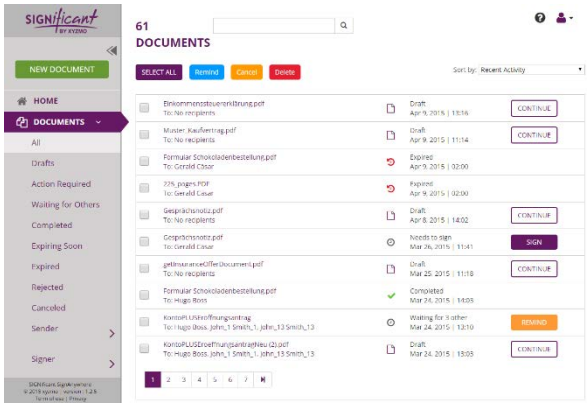
2.4 Erinnerungen und Alarme

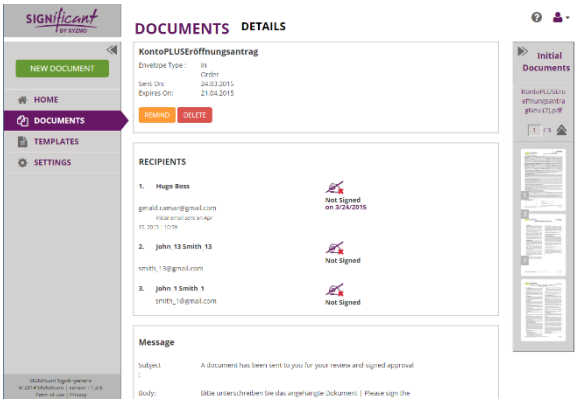


Mit Hilfe von Erinnerungen können Sie Regeln definieren um Ihre Empfänger daran zu erinnern, dass noch Unterschriften offen sind und dass Dokumente ablaufen, wenn sie nicht bis zu einem gewissen Zeitpunkt unterzeichnet wurden. Durch die Verwendung von Alarmen werden Sie informiert werden wenn ein bestimmtes Dokument noch nicht unterschrieben wurde oder ein Empfänger eine Unterschrift ablehnt.

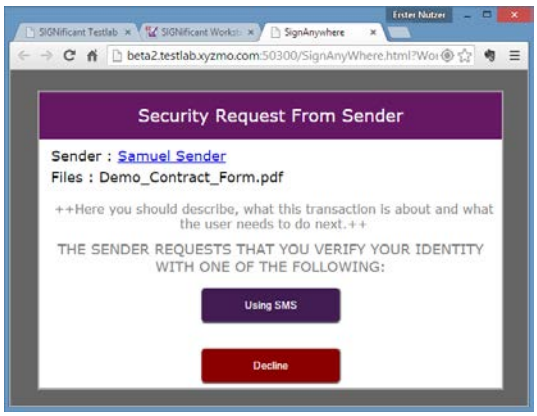
2.5 Dashboards

Dashboard Ansichten sind wichtig um einen kurzen Überblick über den Status von Ihren Unterschriftenmappen zu bekommen. Gute Dashboards bieten nicht nur einen Überblick, sondern erlauben auch ein schnelles Durchsuchen und Bearbeiten der gewünschten Bereiche.





3 Authentifizierungsmethoden



Bei einer Onlinetransaktion kommt dem Feststellen der Identität des Unterzeichners bei der Beweisführung eine entscheidende Rolle zu. Je nach Wichtigkeit der Transaktion bieten sich unterschiedliche Möglichkeiten an, wie z.B.:

- Das Faktum, dass das Email, das mit dem Link zu den Dokumenten dem Unterzeichner zugesandt wurde, ausreicht
- Der Empfänger muss einen Zugangscode eingeben, den er über einen anderen Weg erhalten hat
- Sie nutzen bestehende Verfahren, die sie schon einsetzen oder der Empfänger bekommt den Link ohnedies nur in einem geschützten Bereich, wo er sich vorher anmelden musste
- Der Empfänger muss sich zusätzlich mit Facebook und Co. authentifizieren

- Der Empfänger bekommt eine einmalige PIN auf eine vorher hinterlegte Mobiltelefonnummer zugesandt und muss diese in einem bestimmten Zeitlimit eingeben
- Authentifizierung mit nationalen Personalausweisen oder Reisepässen
- Authentifizierung und Signatur mit digitalen Zertifikaten von Drittanbietern

Wenn Sie die ausgeführten Authentifikationen zudem in einem Protokoll dokumentieren, können Sie die Beweislast erhöhen, da Sie nachweisen können, dass nur der zuvor identifizierte Benutzer das bestimmte Dokument unterzeichnen konnte.

3.1 E-Mail-Authentifizierung

Diese Vorgehensweise ist in der Regel für HTML5 Unterschriften in B2B-Szenarien ausreichend und bei Szenarien mit Konsumenten gut für Dokumente geeignet, die nicht kritisch sind und bei denen Sie es dem Unterzeichner so einfach wie möglich machen möchten. Sie senden den Link zum Dokument in den Posteingang des Empfängers und eine weitere Authentifizierung ist nicht nötig. Im Streitfall können Sie beweisen, dass Sie das Dokument an eine bestimmte E-Mail-Adresse verschickt haben und haben oft auch die IP-Adresse des Computers und die Geolocation, falls der Empfänger dies nicht ausdrücklich blockiert hat.

Alle folgenden Authentifizierungsmethoden beginnen mit diesem Szenario und fügen dem zusätzliche Authentifizierungsschritte hinzu. Obwohl möglicherweise nicht ganz so eindeutig einem Unterzeichner zuordenbar wie eine biometrische Unterschrift, bringen Online-Unterschriften bei einem Streitfall genug Beweiskraft für viele Anwendungsfälle. Mit strengeren Methoden die den Empfänger zweifelsfrei identifizieren lässt sich dann auch eine fortgeschrittene elektronische Signatur umsetzen. Grundsätzlich lässt sich das auch bis zur qualifizierten elektronischen Signatur (QES) weiter treiben, was allerdings letztlich den potentiellen Nutzerkreis dann stark einschränkt. Ein Überblick wird in den nächsten Kapiteln gegeben.

3.2 Empfänger müssen einen Zugangscode eingeben

Zusätzlich zur E-Mail Authentifizierung können Sie den Empfänger mit einer Sicherheitsabfrage konfrontieren und eine Codeeingabe verlangen, damit dieser Zugang zu den Dokumenten bekommt um diese zu lesen und zu unterzeichnen. Wird der Zugriffscode korrekt eingegeben, wird der Empfänger durch den normalen Unterschriftenprozess geführt. Der Zugriffscode wird aus Sicherheitsgründen nicht zusammen mit dem Link in derselben E-Mail versendet. Normalerweise wird der Code auch nicht per E-Mail verschickt, sondern über einen anderen Kanal kommuniziert (zum Beispiel über das Telefon). Damit ein Code über einen längeren Zeitraum funktioniert, können Sie sich entscheiden, in einem getrennten Prozess einen bestimmten länger gültigen Zugangscode beidseitig zu vereinbaren.

Der Vorteil im Fall eines Rechtsstreites: Der Absender kann nachweisen, dass der Unterzeichner Zugriff auf den Zugangscode gehabt haben muss und das Dokument nur so unterschrieben werden konnte.

3.3 Einsatz bestehender Authentifizierungsmodelle

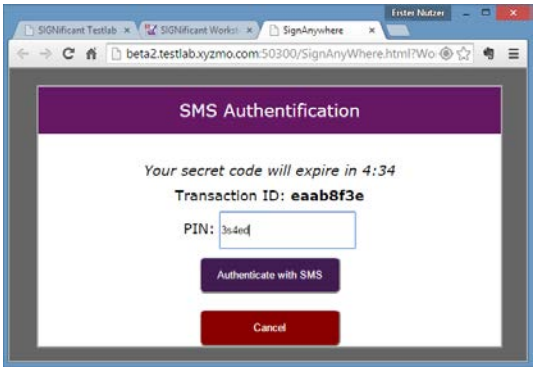
Einige Unternehmen setzen bereits Kundenportale oder andere Software ein, wodurch der Benutzer identifiziert wird. Nehmen wir an, dass sich der Benutzer in einer Bankanwendung befindet, von der aus er all seine Transaktionen verwaltet. Falls der Benutzer ein Dokument unterschreiben muss und sich bereits ordnungsgemäß authentifiziert hat, könnte für eine weitere Authentifizierung keine Notwendigkeit mehr bestehen. Auf jeden Fall muss der Nachweis der Authentifizierung im Protokoll (Audit Trail) enthalten sein, um die Nachweisbarkeit zu gewährleisten.

Eine andere Möglichkeit ist, dass der Empfänger bereits für andere Zwecke eine sichere Authentifizierungsmethode verwendet (zum Beispiel einen Token) und diese Infrastruktur nun mitbenutzt, um ihn für die Unterzeichnung eines Dokuments zu authentifizieren. Wie oben bereits erwähnt, muss der Authentifizierungsprozess im Protokoll des unterschriebenen Dokuments enthalten sein.

3.4 Anmeldung durch die ID sozialer Netzwerke wie z.B. das Facebook-Login

Bei diesem Szenario werden beliebte soziale Netzwerkseiten zur Authentifizierung herangezogen. Die Meisten von ihnen stellen für den Service der Benutzer-Authentifizierung Anwendungen für Drittanbieter bereit. Hierbei hängt die Qualität der Authentifizierung sehr stark von der Qualität des sozialen Netzwerk-Profils ab, das für die Authentifizierung benutzt wird. Zudem wird die Qualität und die Menge der Daten, die Sie über den Benutzer aus dem sozialen Netzwerk zur Protokollierung im Audit Trail erhalten, auf Basisinformationen beschränkt sein.

3.5 Senden einer SMS mit einem einmaligen Passwort



Diese Authentifizierungsmethode nutzt die Gegebenheit, dass Mobiltelefone auf der ganzen Welt für ihre Besitzer eine sehr gute Identifikationsmethode darstellt. Viele Menschen tragen Mobiltelefone den ganzen Tag über bei sich und haben sie zu jeder Zeit griffbereit. Daher ist die Handynummer für den Eigentümer eine eindeutige Identifikationsmöglichkeit. Aus diesem Grund verwenden viele Banken sowie andere Anwendungen diese Methode bereits für Onlinetransaktionen.

Zusätzliche Sicherheit entsteht, wenn das Einmal-Passwort zeitlich begrenzt ist und der Empfänger es z.B. innerhalb der nächsten fünf Minuten nach Erhalt eingeben muss.

Eine weitere Überlegung ist, ob der Transaktionscode nur für eine Unterschrift oder für den gesamten Vorgang gültig sein soll.

Darüber hinaus ist es empfehlenswert, in der SMS, die an den Empfänger zusammen mit dem einmaligen Transaktionscode geschickt wird, eine eindeutige Kennung für die Transaktion einzuschließen. Diese eindeutige Kennung sollte auch im Sicherheitsdialog angezeigt werden, bei dem der Empfänger den Transaktionscode eingeben muss, was es

ihm erlaubt, den Transaktionscode zu überprüfen und sich zu versichern, dass dieser tatsächlich für diese Transaktion und nicht für eine andere bestimmt ist.

All diese Ansätze müssen durch ein entsprechendes Protokoll unterstützt werden, das im Streitfall in der Lage ist zu beweisen, was genau geschehen ist.

Es lohnt sich darüber nachzudenken, wie der Versender die Einstellung für den Transaktionscode handhaben und definieren kann. Es gibt drei wesentliche Szenarien dafür:

1. Der Empfänger hat die Möglichkeit, seine Handynummer selbst einzugeben. Dies ist für Sender und Empfänger sehr praktisch, aber öffnet dem Empfänger eine Tür zum potentiellen Missbrauch.
2. Der Mitarbeiter beim Versender definiert im Vorfeld, welche Handynummer benutzt werden muss und der Empfänger kann das nicht ändern. Dieses Szenario ist sehr häufig, da es dem Verfahren etliches an Sicherheit hinzufügt.
3. Schließlich gibt es Szenarien, in denen beide Parteien – also Empfänger und Mitarbeiter beim Versender – keine Möglichkeit haben sollten, die Mobilnummer für den Empfänger zu definieren oder zu ändern und diese oft nicht einmal sehen dürfen. In diesem Szenario kann der Mitarbeiter den Empfänger nur aus einer Liste auswählen. Die Handynummern sind an einem zentralen Ort gespeichert und können vom Mitarbeiter nicht eingestellt werden. Dies kann mit einem vorgeschalteten Prozess noch einen Schritt weiter gehen, bei dem der Empfänger zum Beispiel bei einem Besuch in einer Filiale schriftlich sein Einverständnis gibt, dass in Zukunft ein Transaktionscode, der an die von ihm definierte Handynummer geschickt wurde, äquivalent für seine Unterschrift verwendet werden kann.

Manche Länder weisen einer ordnungsgemäßen Umsetzung dieser Methode — in Verbindung mit auf einem Zertifikat basierenden Signaturen (siehe Kapitel 0) den gleichen Wert zu, wie einer handschriftlichen Originalunterschrift; ein Beispiel dafür ist die „Handysignatur“ in Österreich.

3.6 Authentifizierung mit nationalen Personalausweisen oder Reisepässen

Viele Länder statten ihre Bürger mit elektronischen ID-Karten (eID) aus, die maschinenlesbar sind, so wie es von der International Civil Aviation Organisation (ICAO) festgelegt worden ist. In Europa basieren die meisten ID-Karten auf der European Citizen Card (ECC) Spezifikation und haben die persönlichen Daten des Karteninhabers (zum Beispiel Name, Datum und Geburtsort, Staatsangehörigkeit) nicht nur auf der Karte aufgedruckt, sondern auch auf dem integrierten Chip gespeichert. Ausweisinhaber können diese eID-Funktion verwenden, um über das Internet Transaktionen mit öffentlichen Stellen und privaten Unternehmen durchzuführen.

Zum Beispiel ermöglicht der neue Personalausweis (nPA) Deutschlands mittels eines Passworts den authentifizierten Verbindungsaufbau (PACE) und die Zugriffskontrolle (Extended Access Control – EAC) auf die gespeicherten personenbezogenen Daten, die sich auf der Karte befinden. Das PACE-Protokoll führt mit einer Persönlichen Identifikations-Nummer (PIN) die Benutzerauthentifizierung durch und stellt zum Schutz

der Kommunikation über die kontaktlose Schnittstelle eine sichere Verbindung zwischen der ID-Karte und dem Kartenlesegerät her. Durch Eingabe der PIN erhält der Karteninhaber seine/ihre Berechtigung zum Zugriff auf die Karte.

3.7 Authentifizierung und Signatur mit digitalen Zertifikaten von Drittanbietern

In den Fällen, in denen der Empfänger bereits eine Public Key-Infrastruktur (PKI) mit persönlichen Zertifikaten für die digitale Signatur hat (zum Beispiel auf Chipcards, USB-Token, als Softwarezertifikat am Computer), kann dieses Zertifikat nicht nur zur Authentifizierung des Unterzeichners verwendet werden, sondern auch zum digitalen Unterschreiben eines Dokuments. Damit kann eine existierende PKI-Infrastruktur, die meist für andere Zwecke vorhanden ist, für Unterschriftsverfahren wiederverwendet werden. So können Sie den Nutzen aus bereits vorhandenen Zertifikaten ziehen um Dokumente digital zu signieren.

Einige nationale ID-Karten bieten auch direkte Funktionen für das Ausführen einer qualifizierten elektronischen Signatur (QES). Obwohl dies theoretisch eine gute Möglichkeit für die Wiederverwendung der bereits vorhandenen Infrastruktur ist, hat sich in der Praxis gezeigt, dass die Marktpenetration und die Akzeptanz durch die Anwender ein Problem ist (siehe Kapitel 0).

4 E-Signatur-Technologie

Es gibt drei unterschiedliche Technologien um ein Dokument elektronisch zu unterschreiben. Die Technologien unterscheiden sich indem

- die erfasste handgeschriebene Unterschrift einer Person forensisch identifizierbar ist (auch bekannt als biometrische Unterschrift)
- die eingebettete „HTML5 Unterschrift“ nur ein Platzhalter (Stempelabdruck) ist, der zusätzliche Methoden zur Authentifizierung und ein Protokoll (Audit Trail) nötig macht, um rechtlich verbindlich zu sein
- die Unterschrift mit einem persönlichen digitalen Signatur-Zertifikat erfolgt.

Die wichtigste Frage bei der Erfassung von handschriftlichen Unterschriften ist, ob die erfassten Unterschriftendaten forensisch auswertbar sind. Man kann sagen, dass durch die Verwendung eines Stylus oder eines ohnedies vom Gerätehersteller vorhandenen originalen Eingabestifts und bei sachgemäßer Implementierung der Unterschriftenerfassungssoftware, das Ergebnis forensisch identifizierbare Unterschriften sind.

In anderen Szenarien – wie etwa bei der Unterzeichnung mit einer Maus, einem Touchpad oder dem Finger (oder wo die erforderliche Erfassungssoftware und/oder die Hardware nicht vorhanden ist) – ist die Unterschrift forensisch kaum identifizierbar. Diese Kategorie ist das, was wir eine „HTML5 Unterschrift“ nennen.

Zertifikat-basierte Unterschriften erfordern im Gegensatz dazu eine PKI-Infrastruktur. Während sie eine gut gewählte Technologie für elektronische Unterschriften innerhalb eines Unternehmens sein können (wenn eine PKI-Infrastruktur verfügbar ist), können sie

in jedem anderen Szenario egal ob B2C oder B2B, nur eine begrenzte Anwendbarkeit bieten.

Unabhängig davon, welche dieser drei Technologien verwendet wird, sollte das unterschriebene Dokument zum Schutz seiner Integrität pro Unterschrift immer mit einer digitalen Signatur versiegelt werden.

4.1 HTML5 Unterschriften

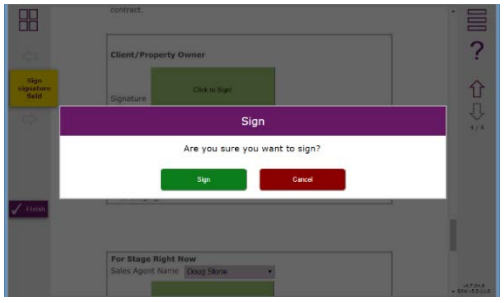
Der große Vorteil von HTML5 Unterschriften besteht darin, dass Unterzeichner keine zusätzliche Software auf ihren Geräten installieren müssen. Sie funktionieren einfach auf jedem HTML5-fähigen Gerät. Abhängig von der Authentifizierungsmethode (siehe Kapitel 3), erfordern sie auch keine komplizierten Abläufe, so dass sie für B2C und B2B-Szenarien gut geeignet sind.

Jedoch hängt der gesamte Prozess vollständig von der richtigen Authentifizierung des Empfängers (siehe Kapitel 3) und der Protokollierung aller Benutzerinteraktionen mit den Dokumenten ab. Wenn alles ordnungsgemäß dokumentiert ist, bieten HTML5 Unterschriften eine zuverlässige Beweiskraft. Ausgehend von der gewählten Methode können diese Unterschriften den fortgeschrittenen elektronischen Signaturstandard erfüllen[1], womit die Beweiskraft einer forensisch identifizierbaren, biometrischen Unterschrift (siehe Kapitel 4.3) gleicht.

Darüber hinaus verschiebt ein ordnungsgemäß aufgesetztes Protokoll, das leicht zu lesen ist und auch von Richtern oder Anwälten, ohne einen Sachverständigen zu Rate zu ziehen, verstanden wird, meistens die Beweislast auf Seiten des Unterzeichners. Dies ist ein Vorteil gegenüber biometrischen Unterschriften, wenn diese nicht in Echtzeit verifiziert wurden.

Die Frage, wie eine HTML5-Unterschrift am Dokument angezeigt wird, ist meist eher eine Frage des Nutzens für den Unterzeichner und weniger eine rechtliche Frage. Möglicherweise kann man argumentieren, dass, wenn der Unterzeichner nicht nur einen Dialog bestätigt, sondern auch das Bild der Unterschrift selbst wählt oder erstellt hat – zum Beispiel weil er seinen Namen als Basis für das Bild eintippt – das mehr Beweiskraft im Vergleich zu Methoden hat, bei denen das nicht der Fall ist.

4.1.1 Click-2-Sign

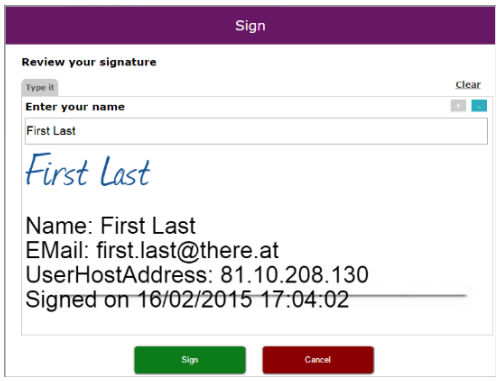


Ist das typische Äquivalent zum Stempelabdruck in der Papierwelt. Die passende elektronische Unterschriftensoftware lässt Sie die Elemente des Stempelabdruckes definieren. Abhängig vom Anwendungsfall können Sie zum Beispiel den Namen des Unterzeichners anzeigen oder die IP-Adresse sowie geografische oder andere Informationen.

[1] Voithofer, Paul – Gutachterliche Stellungnahme SignAnyhwere [2015]

Eventuell möchten Sie einen Text hinzufügen, der explizit besagt, dass dies eine digitale Unterschrift und keine manuell-handschriftliche ist.

4.1.2 Type-2-Sign (Tippen des Namens)



Diese Methode ermöglicht dem Unterzeichner seinen Namen unter Verwendung von verschiedenen Schrifttypen, die wie handschriftliche Unterschriften aussehen, zu erstellen. Der Benutzer kann dabei oft die Schriftart und Schriftgröße auswählen.

Ähnlich wie beim Click-2-Sign, enthält die Type-2-Sign Unterschrift auch zusätzliche Informationen zum Unterzeichner, wie seinen Namen, E-Mail oder IP-Adresse und Datum und Zeit des Unterzeichnens.

4.1.3 Draw-2-Sign (Zeichnen des Namens mit dem Finger, der Maus oder dem Stylus)

Der Unterzeichner „zeichnet“ seine Unterschrift wie er es vom Prozess auf Papier gewohnt ist. Sie gleicht einer biometrischen Unterschriftenerfassung, jedoch sind die meisten Menschen nicht fähig ihre Unterschrift mit dem Finger oder einer Maus zu zeichnen. Aber auch wenn ein Stylus verwendet wird ist die Unterschrift nicht forensisch identifizierbar, da HTM5-basierte Lösungen keine biometrischen Daten verlässlich erfassen und verschlüsseln können sondern nur ein Abbild. Deshalb ist auch hierfür eine zusätzliche Authentifikation nötig.

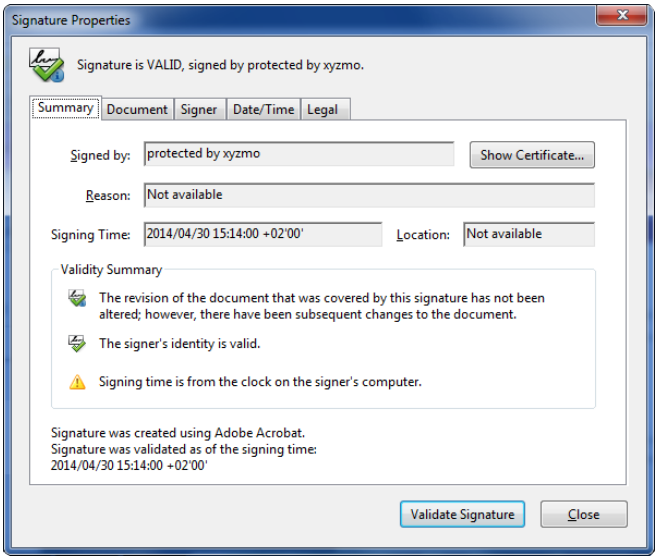
4.2 Zertifikatsbasierte persönliche Unterschriften

Einige Branchen und Länder verlangen zertifikatsbasierte Unterschriften. In diesem Fall müssen Unternehmen von ihren Unterzeichnern digitale Unterschriften mit persönlichen Unterschriftenzertifikaten verlangen.

Der Prozess ist dem Standardverfahren sehr ähnlich:

- Erstellen Sie eine neue Unterschriftenmappe und fügen Sie Dokumente hinzu.
- Fügen Sie die Empfänger wie gewohnt hinzu und verlangen jedoch von einigen Empfängern digitale Zertifikate.
- Fügen Sie alle anderen Optionen bei der Authentifikation wie gewohnt hinzu.
- Schließen Sie die Konfigurierung der Unterschriftenmappe ab und versenden Sie diese wie immer.
- Der Empfänger öffnet die Unterschriftenmappe und fügt wie bei allen anderen Methoden in allen erforderlichen Feldern Informationen ein.

- Wenn der Unterzeichner eine Unterschrift leistet, dann unterschreibt er/sie das Dokument digital mit seinem/ihrem persönlichen Signaturzertifikat, welches er/sie besitzen muss (z.B. auf einer Smartcard oder Token) und auf das nur er/sie mittels Passwort Zugriff hat
- Der Unterzeichner wird gebeten die Informationen zu überprüfen und zu bestätigen, eventuell beinhalten diese den Grund für die Unterschrift und seine/ihre Unternehmensdetails und den Ort der Unterschrift.



Wenn diese Schritte abgeschlossen sind, kann jedermann die digitale Unterschrift in einem geeigneten PDF-Reader überprüfen.

Wie bei allen Technologien finden Kriminelle und Betrüger Wege um Prozesse zu umgehen. Im Falle eines persönlichen digitalen Zertifikats z.B. durch Manipulation des Kartenlesegerätes. Obwohl somit auch diese Methode nicht zweifelsfrei ist wird in einigen Ländern trotzdem der höchste rechtliche Wert einer Unterschrift – der dem einer handgeschriebenen Unterschrift auf Papier gleichgestellt ist – nur mit zertifikatsbasierten Ansätzen erreicht. Oftmals sind genehmigte Chipkarten und Kartenlesegeräte erforderlich, was die Angelegenheit deutlich verteuert und verkompliziert. Dies gilt insbesondere für die für die „Qualifizierte Elektronische Unterschrift“ (QES) in der Europäischen Union. Einige Mitgliedsstaaten bieten sogar eine Infrastruktur, um QES Funktionen auf ihren nationalen Personalausweisen zu aktivieren (zum Beispiel Deutschland mit seinen nPA, siehe Kapitel 3.6 und 3.7). Karteneigentümer müssen diese Funktionen jedoch extra aktivieren und dafür wiederkehrend bezahlen. Zudem benötigen sie ein Kartenlesegerät, um die Funktionen nutzen zu können. All diese Hürden münden letztendlich in einer äußerst niedrigen Marktdurchdringung, was die Verwendung in B2C Szenarios problematisch macht.

4.3 Forensisch identifizierbare Unterschriften (biometrische Unterschrift)

Eine forensisch identifizierbare Unterschrift ist viel mehr als nur ein digitalisiertes Abbild einer handgeschriebenen Unterschrift. Sie erfordert die Aufzeichnung einer handgeschriebenen Unterschrift einer Person mit all seinen Eigenschaften, also zum Beispiel Beschleunigung, Geschwindigkeit und Schreibrhythmus. Diese dynamischen Parameter sind für jeden einzelnen Menschen einzigartig und können von Fälschern nicht reproduziert werden. Deswegen ist eine derart digital aufgezeichnete Unterschrift forensisch identifizierbar und weitaus sicherer als nur das Abbild einer Unterschrift alleine.

Wenn jemand behauptet „Ich habe das nicht unterschrieben“ kann anschließend ein Gutachter jederzeit eine umfangreiche Unterschriftenverifizierung (unter Verwendung spezieller Software) durchführen, um ein aussagekräftiges Ergebnis über die Echtheit der Unterschrift zu erhalten, genauso wie es der Gutachter mit einer Unterschrift auf Papier machen würde. Daher erfüllt[2] die biometrische Unterschrift die fortgeschrittene elektronische Signatur und hat sich, wenn anwendbar, de facto zum Branchenstandard entwickelt.

Einige Lösungen bieten zusätzlich eine Unterschriftenverifikation die die Unterschrift in Echtzeit mit einer vorgefertigten Unterschriftenprofil-Datenbank vergleicht. Dies ermöglicht nicht nur äußerst sichere Transaktionen, sondern bietet im Streitfall auch ein aussagekräftiges Protokoll (Audit Trail), das die Beweislast auf den Unterzeichner verschiebt.

Wieso also die biometrischen Signaturen nicht für jeden Anwendungsfall verwenden?

Das Problem ist, dass die zuverlässige Erfassung solcher Unterschriften eine Echtzeitumgebung auf dem Computer, dem Tablet oder dem Smartphone verlangt, um die dynamischen Eigenschaften der Unterschrift zu erfassen. Da ein HTML5-Ansatz alleine dies nicht bieten kann, wird eine native lokale Softwarekomponente oder ein Java Applet bzw. ein Browser-Plug-In in einer Webapplikation benötigt. Wesentlich bei der Erfassung von biometrischen Unterschriften ist außerdem eine sichere Verschlüsselung, welche wiederrum nicht mit einem HTML5-Ansatz geboten werden kann, sondern ebenfalls eine lokale Softwarekomponente benötigt, da der Source Code der Erfassungslogik bei JavaScript für den Client immer sichtbar ist und so leicht, mit Hilfe eines injizierten JavaScript Codes, durch einen unsicheren Source Code ersetzt werden kann.

Da jedoch in einigen Szenarien vom Unterzeichner nicht verlangt werden kann eine lokale Unterschriftenerfassungskomponente zu installieren, werden für solche Fälle häufig HTML5-basierte Unterschriftenansätze verwendet. Trotzdem ist es wenn möglich für sehr wichtige oder hoch riskante Transaktionen von Vorteil eine handgeschriebene biometrische Unterschrift zu verwenden.

4.3.1 Erfassungsgeräte für biometrische Unterschriften

Einerseits gibt es traditionelle Unterschriftenpads und Stiftbildschirme, andererseits eine breite Auswahl an Smartphones und Tablets, die das Schreiben mit speziellen Stiften unterstützen. Zudem gibt es spezielle Stifte im Handel, die eine sehr gute Unterschriftenerfassung auf Geräten die keinen Stift mitgeliefert bekommen, wie das iPad oder iPhone, ermöglichen. Einige dieser speziellen Stifte bieten Druckwertmessung und manche sogar eine Handballenauflageerkennung. Meist sind diese jedoch nicht so

[2] Voithofer, Paul – Sachverständigengutachten SIGNificant Produkte [2012] & Caspart, Wolfgang – Graphologisches Gutachten [2012]

ausgereift wie mit Originalstiften. Falls kein Stift mitgeliefert wird kann ein kapazitiver Stylus, wie unten angeführt, verwendet werden.

a) Stylus

Die Unterzeichnung mit einem kapazitiven Eingabestift (Stylus) gibt Unterzeichnern das Gefühl mit einem echten Stift zu unterschreiben. Es gibt ein paar Schwächen verglichen mit einem echten Kugelschreiber, was typischerweise in größeren Unterschriften resultiert, die mit einer langsameren Geschwindigkeit geschrieben sind. Im Gegensatz zum Unterzeichnen per Finger ist das erfasste Schriftbild und der Schreibrhythmus allerdings konsistent und der Unterschrift auf Papier ähnlich genug, dass dieses Verfahren für ein Gerichtsgutachten herangezogen werden kann. Zudem erfolgt der Vergleich immer wenn möglich mit Vergleichsunterschriften die in ähnlichen Situationen mit ähnlicher Technik aufgenommen wurden – also präferierter Weise mit Unterschriften die auch mit Hilfe des gleichen Stylus erstellt wurden.

b) Originalstift

Originalstifte bieten im Vergleich zu einem Stylus typischerweise ein Unterschriftenerlebnis, das dem Unterzeichnungsvorgang auf Papier am nächsten kommt.

Gründe dafür sind:

- Eine dünne Schreibspitze wie bei einem Kugelschreiber, die es erlaubt, in kleinen Buchstaben zu unterschreiben.
- Handballenauflageschutz, sodass Sie den Bildschirm während der Unterzeichnung berühren können, ohne die Unterschriften-aufzeichnung zu stören.

Darüber hinaus bieten Originalstifte eine bessere Datenqualität weil:

- Sie eine höhere Datenrate bieten, die es erlaubt, alle Aspekte auch bei sehr schneller Unterschriften zu erfassen.
- Viele erfassen auch die Druckdaten, was für ein Gutachten nicht zwingend nötig wäre. Dennoch erhöhen die erfassten Druckdaten die Sicherheit und Beweiskraft.

c) Fineline-Stylus

Ein Fineline-Stylus ist ein Zusatzprodukt für Geräte, die nicht von Haus aus mit einem Stift ausgestattet sind, wie zum Beispiel das iPad. Er ist ebenfalls ein kapazitiver Eingabestift, aber einer, der mit Zusatztechnologie eine wesentlich feinere Unterschrift ermöglicht und manchmal auch Handballenauflageschutz und Druckaufzeichnung bietet. Noch ist das Schreiberlebnis nicht mit

jenem unter Verwendung eines Originalstiftes gleich, jedoch um einiges besser als mit einem einfachen Stylus. Die Technologie verbessert sich stetig und es kommen immer bessere Hochpräzisionsstifte auf den Markt.

4.3.2 Verwendung eines Smartphones als Signaturpad

Dieses Szenario ist perfekt für Geschäftsfälle, bei denen Sie biometrische Unterschriften erfassen, aber keine Signaturpads, Stiftbildschirme oder Tablets bereitstellen möchten.

Das typische Verfahren ist:

- Sie wollen am Computerbildschirm im Browser Dokumente ansehen und ev. Formularfelder ausfüllen, sowie Anhänge hinzufügen – vielleicht zusammen mit einem Kunden, Mitarbeiter oder Geschäftspartner – und dann ein Smartphone als Unterschriftenerfassungsgerät verwenden.
- Eine native Anwendung verwandelt das Smartphone in ein Unterschriftenerfassungsgerät. Diese Anwendung sollte auf den gängigsten 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. Dies geschieht mit Hilfe eines Tokens (der einfach über die Kamera eines Smartphones mit Hilfe eines, in der nativen Unterschriftenapplikation integrierten, QR-Code Readers eingelesen werden kann).
- Die Unterschriftenapplikation zeigt den Unterschriftenerfassungsvorgang, bei dem das Dokument visuell im Hintergrund angezeigt wird.

- Die Unterschrift wird am Smartphone erfasst. Es wird empfohlen, Smartphones mit Originalstift oder einem Hochpräzisionsstift, 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 eine gesicherte Verbindung an den Server übertragen und in das Dokument eingebettet.

5 Plattform Aspekte

Viele wichtige Anforderungen an eine Online-Unterschriftenlösung sind die gleichen wie für andere Anwendungsfälle (zum Beispiel POS oder mobile Anwendung). Diese können Sie im Whitepaper „Dokumente unterschreiben. Überall. Jederzeit.“ nachlesen.

Folgende Aspekte werden dort erläutert:

- Sicherheit
- Langzeitarchivierung
- Prozessnachweis (inkl. Protokolle)
- Bereitstellungsmethoden
- Enterprise Integration
- Standard versus proprietäre Ansätze.

Um die Aspekte nicht wiederholt anzuführen, empfehlen wir diese im oben genannten Whitepaper nachzuschlagen.

6 SIGNificant-Referenzen

SIGNificant ist eine elektronische Unterschriften-Plattform für Unternehmen, die es Ihnen ermöglicht zu unterschreibende Dokumente zu versenden oder einfach selbst online zu signieren. SIGNificant stellt Ihnen die Benutzeroberfläche und die Werkzeuge, die nötig sind, um den optimalen elektronischen Unterschriftenprozess und das optimale Nutzererlebnis zu definieren, zur Verfügung.

Egal ob für HTML5-Unterschriften, biometrische Unterschriften oder digitale Signaturen mit persönlichem Zertifikat. Die verschiedenen Bausteine der Plattform machen es Ihnen möglich, die beste Kombination von Unterschriftenaufzeichnung und Authentifizierung des Unterzeichners zu wählen. Dabei ist es egal welche Unterschriftenerfassungsgeräte der Empfänger verwendet.

Um besser zu illustrieren, wie SIGNificant in verschiedensten Branchen, für spezielle Anwendungsfälle im online Szenario angewendet werden kann, zeigt das folgende Kapitel eine reale Fallstudie eines Kunden der SIGNificant für online Unterschriften in seinen End-to-end Geschäftsprozesse implementiert hat.

6.1 The Phone House Niederlande

Anwendungsfälle:

- Digitales Unterzeichnen von Versicherungsverträgen für Mobiltelefone, online im Webbrowser und auf jedem HTML5 Gerät.

Bereitgestellte Produkte:

- Unterschriftenapplikation: SIGNificant Server mit der „SignAnywhere“ Applikation

End-to-end Geschäftsprozess:

1. Der Kunde wählt den gewünschten Versicherungsvertrag für sein Mobiltelefon online über die Website von The Phone House.
2. Das Back-end System von The Phone House erstellt automatisch einen Versicherungsvertrag zum Unterschreiben und sendet einen Link an den Kunden mit dem er diesen online anzeigen und unterschreiben kann.
3. Der Kunde öffnet den Versicherungsvertrag in einem Browser der HTML5 unterstützt und unterzeichnet, mittels Type-2-Sign oder Draw-2-Sign, zwei Unterschriftenfelder.
4. Das unterzeichnete Dokument und das Protokoll sind sicher im Archievierungssystem von The Phone House abgelegt.
5. Der Kunde wird online über die Ergebnisse der Transaktion informiert und hat direkt im Webbrowser Zugang zu einer Kopie des unterzeichneten Versicherungsvertrages.