

Vollständig digitale Geschäftsprozesse mit Adobe-Lösungen für elektronische und digitale Signaturen

Adobe Sign bietet eine skalierbare Lösung für Signaturen, mit der Sie nationale und internationale Gesetze und Vorschriften zuverlässig einhalten.

Whitepaper

August 2018

INHALT

3	Digitale Transformation
4	Elektronische und digitale Signaturen: Was ist der Unterschied?
5	Gesetzgebung zu elektronischen Unterschriften
6	Auswahl der richtigen Methode
8	Eine Lösung. Mehrere Optionen.
9	Von Adobe Sign unterstützte Signaturarten
10	Adobe – die Nummer 1 für sichere digitale Dokumente
11	Ressourcen

Digitale Transformation

Organisationen weltweit setzen digitale Technologien ein, um ihre Geschäftsabläufe zu optimieren. Ihr Ziel: mehr Agilität und Effizienz, weniger Kosten und herausragende Kundenerlebnisse. Diese Transformation lässt sich vor allem durch die Unterstützung elektronischer und digitaler Signaturen beschleunigen. Mitarbeiter verlieren viel Zeit damit, Genehmigungen und händische Unterschriften einzuholen und anschließend die entsprechenden Dokumente zu drucken, zu scannen, zu faxen oder per E-Mail zu versenden. Die daraus resultierenden Verzögerungen sind für Kunden, Geschäftspartner und Mitarbeiter gleichermaßen frustrierend und werfen letztendlich ein ungünstiges Licht auf das Unternehmen.

Es ist daher kaum verwunderlich, dass immer mehr Organisationen auf elektronische und [digitale Signaturen](#) umsteigen. Führende Unternehmen in jeder Branche und Region – darunter KLM, Groupon, Jaguar Land Rover, Ricoh, Unum und LeasePlan Corporation – sind inzwischen in der Lage, rechtskräftige und sichere Unterschriften schnell auf elektronischem Weg einzuholen. Mit beeindruckenden Ergebnissen: Ricoh konnte

die Zeit bis zum Abschluss eines Kaufvertrags um fünf Tage verkürzen. LeasePlan hat die durchschnittliche Verarbeitungszeit für Verträge von 23,5 Tagen auf knapp über 4 Tage reduziert und dadurch den zeitlichen Aufwand um 83 % gesenkt.

Die große Frage, die sich Organisationen heute stellen müssen, ist nicht, **ob elektronische Unterschriften** eingeführt werden sollen, sondern **wie** – besonders, da die Compliance-Maßnahmen immer wieder an die aktuellen Anforderungen einzelner Regionen und Branchen angepasst werden müssen. Auch wenn die Begriffe „elektronische Signatur“ (oder „elektronische Unterschrift“) und „digitale Signatur“ ähnlich klingen, beschreiben sie jeweils ein anderes Verfahren zum Unterzeichnen von Dokumenten, u. a. bedingt durch die länderspezifischen Gesetze und Vorschriften für elektronische Unterschriften. Um die richtige Wahl für Ihre Organisation und Ihre Prozesse zu treffen, sollten Sie sich über diese Unterschiede, die Rechtslage in Ihrem Land und infrage kommende, vertrauenswürdige Dienstleistungspartner informieren.

Dieses Whitepaper erläutert die Merkmale von elektronischen und digitalen Signaturen und zeigt auf, wie Sie mit Adobe Sign beide Methoden nutzen können – einzeln oder in Kombination. [Adobe Sign](#) ist eine Lösung von Adobe Document Cloud zur lückenlosen Verwaltung von Unterschriftsprozessen, lässt sich mit bestehenden Geschäftsabläufen integrieren und unterstützt Sie weltweit bei der Erfüllung regionaler und branchenspezifischer Vorschriften. Mit mehr als 20 Jahren Erfahrung in der Entwicklung und Optimierung von PDF- und Signaturtechnologien ist Adobe ideal aufgestellt, um Sie bei der Einrichtung von Unterschriftsprozessen zu unterstützen, die geltenden Gesetzen und Bestimmungen entsprechen.

„Gerichte akzeptieren jetzt Lösungen für fortgeschrittene elektronische Signaturen wie Adobe Sign, die hohe Standards in puncto Sicherheit und Datenschutz gewährleisten. Wir haben gemeinsam mit Adobe eine Reihe von Best Practices in diesem Bereich entwickelt.“

BART VAN DEN HEUVEL
Manager of Corporate Procurement
LeasePlan Corporation

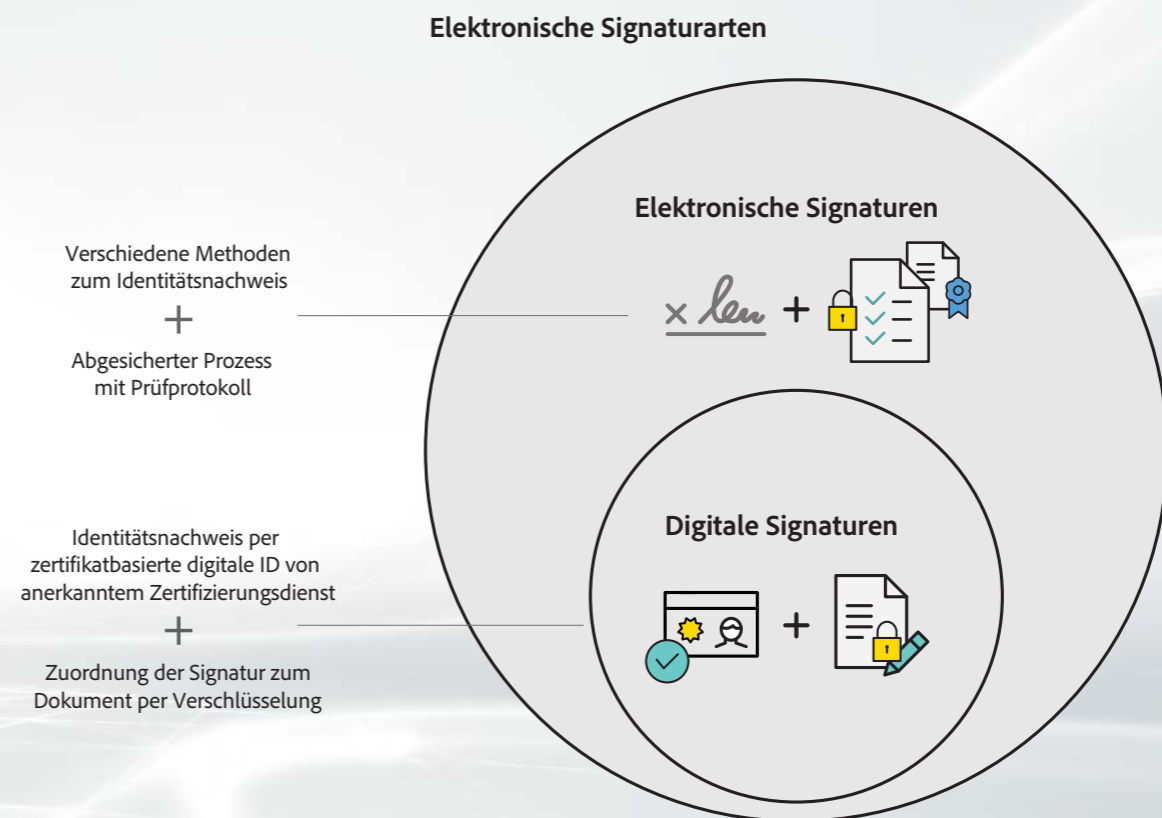
Elektronische und digitale Signaturen: Was ist der Unterschied?

Eine **elektronische Signatur** (*elektronische Unterschrift*) ist ein elektronischer Prozess zum Bekunden der Zustimmung zu einem Vertrag oder Formular.

- Elektronische Signaturen verwenden verschiedene Methoden zur Authentifizierung des Unterzeichners, z. B. E-Mail, Social-ID, Kennwörter oder telefonisch übermittelte PINs. Bei standardmäßigen elektronischen Signaturen kommt die Ein-Faktor-Authentifizierung zum Einsatz, bei erweiterten elektronischen Signaturen die Multi-Faktor-Authentifizierung.
- Elektronische Signaturen weisen die Unterschrift im Rahmen eines abgesicherten Prozesses nach, der oft ein Prüfprotokoll und die endgültige Fassung des Dokuments beinhaltet.

Digitale Signaturen sind eine spezielle Art der elektronischen Unterschrift.

- Digitale Signaturen verwenden eine zertifikatbasierte digitale ID zur Authentifizierung der Identität des Unterzeichners;
- Digitale Signaturen weisen die Unterschrift nach, indem die Signatur verschlüsselt an das Dokument gebunden wird – die Validierung erfolgt durch anerkannte Zertifizierungsstellen oder Vertrauensdienste.



Gesetzgebung zu elektronischen Unterschriften

Elektronische Signaturen sind in fast allen Industrieländern rechtlich bindend. Auch zahlreiche Schwellenländer sind inzwischen im Begriff, entsprechende Gesetze zu erlassen. Im Jahr 2000 wurde das US-amerikanische Gesetz zu elektronischen Signaturen im globalen und nationalen Handel (ESIGN Act) verabschiedet, das die Verwendung digitaler Signaturen für nahezu alle Zwecke gestattet. In der EU ist seit Juli 2016 die eIDAS-Verordnung in Kraft. Damit wurde für die gesamte Gemeinschaft ein einheitliches Regelwerk für elektronische Identifizierung, Unterschriften, Siegel und Dokumente eingeführt. Weitere Informationen über die Gesetzgebung zu elektronischen Signaturen finden Sie in diesem umfassenden Überblick: [Elektronische Signaturen weltweit: Leitfaden zu Gesetzgebung und Durchsetzbarkeit.](#)

Welche Art von Signatur für Ihr Unternehmen am besten geeignet ist, richtet sich nach der für Sie geltenden Rechtslage, Ihrem Risikoprofil und Ihren geschäftlichen Anforderungen. Die EU und die USA beispielsweise gehen aus juristischer Sicht unterschiedlich mit den beiden Signaturarten um. Die US-amerikanische Gesetzgebung verwendet eine allgemeinere Definition und schreibt keine spezielle Technologie vor. Die eIDAS-Verordnung der EU hingegen unterscheidet zwischen drei verschiedenen Arten von elektronischen Signaturen und verlangt eine digitale Signatur für bestimmte Dokumente. Hinzu kommt, dass einige Branchen wie die Biopharmazie und öffentliche Verwaltung restriktivere Bestimmungen für bestimmte Geschäftsprozesse eingeführt haben, die digitale Signaturen erfordern.

Die internationale Gesetzgebung zu elektronischen Signaturen lässt sich in zwei Kategorien einteilen:

Großzügig – Viele Länder wie die USA, Australien, Neuseeland und Kanada regeln elektronische Unterschriften großzügig, d. h., sie sind mit wenigen Einschränkungen allgemein zulässig und haben denselben Status wie händische Unterschriften.

Mehrstufig – In anderen Ländern ist die Verwendung elektronischer Unterschriften generell zulässig. Einer Signatur mit zertifikatbasierter digitaler ID wird jedoch eine höhere Beweiskraft bei der Authentifizierung des Unterzeichners zugemessen. Zu diesen Ländern zählen die EU, China, Indien und Südkorea. In der EU haben beispielsweise nur Signaturen mit einer digitalen ID von einem qualifizierten Anbieter automatisch denselben Status wie eine händische Unterschrift.

Auswahl der richtigen Methode

Die für Ihr Unternehmen optimale Lösung berücksichtigt die Gesetzgebung und das Risiko, sodass Sie sich mit möglichst geringem Aufwand auf rechtlich einwandfreie und zudem sichere Transaktionen verlassen können. Korrekt konfigurierte Prozesse für elektronische Signaturen lassen sich einfacher implementieren und stellen die Einhaltung von gesetzlichen Vorgaben und Sicherheitsanforderungen für zahlreiche Geschäftsprozesse sicher. Bei digitalen Signaturen sind zwar zusätzliche technische Voraussetzungen zu beachten, aber sie ermöglichen eine erweiterte Form der Authentifizierung, die strikteren Compliance-Vorgaben entspricht. Adobe Sign unterstützt beide Ansätze mit einer flexiblen, skalierbaren Lösung, die Ihnen die Wahl zwischen einer der Methoden oder die Verwendung beider Methoden ermöglicht.

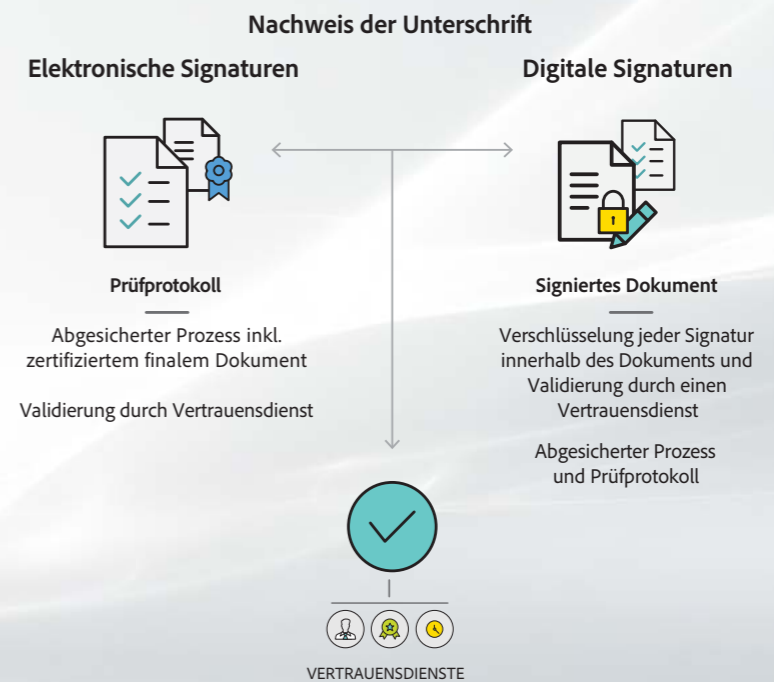
Authentifizierung bei Standardgenehmigungen

Elektronische Unterschriftenprozesse mit Adobe Sign erfüllen Gesetze zu elektronischen Signaturen wie den US-amerikanischen [ESIGN Act](#) und die eIDAS-Verordnung der EU. Durch die Unterstützung für Ein- und Multi-Faktor-Authentifizierung bietet Adobe Sign verschiedene Optionen zur Verifizierung der Identität eines Unterzeichners. Die Standardauthentifizierung erfolgt mittels einer E-Mail-Anfrage an den betreffenden Unterzeichner inkl. einer privaten URL. Diese Methode wird als erste Stufe der Authentifizierung betrachtet, weil die Mehrheit der Unterzeichner alleinigen Zugriff auf ihr E-Mail-Konto hat.

Um die Sicherheit zu erhöhen und Hacker-Angriffen vorzubeugen, können Sie einen weiteren Schritt zur Verifizierung in den Prozess einbinden, bevor der Unterzeichner das Dokument öffnen kann, z. B. die Eingabe einer Social-ID, eines Kennworts, einer telefonisch übermittelten PIN oder die Beantwortung einer Sicherheitsfrage (Knowledge-Based Authentication, KBA)*. Um gesetzliche Bestimmungen noch zuverlässiger einzuhalten, können Sie Prozesse entwickeln, bei denen eine ausdrückliche Zustimmung zur elektronischen Unterschrift erforderlich ist.

Mit Adobe Sign lassen sich Dokumente während des gesamten Prozesses sicher verwalten und nach der Unterzeichnung mit einem manipulationssicheren Siegel speichern, um ihre Integrität zu bestätigen. Jeder wichtige Schritt im Unterzeichnungsprozess wird protokolliert, z. B. der Zeitpunkt, an dem das Dokument gesendet, geöffnet und unterzeichnet wurde, IP-Adresse oder Standort der Unterzeichner sowie die Art der Authentifizierung, die für jeden Unterzeichner oder Prüfer verwendet wurde.

Das Ergebnis wird in einem abgesicherten Prüfprotokoll erfasst. Das unterzeichnete Dokument und das Prüfprotokoll werden an alle Parteien gesendet und sicher bei Adobe Document Cloud gespeichert, um einen eindeutigen und leicht abrufbaren Nachweis der Unterschrift jeder Partei sicherzustellen.



„Mit Adobe Sign beträgt die durchschnittliche Verarbeitungszeit für Kaufverträge 1,3 Stunden. Wenn man bedenkt, dass dieser Prozess mit Papierdokumenten früher mindestens zwei Wochen – und manchmal sogar Monate – gedauert hat, ist dies eine enorme Verbesserung.“

Western Australian Local Government Association (WALGA)

*KBA ist nur in den USA verfügbar.

Authentifizierung bei restriktiveren Anforderungen

Die Prozesse von Adobe Sign für [digitale Signaturen](#) erfüllen strengere Anforderungen, z. B. für fortgeschrittene und qualifizierte elektronische Signaturen gemäß eIDAS-Verordnung, und bieten umfassende Unterstützung für die Zusammenarbeit mit anerkannten Zertifizierungsstellen und Vertrauensdiensten. Darüber hinaus unterstützen sie Geräte zur Erstellung qualifizierter Signaturen, z. B. Chip-Karten, USB-Token oder Cloud-basierte Hardware-Sicherheitsmodule (HSMs).

Dokumente, die mit Adobe Sign digital signiert wurden, enthalten integrierte Nachweise über die Unterschriften aller Beteiligten. Im Unterzeichnungsprozess wird das Zertifikat des Unterzeichners mithilfe des nur ihm zugewiesenen privaten Schlüssels an das Dokument gebunden. Bei der Überprüfung wird aus der Unterschrift der entsprechende öffentliche Schlüssel extrahiert. Er dient dazu, die Identität des Unterzeichners über die anerkannte Zertifizierungsstelle zu authentifizieren und zu bestätigen, dass nach dem Unterschriften keine Änderungen am Dokument vorgenommen wurden. Prüfprotokolle bieten zusätzliche wertvolle Informationen wie die IP-Adresse oder den Standort des Unterzeichners.

Vertrauensdienste

Um höchste Sicherheit zu gewährleisten, verwenden Prozesse für digitale Signaturen eine Technologie namens PKI (Public Key Infrastructure) für Verschlüsselung, Unterzeichnung und zertifikatbasierte Authentifizierung. Digitale IDs werden von Zertifizierungsstellen und Vertrauensdiensten ausgestellt, die bestimmte Anforderungen erfüllen müssen. Diese Anbieter tragen zur Etablierung eines einheitlichen, auf Standards basierenden Prozesses bei, der die Überprüfung der Identität von Unterzeichnern und der Authentizität von Dokumenten auf globaler Ebene ermöglicht.

Regierungseinrichtungen und Unternehmen veröffentlichen Listen von Dienstleistern, die die festgelegten Anforderungen erfüllen. Adobe ist der einzige Software-Anbieter, der Vertrauenslisten veröffentlicht und verwaltet und damit die Validierung von elektronischen Unterschriften auf globaler Ebene möglich macht. Globale und regionale Listen wie die [Adobe Approved Trust List \(AATL\)](#) und die [European Union Trust Lists \(EUTL\)](#) werden von Adobe-Lösungen vollständig unterstützt.

Vertrauensdienste bieten verschiedene Dienste für sichere Identitäten und Transaktionen an und sind u. a. tätig als:

- Registrierungsstelle – Die Identität des Unterzeichners wird persönlich überprüft.
- Zertifizierungsstelle – Nach Bestätigung der Identität gibt die Zertifizierungsstelle einen privaten Schlüssel und das entsprechende Zertifikat aus. Die Verwaltung der Daten erfolgt ebenfalls durch diese Stelle. Der private Schlüssel wird durch ein Kennwort oder eine PIN geschützt, das/die nur dem Unterzeichner bekannt ist.
- Zeitstempeldienst – Anerkannte Zeitstempeldienste dokumentieren die exakte Uhrzeit für jede Unterschrift.

Über Adobe Sign können Sie mit einem Vertrauensdienst Ihrer Wahl zusammenarbeiten, um Dokumente zu unterzeichnen und mit einem Zeitstempel zu versehen. Dadurch können Sie sicher sein, dass Sie die Gesetze und Vorschriften in Ihrem Land oder Ihrer Branche einhalten. Und mit einem qualifizierten Zeitstempel von Adobe oder einem Vertrauensdienst Ihrer Wahl erfüllen Sie die Anforderungen an digitale Langzeitarchivierung. Während des Validierungsprozesses bestätigt Adobe, dass die ausgewählten Dienstleister vertrauenswürdige Partner mit entsprechender internationaler, regionaler oder branchenspezifischer Akkreditierung sind. Vertrauenslisten wie AATL und EUTL sind eine zuverlässige, anerkannte Quelle für vertrauenswürdige Anbieter. Sie werden u. a. verwendet von:

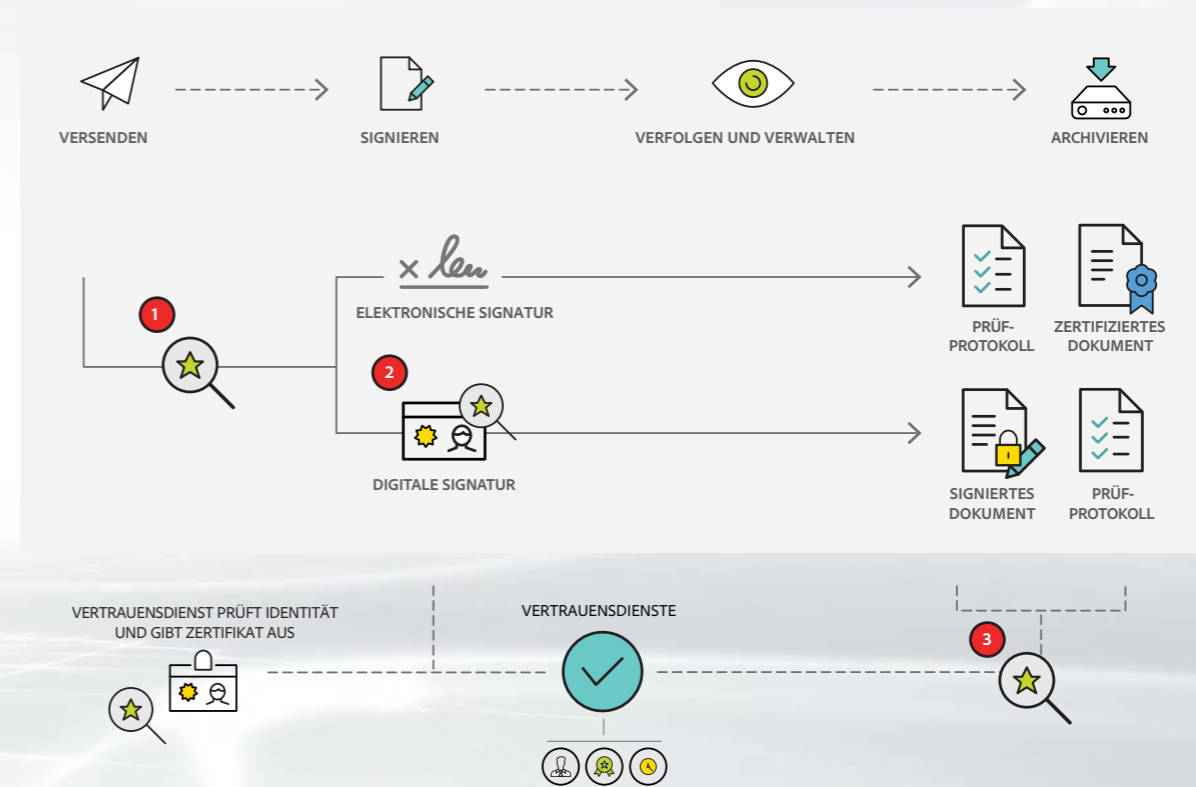
- der US-Regierung und dem US-Verteidigungsministerium
- allen 28 Mitgliedsstaaten der EU
- den Regierungen von Japan, Brasilien, Schweiz, Indien und Uruguay
- Postdiensten in Deutschland, Frankreich, Italien, Hongkong und Südafrika
- SAFE-BioPharma und IdenTrust

Eine Lösung. Mehrere Optionen.

Adobe Sign ist darauf ausgerichtet, die maximale Bandbreite an globalen und nationalen Anforderungen für elektronische und digitale Signaturen abzudecken, sodass Sie das optimale Verfahren für Ihre individuellen Geschäftsprozesse wählen können. Mit Adobe Sign können Sie vollständig digitale Workflows entwickeln, die elektronische Signaturen, digitale Signaturen oder beides umfassen. Adobe Sign bietet außerdem branchenführende Unterstützung für die Authentifizierung und Validierung der Identität von Unterzeichnern.

- 1 Bevor ein Dokument von einem Unterzeichner geöffnet werden kann, muss er seine Identität per Ein- oder Multi-Faktor-Authentifizierung nachweisen.
- 2 Der Unterzeichner fügt seine digitale Signatur unter Angabe eines Kennworts oder eines per PIN geschützten privaten Schlüssels für sein Zertifikat hinzu, um die Signatur an das Dokument zu binden.
- 3 Die Authentizität des Unterzeichners und Dokuments wird durch einen Vertrauensdienst bestätigt, der digitale IDs ausstellt. Adobe Sign kooperiert mit mehr als 200 Vertrauensdiensten weltweit und verfügt über ein ständig wachsendes Netzwerk von Partnern, die Cloud-basierte digitale Unterschriften unterstützen, um Anwendern das Unterschriften jederzeit – auch unterwegs – zu ermöglichen.

Elektronische Signaturen und digitale Signaturen mit Adobe Sign



„Anstatt einen ganzen Tag damit zu verbringen, eine Police in Papierform vorzubereiten und dann eine Woche oder länger auf das ausgefüllte Antwortformular zu warten, erhalten wir jetzt 70 % des Rücklaufs innerhalb von 24 Stunden – dank Adobe Sign. Der gesamte Prozess ist einfacher geworden und führt zu einem deutlich besseren Kundenerlebnis.“

CHRISTINE FRANCIS
Business Operations Development
Manager of Shared Services
Unum

Von Adobe Sign unterstützte Signaturarten

Ganz gleich, ob die Empfänger Ihrer Dokumente mit elektronischen oder digitalen Signaturen unterschreiben: Adobe Sign erfüllt die grundlegenden Voraussetzungen für durchgängig gesetzeskonforme Geschäftsprozesse.

		Elektronische Signaturen	Digitale Signaturen
Zustimmung	Ausdrückliche Zustimmung im laufenden Prozess	✓	✓
Authentifizierung	Ein-Faktor-Authentifizierung mit E-Mail-ID und einem abgesicherten, verfolgten Prozess	✓	✓
	Multi-Faktor-Authentifizierung (z. B. mit E-Mail plus Social-ID, telefonisch übermittelter PIN, Sicherheitsfrage, Kennwort usw.)	✓	✓
	Authentifizierung mit digitaler ID und privater PIN	—	✓
Signatur	Elektronische Unterschrift im Webbrowser oder auf einem Mobilgerät; kein Download oder Log-in erforderlich	✓	✓
	Unterschrift mit digitaler ID auf dem Desktop-Computer; ausgeführt per Chip-Karte, USB-Token, HSM und weltweit mehr als 200 Zertifizierungsstellen	—	✓
	Unterschrift mit Cloud-basierter digitaler ID im Webbrowser oder auf einem Mobilgerät; Unterstützung offener Standards für Cloud-basierte digitale Signaturen	—	✓
Gewährleistung der Dokumentenintegrität	Zertifizierung von Adobe	✓	✓
	Digitale Signatur von allen Teilnehmern	—	✓
Verfolgung	Von Adobe zertifiziertes Prüfprotokoll	✓	✓
Validierung durch Vertrauensdienst	Identität und Signatur des Unterzeichners	—	✓
	Manipulationssicheres Siegel	✓	✓
	Zeitstempel von Adobe für langfristige Validierung oder Zeitstempel eines Drittanbieters	—	✓
Sicherheit	ISO 27001, SOC 2 Type 2, PCI DSS, SAFE-BioPharma-Zertifizierung; Adobe SPLC	✓	✓
	Entspricht den SPLC-Standards (Adobe Secure Product Lifecycle)	✓	✓
Compliance	HIPAA, FERPA, GLBA und andere	✓	✓
	Konform mit Title 21 CFR Part 11 der FDA	✓	✓
Wahrung der Datenhoheit	Rechenzentren in Nordamerika, Europa, Australien, Indien und Japan	✓	✓

Adobe – die Nummer 1 für sichere digitale Dokumente

Adobe ist der weltweit führende Anbieter für sichere digitale Dokumentenlösungen und standardkonforme elektronische Unterschriften. Technologien von Adobe kommen bei mehr als 6 Milliarden Transaktionen pro Jahr zum Einsatz. Adobe Sign ermöglicht reibungslose, einfache Unterschriftsprozesse bei gleichzeitiger Compliance mit nationalen und internationalen Gesetzen zu elektronischen Signaturen. Adobe-Lösungen werden von Fortune 1000-Unternehmen, Behörden, Gesundheitsorganisationen und Finanzinstituten zur abteilungsübergreifenden Automatisierung von Unterschrifts- und Genehmigungsprozessen verwendet.

Die wichtigsten Vorteile von Adobe Sign

Auf Standards basierende Signaturen – Adobe ist der Erfinder von PDF und den digitalen Signaturen, die von PDF unterstützt werden. In Zusammenarbeit mit den Normungsorganisationen ISO und ETSI wurden daraus offene Standards. Adobe kooperiert mit mehr als 200 Zertifizierungsstellen weltweit. Zudem ist Adobe der einzige internationale Anbieter, der alle von der EU akkreditierten Vertrauensdienste für die Ausstellung von qualifizierten digitalen IDs unterstützt. Als Mitglied des Cloud Signature Consortium arbeitet Adobe auch an einem weltweiten Standard für digitale Signaturen über Mobilgeräte oder das Web. Die [Cloud Signature-Lösungen](#) von Adobe ermöglichen die Verwendung von vertrauenswürdigen digitalen IDs branchenführender Anbieter, die durch ihre unkomplizierte Verwendung und Bereitstellung sowie die Einhaltung von Compliance-Vorgaben überzeugen.

Erstklassige Workflows – Adobe Sign vereinfacht die Verwaltung durchgängig digitaler Geschäftsprozesse. Sie können Dokumente bequem zur Unterzeichnung versenden und Transaktionen in Rekordzeit abwickeln. Dokumente lassen sich in Ihrem Netzwerk, in einem Repository Ihrer Wahl oder bei [Adobe Document Cloud](#) speichern. Prozesse mit Adobe Sign sind sicher, sodass Ihre Mitarbeiter Dokumente überall speichern, anzeigen, in Echtzeit verfolgen und verwalten können.

Maximale Flexibilität – Adobe Sign bietet eine skalierbare Lösung zur Erstellung lückenloser Unterschriftsprozesse mit digitalen Signaturen, elektronischen Signaturen oder beidem. Entwickeln Sie Workflows, die sich flexibel auf die für Sie geltende Rechtslage, Ihr Risikoprofil und Ihre geschäftlichen Anforderungen abstimmen lassen. Für Prozesse mit digitalen Signaturen in Ihrer Organisation oder in der Cloud können Sie Adobe Sign plus eine Zertifizierungsstelle oder einen Vertrauensdienst Ihrer Wahl nutzen. Unterstützt werden sämtliche Geräte zur Erstellung von Signaturen, darunter Chip-Karten, USB-Token und Cloud-basierte HSMs.

Umfassende Sicherheitsmaßnahmen – Adobe nimmt die Sicherheit Ihrer digitalen Inhalte ernst. Adobe Sign entspricht strengen Sicherheitsstandards wie ISO 27001, SOC 2 Type 2, HIPAA und PCI DSS. Im Rahmen des SPLC-Programms (Adobe Secure Product Lifecycle) werden zahlreiche spezielle, auf größtmögliche Sicherheit ausgerichtete Methoden, Prozesse und Werkzeuge implementiert, die während des gesamten Produktzyklus zum Einsatz kommen.

Eine Lösung für Organisationen jeder Größe – Die leistungsstarken Admin-Werkzeuge von Adobe Sign vereinfachen die Verwaltung von Einstellungen für Anwender und Gruppen, Einschränkungen und Sprachen. Rechenzentren in Nordamerika, Europa, Australien, Indien und Japan mit höchster Datenverfügbarkeit stellen den reibungslosen Betrieb Ihrer Organisation sicher.

Schlüsselfertige Integrationen – Mit vorintegrierten, umfangreichen Lösungen lassen sich Funktionen für elektronische Unterschriften in Ihre Datensysteme einbinden. Adobe Sign umfasst schlüsselfertige Integrationen und zuverlässige APIs zur Einbettung von elektronischen Unterschriftsprozessen in Enterprise-Systeme und -Applikationen, z. B. Salesforce, Workday, Microsoft Dynamics CRM, Ariba, SAP oder Apttus.

Überzeugende Kundenerlebnisse – Mit den Lösungen von Adobe können Sie schneller auf Kundenanfragen reagieren und die Abwicklung von Vertragsabschlüssen beschleunigen. Kunden können Dokumente elektronisch unterzeichnen. Zwischenschritte wie das Ausdrucken oder Faxen, die Installation von Software, die Erstellung neuer Anwenderkonten oder das Scannen von Dokumenten entfallen. Der gesamte Prozess erfordert viel weniger Zeit, sodass Sie sich schnell anderen Aufgaben widmen können.

Um mehr darüber zu erfahren, wie Ihre Organisation von Adobe Sign profitieren kann, wenden Sie sich an einen Vertriebsmitarbeiter von Adobe.

Ressourcen

Weitere Informationen finden Sie unter:

- Einführung in Fernsignaturen mit Adobe Sign
- Elektronische Signaturen weltweit: Leitfaden zu Gesetzgebung und Durchsetzbarkeit
- Entwicklung einer effektiven Richtlinie für elektronische Signaturen
- Einführung in Adobe Sign

Weitere Informationen

<https://adobe.com/go/adobesign-de>



Copyright © 2018 Adobe Systems Incorporated. All rights reserved.
Adobe and the Adobe logo are either registered trademarks or
trademarks of Adobe Systems Incorporated in the United States
and/or other countries.