DocuWare

White Paper
Elektronische Signaturen mit DocuWare

Sichere Geschäftsprozesse durch Vertrauen in Dokumente

März 2021

Dieses Dokument wurde erstellt mit AuthorIT.

DocuWare GmbH
Planegger Straße 1
82110 Germering
www.docuware.com

Inhalt

1 Sichere Geschäftsprozesse durch Vertrauen in Dokumente

Vertrauen bildet die Grundlage für jede Zusammenarbeit und jeden Austausch von Waren und Informationen, ob im privaten oder im geschäftlichen Rahmen. In Verträgen oder anderen Vereinbarungen steht als verbindliches Symbol für dieses Vertrauen die Unterschrift einer Person.

Was früher nur mit Papier und Stift möglich war, gelingt heute mit der elektronischen Signatur: eine Übereinkunft schaffen, die so verbindlich ist wie die Unterschrift per Hand – und das mit Geschäftspartnern in der ganzen Welt. Signaturen schaffen auch über große Entfernungen Rechtssicherheit für Ihre Dokumente.

Fast alle Branchen haben sich zudem darauf eingestellt, dass ihre Mitarbeiter von verschiedenen Standorten aus zusammenarbeiten, einschließlich Home-Office und mobilen Büros.

Cloud-Signaturen tragen erheblich zu Ihrem Unternehmenserfolg bei: Sie ermöglichen die Überprüfung der Echtheit von Dokumenten auch über die Ferne und stellen Ihre Geschäftskontinuität und Produktivität sicher.

Integrität und Authentizität von Dokumenten belegen

Täglich schreiben oder erhalten wir Unmengen von Dokumenten. Ein Teil davon benötigt im geschäftlichen oder behördlichen Umfeld keine besondere Beweiskraft. Andere Dokumente, zum Beispiel bestimmte Verträge, müssen rechtssicher gestaltet sein, damit auch ein Gericht sie als verbindlich ansehen würde. Je nach Branche, Prozess, Vorliebe, Unternehmensstandort und Geschäftspartnern gibt es unterschiedliche Regeln, um Rechtssicherheit zu schaffen.

Die elektronische Signatur ermöglicht es Ihnen, die Authentizität, Integrität und Herkunft eines Dokuments zu überprüfen:

- Authentizität: Das Dokument ist echt.
- Integrität: Der Inhalt des Dokuments wurde nicht verändert.
- Herkunft: Die Person, die das Dokument erstellt hat, ist identifizierbar.

Elektronische Signaturen für vernetztes Business und Remote-Arbeit

Geschäftsdokumente gehören nicht mehr nur in Firmenbüros zum Alltag. Sie finden sich auch im Home Office und beim mobilen Arbeiten. Eine solche verteilte Umgebung verlangt nach Verbindlichkeit und Rechtssicherheit auch über große Distanzen hinweg. Elektronische Signaturen helfen den Mitarbeitern, ihre Aufgaben sofort und von jedem Ort aus zu erfüllen. Schließlich soll ein Prozess nicht ins Stocken geraten, nur weil ein Mitarbeiter beim mobilen Arbeiten ein Dokument mangels Druckmöglichkeit nicht unterschreiben kann.

Standortunabhängige Transaktionen rechtskonform vollziehen

Auch wenn die gesetzlichen Modelle regional variieren, eines ist klar: Die Hardware-Sicherheitsmodule zum Erstellen digitaler Zertifikate können sich überall in hochsicheren Cloud-Infrastrukturen befinden.

Wo früher eine physische Smartcard und ein Lesegerät nötig war, genügt heute die Anbindung über Signaturanbieter, die nach klaren Sicherheitsstandards geprüft und zertifiziert sind. So sind auch die Daten, die beim Signaturvorgang ausgetauscht werden, sicher.

Signieren von jedem Gerät

Durch das Einbinden elektronischer Signaturen in automatisierte Workflows können Unternehmen alle Prozesse rechtssicher abschließen, unabhängig vom genutzten Gerät. Dies bezieht Unterschriften ein, die auf PCs, Tablets und mobilen Geräten geleistet werden, gleich ob diese dem Unternehmen oder dem Kunden gehören.

Die Transaktionsdaten sind sicher und geschützt. Mit modernen Signaturen erfüllen Unternehmen die Compliance-Anforderungen ihrer jeweiligen Region, sowohl bei der Informationssicherheit als auch beim Datenschutz.

Authentifizierung und Identitätsübermittlung

Viele Dokumente wie z. B. Verträge werden von einer Person in einer Organisation erstellt und unterzeichnet und dann von einer Person außerhalb der Organisation gegengezeichnet. In diesen Fällen wird sehr häufig eine fortgeschrittene elektronische Signatur verwendet. Anerkannte Verfahren hierfür sind die Bestätigung per Zugangscode, Telefon oder SMS oder auch die wissensbasierte Authentifizierung.

Je nach Anforderungen an die Signatur kann es jedoch nötig sein, die Identität des Unterzeichners zweifelsfrei zu verifizieren. In diesen Fällen empfiehlt sich eine qualifizierte elektronische Signatur. Die Verifizierung erfolgt hier über einen Drittanbieter, der den Nutzer authentifiziert und so dessen Identität beim Signieren sicherstellt.

Was Sie bei Ihrer Entscheidung beachten sollten

Wenn Sie in Ihrem Unternehmen elektronische Signaturen einsetzen möchten, sollten Sie bei der Auswahl einer Lösung u.a. diese Fragen berücksichtigen:

- Eignet sich die Signaturlösung, um Integrität und Authentizität der Dokumente zu belegen?
- Läuft das Signieren in automatisierten Workflows ab, in die Sie auch Mitarbeiter mit Remote-Arbeitsplatz einbinden können?
- Bietet die Lösung das Signieren auf firmen- wie auf kundeneigenen Geräten?
- Erlaubt die Lösung das Signieren mit unterschiedlichen Stufen der Beweiskraft (fortgeschritten und qualifiziert)?
- Werden die Daten des Signaturvorgangs rechtskonform in der gewünschten Datenschutzregion gespeichert?
- Setzt der Signaturdienstleister hochsichere Hardware-Sicherheitsmodule (HSM) mit Compliance-Nachweis ein?

2 Dokumente im Workflow signieren mit DocuWare

Mit dem DocuWare Signature Service versehen Sie Ihre Dokumente in einem Workflow mit einer elektronischen Signatur. Zwei Faktoren sorgen dafür, dass Ihr Unternehmen noch zukunftsfähiger wird:

- Durch das Signieren innerhalb von Workflows halten Sie den Aufwand für Ihre Mitarbeiter so gering wie möglich und beschleunigen Ihre Prozesse.
- Sie nutzen Fernsignaturen, auch Cloud-Signaturen genannt, und sind deshalb unabhängig vom Arbeitsort der Beteiligten.

Bei Cloud-Signaturen läuft der Signiervorgang über das Internet in der Cloud ab, gleich ob Sie mit DocuWare Cloud oder mit einem On-Premises-System von DocuWare arbeiten. Sie müssen dafür also nichts zusätzlich installieren.

Der DocuWare Signature Service sorgt dafür, dass Ihre Dokumente über einen anerkannten, geprüften Signaturanbieter signiert werden. Er bietet Ihnen maximale Geschwindigkeit und Flexibilität beim Einsatz der elektronischen Signaturen:

- Nahtlos binden Sie externe Signaturanbieter wie Validated ID oder DocuSign in Ihre DocuWare-Workflows ein. Die Dokumente werden automatisch an den Dienstleister übermittelt, ebenso automatisch erhält der Empfänger die Nachricht, dass ein Dokument zur Unterschrift vorliegt.
- Zeitnah sammeln Sie die Unterschriften zu einem Dokument von allen relevanten Mitarbeitern ein.
- Fortgeschritten oder qualifiziert? Sie wählen den Sicherheitslevel für die Signatur entsprechend Ihren Anforderungen. Der Unterschied besteht vor allem im Authentifizierungsverfahren. Bei der fortgeschrittenen Signatur genügt zum Beispiel eine Zwei-Faktor-Authentifizierung des Unterzeichners (z.B. E-Mail und SMS). Bei der qualifizierten Signatur ist zur Authentifizierung das Zertifikat eines Vertrauensdienstanbieters erforderlich.
- Die qualifizierten Zertifikate für eine qualifizierte elektronische Signatur sind beim externen Dienstleister zentral hintergelegt, sodass sie jederzeit abgerufen werden können.
- Das Dokument wird zusammen mit der Signatur revisionssicher im Archiv gespeichert.

3 So profitieren Ihre Prozesse von elektronischen Signaturen

Das Signieren in Workflows bietet sich für viele Unternehmensprozesse an. Die folgenden Szenarien stehen beispielhaft für unterschiedlichste Geschäftsbereiche.

Verträge papierlos abwickeln

Schließen Sie Verträge ohne zeitlichen Verzug und ohne Medienbruch, zum Beispiel Leasing-Verträge für Mitarbeiter-PKWs.

Arbeitsverträge unterzeichnen

In Zeiten von Fachkräftemangel und Home-Office kann Ihre HR-Abteilung viele Arten von Arbeitsverträgen ohne Verzögerung und persönliche Anwesenheit unterschreiben lassen. Dies spart nicht nur Kosten für Papier und Porto, sondern vereinfacht den Prozess enorm. Wenn Sie viel Geld ins Recruiting von qualifizierten Mitarbeitern stecken, darf die Unterzeichnung von Arbeitsverträgen sich nicht verzögern, nur weil der digitale Unterschriftsprozess dafür fehlt. Elektronische Signaturen ermöglichen es, Onboarding und Einstellung von neuen Mitarbeitern zu 100 Prozent im Remote-Prozess zu erledigen.

Personalwesen

Für die Unternehmens-Compliance lassen Sie Mitarbeiter-SOPs, Arbeitsanweisungen, Geheimhaltungserklärungen oder andere Vereinbarungen ohne Medienbruch oder zeitlichen Verzug im Workflow elektronisch signieren. Wenn Ihre Mitarbeiter im Remote-Office arbeiten, helfen elektronische Signaturen sicherzustellen, dass alle den gleichen Vertrauensstandard anwenden. Für Auditings und Zertifizierungen liegen alle Nachweise rechtssicher im Archiv vor und sind auf Knopfdruck vorzeigbar.

Ausstattung mit IT-Geräten für Büro und Home-Office

Geräte für Mitarbeiter bereitzustellen ist eine Schlüsselkomponente des Onboarding-Prozesses, häufig kommt es dabei aber zu Zeitverlusten und erhöhten Kosten. Automatisierte Workflows führen zu optimierten Prozessen, in denen die Mitarbeiter per elektronischer Unterschrift den Erhalt von Geräten effizient bestätigen können.
Auch um Mitarbeiter für das Home-Office auszustatten, eignet sich diese Form der Empfangsbestätigung.

Kundendarlehen

Ein Handelsunternehmen gewährt seinen Kunden jeweils eigene Kreditrahmen. Die zugehörigen Unterlagen und vertraglichen Vereinbarungen werden automatisch an die Kunden zur Prüfung weitergeleitet und sie können ihre Unterschrift elektronisch auf allen verfügbaren PCs, Tablets oder mobilen Geräten leisten.

4 Signaturdienstleister für DocuWare

DocuWare arbeitet mit Signatur-Dienstleistern wie Validated ID oder DocuSign zusammen, um Dokumente in einem DocuWare Workflow zu signieren. Beide sind Anbieter von Vertrauensdiensten. Dabei bieten die Signaturverfahren von Validated ID und DocuSign verschiedene Authentifizierungsverfahren, die Sie je nach Wahl der Signaturmethode festlegen können.

Die Signaturmethoden sind die fortgeschrittene elektronische Signatur (Advanced Electronic Signature, AES) und die qualifizierte elektronische Signatur (Qualified Electronic Signature, QES), die im Kapitel Compliance durch elektronische Signaturen weltweit genauer erläutert werden.

Validated ID

Validated ID sendet zum Signieren in der Regel eine E-Mail mit einem Link zum Dokument. Der Unterzeichner kann aus folgenden Authentifizierungsmethoden für das Signieren wählen, je nachdem, wie die Anforderung übermittelt wurde und welche AES- oder QES-Signaturmethode damit verbunden ist:

- Remote – Authentifizierung per SMS (AES)
  Die Person, die ein Dokument unterzeichnen soll, erhält eine SMS, die es ihr ermöglicht, ihre Unterschrift unter das Dokument zu setzen.
- Biometrisch – Vor-Ort-Authentifizierung (AES)
  Ein Kunde unterschreibt auf einem Tablet. Dabei werden biometrische Daten wie Schreibdruck und -geschwindigkeit erfasst und mit der Signatur in das Dokument eingebettet. Die Geräte, die hierfür verwendet werden, müssen vorab registriert werden und sind somit beim Signaturdienstleister bekannt (unterstützte Geräte). Nur im Fall der biometrischen Option wird direkt das Dokument zur Signatur an ein registriertes Gerät gesendet.
- Zentralisiert – einmalige Authentifizierung beim Signaturdienstleister (AES / QES)
  Bei dieser Signatur wird bei Validated ID nach einer Identifizierung des Nutzers ein Zertifikat hinterlegt, das dessen Identität bestätigt. So kann der Nutzer sich von überall und jederzeit bei Validated ID authentifizieren und Dokumente unterzeichnen.

DocuSign

DocuSign sendet zum Signieren eine E-Mail mit einem Link zum Dokument. Der Unterzeichner wählt für das Signieren eine der folgenden Authentifizierungsmethoden, je nachdem, wie die Anfrage eingereicht wurde und welche AES- oder QES-Signaturmethode damit verbunden ist:

- Keine besondere Authentifizierung (AES)
- Authentifizierung per Telefonanruf (AES)
- Authentifizierung per Zugangscode, zum Beispiel Passwort (AES)
- Wissensbasierte Authentifizierung (AES). Bei dieser nur in den USA verfügbaren Methode beantwortet der Unterzeichner spezielle Fragen zu seiner Person, deren Antworten aus öffentlichen Aufzeichnungen verfügbar sind (z.B. seine aktuelle und frühere Adresse).
- ID-Prüfung für eIDAS (AES / QES)

5 So läuft das Signieren ab

Um ein Dokument, zum Beispiel einen Vertrag, mit dem DocuWare Signature Service zu signieren, muss es zunächst in einem DocuWare Archiv abgelegt worden sein. Der Service wird dann innerhalb einer Workflow-Aufgabe gestartet.

Nach diesem Anstoß laufen mehrere Schritte zwischen einer Person 1 ab, die eine Signatur in einem DocuWare-Workflow anfordert, und einer Person 2, die das Dokument signiert. Dabei können beide Personen auch identisch sein.

Vom Grundsatz her sieht der Signierprozess mit dem DocuWare Signature Service stets gleich aus:

1. Der Workflow sendet Informationen über das Dokument und die Signatur an den Signature Service.
2. Der Signature Service lädt das Dokument aus DocuWare und übergibt es an den Signaturdienstleister.
3. Der Signaturdienstleister informiert die signierende Person per E-Mail.
4. Die signierende Person öffnet den mitgesandten Link und startet den Signaturprozess.
5. Der Signaturdienstleister authentifiziert die signierende Person.
6. Die Signatur wird mit dem Dokument verbunden.
7. Der Signaturdienstleister informiert den Signature Service über das signierte Dokument.
8. Der Signature Service lädt das Dokument vom Signaturdienstleister und legt es in DocuWare ab.

Ein Dokument kann von einer einzigen oder von mehreren Personen signiert werden. Der Signiervorgang läuft dabei stets pro Unterzeichner gleich ab, weil eine elektronische Signatur immer an eine natürliche Person gebunden ist.

Letztlich kommt es auf die Art des Dokuments und die gesetzlichen Vorschriften dafür an, ob eine oder mehrere Personen es signieren sollten und mit welchem Signatur-Sicherheitslevel dies zu tun ist, also mit einer fortgeschrittenen (AES) oder einer qualifizierten elektronischen Signatur (QES). Mehr dazu lesen Sie unter Compliance durch elektronische Signaturen weltweit.

Die verschiedenen Signiervorgänge

Die Signiervorgänge unterscheiden sich vor allem in der Authentifizierungsmethode. Die im Folgenden beschriebenen Authentifizierungsverfahren gehen davon aus: Person 1 (P1) arbeitet in einem Unternehmen, das DocuWare einsetzt. Person 2 (P2) kann ein interner Kollege oder ein externer Geschäftspartner sein, muss aber kein DocuWare-Nutzer sein. Es ist immer Person 1, die die Signatur innerhalb eines Workflows anfordert, und Person 2, die signiert.

Validated ID: Remote (AES)

Für Person 2 ist keine Registrierung bei Validated ID erforderlich.

Schritte:

1. P2 teilt P1 Name, E-Mail-Adresse und SMS-fähige Telefonnummer mit.
2. P1 trägt die Daten von P2 in das Workflow-Formular ein und fordert damit die Signatur bei Validated ID an.
3. P2 erhält eine E-Mail mit dem Link zum Dokument sowie eine SMS mit einer TAN, die sie zum Auslösen der Signatur verwendet.

Validated ID: Biometrisch (AES)

Für Person 2 ist keine Registrierung bei Validated ID erforderlich.

Schritte:

1. P1 arbeitet am Firmenempfang und prüft die Identität des Besuchers P2 per Augenschein. P1 bestätigt die Identität von P2 und trägt deren Namen im Formular einer Workflow-Aufgabe ein. Die Information wird an ein Unterschriftstablet geschickt.
2. P2 unterschreibt auf dem Tablet, dabei werden biometrische Daten wie der Schreibdruck für eine eventuelle spätere Überprüfung gespeichert.

Validated ID: Zentralisiert (AES)

Person 1 und Person 2 arbeiten im selben Unternehmen, das einen Vertrag mit Validated ID hat. P2 ist bei Validated ID registriert.

Schritte:

1. P2 teilt P1 seinen Namen, seine E-Mail-Adresse und die Benutzer-ID mit, die P2 bei der Authentifizierung von Validated ID erhalten hat (z. B. die Ausweisnummer).
2. P1 gibt die Daten von P2 in das Workflow-Formular ein und fordert damit die Signatur an.
3. P2 signiert.

Validated ID: Zentralisiert (QES)

Person 1 und Person 2 arbeiten im selben Unternehmen, das einen Vertrag mit Validated ID hat. P2 ist bei Validated ID registriert und hat für ein qualifiziertes Zertifikat eine separate Identifizierung bei Validated ID durchlaufen.

Schritte:

1. P2 teilt P1 seinen Namen, seine E-Mail-Adresse und die Benutzer-ID mit, die P2 bei der Authentifizierung von Validated ID erhalten hat (z. B. die Ausweisnummer).
2. P1 gibt die Daten von P2 in das Workflow-Formular ein und fordert damit die Signatur an.
3. P2 signiert mit qualifiziertem Zertifikat.

DocuSign: Keine Authentifizierung (AES)

Für Person 2 ist keine Registrierung bei DocuSign erforderlich.

Schritte:

1. P2 teilt P1 seinen Namen und seine E-Mail-Adresse mit.
2. P1 gibt die Daten von P2 in das Workflow-Formular ein und fordert damit die Signatur bei DocuSign an.
3. P2 erhält eine E-Mail mit einem Link zu dem Dokument in DocuSign, wo sie es signiert.

DocuSign: Authentifizierung durch SMS (AES)

Für Person 2 ist keine Registrierung bei DocuSign erforderlich.

Schritte:

1. P2 teilt P1 seinen Namen, seine E-Mail-Adresse und seine SMS-fähige Telefonnummer mit.
2. P1 gibt die Daten von P2 in das Workflow-Formular ein und fordert damit die Unterschrift bei DocuSign an.
3. P2 erhält von DocuSign eine E-Mail mit einem Link auf das Dokument sowie eine TAN per SMS, mit der sie die Signatur auslöst.

DocuSign: Authentifizierung durch Telefonanruf (AES)

Für Person 2 ist keine Registrierung bei DocuSign erforderlich.

Schritte:

1. P2 teilt P1 seinen Namen, seine E-Mail-Adresse und seine Telefonnummer mit.
2. P1 gibt die Daten von P2 in das Workflow-Formular ein und fordert damit die Unterschrift bei DocuSign an.
3. P2 erhält von DocuSign eine E-Mail mit einem Link auf das Dokument sowie eine per Telefonanruf erhaltene Information, z.B. einen Code, mit der sie die Signatur auslöst.

DocuSign: Authentifizierung durch Zugangscode (AES)

Für Person 2 ist keine Registrierung bei DocuSign erforderlich.

Schritte:

1. P2 teilt P1 seinen Namen und seine E-Mail-Adresse mit.
2. P1 gibt die Daten von P2 und einen Zugangscode (z.B. Passwort) in das Workflow-Formular ein und fordert damit die Signatur bei DocuSign an.
3. P2 erhält eine E-Mail mit einem Link auf das Dokument in DocuSign.
4. P1 überträgt den Zugangscode aktiv an P2. Dies kann mündlich erfolgen (Präsenzgespräch, Telefonat) oder über eine Vorabvereinbarung (z.B. kann immer das Geburtsdatum oder eine Mitgliedsnummer als Code verwendet werden).
5. P2 nutzt den Code, um die Signatur auszulösen.

DocuSign: Wissensbasierte Authentifizierung, nur USA (AES)

Für Person 2 ist keine Registrierung bei DocuSign erforderlich

Schritte:

1. P2 teilt P1 ihren Namen und ihre E-Mail-Adresse mit.
2. P1 gibt die Daten von P2 in das Workflow-Formular ein und fordert damit die Signatur bei DocuSign an.
3. P2 erhält eine E-Mail mit einem Link zu dem Dokument und muss eine auf sie persönlich zugeschnittene, wissensbasierte Multiple-Choice-Frage von DocuSign beantworten.

DocuSign: Authentifizierung durch ID-Prüfung für eIDAS (AES / QES)

Für Person 2 ist keine Registrierung bei DocuSign erforderlich. Falls eine qualifizierte Signatur benötigt wird, erfolgt zum Zeitpunkt der Signatur zuerst eine Video-Identifizierung.

Schritte:

1. P2 teilt P1 ihren Namen und ihre E-Mail-Adresse mit.
2. P1 fordert die Signatur an und übermittelt den Namen und die E-Mail-Adresse von P2 an DocuSign.
3. P2 erhält eine E-Mail mit einem Link zum Dokument und wird für eine qualifizierte Signatur aufgefordert, ein Foto eines behördlich ausgestellten Identitätsnachweises (z.B. Führerschein, Reisepass) oder einer europäischen ID-Karte zu machen. Dieses wird auf Sicherheitsmarkierungen und Wasserzeichen überprüft und es wird verifiziert, dass der Name auf dem Identitätsnachweis mit dem Namen auf dem Vertrag übereinstimmt.

6 Lizenzierung

Um den DocuWare Signature Service mit Validated ID oder DocuSign nutzen zu können, schließen Sie einen Servicevertrag mit einem der beiden ab. Je nachdem, ob Sie mit DocuWare Cloud oder einem lokal installierten System arbeiten, benötigen Sie folgende Lizenzelemente.

	DocuWare Cloud	**On-Premises-Systeme**
Signature Service	Inbegriffen	Zusatzlizenz *Electronic Signature Integration* erforderlich
Client-Lizenzen	Der Signature Service benötigt eine eigene DocuWare Client Lizenz	Der Signature Service benötigt eine eigene DocuWare Client Lizenz
Weitere DocuWare-Lizenzen	---	- Workflow Manager - Gültiger Wartungs- und Supportvertrag
Signaturvolumen	Muss zusätzlich erworben werden, entweder beim Provider oder – für Validated ID – auch bei DocuWare	Muss zusätzlich erworben werden, entweder beim Provider oder – für Validated ID – auch bei DocuWare
Signaturzertifikat	Muss zusätzlich erworben werden (nur für QES erforderlich)	Muss zusätzlich erworben werden (nur für QES erforderlich)

7 Was technisch beim elektronischen Signieren passiert

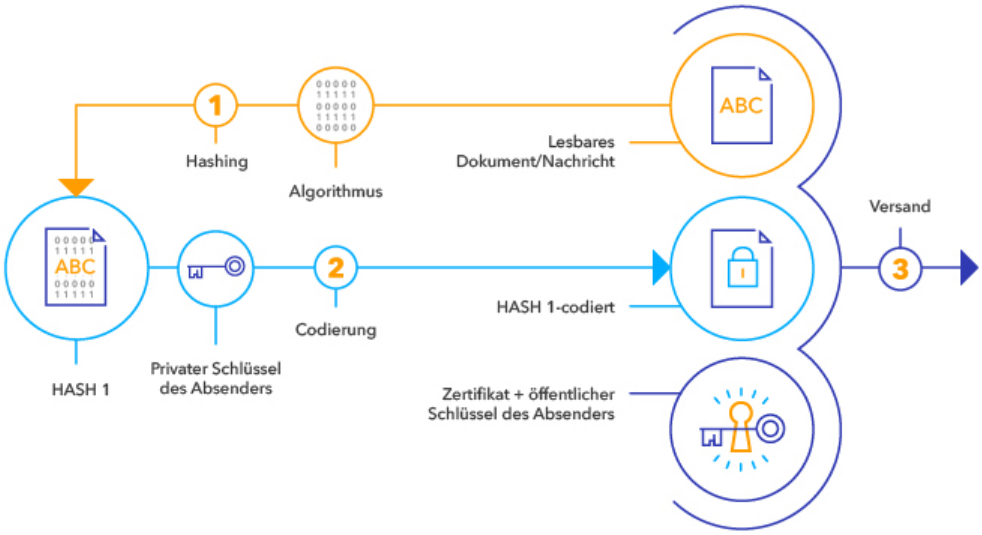
Wenn Sie ein Dokument elektronisch signieren, beinhaltet dieser Prozess mehr, als wenn Sie nur eine Unterschrift unter einen Text setzen. Die meisten Schritte finden von Software gesteuert hinter den Kulissen statt.

Jede Form von elektronischer Signatur besteht vereinfacht gesagt aus Daten, die einem Dokument bzw. einer Datei hinzugefügt werden. Deshalb werden alle Signaturen "elektronisch" genannt. Für die fortgeschrittene und die qualifizierte Signatur gibt es auch den Begriff digitale Signatur, weil sie auf einem Verschlüsselungsverfahren beruhen.

Bei der qualifizierten elektronischen Signatur werden die zusätzlichen Daten durch Hardware-Sicherheitsmodule (HSM) in einer besonders sicheren technischen Umgebung erzeugt. In Regionen mit einer abgestuften gesetzlichen Regelung für Signaturen als Vertrauensdienst, wie z. B. in der EU, gibt es ein zusätzliches Sicherheitskriterium: Das digitale Zertifikat, also der authentifizierte Identitätsnachweis des Unterzeichners, wurde von einer speziell dafür autorisierten und qualifizierten Stelle ausgestellt.

Das Signieren findet in einer sogenannten Public-Key-Infrastruktur statt, in der ein Verschlüsselungsverfahren mit zwei Software-Schlüsseln zum Einsatz kommt. Einer ist der private, den nur die verschlüsselnde Stelle kennt, und einer der öffentliche. Dieser wird dem Dokument im Signaturzertifikat für den Empfänger mitgegeben.

Dabei laufen drei Schritte ab:



1. **Hashwert berechnen**
   Aus den Daten des Dokuments bzw. der Datei wird mit einer mathematischen Funktion eine Prüfsumme berechnet, die man Hashwert nennt. Das ist eine Art Fingerabdruck des Dokuments.
2. **Hashwert verschlüsseln**
   Dieser Hashwert wird mit dem privaten Softwareschlüssel (Private Key) des Unterzeichners verschlüsselt.

3. **Verschlüsselten Hashwert + Zertifikat mit Dokument verbinden**
   Der verschlüsselte Hashwert und das Zertifikat werden an das Dokument gehängt. Das Zertifikat enthält den öffentlichen Schlüssel zum Entschlüsseln des Hashwertes, die Information, dass dieser Schlüssel mit der Identität des Unterzeichners verbunden ist, sowie die Gültigkeit des Zertifikats.

8 Datensicherheit, Datenschutz und sichere Authentifizierung

Cloud-Signaturen beim DocuWare Signature Service können Sie völlig unabhängig davon einsetzen, ob Sie ein Cloud- oder ein On-Premises-System für Ihr Dokumentenmanagement und Workflows nutzen. Der Begriff Cloud-Signatur beschreibt nur, dass der Signature Service wie auch DocuWare Cloud in den Datenzentren von Microsoft Azure gehostet wird. Mit Cloud-Signaturen wie beim DocuWare Signature Service sind Sie mit beiden Lösungen auf der sicheren und rechtskonformen Seite.

Datensicherheit: Signaturvorgang in hochsicheren Krypto-Prozessoren

Früher konnten Unternehmen qualifizierte elektronische Signaturen nur erstellen, wenn die Hardware dafür, die Sichere Signaturerstellungseinheit (SSEE), auf einer Smartcard unter ihrer Kontrolle war.

Heute kann sich die Signaturerstellungseinheit auch bei einem Signaturdienstleister befinden, der das Zertifikat und die Schlüssel für den Signaturersteller verwahrt und anwendet. Diese Anbieter stellen per Internet eine hochsichere Cloud-Signierplattform zur Verfügung, über die Unternehmen, Behörden oder Privatpersonen ihre Dokumente signieren können.

Der eigentliche Signiervorgang findet in Hardware-Sicherheitsmodulen (HSM) statt, die der Signaturdienstleister in einer abgesicherten Cloud-Server-Infrastruktur betreibt. Hardware-Sicherheitsmodule sind besondere Krypto-Prozessoren, die den Schutz von Signatur und Softwareschlüsseln sicherstellen.

Die Signaturdienstleister, mit denen DocuWare zusammenarbeitet, nutzen HSMs, die den US-Standard FIPS 140-2 Level 3 für kryptografische Module erfüllen.

Datenschutz: Die Daten bleiben in Ihrer Region

Signaturdaten enthalten persönliche und vertrauliche Daten. Daher sollte sichergestellt sein, dass diese auch beim Signiervorgang in der Datenschutzregion bleiben, deren Datenschutzrecht anzuwenden ist. Das ist bei den Signaturdienstleistern, mit denen DocuWare zusammenarbeitet, gewährleistet.

Validated ID nutzt hochsichere Datenzentren in Irland und den Niederlanden, die der europäischen Datenschutzgrundverordnung (DSGVO) unterliegen, und für Kunden aus dem Vereinigten Königreich ein dortiges Datenzentrum.

DocuSign nutzt mehrere hochsichere Datenzentren sowohl in den USA als auch in der EU für den Signaturdienst.

9 Compliance durch elektronische Signaturen weltweit

Elektronische Signaturen haben sich weltweit als Mittel für rechtssichere Dokumente etabliert. Die rechtlichen Anforderungen variieren jedoch je nach Region und Land. Jedes Unternehmen muss für sich klären, welche rechtlichen Anforderungen an die Transaktionen bestehen, die durch elektonische Signaturen abgesichert werden sollen.

Wichtig ist, zwischen dem Gerichtsstand und der Rechtswahl zu unterscheiden, also der Frage, welches Recht nach dem Grundsatz der Vertragsfreiheit anzuwenden ist. Der *Gerichtsstand* ist der Ort, dessen Gericht im Zweifelsfall angerufen werden kann. Das *anwendbare Recht* bezieht sich auf das nationale Recht, nach dem über das Dokument im Streitfall entschieden werden würde. Letzteres wird sowohl für den Inhalt eines Dokuments als auch für dessen elektronische Signaturen zugrunde gelegt.

Rechtliche Modelle für Signaturen

Die Rechtsmodelle für elektronische Signaturen lassen sich auf einer Skala zwischen wenig bis stark reguliert abbilden. Wenig reguliert sind die Anforderungen zum Beispiel in Nordamerika, wo man eine große Bandbreite an technologischen Lösungen und Sicherheitslevel als rechtssicher akzeptiert. Eine mittlere oder abgestufte Regulierung weisen zum Beispiel die Länder der Europäischen Union (EU) auf, für die die eIDAS-Verordnung den Rechtsrahmen bildet. Eine besonders starke oder restriktive Regulierung sehen nur einige wenige Länder vor. Die Tabelle zeigt einige Beispiele:

Geringe Regulierung	Abgestufte Regulierung	Restriktive Regulierung
USA Kanada Australien Neuseeland	EU Japan China Südkorea	Brasilien Indien Israel Malaysia

Konzentrieren wir uns auf die beiden geläufigsten Modelle: die geringe und die abgestufte Regulierung.

Geringe Regulierung

In den USA, Kanada, Australien und Neuseeland sind elektronische Signaturen allgemein akzeptiert und haben die gleiche rechtliche Wirkung wie manuelle Signaturen. Alle Arten von elektronischen Signaturen sind legal und durchsetzbar und werden als gleichwertig angesehen.

Beispiel USA

Elektronische Signaturen sind in den Vereinigten Staaten rechtlich zulässig und gut etabliert. Zwei Gesetze erkennen die Gültigkeit und Durchsetzbarkeit von elektronischen Signaturen an: der Uniform Electronic Transactions Act (UETA) 1999 und der Electronic Signatures in Global and National Commerce Act (ESIGN) 2000. Beide Gesetze sehen ausdrücklich vor, dass einer Unterschrift, einem Vertrag oder einer anderen Aufzeichnung im Zusammenhang mit einer kommerziellen Transaktion nicht allein deshalb die Rechtsgültigkeit abgesprochen werden darf, weil sie in elektronischer Form vorliegt.

Abgestufte Regulierung

Beispiel Europäische Union

Der Rechtsrahmen für elektronische Signaturen in der EU ist die eIDAS-Verordnung. Die Abkürzung steht für Electronic IDentification, Authentication and Trust Services – elektronische Identifizierung, Authentifizierung und Vertrauensdienste im europäischen Binnenmarkt. Die Verordnung ist seit 2016 in Kraft.

Die eIDAS gibt ein abgestuftes Rechtsmodell vor, um elektronische Transaktionen sicherer, vertrauenswürdiger und einfacher zu machen. Als EU-Verordnung ist sie eine Art europäisches Gesetz und steht über den nationalen Gesetzgebungen der EU-Mitgliedsstaaten. Jeder Mitgliedsstaat musste seine Gesetze dem Inhalt der Verordnung anpassen. In Deutschland zum Beispiel wurde eIDAS unter anderem im Vertrauensdienstegesetz umgesetzt.

Die eIDAS gilt für den gesamten Europäischen Wirtschaftsraum (EWR), zu dem auch Norwegen, Island und Liechtenstein gehören. Allerdings sollten auch außereuropäische Unternehmen, die mit EU-Unternehmen Geschäfte machen, die eIDAS berücksichtigen. So haben zum Beispiel viele US-amerikanische Unternehmen Niederlassungen oder Kunden in der EU und müssen in diesem Fall auch die eIDAS-Vorgaben beachten.

Die eIDAS sieht drei Level von elektronischen Signaturen mit unterschiedlicher Beweiskraft vor, und zwar die einfache, die fortgeschrittene und die qualifizierte elektronische Signatur.

- **Einfach: formlos bei geringem rechtlichen Risiko**
  Für viele Dokumente wird die einfache elektronische Signatur verwendet. So genügt unter einer E-Mail und vielen Verträgen der getippte Name und/oder das Bitmap-Bild des handschriftlichen Namens. Für solche Dokumente ist gesetzlich keine besondere Form vorgeschrieben und es besteht nur ein geringes Risiko, dass ihre Rechtsgültigkeit angezweifelt wird. Mit DocuWare setzen Sie eine einfache elektronische Signatur zum Beispiel mit einem Stempel.
- **Fortgeschritten bei mittlerem rechtlichen Risiko**
  Damit im Streitfall zumindest der Unterzeichner eines Dokuments bzw. der Signaturersteller identifiziert werden kann, benötigen Sie eine fortgeschrittene elektronische Signatur. Sie ist beispielsweise für Handelsverträge im B2B-Bereich verbreitet. Die eIDAS schreibt für diese Signaturstufe bestimmte Regeln vor. So kann der Signaturersteller beispielsweise über den Einsatz eines elektronischen Signaturzertifikats identifiziert werden. Die fortgeschrittene Signatur hat eine mittlere Beweiskraft.
- **Die qualifizierte Signatur bietet die größte Rechtssicherheit**
  Für manche Dokumente, wie bestimmte Verträge, schreiben Gesetzgeber die eigenhändige Unterschrift vor. In diesen Fällen kommt die qualifizierte elektronische Signatur zum Einsatz, die der eigenhändigen Unterschrift vor Gericht bis auf Ausnahmen gleichkommt und die höchste Beweiskraft besitzt.

Fortgeschrittene elektronische Signaturen können von anderen EU-Mitgliedsstaaten akzeptiert werden, qualifizierte dagegen müssen in der gesamten EU akzeptiert werden. Jeder Mitgliedsstaat reguliert allerdings für sich, ob eine geschäftliche oder behördliche Transaktion eine elektronische Signatur benötigt und welchem Level diese entsprechen muss.

Qualifizierte Zertifikate werden von Vertrauensdiensteanbietern (VDA) bereitgestellt, die dafür spezielle Sicherheitsanforderungen erfüllen müssen. Diese Anbieter haben nach einer offiziellen Prüfung durch eine nationale Behörde den qualifizierten Status erhalten und werden in der EU-Liste der eIDAS Trusted Lists (LOTL) geführt.

Beispiel Japan

Auch Japan hat ein abgestuftes Rechtsmodell für die Regulierung von elektronischen Signaturen. Das japanische Gesetz über elektronische Signaturen und Zertifizierungsgeschäfte (Gesetz Nr. 102 vom 31. Mai 2000) ist seit April 2001 in Kraft. Es sieht eine qualifizierte elektronische Signatur als rechtskonforme elektronische Signatur an. Eine fortgeschrittene elektronische Signatur ist möglich, hat aber eine geringere Beweiskraft.

DocuWare unterstützt alle Szenarien und rechtlichen Anforderungen

Mit dem DocuWare Signature Service können Sie elektronische Signaturen in Ihrem Unternehmen effizient einsetzen und für eine größere Compliance sorgen. In Zusammenarbeit mit den Signaturdienstleistern Validated ID und DocuSign bietet DocuWare Ihnen dafür die verschiedensten sicheren Verfahren.

Legen Sie fest, welche Ihrer Dokumente welche Beweiskraft benötigen, um den rechtlichen Vorgaben zu entsprechen. Entscheiden Sie auf dieser Grundlage, welche der vielfältigen Signieroptionen Sie nutzen möchten.