



Digital signieren



© *intex Informations-Systeme GmbH 2021 | Vervielfältigung, auch auszugsweise,
nur mit schriftlicher Genehmigung der intex Informations-Systeme GmbH*

*Die Inhalte sind nach aktuellem Planungs- und Entwicklungsstand erstellt worden
und können sich jederzeit ändern.*

Digitale Signatur

DER KUGELSCHREIBER HAT AUSGEDIENT.

Zunehmend werden Unternehmen digitaler und die Einführung eines elektronischen Dokumentenmanagementsystems hat die Geschäftsprozesse innerhalb, sowie zwischen Unternehmen grundlegend geändert. Die Verwaltung und die Verarbeitung von Dokumenten läuft in immer größerem Maße mit digitalen Lösungen ab. Jedoch scheitert die durchgängige Digitalisierung der Dokumentenarbeit aber oft bei einem entscheidenden Schritt: bei der Unterschrift. Hier wird der Prozess wieder analog, wenn beispielsweise der Geschäftsführer rechtlich bindende Dokumente per Hand unterschreiben muss. Verschiedene Studien belegen, dass eine Großzahl an Unternehmen Dokumente nur noch wegen einer benötigten Unterschrift ausdrucken. Genau an dieser Stelle entsteht der Medienbruch, der heutzutage nicht mehr notwendig ist.

eIDAS-VERORDNUNG



Seit der Verabschiedung der EU-Verordnung Nr. 910/2014 gilt seit dem 01.07.2016 in allen Mitgliedsstaaten der EU die Verordnung über „elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“, kurz eIDAS. Damit ist das elektronische Signieren von Dokumenten sehr vereinfacht worden, denn die eIDAS regelt, dass eine qualifizierte elektronische Signatur die gleiche Rechtswirkung wie eine handschriftliche Unterschrift entfaltet. Folglich ist eine europaweite, grenzüberschreitende elektronische Kommunikation in rechtsverbindlicher Form möglich gemacht worden und eine Unterschrift auf Papier ist im Geschäftsalltag somit also nicht mehr vorgeschrieben.

Rechtlich gesehen steht einem vollständig digitalen Prozess also nichts mehr im Wege. Was dennoch bleibt, sind Fragen bezüglich der Umsetzung. Diese Fragen werden in diesem Whitepaper beantwortet. Außerdem klären wir hartnäckige Mythen auf und Sie erhalten Demoeinblicke, wie unsere Lösung zur digitalen Signatur aussieht und gehandhabt wird.

Definition

WAS BEDEUTET „ELEKTRONISCHE SIGNATUR“

Im Allgemeinen versteht man unter dem Begriff „elektronische Signatur“ mit elektronischen Informationen verknüpfte Daten, die eine eindeutige Identifizierung des Unterzeichners zulassen und somit zweckmäßig der eigenhändigen Unterschrift auf Papier gleichzustellen ist. Hiervon gilt es die „digitale Signatur“ zu unterscheiden.

IM IDEALFALL SOLLTE EINE ELEKTRONISCHE SIGNATUR

- die eIDAS-Verordnung, die die elektronische Identifizierung und Vertrauensdiensteanbieter für digitale Transaktionen reglementiert, einhalten.
- auf der Verwendung eines elektronischen Zertifikats beruhen.
- die Identität des Unterzeichners überprüfen.
- nachweisen, dass das Dokument seit seiner Unterzeichnung nicht mehr verändert wurde.

3 NIVEAUS DER ELEKTRONISCHEN SIGNATUR

In der EU-Verordnung werden drei verschiedene Stufen der elektronischen Signatur definiert. Der grundlegende Unterschied zwischen diesen Stufen betrifft dabei die Unverfälschbarkeit des Validierungsprozesses der Identität des Unterzeichners und damit das Niveau der Sicherheit, das mit den oben genannten Kriterien verbunden ist. Um zu wissen, welches Niveau in Ihrem Unternehmen benötigt wird, sollten Sie die drei Signatur-Niveaus und deren Unterschiede kennen.

EINFACHE ELEKTRONISCHE SIGNATUR

Die Mehrheit der erstellten elektronischen Unterschriften sind „einfache“ Signaturen, denn diese sind in Sachen Reibungslosigkeit und Nutzerfreundlichkeit unschlagbar. Diese Art von Signatur unterliegt keinen konkreten Prozess der Identitätsprüfung oder Zustimmung und die Erstellung eines Nachweisdokuments ist nicht vorgeschrieben. Als wohl bekanntestes Beispiel einer „einfachen elektronischen Signatur“ kann der Absender einer E-Mail an dieser Stelle gelistet werden. Auch eine eingescannte Unterschrift, die als Bild in ein Dokument eingefügt wird, zählt zur Kategorie „einfache elektronische Signatur“.

Verwendung: Bei Unterlagen, die routinemäßig oder mit einem begrenzten rechtlichen oder finanziellen Risiko verbunden sind, z.B. Kostenvoranschläge, Datenschutzerklärung, Dienstleistungsverträge, unbefristete Arbeitsverträge, Übergabeprotokolle (Immobilien),...

FORTGESCHRITTENE ELEKTRONISCHE SIGNATUR

Eine „fortgeschrittene elektronische Signatur“ muss unter der eIDAS festgelegte Anforderungen erfüllen:

- Sie muss eindeutig dem Unterzeichner zugeordnet sein.
- Sie muss die Identifizierung des Unterzeichners ermöglichen.
- Sie muss mit Mitteln erstellt worden sein, die der Unterzeichner unter seiner alleinigen Kontrolle hat.

Eine nachträgliche Veränderung der Daten muss ausgeschlossen, bzw. eindeutig erkennbar sein.

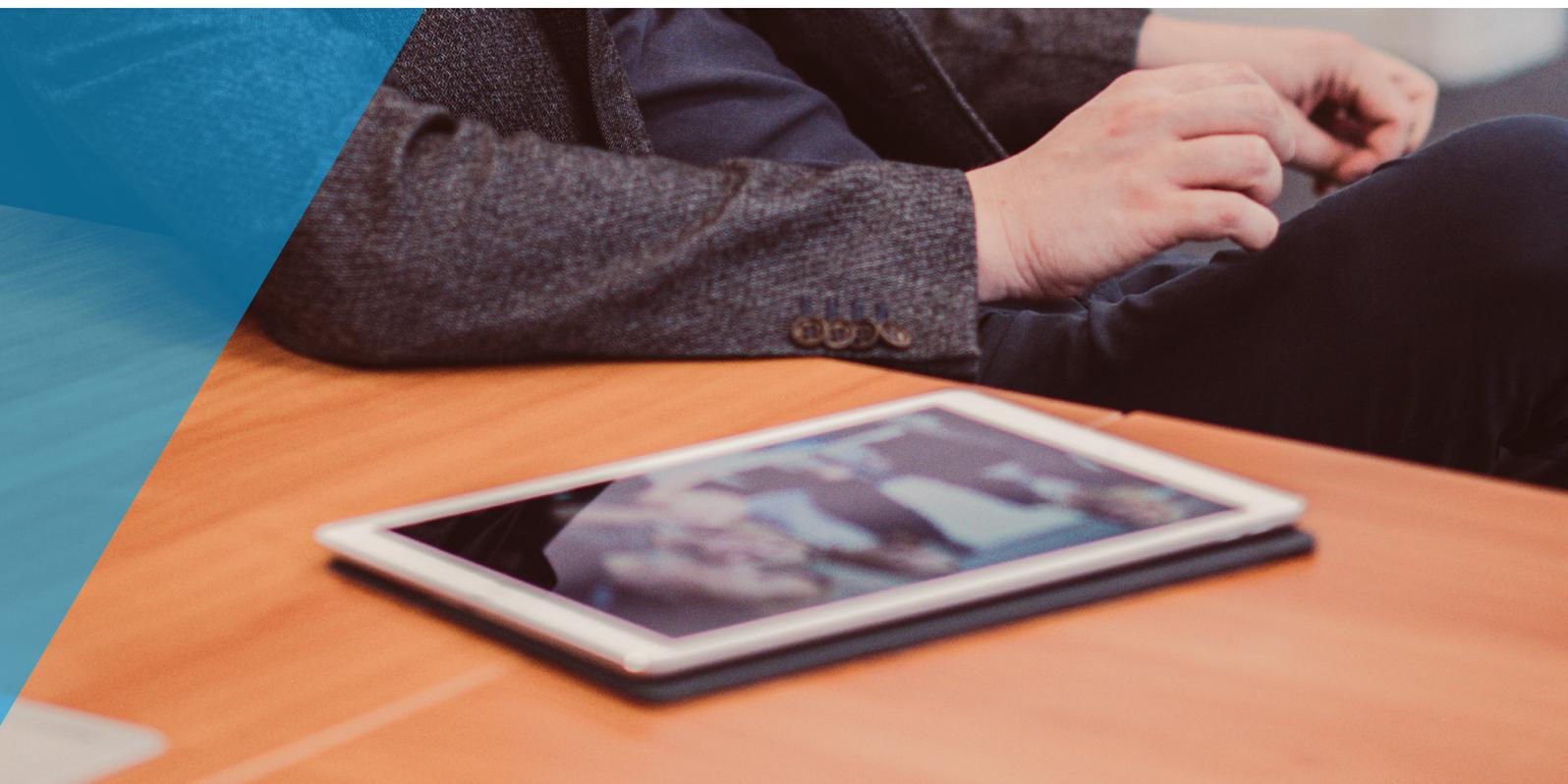
Generiert wird die Signatur mit einem einmaligen Signaturschlüssel und hat daher vor Gericht mehr Gewicht als die „einfache Signatur“.

Verwendung: Empfohlen bei der Unterzeichnung von Dokumenten, bei denen erhebliche rechtliche Risiken bestehen können, sowie für Finanztransaktionen. Zum Beispiel: Gesellschaftsvertrag, Sozialversicherungsdokumente, Personenversicherungen,...

QUALIFIZIERTE ELEKTRONISCHE SIGNATUR

Die „qualifizierte elektronische Signatur“ entspricht einer persönlichen Unterschrift und bietet so die höchste Beweiskraft vor Gericht. Voraussetzung für dieses Signatur-Niveau ist eine Identifizierung des Unterzeichners durch einen zertifizierten Vertrauensdiensteanbieter. Eine vollständige Liste aller qualifizierten Vertrauensdiensteanbieter ist auf der Webseite der Bundesnetzagentur zu finden. Aufgrund ihrer hohen Anforderungen wird diese Form der elektronischen Signatur jedoch nur in ganz bestimmten Fällen eingesetzt.

Verwendung: Geeignet für alle Transaktionen und Unternehmen, bei denen eine handschriftliche Unterschrift gesetzlich vorgeschrieben ist. Z.B. amtliche Geschäfte, Zeitarbeitsverträge, SEPA Lastschriftmandate,...



DIE DIGITALE SIGNATUR

Die Begriffe „elektronische Signatur“ und „digitale Signatur“ werden oftmals synonym verwendet, bezeichnen jedoch nicht das Gleiche.

Die „digitale Signatur“ bezieht sich auf die Verschlüsselungs- / Entschlüsselungstechnologie, auf der eine „elektronische Signatur“ basiert und hilft somit bei der Überprüfung der Authentizität eines signierten Datensatzes. Somit kann man also in Kürze sagen, dass jede „digitale Signatur“ eine „elektronische Signatur“ ist, jedoch nicht umgekehrt.

Die digitale Signatur nutzt die Public Key Infrastructure (PKI) Technologie, mit der ein privater Schlüssel erzeugt wird. Wenn also ein Benutzer ein Dokument elektronisch unterschreibt, wird mithilfe dieses Schlüssels eine Signatur erzeugt, die aus dem sogenannten Hash-Wert besteht. In Kombination mit einem Zeitstempel ist der Abgleich dieses Hash-Werts eine sehr sichere Methode, um ein Dokument auf Echtheit zu prüfen. Somit werden zwei mögliche Sicherheitslücken durch den Einsatz einer digitaler Signatur geschlossen:

1. Der Beweis der Integrität und Authentizität digitaler Daten.
2. Die Validierung der Signatur und damit die Sicherstellung, dass das Dokument nicht verändert wurde.



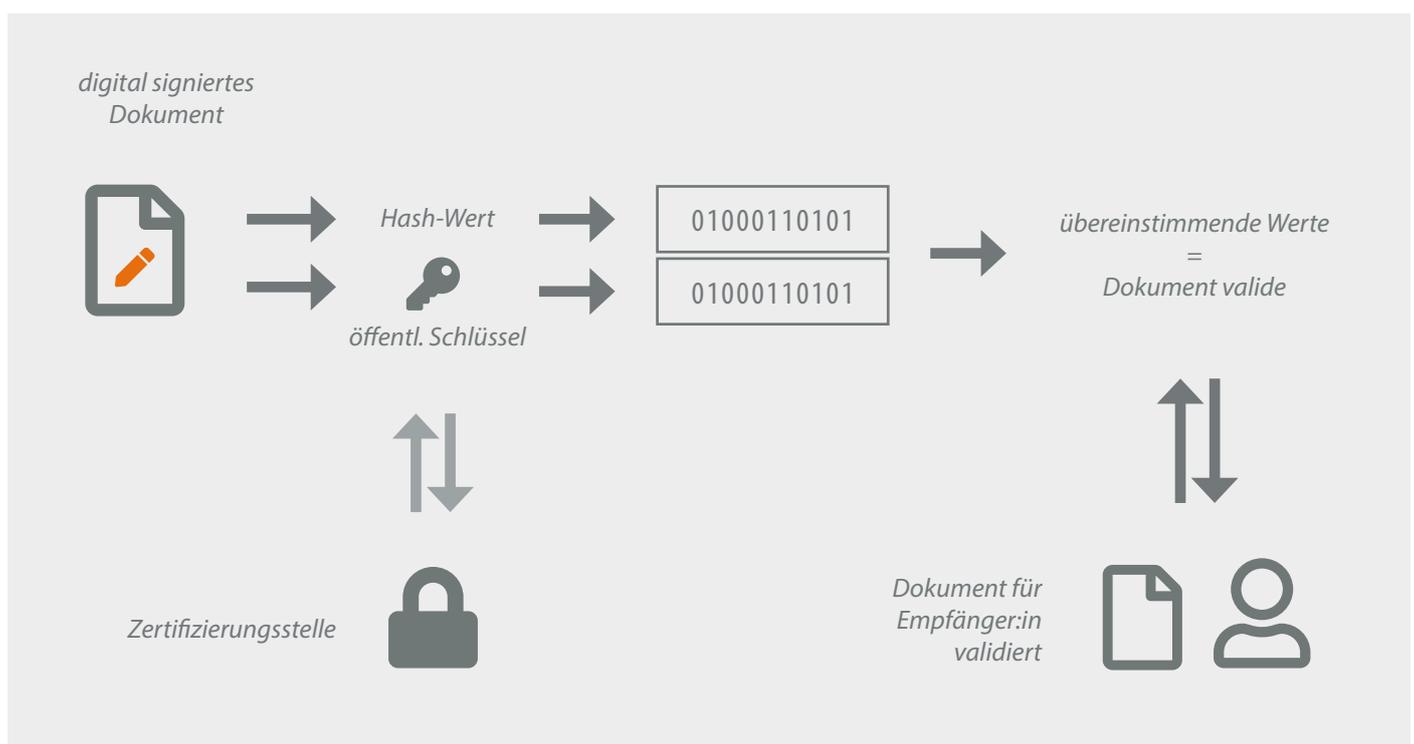
SIGNATUR-ERSTELLUNG

Der Hash-Wert wird mit dem privaten Schlüssel verschlüsselt. Dieser verschlüsselte Wert ist zusammen mit dem öffentlichen Schlüssel Bestandteil der Signatur.



SIGNATUR-VALIDIERUNG

Der verschlüsselte Hash-Wert wird mit dem öffentlichen Schlüssel entschlüsselt. Gelingt dies, so wurde offensichtlich der dazugehörige private Schlüssel zum Verschlüsseln genutzt, auf den nur der Inhaber zugreifen kann. Daraufhin wird der entschlüsselte Hash-Wert mit dem aktuellen verglichen. Bei Übereinstimmung ist die Validität nachgewiesen.



Highlights

WARUM DIGITAL SIGNIEREN?

Digital zu signieren bedeutet ressourcenschonend zu signieren, und das in jeglicher Hinsicht: um Aufwand zu minimieren, Kosten zu sparen und letztlich auch die Umwelt zu schonen. Digitale Signaturen sind die Basis für ein papierfreies Büro und für vollständig digitale Geschäftsprozesse.



PROZESSKONTROLLE.

Es ist jederzeit nachvollziehbar, auf welchem Schreibtisch ein zu unterzeichnendes Dokument liegt. Dank einem Signatur-Cockpit behalten Sie stets den Überblick wo und bei wem ein Dokument gerade steckt, was der Status ist (versendet, ausstehend, unterschrieben), den Verlauf der signierten Dokumente, das Archiv sowie die Aufzeichnung von Beweismitteln.



EINSPARUNG VON KOSTEN UND RAUM.

Schätzungsweise kostet jede Unterschrift auf Papier ein Unternehmen 5 Euro, wozu mitunter die Kosten für Papier, drucken, dokumentieren, Porto und die Ersetzung von verlorenen Dokumenten zählen. Mit der digitalen Signatur werden diese Kosten überflüssig.

Zudem entfallen Verzögerungen im Arbeitsprozess, die jeden Unternehmer bares Geld kosten. Durch verzögerte oder nicht geleistete Unterschriften verlorene Einnahmen gehören der Vergangenheit an.

Nicht zu vergessen: Dank der elektronischen Unterschrift sind physische Archive, für die nicht selten große Lagerräume bereitgestellt werden müssen, für die Aufbewahrung von Dokumenten unnötig, da nun alles digital archiviert werden kann.



VERBINDLICHKEIT.

Mündliche Vereinbarungen, die sonst in Vergessenheit geraten könnten, werden ohne großen Aufwand formal korrekt geschlossen, wodurch Verbindlichkeiten geschaffen werden. Dank unkomplizierter Handhabung dauert die digitale Signatur nur wenige Augenblicke und sorgt für stabilere Geschäftsbeziehungen.



SCHNELLIGKEIT.

Bis zu 50% schnellere Rückmeldungen können bei digitalen Signaturprozessen verzeichnet werden. Der Weg zur Unterschrift und zu schnelleren Geschäftsabschlüssen verkürzt sich erheblich, was für mehr Planungssicherheit, reibungslose Abläufe und damit mehr finanziellen Vorteile sorgt. Die Tatsache, dass dritte Personen problemlos in den Prozess eingebunden werden können, ohne besondere Zugriffe oder Software zu benötigen, sorgt außerdem für schnellere Abschlüsse.



DATEN- UND RECHTSSICHERHEIT.

Seit der eIDAS-Verordnung sind qualifizierte elektronische Signaturen der händischen Unterschrift auf Papier hinsichtlich Rechtsgültigkeit und Sicherheit ebenbürtig. Aufgrund des nachvollziehbaren Signaturprozesses sind sie hinsichtlich Sicherheit sogar einen Schritt voraus.



SCHONUNG DER UMWELT.

Durch die elektronische Unterschrift ist es nicht mehr nötig, Papier zu verwenden. 100 Blatt Papier stehen für den Verbrauch von 1081,49 Liter Wasser, 45,36 kg Holz und 10,89 kg an Abfällen.



EFFIZIENZGEWINN.

Auf lange Postwege wird verzichtet. Scannen, drucken, und mailen wird überflüssig. Verzögerungen gehören der Vergangenheit an. Stattdessen sind schnellere Vertragsabschlüsse die Folge.

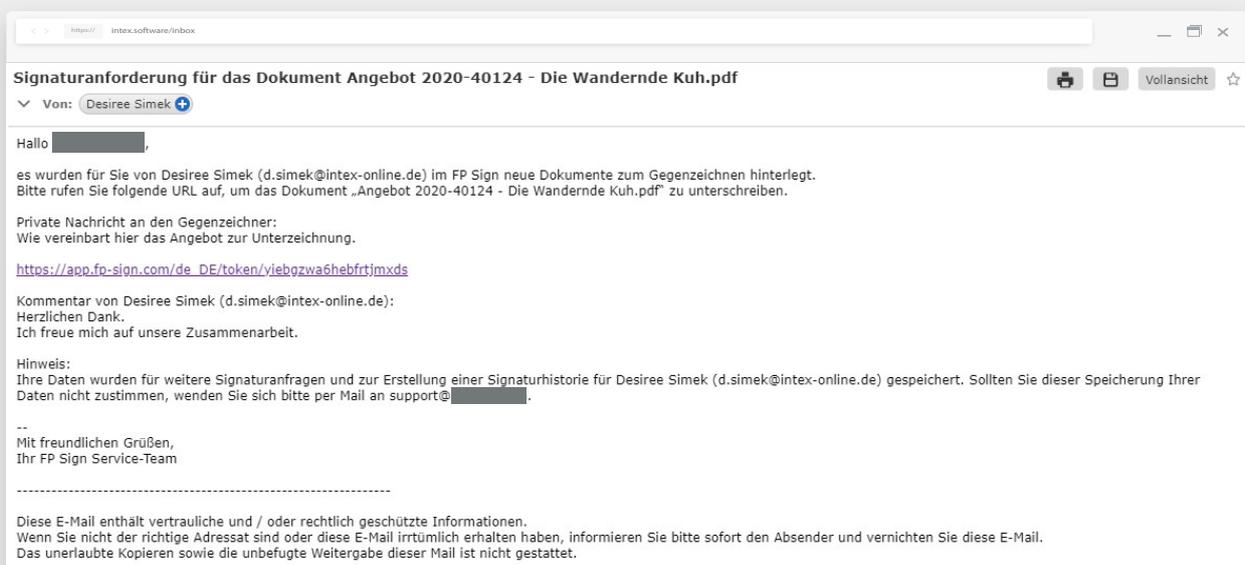
Im ersten Schritt wird das zu unterzeichnende Dokument hochgeladen. Das ausgewählte Dokument wird Ihnen in der Dokumentenvorschau auf der rechten Seite angezeigt. Optional können weitere Anlagen hochgeladen werden, beispielsweise AGBs, um diese dem Empfänger als zusätzliche Information zukommen zu lassen. Im nächsten Schritt werden die Einstellungen für Ihre Signaturanfrage vorgenommen. Es kann zwischen den Optionen „Lesebestätigung ohne Unterschrift“ und „Signieren / Unterzeichnen“ gewählt werden. Im Falle, dass Sie selbst das Dokument ebenfalls unterzeichnen möchten, wird die Option „Signieren / Unterzeichnen“ gewählt. An dieser Stelle könnte auch das Firmenlogo als graphische Signatur genutzt werden.

Im dritten Schritt wird ein oder mehrere Empfänger der Anfrage bestimmt. Hier kann u.a. auch die Sprache gewählt werden, in der der Empfänger angesprochen und durch den Signaturprozess geführt werden soll.

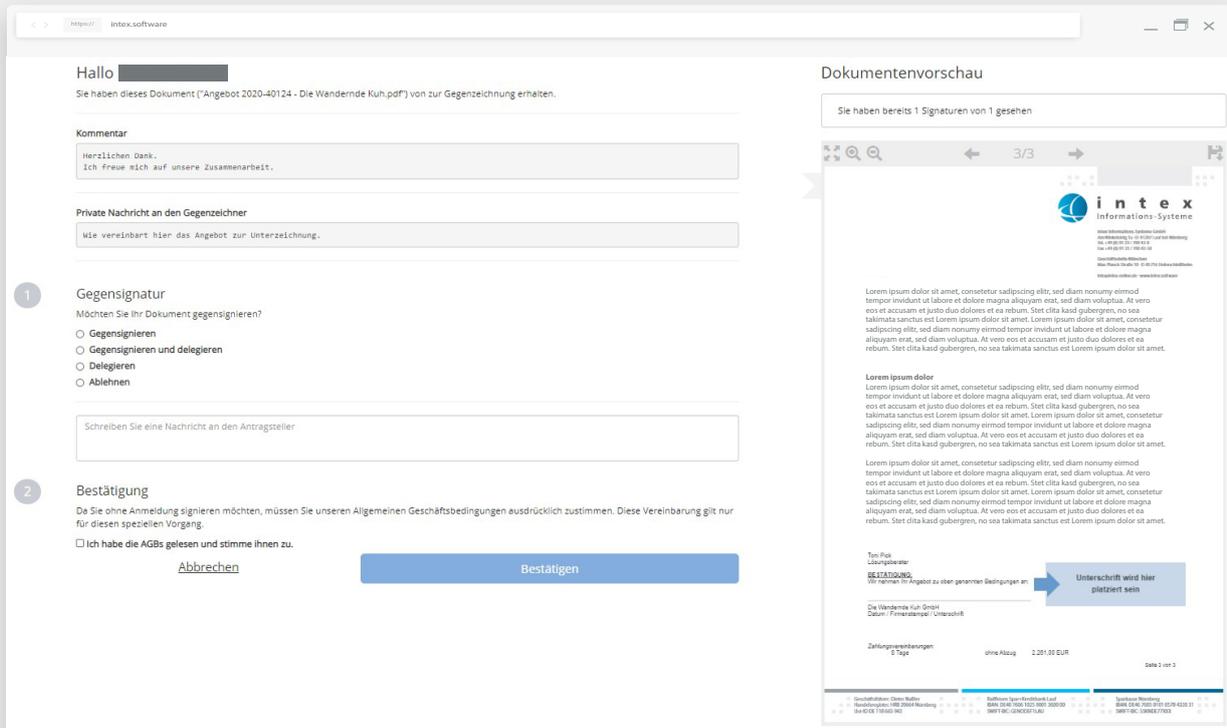
Im Weiteren wird ausgewählt, wer bei vollendetem Signaturprozess benachrichtigt werden soll. Nachdem alle Angaben gemacht wurden, kann die Anfrage versendet werden.

DOKUMENTE GEGENZEICHNEN

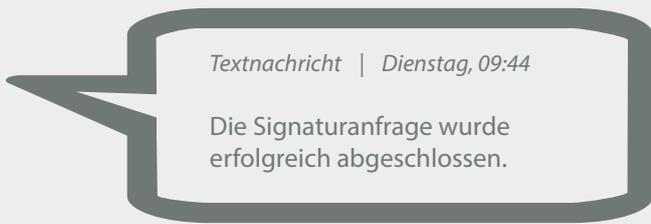
Nach dem Versenden eines Dokuments durch den Absender, erhält der Empfänger eine Signatur-Anforderung per E-Mail. Sie enthält eine Mitteilung darüber, dass der Absender ein Dokument zum Gegenzeichnen hinterlegt hat, welches über einen Link aufgerufen und schließlich gegensigniert werden kann.



Nach Aufrufen des Links öffnet sich die Lösung im Browser. Auf der rechten Seite wird eine Vorschau des Dokuments, das unterzeichnet werden soll, angezeigt. Der Empfänger hat die Wahl, ob er das Dokument gegensignieren, delegieren oder ablehnen will. Das Gegensignieren ist einfach gestaltet. Der Empfänger hat die Wahl eine generierte Unterschrift auszuwählen, oder eine eigene, eingescannte Signatur hochzuladen. Die gewählte Unterschrift wird dann an der gewünschten Stelle platziert.



Nach abgeschlossenem Prozess werden alle Teilnehmer des Signatur-Prozesses per E-Mail (oder falls gewünscht auch per SMS) benachrichtigt, dass der Prozess abgeschlossen ist und ob das Dokument gegengezeichnet wurde.



KOSTENLOSER TESTZUGANG



Wir geben Ihnen die Möglichkeit, die Lösung völlig **kostenfrei und unverbindlich für 30 Tage zu testen**. Für Sie entstehen keine Verpflichtungen und es sind keine Kreditkarten oder Zahlungsdaten notwendig. Nach 30 Tagen endet der Test automatisch. Sprechen Sie uns einfach an!

Q & A

WICHTIGE FRAGEN & ANTWORTEN IN KÜRZE.

WELCHE DATEIFORMATE KÖNNEN MIT DER LÖSUNG SIGNIERT WERDEN?

Alle bekannten Formate können hochgeladen werden. Diese werden dann stets zur PDF umgewandelt, da dies ein unveränderliches Dateiformat ist und somit standardmäßig in unserer Lösung genutzt wird.

IN WELCHEN SPRACHEN IST DIE LÖSUNG VERFÜGBAR?

Ihr Profil können Sie in den Sprachen Deutsch, Englisch, Französisch, Niederländisch, Spanisch, Italienisch und Schwedisch pflegen. Für jeden Empfänger kann einzeln eingestellt werden, in welcher Sprache die Anwendung für ihn angezeigt werden soll. Hier kann aus 12 Sprachen gewählt werden.

WELCHE MÖGLICHKEITEN HABE ICH, EIN DOKUMENT ZU SIGNIEREN UND ZU VERSENDEN? WELCHE INTEGRATIONSMÖGLICHKEITEN GIBT ES?

Signaturen können einfach und intuitiv in der Browseranwendung gesetzt werden, sowie mithilfe einer mobilen App, die auf iOS und Android installiert werden kann.

Desweiteren kann die Lösung allgemeingültig in Documents integriert werden. So ist es beispielsweise möglich direkt aus Ihrer Lösung für digitale Vertragsverwaltung ein Dokument an Dritte zum Gegenzeichnen zu versenden. Andere Beispiele wären die digitale Unterzeichnung von Reisekostenabrechnungen oder Tätigkeitsnachweisen direkt aus Documents. Für weitere Integrationsmöglichkeiten kontaktieren Sie uns gerne!

GEMEINSAM DIGITAL SIGNIEREN & RESSOURCEN SCHONEN



Wir bei intex setzen die digitale Signatur bereits ein. Sie erspart uns administrativen Aufwand und beschleunigt Prozesse ungemein. Was uns an der Lösung am meisten begeistert ist die Tatsache, dass wir damit aktiv und jeden Tag aufs Neue unsere Umwelt schonen, indem wir auf Ausdrücke und physischen Transport von Dokumenten verzichten.

Doch damit nicht genug. intex hat sich entschieden, für jede digitale Unterschrift einen Beitrag zum Umweltschutz zu leisten: Für jede Unterschrift, die in unserem Jubiläumsjahr 2021 geleistet wird, sei sie intern, mit Geschäftspartnern oder Kunden, spenden wir einen Betrag von 2€ an die deutsche Klimaschutzorganisation *GermanZero*.

GermanZero setzt sich dafür ein, dass Deutschland bis 2035 klimaneutral wird. Sie helfen der Politik, das Versprechen der UN-Klimakonferenz von Paris einzuhalten: mit einem wirksamen 1,5 Grad-Klimaschutzgesetz. [Neugierig? Besuchen Sie die Webseite www.germanzero.de für weitere Infos.]

So tragen wir – gemeinsam mit Ihnen und jeden Tag aufs Neue – zum Schutz unserer Umwelt und dem Erreichen des Klimaziels bei.

Mythen aufgeklärt!

DIE VIER HÄUFIGSTEN IRRGLAUBEN.

Auch wenn die eIDAS-Verordnung schon seit geraumer Zeit verabschiedet ist, ranken sich noch immer zahlreiche Mythen und Irrglauben um die elektronische Unterschrift. Wir möchten die am meisten gestellten Fragen beantworten und mit den häufigsten Irrtümern aufräumen.

IRRTUM 1

FÜR DIE ELEKTRONISCHE SIGNATUR BENÖTIGT MAN EIN KARTENLESEGERÄT.

Seit der Einführung der eIDAS-Verordnung sind Hardware-Applikationen nicht mehr von Nöten. Stattdessen kommt die sogenannte Fernsignatur ins Spiel, was ein deutlich einfacheres Verfahren für die Erstellung einer Signatur ist: Die für die Signatur benötigten privaten Signaturschlüssel werden auf den Servern eines Vertrauensdienstanbieters generiert – also aus der Ferne. Das ermöglicht die sichere, mobile Signatur vom Laptop, Smartphone oder Tablet und macht Kartenlesegeräte, zusätzliche Software oder Signaturkarten bzw. Chipkarten überflüssig.

IRRTUM 2

WENN MEINE GESCHÄFTSPARTNER SELBST KEINEN EIGENEN ACCOUNT BEI EINEM ANBIETER FÜR ELEKTRONISCHE SIGNATUREN VERWENDEN, KÖNNEN SIE NICHT UNTERSCHREIBEN.

Dies ist ein sehr hartnäckiger Mythos. Unsere Signaturlösung ermöglicht einen unkomplizierten Signaturprozess, in dem vom Signaturempfänger kein eigener Account verlangt wird, um ein Dokument elektronisch zu signieren. Es reicht aus, wenn der Initiator der Signatur einen Account bei seinem Wunsch-Vertrauensdienstanbieter besitzt. Etwas anders verhält es sich, wenn beide Unterschriftsparteien auf höchstmöglicher Rechtsgültigkeit ihrer Vereinbarung bestehen oder das zu unterschreibende Dokument die Schriftform erfordert: Hierzu muss die „qualifizierte elektronische Signatur“ zum Einsatz kommen, was bedeutet dass alle Unterzeichner im Besitz einer QES sein und sich an deren Identifizierungs- und Authentifizierungsanforderungen halten müssen.

IRRTUM 3

ELEKTRONISCHE SIGNATUREN SIND LEDIGLICH EIN ABBILD EINER EIGENHÄNDIGEN UNTERSCHRIFT.

Der Irrglaube, dass die elektronische Signatur nur ein optischer Platzhalter für die eigene handschriftliche Unterschrift auf digitalen Dokumenten sei, hält sich hartnäckig. Doch die elektronische Signatur ist keinerlei eine Bilddatei, sondern vielmehr ein kryptografisches Verfahren: Die Information zur Person und der sogenannte Hash-Wert des Dokumentes (einmalige mathematische Quersumme) werden mithilfe eines digitalen Zertifikates berechnet und verschlüsselt. So wird die Signatur untrennbar mit dem elektronischen Dokument verbunden und die Integrität des Dokumentes gesichert. Dieses Verfahren begleitet das Unterschreiben mittels der sogenannten fortgeschrittenen (AES) und der qualifizierten elektronischen Signatur (QES).

Beim elektronischen Signieren etwa mit einer gescannten Unterschrift ohne dieses Verschlüsselungsverfahren ist dagegen die Rede von einer einfachen Signatur. Diese weist eine deutlich niedrigere Beweiskraft und Sicherheit des Signierprozesses auf und ist in diesem Sinne nicht der fortgeschrittenen und der qualifizierten elektronischen Signatur gleichgestellt. Weitere Informationen zu den unterschiedlichen Signatur-Niveaus sind im Kapitel „3 Niveaus der elektronischen Signatur“ nachzulesen.

IRRTUM 4

BELIEBIGE PERSONEN KÖNNEN MIT BELIEBIGEN NAMEN UNTERSCHREIBEN.

Je höher das Niveau der elektronischen Unterschrift, umso höher sind die Anforderungen, die der Unterzeichner in seine Identifizierung investieren muss. Eine QES setzt beispielsweise ein einmaliges Identifizieren durch einen Vertrauensdiensteanbieter voraus, was mittels Video-Ident-Verfahren oder die Online-Ausweisfunktion des Personalausweises vorstattengehen kann. Hiernach wird bei jeder weiteren Anwendung der Signatur die Identität über eine Zwei-Faktor-Authentifizierung bestätigt, welche aus einem Login mit Passwort sowie einer SMS-Tan bestehen kann. Desweiteren werden dank des nachvollziehbaren Signaturprozesses nachträgliche Änderungen betreffender Dokumente sichtbar gemacht. Diese strengen Authentifizierungsverfahren und Prozessnachverfolgungen machen es nahezu unmöglich, eine elektronische Signatur zu fälschen und unbefugt im Namen anderer Personen zu unterzeichnen.

Besuchen Sie uns auch
auf unseren
sozialen Netzwerken:



Wir sind für Sie da:

Zentrale:

*intex Informations-Systeme GmbH
Am Winkelsteig 1a
D-91207 Lauf a. d. Pegnitz*

Tel: +49 (0) 9123 / 700 43-0

Fax: +49 (0) 9123 / 700 43-50

Geschäftsstelle München:

*intex Informations-Systeme GmbH
Max-Planck-Straße 10
D-85716 Unterschleißheim*

Tel: +49 (0) 89 / 89 06 58 1-0

Fax: +49 (0) 89 / 89 06 58 1-29

web: www.intex.software

mail: info@intex-online.de