

Digitales Vertrauen, von dem Sie profitieren

Mit unserer hochflexiblen Lösung können Sie jederzeit und von überall auf jedem modernen Mobilgerät signieren. Die Lösung umfasst digitale Identitäten, Zertifikate, Technologien und Automatisierungsoptionen, die für vertrauenswürdige digitale Dokumente sorgen. Hier die wichtigsten Vorzüge von Document Trust Manager im Überblick:

Einhaltung gesetzlicher Vorgaben rings um den Erdball

In vielen Ländern sind digitale Signaturen mit hohem Sicherheitsgrad gesetzlich vorgeschrieben, basierend auf Zertifikaten, die von einem im jeweiligen Land zugelassenen Vertrauensdiensteanbieter (VDA) ausgestellt wurden. So kann etwa eine qualifizierte elektronische Signatur in der EU, Großbritannien oder der Schweiz nur von einem qualifizierten Vertrauensdiensteanbieter (qVDA) wie DigiCert ausgestellt werden. Hochsichere digitale Signaturen von DigiCert

Digitale Signaturen

Eine digitale Signatur ist eine elektronische Unterschrift basierend auf einem digitalen Zertifikat, das über eine Public Key Infrastructure (PKI) kryptografisch mit dem Signaturfeld verknüpft ist. Jedes digitale Zertifikat – oft auch als digitale Identität bezeichnet – ist personengebunden und wird seinem Inhaber nach einer Identitätsprüfung zugewiesen.

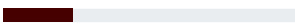


Elektronische Siegel

Ein elektronisches Siegel ist eine digitale Signatur, die von einer juristischen Unternehmen vertrauenswürdige digitale Signaturen, elektronische Siegel und Zeitstempel anfordern, die für vielfältige Anwendungsbereiche geeignet sind und den branchenspezifischen und rechtlichen Vorschriften in den USA, der Europäischen Union, Großbritannien, der Schweiz und vielen anderen Ländern der Welt entsprechen.

Starke elektronische Signaturen

Elektronische Signatur ist nicht gleich elektronische Signatur. Tatsächlich reicht das Spektrum von einfachen Kontrollkästchen und auf Tablets gezeichneten Bildunterschriften bis zu Signaturen mit hohem Vertrauensgrad in der Cloud, denen eine strenge Identitätsprüfung durch eine akkreditierte Zertifizierungsstelle wie DigiCert zugrunde liegt. Zuverlässige digitale Signaturen, die den Unterzeichner zweifelsfrei mit einem bestimmten Dokument verknüpfen, können dazu beitragen, wichtige elektronische Transaktionen zu schützen – auch grenzüberschreitend.

Die unten stehende Tabelle gibt einen Überblick über verschiedene Typen von Signaturen und deren Merkmale, Sicherheitsniveau und rechtlichen Status:

Art der Signatur	Elektronische Signatur	Digitale Signatur (AATL-konform)	Digitale Signatur (reguliert/qualifiziert)
	Ein Überbegriff, der alle elektronischen Prozesse für das Akzeptieren einer Vereinbarung oder eines Protokolls umfasst. In ihrer einfachsten Variante kann es sich bei einer elektronischen Signatur um einen getippten Namen oder ein Häkchen in einer Checkbox handeln.	Eine sicherere elektronische Signatur erfordert eine von einem Vertrauensdiensteanbieter (VDA) ausgegebene digitale Identität, die den Anforderungen der Adobe Approved Trust List (AATL) an Identitätsverifizierung und Sicherheit entspricht.	Eine hochsichere elektronische Signatur erfordert eine regulierte, von einem Vertrauensdiensteanbieter (VDA) ausgegebene digitale Identität. Dieser VDA muss zur Ausstellung dieser Identitäten in einer bestimmten Region zertifiziert sein – dazu zählen unter anderem qualifizierte Vertrauensdiensteanbieter (qVDA) in der EU oder der Schweiz.
	keine Anforderungen	von Adobe Acrobat und Reader als vertrauenswürdig eingestuft	von Adobe Acrobat und Reader als vertrauenswürdig eingestuft
	keine einzigartige digitale Identität erforderlich	Nachweis der einzigartigen digitalen Identität des Unterzeichners erforderlich, die kryptografisch über PKI an das Signaturfeld gebunden sein muss	Nachweis der einzigartigen digitalen Identität des Unterzeichners erforderlich, die kryptografisch über PKI an das Signaturfeld gebunden sein muss
	limitierte oder wenig strikte Identitätsprüfung 	Identitätsprüfung erforderlich 	gründliche Identitätsprüfung (persönlich oder ähnlich) erforderlich 
	nicht erforderlich	für das Signieren des Dokuments erforderlich	für das Signieren des Dokuments erforderlich
	nicht erforderlich; kann einigen Signatur-Workflow-Lösungen hinzugefügt werden	Signierte Dokumente werden mit einem manipulationssicheren Siegel und Zeitstempel versehen	Signierte Dokumente werden mit einem manipulationssicheren Siegel und Zeitstempel versehen

Verlässlicher Identitätsnachweis

Sicherer Beleg für die Identität des Unterzeichners, den Signierzeitpunkt und die Authentizität des Dokuments durch eine kryptografische Verbindung zu unterzeichneten Verträgen

Skalierbare Integrationen

Kompatibel mit führenden digitalen Signierlösungen wie Adobe Acrobat Sign, Ascertia SigningHub und DocuSign

Identitätsprüfung aus der Ferne

Zur zweifelsfreien Identifizierung von Kunden, Bürgern und Mitarbeitern mithilfe von Ausweisdokumenten und modernen Mobilgeräten

Flexible Bereitstellungsoptionen

Schutz Ihrer digitalen Dokumente

Immer mehr Unternehmen setzen auf digitale Dokumente statt papiergebundener Prozesse und nutzen daher vertrauenswürdige elektronische Siegel, um ihre digitalen Dokumente zu authentifizieren. In Kombination mit digitalen Signaturen mit hohem Vertrauensgrad tragen elektronische Siegel dazu bei, Dokumente wie Verträge und die zugrunde liegenden elektronischen Transaktionen gegen Cyberangriffe oder Betrug abzusichern.

Mit Document Trust Manager können Sie sicherstellen, dass alle Ihre Dokumente mit elektronischen Siegeln, Zeitstempeln und digitalen Signaturen auf der Grundlage strenger Identitätsprüfungen geschützt sind.

DigiCert ONE Die Plattform für digitales Vertrauen

DigiCert Document Trust Manager ist Teil der Plattform DigiCert ONE, die alle DigiCert-Lösungen für digitales Vertrauen auf einer modernen, containerisierten Architektur vereinheitlicht. Die Plattform punktet mit hoher Skalierbarkeit, flexibler Bereitstellung, schneller Amortisierung und einheitlichem PKI-Management.

Gleich loslegen

Legen Sie noch heute los mit DigiCert® Document Trust Manager – wenden Sie sich einfach an Ihren Account Manager bei DigiCert oder per E-Mail an sales@digicert.com.

Über DigiCert Inc.

Als einer der weltweit führenden Anbieter digitaler Vertrauenslösungen sorgt DigiCert dafür, dass Unternehmen und Einzelpersonen digitalen Interaktionen in dem Wissen vertrauen können, dass ihre digitale Infrastruktur und ihre Anbindung an eine Welt voller Online-Transaktionen sicher und geschützt sind. DigiCert® ONE, die Plattform für digitale Vertrauensdienste, bietet Unternehmen eine zentrale Anlaufstelle für Einblicke und die Kontrolle über eine Vielzahl von öffentlichen und privaten Anwendungsbereichen, in denen das Vertrauen eine wichtige Rolle spielt. Dazu gehören der sichere Zugriff auf Unternehmenssysteme, sichere Business-Kommunikation sowie der Schutz von Webseiten, Software, Identitäten, Inhalten und Geräten. DigiCert bietet nicht nur preisgekrönte Softwarelösungen an, sondern hat sich nicht zuletzt auch durch seine branchenweite Führungsrolle bei Standards, Support und Betrieb als bevorzugter Anbieter digitaler Vertrauenslösungen bei Unternehmen auf der ganzen Welt einen Namen gemacht. Weitere Informationen finden Sie unter digicert.com/de oder auf Twitter unter [@digicert](https://twitter.com/digicert).