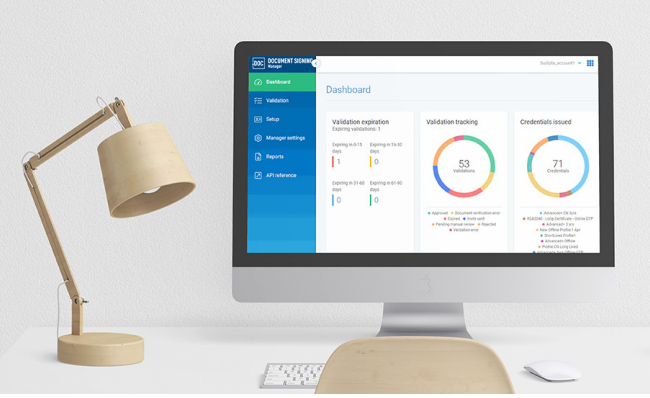
UNTERNEHMERISCHE UND RECHTLICHE COMPLIANCE AUF HÖCHSTEM NIVEAU

Vertrauen und Identitätsschutz als zentrale Merkmale digitaler Dokumente

Papierunterlagen werden zunehmend durch digitale Dokumente ersetzt. Deshalb sind vertrauenswürdige Signaturlösungen gefragter denn je. Ohne Vertrauensdienste gibt es keine Sicherheit bezüglich der Identität von juristischen und natürlichen Personen. Für Unternehmen, Behörden und Privatpersonen entsteht in solchen Fällen das Risiko von Betrug und Manipulation im Kontext von Transaktionen und Verträgen.

DigiCert Document Signing Manager sorgt für Identitätsschutz und Vertrauen

Obwohl sich digitale Unterschriften immer mehr durchsetzen, bieten nicht alle Lösungen den gleichen Schutz. DigiCert Document Signing Manager basiert auf einer PKI (Public Key Infrastructure), einer bewährten Technologie für Verschlüsselung, Authentifizierung und Identitätsprüfung. Mit Document Signing Manager wird ein Dokument nicht nur kryptografisch verifizierbar signiert, sondern auch soweit geschützt, dass die Identität des Unterzeichners zweifelsfrei feststeht und dass das Dokument nach dem Signiervorgang nicht mehr geändert werden kann.



Was ist ein qualifizierter Vertrauensdienstanbieter?

Die für Signaturdienste verbindlichen Vorschriften der EU und des ETSI (Europäisches Institut für Telekommunikationsnormen) sind die weltweit strengsten Normen rund um die elektronische Identifizierung und digitale Unterschriften. Das höchste Sicherheitsniveau nach diesem Standard bieten qualifizierte Vertrauensdienstanbieter (qVDA) oder Qualified Trust Service Provider (QTSP). Durch die Übernahme von QuoVadis wird DigiCert von der EU und dem ETSI als Anbieter eIDAS-konformer Vertrauensdienste anerkannt und ist somit einer der wenigen global tätigen qVDA. DigiCert erfüllt zudem alle Anforderungen an qualifizierte elektronische Signaturen gemäß dem Schweizer Bundesgesetz über die elektronische Signatur (ZertES).

Die mit den Lösungen von DigiCert+QuoVadis erstellten Signaturen sind einer handschriftlichen Unterschrift gleichgestellt. Die signierten Dokumente werden vielerorts auch als Identitätsnachweis anerkannt, der mit einem amtlichen Ausweis vergleichbar ist.

Als qVDA erfüllt und übertrifft DigiCert mit seinen Signaturlösungen rund um den Globus die höchsten Standards für Sicherheit, Authentifizierung und elektronische Identifizierung.

Unterschiedliche Sicherheitsgrade für verschiedene Dokumenttypen

Je nach gefordertem Sicherheitsgrad unterscheiden sich anerkannte digitale Signaturen hinsichtlich der spezifizierten Anforderungen und des Umfangs der Validierung.

Art der Signatur	**Einfache elektronische Signatur (EES)**	**Fortgeschrittene elektronische Signatur (FES/AATL)**	**Qualifizierte elektronische Signatur (QES)**
Anforderungen an die Signatur	Durch diese elektronische Signatur bringt der Unterzeichner seine Bestätigung oder Zustimmung zum Ausdruck. Mögliche Formate sind etwa ein gescanntes Bild der handschriftlichen Unterschrift oder das Klicken auf den Button „Ich stimme zu“.	Diese digitale Signatur erfüllt bestimmte Anforderungen und bietet mehr Sicherheit hinsichtlich der tatsächlichen Identität des Unterzeichners und mehr Schutz vor Manipulationen.	Diese digitale Signatur erfüllt höchste Anforderungen. Sie wird von einem qualifizierten Vertrauensdienstanbieter (qVDA) bereitgestellt, der in der Vertrauensliste der Schweiz oder der EU geführt wird und von einem Mitgliedsstaat zertifiziert wurde. Signaturen dieser Art sind in der Regel einer eigenhändigen Unterschrift gleichgestellt.
Anforderungen an die Signatursicherheit und elektronische Identifizierung des Unterzeichners	Keine	Signatur ist einem bestimmten Unterzeichner zuordenbar. Unterzeichner ist anhand von (ungeprüften) Ausweisdaten identifizierbar. Die zur Erstellung der Signatur genutzten Identitätsdaten unterliegen der alleinigen Kontrolle des Unterzeichners. Nachträgliche Änderungen der signierten Daten sind nachvollziehbar. Signatur entspricht den Anforderungen der Adobe Approved Trust List (AATL).	Der qVDA ist verpflichtet, die Identität des Unterzeichners zu überprüfen: 1. Die Daten der elektronischen Signatur sind sicher und vertraulich. 2. Die Identität des Unterzeichners kann vom qVDA durch eine Gegenüberstellung oder eine ähnlich zuverlässige Identitätsprüfung nachgewiesen werden.
Beispiele	Unterschriften von Mitarbeitenden während der Neueinstellung Handelsverträge zwischen Unternehmen Verträge mit Verbrauchern Lizenzvereinbarungen (Software)	Verbraucherkredit oder Darlehensvertrag Arbeitsrechtliche Kollektivverträge Arbeitsvertrag zwischen Agentur und Mitarbeiter	Verträge über die Vermietung, Übertragung oder den Kauf von Immobilien Familienrechtliche Dokumente Gründungsdokumente einer GmbH
Sicherheitsniveau gemäß eIDAS	Eher unsicher	Ziemlich sicher	Extrem sicher
Validierungsstufe	Keine Validierung	Gewisse Validierung	Sorgfältige Validierung

Zwei Arten der Signatur

Privater Unterzeichner (E-Signatur)

Eine natürliche Person kann als privater Unterzeichner einfach und sicher Dokumente wie Verträge über Immobiliengeschäfte, Bankkonten und vertrauliche Informationen wie Patientenakten signieren.

Zeichnungsbevollmächtigter (E-Siegel)

Ein Zeichnungsbevollmächtigter kann im Namen von juristischen Personen wie Unternehmen oder Behörden Unterschriften leisten. Optional sind auch Massensignaturen möglich. Zudem wird das Dokument durch die Signatur vor Manipulation und Fälschung geschützt.

Vorsprung durch digitale Signaturen

Geben Sie Ihren Kunden die Möglichkeit, jederzeit und überall digital zu unterschreiben. Unsere Komplettlösung umfasst Zertifikate, Technologien und Automatisierungsfunktionen, die Ihnen Wettbewerbsvorteile verschaffen und die Zufriedenheit Ihrer Kunden steigern werden.

Funktionsmerkmale

Individuelle Signatur-Workflows
Sie können komplexe Abläufe mit mehreren Technologien wie Ascertia SigningHub, Adobe Sign oder DocuSign definieren.

Problemlose Validierung
Mit DigiCert Verify powered by IDnow können Sie die Identität Ihrer Kunden in wenigen Minuten aus der Ferne überprüfen.

Einfachere Schlüsselverwaltung
Ihre Schlüssel werden auf einer qualifizierten Signaturerstellungseinheit (QSEE) gespeichert und in einer vertrauenswürdigen Umgebung gehostet.

Effiziente Administration
Administratoren profitieren von einer zentralen Richtlinie und Kontrollfunktionen für Nutzer und Unterzeichner.

Detailliertes Tracking
Berichte und Prüfpfade liefern eine solide Basis für die Einhaltung von Unternehmensrichtlinien und gesetzlichen Vorschriften.

Mehr Sicherheit
2FA-Unterstützung (Zwei-Faktor-Authentifizierung) ermöglicht eine sichere Anmeldung.

Einfache Integration
Sie können Webservices und Drittlösungen einbinden, z. B. Adobe Sign, Ascertia SigningHub und mehr.

Flexible Bereitstellungsoptionen
Die Lösung kann gehostet oder lokal bereitgestellt werden.

Wichtige Vorteile

- Kosteneinsparungen in den Bereichen Bürobedarf, Verwaltung und Porto
- Stärkere Kundenbindung und mehr Zufriedenheit dank vereinfachter Registrierungs- und Signierverfahren
- Reduzierung des Zeitaufwands bei unterschriftspflichtigen Transaktionen (wenige Minuten statt mehrerer Tage)
- Erhöhte Sicherheit bei hohen Transaktionssummen
- Mehr Vertrauen durch rechtsgültige Signaturen
- Wettbewerbsvorteile und Sicherung der Geschäftskontinuität
- Einhaltung globaler und branchenspezifischer Richtlinien und Vorschriften

Technische Daten und Integrationsmöglichkeiten

Signaturprotokolle

- Rest API
- CSC API

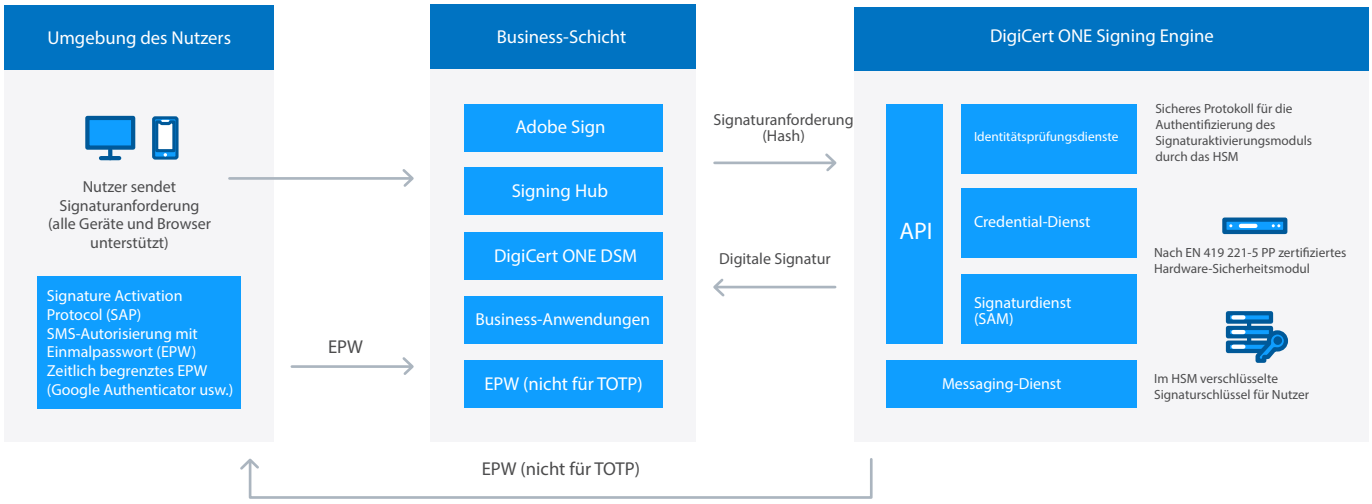
Mögliche Integrationen

- Adobe Sign
- Ascertia SigningHub
- DocuSign

Kompatibel mit

- Microsoft Office®
- Adobe® Acrobat und Adobe Reader
- LibreOffice®
- Open Office™
- Externen Lösungen wie DocuSign
- Verschiedenen Dateitypen wie PDF, ODF, DOCX und XML

Cloudbasierte Architektur für Fernsignaturen



DigiCert® ONE

Document Signing Manager basiert auf DigiCert ONE, einer modernen und ganzheitlichen Lösung für PKI-Management. Die innovative, containerbasierte Architektur von DigiCert ONE ermöglicht eine schnelle Bereitstellung in jeder Umgebung. So lassen sich neue Dienste in einem Bruchteil der Zeit einführen und Nutzer- und Gerätezertifikate jeder Größenordnung problemlos verwalten.

Falls Sie Fragen zu DigiCert® Document Signing Manager haben, wenden Sie sich unter docsigning@digicert.com an unsere PKI-Experten für elektronische Signaturen.

Bewährter Marktführer in Sachen PKI

DigiCert steht für mehr Sicherheit im Internet. Dieses Ziel prägt unsere gesamte Unternehmensgeschichte bis heute. Und genau das ist der Grund, warum führende Unternehmen auf der ganzen Welt unseren Lösungen vertrauen, unsere Zertifikate täglich milliardenfach genutzt werden und warum unsere Kunden unsere Services und unseren Support so oft mit fünf Sternen bewerten. Das ist auch der Grund, weshalb wir weiterhin in unserer Branche Maßstäbe setzen werden. So stellen wir sicher, dass DigiCert auch in Zukunft eine Vorreiterrolle bei der Entwicklung innovativer SSL-, IoT- und PKI-Lösungen einnimmt.