DigiCert® Document Trust Manager

Govern every digital signature—centrally.

Overview / About

DigiCert Document Trust Manager brings certificate-backed trust to everyday document workflows. Built on the DigiCert ONE platform, it lets organizations sign with high-assurance eSignatures and eSeals, apply trusted timestamps, and manage signer identity and policy. All this from a single, scalable service that works inside the tools people already use, like DocuSign, Adobe Sign, Adobe Acrobat, and cloud-native integrations. Document Trust Manager supports both simple eSigning and regulated, high-assurance use cases across regions and industries in a secure, non-repudiable, and compliant way.

Key Benefits

Transforming paper-based workflows into digital processes can reduce costs by up to 70%. Organizations that move from wet signatures and manual processing to PKI-backed digital signing report major operational and financial benefits.

- Establish verifiable provenance and authorship for digital assets
- Detect and prevent tampering or misuse across distributed ecosystems
- Comply with content-authenticity and attestation standards such as AATL, Time Stamping, and eIDAS 2.0
- Integrate seamlessly with document creation and publishing workflows

How DigiCert Document Trust Manager Works

DigiCert Document Trust Manager supports the Digital Signing with PKI-backed identity as required by regions, countries, or industry standards. At the same time, the solution backs business units that must comply with different rules, manage private keys separately for document-signing standards, and use different signing tools to optimize workflows. Each team also uses different signing tools to optimize business.

Document Trust Manager integrates with enterprise document signing tools via global industry standards, Cloud Signing Consortium API, and it manages private key and signing activities throughout the organization.

Enhance digital transformation while minimizing business risk

Digital transformation can reduce costs associated with creating, storing, mailing, and searching official documents, while also saving time in the contracting and document-signing process. However, it introduces risks like fake identities and a lack of assurance about document origin and compliance with standard requirements. PKI-backed signing solves this challenge by providing clear signer identity and non-repudiation.

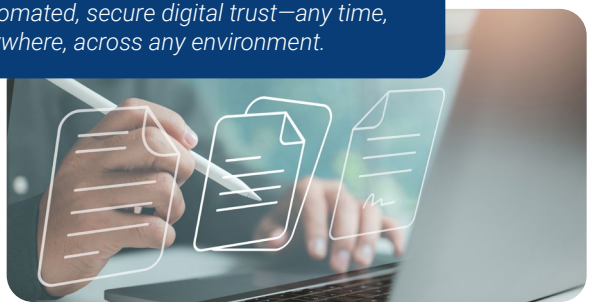
Sign digitally with compliance upon regional/global trade and vertical requirements

Each region and country legislates laws and standards for legally valid digital signing. In addition, industries impose standards that businesses must comply with. These requirements often involve separate Trust Lists and verification processes, which can complicate compliance management. DigiCert Document Trust Manager manages multiple Trust Lists on a single platform to support compliance and non-repudiation.

Keep existing business workflows while adding corporate audit and management

Enterprises deploy various signing tools and processes, even within the same location, and often across multiple locations, including the cloud. DigiCert Document Trust Manager ties together PKI-backed trust with management for private keys, certificates, and signing activities, providing visibility for executives and supporting security teams and administrators.

DigiCert® Document Trust Manager enables automated, secure digital trust—any time, anywhere, across any environment.



Functionality

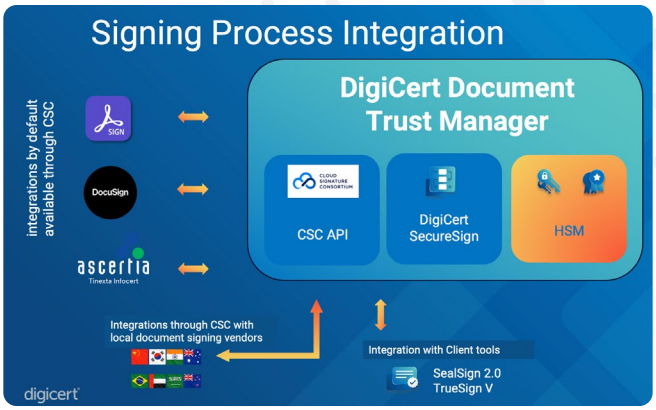
To achieve compliant document signing and centralized management, DigiCert Document Trust Manager offers the following capabilities:

- **Trusted roots:** AATL-, eIDAS-, ZertES-compliant validation provided by a Qualified Trust Service Provider (QTSP) as DigiCert to support global business requirements, including cross border trade and European standards.
- **Secure storage and management for signing keys:** Document-signing private keys are stored in cloud-based HSMs and never leave the platform, eliminating concerns about lost or stolen keys and certificates.
- **Role-based administration:** Role-based access across DigiCert ONE (Account Manager + Document Trust Manager roles) to ensure clean separation of duties at scale.
- **Management for policies, roles, audit logs, and signing keys from a single control pane:** A centralized dashboard and admin UI to manage signing activity, accounts, licenses, and usage. This supports auditing of signing actions and planning for future algorithm transitions.
- **Integrated 2FA:** Integrated into the signing workflow, allowing users to sign documents without USB tokens.
- **Remote Identity Verification support:** Verifies signer identity using strong proofing methods, including biometrics, liveness detection, and ID document validation.
- **DigiCert SecureSign:** Enables countersigning directly on the DigiCert Document Trust Manager cloud platform without requiring a dedicated signing tool.
- **CSC-standardized API:** The CSC API connects multiple signing tools and workflows, including Adobe Sign, DocuSign, SigningHub and other desktop signing tools.

Key Value

DigiCert Document Trust Manager helps you transition legacy paper workflows to a fully digital ecosystem while maintaining non-repudiation and meeting multiple standards and business requirements.

- **Multiple workflows united:** Multiple document-signing processes, such as DocuSign, Adobe Sign, and Adobe Acrobat, can be centrally managed through DigiCert® Document Trust Manager.
- **Multiple signing methods:** Supports cloud signing UX, common signing applications, and local desktop signing tools to match departmental needs.
- **Keyless signing:** Users can perform digital signatures without direct access to private keys, eliminating the risk of key loss or leakage, while administrators centrally manage signing activities.



Integration with Signing Systems

- CSC API enables global integrations for document signing flows
- Pre-setting connector integrations on CSC with Adobe Sign and DocuSign
- Desktop Signing tools, such as Adobe Acrobat and Office 365 with TrueSign V
- Mass Sealing support with SealSign 2.0 client tool.

PKI-backed signatures by industry

Various regional and national standards and regulations support or require PKI -backed signatures for official documentation. Although PKI or X.509 is not mandatory for every regulation or standard, PKI has been widely adopted over time and is commonly used as a technical implementation option. The examples below illustrate common business use cases.

Industry	Regulation / Standard	Key Requirements	Value provided by Document Trust Manager
Financial Services	eIDAS/National financial regulations	Integrity, auditability, signer authentication	PKI + HSM + audit-ready digital signatures
Medical/Healthcare	HIPAA/EU eHealth	Record integrity and authenticity	Long-term verifiable electronic signatures
Government/Public Sector	e-Government framework/ National regulations	Authenticity, non-repudiation	Legally enforceable digital signatures

Please note that final legal compliance depends on customer-specific implementation and operational controls. DigiCert Document Trust Manager provides a technical foundation aligned with applicable laws and international standards.

Regional and national regulations at glance

Below is a brief overview of regional and national regulations. While many countries are technology-neutral, PKI-based digital signatures are widely accepted as a best practice for high-value, regulated, and cross-border transactions. Because each country and region follows a different legal system, country-specific regulations and trust service providers exist. Although DigiCert may not offer all local providers directly, customers can integrate with local providers through the CSC API to enable consolidated enterprise management across local and cross-border transactions.

Country/Region	Law/Regulation	Requirements for Electronic Signatures
EU	eIDAS/eIDAS 2.0	Advanced/Qualified Electronic Signatures (PKI, signer identity, integrity, long-term validation)
USA	ESIGN Act/UETA	Technology-neutral (authenticity, intent, record retention)
Australia	Electronic Transactions Act (ETA)	Authenticity, non-repudiation
Brazil	MP 2.200-2/ICP-Brazil Framework	PKI-based digital signatures using ICP-Brazil–accredited CAs required for highest legal validity
China	Electronic Signature Law	Reliable electronic signatures (state-approved CA, PKI); signing algorithm may differ from western countries
India	Information Technology Act, 2000	Digital signatures based on asymmetric cryptography and hash functions, issued by licensed certificate authorities
Japan	Electronic Signature Act	Signer authenticity, integrity, certificate-based identity. CA approved by the government.
Saudi Arabia	Electronic Transactions Law + NCA/ SDAIA frameworks	Government-backed PKI, identity assurance, strong authentication. Sharia-compliant evidence principles.
South Korea	Electronic Signature Act	High-assurance electronic signatures (PKI dominant in finance/ government)
UAE	Federal Decree-Law No. 46 of 2021	Trust services, identity verification, government-recognized trust service providers. PKI for high-assurance use.

Everyday use cases for PKI-backed signatures

Industry verticals are not the only drivers for PKI-backed signatures. Each department produces specific digital documents and publications that must—or are strongly recommended to—use PKI-backed signatures. The examples below illustrate common use cases in everyday business operations.

Department	Example	Impact	Regulatory/Standards Drivers
Legal	Contract/Agreement (Commercial, vender, Partnership), NDA	eSeal	eIDAS (EU), National electronic signature laws, court evidentiary requirements
Finance / Accounting	Invoices, receipts, financial statements, audit reports, tax filings, SOX-related approvals	eSeal/ eSignature	SOX (US), eIDAS (EU), national tax authority requirements, ISO 14641 (archiving)
IT	Security policies, change approvals, access authorization records, incident response reports	eSeal	ISO/IEC 27001, SOC 2, NIST frameworks
Medical Operations	Medical records, prescriptions, clinical trial documentation, patient consent forms	eSeal	HIPAA (US), FDA(US), EU eHealth regulations, My Health Records Act (AU), National regulations
Procurement	Purchase orders, supplier contracts, SLAs. Delivery and acceptance certificates.	eSeal/ eSignature	Commercial law, industry procurement standards
Sales Operations	Quote, vender contract, pricing document	eSeal	Commercial law, industry or national compliant rules
HR	Employment contracts, offer letters, employee consent forms, compensation and benefits agreements	eSeal/ eSignature	National labor regulations, data protection and audit requirements
Business Operations	Design approvals, quality assurance records, compliance certificates	eSeal	ISO 9001, ISO 13485, industry safety standards

Get Started Today

Get started with DigiCert Document Trust Manager today. Contact your DigiCert account manager or submit a request through the web form at digicert.com

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com