

# DIGICERT® DOCUMENT TRUST MANAGER

Digital signatures, electronic seals, and timestamps to protect your digital document transactions around the world.

## Keep global business moving

DigiCert® Document Trust Manager enables organizations to obtain trusted, compliant digital signatures, electronic seals, and timestamps that scale across a wide range of global use cases. DigiCert helps organizations confidently comply with industry and local regulations in the U.S., European Union (EU), United Kingdom (UK), and Switzerland, as well as other countries around the world.

## Comply with laws around the world

Many countries' laws require high-assurance digital signatures which are backed by certificates issued by a trust service provider (TSP) certified in that region. For example, a Qualified Electronic Signature (QES) in the EU, UK, or Switzerland, can only be issued by a Qualified Trust Service Provider (QTSP) like DigiCert. High assurance digital signatures from DigiCert comply with the Adobe Approved Trust List (AATL), EU Regulation (No 910/2014) on electronic identification and trust services for electronic transactions (eIDAS), UK eIDAS, and ZertES in Switzerland.

## Key benefits

- Speed document signing processes remotely—without compromising on security or compliance
- Use with leading e-signature applications from Adobe, Ascertia, and DocuSign
- Ensure that e-signatures are backed by the highest levels of identity assurance
- Comply with industry regulations like know your customer (KYC) or anti-money laundering (AML)
- Obtain trusted e-signatures in the U.S., EU, UK, Switzerland, and many other countries

## The digital trust advantage

Sign anytime, anywhere, and on any modern mobile device. Our highly flexible solution includes digital identities, certificates, technology, and automation options to build strong digital document trust. Document Trust Manager delivers:



### Digital Signatures

A digital signature is an e-signature backed by a digital certificate that is cryptographically bound to the signature field using Public Key Infrastructure (PKI). Commonly referred to as a digital identity (digital ID), each digital certificate is unique to an individual and obtained after verification of their identity.



### Electronic Seals

An electronic seal (e-seal) is a digital signature used by a legal entity such as a business or organization to certify the origin, authenticity, and integrity of documents. E-seals may provide strong legal evidence that the document has originated from the entity and has not been altered. E-seals are often used in automated systems to handle high volume processes such as bulk invoicing or paychecks.



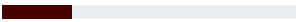


### Timestamps

A timestamp is a digitally signed record of the time and date of an event. Timestamps provide added assurance that a document, e-signature, or e-seal was valid at the time the timestamp was applied and has not been altered.

## E-signature trust built in

Not all electronic signatures (e-signatures) are equal. In fact, there are a lot of different types of e-signatures—from a simple checkbox or a scribbled image on a tablet to a high-assurance digital signature in the cloud backed by rigorous identity verification from an accredited authority, like DigiCert. This is why incorporating high assurance digital signatures that definitively link the signatory to a specific document helps protect your high-value, cross-border, and other electronic transactions.

The following chart shows the wide range of security attributes, regulatory compliance, and level of assurance of different types of e-signatures:

Type of signature	Electronic Signature	Digital Signature (AATL)	Digital Signature (Regulated/Qualified)
<b>Description</b>	A broad term that includes any electronic process that indicates acceptance of an agreement or record. The most basic form of an e-signature can be a name typed on a signature line or selection of a checkbox.	A more secure e-signature that requires use of a digital ID issued by a Trust Service Provider (TSP) that meets specific Adobe Approved Trust List (AATL) requirements for identity verification and security.	A highly secure e-signature that requires use of a regulated digital ID issued by a TSP that is certified in a specific region—such as a Qualified Trust Service Provider (QTSP) in the EU or Switzerland.
<b>Public Trust</b>	No requirement	Trusted by Adobe Acrobat and Reader	Trusted by Adobe Acrobat and Reader*
<b>Digital Identity</b>	No requirement to be uniquely linked to the signatory	Proof of signatory's unique digital ID cryptographically bound to signature field (PKI)	Proof of signatory's unique digital ID cryptographically bound to signature field (PKI)
<b>Level of Assurance (LoA)</b>	<b>Low</b> Limited or low identity verification 	<b>Substantial</b> Identity verification required 	<b>High</b> Rigorous identity verification in-person or equivalent 
<b>Two-Factor Authentication (2FA)</b>	Not required to sign document	Required to sign document	Required to sign document
<b>Long-Term Validity</b>	No requirement; may be included with a signature workflow solution	Tamper-evident seal and timestamp applied to the signed document	Tamper-evident seal and timestamp applied to the signed document
<b>Equivalent to wet ink signature</b>	No	No	Meets specific regulatory requirements in the EU, UK, and Switzerland*

## Key features

### Proof of Signing

Strong evidence of signatory identity, time of signature, and document authenticity cryptographically bound to signed agreements.

### Scalable Integrations

Works with leading signature workflow solutions including Adobe Acrobat Sign, Ascertia SigningHub, and DocuSign..

### Remote Identity Verification

Identify customers, citizens, and employees using modern mobile devices and ID documents.

### Flexible deployment options

Deploy Document Trust Manager as a hosted, on premises, or hybrid solution.

### Customized solutions

Create a private instance of Document Trust Manager or use the Cloud Signature Consortium (CSC) API to integrate with custom signing solutions.

### Centralized Control

Simplify administration for digital IDs and certificates using the DigiCert ONE platform.

### Secured Signature Keys

Protect private keys used for digital signatures in accredited Hardware Security Modules (HSM) and Qualified Signature Creation Devices (QSCD) hosted in secure, certified environments in the U.S., EU, and Switzerland.

## Protect your digital documents

As digital documents rapidly replace paper processes, organizations are also deploying trusted electronic sealing (e-sealing) solutions to protect document authenticity. When paired with high assurance digital signatures, applying e-seals to contracts, agreements, and other digital documents help protect your organization from the cost of potential cybercrime or fraud related to electronic transactions.

Document Trust Manager helps you ensure that all your documents are secured with e-seals, timestamps, and digital signatures backed by the highest levels of identity assurance.

## DigiCert ONE Platform for Digital Trust

DigiCert Document Trust Manager is part of the DigiCert ONE platform for digital trust, which unifies DigiCert's digital trust offerings on a modern, containerized architecture delivering high scalability, deployment flexibility, fast time to value, and unified PKI management.

## Get started today

Get started with DigiCert® Document Trust Manager today. Contact your DigiCert account manager or email [sales@digicert.com](mailto:sales@digicert.com).

## About DigiCert, Inc.

DigiCert is the world's leading provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. DigiCert® ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs its award-winning software with its industry leadership in standards, support and operations, and is the digital trust provider of choice for leading companies around the world. For more information, visit [digicert.com](https://digicert.com) or follow [@digicert](https://twitter.com/digicert).