

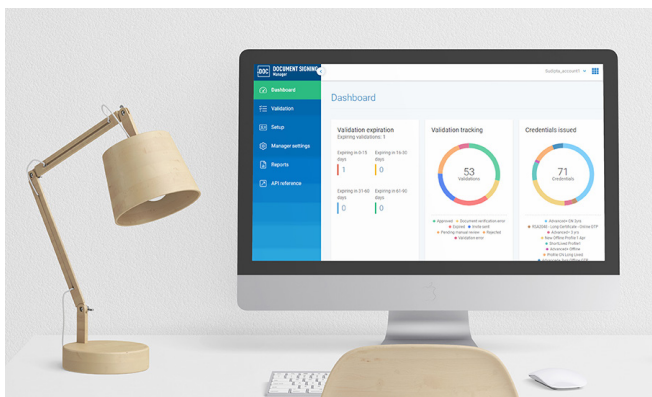
DELIVER BUSINESS AND LEGAL COMPLIANCE WITH THE HIGHEST LEVEL OF TRUST

Trust and identity are crucial in the age of digital documents

As digital documents increasingly replace paper processes, the need for trusted signing solutions is growing at a rapid pace. Without trust, businesses, governments and individuals cannot be certain of the validity of people and organizations, creating a risk for tampering or fraud in transactions, agreements and contracts.

DigiCert Document Signing Manager delivers identity and trust

Even in the world of secured signing, not all document signing solutions are the same. DigiCert Document Signing Manager is built on Public Key Infrastructure, a proven encryption, authentication and identity technology. With Document Signing Manager, a document is not only signed with cryptographically secure identity, any person reviewing knows who signed the document and they will see that the document is unaltered.



What is a Qualified Trust Service Provider?

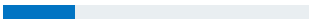


Signing service regulations set by the European Union and the European Technical Standard Institute (ETSI) represent the highest benchmark for signing security and identity in the world. The highest level of assurance in this standard is a Qualified Trust Service Provider (QTSP). As part of the acquisition of QuoVadis, DigiCert is recognized by the EU and ETSI as meeting the signing standards laid out in eIDAS regulations, making DigiCert one of a select few global QTSPs. DigiCert also meets all requirements for qualified signatures in Switzerland, according to the Swiss Signature Law (ZertES).

In fact, DigiCert + QuoVadis document signing is recognized both as equivalent to a handwritten signature and in many places, proof of identity equal to a form of government ID.

As a QTSP, signing solutions from DigiCert meets and exceeds the highest standards for signing security, authentication and identity in every region around the world.

Different grades of assurance for different types of documents

Recognized digital signatures vary in requirements and validation, according to the level of assurance needed by an individual or organization.

| Type of signature | Basic/Standard Electronic Signature (SES) | Advanced Plus Digital Signature (ADS/AATL) | Qualified Electronic Digital Signature (QES) |
|--|---|--|---|
| Signature requirements | An electronic signature a signer applies to a document as evidence of their acceptance or approval. This can include a scanned image of a signature or selecting the "I accept" button. | A digital signature that meets specific requirements, providing a higher level of signer identity verification, security and tamper-proofing. | A digital signature that meets advanced requirements and backed by a Qualified Trust Service Provider (QTSP) on the EU Trusted List (ETL) and certified by an EU member state or a QTSP on the Swiss Trusted List. This advanced digital signature is often used as an equivalent to a "wet signature." |
| Assurance and identity validation requirements | None | Signature linked to unique signer Signer can be identified by government identification, but not guaranteed Signature created using the specific identity data under the signer's sole control Signature is tied to signed data for which changes are detectible Signature is qualified for Adobe Approved Trust List (AATL) | QTSP must establish the integrity and authenticity of the signer: 1. The electronic signature creation data is secure and confidential 2. The identity of the signer can be proven by the QTSP by face-to-face, or similarly robust identity verification process |
| Examples | Employees signing documents during onboarding Commercial agreements between corporate entities Consumer agreements Software license agreements | Consumer credit or loan agreement Collective employment contracts Employment agreement between agent and employee | Contracts to lease, transfer or buy real estate Family law documents Incorporation of limited liability company |
| eIDAS Level of Assurance (LoA) | Low assurance  | Substantial assurance  | High assurance  |
| Validation level | No validation | Some validation | Maximum (rigorous) validation |

Two ways to sign

Individual signatory (eSignature)

A natural person, as an individual signatory, can easily and securely sign documents like personal contracts for real estate transactions, bank accounts and confidential information like medical documentation.

Organizational signatory (eSeal)

For business and government, a legal person, as an organizational signatory, can sign for the company or entity—with the option for mass or bulk signing—while ensuring the document remains tamper-proof.

The document signing advantage

Empower your customers to digitally sign anytime, anywhere. Our all-in-one solution includes certificates, technology and automation options that deliver a competitive edge while improving the customer experience.

Features

Customized signing workflows

Build comprehensive workflows with multiple technology options such as Ascertia SigningHub, Adobe Sign or DocuSign.

Effortless validation

Allow your customers to remotely create a secure identity in minutes using Verify by DigiCert powered by IDnow.

Simplified key management

Protect keys in a Qualified Signature Creation Device, hosted in a trustworthy environment.

Streamlined administration

Make management easy for Admins with centralized policy and control for users and signers.

Detailed tracking

Obtain reports and check audit trails for corporate or government regulation and policy.

Stronger security

Create stronger security with options for Two Factor Authentication (2FA).

Easy integration

Incorporate web services and third-party workflows like Adobe Sign, Ascertia Signing Hub and others.

Flexible deployment options

Deploy a hosted or on-premises solution.

Key benefits

- Reduce the cost of paper, administration, and shipping fees
- Improve customer loyalty and experience by simplifying on-boarding or signing requirements
- Decrease turn-around time for signature transactions from days to minutes
- Increase security for high dollar value transactions
- Deploy trust with legally valid signatures
- Ensure business continuity while creating a competitive advantage
- Satisfy global and industry governance and regulations

Technical specifications and integrations

Digital signing protocols

- Rest API
- CSC API

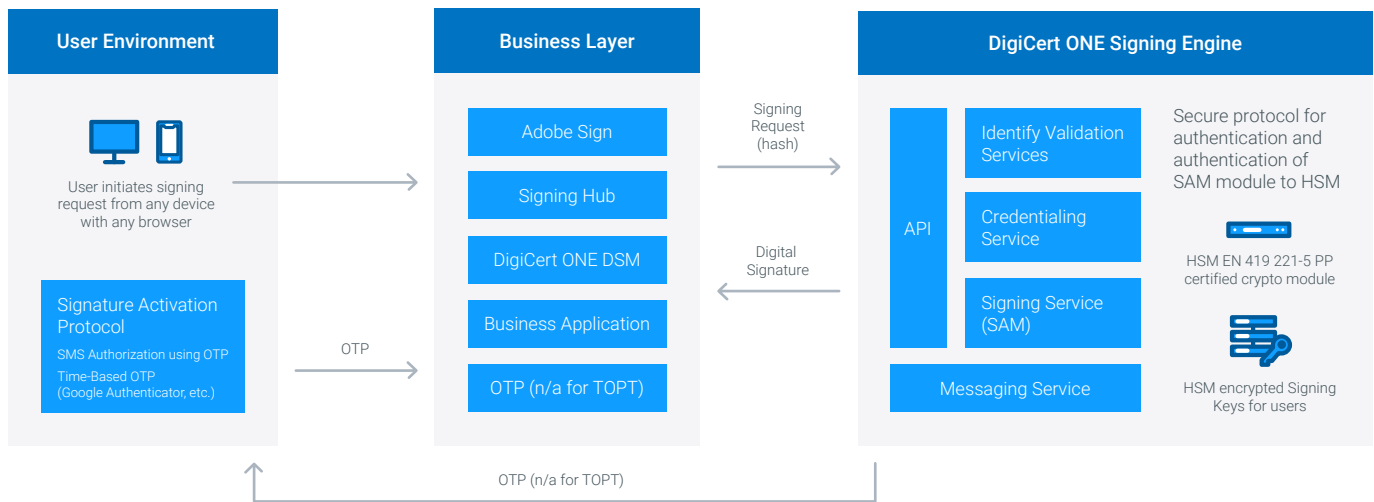
Available integrations

- Adobe Sign
- Ascertia SigningHub
- DocuSign

Compatible with

- Microsoft Office®
- Adobe® Acrobat & Adobe Reader
- LibreOffice®
- Open Office™
- Other third-party solutions like DocuSign
- Plus, a variety of document types including PDFs, ODF, DOCX and XML

Cloud based remote signing architecture



DigiCert® ONE

Document Signing Manager is part of DigiCert ONE, a modern, holistic approach to PKI management. Built on advanced, container-based architecture, DigiCert ONE allows you to rapidly deploy in any environment, roll out new services in a fraction of the time, and manage users and devices across your organization at any scale.

For more information on DigiCert® Document Signing Manager, contact one of our document PKI experts at docsigning@digicert.com

The trusted leader in PKI

At DigiCert, finding a better way to secure the internet is a concept that goes all the way back to our roots. That's why our certificates are trusted everywhere, millions of times every day, by companies across the globe. It's why our customers consistently award us the most five-star service and support reviews in the industry. And it's why we'll continue to lead the industry toward a more innovative and secure future. In SSL, IoT, PKI, and beyond—DigiCert is the uncommon denominator.