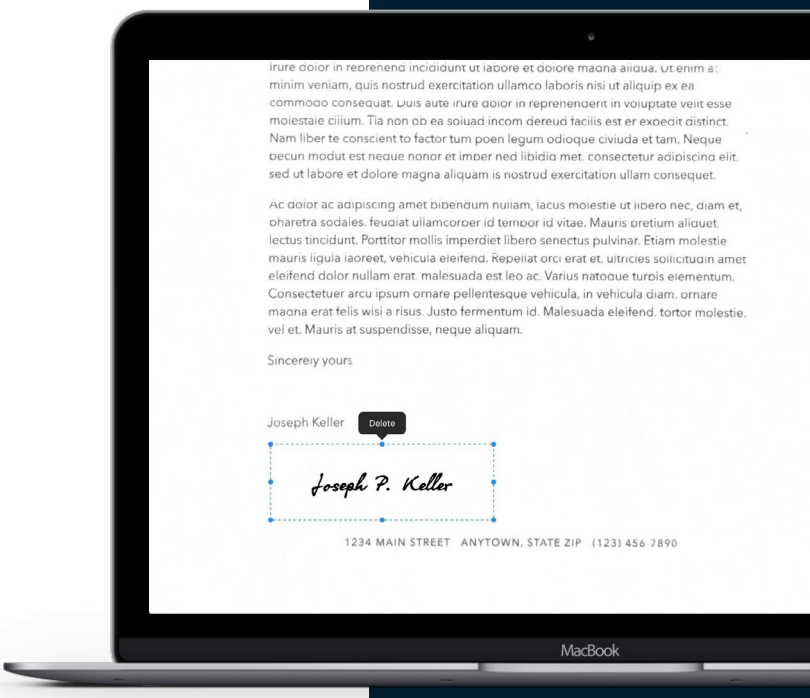
Sectigo Document Signing Certificates

Enable secure electronic document exchange and workflows, ensure document integrity and authorship, and satisfy electronic document compliance requirements with Sectigo Document Signing Certificates.

Document Signing Certificates guarantee authorship of electronic documents with secure digital signatures that authenticate the signer's identity and document origin, verify the document is unaltered and uncompromised, and protect information within the electronic document.

Sectigo Document Signing Certificates enable users to apply digital signatures to Adobe® and Microsoft Office® documents, providing trusted assurance of authenticity for electronically transmitted documents usable on any operating system and any Adobe product.



SECTIGO

WWW.SECTIGO.COM

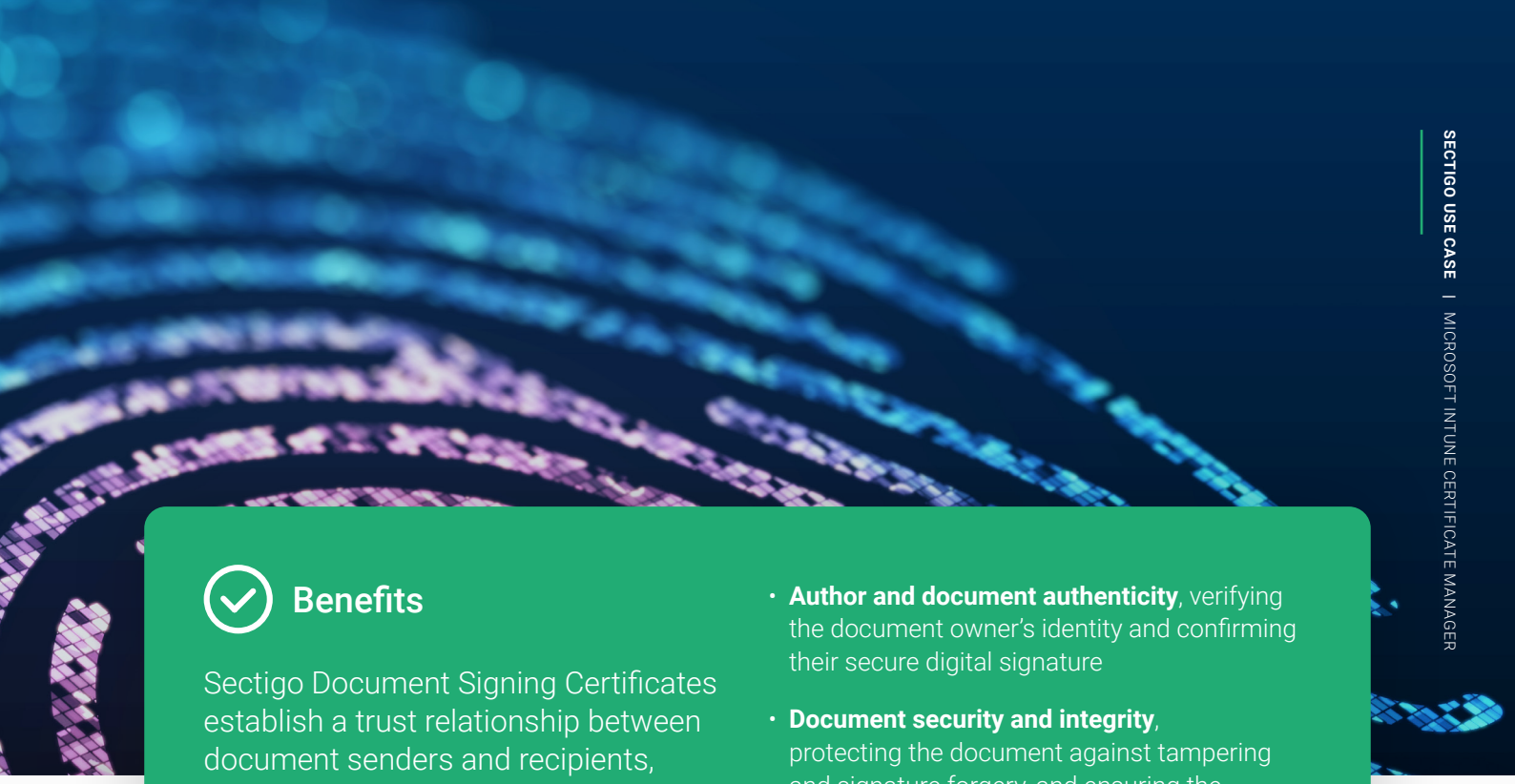
How it works

Sectigo validates the identity that is named in the certificate through a series of checks which conform to the policies of Adobe and/or Regulation (EU) No 910/2014. The certificate is then created, and paired with a private key that is installed in a FIPS 140-2 level 2 or Qualified Signature Creation Device. This prevents the key from being duplicated, stolen, or otherwise used maliciously.

When the author initiates the digital signature of the document, the signing application will create a HASH value which represents the entire content of the document. After a proper authentication of the author, often using a PIN, the HASH value is signed and embedded into the document itself. Any attempt to change the content of the document after it is signed will change the HASH value and the signature will be marked as invalid.

Visual trust indicators enable users to instantly verify the signer's identity, assure recipients of the document's authenticity, and authenticate documents signed by multiple parties.

Optionally, the author may embed a timestamp into the document using the signing application. The Sectigo provided timestamp ensures the recipients know the true time the document was signed. If the author chooses instead to use the time from the desktop or server, it could end up incorrect, either accidentally or maliciously. If there's no timestamp for the signature, the certificate validity is checked for the time of the signature validation, which is not always acceptable since the certificate could have expired since signing the document.



Benefits

Sectigo Document Signing Certificates establish a trust relationship between document senders and recipients, guaranteeing:

- **Author and document authenticity**, verifying the document owner's identity and confirming their secure digital signature
- **Document security and integrity**, protecting the document against tampering and signature forgery, and ensuring the document remains unchanged

Sectigo Document Signing Certificate products

Sectigo Document Signing Certificate products are available to meet the specific needs of enterprises with high-volume document workflows such as financial reports, invoices, pharmaceutical tests, engineering diagrams, contracts and statements produced by automated document-generation systems.

Enabling easy integration of Sectigo Document Signing Certificates with existing enterprise document management systems, three solution options are available to accommodate different types of secure systems used for enterprise key storage:

- **Document Signing USB**
- **Document Signing Cloud HSM**
- **Document Signing On-Premise HSM**

Sectigo Document Signing Certificate solutions offer additional flexibility by supporting document signature authority designations restricted to individuals or applied at the workgroup/division level or organizational/enterprise-wide level.

Regulatory Compliance

Sectigo Document Signing Certificates leverage the digital signing capabilities of Adobe® and Microsoft Office® documents to enable compliance with standards such as:

- U.S. Federal ESIGN Act
- GLBA
- HIPAA/HITECH
- PCI DSS
- US-EU Safe Harbor
- eIDAS (coming soon)

Membership in AATL and CSC

Sectigo is a member of the Adobe Approved Trust List (AATL) and the Cloud Signature Consortium (CSC).

Sectigo Document Signing Certificate Key Features

Secure your electronic document exchange and workflows with these key Sectigo Document Signing Certificates features and capabilities:

Electronic signature security

Sectigo Document Signing certificates are verified by Sectigo,a trusted Certificate Authority and member of the AdobeApproved Trust List and use SHA-2 signing and 2048-bit encryption for highest levels of security and browser compliance.

Scalable document signatures

Whether your workflows require one, hundreds, thousands, or even millions of signatures, Sectigo Document Signing supports an unlimited number of signatures with each document signing certificate.

Signature validation

Signatures are valid throughout the lifetime of the secured document, and feature time stamping indicating the time and date the document was signed, and displaying organization, department, or group signatures.

Certificate lifecycle management

Sectigo Certificate Manager enables you to issue document signing certificates quickly, with automatic notification when certificates expire.

Secure certificate delivery

The Sectigo Document Signing Certificate's private signing key is protected from theft, by being installed in a FIPS 140-2 level 2 or Qualified Signature Creation Device, using a cloud-based or on-premises hardware security module (HSM), a smart card or a USB.

Electronic signature security

Sectigo Document Signing Certificates are compatible with Adobe Acrobat, Adobe Reader, and Microsoft Office.

Cloud-based integrations

Sectigo Document Signing Certificates can be utilized with Azure Key Vault, AWS Key Management Service (KMS) and Google Cloud KMS.

About Sectigo

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As the world's largest commercial Certificate Authority with more than 700,000 customers and over 20 years of experience in online trust, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions for securing webservers, user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow. For more information, visit www.sectigo.com and follow @SectigoHQ.

SECTIGO