

Sectigo Document Signing Certificates

Scalable document signing solutions for organizations and individuals

Digital signatures are now embedded in everyday business operations, yet many organizations struggle to meet legal and compliance standards. While simple electronic signatures are widely accepted under regulations such as eIDAS and E-SIGN, certificate based digital signing solutions provide the higher level of identity assurance, document integrity, and non repudiation needed when stronger evidentiary confidence is important.

Electronic signing relies on vendor managed audit trails, while digital signatures embed verifiable proof directly in the document, enabling independent validation without reliance on the signing provider.

Demand for document signing certificates is growing steadily across businesses of all sizes, including solo practitioners as digital signing becomes routine and trust becomes the differentiator. Organizations and individuals need clear, verifiable assurance of who signed, when signed, and whether the document can withstand legal or regulatory scrutiny over time.

Key benefits

- ✓ Unlimited document signatures during the certificate term. 1-, 2-, or 3-year certificate validity options.
- ✓ Secure delivery on FIPS-compliant hardware tokens.
- ✓ Tamper-evident protection. The signature is invalidated if the document is modified.
- ✓ Compatible with trusted timestamping for long-term document to support long-term document validation.
- ✓ Globally trusted across platforms such as Microsoft 365 and Adobe Acrobat.
- ✓ Support for long-term authenticity and non-repudiation.
- ✓ 24/7 expert support.

Provide secure document signing with verified identity and document integrity

Whether you manage document workflows across a global enterprise or sign contracts as an independent professional, secure digital signatures help protect your work. Sectigo Document Signing Certificates enable verified digital signing, helping prevent tampering and unauthorized changes.

A digital signature uses cryptography to ensure document integrity and to authenticate the signer via a trusted digital certificate, providing verifiable evidence and non repudiation. Digital signature certificates give recipients confidence in the signer's verified identity and the integrity of the signed document, reinforcing trust in every transaction.

How does Sectigo document signing work?

When a document is digitally signed, the signer’s private key is used to create a cryptographic signature over the document content. This signature, along with the associated Sectigo Document Signing certificate, is embedded within the document as a digital signature container.

This digital signature enables recipients to verify both:

- **Document integrity**
Confirming that the document has not been altered since it was signed.
- **Signer identity**
Confirming that the signature was created using the private key corresponding to the certificate.

When a document is received, the document signature can be validated using the public key contained in the Sectigo Document Signing certificate. The validation process confirms that the signature is valid and that the document remains unchanged. The signer’s identity is displayed in the Subject field of the Sectigo Document Signing certificate.

Because Sectigo is a trusted Certificate Authority (CA), its certificates are recognized by major platforms and applications. As a result, the signer’s identity can be verified and trusted based on Sectigo’s established trust relationships.

Which document signing product is right for you?

Capability	Document Signing Enterprise	Document Signing Professional
Primary user	Organizations’ employees	Independent professionals—or any person needing to sign the document
Setup	Often IT-assisted	Self-service
Signing control	Commonly managed centrally	Sole signer control
Adobe & Microsoft trust	✔	✔
Tamper-evident integrity	✔	✔
Compliance & non-repudiation	✔	✔

Sectigo Document Signing certificates delivery options

Sectigo Document Signing Certificates are delivered on secure USB tokens certified to FIPS 140–2 Level 2 or higher, helping protect private keys from unauthorized access or use. After validation is complete, the USB token is shipped to the customer and the access PIN is sent separately by email.

Disclaimer: Sectigo does not provide legal advice, and this document is for informational purposes only. Organizations should consult their own legal counsel regarding applicable laws, regulations, and signing requirements.

Sectigo Document Signing certificates delivery options

Sectigo Document Signing Certificates are delivered on secure USB tokens certified to FIPS 140-2 Level 2 or higher, helping protect private keys from unauthorized access or use. After validation is complete, the USB token is shipped to the customer and the access PIN is sent separately by email.

Disclaimer: Sectigo does not provide legal advice, and this document is for informational purposes only. Organizations should consult their own legal counsel regarding applicable laws, regulations, and signing requirements.

About Sectigo

Sectigo is a leading provider of Certificate Lifecycle Management (CLM), helping organizations secure human and machine identities while reducing the hidden risks of modern digital trust. As certificate volumes grow and lifespans shrink, unmanaged certificates are becoming a source of outages, compliance exposure, and operational disruption. Sectigo uses Orchestrated Automation to deliver Simplicity at Scale through its cloud native CLM platform, bringing visibility, control, and lifecycle management together across complex environments. With more than 700,000 customers, including 65% of the Fortune 500, Sectigo is one of the largest and longest standing certificate authorities, with over 20 years of delivering unparalleled digital trust.

Learn more about Sectigo Document Signing solutions:

[Document Signing Certificate – PDF Signing | Sectigo® Official](#)

