Document Signing Certificates

10 September 2019

Table of Contents

Document Signing Certificates

Document signing certificates provide trusted assurance of authenticity for electronically transmitted documents by confirming the identity of the signer and ensuring the integrity of the document.

Sectigo's Document Signing Certificates enable organizations to secure documents with digital signatures. These certificates comply with the U.S. Federal ESIGN Act and other applicable international laws.

Supported file formats

Document Signing Certificates can be used on any platform that trusts the Sectigo root certificate. Most PDF file formats are supported, including Adobe PDF.

Key features

- Unlimited signatures
- iKey USB token
- Displays organization, department or group signature
- Adobe Approved Trust List member
- FIPS compliant

Certificate Signing Requirements

In order to use Document Signing Certificate, you need a PDF product that supports digital signatures.

What you need to know before you place an order

Requests for Sectigo certificates are subject to rigorous validation procedures. Validation is an important part of certificate issuing process. Sectigo adopted stringent validation policies and procedures to provide secure and verifiable digital document exchange.

Sectigo will verify the following:

- The identity of the organization and its contact who signed the request for the Document Signing Certificate.
- The address of the organization.
- That the organization has authorized the issuance of the certificate.

All validation work is done by Sectigo. You are only required to respond to emails and provide the requested documents and information.

After the order is placed by an organization or an individual within organization

After an organization has placed an order, the contact specified in the request will receive an Order Acknowledgement email. The contact must follow the included instructions to get approval for the Sectigo Document Signing Certificate request.

Sectigo must perform validation that involves the following:

- Verifying business identity, address and main business telephone number.
- Using Face-to-Face Document to verify the contact (signer on the agreement) is an identifiable individual (that is, a natural person).
- Verifying the license status of the Notary, Attorney, or Certified Public Accountant who notarized the Face-to-Face Document.
- A call to the verified business phone number to verify organization's existence.
- A call to the verified business phone number to verify the contact's signature, agency and authority to request Document Signing Certificates on behalf of the organization.

Most of the validation is completed by Sectigo with typically very little action needed by the customer.

Sectigo validates the organization using the following sources:

- A government registration agency in the jurisdiction of the Applicant;
- Independent reliable public database that can provide accurate business information;
- Regional phone directories that contain verified information;
- Business credit reporting services.

The Applicant is required to respond to an email challenge and to complete, sign and notarize a Face-to-Face Document.

Face-to-Face authentication of the organization's contact

The organization's contact is required to submit a Face-to-Face Verification Document. This document contains the Personal Statement Declaration asserting the contact's identity and confirming that the information provided in the application is true and accurate. The document must be notarized by the Notary Public, Latin Notary, Attorney, or Certified Public Accountant (hereafter referred to as the Confirming Person). The Confirming Person must be authorized to conduct business in the organization's area/country.

The organization's contact is required to do the following steps:

1. Complete the Face-to-Face Verification Document and notarize it with a Confirming Person. Make sure that the Confirming Person is licensed with an active status in contact's jurisdiction.
2. Prepare the following supporting documents:
    - A government issued Photo ID.
    - A document from an acceptable financial institution. The document must contain the contact's name.

- A non-financial document that contains the contact's name.

3. Upload the Face-to-Face Verification Document along with the supporting documents at the link provided to the contact in the Order Acknowledgement email.
4. When Sectigo's representative calls the contact, acknowledge that they in fact signed the Agreement.

Acceptable proof of identity documents

The following documents are accepted for the purpose of validation for a Sectigo Document Signing Certificate:

A. One of the following valid government-issued forms of photo ID:

- A driver's license
- A passport
- A personal identification card
- A military ID
- A concealed weapons permit

B. One of the following valid documents issued by a financial institution:

- A credit card, provided it contains an expiration date and has not expired
- A debit card, provided it contains an expiration date and has not expired
- A mortgage statement from a recognizable lender that is less than six months old
- A bank statement from a regulated financial institution that is less than six months old.

The above documents must contain the contact's name.

C. One of the following valid documents issued by a non-financial institution:

- Recent original utility bill or certificate from a utility company confirming the arrangements to pay for the services at a fixed address (a gas bill, water bill, power bill)
- Recent original landline phone bill showing contact's name, address and phone number (not a mobile/cellular telephone bill)
- A copy of a statement for a payment of a lease, provided the statement is dated within the past six months
- A certified copy of a birth certificate
- A local authority tax bill for the past year
- A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.

Documents that are not accepted for identity verification purposes

The following are examples of some documents that are not acceptable for identity verification purposes:

- Health card
- Employee ID card
- Library card

The license status of the Confirming Person who notarized the Face-to-Face Verification Document will be verified with a Status of Author Document. Sectigo will verify that the Confirming Person is licensed with an active status in the Applicant's jurisdiction. Sectigo will use a government-accredited licensing agency in the Applicant's jurisdiction for verification.

Validation process

The organization's representative will be contacted by Sectigo over the phone and is required to complete the following steps:

1. Confirm the organization's existence.
2. Confirm the authority of the contact specified in the request to represent the organization.

The Sectigo validation department will verify your company and will contact you in case additional information is required.

When a request for certificate from an organization is received, Sectigo will verify the following:

- Organization's existence, address and a reliable method of communication with the organization.
- That the specified organization's contact person is an employee of the organization or is authorized to request Document Signing Certificates on behalf of the organization.
- That the organization is operating at a verifiable address.
- Consistency of the information provided by the organization.

Challenge email response

The contact will receive a challenge email that will verify the email address to be listed on the certificate. The email is sent by Sectigo during the validation process. The contact must respond to the challenge email prior to the certificate issuance.

Business validation

Sectigo is required to verify the identity of the business. Sectigo will use only qualified and dependable resources to verify the business identity, address and main telephone number.

The contact is not required to confirm the business registration unless Sectigo is not able to correctly verify the business using qualified resources. Sectigo may ask the contact to provide documentation such as a Legal Opinion Letter attesting to the business identity and status. If a Legal Opinion Letter is needed, Sectigo will provide a sample letter and instructions.

The Legal Opinion Letter must be completed by an Attorney or Certified Public Accountant licensed in the country of the Applicant's jurisdiction.

The Attorney or Certified Public Accountant completing the letter will be verified with the appropriate government professional licensing agency in the Applicant's jurisdiction.

Verifying information by telephone

Certain aspects of the validation process require Sectigo to call the verified main business telephone number to talk with the contact. The purpose of the call is to verify the following:

- That the contact has signed the certificate request.
- That the contact has the authority to sign the agreement.
- That the contact is an employee of the organization or requested the certificate on behalf of the organization.

Order completion

Sectigo's goal is to promptly complete your order while adhering to validation standards. To ensure the integrity of the certificate, Sectigo will not issue a certificate which has not passed stringent validation.

After you have submitted the required documents, Sectigo will validate organization and the contact's identity. The validation process may take 1 to 5 business days. You will be notified by email when the validation process is completed. Once the certificate is issued, it will be installed on the USB token and mailed to you. Arrival time depends on your location and shipping methods. You will receive tracking information via email.

What happens if validation fails?

If Sectigo is unable to authenticate the submitted information, the request for a Document Signing Certificate will be rejected.

Sectigo support team monitors rejected certificates and will contact the Applicant via the email associated with the account. The Applicant may be able to rectify the certificate denial problem by providing additional information to enable authentication. Sectigo will notify you if additional documentation is needed.

All payments are non-refundable, except that Sectigo will refund a payment if 1) Sectigo was not able to authenticate the submitted information, and 2) the Applicant made a written request to Sectigo to issue a refund.

If you know that your certificate is rejected or simply wonder why the certificate status is not changing or why the certificate is not sent to you after it was approved, do not hesitate to submit a ticket with the Sectigo support team here or click the Live Chat link on the Support page to start a Live Chat conversation with one of Sectigo's agents. The Sectigo support team will give you an advice or assist with the refund.

Certificate delivery

Sectigo Document Signing Certificates are provided on secure USB tokens that are certified to FIPS 140-2 level 2 or greater. This level of security prevents unauthorized access to or use of the private keys on the certificate. Once the certificate request validation process is completed, the USB token will be mailed to you and you will receive an access PIN via email.

USB installation

Certificate installation is straightforward and does not require you to have elevated privileges.

Plug the USB smart card token with the certificate into the USB port of your computer. You can now digitally sign and verify documents using the Sectigo Document Signing Certificate.

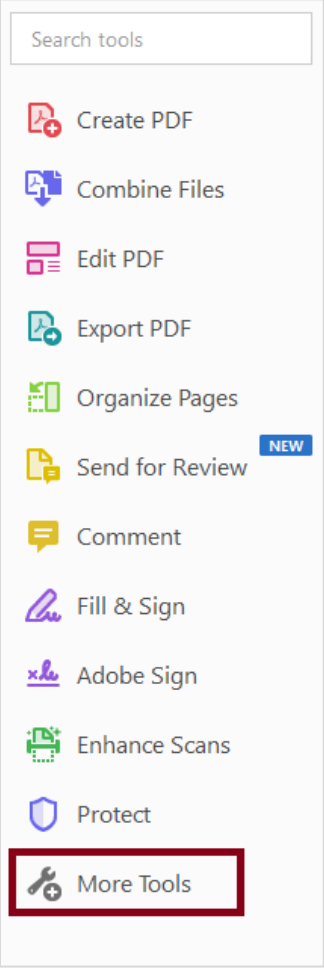
Note: Do not lose the PIN for your USB token or enter a wrong PIN multiple times. The USB token will be locked after the 15th consecutive attempt to enter a wrong PIN.

In case the PIN is lost or the USB token is locked, there is no way to retrieve or use the certificate. You will have to purchase a new Document Signing Certificate.

Using a Document Signing Certificate to sign a document

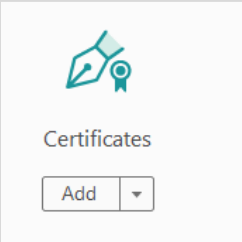
To digitally sign a document using a certificate, follow these steps:

1. Open the document that needs to be signed.
2. Plug the USB smart card token with the certificate into the USB port of your computer. Microsoft will automatically copy the certificate to your computer's cryptographic API (CAPI) certificate store.
3. Click **More Tools** on the Tools pane.

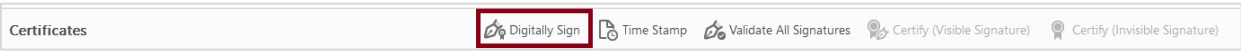


The Create & Edit page will appear.

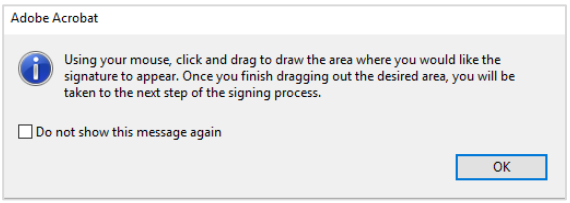
4. Select **Certificates**.



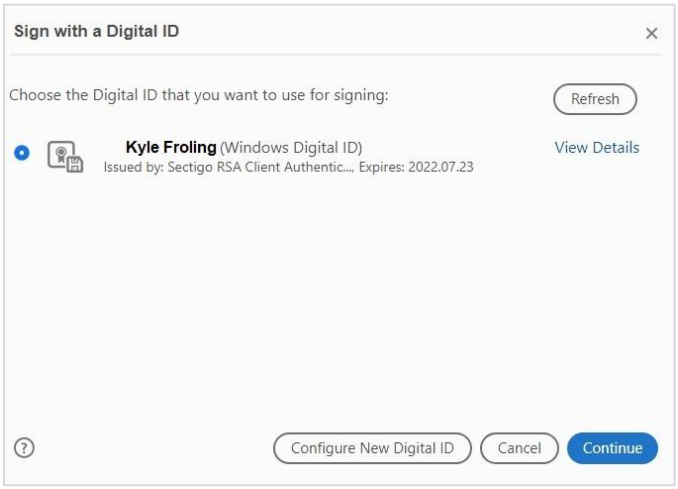
5. On the Certificates toolbar, Select **Digitally Sign**.



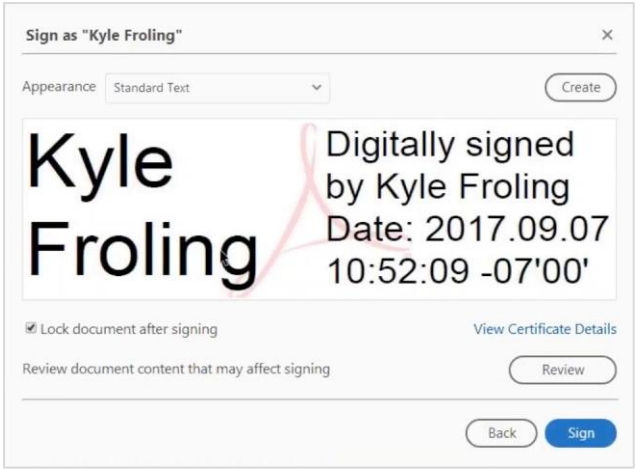
The Signature Area Selection dialog box will appear.



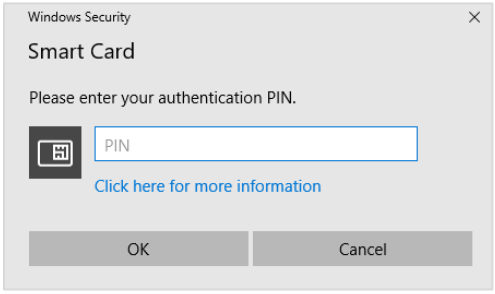
6. Click **OK** in the Signature Area Selection dialog box.
7. Using your mouse, click and drag to draw the area where you would like the signature to appear. The Sign with a Digital ID dialog box will appear.



8. Click **Continue**. The Sign as <Your name> dialog box will appear.



9. Click **Sign**. The Windows Explorer dialog box will open.
10. Select the folder where to save the signed document.
11. Type the document name.
12. Click **Save**. You will be prompted to enter your PIN.



13. Enter your PIN and click **OK**.

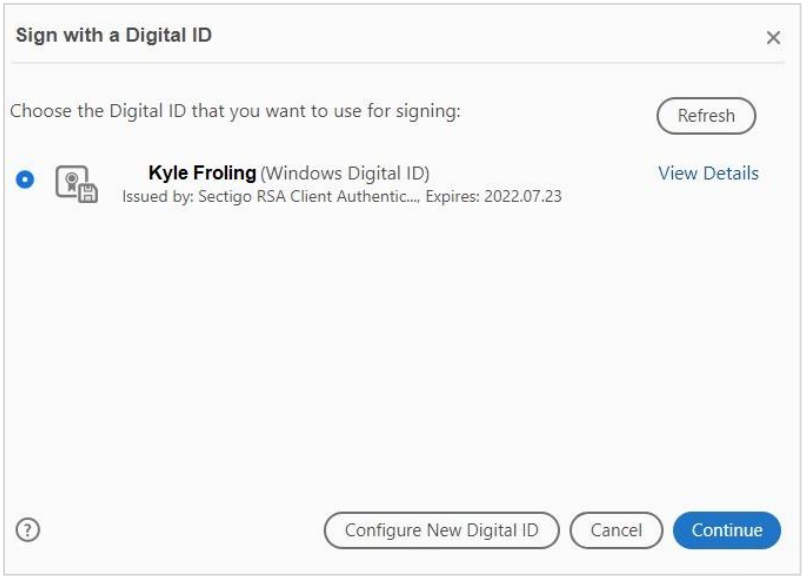
    Your signature will appear in the document.

Using a Document Signing Certificate to countersign a document

To countersign a digitally signed document, follow these steps:

1. Plug the USB smart card token with the certificate into the USB port of your computer. Microsoft will automatically copy the certificate to your computer's cryptographic API (CAPI) certificate store.
2. Open the document that needs to be countersigned.
3. Click the blue box beside the "Please counter sign this form" label.

4. The Sign with a Digital ID dialog box will appear.



5. Repeat steps 7-13 described in the *Using a Document Signing Certificate to sign a document* section.

Support

If you have questions or require support, please create a case using Sectigo Ticketing System or contact Sectigo support team via Sectigo Support page.