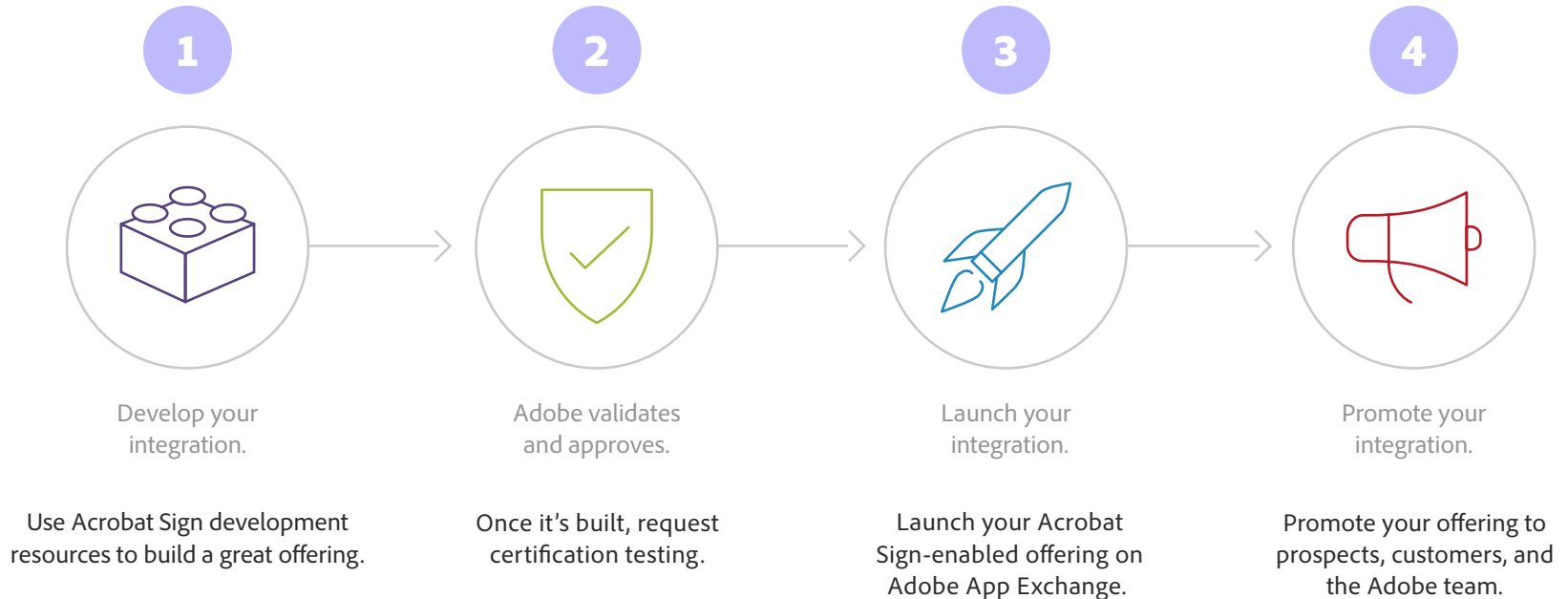


Build, test, and deliver in 4 easy steps.



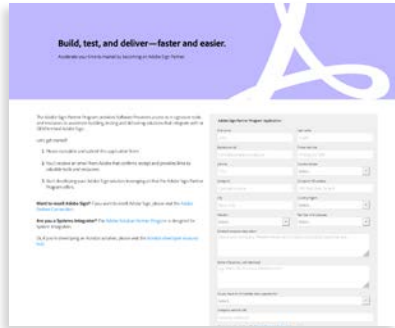
The Acrobat Sign Partner Program provides the tools and resources you need to deliver solutions that integrate with Acrobat Sign. [Apply now, if you haven't already.](#)



Robust developer resources make it easy to build your integration.

1

Start



Get a FREE Acrobat Sign Developer Edition specifically designed for development and demonstration.

[Sign up now](#)

2

Build

Use these helpful tools in the [Acrobat Sign Developer Center](#)

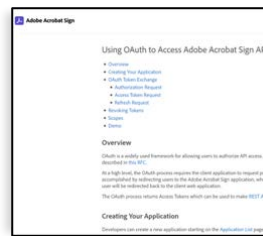
Rest API Documentation



Easily integrate Acrobat Sign functionality into your offering.

[Access](#)

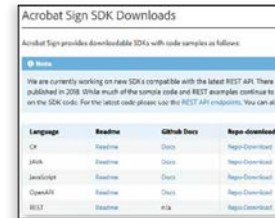
OAuth Documentation



Widely used framework allows users to authorize API access.

[Access](#)

SDK



Get access to all repositories.

[Access](#)

Webhooks



Improve your user experience with webhooks.

[Access](#)

[Return to Overview Page 1](#)

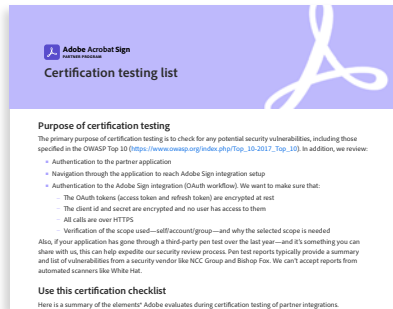


Everything you need to know about the Adobe certification test.

Once you've built your integration, you'll need to request a certification test from Adobe. This information will help the certification testing process run smoothly.

1

Know what Adobe looks for



Get checklist

2

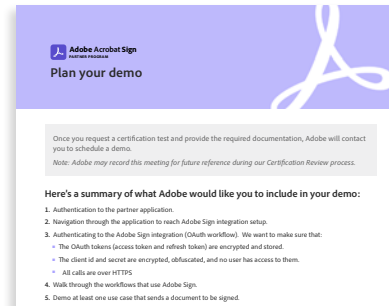
Request your test



Request a test

3

Prepare and execute your live demo



Get details

4

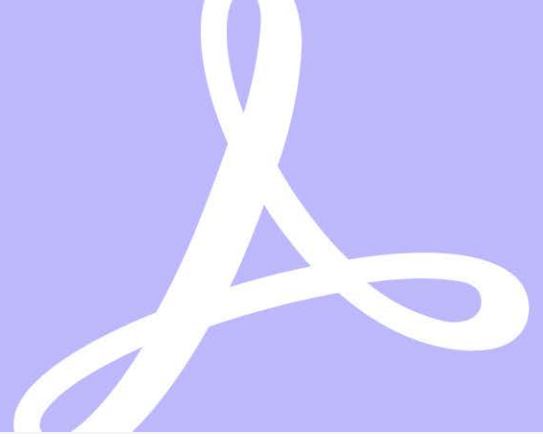
Get certification status



Partners typically are notified of certification status approximately 2 weeks after demo.

[Return to Overview Page 1](#)

Certification testing list



Purpose of certification testing

The primary purpose of certification testing is to check for any potential security vulnerabilities, including those specified in the OWASP Top 10 (https://www.owasp.org/index.php/Top_10-2017_Top_10). In addition, we review:

- Authentication to the partner application
- Navigation through the application to reach Acrobat Sign integration setup
- Authentication to the Acrobat Sign integration (OAuth workflow). We want to make sure that:
 - The OAuth tokens (access token and refresh token) are encrypted at rest
 - The client secret is encrypted and no user has access to it
 - All calls are over HTTPS
 - Verification of the scope used—self/account/group—and why the selected scope is needed

Also, if your application has gone through a third-party pen test over the last year—and it's something you can share with us, this can help expedite our security review process. Pen test reports typically provide a summary and list of vulnerabilities from a security vendor like NCC Group and Bishop Fox. We can't accept reports from automated scanners like White Hat.

Use this certification checklist

Here is a summary of the elements* Adobe evaluates during certification testing of partner integrations. (*Note: this list is non-exhaustive)

1. Auth flow

- Client secret must never be transmitted to the browser.
- Use only needed scopes for your application.
 - Including the modifier (self, group, account)
Tip: if you do not use x-api-user header, you can keep the default (or self)
 - You can check in Acrobat Sign REST API documentation which scopes is needed for each API
- Make sure to use the state parameter correctly
(see <https://auth0.com/docs/protocols/oauth2/oauth-state>)

2. Server-side request forgery (SSRF)

Never trust any URL provided by the user (including coming from Acrobat Sign). Ensure that you verify that it is a legitimate URL.

Reference: https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

3. Client-side request forgery (CSRF)

Reference: <https://owasp.org/www-community/attacks/csrf>

4. Injections (XSS/SQL)

- Including on while retrieving data from Acrobat Sign (like the signer's name).

5. Session handling

- Calls dealing with sensitive information need to be authenticated.
- Make sure to terminate the session on the server upon log out.
- In case of usage of Acrobat Sign API from the browser, revoke the access token part of your logout mechanism.(using /oauth/revoke/ see <https://secure.na1.echosign.com/public/static/oauthDoc.jsp#revokingtokens>)

6. Security headers

- Cookies must be set with Secure Flags, if no need to be accessed by JavaScript, set HttpOnly too .
- Header strict-transport-security (HSTS): Acrobat Sign advise you to set this header. If set, the browser will enforce the communication using https (even if the user forgot to use it).
If HSTS is missing and *cookies doesn't have the Secure Flag, the application will not be certified.*
- Cache control: Sensitive data should not be cached, make sure to have caching headers in place:
 - Cache-control: no-store (HTTP 1.1)—see <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control>
 - Pragma: no-cache (HTTP 1.0) References:
 1. CWE-524: <https://cwe.mitre.org/data/definitions/524.html>
 2. CWE-525: <https://cwe.mitre.org/data/definitions/525.html>

7. Test the webhooks

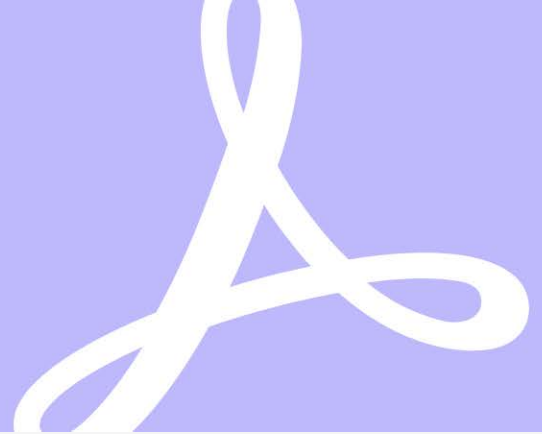
Good practice: in the webhook implementation, you can check the webhookid (or the agreementId). It's a good way to identify a legitimate call.

- At minimum, check that X-AcrobatSign-ClientId is present.
- Try to post unexpected data to the webhook.
 - Empty JSON
 - Valid webhook json but no IDs



Adobe Acrobat Sign
PARTNER PROGRAM

Plan your demo



Once you request a certification test and provide the required documentation, Adobe will contact you to schedule a demo.

Note: Adobe may record this meeting for future reference during our Certification Review process.

Here's a summary of what Adobe would like you to include in your demo:

1. Authentication to the partner application.
2. Navigation through the application to reach Acrobat Sign integration setup.
3. Authenticating to the Acrobat Sign integration (OAuth workflow). We want to make sure that:
 - The OAuth tokens (access token and refresh token) are encrypted and stored.
 - The client id and secret are encrypted, and no user has access to them.
 - All calls are over HTTPS
4. Walk through the workflows that use Acrobat Sign.
5. Demo at least one use case that sends a document to be signed.



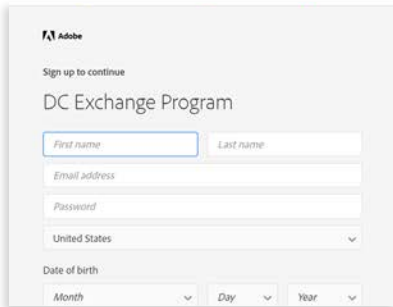
Congratulations! You're ready to launch.



Follow these steps to launch your offering on Adobe DC (Document Cloud) Exchange.

1

Register for the Adobe DC Exchange

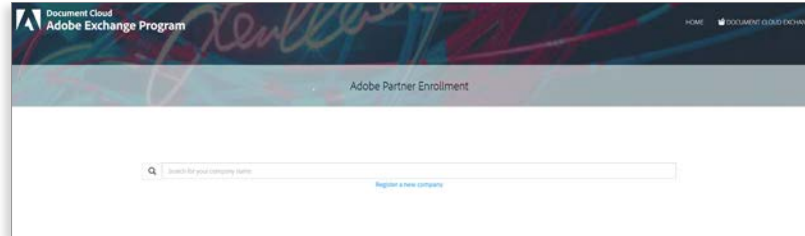


The screenshot shows the Adobe DC Exchange registration form. It includes fields for First name, Last name, Email address, Password, United States (dropdown), and Date of birth (Month, Day, Year dropdowns). The Adobe logo and 'Sign up to continue' text are visible at the top.

[Register here](#)

2

Create Adobe DC Exchange product listing



The screenshot shows the Adobe DC Exchange Partner Enrollment page. It features a search bar for company names and a 'Register a new company' link. The Adobe logo and 'Document Cloud Adobe Exchange Program' text are visible at the top.

[Have this info ready](#)

[Submit your listing](#)

3

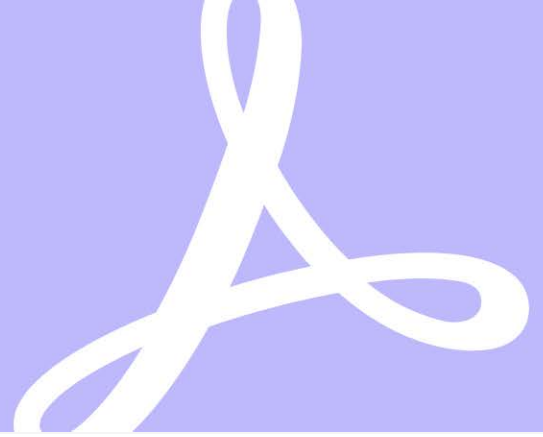
Adobe reviews



Typically, within one week, Adobe will notify you whether your product listing is complete and approved.

[Return to Overview Page 1](#)

What you'll need to complete your Adobe DC Exchange product listing



How to create your Adobe DC Exchange product listing

When you visit the [Adobe DC Exchange for Adobe Document Cloud registration site](#), you'll need all the items below to complete your product listing. Once submitted, Adobe will review your listing and either approve it or notify you regarding missing items within approximately one week.

Please ensure you are using the correct Adobe Acrobat Sign logo on all of your content. You'll find logos and Acrobat Sign content you can leverage on our [Adobe Partner Co-marketing Site](#).

Complete you APP PROFILE

- Enter app name
- Upload your app icon
- Upload a featured image
- Upload the app publisher logo
- Enter brief app description
- Enter detailed app description
- Select your app publisher

OPTIONAL

- Enter app publisher display name

Provide information related to INSTALLATION & SUPPORT

- Confirm if you need an Acrobat Sign integration trial or not
- Enter a "Learn More" link where interested parties can find out more about your integration
- Provide your support URL

OPTIONAL

- Enter support email address
- Enter support phone number
- Provide installation instructions

Provide information about TAGS

- Select Application type
- Select supported languages
- Select tags
- Select Supported Product

OPTIONAL

- Select Industry tags
- Enter custom tags

Provide MEDIA

- Add at least 1 preview image or video

OPTIONAL

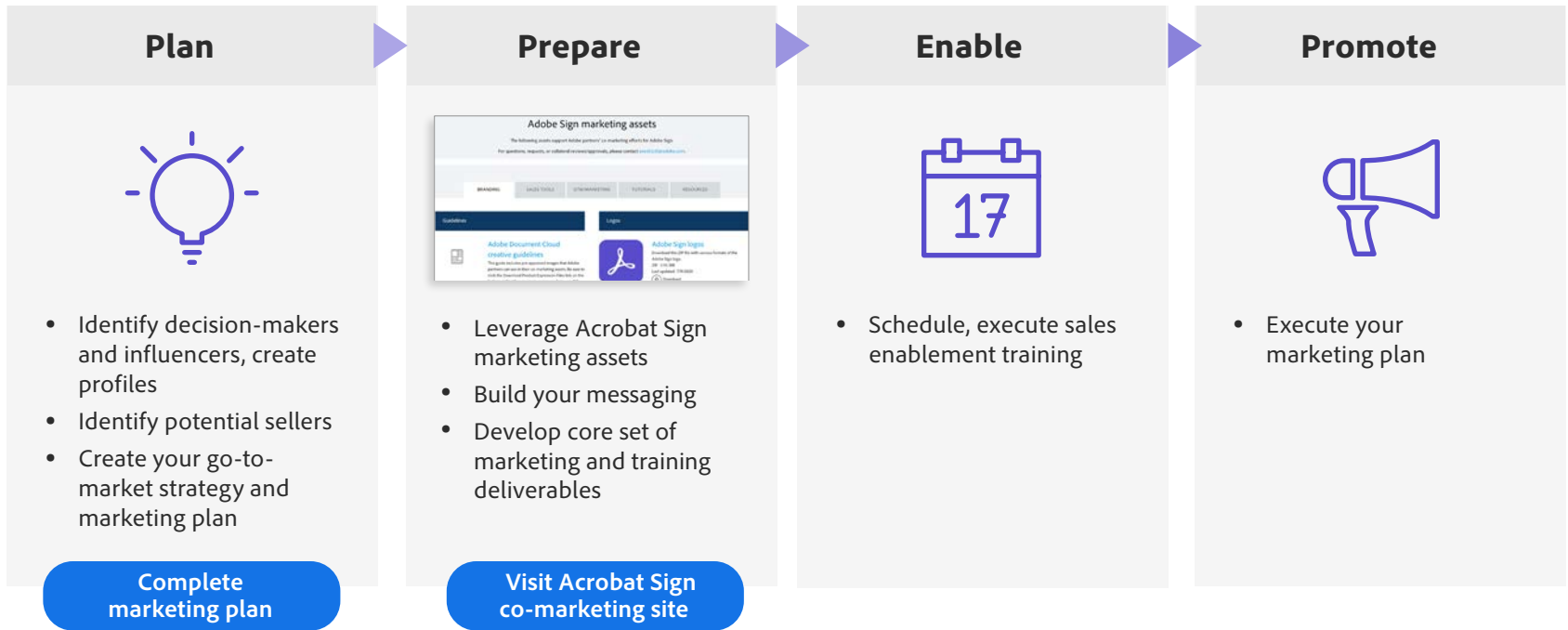
- Add up to 10 documents
- Explain how to sell

Congratulations! You're ready to submit your product listing for the Adobe DC Exchange!

Best practices to promote your new integration.



You'll want to promote your new offering on an ongoing basis. Here are tips and resources to get started.



Ideas to create your Acrobat Sign integration marketing plan

Joint Positioning	Sales Tools	Awareness and Understanding	Evaluation and Credibility	Purchase and Grow
<p>Why e-signatures are essential to your offering and audience</p> <p>Why your solution and Acrobat Sign are better together</p>	<p>Internal enablement presentation</p> <p>Internal FAQ</p> <p>Battlecard</p> <p>Customer-facing pitch deck</p> <p>Demos</p>	<p>New offering + Acrobat Sign web landing page</p> <p>New offering + Acrobat Sign solution brief</p> <p>Other awareness activities such as webinars, campaigns, blog series, etc.</p>	<p>Technical 'how to' content on web, tutorials, best practices</p> <p>'Try before you buy' experience</p> <ul style="list-style-type: none">Consider utilizing the Acrobat Sign 14-day enterprise trial as the foundation so your audience becomes familiar with Acrobat Sign <p>Success stories</p> <p>'How to' tutorials that show prospects how to use the product:</p>	<p>Discount or bundle programs, special promos</p>

Create your own plan

Create your marketing plan

Joint Positioning

Sales Tools

Awareness and Understanding

Evaluation and Credibility

Purchase and Grow