

# Adobe Document Services Security Overview



## Table of Contents

1	Adobe Security
1	About Adobe Document Services
2	Adobe Document Services Hosting and Security
2	PDF Services API Security
2	PDF Embed API Security
3	Adobe Document Services Compliance
3	Other Pertinent Adobe Security Information
3	Conclusion

## Adobe Security

At Adobe, we know the security of your digital experience is important. Security practices are deeply ingrained into our internal software development, operations processes, and tools. These practices are strictly followed by our cross-functional teams to help prevent, detect, and respond to incidents in an expedient manner. We keep up to date with the latest threats and vulnerabilities through our collaborative work with partners, leading researchers, security research institutions, and other industry organizations. We regularly incorporate advanced security techniques into the products and services we offer. This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to secure Adobe Document Services and their associated data.

## About Adobe Document Services

Adobe Document Services gives third-party developers access to some of the same underlying technology used by Adobe products (including Adobe Acrobat DC and Adobe Acrobat Web) via APIs. There are two APIs currently available.

### Adobe PDF Services API

Adobe PDF Services API is a cloud-based service that allows developers to manipulate PDFs in document workflows. Using PDF Services API, developers can:

- Convert files from other formats to PDF files (e.g., HTML to PDF) and PDF files to other formats (e.g., PDF to Microsoft Word)
- Combine multiple PDFs into a single document
- Apply OCR to create searchable and editable PDF files

Developers can implement PDF Services API via SDKs for Node.js, Java, and .NET.

### Adobe PDF Embed API

Adobe PDF Embed API is a client-side JavaScript library that allows developers to embed PDFs and to enable users to view and collaborate on PDFs in any web application. It provides a customizable user interface and out-of-the-box analytics support. With PDF Embed API, developers can:

- Embed PDFs without forcing end users to download additional plug-ins
- Provide a rich PDF viewing experience within their web applications
- Enable digital collaboration and document analytics

Developers implement PDF Embed API through JavaScript, with support for React and Angular frameworks. For a complete list of functionality and other details for these APIs, please [review the product documentation](#).

## Adobe Document Services Hosting and Security

All server-side components of PDF Services API and PDF Embed API are hosted on AWS using standard storage services from the cloud infrastructure provider. Amazon EC2 is a web service that provides automatically scalable compute capacity in the cloud, making web-scale computing easier. Amazon S3 is generally recognized as a highly reliable data storage infrastructure for storing and retrieving any amount of data.

The AWS platform provides services in accordance with industry-standard practices and undergoes regular industry-recognized certifications and audits. You can find more detailed information about AWS and Amazon's security controls on the [AWS Cloud Security website](#).

All content is processed by services running on Amazon Elastic Compute Cloud (Amazon EC2) instances and may be stored temporarily on a combination of Amazon Web Services (AWS) standard storage services—all protected by Identity and Access Management (IAM) roles within that Amazon Web Services (AWS) Region. All content in transit is protected by TLS encryption.

Publicly accessible and downloadable components such as SDKs for the PDF Services API and PDF Embed API JavaScript library are hosted on providers relevant to the component, such as library repositories and CDNs.

For more information about the operational responsibilities of Adobe and AWS, please see the corresponding section in the [Acrobat DC with Document Cloud Service Security Overview](#), starting on page 5.

## PDF Services API Security

### Identity Management

Adobe Identity Management Services (IMS) is used to manage access, including authentication and authorization, to PDF Services API. For more information on the Adobe IMS, please refer to the [Adobe Identity Management Services Security Overview](#).

### API Authentication

PDF Services API currently supports Service Account authentication. For more information on this authentication type, please refer to the [Service Account Integration Overview](#) on adobe.io.

### User-Generated Content Storage

PDF Services API accepts and returns user-generated content (UGC). This content is uploaded to Document Cloud and stored temporarily in cloud storage as part of normal service operations, but it is never stored permanently. AWS US-East (Virginia) regional data centers are used for temporary storage of UGC.

## PDF Embed API Security

### API Authentication

PDF Embed API is a client-side JavaScript- and WASM-based library and does not make any calls to cloud-based services. There are only three purposes for which it makes network calls:

1. At the time of loading, it calls into a service that validates the client.
2. If given an Adobe Analytics report suite ID by the PDF Embed API integrator, it logs event data for out-of-the-box analytics and a pre-configured analytics dashboard.
3. It logs anonymous usage data in Adobe Analytics.

### Iframe Security

The core functionality of PDF Embed API is contained within a sandboxed iframe. This helps prevent any vulnerabilities in the library from affecting the host website and vice versa. It also prevents unintended DOM access and manipulation across the iframe boundary.

## Content Security Policy (CSP)

The content loaded in the iframe is governed by CSP directives that help protect against certain kinds of attacks, including XSS.

## Storage

PDF Embed API does not manage content in cloud storage. Its primary functionality is restricted to loading and rendering PDF files supplied by the client and, when asked to, saving a copy of the loaded file to local drives or external storage.

## Adobe Document Services Compliance

PDF Services API and the domain validation service used by PDF Embed API currently comply with the following regulations:

- SOC2 — a set of security principles that define leading practice controls relevant to security, confidentiality, and privacy.
- ISO 27001:2013 — a set of globally adopted standards that outline stringent security requirements and provide a systematic approach to managing the confidentiality, integrity, and availability of customer information.

**Ultimately, customers are responsible for ensuring compliance with their legal obligations and for making sure that our solutions meet their compliance needs and are secured in an appropriate way.**

For more information about the Adobe Common Controls Framework (CCF) and product/service compliance, please see the [Compliance section on the Adobe Trust Center](#).

## Other Pertinent Adobe Security Information

For more information about Adobe risk and vulnerability management, the Adobe security organization, Adobe secure product development, the Adobe Secure Product Lifecycle (SPLC), the Adobe Software Security Certification Program, and internal Adobe security processes and procedures, please see the [Adobe Acrobat DC with Document Cloud Services security overview](#), starting on page 8.

For more information on the Adobe Software Security Certification Program, please see the [Adobe security culture white paper](#).

## Conclusion

Adobe's proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Document Services and your confidential data. We continuously monitor the evolving threat landscape to stay ahead of malicious activities and help ensure the security of our customers' data.

For more information, please visit the [Adobe Trust Center](#).

